Jason Hodge

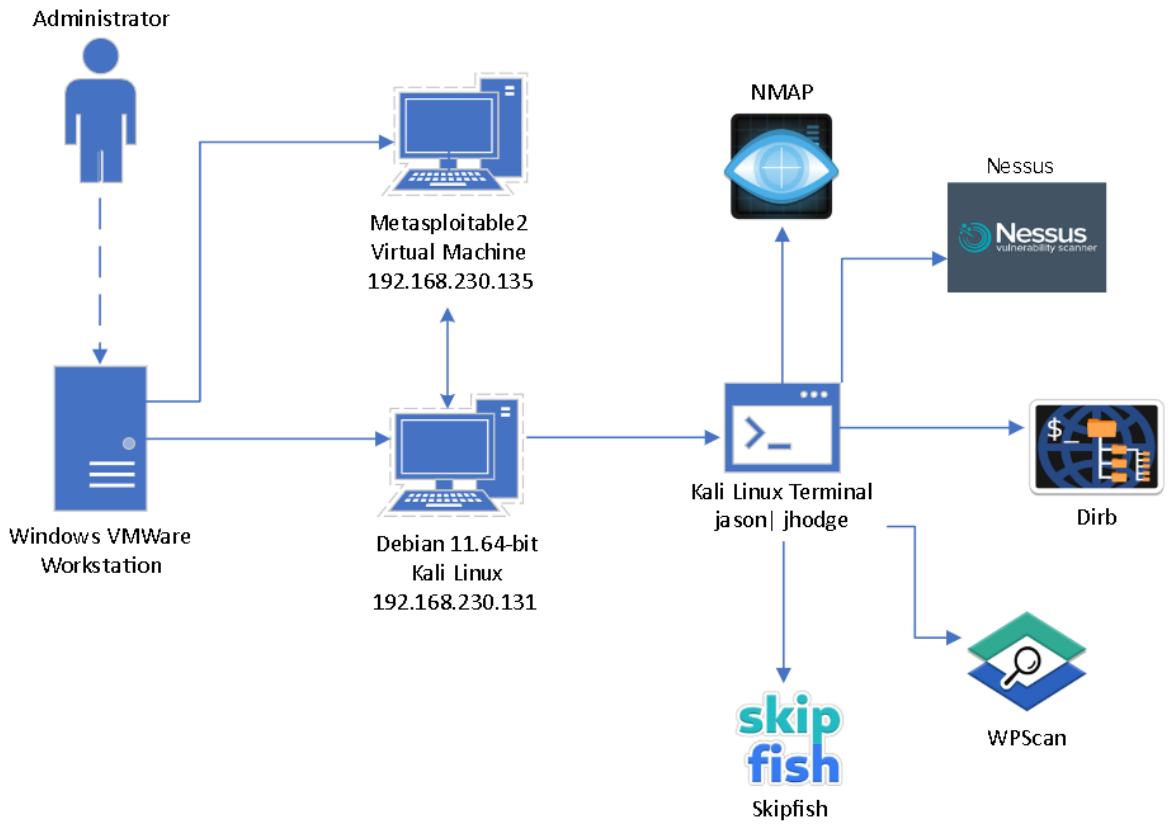
Lab 04 – Scanning the Target for Vulnerabilities

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:



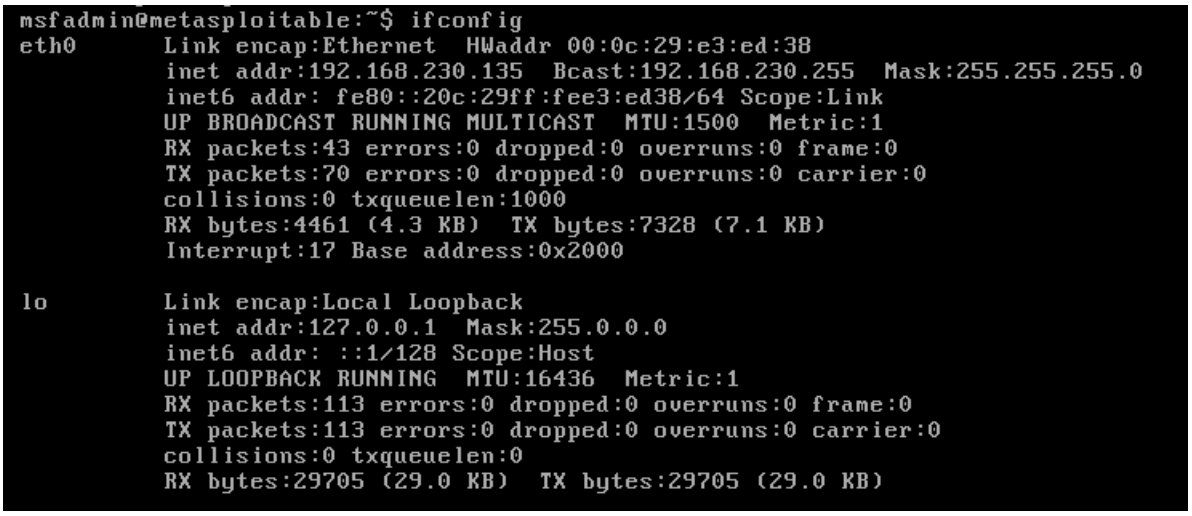
This is an overview of the entire lab's connections and the active discovery tools used within my Debian Kali Linux machine on VMWare Workstation.

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.

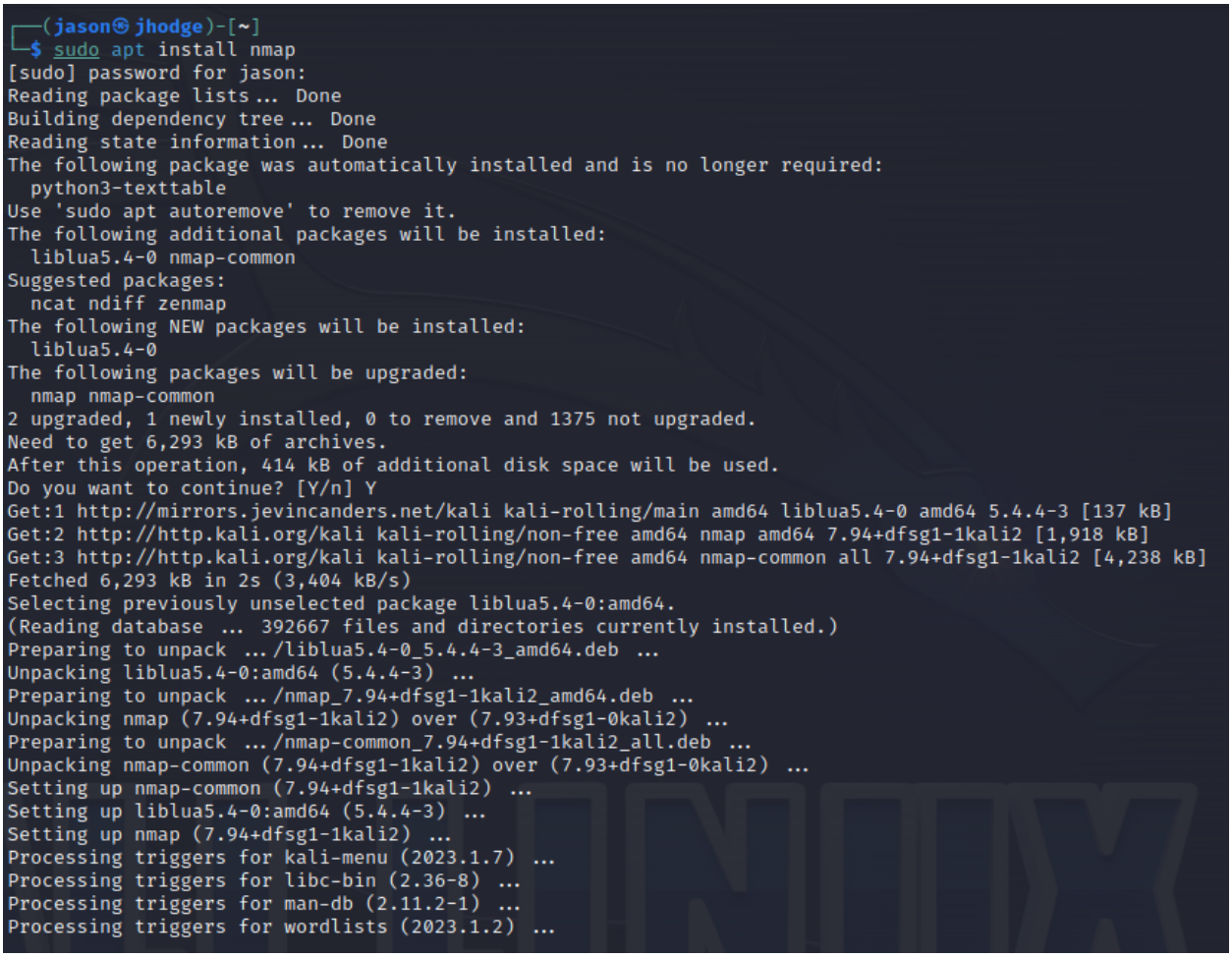
Verification:

TASK ONE: Active Discovery



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.



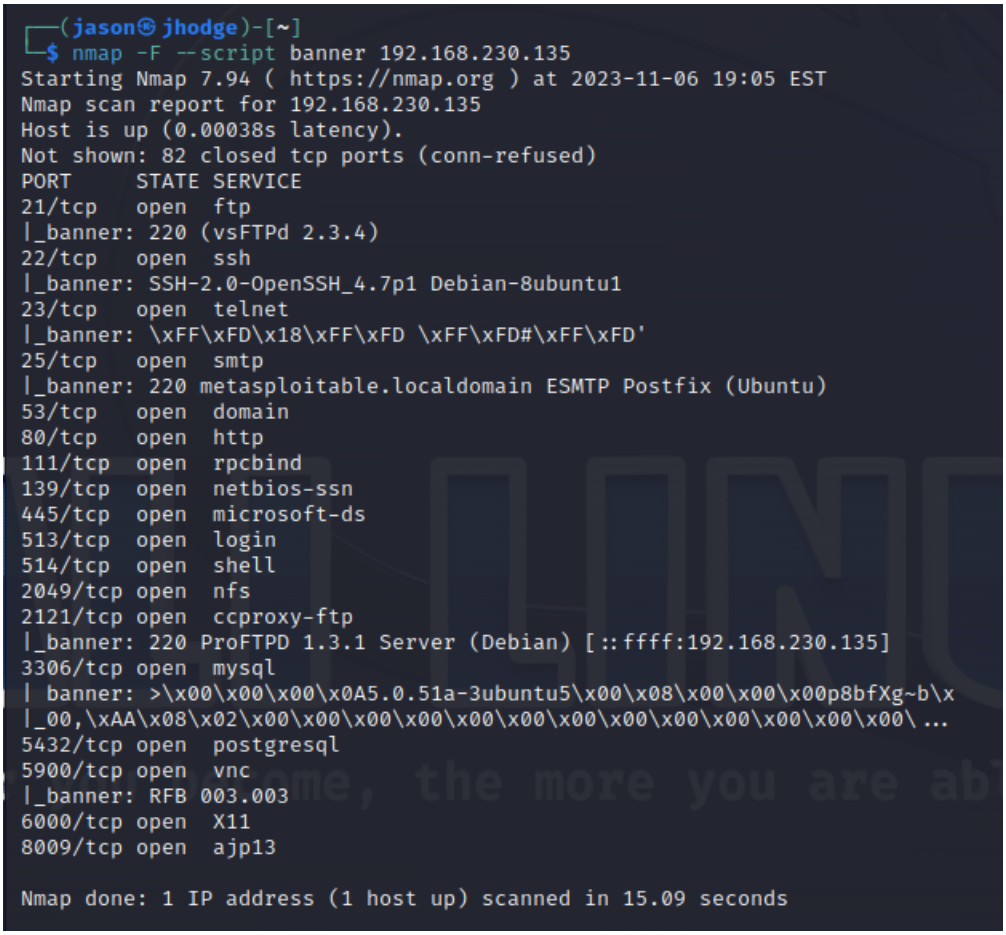
Here we can see the Kali Linux tool, Nmap being installed on the machine with the command “sudo apt install nmap”.

```
┌──(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/PU/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.



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\ ...
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.

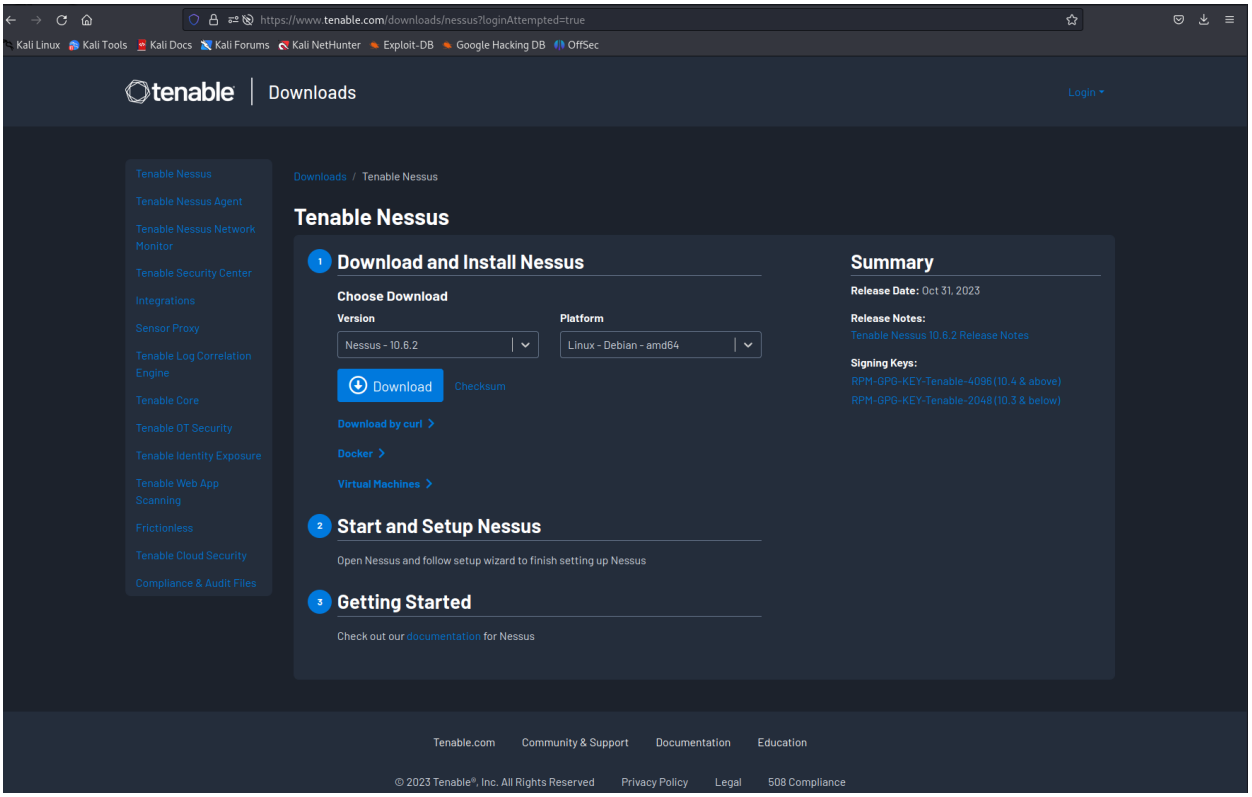
```
┌──(root㉿jhodge)-[~]
└─# nmap -F -sA --script banner 192.168.230.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 19:40 EST
Nmap scan report for 192.168.230.135
Host is up (0.00018s latency).
All 100 scanned ports on 192.168.230.135 are in ignored states.
Not shown: 100 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:E3:ED:38 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.83 seconds

┌──(root㉿jhodge)-[~]
└─# nmap -F -sT --script banner 192.168.230.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 19:44 EST
Nmap scan report for 192.168.230.135
Host is up (0.00034s 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\x0C\x00\x00\x00IO2J^{o:\x
|_00,\xAA\x08\x02\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 15.14 seconds
```

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).

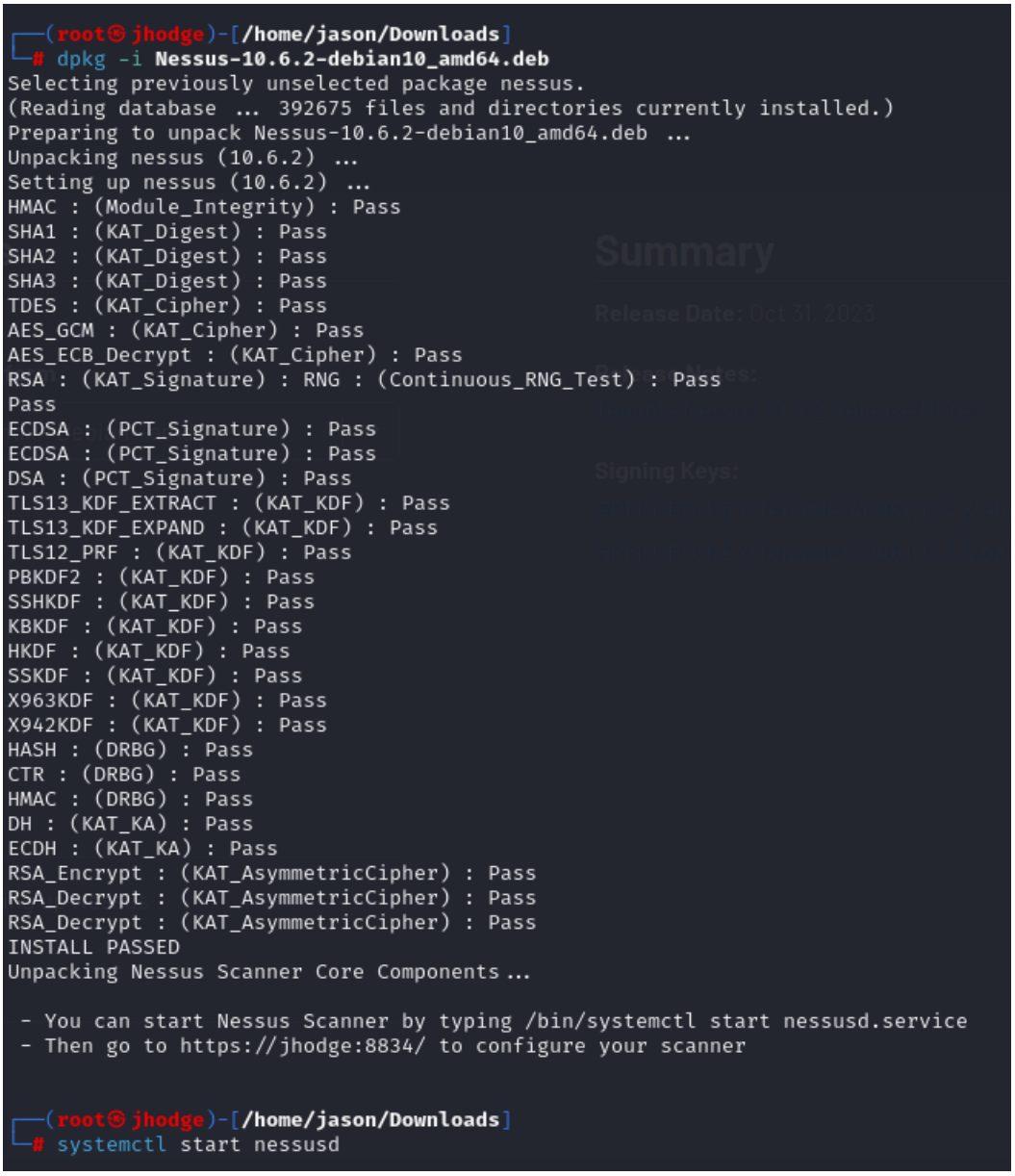
The results of these scans provided insight into many open TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports that can be leveraged by finding potential vulnerability openings to exploit. There are quite a few ports here that would be interesting to explore deeper to see whether 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)

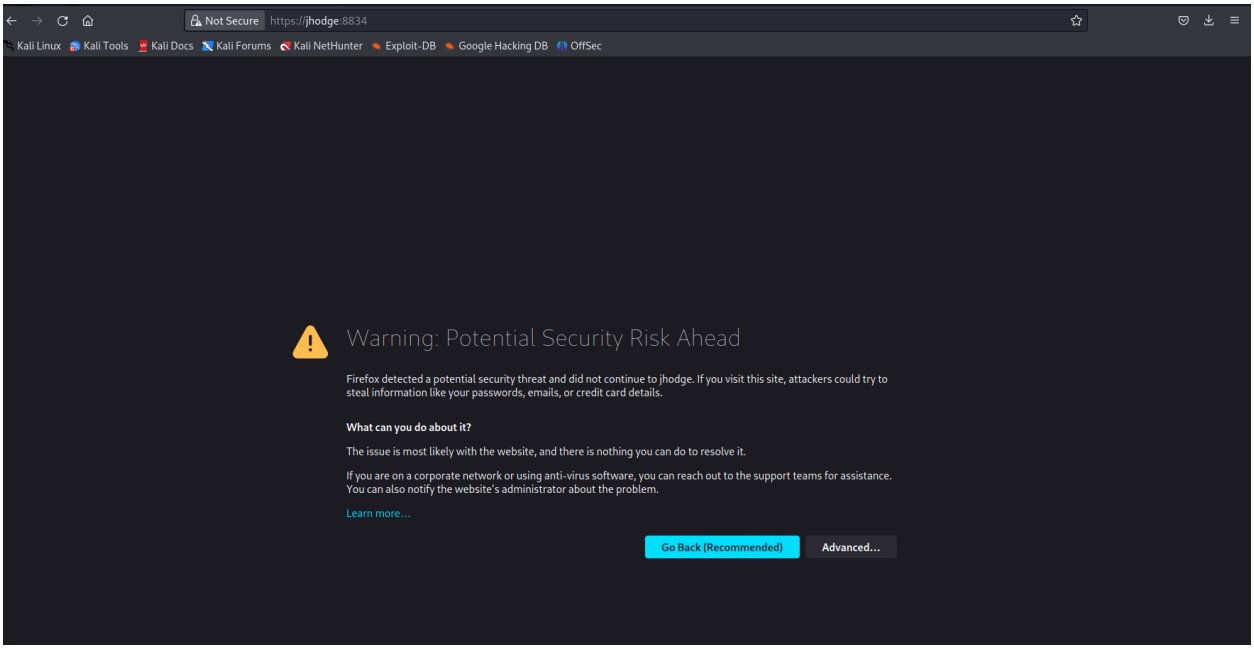
Nessus: A vulnerability scanning tool that clearly identifies and explains its discoveries.

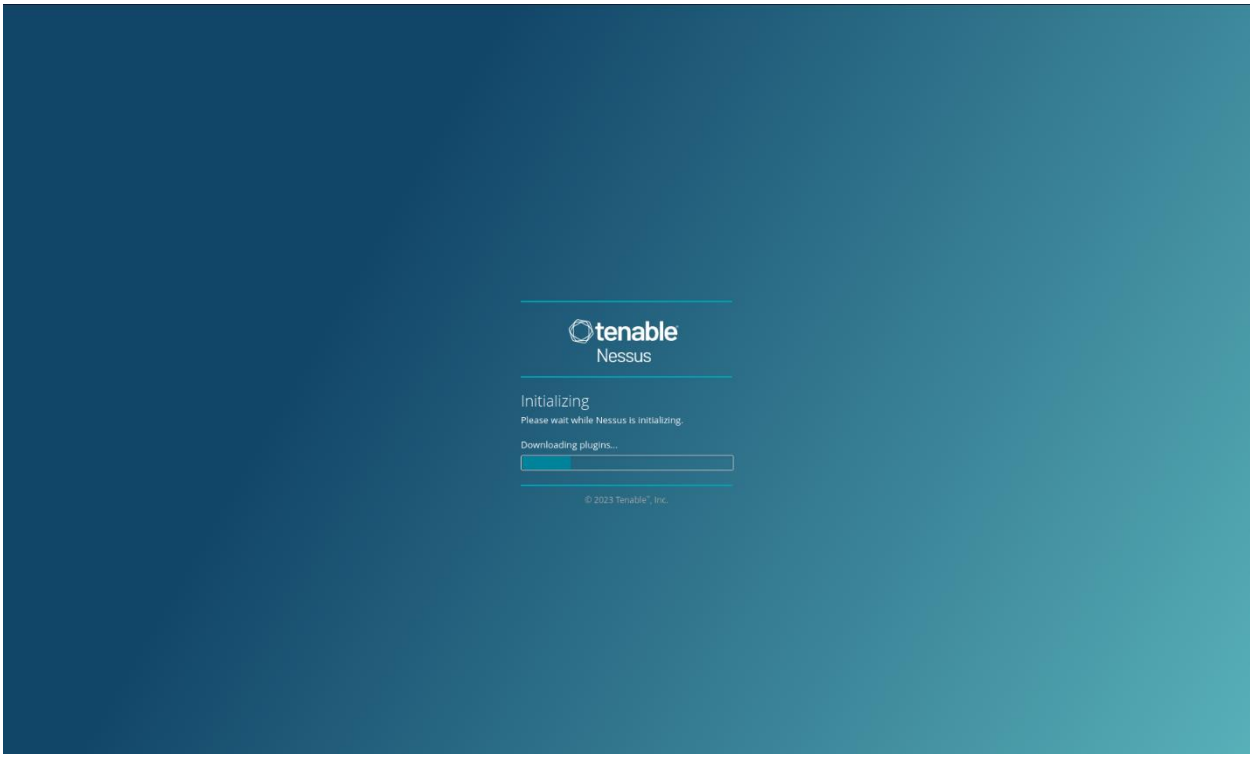


The first part of this was downloading and installing Nessus for my Linux Debian machine.

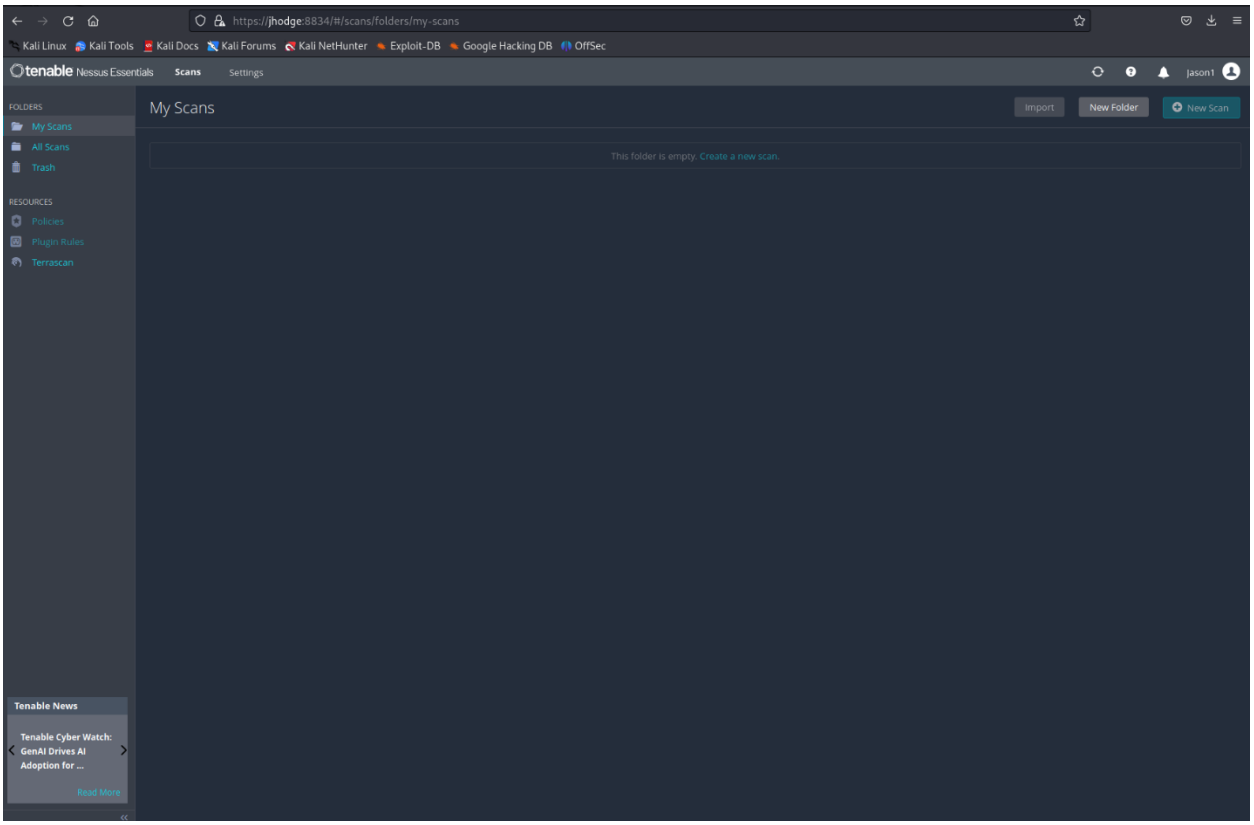


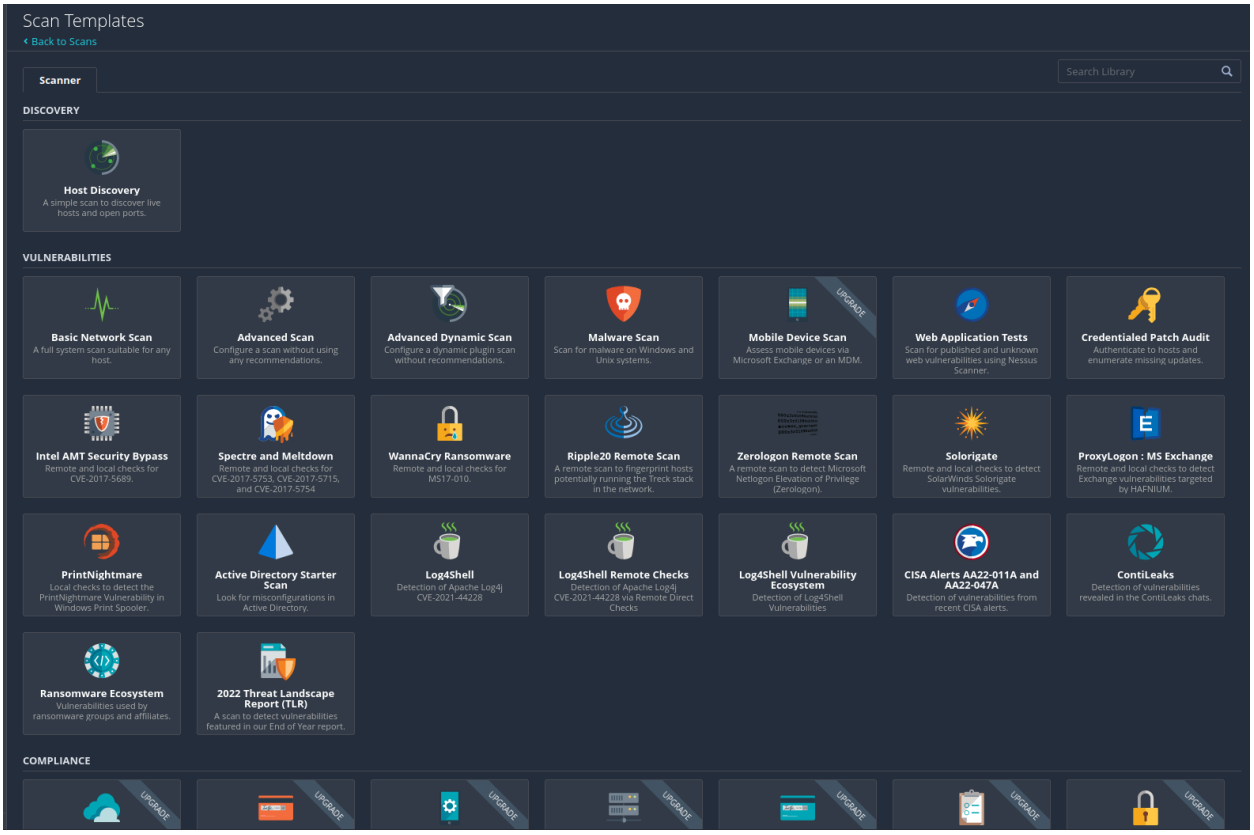
This command finishes the install by downloading the file from the downloads folder. Then I started Nessus in the web browser by running the command “systemctl start nessusd” and went to the Nessus scanner browser page https://jhodge:8834/ to go through the next steps.



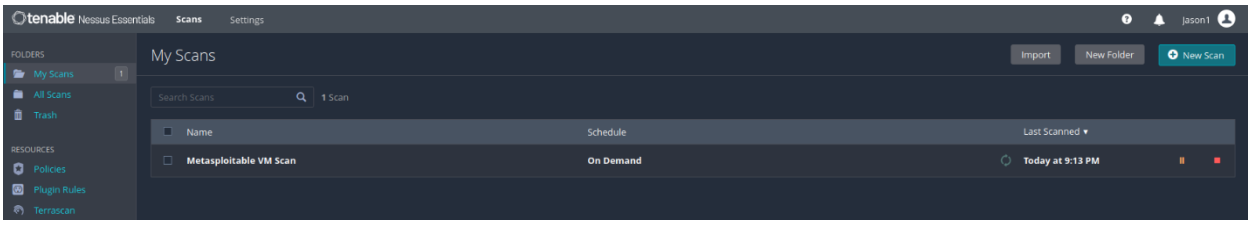


When you first run the web browser you get a “Warning: Potential Security Risk Ahead”. From here you click advanced and accept then you need to create an account and put in a Nessus activation code sent to your email address. From here the essential packages and plugins are automatically installed.

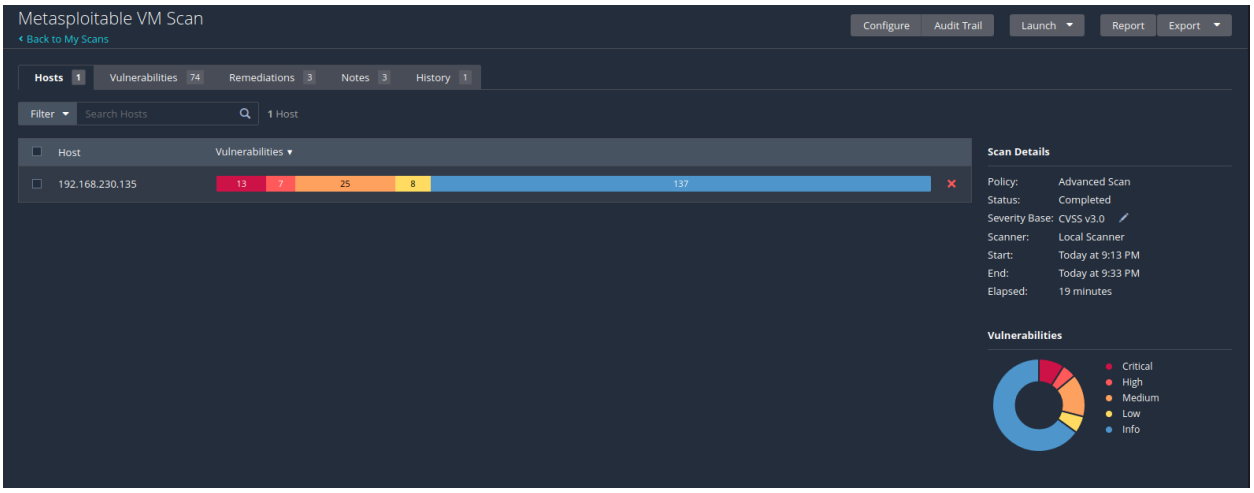

https://jhodge:8834/#/scans/folders/my-scans
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
tenable Nessus Essentials
Scans
Settings
jason1
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
Tenable News
Tenable Cyber Watch: GenAI Drives AI Adoption for ...
Read More


Scan Templates
Back to Scans
Scanner
Search Library
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-2017-5754
WannaCry Ransomware
Remote and local checks for MS17-010.
Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck 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 SolarWinds Solorigate vulnerabilities.
ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.
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
UPGRADE

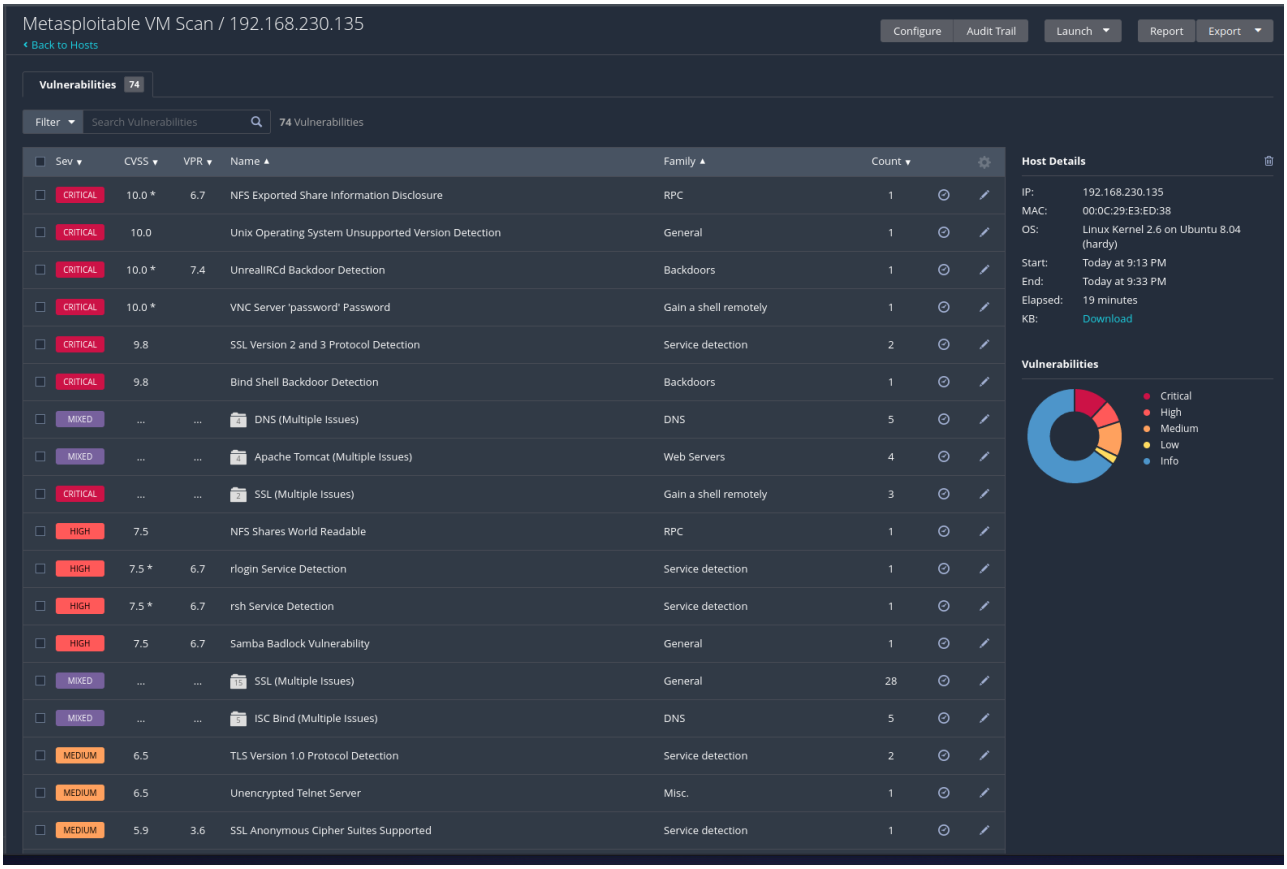
Here is the homepage and scans page, which displays the various scans that can be run.

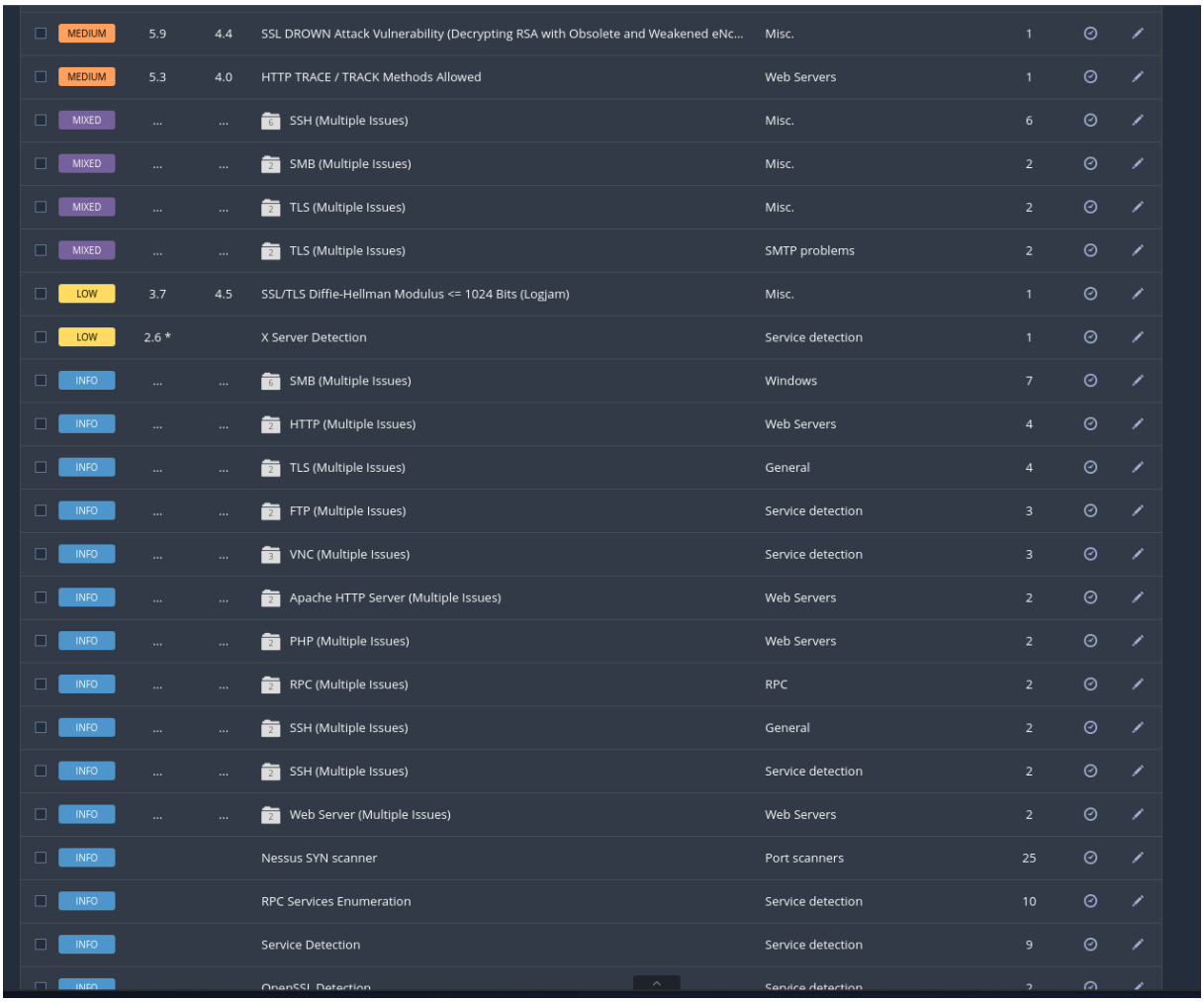


Here is a scan that I ran on the Metasploitable VM, IP address: 192.168.230.135.



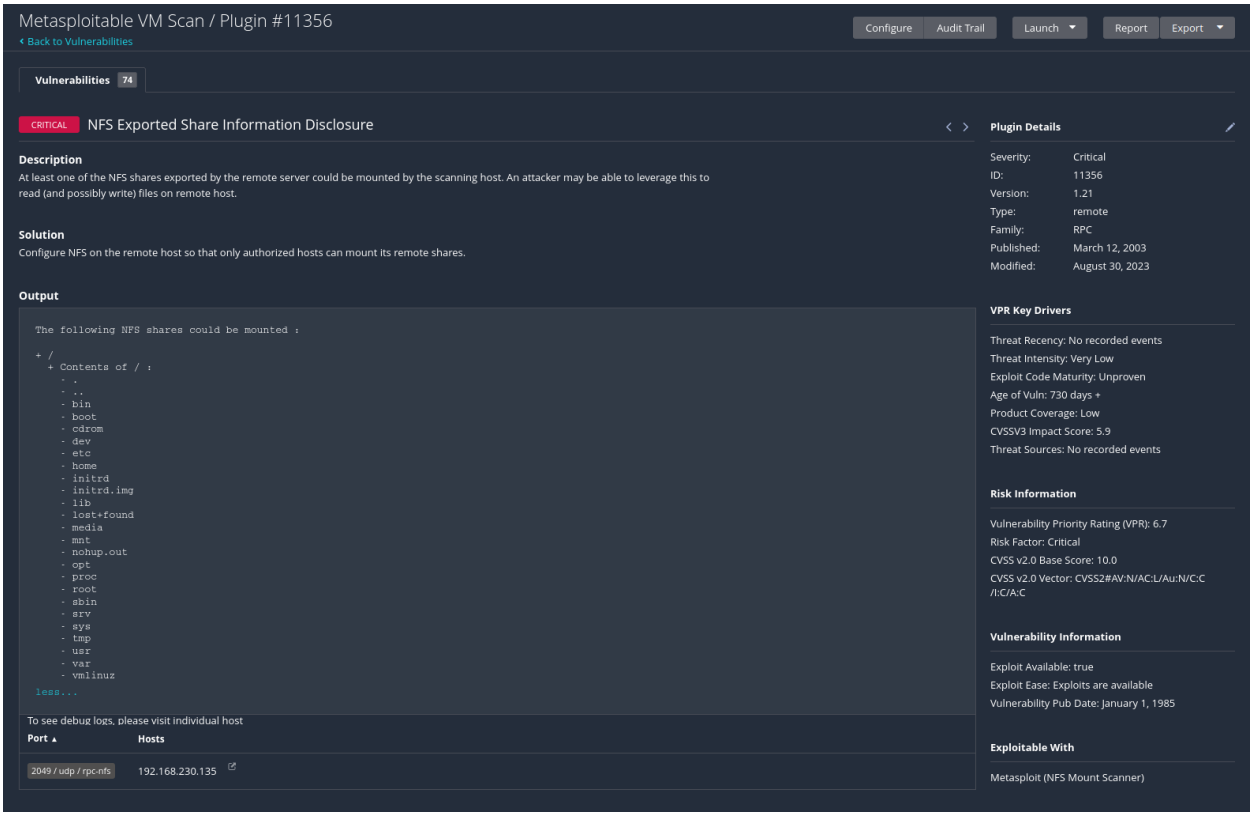
When the scan was completed and opened displayed is the most basic breakdown of what was discovered, color coded based on how critical the vulnerability is.


Metasploitable VM Scan / 192.168.230.135
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
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 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

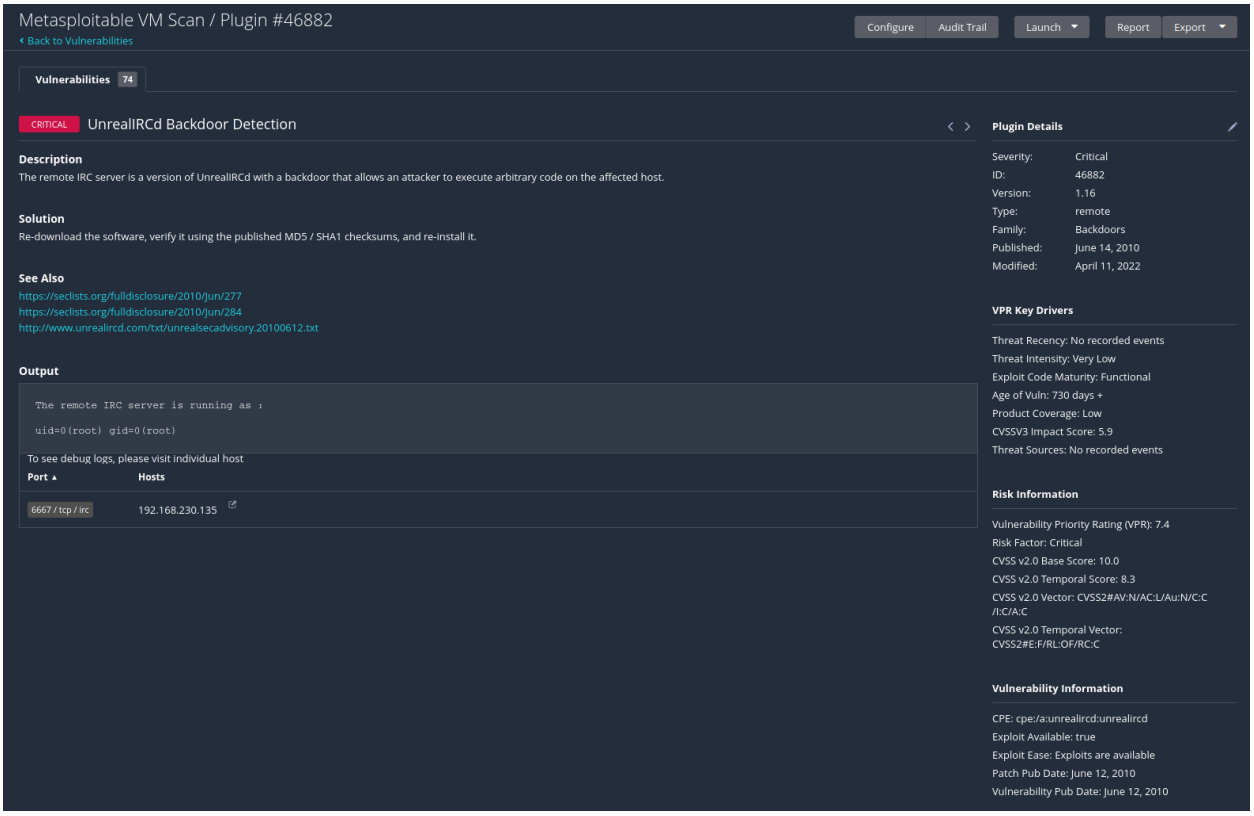


MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNc...	Misc.	1	
MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	
MIXED	...	...	SSH (Multiple Issues)	Misc.	6	
MIXED	...	...	SMB (Multiple Issues)	Misc.	2	
MIXED	...	...	TLS (Multiple Issues)	Misc.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

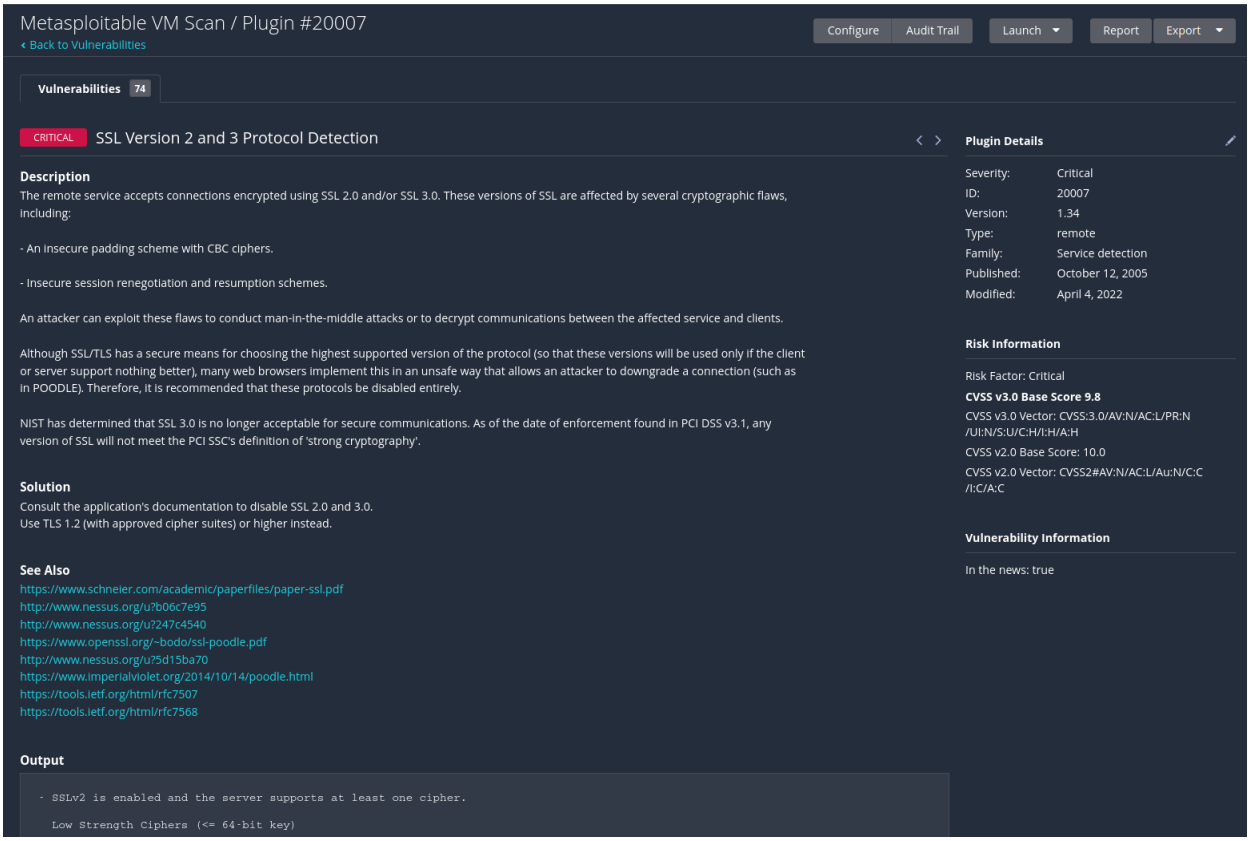
Here we see a narrower breakdown of the results based on severity, the name of the issue, and what family category each falls under.

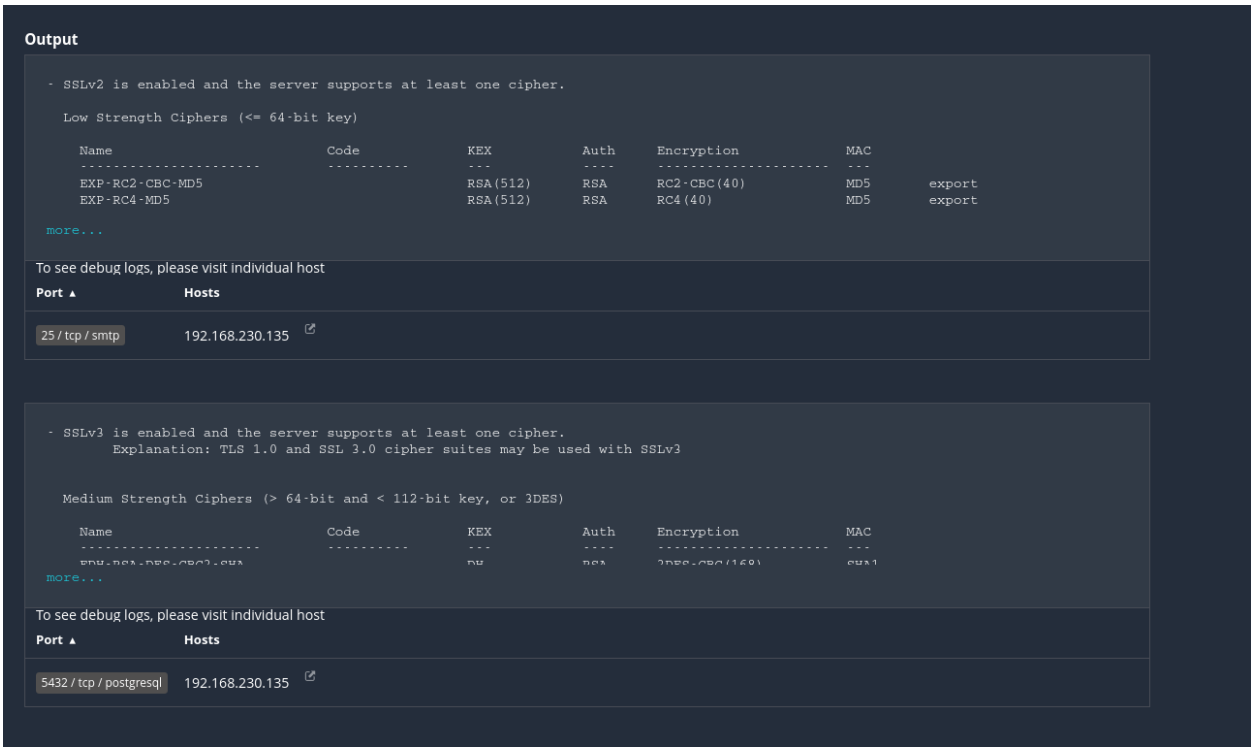


Here we see the topmost critical vulnerability, which if exploited could give the hacker read and possibly write access on their machine, which could cause tremendous harm to any data contained in the file system. A solution to this problem is also offered, which says to configure the Network File System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



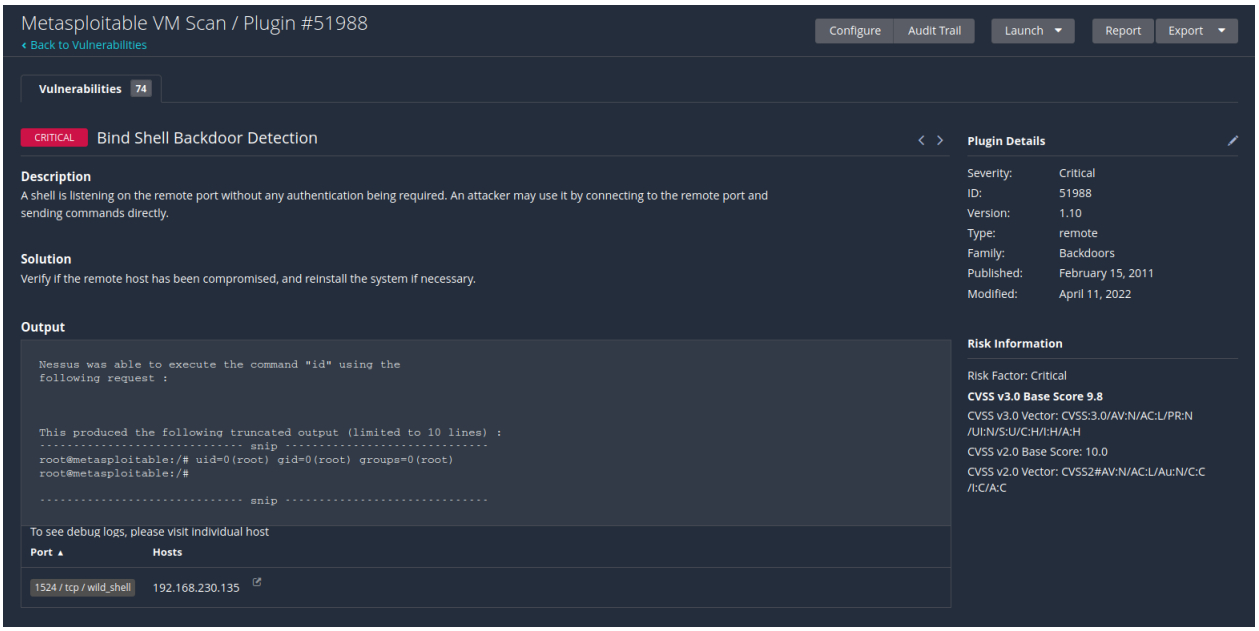
Another critical vulnerability found is an out-of-date software called UnrealIRCd. It appears the current software has a known vulnerability and or is corrupted. The solution would be to delete and reinstall this software.



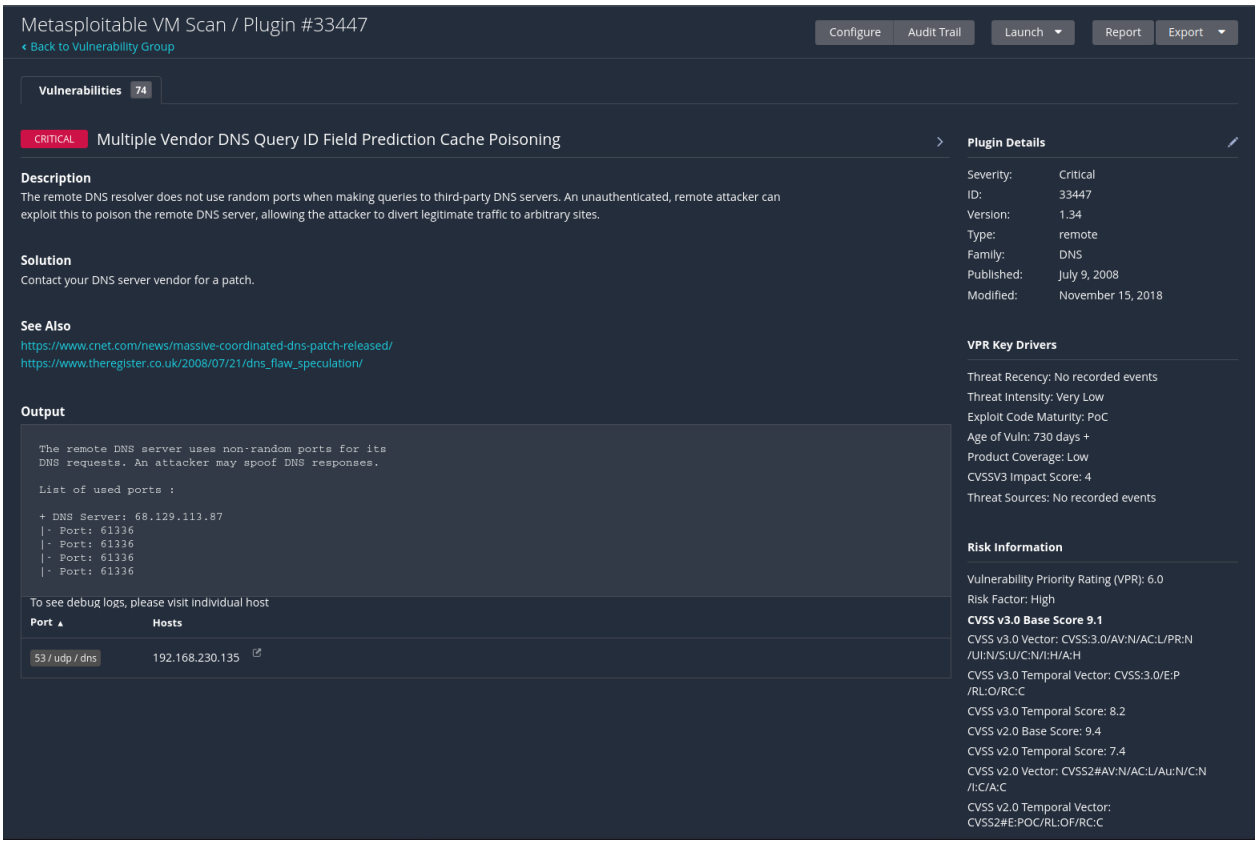


We see in this vulnerability the secure socket layer (SSL), which deals with security and integrity, has outdated versions being used, SSL 2.0 and 3.0. Both of these appear to have known

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.



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.



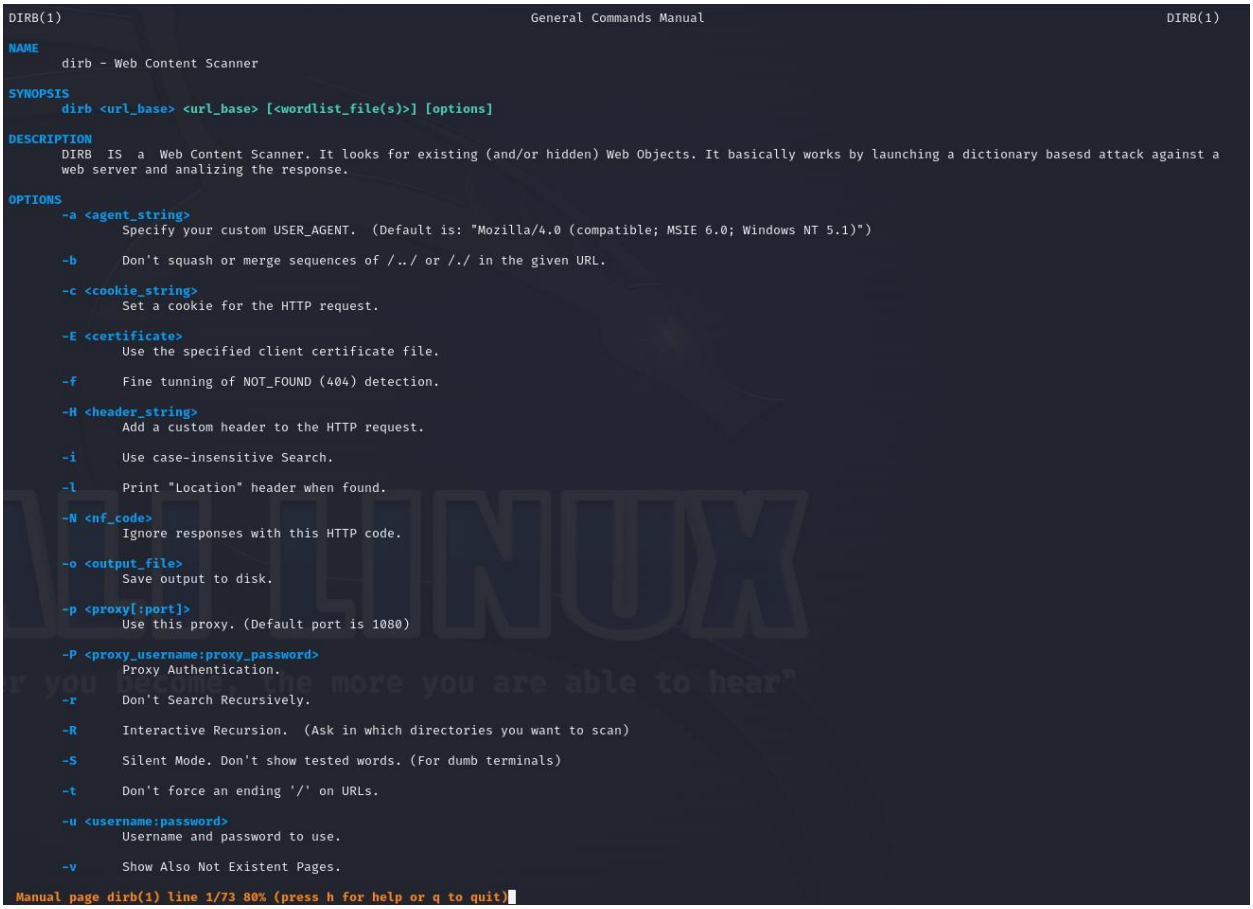
Another critical vulnerability is the possibility of a cache poisoning attack, which the DNS server port needs a patch.

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”.



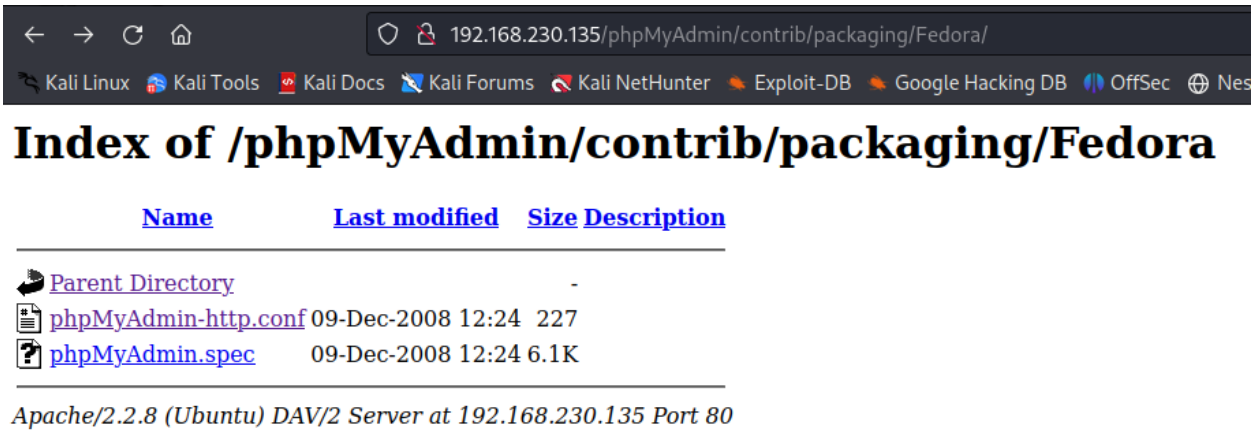
Here is the list of scan commands displayed with the “man dirb” command.

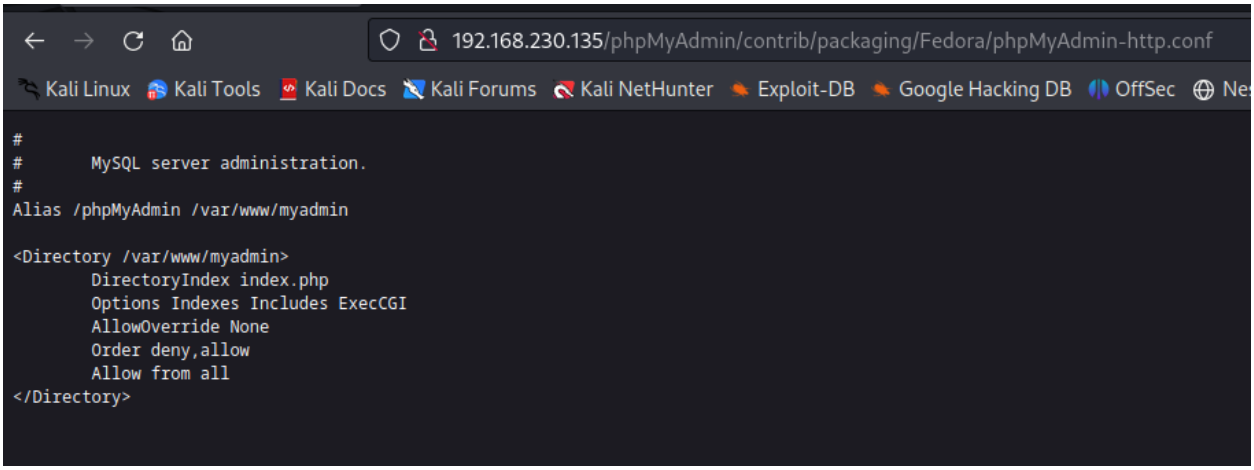
```
┌──(root㉿jhodge)-[~]
└─# dirb http://192.168.230.135/

-----------------
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.

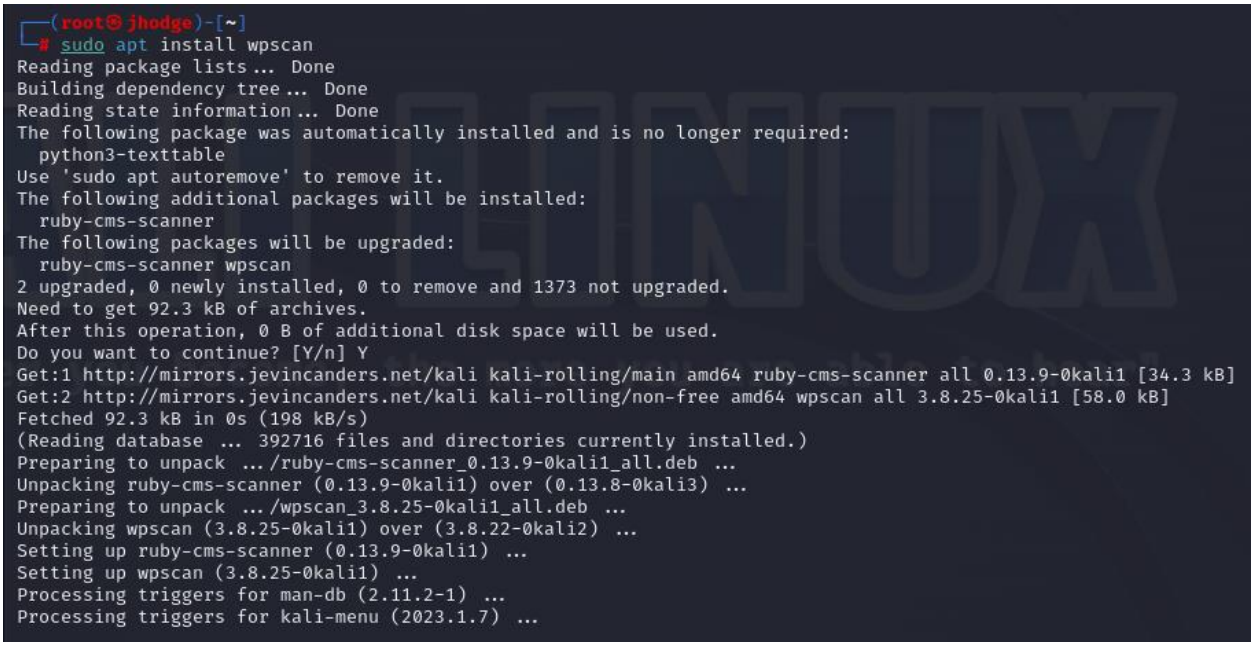




At the completion of the scan, this is the directory and contents of a file.

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.



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

```
                                     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-content-based REGEXP_OR_STRING  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.
      --plugins-detection MODE                  Use the supplied mode to enumerate Plugins.
                                                Default: passive
                                                Available choices: mixed, passive, aggressive
      --plugins-version-detection MODE          Use the supplied mode to check plugins' versions.
                                                Default: mixed
                                                Available choices: mixed, passive, aggressive
      --exclude-usernames REGEXP_OR_STRING      Exclude usernames matching the Regexp/string (case insensitive). Regexp delimiters are not required.
  -P, --passwords FILE-PATH                     List of passwords to use during the password attack.
                                                If no --username/s option supplied, user enumeration will be run.
  -U, --usernames LIST                          List of usernames to use during the password attack.
                                                Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt'
      --multicall-max-passwords MAX_PWD         Maximum number of passwords to send by request with XMLRPC multicall
                                                Default: 500
      --password-attack ATTACK                  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
      --login-uri URI                           The URI of the login page if different from /wp-login.php
      --stealthy                                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.

In order to get passed the website not running WordPress issue I brute forced the test by using "--force". This allows us to run scans even though in this case it was not running WordPress. I also added some other commands for custom or unknown content and plugins.

With this tool we were searching for the WordPress version, which was actually not detected, and is not always the case with brute forcing. I thought this tool would be good practice to use, and I have used it before. To know the WordPress version a website is using could be helpful because there may be known vulnerabilities that could be exploited by a hacker. This test was disappointing in that I only real received headers for the Metasploitable VM and no WordPress version or plugins. I would like to experiment with more WPScan commands in the future.

Skipfish: A reconnaissance tool used to gain information about system vulnerabilities where a hacker can gain entry to a system. The scan I performed did not limit the crawling depth, by using the -o command to adjust a certain time constraint. This simply allows the user to adjust the crawls depth if needed.

```
┌──(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”.

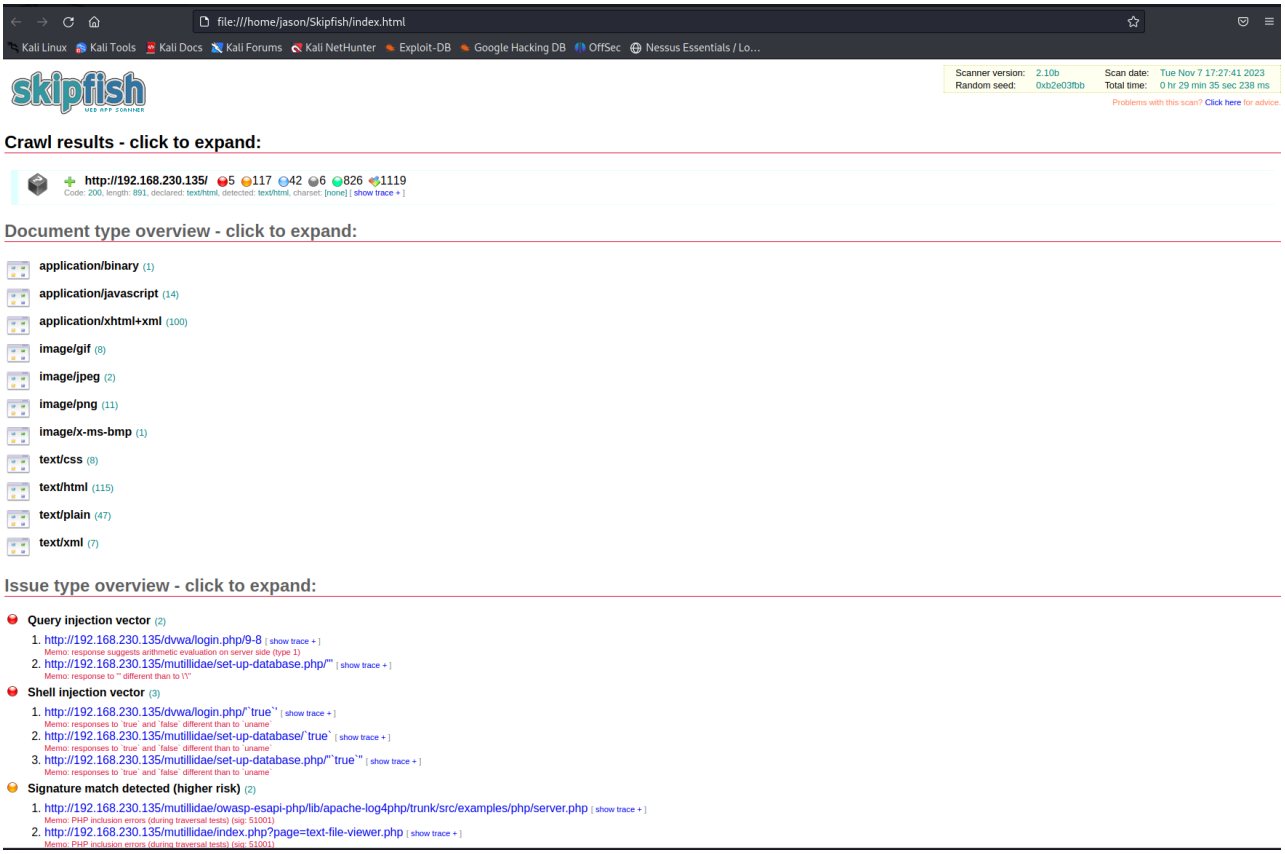
```
┌──(jason㉿jhodge)-[~]
└─$ skipfish -h
skipfish web application scanner - version 2.10b
Usage: skipfish [ options ... ] -W wordlist -o output_dir start_url [ start_url2 ... ]

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%)
    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: 0xb2e03fbb
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: 891, declared: text/html, detected: text/html, charset: [none] [show trace +]
Document type overview - click to expand:
application/binary (1)
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/"' [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)

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/"' [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/