

Jason Hodge

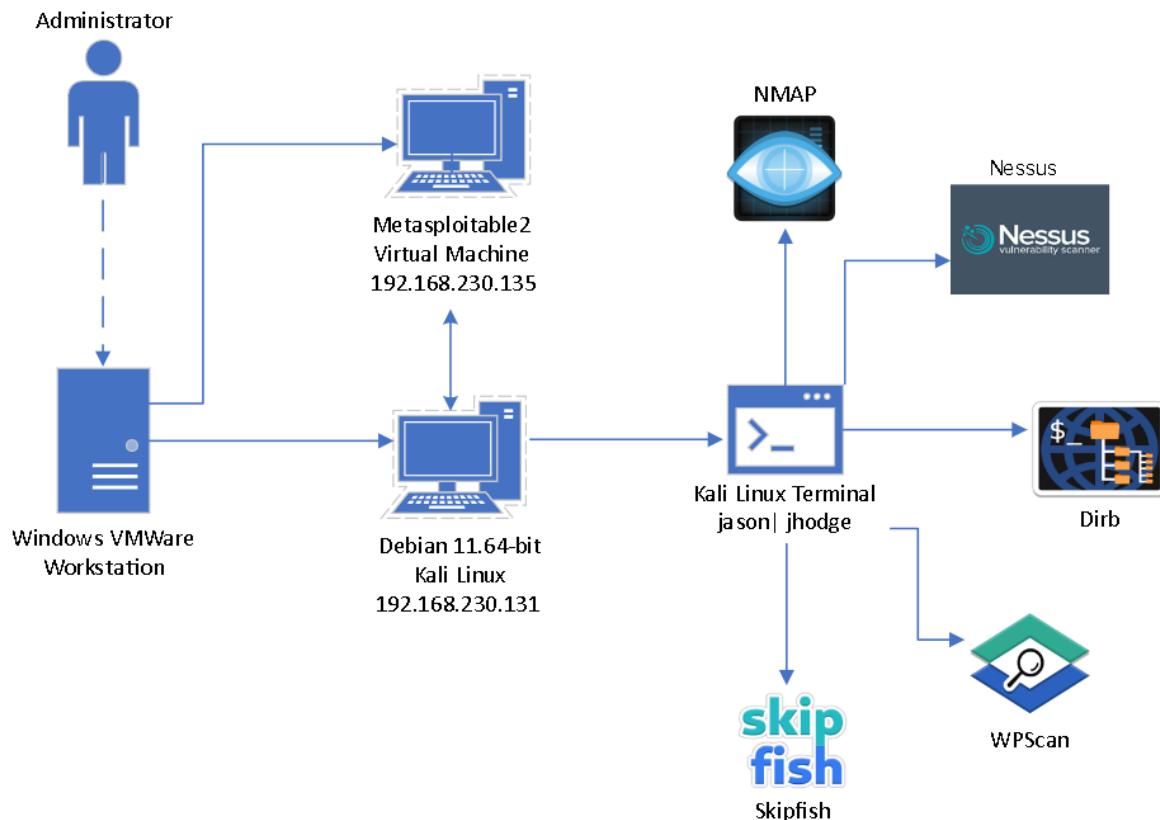
Lab 04 – Scanning the Target for Vulnerabilities

November 8, 2023

Description:

In the first part of this lab, I downloaded the Metasploitable virtual machine (VM) I used as my target VM from my Debian Kali Linux machine. Through using active reconnaissance tools, I discovered lots of information about the Metasploitable VM including numerous security vulnerabilities and open ports where hackers can gain access to the system. Active tools utilized in this lab include NMAP, Nessus, Dirb, WPScan, and Skipfish. All five of these tools are used to find vulnerable areas and openings through ports, services, and application resources. With the discovered information I conducted an analysis of each tool and the results.

Topology:



This is an overview of the entire lab's connections and the active discovery tools used within my Debian Kali Linux machine on VMWare Workstation.

Key Syntax:

- The name of the Kali tool you are using always goes before the command you are running.
- Various commands to download and run all of these tools are included throughout the report.
- The help command for some tools are different from each other.

Verification:

TASK ONE: Active Discovery

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e3:ed:38
          inet addr:192.168.230.135 Bcast:192.168.230.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3:ed38/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:43 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:4461 (4.3 KB) TX bytes:7328 (7.1 KB)
                  Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:16436 Metric:1
                  RX packets:113 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:29705 (29.0 KB) TX bytes:29705 (29.0 KB)
```

First, once the Metasploitable VM was up and running I used the “ifconfig” command to find the IP address of the Metasploitable VM, which is 192.168.230.135.

NMAP: NMAP is an open-source network scanner used to scan ports and IP addresses.

```
(jason@jhodge)-[~]
$ sudo apt install nmap
[sudo] password for jason:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-texttable
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  liblua5.4-0 nmap-common
Suggested packages:
  ncat ndiff zenmap
The following NEW packages will be installed:
  liblua5.4-0
The following packages will be upgraded:
  nmap nmap-common
2 upgraded, 1 newly installed, 0 to remove and 1375 not upgraded.
Need to get 6,293 kB of archives.
After this operation, 414 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 liblua5.4-0 amd64 5.4.4-3 [137 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.94+dfsg1-1kali2 [1,918 kB]
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.94+dfsg1-1kali2 [4,238 kB]
Fetched 6,293 kB in 2s (3,404 kB/s)
Selecting previously unselected package liblua5.4-0:amd64.
(Reading database ... 392667 files and directories currently installed.)
Preparing to unpack .../liblua5.4-0_5.4.4-3_amd64.deb ...
Unpacking liblua5.4-0:amd64 (5.4.4-3) ...
Preparing to unpack .../nmap_7.94+dfsg1-1kali2_amd64.deb ...
Unpacking nmap (7.94+dfsg1-1kali2) over (7.93+dfsg1-0kali2) ...
Preparing to unpack .../nmap-common_7.94+dfsg1-1kali2_all.deb ...
Unpacking nmap-common (7.94+dfsg1-1kali2) over (7.93+dfsg1-0kali2) ...
Setting up nmap-common (7.94+dfsg1-1kali2) ...
Setting up liblua5.4-0:amd64 (5.4.4-3) ...
Setting up nmap (7.94+dfsg1-1kali2) ...
Processing triggers for kali-menu (2023.1.7) ...
Processing triggers for libc-bin (2.36-8) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for wordlists (2023.1.2) ...
```

Here we can see the Kali Linux tool, Nmap being installed on the machine with the command “`sudo apt install nmap`”.

```
(jason@jhodge)@[~]
$ nmap --help
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2, ... ]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
```

```

--script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
    script-categories.

OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
    probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second

FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME], ...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g--source-port <portnum>: Use given port number
--proxies <url1,[url2], ...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
    and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute

```

```

-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.

EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

```

The help command, “--help” shows the available commands that could be utilized in an Nmap scan.

```
└──(jason@jhodge)@[~]
$ nmap -F --script banner 192.168.230.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 19:05 EST
Nmap scan report for 192.168.230.135
Host is up (0.00038s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
|_banner: 220 (vsFTPd 2.3.4)
22/tcp    open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp    open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp    open  smtp
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.230.135]
3306/tcp  open  mysql
|_banner: >\x00\x00\x00\x0A5.0.51a-3ubuntu5\x00\x08\x00\x00\x00\x00p8bfXg~b\x
|_00,\xAA\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
5432/tcp  open  postgresql
5900/tcp  open  vnc
|_banner: RFB 003.003
6000/tcp  open  X11
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
```

This is the most basic command, a simple sped up scan with a banner aimed at our target 192.168.230.135.

```
└─(root@jhodge)-[~]
# nmap -F -sS --script banner 192.168.230.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 19:29 EST
Nmap scan report for 192.168.230.135
Host is up (0.00064s latency).
Not shown: 82 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_banner: 220 (vsFTPD 2.3.4)
22/tcp    open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp    open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp    open  smtp
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.230.135]
3306/tcp  open  mysql
|_banner: >\x00\x00\x00\x0A5.0.51a-3ubuntu5\x00\x09\x00\x00\x00?iu0.4\Q\x
|_00,\xAA\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
5432/tcp  open  postgresql
5900/tcp  open  vnc
|_banner: RFB 003.003
6000/tcp  open  X11
8009/tcp  open  ajp13
MAC Address: 00:0C:29:E3:ED:38 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.20 seconds
```

This is a similar command except I added “-sS” which is called a TCP SYN or Stealth Scan which is the fastest way to scan TCP protocol ports (NMAP.org).

```
└─(root@jhodge)-[~]
# nmap -F -sU --script banner 192.168.230.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 19:32 EST
Nmap scan report for 192.168.230.135
Host is up (0.00034s latency).
Not shown: 93 closed udp ports (port-unreach)
PORT      STATE      SERVICE
53/udp    open       domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open       nfs
MAC Address: 00:0C:29:E3:ED:38 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 102.53 seconds
```

In this scan I used the “-sU” command, which filters out all other ports and only returns UDP.

I also used the “-sA” and “-sT” commands. The first scan was looking for TCP acknowledgement (ACK) to map out firewall rulesets but found nothing. The second scan here is a TCP Connect scan, which uses the system call of the same name to scan instead of relying on packets as other methods shown do (nmap.org).

The results of these scans provided insight into many open TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports that can be leveraged by finding potential vulnerability openings to exploit. There are quite a few ports here that would be interesting to explore deeper to see whether proper precautions have been put in place. Some services I would target in the next phase, if I were to continue would be ports 21, 53, 80, 139, and 445. Port 21, FTP, is a

good port to go after because it allows for data transfer between a server and a PC. In addition, port 53, the domain (DNS), is what manages domain names and IP addresses. Port 80 is our HTTP service, which manages unencrypted web traffic. Furthermore, port 139, the NetBIOS Session provides access to shared resources on the network like files and printers. Lastly, port 445 is similar to data transferred on port 139, except this is a Microsoft port for shared resources. These five ports can all be leveraged by not having proper precautions in place, packet injection attacks, data loss, etc. (Cloud Flare)

Nessus: A vulnerability scanning tool that clearly identifies and explains its discoveries.

The screenshot shows the Tenable Nessus download page. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation is a search bar and a login link. The main content area has a dark background with white text. On the left, a sidebar lists various Tenable products: Tenable Nessus, Tenable Nessus Agent, Tenable Nessus Network Monitor, Tenable Security Center, Integrations, Sensor Proxy, Tenable Log Correlation Engine, Tenable Core, Tenable OT Security, Tenable Identity Exposure, Tenable Web App Scanning, Frictionless, Tenable Cloud Security, and Compliance & Audit Files. The main content area has three sections: 'Download and Install Nessus' (with a 'Download' button), 'Start and Setup Nessus' (with links to curl, Docker, and Virtual Machines), and 'Getting Started' (with a link to documentation). To the right, there's a 'Summary' section with release date (Oct 31, 2023), release notes (Tenable Nessus 10.6.2 Release Notes), and signing keys (RPM-GPG-KEY-Tenable-4096 and RPM-GPG-KEY-Tenable-2048). At the bottom, there are links to Tenable.com, Community & Support, Documentation, Education, and footer links for Privacy Policy, Legal, and 508 Compliance.

The first part of this was downloading and installing Nessus for my Linux Debian machine.

```

└─(root@jhodge)-[/home/jason/Downloads]
└─# dpkg -i Nessus-10.6.2-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 392675 files and directories currently installed.)
Preparing to unpack Nessus-10.6.2-debian10_amd64.deb ...
Unpacking nessus (10.6.2) ...
Setting up nessus (10.6.2) ...
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
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://jhodge:8834/ to configure your scanner

└─(root@jhodge)-[/home/jason/Downloads]
└─# systemctl start nessusd

```

Summary

Release Date: Oct 31, 2023

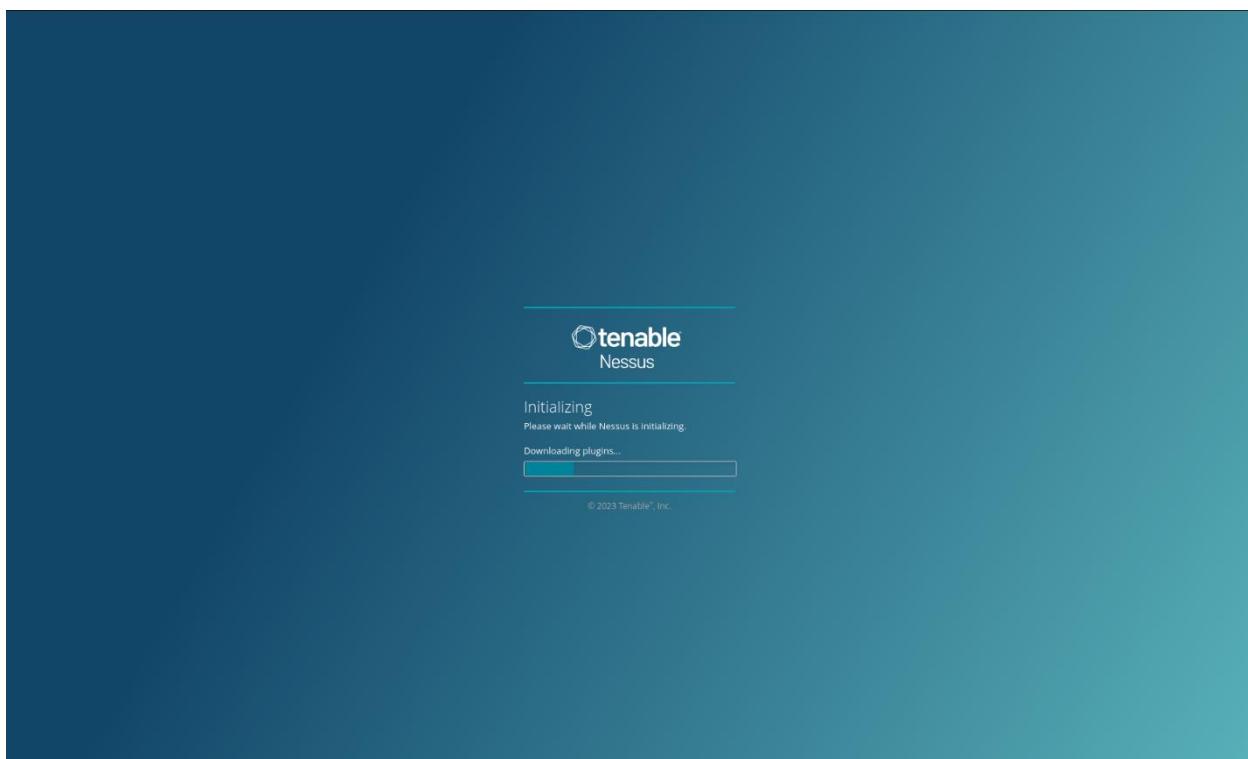
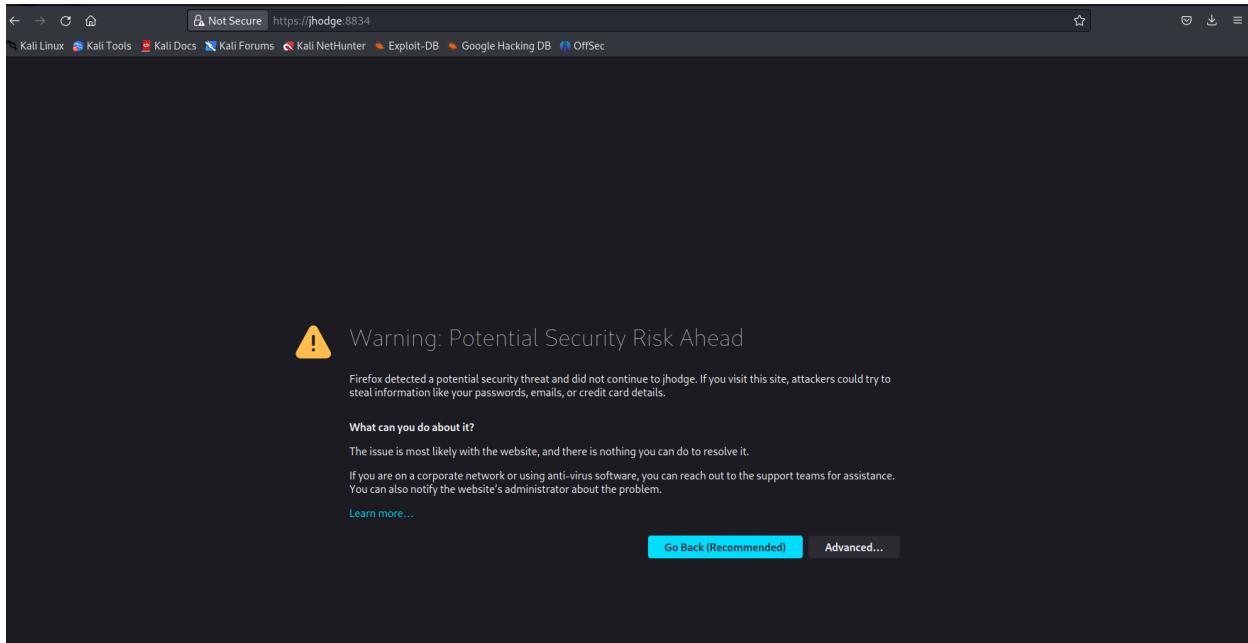
Tenable Nessus 10.6.2 Release Notes

Signing Keys:

RPM-GPG KEY Tenable-4096 (0.4.3.ab)

RPM-GPG KEY Tenable-2048 (0.3.8.be)

This command finishes the install by downloading the file from the downloads folder. Then I started Nessus in the web browser by running the command “systemctl start nessusd” and went to the Nessus scanner browser page <https://jhodge:8834/> to go through the next steps.



When you first run the web browser you get a “Warning: Potential Security Risk Ahead”. From here you click advanced and accept then you need to create an account and put in a Nessus activation code sent to your email address. From here the essential packages and plugins are automatically installed.

https://jhodge:8834/#/scans/folders/my-scans

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

Tenable Nessus Essentials Scans Settings

My Scans

This folder is empty. Create a new scan.

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terascan

Tenable News

Tenable Cyber Watch: GenAI Drives AI Adoption for ... Read More

Scan Templates

Back to Scans

Scanner

DISCOVERY

Host Discovery

A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan

A full system scan suitable for any host.

Advanced Scan

Configure a scan without using any recommendations.

Advanced Dynamic Scan

Configure a dynamic plugin scan without recommendations.

Malware Scan

Scan for malware on Windows and Unix systems.

Mobile Device Scan

Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests

Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass

Remote and local checks for CVE-2017-5689.

Spectre and Meltdown

Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5724.

WannaCry Ransomware

Remote and local checks for MS17-010.

Ripple20 Remote Scan

A remote scan to fingerprint hosts potentially running the Trex stack in the network.

Zerologon Remote Scan

A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate

Remote and local checks to detect Solaris Solorigate vulnerabilities.

ProxyLogon : MS Exchange

Remote and local checks to detect Exchange vulnerabilities targeted by mafuxium.

PrintNightmare

Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan

Look for misconfigurations in Active Directory.

Log4Shell

Detection of Apache Log4j CVE-2021-44228

Log4Shell Remote Checks

Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks

Log4Shell Vulnerability Ecosystem

Detection of Log4Shell Vulnerabilities

CISA Alerts AA22-011A and AA22-047A

Detection of vulnerabilities from recent CISA alerts.

ContiLeaks

Detection of vulnerabilities revealed in the ContiLeaks chats.

Ransomware Ecosystem

Vulnerabilities used by ransomware groups and affiliates.

2022 Threat Landscape Report (TLR)

A scan to detect vulnerabilities featured in our End of Year report.

COMPLIANCE

Cloud Security

PCI DSS

GDPR

HIPAA

PCI DSS

GDPR

HIPAA

Here is the homepage and scans page, which displays the various scans that can be run.

The screenshot shows the Otenable Nessus Essentials interface. At the top, there's a navigation bar with 'Otenable' logo, 'Nessus Essentials', 'Scans', and 'Settings'. On the right side of the top bar, there are user icons for 'jason1' and a profile picture. Below the top bar, there's a sidebar on the left with sections for 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and a search bar labeled 'Search Scans' with a count of '1 Scan'. The main area is titled 'My Scans' and contains a table with columns for 'Name', 'Schedule', and 'Last Scanned'. A single scan entry is listed: 'Metasploitable VM Scan' with 'On Demand' schedule and 'Today at 9:13 PM' last scanned time. There are also 'Import', 'New Folder', and 'New Scan' buttons at the top right of the main area.

Here is a scan that I ran on the Metasploitable VM, IP address: 192.168.230.135.

The screenshot shows the details of the 'Metasploitable VM Scan'. At the top, it says 'Metasploitable VM Scan' and has links for 'Back to My Scans', 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below that, there's a summary bar with counts for 'Hosts' (1), 'Vulnerabilities' (74), 'Remediations' (3), 'Notes' (3), and 'History' (1). There's also a 'Filter' dropdown and a 'Search Hosts' input field. The main content area shows a table for 'Hosts' with one row for '192.168.230.135'. To the right of the table is a 'Scan Details' panel with the following information:

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:13 PM
End:	Today at 9:33 PM
Elapsed:	19 minutes

Below the scan details is a 'Vulnerabilities' section featuring a donut chart. The legend indicates the following colors for severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue). The chart shows a large proportion of vulnerabilities are categorized as 'Info'.

When the scan was completed and opened displayed is the most basic breakdown of what was discovered, color coded based on how critical the vulnerability is.

Metasploitable VM Scan / 192.168.230.135

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Hosts](#)

Vulnerabilities 74

Filter ▾ Search Vulnerabilities 74 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	⋮
CRITICAL	10.0 *	6.7	NFS Exported Share Information Disclosure	RPC	1	🔗
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔗
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	🔗
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	🔗
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔗
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	🔗
MIXED	DNS (Multiple Issues)	DNS	5	🔗
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4	🔗
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	🔗
HIGH	7.5		NFS Shares World Readable	RPC	1	🔗
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	🔗
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	🔗
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	🔗
MIXED	SSL (Multiple Issues)	General	28	🔗
MIXED	ISC Bind (Multiple Issues)	DNS	5	🔗
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔗
MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1	🔗
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	🔗

Host Details

IP: 192.168.230.135
 MAC: 00:0C:29:E3:ED:38
 OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
 Start: Today at 9:13 PM
 End: Today at 9:33 PM
 Elapsed: 19 minutes
 KB: [Download](#)

Vulnerabilities

Critical
High
Medium
Low
Info

<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNc...	Misc.	1		
<input type="checkbox"/>	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1		
<input type="checkbox"/>	MIXED	SSH (Multiple Issues)	Misc.	6		
<input type="checkbox"/>	MIXED	SMB (Multiple Issues)	Misc.	2		
<input type="checkbox"/>	MIXED	TLS (Multiple Issues)	Misc.	2		
<input type="checkbox"/>	MIXED	TLS (Multiple Issues)	SMTP problems	2		
<input type="checkbox"/>	LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1		
<input type="checkbox"/>	LOW	2.6 *		X Server Detection	Service detection	1		
<input type="checkbox"/>	INFO	SMB (Multiple Issues)	Windows	7		
<input type="checkbox"/>	INFO	HTTP (Multiple Issues)	Web Servers	4		
<input type="checkbox"/>	INFO	TLS (Multiple Issues)	General	4		
<input type="checkbox"/>	INFO	FTP (Multiple Issues)	Service detection	3		
<input type="checkbox"/>	INFO	VNC (Multiple Issues)	Service detection	3		
<input type="checkbox"/>	INFO	Apache HTTP Server (Multiple Issues)	Web Servers	2		
<input type="checkbox"/>	INFO	PHP (Multiple Issues)	Web Servers	2		
<input type="checkbox"/>	INFO	RPC (Multiple Issues)	RPC	2		
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	General	2		
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	Service detection	2		
<input type="checkbox"/>	INFO	Web Server (Multiple Issues)	Web Servers	2		
<input type="checkbox"/>	INFO			Nessus SYN scanner	Port scanners	25		
<input type="checkbox"/>	INFO			RPC Services Enumeration	Service detection	10		
<input type="checkbox"/>	INFO			Service Detection	Service detection	9		
<input type="checkbox"/>	INFO			OpenSSL Detection	Service detection	2		

Here we see a narrower breakdown of the results based on severity, the name of the issue, and what family category each falls under.

Metasploitable VM Scan / Plugin #11356

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

Vulnerabilities 74

CRITICAL NFS Exported Share Information Disclosure

Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :
+ /
+ Contents of / :
. .
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz

less...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.230.135

Plugin Details

- Severity: Critical
- ID: 11356
- Version: 1.21
- Type: remote
- Family: RPC
- Published: March 12, 2003
- Modified: August 30, 2023

VPR Key Drivers

- Threat Recency: No recorded events
- Threat Intensity: Very Low
- Exploit Code Maturity: Unproven
- Age of Vuln: 730 days +
- Product Coverage: Low
- CVSSV3 Impact Score: 5.9
- Threat Sources: No recorded events

Risk Information

- Vulnerability Priority Rating (VPR): 6.7
- Risk Factor: Critical
- CVSS v2.0 Base Score: 10.0
- CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

- Exploit Available: true
- Exploit Ease: Exploits are available
- Vulnerability Pub Date: January 1, 1985

Exploitable With

- Metasploit (NFS Mount Scanner)

Here we see the topmost critical vulnerability, which if exploited could give the hacker read and possibly write access on their machine, which could cause tremendous harm to any data contained in the file system. A solution to this problem is also offered, which says to configure the Network File System (NFS) on the host machine.

Metasploitable VM Scan / Plugin #46882

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

Vulnerabilities 74

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output
The remote IRC server is running as :
uid=0(root) gid=0(root)
To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	192.168.230.135

Plugin Details

Severity:	Critical
ID:	46882
Version:	1.16
Type:	remote
Family:	Backdoors
Published:	June 14, 2010
Modified:	April 11, 2022

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
Risk Factor:	Critical
CVSS v2.0 Base Score:	10.0
CVSS v2.0 Temporal Score:	8.3
CVSS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/I/C:A/C
CVSS v2.0 Temporal Vector:	CVSS2#E:F/R:L/OF/RC:C

Vulnerability Information

CPE:	cpe:/a:unrealircd:unrealircd
Exploit Available:	true
Exploit Ease:	Exploits are available
Patch Pub Date:	June 12, 2010
Vulnerability Pub Date:	June 12, 2010

Another critical vulnerability found is an out-of-date software called UnrealIRCd. It appears the current software has a known vulnerability and or is corrupted. The solution would be to delete and reinstall this software.

Metasploitable VM Scan / Plugin #20007

< Back to Vulnerabilities

Configure Audit Trail Launch ▾ Report Export ▾

Vulnerabilities 74

CRITICAL SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as In POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

- <https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>
- <http://www.nessus.org/u7b06c7e95>
- <http://www.nessus.org/u247c4540>
- <https://www.openssl.org/~bodo/ssl-poodle.pdf>
- <http://www.nessus.org/u7d15ba70>
- <https://www.imperialviolate.org/2014/10/14/poodle.html>
- <https://tools.leef.org/html/rfc7507>
- <https://tools.leef.org/html/rfc7568>

Output

```
- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)
```

Name	Code	KEX	Auth	Encryption	MAC
EXP-RC2-CBC-MD5	RSA(512)	RSA	RC2-CBC(40)	MD5	export
EXP-RC4-MD5	RSA(512)	RSA	RC4(40)	MD5	export

more...

To see debug logs, please visit individual host

Port ▾	Hosts
25 / tcp / smtp	192.168.230.135

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
TLS-DHE-RSA-AES256-GCM-SHA384	rsa	rsa	TLS-DHE-RSA-AES256-GCM-SHA384	rsa	

more...

To see debug logs, please visit individual host

Port ▾	Hosts
5432 / tcp / postgresql	192.168.230.135

Plugin Details

Severity: Critical
ID: 20007
Version: 1.34
Type: remote
Family: Service detection
Published: October 12, 2005
Modified: April 4, 2022

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:U/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

In the news: true

We see in this vulnerability the secure socket layer (SSL), which deals with security and integrity, has outdated versions being used, SSL 2.0 and 3.0. Both of these appear to have known

vulnerabilities and out of date cryptographic flaws. The solution provided is to disable SSL 2.0 and 3.0 and replace it with Transport Layer Security (TLS) 1.2 or higher.

The screenshot shows a web-based interface for a security scan. At the top, it says "Metasploitable VM Scan / Plugin #51988" and has links for "Configure", "Audit Trail", "Launch", "Report", and "Export". Below this, a navigation bar includes "Vulnerabilities" (74), "Back to Vulnerabilities", and "Bind Shell Backdoor Detection".

Description: A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution: Verify if the remote host has been compromised, and reinstall the system if necessary.

Output:

```
Nessus was able to execute the command "id" using the following request :  
.....snip.....  
This produced the following truncated output (limited to 10 lines) :  
.....snip.....  
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:/#  
.....snip.....
```

To see debug logs, please visit individual host

Port ▲ Hosts

1524 / tcp / wild_shell 192.168.230.135

Plugin Details:

Severity:	Critical
ID:	51988
Version:	1.10
Type:	remote
Family:	Backdoors
Published:	February 15, 2011
Modified:	April 11, 2022

Risk Information:

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/Ut/N/S/UC/H/I/H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I/C:A:C

This vulnerability is alerting to the fact a shell is listening on the remote port unchecked and an attack could be currently ongoing. The solution would be verifying this connection is compromised and reinstalling the system if needed.

Metasploitable VM Scan / Plugin #33447

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerability Group](#)

Vulnerabilities 74

Critical Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Description
The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.

Solution
Contact your DNS server vendor for a patch.

See Also
<https://www.cnet.com/news/massive-coordinated-dns-patch-released/>
https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/

Output

```
The remote DNS server uses non-random ports for its
DNS requests. An attacker may spoof DNS responses.

List of used ports :
+ DNS Server: 68.129.113.87
|: Port: 61336
|: Port: 61336
|: Port: 61336
|: Port: 61336

To see debug logs, please visit individual host
Port ▲ Hosts
53 / udp / dns 192.168.230.135 ↴
```

Plugin Details

Severity:	Critical
ID:	33447
Version:	1.34
Type:	remote
Family:	DNS
Published:	July 9, 2008
Modified:	November 15, 2018

VPR Key Drivers

Threat Recency:	No recorded events
Threat Intensity:	Very Low
Exploit Code Maturity:	PoC
Age of Vuln:	730 days +
Product Coverage:	Low
CVSSv3 Impact Score:	4
Threat Sources:	No recorded events

Risk Information

Vulnerability Priority Rating (VPR):	6.0
Risk Factor:	High
CVSS v3.0 Base Score 9.1	
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/U:U/S:U/C:N/I:H/A:H
CVSS v3.0 Temporal Vector:	CVSS:3.0/E:P/R:L/O:R/C:C
CVSS v3.0 Temporal Score:	8.2
CVSS v2.0 Base Score:	9.4
CVSS v2.0 Temporal Score:	7.4
CVSS v2.0 Vector:	CVSS2:AV:N/AC:L/Au:N/C:N/I:C/A:C
CVSS v2.0 Temporal Vector:	CVSS2#E:POC/R:LOF/R:CC

Another critical vulnerability is the possibility of a cache poisoning attack, which the DNS server port needs a patch.

Overall, there are many exploitable issues on the Metasploitable VM that if left any longer could lead to potential issues.

Dirb: A Kali tool that scans the content of web servers by using a dictionary-based attack. This can also be sourced from a wordlist text file when looking for web content vulnerabilities.

```
(root@jhodge)-[~]
# sudo apt install dirb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dirb is already the newest version (2.22+dfsg-5).
The following package was automatically installed and is no longer required:
python3-texttable
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1375 not upgraded.
```

Here we are installing Dirb on the machine with the command “`sudo apt install dirb`”.

```

DIRB(1)                               General Commands Manual                  DIRB(1)

NAME
    dirb - Web Content Scanner

SYNOPSIS
    dirb <url_base> <url_base> [<wordlist_file(s)>] [options]

DESCRIPTION
    DIRB IS a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary basesd attack against a web server and analizing the response.

OPTIONS
    -a <agent_string>
        Specify your custom USER_AGENT. (Default is: "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)")

    -b
        Don't squash or merge sequences of ../ or ./ in the given URL.

    -c <cookie_string>
        Set a cookie for the HTTP request.

    -E <certificate>
        Use the specified client certificate file.

    -f
        Fine tunning of NOT_FOUND (404) detection.

    -H <header_string>
        Add a custom header to the HTTP request.

    -i
        Use case-insensitive Search.

    -l
        Print "Location" header when found.

    -N <nf_code>
        Ignore responses with this HTTP code.

    -o <output_file>
        Save output to disk.

    -p <proxy[:port]>
        Use this proxy. (Default port is 1080)

    -P <proxy_username:proxy_password>
        Proxy Authentication.

    -r
        Don't Search Recursively.

    -R
        Interactive Recursion. (Ask in which directories you want to scan)

    -s
        Silent Mode. Don't show tested words. (For dumb terminals)

    -t
        Don't force an ending '/' on URLs.

    -u <username:password>
        Username and password to use.

    -v
        Show Also Not Existnt Pages.

    Manual page dirb(1) line 1/73 80% (press h for help or q to quit)

```

```

    -u <username:password>
        Username and password to use.

    -v
        Show Also Not Existnt Pages.

    -w
        Don't Stop on WARNING messages.

    -x <extensions_file>
        Amplify search with the extensions on this file.

    -X <extensions>
        Amplify search with this extensions.

    -z <milisecs>
        Amplify search with this extensions.

SEE ALSO
    brain(x)

The Dark Raver
Manual page dirb(1) line 16/73 (END) (press h for help or q to quit)

```

27/01/2009

DIRB(1)

Here is the list of scan commands displayed with the “man dirb” command.

```
[root@jhodge ~]# dirb http://192.168.230.135/
```

DIRB v2.22
By The Dark Raver

START_TIME: Mon Nov 6 22:26:22 2023
URL_BASE: http://192.168.230.135/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

```
--- Scanning URL: http://192.168.230.135/ ---
+ http://192.168.230.135/cgi-bin/ (CODE:403|SIZE:296)
=> DIRECTORY: http://192.168.230.135/dav/
+ http://192.168.230.135/index (CODE:200|SIZE:891)
+ http://192.168.230.135/index.php (CODE:200|SIZE:891)
+ http://192.168.230.135/phpinfo (CODE:200|SIZE:48107)
+ http://192.168.230.135/phpinfo.php (CODE:200|SIZE:48119)
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/
+ http://192.168.230.135/server-status (CODE:403|SIZE:301)
=> DIRECTORY: http://192.168.230.135/test/
=> DIRECTORY: http://192.168.230.135/twiki/

--- Entering directory: http://192.168.230.135/dav/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/phpMyAdmin/
+ http://192.168.230.135/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.230.135/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.230.135/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/contrib/
+ http://192.168.230.135/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.230.135/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.230.135/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.230.135/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.230.135/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.230.135/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.230.135/phpMyAdmin/index.php (CODE:200|SIZE:4145)
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/js/
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/lang/
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/libraries/
+ http://192.168.230.135/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.230.135/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.230.135/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.230.135/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.230.135/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.230.135/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.230.135/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.230.135/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.230.135/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.230.135/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.230.135/phpMyAdmin/robots (CODE:200|SIZE:26)
```

```
+ http://192.168.230.135/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.230.135/phpMyAdmin/robots (CODE:200|SIZE:26)
+ http://192.168.230.135/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/scripts/
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/setup/
+ http://192.168.230.135/phpMyAdmin/sql (CODE:200|SIZE:4145)
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/test/
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/themes/
+ http://192.168.230.135/phpMyAdmin/TODO (CODE:200|SIZE:235)
+ http://192.168.230.135/phpMyAdmin/webapp (CODE:200|SIZE:6903)

--- Entering directory: http://192.168.230.135/test/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/twiki/ ---
=> DIRECTORY: http://192.168.230.135/twiki/bin/
+ http://192.168.230.135/twiki/data (CODE:403|SIZE:298)
+ http://192.168.230.135/twiki/index (CODE:200|SIZE:782)
+ http://192.168.230.135/twiki/index.html (CODE:200|SIZE:782)
=> DIRECTORY: http://192.168.230.135/twiki/lib/
+ http://192.168.230.135/twiki/license (CODE:200|SIZE:19440)
=> DIRECTORY: http://192.168.230.135/twiki/pub/
+ http://192.168.230.135/twiki/readme (CODE:200|SIZE:4334)
+ http://192.168.230.135/twiki/templates (CODE:403|SIZE:303)

--- Entering directory: http://192.168.230.135/phpMyAdmin/contrib/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/phpMyAdmin/js/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/phpMyAdmin/lang/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/phpMyAdmin/libraries/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/phpMyAdmin/scripts/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/phpMyAdmin/setup/ ---
+ http://192.168.230.135/phpMyAdmin/setup/config (CODE:303|SIZE:1373)
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/setup/frames/
+ http://192.168.230.135/phpMyAdmin/setup/index (CODE:200|SIZE:8622)
+ http://192.168.230.135/phpMyAdmin/setup/index.php (CODE:200|SIZE:8630)
=> DIRECTORY: http://192.168.230.135/phpMyAdmin/setup/lib/
+ http://192.168.230.135/phpMyAdmin/setup/scripts (CODE:200|SIZE:21967)
+ http://192.168.230.135/phpMyAdmin/setup/styles (CODE:200|SIZE:6218)

--- Entering directory: http://192.168.230.135/phpMyAdmin/test/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
```

```

--- Entering directory: http://192.168.230.135/phpMyAdmin/themes/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/twiki/bin/ ---
+ http://192.168.230.135/twiki/bin/attach (CODE:200|SIZE:4362)
+ http://192.168.230.135/twiki/bin/changes (CODE:200|SIZE:21791)
+ http://192.168.230.135/twiki/bin/edit (CODE:200|SIZE:5351)
+ http://192.168.230.135/twiki/bin/manage (CODE:302|SIZE:0)
+ http://192.168.230.135/twiki/bin/passwd (CODE:302|SIZE:0)
+ http://192.168.230.135/twiki/bin/preview (CODE:302|SIZE:0)
+ http://192.168.230.135/twiki/bin/register (CODE:302|SIZE:0)
+ http://192.168.230.135/twiki/bin/save (CODE:302|SIZE:0)
+ http://192.168.230.135/twiki/bin/search (CODE:200|SIZE:3554)
+ http://192.168.230.135/twiki/bin/statistics (CODE:200|SIZE:1142)
+ http://192.168.230.135/twiki/bin/upload (CODE:302|SIZE:0)
+ http://192.168.230.135/twiki/bin/view (CODE:200|SIZE:10054)
+ http://192.168.230.135/twiki/bin/viewfile (CODE:302|SIZE:0)

--- Entering directory: http://192.168.230.135/twiki/lib/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/twiki/pub/ ---
+ http://192.168.230.135/twiki/pub/favicon.ico (CODE:200|SIZE:1078)
⇒ DIRECTORY: http://192.168.230.135/twiki/pub/Main/

--- Entering directory: http://192.168.230.135/phpMyAdmin/setup/frames/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/phpMyAdmin/setup/lib/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.230.135/twiki/pub/Main/

```

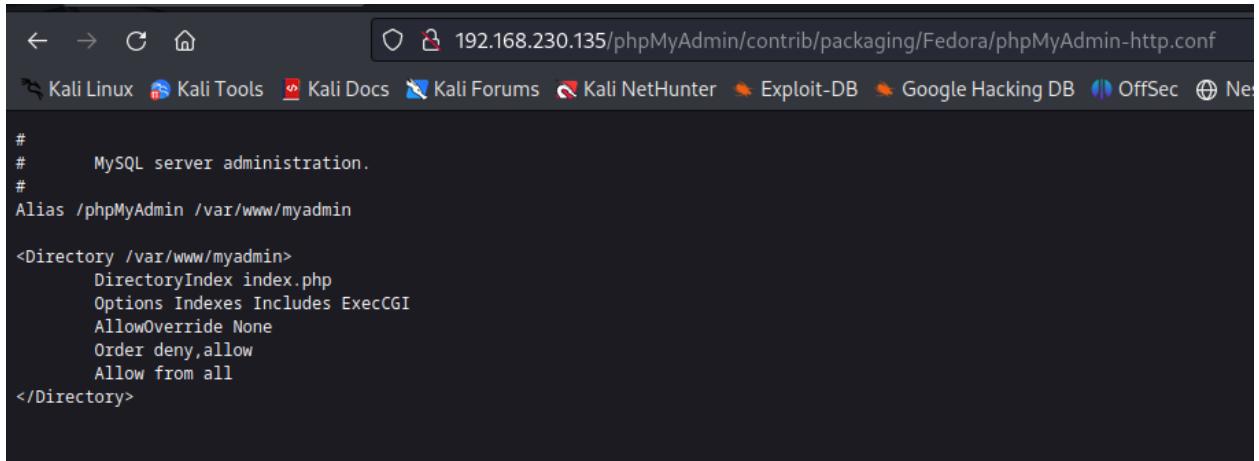
END_TIME: Mon Nov 6 22:26:42 2023
DOWNLOADED: 32284 - FOUND: 56

Here I ran a basic Dirb scan on the Metasploitable VM <http://192.168.230.135/>. With this test I scanned for web content objects.

Index of /phpMyAdmin/contrib/packaging/Fedora

Name	Last modified	Size	Description
Parent Directory		-	
phpMyAdmin-http.conf	09-Dec-2008 12:24	227	
phpMyAdmin.spec	09-Dec-2008 12:24	6.1K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.230.135 Port 80



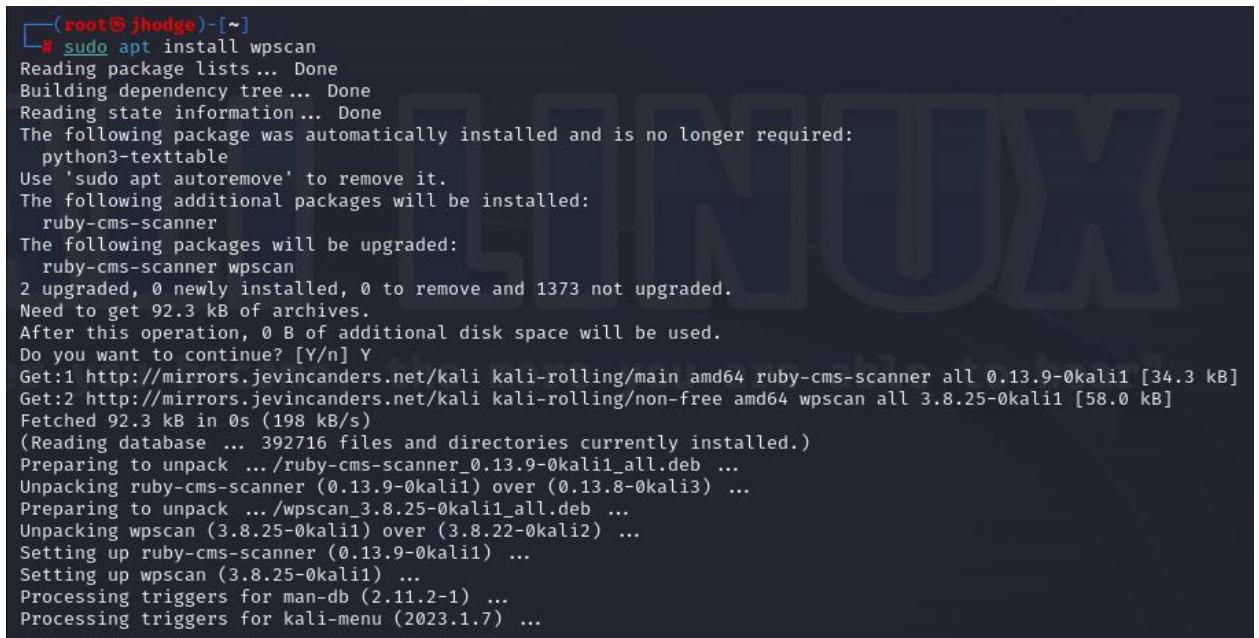
```
# MySQL server administration.
#
# Alias /phpMyAdmin /var/www/myadmin

<Directory /var/www/myadmin>
    DirectoryIndex index.php
    Options Indexes Includes ExecCGI
    AllowOverride None
    Order deny,allow
    Allow from all
</Directory>
```

At the completion of the scan, this is the directory and contents of a file.

With this tool we are searching for possible sensitive webpages hackers can obtain information about. I thought this tool would be good practice to use, since it checks for different information than many others. In the future it would be good to run this test with a premade wordlist text file to get even more results or even narrowed to specific results. With this test I did find access to 56 directories, mostly webpage background running processes.

WPScan: This tool searches for numerous vulnerabilities pertaining to the WordPress version installed, plugins installed, username enumeration, etc.



```
[root@jhodge ~]# sudo apt install wpscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
python3-texttable
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
ruby-cms-scanner
The following packages will be upgraded:
ruby-cms-scanner wpscan
2 upgraded, 0 newly installed, 0 to remove and 1373 not upgraded.
Need to get 92.3 kB of archives.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 ruby-cms-scanner all 0.13.9-0kali1 [34.3 kB]
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 wpscan all 3.8.25-0kali1 [58.0 kB]
Fetched 92.3 kB in 0s (198 kB/s)
(Reading database ... 392716 files and directories currently installed.)
Preparing to unpack .../ruby-cms-scanner_0.13.9-0kali1_all.deb ...
Unpacking ruby-cms-scanner (0.13.9-0kali1) over (0.13.8-0kali3) ...
Preparing to unpack .../wpscan_3.8.25-0kali1_all.deb ...
Unpacking wpscan (3.8.25-0kali1) over (3.8.22-0kali2) ...
Setting up ruby-cms-scanner (0.13.9-0kali1) ...
Setting up wpscan (3.8.25-0kali1) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for kali-menu (2023.1.7) ...
```

Here we can see the Kali Linux tool, wpscan being installed on the machine with the command “sudo apt install wpscan”.

```
[root@jhodge ~]# wpscan --help
  \  ^__\  \    /  ^__\ 
   \    \|  /  \|  \ 
    ^  _ \|  \|  _ \ 
     \| \| \| \| \| \| 
WordPress Security Scanner by the WPScan Team
Version 3.8.25

 @_WPScan_, @_ethicalhack3r, @_erwan_lr, @_firefart

Usage: wpscan [options]
      --url URL          The URL of the blog to scan
                           Allowed Protocols: http, https
                           Default Protocol if none provided: http
                           This option is mandatory unless update or help or hh or version is/are supplied
      -h, --help           Display the simple help and exit
      --hh               Display the full help and exit
      --version          Display the version and exit
      -v, --verbose        Verbose mode
      --[no-]banner       Whether or not to display the banner
                           Default: true
      -o, --output FILE   Output to FILE
      -f, --format FORMAT Output results in the format supplied
                           Available choices: cli-no-colour, cli-no-color, json, cli
                           Default: mixed
                           Available choices: mixed, passive, aggressive
      --user-agent, --ua VALUE
      --random-user-agent, --rua
      --http-auth login:password
      -t, --max-threads VALUE
                           Use a random user-agent for each scan
                           The max threads to use
                           Default: 5
                           Milliseconds to wait before doing another web request. If used, the max threads will be set to 1.
                           The request timeout in seconds
                           Default: 60
                           The connection timeout in seconds
                           Default: 30
                           Disables SSL/TLS certificate verification, and downgrade to TLS1.0+ (requires cURL 7.66 for the latter)
                           Supported protocols depend on the cURL installed
      --cookie-string COOKIE
      --cookie-jar FILE-PATH
                           Cookie string to use in requests, format: cookie1=value1[; cookie2=value2]
                           File to read and write cookies
                           Default: /tmp/wpscan/cookie_jar.txt
      --force             Do not check if the target is running WordPress or returns a 403
      --[no-]update       Whether or not to update the Database
      --api-token TOKEN   The WPScan API Token to display vulnerability data, available at https://wpscan.com/profile
      --wp-content-dir DIR
      --wp-plugins-dir DIR
                           The wp-content directory if custom or not detected, such as "wp-content"
                           The plugins directory if custom or not detected, such as "wp-content/plugins"
      -e, --enumerate [OPTS]
                           Enumeration Process
                           Available Choices:
                           vp  Vulnerable plugins
                           ap  All plugins
                           p   Popular plugins
                           vt Vulnerable themes
```

```
p  Popular plugins
vt Vulnerable themes
at All themes
t  Popular themes
tt Timthumbs
cb Config backups
dbe Db exports
u   User IDs range. e.g: u1-5
     Range separator to use: '-'
     Value if no argument supplied: 1-10
m   Media IDs range. e.g m1-15
     Note: Permalink setting must be set to "Plain" for those to be detected
     Range separator to use: '-'
     Value if no argument supplied: 1-100
Separator to use between the values: ','
Default: All Plugins, Config Backups
Value if no argument supplied: vp,vt,tt,cb,dbe,u,m
Incompatible choices (only one of each group/s can be used):
- vp, ap, p
- vt, at, t
Exclude all responses matching the Regexp (case insensitive) during parts of the enumeration.
Both the headers and body are checked. Regexp delimiters are not required.
Use the supplied mode to enumerate Plugins.
Default: passive
Available choices: mixed, passive, aggressive
Use the supplied mode to check plugins' versions.
Default: mixed
Available choices: mixed, passive, aggressive
Exclude usernames matching the Regexp/string (case insensitive). Regexp delimiters are not required.
List of passwords to use during the password attack.
If no --username/s option supplied, user enumeration will be run.
List of usernames to use during the password attack.
Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt'
Maximum number of passwords to send by request with XMLRPC multicall
Default: 500
Force the supplied attack to be used rather than automatically determining one.
Multicall will only work against WP < 4.4
Available choices: wp-login, xmlrpc, xmlrpc-multicall
The URL of the login page if different from /wp-login.php
Alias for --random-user-agent --detection-mode passive --plugins-version-detection passive

[!] To see full list of options use --hh.
```

The help command, “--help” shows the available commands that could be utilized with WPScan.

```
[root@jhodge ~]# wpscan --url http://192.168.230.135
```

```
Wordpress Security Scanner by the WPScan Team
Version 3.8.25
```

```
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
[i] Updating the Database ...
[i] Update completed.
```

```
Scan Aborted: The remote website is up, but does not seem to be running WordPress.
```

Here is a first initial scan and it appears the host, Metasploitable VM, is not running WordPress. This is actually a good thing since it stopped the test before it began.


```
(jason@jhodge:[~]
$ sudo apt install skipfish
[sudo] password for jason:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
skipfish is already the newest version (2.10b-2kali7).
skipfish set to manually installed.
The following package was automatically installed and is no longer required:
  python3-texttable
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1378 not upgraded.
```

Here we can see Skipfish being installed on the machine using the command “`sudo apt install skipfish`”.

```
(jason@jhodge:[~]
$ skipfish -h
skipfish web application scanner - version 2.10b
Usage: skipfish [ options ... ] -W wordlist -o output_dir start_url [ start_url2 ... ]

Authentication and access options:
-A user:pass      - use specified HTTP authentication credentials
-F host=IP        - pretend that 'host' resolves to 'IP'
-C name=val       - append a custom cookie to all requests
-H name=val       - append a custom HTTP header to all requests
-B (i|f|p)         - use headers consistent with MSIE / Firefox / iPhone
-N                - do not accept any new cookies
--auth-form url   - form authentication URL
--auth-user user   - form authentication user
--auth-pass pass   - form authentication password
--auth-verify-url - URL for in-session detection

Crawl scope options:
-d max_depth      - maximum crawl tree depth (16)
-c max_child       - maximum children to index per node (512)
-x max_desc        - maximum descendants to index per branch (8192)
-r r_limit          - max total number of requests to send (100000000)
-p crawl%          - node and link crawl probability (100%)
-q hex             - repeat probabilistic scan with given seed
-I string          - only follow URLs matching 'string'
-X string          - exclude URLs matching 'string'
-K string          - do not fuzz parameters named 'string'
-D domain          - crawl cross-site links to another domain
-B domain          - trust, but do not crawl, another domain
-Z                - do not descend into 5xx locations
-O                - do not submit any forms
-P                - do not parse HTML, etc, to find new links

Reporting options:
-o dir            - write output to specified directory (required)
-M                - log warnings about mixed content / non-SSL passwords
-E                - log all HTTP/1.0 / HTTP/1.1 caching intent mismatches
-U                - log all external URLs and e-mails seen
-Q                - completely suppress duplicate nodes in reports
-u                - be quiet, disable realtime progress stats
-v                - enable runtime logging (to stderr)

Dictionary management options:
-W wordlist        - use a specified read-write wordlist (required)
-S wordlist        - load a supplemental read-only wordlist
-L                - do not auto-learn new keywords for the site
-Y                - do not fuzz extensions in directory brute-force
-R age             - purge words hit more than 'age' scans ago
-T name=val        - add new form auto-fill rule
-G max_guess       - maximum number of keyword guesses to keep (256)
-z sigfile         - load signatures from this file

Performance settings:
-g max_conn        - max simultaneous TCP connections, global (40)
-m host_conn       - max simultaneous connections, per target IP (10)
-f max_fail        - max number of consecutive HTTP errors (100)
-t req_tmout       - total request response timeout (20 s)
```

The help command, “`-h`” shows the available commands that could be utilized in a Skipfish scan.

```
(jason@jhodge:[~] $ skipfish -o Skipfish http://192.168.230.135/wordpress
skipfish version 2.10b by lcamtuf@google.com
- 192.168.230.135 -
Scan statistics:
  Scan time : 0:29:35.191
  HTTP requests : 607846 (343.7/s), 2106546 kB in, 274571 kB out (1341.3 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 12 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 6275 total (99.7 req/conn)
  TCP faults : 0 failures, 12 timeouts, 1 purged
  External links : 1151989 skipped
  Reqs pending : 17503

Database statistics:
  Pivots : 2190 total, 1735 done (79.22%) application/binary
  In progress : 226 pending, 86 init, 20 attacks, 123 dict
  Missing nodes : 567 spotted
  Node types : 1 serv, 356 dir, 326 file, 593 pinfo, 574 unkn, 339 par, 1 val
  Issues found : 2015 info, 7 warn, 49 low, 456 medium, 5 high impact
  Dict size : 1259 words (1259 new), 23 extensions, 256 candidates
  Signatures : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 2190
[+] Looking for duplicate entries: 2190
[+] Counting unique nodes: 1121
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 2190
[+] Generating summary views ...
[+] Report saved to 'Skipfish/index.html' [0xb2e03fbb].
[+] This was a great day for science!
```

This shows the brief results of the Skipfish test I ran. In order to gain a substantial amount of data I let this test run for a while and eventually ended the test. As I stated above, I chose not to limit the crawl search depth time in an effort to give the search time to find those high impact potential threats. The command I used saved the index.html file to the folder Skipfish. As you can see, I discovered 5 high impact, 456 medium, 49 low, 7 warn, and 2015 information issues.

← → ⌛ file:///home/jason/Skipfish/index.html ⌂

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Lo...

skipfish
WEB APP SCANNER

Scanner version: 2.10b Random seed: 0xb2e03fb Scan date: Tue Nov 7 17:27:41 2023 Total time: 0 hr 29 min 35 sec 238 ms Problems with this scan? Click here for advice.

Crawl results - click to expand:

<http://192.168.230.135/> !5 !117 !42 !6 !826 !1119
Code: 200, Length: 694, declared: text/html, charset: [none] | Show trace +

Document type overview - click to expand:

application/binary (3)
 application/javascript (14)
 application/xhtml+xml (100)
 image/gif (8)
 image/jpeg (2)
 image/png (11)
 image/x-ms-bmp (1)
 text/css (8)
 text/html (115)
 text/plain (47)
 text/xml (7)

Issue type overview - click to expand:

! **Query injection vector** (2)
1. <http://192.168.230.135/dvwa/login.php?9-8> [show trace +]
Memo: response suggests arithmetic evaluation on server side (type 1)
2. <http://192.168.230.135/mutillidae/set-up-database.php?%00> [show trace +]
Memo: response to " different than to '\\"'
! **Shell injection vector** (3)
1. <http://192.168.230.135/dvwa/login.php?true%00> [show trace +]
Memo: responses to 'true' and 'false' different than to 'uname'
2. <http://192.168.230.135/mutillidae/set-up-database/?true%00> [show trace +]
Memo: responses to 'true' and 'false' different than to 'uname'
3. <http://192.168.230.135/mutillidae/set-up-database.php?%true%00> [show trace +]
Memo: responses to 'true' and 'false' different than to 'uname'
! **Signature match detected (higher risk)** (2)
1. <http://192.168.230.135/mutillidae/owasp-esapi-php/lib/apache-log4php/trunk/src/examples/php/server.php> [show trace +]
Memo: PHP inclusion errors (during traversal tests) (sig: 51001)
2. <http://192.168.230.135/mutillidae/index.php?page=text-file-viewer.php> [show trace +]
Memo: PHP inclusion errors (during traversal tests) (sig: 51001)

Issue type overview - click to expand:

● Query injection vector (2)

1. <http://192.168.230.135/dvwa/login.php?9-8> [show trace +]
Memo: response suggests arithmetic evaluation on server side (type 1)
2. [http://192.168.230.135/mutillidae/set-up-database.php/\"](http://192.168.230.135/mutillidae/set-up-database.php/\) [show trace +]
Memo: response to " different than to \\\"

● Shell injection vector (3)

1. <http://192.168.230.135/dvwa/login.php/`true`> [show trace +]
Memo: responses to 'true' and 'false' different than to 'uname'
2. <http://192.168.230.135/mutillidae/set-up-database/`true`> [show trace +]
Memo: responses to 'true' and 'false' different than to 'uname'
3. <http://192.168.230.135/mutillidae/set-up-database.php/`true`> [show trace +]
Memo: responses to 'true' and 'false' different than to 'uname'

● Signature match detected (higher risk) (2)

1. <http://192.168.230.135/mutillidae/owasp-esapi-php/lib/apache-log4php/trunk/src/examples/php/server.php> [show trace +]
Memo: PHP inclusion errors (during traversal tests) (sig: 51001)
2. <http://192.168.230.135/mutillidae/index.php?page=text-file-viewer.php> [show trace +]
Memo: PHP inclusion errors (during traversal tests) (sig: 51001)

● Interesting server message (22)

● Interesting file (8)

● Incorrect or missing charset (higher risk) (34)

● Generic MIME type (higher risk) (1)

● Incorrect or missing MIME type (higher risk) (1)

● External content embedded on a page (higher risk) (6)

● XSS vector in document body (43)

● Signature match detected (1)

● Incorrect caching directives (lower risk) (18)

● HTML form with no apparent XSRF protection (16)

● External content embedded on a page (lower risk) (7)

● Resource fetch failed (6)

● Numerical filename - consider enumerating (19)

● Incorrect or missing charset (low risk) (194)

● Generic MIME used (low risk) (44)

● Incorrect or missing MIME type (low risk) (79)

● File upload form (1)

● Password entry form - consider brute-force (10)

● HTML form (not classified otherwise) (1)

● Unknown form field (can't autocomplete) (15)

● Hidden files / directories (29)

● Directory listing enabled (329)

● Server error triggered (1)

● Resource not directly accessible (1)

● New 404 signature seen (1)

● New 'X-*' header value seen (123)

● New 'Server' header value seen (1)

● New HTTP cookie added (7)

Most of the results of this scan are all relatively low risk, but there are some high risks that need some attention. That being said, there are a couple vulnerable areas for SQL injection and OS shell injection attacks, which can potentially be dangerous. A hacker can perform SQL injection attacks by querying their way into a part of a database through an application page, if this page is a login page it can be a greater security risk as they can get their hands on login information and user records. The Metasploitable VM is also vulnerable to OS shell injection attacks where “an attacker to execute operating system (OS) commands on the server that is running an application, and typically fully compromise the application and its data (Port Swigger).”

I like how self-explanatory this tool is in showing issues and traces within a system. I have used this tool before and thought it would be good practice. I also like the vulnerability information it displays.

Conclusion:

Everything went smoothly in this lab as I was able to accurately run all five of the active security tools, the two chosen and the three I chose. With these tools I was able to gain quite a bit of knowledge about the Metasploitable virtual machine to go a step further with information I gathered.

Furthermore, I believe the results I gained from these tools were beneficial, even though WPScan did not amount to much. The only other thing I would do is take more time to sift through the data found by some of the tools I used.

References:

Command-line flags: Nmap network scanning. Command-line Flags | Nmap Network Scanning. (n.d.). <https://nmap.org/book/port-scanning-options.html>

Dirb: Kali linux tools. Kali Linux. (2023a, August 10). <https://www.kali.org/tools/dirb/>

Ibeakanma, C. (2023, February 4). How to install nessus on Kali Linux. MUO. <https://www.makeuseof.com/how-to-install-nessus-kali-linux/>

Skipfish: Kali linux tools. Kali Linux. (2023b, March 8). <https://www.kali.org/tools/skipfish/>

What is a computer port? | ports in Networking | Cloudflare. CloudFlare. (n.d.). <https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/>

What is Os Command Injection, and how to prevent it?: Web security academy. What is OS command injection, and how to prevent it? | Web Security Academy. (n.d.). <https://portswigger.net/web-security/os-command-injection>

WPSCAN: Kali linux tools. Kali Linux. (2023c, August 10). <https://www.kali.org/tools/wpscan/>