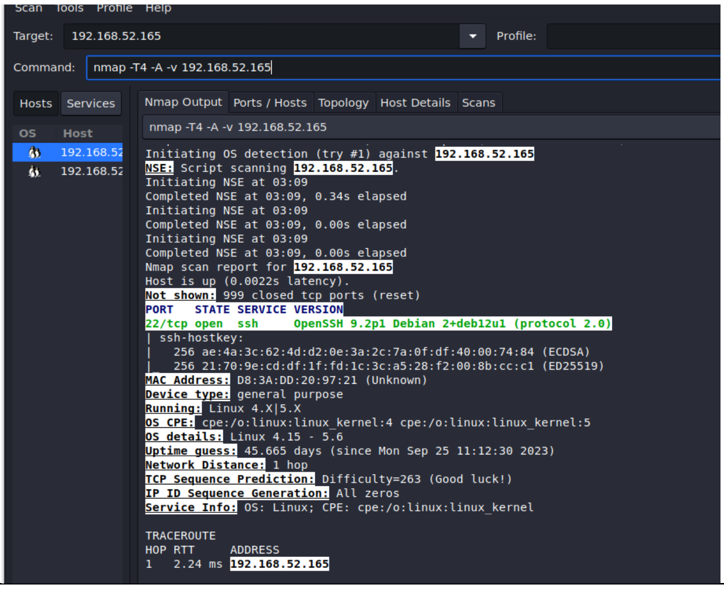
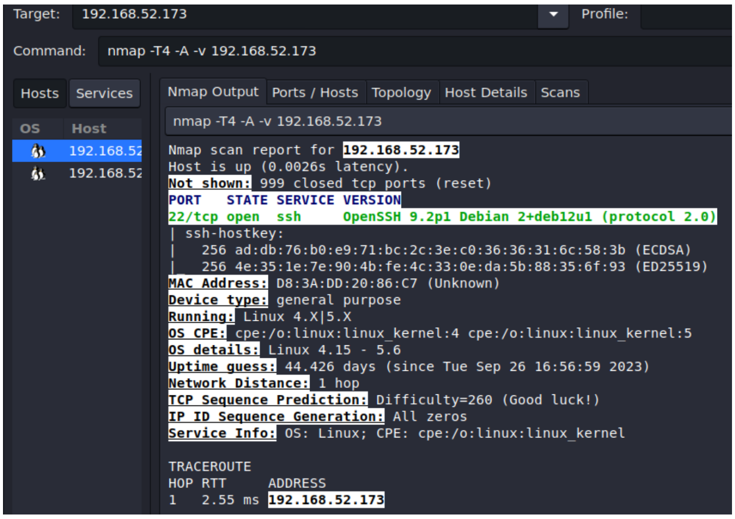
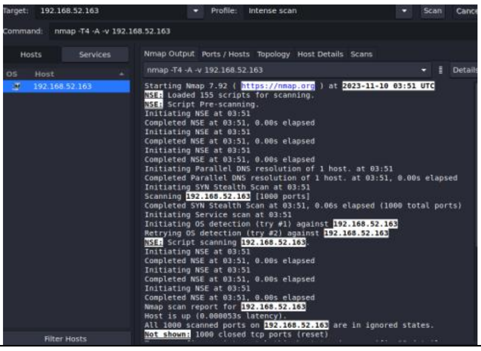
Network Scanning

Device	Description
Web Application	192.168.52.165 
Honeypot	192.168.52.173 
Kali	192.168.52.163 

Target: 192.168.52.165 Profile:

Command: nmap -T4 -A -v 192.168.52.165

nmap -T4 -A -v 192.168.52.165

```
Initiating OS detection (try #1) against 192.168.52.165
NSE: Script scanning 192.168.52.165.
Initiating NSE at 03:09
Completed NSE at 03:09, 0.34s elapsed
Initiating NSE at 03:09
Completed NSE at 03:09, 0.00s elapsed
Initiating NSE at 03:09
Completed NSE at 03:09, 0.00s elapsed
Nmap scan report for 192.168.52.165
Host is up (0.0022s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 ae:4a:3c:62:4d:d2:0e:3a:2c:7a:0f:df:40:00:74:84 (ECDSA)
|_  256 21:70:9e:cd:df:1f:fd:1c:3c:a5:28:f2:00:8b:cc:c1 (ED25519)
MAC Address: D8:3A:DD:20:97:21 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 45.665 days (since Mon Sep 25 11:12:30 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   2.24 ms 192.168.52.165
```

Target: 192.168.52.173 Profile:

Command: nmap -T4 -A -v 192.168.52.173

nmap -T4 -A -v 192.168.52.173

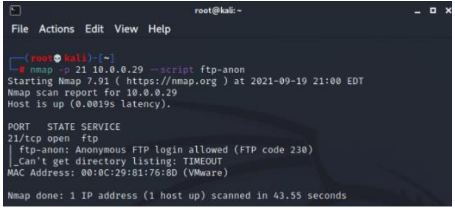
```
Nmap scan report for 192.168.52.173
Host is up (0.0026s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 ad:db:76:b0:e9:71:bc:2c:3e:c0:36:36:31:6c:58:3b (ECDSA)
|_  256 4e:35:1e:7e:90:4b:fe:4c:33:0e:da:5b:88:35:6f:93 (ED25519)
MAC Address: D8:3A:DD:20:86:C7 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 44.426 days (since Tue Sep 26 16:56:59 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   2.55 ms 192.168.52.173
```

Target: 192.168.52.163 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.163

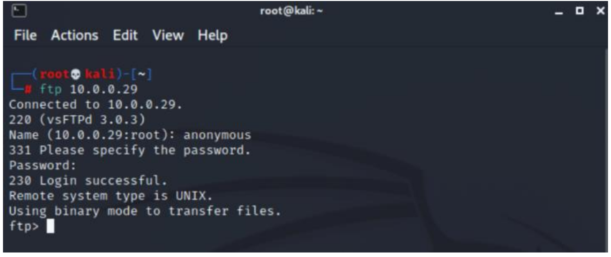
nmap -T4 -A -v 192.168.52.163

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-10 03:51 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:51
Completed NSE at 03:51, 0.00s elapsed
Initiating NSE at 03:51
Completed NSE at 03:51, 0.00s elapsed
Initiating NSE at 03:51
Completed NSE at 03:51, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 03:51
Completed Parallel DNS resolution of 1 host. at 03:51, 0.00s elapsed
Initiating SYN Stealth Scan at 03:51
Scanning 192.168.52.163 [1000 ports]
Completed SYN Stealth Scan at 03:51, 0.06s elapsed (1000 total ports)
Initiating Service scan at 03:51
Initiating OS detection (try #1) against 192.168.52.163
Retrying OS detection (try #2) against 192.168.52.163
NSE: Script scanning 192.168.52.163.
Initiating NSE at 03:51
Completed NSE at 03:51, 0.00s elapsed
Initiating NSE at 03:51
Completed NSE at 03:51, 0.00s elapsed
Initiating NSE at 03:51
Completed NSE at 03:51, 0.00s elapsed
Nmap scan report for 192.168.52.163
Host is up (0.000053s latency).
All 1000 scanned ports on 192.168.52.163 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

<table>
<tr><td></td><td></td></tr>
<tr><td>Tool</td><td>nmap/zenmap</td></tr>
<tr><td>Command Lines</td><td>nmap localhost [or ip addr]
sudo nmap -sU localhost [or ip addr]
sudo nmap -sV --script vulners [ip addr]
sudo nmap -A localhost
man nmap</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Target Device</td><td>IP Address:
1. 192.168.52.146
2. 192.168.52.161
3. 192.168.52.172</td></tr>
<tr><td>Vulnerabilities</td><td>vsftpd- FTP server for unix-like file systems
-Directory Traversal Attack
-XSS
-Brute Force Attack
-Buffer Overflow</td></tr>
<tr><td>-Directory Traversal Attack
Reference:
https://www.linkedin.com/pulse/pentesting-exploiting-ftp-servers-kubotor</td><td>-This FTP vulnerability includes directory traversal attacks in which the successful attack overwrites or creates unauthorized files that are stored outside of the web root folder.</td></tr>
<tr><td>-XSS</td><td>-The vulnerability of web security that allows the attacker to compromise the interaction of potential users with the vulnerable application
Ex. <img src=x onmouseover=alert(1)></td></tr>
<tr><td>-Brute Force Attack</td><td>-Violent power attacks use temptation and error to guess login details, encryption keys, or to discover a hidden webpage.</td></tr>
<tr><td>-Buffer Overflow</td><td>-Attackers use full overflow issues by overwriting the app's memory. This changes the way the system works, triggers a response that damages files or reveals confidential information. Types of Buffer Overflow Exploit</td></tr>
<tr><td>EXPLOITATION
-Anonymous login</td><td>Scanning


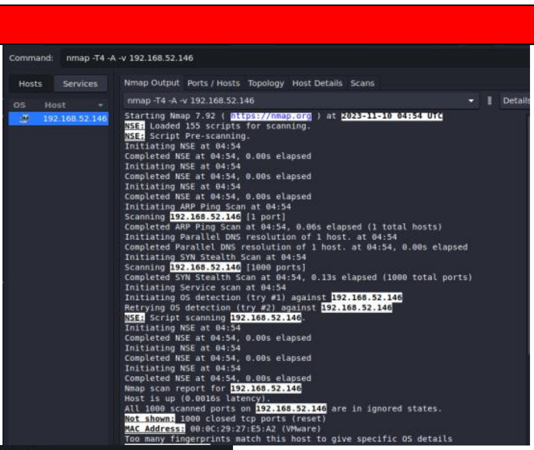
<pre>
┌──(root💀kali)-[~]
└─# nmap -p 21 10.0.0.29 --script ftp-anon
Starting Nmap 7.91 (https://nmap.org) at 2021-09-19 21:00 EDT
Nmap scan report for 10.0.0.29
Host is up (0.0019s latency).

PORT   STATE SERVICE
21/tcp open ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
MAC Address: 00:0C:29:81:76:8D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 43.55 seconds
</pre>
nmap -p 192.168.52.x –script ftp-anon</td></tr>
<tr><td></td><td>Exploitation (anonymous login)


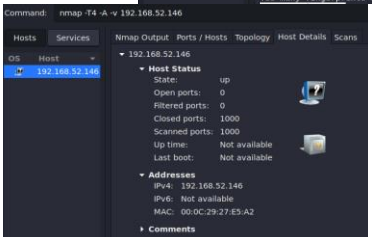
<pre>
┌──(root💀kali)-[~]
└─# ftp 10.0.0.29
Connected to 10.0.0.29.
220 (vsFTPd 3.0.3)
Name (10.0.0.29:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
</pre>
ftp 192.168.52.x</td></tr>
</table>

<table>
<tr><td>FTP</td><td>9-FTP Exploit - LAB(1).docx</td></tr>
<tr><td></td><td>FTP.docx</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Network Scanning: Zenmap</td><td>



```
nmap -T4 -A -v 192.168.52.146
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-10 04:54 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating ARP Ping Scan at 04:54
Scanning 192.168.52.146 [1 port]
Completed ARP Ping Scan at 04:54, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:54
Completed Parallel DNS resolution of 1 host. at 04:54, 0.00s elapsed
Initiating SYN Stealth Scan at 04:54
Scanning 192.168.52.146 [1000 ports]
Completed SYN Stealth Scan at 04:54, 0.13s elapsed (1000 total ports)
Initiating Service scan at 04:54
Initiating OS detection (try #1) against 192.168.52.146
Retrying OS detection (try #2) against 192.168.52.146
NSE: Script scanning 192.168.52.146.
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Nmap scan report for 192.168.52.146
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.52.146 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:27:E5:A2 (VMware)
Too many fingerprints match this host to give specific OS details
```



```
nmap -T4 -A -v 192.168.52.146
```

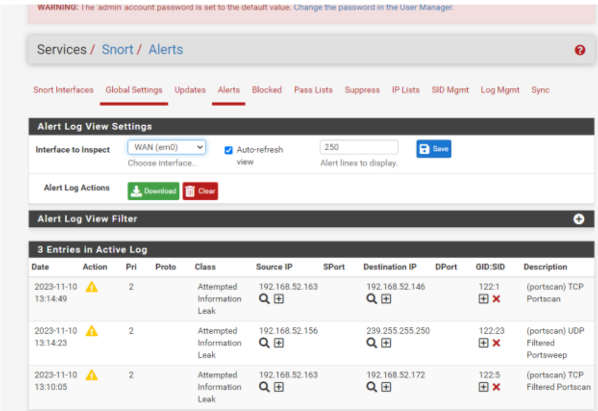
192.168.52.146

Host Status
State: up
Open ports: 0
Filtered ports: 0
Closed ports: 1000
Scanned ports: 1000
Up time: Not available
Last boot: Not available

Addresses
IPv4: 192.168.52.146
IPv6: Not available
MAC: 00:0C:29:27:E5:A2

Comments

192.168.52.146
localhost



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: WAN (em0) — Choose interface..
☑ Auto-refresh view
250 — Alert lines to display.

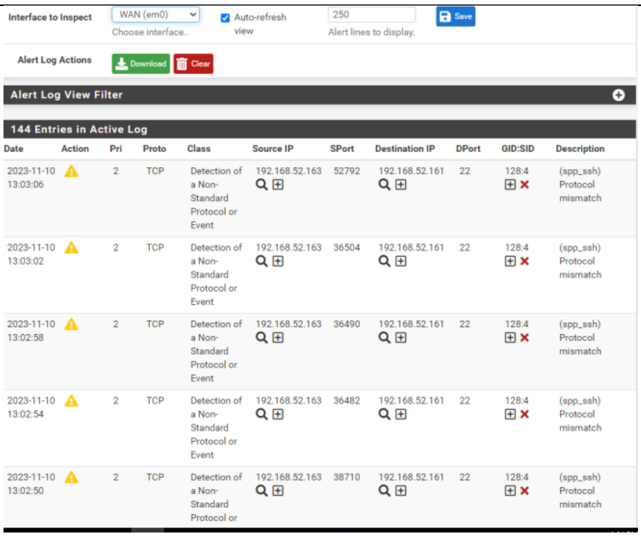
Alert Log Actions

Alert Log View Filter

3 Entries in Active Log

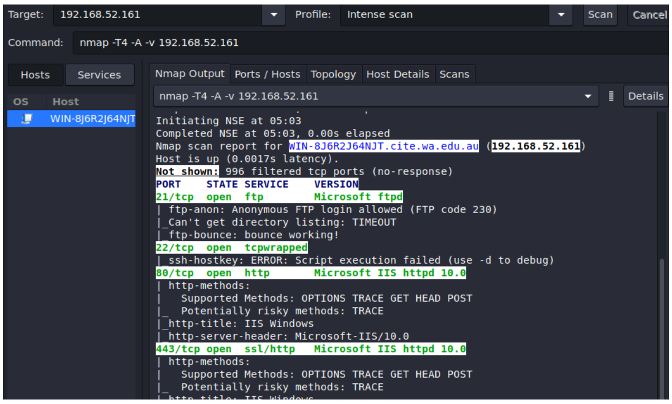
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-11-10 13:14:49	⚠	2		Attempted Information Leak	192.168.52.163		192.168.52.146		122:1	(portscan) TCP Portscan
2023-11-10 13:14:23	⚠	2		Attempted Information Leak	192.168.52.156		239.255.255.250		122:23	(portscan) UDP Filtered Portsweep
2023-11-10 13:10:05	⚠	2		Attempted Information Leak	192.168.52.163		192.168.52.172		122:5	(portscan) TCP Filtered Portscan

</td></tr>
<tr><td></td><td></td></tr>
</table>



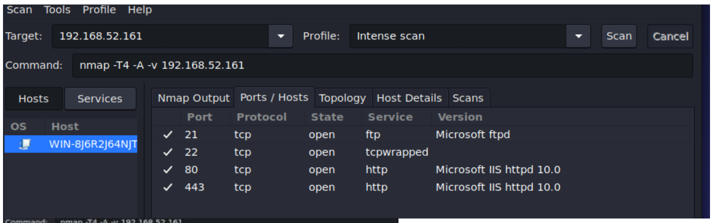
144 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-11-10 13:03:06	⚠	2	TCP	Detection of a Non-Standard Protocol or Event	192.168.52.163	52792	192.168.52.161	22	128:4	(spp_ssh) Protocol mismatch
2023-11-10 13:03:02	⚠	2	TCP	Detection of a Non-Standard Protocol or Event	192.168.52.163	36504	192.168.52.161	22	128:4	(spp_ssh) Protocol mismatch
2023-11-10 13:02:58	⚠	2	TCP	Detection of a Non-Standard Protocol or Event	192.168.52.163	36490	192.168.52.161	22	128:4	(spp_ssh) Protocol mismatch
2023-11-10 13:02:54	⚠	2	TCP	Detection of a Non-Standard Protocol or Event	192.168.52.163	36482	192.168.52.161	22	128:4	(spp_ssh) Protocol mismatch
2023-11-10 13:02:50	⚠	2	TCP	Detection of a Non-Standard Protocol or	192.168.52.163	38710	192.168.52.161	22	128:4	(spp_ssh) Protocol mismatch



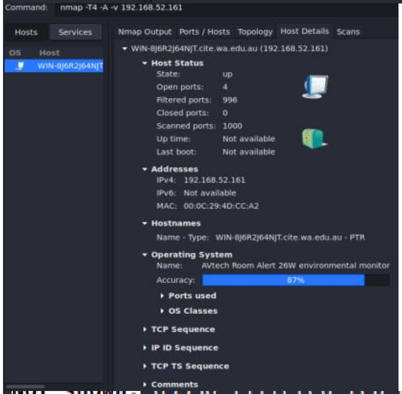
Target: 192.168.52.161
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.52.161

```
Initiating NSE at 05:03
Completed NSE at 05:03, 0.00s elapsed
Nmap scan report for WIN-8J6R2J64NJT.cite.wa.edu.au (192.168.52.161)
Host is up (0.0017s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
|_ftp-bounce: bounce working!
22/tcp  open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp  open  http       Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
443/tcp open  ssl/http   Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
```



Target: 192.168.52.161
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.52.161

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Microsoft ftpd
✓	22	tcp	open	tcpwrapped	
✓	80	tcp	open	http	Microsoft IIS httpd 10.0
✓	443	tcp	open	http	Microsoft IIS httpd 10.0



Command: nmap -T4 -A -v 192.168.52.161

WIN-8J6R2J64NJT.cite.wa.edu.au (192.168.52.161)

Host Status

State:	up
Open ports:	4
Filtered ports:	996
Closed ports:	0
Scanned ports:	1000
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	192.168.52.161
IPv6:	Not available
MAC:	00:0C:29:4D:CC:A2

Hostnames

Name - Type: WIN-8J6R2J64NJT.cite.wa.edu.au - PTR

Operating System

Name: AVtech Room Alert 26W environmental monitor

Accuracy: 87%

Ports used

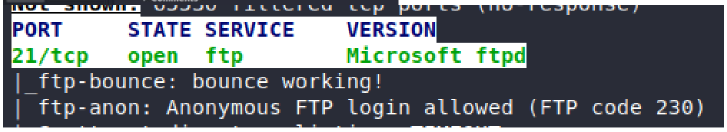
OS Classes

TCP Sequence

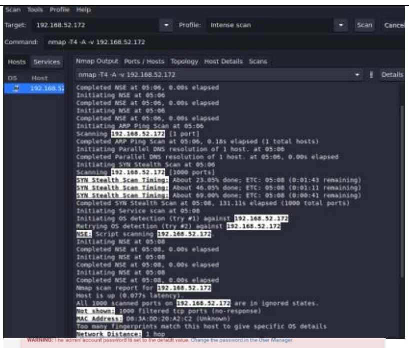
IP ID Sequence

TCP TS Sequence

Comments

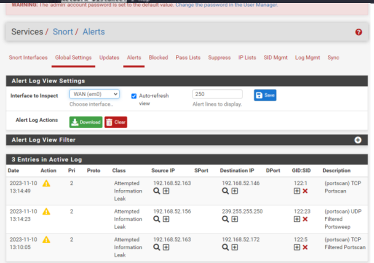


```
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        Microsoft ftpd
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```



Command: nmap -T4 -A -v 192.168.52.172

```
nmap -T4 -A -v 192.168.52.172
Completed NSE at 05:06, 0.00s elapsed
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
Initiating ARP Ping Scan at 05:06
Scanning 192.168.52.172 [1 port]
Completed ARP Ping Scan at 05:06, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:06
Completed Parallel DNS resolution of 1 host. at 05:06, 0.00s elapsed
Initiating SYN Stealth Scan at 05:06
Scanning 192.168.52.172 [1000 ports]
SYN Stealth Scan Timing: About 23.05% done; ETC: 05:08 (0:01:43 remaining)
SYN Stealth Scan Timing: About 46.05% done; ETC: 05:08 (0:01:11 remaining)
SYN Stealth Scan Timing: About 69.00% done; ETC: 05:08 (0:00:41 remaining)
Completed SYN Stealth Scan at 05:08, 131.11s elapsed (1000 total ports)
Initiating Service scan at 05:08
Initiating OS detection (try #1) against 192.168.52.172
Retrying OS detection (try #2) against 192.168.52.172
NSE: Script scanning 192.168.52.172.
Initiating NSE at 05:08
Completed NSE at 05:08, 0.00s elapsed
Initiating NSE at 05:08
Completed NSE at 05:08, 0.00s elapsed
Initiating NSE at 05:08
Completed NSE at 05:08, 0.00s elapsed
Nmap scan report for 192.168.52.172
Host is up (0.077s latency).
All 1000 scanned ports on 192.168.52.172 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: D8:3A:DD:20:A2:C2 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: WAN (em0) — Choose interface..

☑ Auto-refresh view

250 — Alert lines to display.

Save

Alert Log Actions: Download Clear

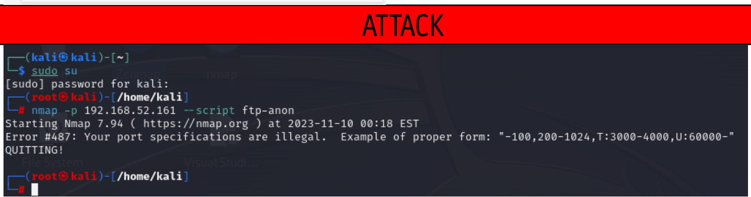
Alert Log View Filter

3 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-11-10 13:14:49	⚠	2		Attempted Information Leak	192.168.52.163		192.168.52.146		122:1	(portscan) TCP Portscan
2023-11-10 13:14:23	⚠	2		Attempted Information Leak	192.168.52.156		239.255.255.250		122:23	(portscan) UDP Filtered Portsweep
2023-11-10 13:10:05	⚠	2		Attempted Information Leak	192.168.52.163		192.168.52.172		122:5	(portscan) TCP Filtered Portscan

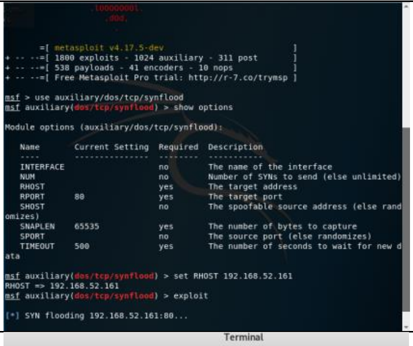
ATTACK

nmap
Trying to exploit ftp-anonymous login

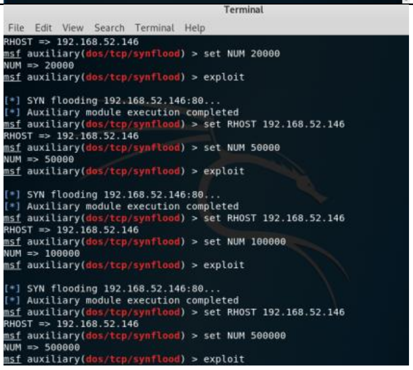


```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 192.168.52.161 --script ftp-anon
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 00:18 EST
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(root㉿kali)-[/home/kali]
└─# 
```

Metasploit:
Perform “synflood” for dos attacks

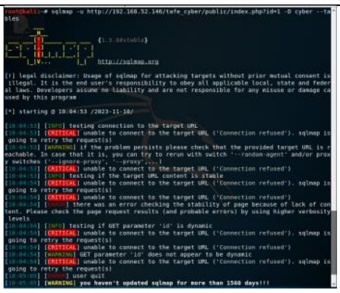


```
       =[ metasploit v4.17.5-dev                          ]
+ -- --=[ 1800 exploits - 1024 auxiliary - 311 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else rand
omizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new d
ata

msf auxiliary(dos/tcp/synflood) > set RHOST 192.168.52.161
RHOST => 192.168.52.161
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 192.168.52.161:80...
```



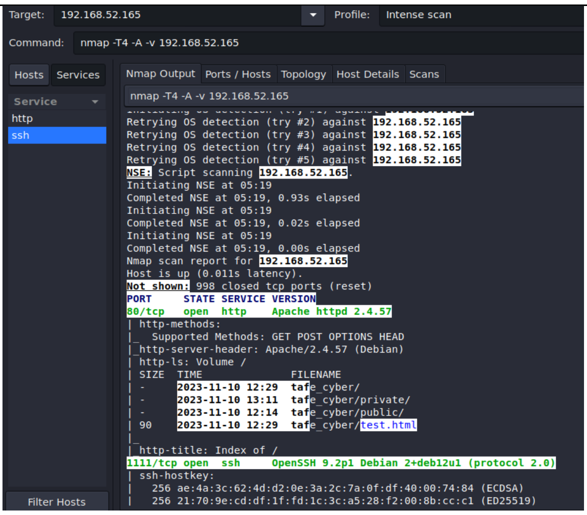
```
RHOST => 192.168.52.146
msf auxiliary(dos/tcp/synflood) > set NUM 20000
NUM => 20000
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 192.168.52.146:80...
[*] Auxiliary module execution completed
msf auxiliary(dos/tcp/synflood) > set RHOST 192.168.52.146
RHOST => 192.168.52.146
msf auxiliary(dos/tcp/synflood) > set NUM 50000
NUM => 50000
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 192.168.52.146:80...
[*] Auxiliary module execution completed
msf auxiliary(dos/tcp/synflood) > set RHOST 192.168.52.146
RHOST => 192.168.52.146
msf auxiliary(dos/tcp/synflood) > set NUM 100000
NUM => 100000
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 192.168.52.146:80...
[*] Auxiliary module execution completed
msf auxiliary(dos/tcp/synflood) > set RHOST 192.168.52.146
RHOST => 192.168.52.146
msf auxiliary(dos/tcp/synflood) > set NUM 500000
NUM => 500000
msf auxiliary(dos/tcp/synflood) > exploit
```

SQL Injection
-u
http://192.168.52.146/tafe_cyber/
public/index.php?id=1 -D cyber –table



```
root@kali:~# sqlmap -u http://192.168.52.146/tafe_cyber/public/index.php?id=1 -D cyber --ta
bles

                              {1.3.8#stable}

                              http://sqlmap.org

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

[*] starting @ 10:04:53 /2023-11-10/

[10:04:53] [INFO] testing connection to the target URL
[10:04:53] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is
 going to retry the request(s)
[10:04:53] [WARNING] if the problem persists please check that the provided target URL is r
eachable. In case that it is, you can try to rerun with switch '--random-agent' and/or prox
y switches ('--ignore-proxy', '--proxy',...)
[10:04:53] [CRITICAL] unable to connect to the target URL ('Connection refused')
[10:04:53] [INFO] testing if the target URL content is stable
[10:04:54] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is
 going to retry the request(s)
[10:04:54] [CRITICAL] unable to connect to the target URL ('Connection refused')
[10:04:54] [ERROR] there was an error checking the stability of page because of lack of con
tent. Please check the page request results (and probable errors) by using higher verbosity
 levels
[10:04:54] [INFO] testing if GET parameter 'id' is dynamic
[10:04:54] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is
 going to retry the request(s)
[10:04:54] [CRITICAL] unable to connect to the target URL ('Connection refused')
[10:04:54] [WARNING] GET parameter 'id' does not appear to be dynamic
[10:04:54] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is
 going to retry the request(s)
[10:05:05] [ERROR] user quit
[10:05:05] [WARNING] you haven't updated sqlmap for more than 1560 days!!!
```

Internal Testing-Web Application (prior to modification of setting)

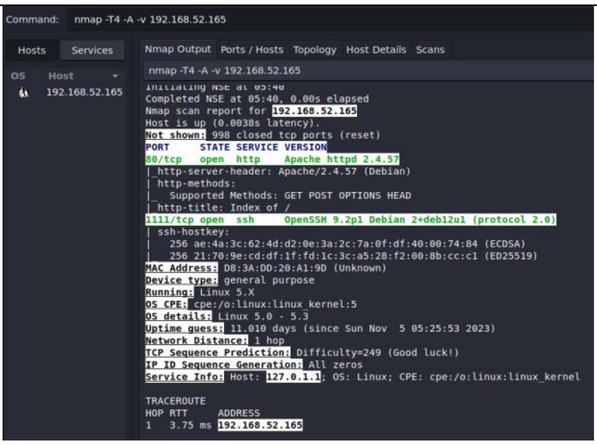


Target: 192.168.52.165 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.165

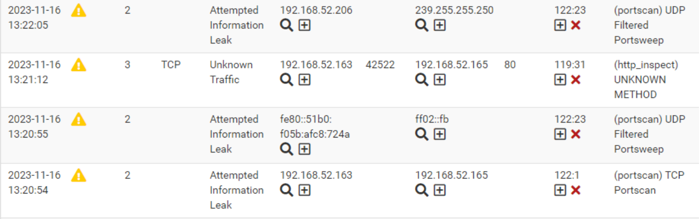
```
nmap -T4 -A -v 192.168.52.165
Initiating OS detection (try #1) against 192.168.52.165
Retrying OS detection (try #2) against 192.168.52.165
Retrying OS detection (try #3) against 192.168.52.165
Retrying OS detection (try #4) against 192.168.52.165
Retrying OS detection (try #5) against 192.168.52.165
NSE: Script scanning 192.168.52.165.
Initiating NSE at 05:19
Completed NSE at 05:19, 0.93s elapsed
Initiating NSE at 05:19
Completed NSE at 05:19, 0.02s elapsed
Initiating NSE at 05:19
Completed NSE at 05:19, 0.00s elapsed
Nmap scan report for 192.168.52.165
Host is up (0.011s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.57
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.57 (Debian)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2023-11-10 12:29  tafe_cyber/
| -     2023-11-10 13:11  tafe_cyber/private/
| -     2023-11-10 12:14  tafe_cyber/public/
| 90    2023-11-10 12:29  tafe_cyber/test.html
|_
|_http-title: Index of /
1111/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 ae:4a:3c:62:4d:d2:0e:3a:2c:7a:0f:df:40:00:74:84 (ECDSA)
|   256 21:70:9e:cd:df:1f:fd:1c:3c:a5:28:f2:00:8b:cc:c1 (ED25519)
```

Scanning (after security-setting-modification)



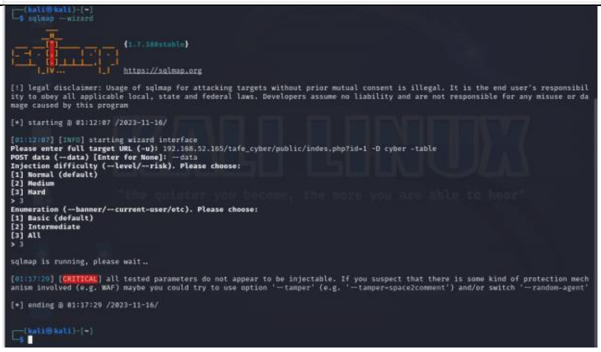
Command: nmap -T4 -A -v 192.168.52.165

```
nmap -T4 -A -v 192.168.52.165
Initiating NSE at 05:40
Completed NSE at 05:40, 0.00s elapsed
Nmap scan report for 192.168.52.165
Host is up (0.0038s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.57
|_http-server-header: Apache/2.4.57 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
| http-title: Index of /
1111/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 ae:4a:3c:62:4d:d2:0e:3a:2c:7a:0f:df:40:00:74:84 (ECDSA)
|   256 21:70:9e:cd:df:1f:fd:1c:3c:a5:28:f2:00:8b:cc:c1 (ED25519)
MAC Address: D8:3A:DD:20:A1:9D (Unknown)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.3
Uptime guess: 11.010 days (since Sun Nov  5 05:25:53 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=249 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   3.75 ms 192.168.52.165
```

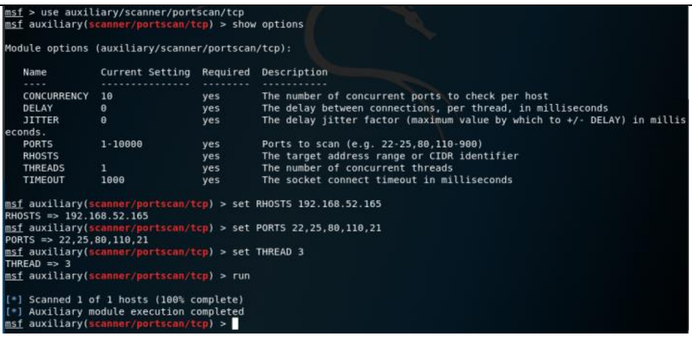


2023-11-16 13:22:05	⚠	2		Attempted Information Leak	192.168.52.206		239.255.255.250		122:23	(portscan) UDP Filtered Portsweep
2023-11-16 13:21:12	⚠	3	TCP	Unknown Traffic	192.168.52.163	42522	192.168.52.165	80	119:31	(http_inspect) UNKNOWN METHOD
2023-11-16 13:20:55	⚠	2		Attempted Information Leak	fe80::51b0:f05b:afc8:724a		ff02::fb		122:23	(portscan) UDP Filtered Portsweep
2023-11-16 13:20:54	⚠	2		Attempted Information Leak	192.168.52.163		192.168.52.165		122:1	(portscan) TCP Portscan

SQL Injection

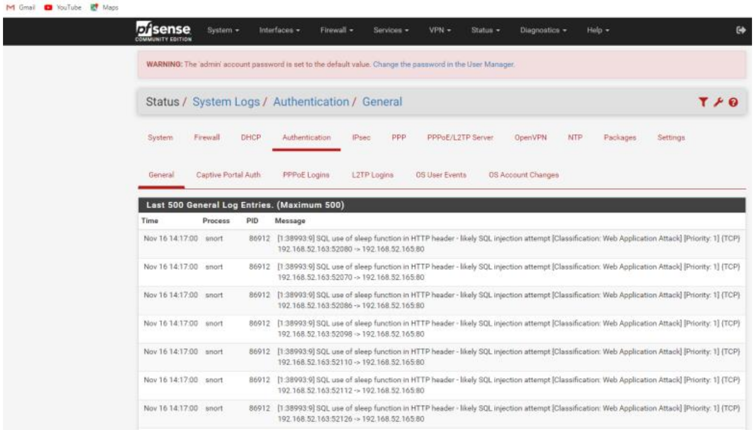


```
┌──(kali㉿kali)-[~]
└─$ sqlmap --wizard

                                  {1.7.10#stable}

                                  https://sqlmap.org

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

[*] starting @ 01:12:07 /2023-11-16/

[01:12:07] [INFO] starting wizard interface
Please enter full target URL (-u): 192.168.52.165/tafe_cyber/public/indes.php?id=1 -D cyber -table
POST data (--data) [Enter for None]: --data
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
> 3
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 3

sqlmap is running, please wait..

[01:17:29] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mech
anism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 01:17:29 /2023-11-16/

┌──(kali㉿kali)-[~]
└─$ 
```



```
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in millis
econds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target address range or CIDR identifier
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.52.165
RHOSTS => 192.168.52.165
msf auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21
PORTS => 22,25,80,110,21
msf auxiliary(scanner/portscan/tcp) > set THREAD 3
THREAD => 3
msf auxiliary(scanner/portscan/tcp) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) > 
```

System Logs (Alerts)



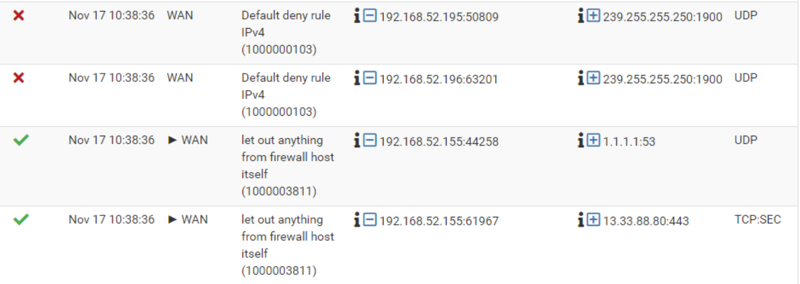
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / System Logs / Authentication / General

Last 500 General Log Entries. (Maximum 500)

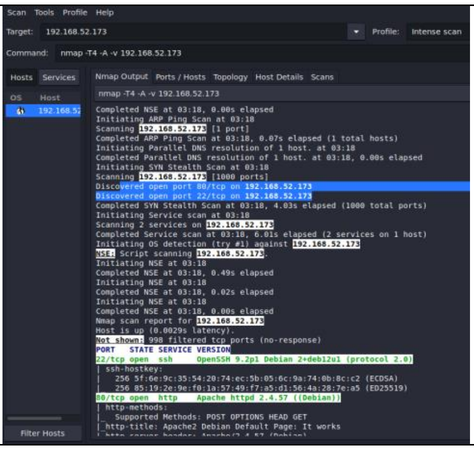
Time	Process	PID	Message
Nov 16 14:17:00	snort	86912	[1:38993:9] SQL use of sleep function in HTTP header - likely SQL injection attempt [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.52.163:52080 -> 192.168.52.165:80
Nov 16 14:17:00	snort	86912	[1:38993:9] SQL use of sleep function in HTTP header - likely SQL injection attempt [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.52.163:52070 -> 192.168.52.165:80
Nov 16 14:17:00	snort	86912	[1:38993:9] SQL use of sleep function in HTTP header - likely SQL injection attempt [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.52.163:52086 -> 192.168.52.165:80
Nov 16 14:17:00	snort	86912	[1:38993:9] SQL use of sleep function in HTTP header - likely SQL injection attempt [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.52.163:52098 -> 192.168.52.165:80
Nov 16 14:17:00	snort	86912	[1:38993:9] SQL use of sleep function in HTTP header - likely SQL injection attempt [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.52.163:52110 -> 192.168.52.165:80
Nov 16 14:17:00	snort	86912	[1:38993:9] SQL use of sleep function in HTTP header - likely SQL injection attempt [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.52.163:52112 -> 192.168.52.165:80
Nov 16 14:17:00	snort	86912	[1:38993:9] SQL use of sleep function in HTTP header - likely SQL injection attempt [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.52.163:52126 -> 192.168.52.165:80

System Logs (Firewall)



✗	Nov 17 10:38:36	WAN	Default deny rule IPv4 (1000000103)	192.168.52.195:50809	239.255.255.250:1900	UDP
✗	Nov 17 10:38:36	WAN	Default deny rule IPv4 (1000000103)	192.168.52.196:63201	239.255.255.250:1900	UDP
✓	Nov 17 10:38:36	▶ WAN	let out anything from firewall host itself (1000003811)	192.168.52.155:44258	1.1.1.1:53	UDP
✓	Nov 17 10:38:36	▶ WAN	let out anything from firewall host itself (1000003811)	192.168.52.155:61967	13.33.88.80:443	TCP:SEC

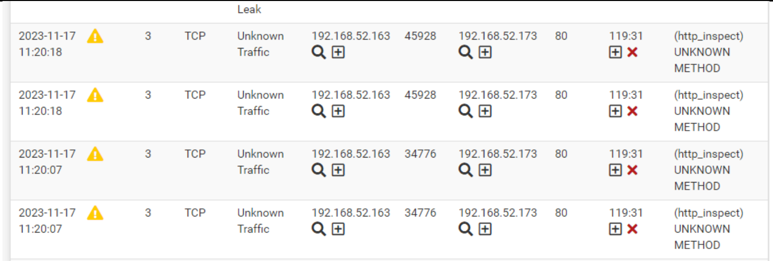
192.168.52.173 (Webpage)



Target: 192.168.52.173 Profile: Intense scan

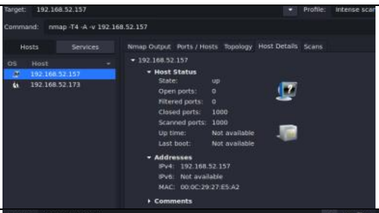
Command: nmap -T4 -A -v 192.168.52.173

```
nmap -T4 -A -v 192.168.52.173
Completed NSE at 03:18, 0.00s elapsed
Initiating ARP Ping Scan at 03:18
Scanning 192.168.52.173 [1 port]
Completed ARP Ping Scan at 03:18, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:18
Completed Parallel DNS resolution of 1 host. at 03:18, 0.00s elapsed
Initiating SYN Stealth Scan at 03:18
Scanning 192.168.52.173 [1000 ports]
Discovered open port 80/tcp on 192.168.52.173
Discovered open port 22/tcp on 192.168.52.173
Completed SYN Stealth Scan at 03:18, 4.03s elapsed (1000 total ports)
Initiating Service scan at 03:18
Scanning 2 services on 192.168.52.173
Completed Service scan at 03:18, 6.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.52.173
NSE: Script scanning 192.168.52.173.
Initiating NSE at 03:18
Completed NSE at 03:18, 0.49s elapsed
Initiating NSE at 03:18
Completed NSE at 03:18, 0.02s elapsed
Initiating NSE at 03:18
Completed NSE at 03:18, 0.00s elapsed
Nmap scan report for 192.168.52.173
Host is up (0.0029s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 5f:6e:9c:35:54:20:74:ec:5b:05:6c:9a:74:0b:8c:c2 (ECDSA)
|   256 85:19:2e:9e:f0:1a:57:49:f7:a5:d1:56:4a:28:7e:a5 (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
```



				Leak						
2023-11-17 11:20:18	⚠	3	TCP	Unknown Traffic	192.168.52.163	45928	192.168.52.173	80	119:31	(http_inspect) UNKNOWN METHOD
2023-11-17 11:20:18	⚠	3	TCP	Unknown Traffic	192.168.52.163	45928	192.168.52.173	80	119:31	(http_inspect) UNKNOWN METHOD
2023-11-17 11:20:07	⚠	3	TCP	Unknown Traffic	192.168.52.163	34776	192.168.52.173	80	119:31	(http_inspect) UNKNOWN METHOD
2023-11-17 11:20:07	⚠	3	TCP	Unknown Traffic	192.168.52.163	34776	192.168.52.173	80	119:31	(http_inspect) UNKNOWN METHOD

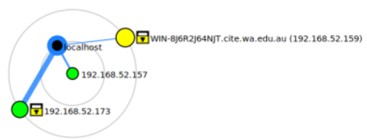
192.168.52.157

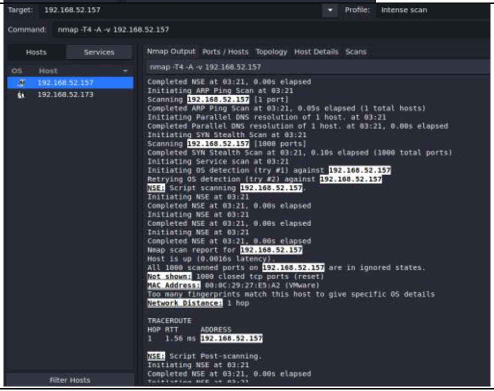


Target: 192.168.52.157 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.157

```
▾ 192.168.52.157
  ▾ Host Status
      State:          up
      Open ports:     0
      Filtered ports: 0
      Closed ports:   1000
      Scanned ports:  1000
      Up time:        Not available
      Last boot:      Not available
  ▾ Addresses
      IPv4: 192.168.52.157
      IPv6: Not available
      MAC:  00:0C:29:27:E5:A2
  ▸ Comments
```





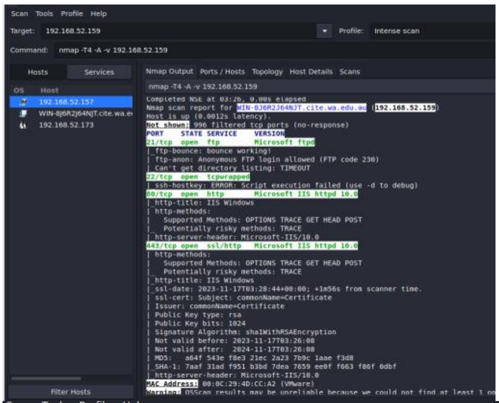
Target: 192.168.52.157 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.157

nmap -T4 -A -v 192.168.52.157

```
Completed NSE at 03:21, 0.00s elapsed
Initiating ARP Ping Scan at 03:21
Scanning 192.168.52.157 [1 port]
Completed ARP Ping Scan at 03:21, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:21
Completed Parallel DNS resolution of 1 host. at 03:21, 0.00s elapsed
Initiating SYN Stealth Scan at 03:21
Scanning 192.168.52.157 [1000 ports]
Completed SYN Stealth Scan at 03:21, 0.10s elapsed (1000 total ports)
Initiating Service scan at 03:21
Initiating OS detection (try #1) against 192.168.52.157
Retrying OS detection (try #2) against 192.168.52.157
NSE: Script scanning 192.168.52.157.
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Nmap scan report for 192.168.52.157
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.52.157 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:27:E5:A2 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.56 ms 192.168.52.157

NSE: Script Post-scanning.
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
```

192.168.52.159 (Honeypot)

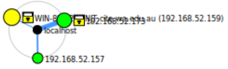


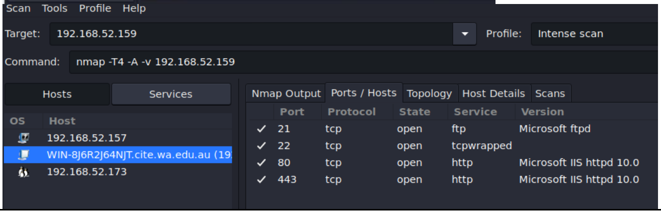
Target: 192.168.52.159 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.159

nmap -T4 -A -v 192.168.52.159

```
Completed NSE at 03:26, 0.00s elapsed
Nmap scan report for WIN-8J6R2J64NJT.cite.wa.edu.au (192.168.52.159)
Host is up (0.0012s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        Microsoft ftpd
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp  open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp  open  http       Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
443/tcp open  ssl/http   Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_ssl-date: 2023-11-17T03:28:44+00:00; +1m56s from scanner time.
| ssl-cert: Subject: commonName=Certificate
| Issuer: commonName=Certificate
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2023-11-17T03:26:08
| Not valid after:  2024-11-17T03:26:08
| MD5:   a64f 543e f8e3 21ec 2a23 7b9c 1aae f3d8
|_SHA-1: 7aaf 31ad f951 b3bd 7dea 7659 ee8f f663 f86f 0dbf
|_http-server-header: Microsoft-IIS/10.0
MAC Address: 00:0C:29:4D:CC:A2 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 op
```

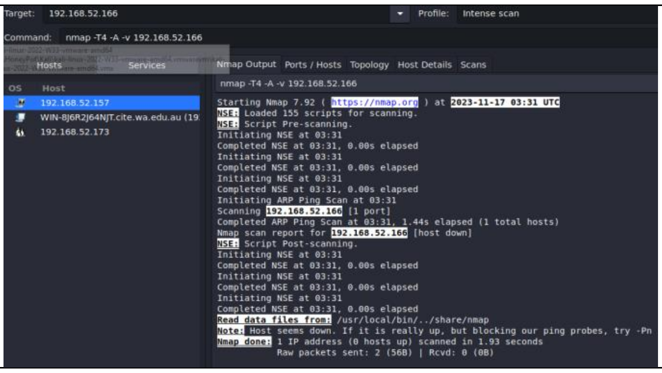




Target: 192.168.52.159 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.159

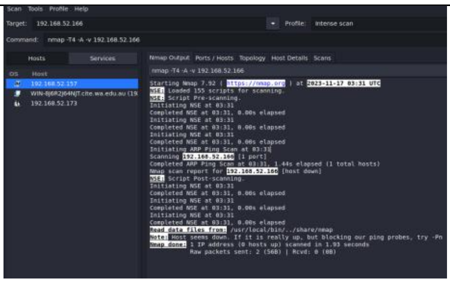
	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Microsoft ftpd
✓	22	tcp	open	tcpwrapped	
✓	80	tcp	open	http	Microsoft IIS httpd 10.0
✓	443	tcp	open	http	Microsoft IIS httpd 10.0



Target: 192.168.52.166 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.166

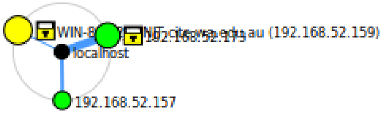
```
nmap -T4 -A -v 192.168.52.166

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-17 03:31 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating ARP Ping Scan at 03:31
Scanning 192.168.52.166 [1 port]
Completed ARP Ping Scan at 03:31, 1.44s elapsed (1 total hosts)
Nmap scan report for 192.168.52.166 [host down]
NSE: Script Post-scanning.
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.93 seconds
           Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```



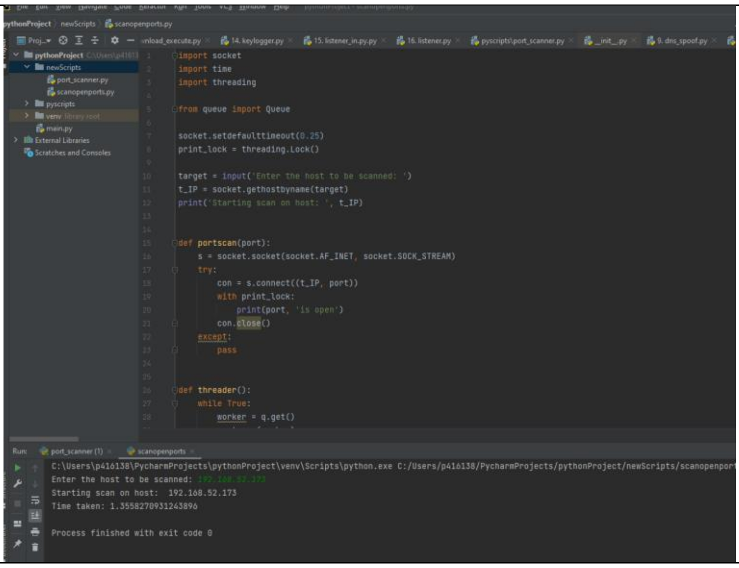
Target: 192.168.52.166 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.52.166

```
nmap -T4 -A -v 192.168.52.166

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-17 03:31 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating ARP Ping Scan at 03:31
Scanning 192.168.52.166 [1 port]
Completed ARP Ping Scan at 03:31, 1.44s elapsed (1 total hosts)
Nmap scan report for 192.168.52.166 [host down]
NSE: Script Post-scanning.
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Initiating NSE at 03:31
Completed NSE at 03:31, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.93 seconds
           Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```



Python script to scan host and find open ports



```python
import socket
import time
import threading

from queue import Queue

socket.setdefaulttimeout(0.25)
print_lock = threading.Lock()

target = input('Enter the host to be scanned: ')
t_IP = socket.gethostbyname(target)
print('Starting scan on host: ', t_IP)


def portscan(port):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        con = s.connect((t_IP, port))
        with print_lock:
            print(port, 'is open')
        con.close()
    except:
        pass


def threader():
    while True:
        worker = q.get()
```

```
C:\Users\p416138\PycharmProjects\pythonProject\venv\Scripts\python.exe C:/Users/p416138/PycharmProjects/pythonProject/newScripts/scanopenport
Enter the host to be scanned: 192.168.52.173
Starting scan on host:  192.168.52.173
Time taken: 1.3558270931243896

Process finished with exit code 0
```