2024

Week 4

PENETRATION TESTING INTERNSHIP

MICHELLE PANTELOURIS

1. The number of ports open are 29.

```
┌──(michelle㉿kali)-[~]
└─$ nmap -p0-65535 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 07:17 GMT
Stats: 0:32:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 62.90% done; ETC: 08:09 (0:19:20 remaining)
Stats: 0:32:49 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 62.99% done; ETC: 08:09 (0:19:17 remaining)
Stats: 0:36:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 69.59% done; ETC: 08:09 (0:15:54 remaining)
Stats: 0:41:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 79.38% done; ETC: 08:08 (0:10:40 remaining)
Stats: 0:46:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 89.12% done; ETC: 08:09 (0:05:39 remaining)
Nmap scan report for 192.168.0.122
Host is up (0.0054s latency).
Not shown: 65506 filtered tcp ports (no-response), 1 filtered tcp ports (net-
unreach)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35867/tcp open  unknown
36483/tcp open  unknown
42155/tcp open  unknown
50357/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3110.68 seconds
```

2. The output that was displayed for this port is shown in the image below. The service is Microsoft-DS and the reason is syn-ack. syn-ack is a tcp handshake.

```
┌──(michelle㉿kali)-[~]
└─$ nmap 192.168.0.122 -p 445 --reason
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 08:18 GMT
Nmap scan report for 192.168.0.122
Host is up, received syn-ack (0.0071s latency).

PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

3. The state of this port is filtered.

```
┌──(michelle㉿kali)-[~]
└─$ nmap -p 8782 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 08:42 GMT
Nmap scan report for 192.168.0.122
Host is up (0.0043s latency).

PORT     STATE    SERVICE
8782/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

4. The flag that only displays open ports is *'—open'*.

```
  --open: Only show open (or possibly open) ports
```

5. The port number is 137

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -sU 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 03:15 GMT
Nmap scan report for 192.168.0.122
Host is up (0.030s latency).
Not shown: 996 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
```

6. Scan relating to -sn.

```
└─# nmap -h
Nmap 7.94SVN ( 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
```

7. The flag to save the file to XML format is -oX.

```
root@kali: /home/michelle
File  Actions  Edit  View  Help
  --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
  --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
```

8. The flag to save the output to normal format is -oN.

```
root@kali: /home/michelle
File  Actions  Edit  View  Help
  --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
  --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
```

9. The flag to save the output to Grepable format is -oG.

```
root@kali: /home/michelle
File  Actions  Edit  View  Help
  --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
  --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
```

10. The file that contains the mac address vendors is nmap-mac-prefixes

```
┌──(root㉿kali)-[/usr/share/nmap]
└─# ls
nmap-mac-prefixes  nmap-rpc            nmap.dtd      nselib
nmap-os-db         nmap-service-probes nmap.xsl      scripts
nmap-protocols     nmap-services       nse_main.lua

┌──(root㉿kali)-[/usr/share/nmap]
└─#
```

11. 23 ports are scanned when executing the *'nmap 192.168.0.122'* command.

```
root@kali: /usr/share/nmap
File  Actions  Edit  View  Help
Host is up (0.018s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  closed pop3
111/tcp  open   rpcbind
135/tcp  closed msrpc
139/tcp  open   netbios-ssn
199/tcp  closed smux
256/tcp  closed fw1-secureremote
443/tcp  closed https
445/tcp  open   microsoft-ds
513/tcp  open   login
587/tcp  closed submission
995/tcp  closed pop3s
1025/tcp closed NFS-or-IIS
1720/tcp closed h323q931
1723/tcp closed pptp
3306/tcp open   mysql
5900/tcp open   vnc
8080/tcp closed http-proxy
```

12. The state of ftp when running the command is open.

```
21/tcp    open    ftp
```

13. There are 3 ports found, 20,21 and 22.

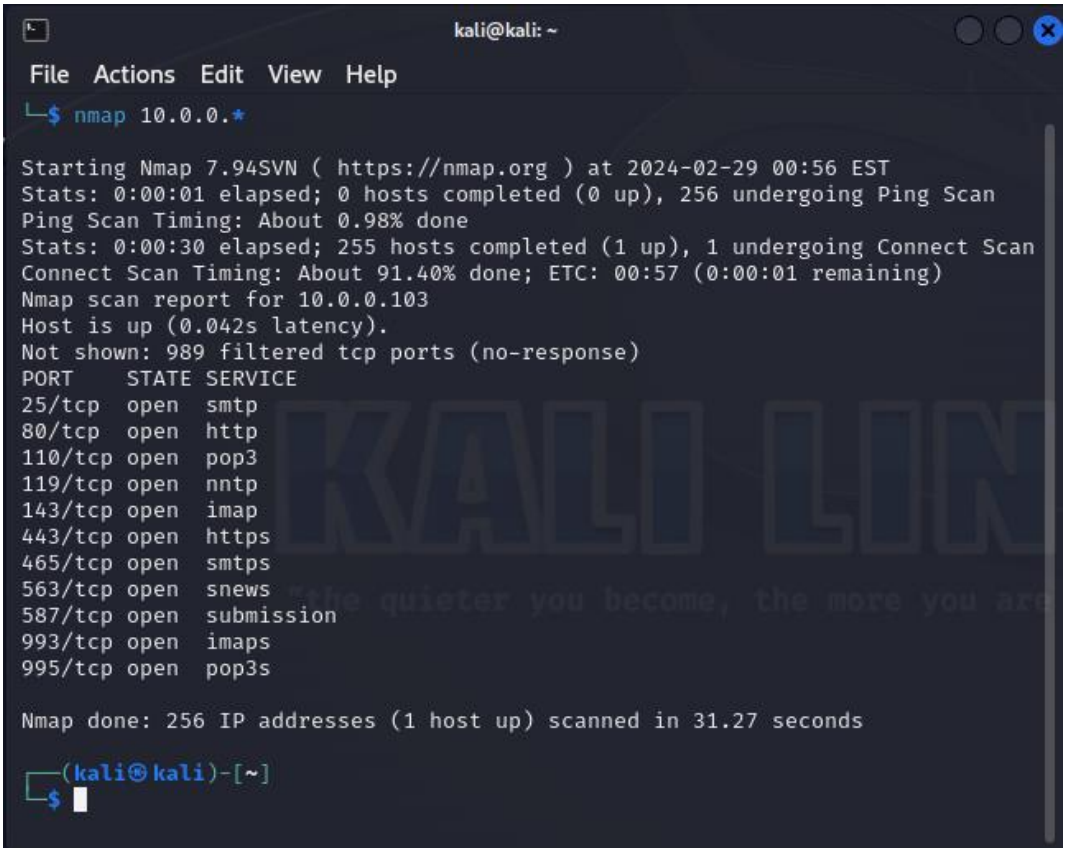
```
┌──(root㉿kali)-[/usr/share/nmap]
└─# nmap 192.168.0.122 -p 22,21,20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 05:02 GMT
Nmap scan report for 192.168.0.122
Host is up (0.0057s latency).

PORT    STATE    SERVICE
20/tcp filtered ftp-data
21/tcp open     ftp
22/tcp open     ssh

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds

┌──(root㉿kali)-[/usr/share/nmap]
└─#
```

14. 18 ports are scanned.

```
File  Actions  Edit  View  Help
Nmap scan report for 192.168.0.122
Host is up (0.028s latency).
Not shown: 82 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds

┌──(root㉿kali)-[/usr/share/nmap]
└─#
```

15. 256 IP Addresses were found.

16. The number of IP Addresses scanned were 256.



17. The number of IP Addresses found are 91.

```
root@kali: /home/michelle
File  Actions  Edit  View  Help
All 1000 scanned ports on 10.0.0.96 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.97
Host is up (0.010s latency).
All 1000 scanned ports on 10.0.0.97 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.98
Host is up (0.036s latency).
All 1000 scanned ports on 10.0.0.98 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.99
Host is up (0.030s latency).
All 1000 scanned ports on 10.0.0.99 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.100
Host is up (0.046s latency).
All 1000 scanned ports on 10.0.0.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 91 IP addresses (91 hosts up) scanned in 9922.02 seconds

┌──(root㉿kali)-[/home/michelle]
└─#
```

18. The number of IP Addresses scanned were 256.

```
root@kali: /home/michelle
File  Actions  Edit  View  Help
All 1000 scanned ports on 10.0.0.251 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.252
Host is up (0.015s latency).
All 1000 scanned ports on 10.0.0.252 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.253
Host is up (0.040s latency).
All 1000 scanned ports on 10.0.0.253 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.254
Host is up (0.022s latency).
All 1000 scanned ports on 10.0.0.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.255
Host is up (0.024s latency).
All 1000 scanned ports on 10.0.0.255 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 256 IP addresses (256 hosts up) scanned in 3421.62 seconds

┌──(root㉿kali)-[/home/michelle]
└─#
```

19. Output of domain scanning using nmap.

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -oA /root/Desktop -v rest.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 13:28 GMT
Initiating Ping Scan at 13:28
Scanning rest.vulnweb.com (35.81.188.86) [4 ports]
Completed Ping Scan at 13:28, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:28
Completed Parallel DNS resolution of 1 host. at 13:28, 0.06s elapsed
Initiating SYN Stealth Scan at 13:28
Scanning rest.vulnweb.com (35.81.188.86) [1000 ports]
Completed SYN Stealth Scan at 13:28, 4.03s elapsed (1000 total ports)
Nmap scan report for rest.vulnweb.com (35.81.188.86)
Host is up (0.00051s latency).
rDNS record for 35.81.188.86: ec2-35-81-188-86.us-west-2.compute.amazonaws.co
m
All 1000 scanned ports on rest.vulnweb.com (35.81.188.86) are in ignored stat
es.
Not shown: 1000 filtered tcp ports (no-response)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds
           Raw packets sent: 2007 (88.272KB) | Rcvd: 4 (160B)
```

Output of the scan.

```
┌──(root㉿kali)-[~]
└─# cat Desktop.gnmap
# Nmap 7.94SVN scan initiated Thu Feb 29 13:28:30 2024 as: nmap -oA /root/Desktop -v rest.vulnwe
b.com
# Ports scanned: TCP(1000;1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,
106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,
306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-
545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,
722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,
995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-113
2,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198
-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,
1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1
556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,18
05,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-202
2,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126
,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,
2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2
717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,30
11,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,330
6,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689
-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,
3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4
443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-50
61,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,543
1-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810
-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,
5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6
510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,69
69,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,762
7,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045
,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,
8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9
071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,95
35,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,
10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-
11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-
15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,
18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,
23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,
31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-
44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,
50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,
56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389)
 UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 35.81.188.86 (ec2-35-81-188-86.us-west-2.compute.amazonaws.com)   Status: Up
Host: 35.81.188.86 (ec2-35-81-188-86.us-west-2.compute.amazonaws.com)   Ports:  Ignored State: f
iltered (1000)
# Nmap done at Thu Feb 29 13:28:39 2024 -- 1 IP address (1 host up) scanned in 9.19 seconds
```

20. The ip address for this website is 35.81.188.86.

```
┌──(root㉿kali)-[~]
└─# nmap -sn rest.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 13:35 GMT
Nmap scan report for rest.vulnweb.com (35.81.188.86)
Host is up (0.00027s latency).
rDNS record for 35.81.188.86: ec2-35-81-188-86.us-west-2.compute.amazonaws.com
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

21. There are 13 ports open.

```
┌──(root㉿kali)-[~]
└─# sudo nmap -sS 192.168.0.122 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 05:50 GMT
Warning: 192.168.0.122 giving up on port because retransmission cap hit (6).
Stats: 0:03:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 05:54 (0:00:00 remaining)
Nmap scan report for 192.168.0.122
Host is up (0.15s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
111/tcp  open  rpcbind
513/tcp  open  login
514/tcp  open  shell
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
6000/tcp open  X11
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 227.87 seconds
```

22. To scan ports 21,22,80 I used the command was *'nmap -p 21,22,80 192.168.0.122'*

```
┌──(root㉿kali)-[~]
└─# nmap -p 21,22,80 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 06:16 GMT
Nmap scan report for 192.168.0.122
Host is up (0.00034s latency).

PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

23. Execute a TCP ACK Scan

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -T5 -sA 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 03:35 GMT
Nmap scan report for 192.168.0.122
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.0.122 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

24. Scan for UDP ports

```
root@kali: /home/michelle
File  Actions  Edit  View  Help

┌──(michelle㉿kali)-[~]
└─$ sudo su
[sudo] password for michelle:
┌──(root㉿kali)-[/home/michelle]
└─# nmap -sU -T4  192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 06:43 GMT
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 28.60% done; ETC: 06:49 (0:03:42 remaining)
Stats: 0:05:29 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 42.45% done; ETC: 06:56 (0:07:27 remaining)
Nmap scan report for 192.168.0.122
Host is up (0.0063s latency).
Not shown: 996 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 1593.27 seconds

┌──(root㉿kali)-[/home/michelle]
└─#
```

25. Perform a comprehensive scan of all ports.

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/michelle]
└─# nmap -p- -A 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 07:13 GMT
Stats: 0:09:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 45.61% done; ETC: 07:33 (0:10:58 remaining)
Nmap scan report for 192.168.0.122
Host is up (0.0017s latency).
Not shown: 65317 filtered tcp ports (no-response), 207 closed tcp ports (rese
t)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
22/tcp   open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
23/tcp   open  tcpwrapped
25/tcp   open  tcpwrapped
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-03-01T07:34:10+00:00; -2s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  tcpwrapped
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  tcpwrapped
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  tcpwrapped
139/tcp  open  tcpwrapped
445/tcp  open  tcpwrapped Samba smbd 3.0.20-Debian
3306/tcp open  tcpwrapped
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 15
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, SupportsCompression, Support41Aut
h, LongColumnFlag, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41P
rotocolNew
|   Status: Autocommit
|_  Salt: tvs][1"RWA{i}Y$Enz<X
5900/tcp open  tcpwrapped
OS fingerprint not ideal because: Didn't receive UDP response. Please try aga
in with -sSU
No OS matches for host
Network Distance: 2 hops

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

26. Use service version detection on port 21 (FTP).

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -sV -p 21 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 08:05 GMT
Nmap scan report for 192.168.0.122
Host is up (0.018s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

27. Identify the version of the SSH service.

```
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

28. Perform service version detection on port 80 (HTTP).

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -sV -p 80 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 08:10 GMT
Nmap scan report for 192.168.0.122
Host is up (0.00053s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
```

29. Detect the version of the Telnet service.

```
23/tcp   open  telnet      Linux telnetd
```

30. Identify the versions of any running database services (e.g., MySQL, PostgreSQL).

```
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

31. Utilize Nmap to detect the operating system of the machine.

```
└─# nmap -O 192.168.0.122 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 03:43 GMT
Warning: 192.168.0.122 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.122
Host is up (0.045s latency).
Not shown: 948 filtered tcp ports (no-response), 29 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.24 seconds
```

Nmap reports Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%).

32. Verify the accuracy of the operating system detection by Nmap against the actual OS running on the machine.

```
msfadmin@metasploitable:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
msfadmin@metasploitable:~$
```

We can see that Ubuntu is the actual OS.

33. Run a script to identify common vulnerabilities on the FTP service.

```
└─# nmap -sCV -p 21 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 03:46 GMT
Nmap scan report for 192.168.0.122
Host is up (0.00030s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.177
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

We can see anonymous login is allowed.

34. Use Nmap scripting to identify potential security issues with the Telnet.

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -sCV -p 23 192.168.0.122 --script telnet*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 03:49 GMT
Nmap scan report for 192.168.0.122
Host is up (0.0027s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
| telnet-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 1185 guesses in 353 seconds, average tps: 3.5
| telnet-encryption:
|_  Telnet server does not support encryption
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see that valid user credentials were found, and the protocol does not support encryption.

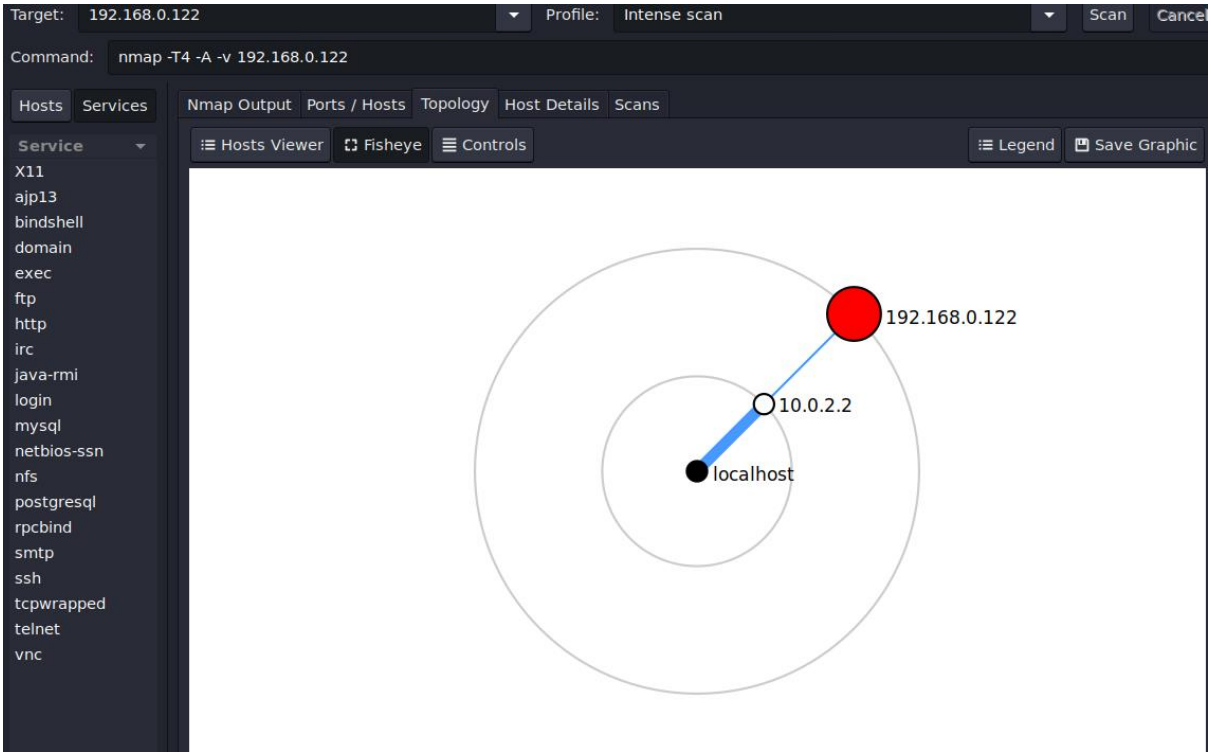
35. Execute a script to gather more information about the HTTP service (port 80).

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -sCV -p 80 192.168.0.122 --script http-enum -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 04:05 GMT
Nmap scan report for 192.168.0.122
Host is up (0.00019s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.81 seconds

┌──(root㉿kali)-[/home/michelle]
└─# nmap -sCV -p 80 192.168.0.122 --script http-vuln* -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 04:06 GMT
Nmap scan report for 192.168.0.122
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.85 seconds
```

36. Performed a traceroute on the machine to identify the network path.

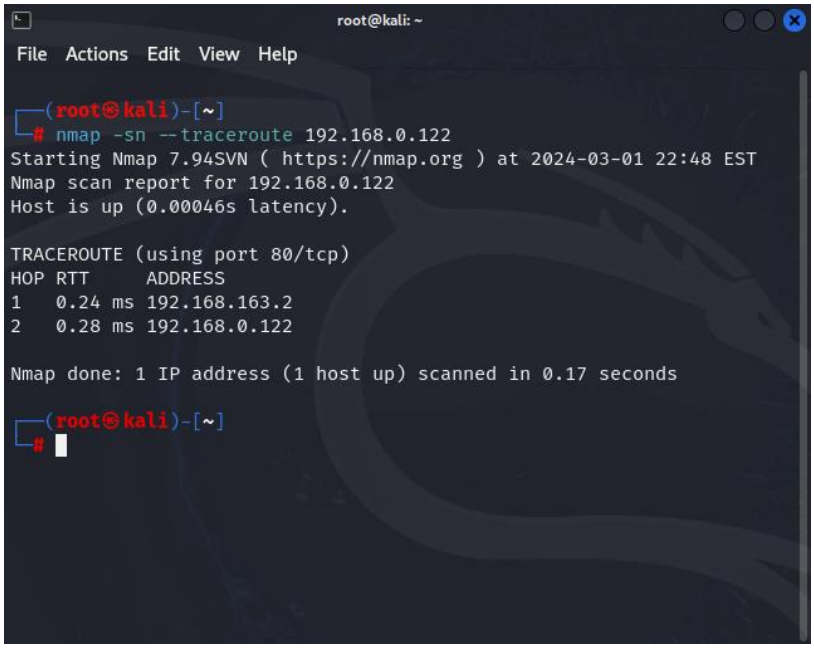
```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# nmap -sn --traceroute 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 22:48 EST
Nmap scan report for 192.168.0.122
Host is up (0.00046s latency).

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.24 ms 192.168.163.2
2   0.28 ms 192.168.0.122

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

┌──(root㉿kali)-[~]
└─#
```

37. Map the network topology of the machine using Nmap.



Zenmap was used to generate a graphical representation of the topology.

38. Identify the number of hops between your machine and the target machine using Nmap.



There are two hops between the attacking machine and the victim machine.

39. Check for any firewall restrictions using Nmap against the machine.

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -sCV -p 80 192.168.0.122 --script http-waf* -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 04:09 GMT
Nmap scan report for 192.168.0.122
Host is up (0.00019s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.44 seconds
```

Nmap reports no WAF.

40. Identify if any intrusion detection/prevention systems are active on machine using Nmap.

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -fD 10.10.10.10 -p 80 192.168.0.122 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 04:57 GMT
Nmap scan report for 192.168.0.122
Host is up (0.0027s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Sending fragmented packets and spoofing our IP to 10.10.10.10 shows the http port is filtered.

41. Perform a TCP SYN scan and a TCP connect scan with different timing options.

```
┌──(root㉿kali)-[/home/michelle]
└─# nmap -T4 -sS 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 05:03 GMT
Warning: 192.168.0.122 giving up on port because retransmission cap hit (6).
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 05:05 (0:00:00 remaining)
Nmap scan report for 192.168.0.122
Host is up (2.0s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

This is a SYN scan with -T4 timing

```
File  Actions  Edit  View  Help
[sudo] password for michelle:
┌──(root㉿kali)-[/home/michelle]
└─# nmap -T5 -sT 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 16:03 GMT
Nmap scan report for 192.168.0.122
Host is up (0.010s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
2049/tcp open  nfs
3306/tcp open  mysql
5900/tcp open  vnc
6000/tcp open  X11

Nmap done: 1 IP address (1 host up) scanned in 10.61 seconds

┌──(root㉿kali)-[/home/michelle]
└─# 
```

This is a TCP connect scan with T5 timing.

42. Null Scan on port 80.

```
┌──(root㉿kali)-[~]
└─# nmap -sN 192.168.0.122 -p 80 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 23:56 EST
Nmap scan report for 192.168.0.122
Host is up (0.00046s latency).

PORT   STATE         SERVICE
80/tcp open|filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

43. Xmas Scan

```
┌──(root㉿kali)-[~]
└─# nmap -sX 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 00:03 EST
Nmap scan report for 192.168.0.122
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.0.122 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

44. Save the Nmap scan results in different output formats (XML, grepable, normal).

```
└─# nmap -T5 -sCV -p- -oA /root/Output 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 05:21 GMT
Warning: 192.168.0.122 giving up on port because retransmission cap hit (2).
Stats: 0:04:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 05:25 (0:00:04 remaining)
Nmap scan report for 192.168.0.122
Host is up (0.011s latency).
Not shown: 65471 filtered tcp ports (no-response), 34 closed tcp ports (reset
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
```

```
┌──(root㉿kali)-[/home/michelle]
└─# ls -l /root | grep Output
-rw-r--r-- 1 root root  1696 Mar  2 05:26 Output.gnmap
-rw-r--r-- 1 root root  5834 Mar  2 05:26 Output.nmap
-rw-r--r-- 1 root root 24186 Mar  2 05:26 Output.xml
```

45. The following ports are open and are potentially vulnerable:
    21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 80 (HTTP), 3306 (MySQL), 2121 (FTP), 3632 (Unknown), 5900 (VNC), 6667 (IRC), 8009 (Jserv), 8180 (Tomcat)

46. Filter the Nmap scan output to display only the open ports/services.

```
┌──(root㉿kali)-[~]
└─# awk '/^Host:/{ip=$2} /Ports:/{gsub("/open/", "\n/open/", $0); gsub("/closed/", "\n/closed/", $0); gsub("/filtered/", "\n/filtered/", $0); print ip,$0}' Output.gnmap | awk -F '[ /]+' '/open/{print $3"/"$5, $7, $6, $8}'

tcp/vsftpd , 2.3.4 22
tcp/OpenSSH Debian 4.7p1 8ubuntu1
tcp/Linux , telnetd 25
tcp/Postfix , smtpd 53
tcp/ISC 9.4.2 BIND ,
tcp/Apache 2.2.8 httpd ((Ubuntu)
tcp/2 #100000) (RPC ,
tcp/Samba 3.X smbd ~
tcp/Samba 3.0.20-Debian smbd (workgroup:
tcp/netkit-rsh , rexecd 513
tcp/,  514
tcp/,  1099
tcp/GNU grmiregistry Classpath ,
tcp/Metasploitable shell root ,
tcp/2-4 #100003) (RPC ,
tcp/ProFTPD , 1.3.1 3306
tcp/MySQL , 5.0.51a-3ubuntu5 3632
tcp/distccd ((GNU) v1 4.2.4
tcp/PostgreSQL 8.3.0 DB ~
tcp/VNC 3.3) (protocol ,
tcp/(access , denied) 6667
tcp/UnrealIRCd 6697 ,
tcp/UnrealIRCd 8009 ,
tcp/Apache (Protocol Jserv v1.3)
tcp/Apache JSP Tomcat|Coyote engine
tcp/Ruby RMI DRb (Ruby
tcp/1 #100024) (RPC ,
tcp/GNU grmiregistry Classpath ,
tcp/1-4 #100021) (RPC ,
tcp/1-3 #100005) (RPC
```

47&48. Exploitable software/ versions.

Port 21

Is vsftpd-2.3 4 vulnerable?

vsftpd is prone to a backdoor vulnerability because the 'vsftpd-2.3. 4. tar. gz' source package file contains a backdoor.

Port 80

Fixed in Apache HTTP Server 2.2.8

moderate: mod_imagemap XSS (CVE-2007-5000)

A flaw was found in the mod_imagemap module. On sites where mod_imagemap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

Reported to security team	2007-10-23
Issue public	2007-12-11
Update 2.2.8 released	2008-01-19
Update 2.0.63 released	2008-01-19
Update 1.3.41 released	2008-01-19
Affects	2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0, 2.0.61, 2.0.59, 2.0.58, 2.0.55, 2.0.54, 2.0.53, 2.0.52, 2.0.51, 2.0.50, 2.0.49, 2.0.48, 2.0.47, 2.0.46, 2.0.45, 2.0.44, 2.0.43, 2.0.42, 2.0.40, 2.0.39, 2.0.37, 2.0.36, 2.0.35, 1.3.39, 1.3.37, 1.3.36, 1.3.35, 1.3.34, 1.3.33, 1.3.32, 1.3.31, 1.3.29, 1.3.28, 1.3.27, 1.3.26, 1.3.24, 1.3.22, 1.3.20, 1.3.19, 1.3.17, 1.3.14, 1.3.12, 1.3.11, 1.3.9, 1.3.6, 1.3.4, 1.3.3, 1.3.2, 1.3.1, 1.3.0

moderate: mod_status XSS (CVE-2007-6388)

A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.

Reported to security team	2007-12-15
Issue public	2008-01-02
Update 2.2.8 released	2008-01-19
Update 2.0.63 released	2008-01-19
Update 1.3.41 released	2008-01-19
Affects	2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0, 2.0.61, 2.0.59, 2.0.58, 2.0.55, 2.0.54, 2.0.53, 2.0.52, 2.0.51, 2.0.50, 2.0.49, 2.0.48, 2.0.47, 2.0.46, 2.0.45, 2.0.44, 2.0.43, 2.0.42, 2.0.40, 2.0.39, 2.0.37, 2.0.36, 2.0.35, 1.3.39, 1.3.37, 1.3.36, 1.3.35, 1.3.34, 1.3.33, 1.3.32, 1.3.31, 1.3.29, 1.3.28, 1.3.27, 1.3.26, 1.3.24, 1.3.22, 1.3.20, 1.3.19, 1.3.17, 1.3.14, 1.3.12, 1.3.11, 1.3.9, 1.3.6, 1.3.4, 1.3.3, 1.3.2

low: mod_proxy_balancer XSS (CVE-2007-6421)

A flaw was found in the mod_proxy_balancer module. On sites where mod_proxy_balancer is enabled, a cross-site scripting attack against an authorized user is possible.

Port 212

SQL injection vulnerability in ProFTPD Server 1.3. 1 through 1.3. 2rc2 allows remote attackers to execute arbitrary SQL commands via a "%" (percent) character in the username, which introduces a "'" (single quote) character during variable substitution by mod_sql.

CVEDetails
https://www.cvedetails.com › version_id-428078 › Proft...

Proftpd Project Proftpd version 1.3.1 : Security vulnerabilities ...

About featured snippets • Feedback

Port 3306

Description

The version of MySQL installed on the remote host is earlier than 5.0.51a / 5.1.23 / 6.0.4 and thus reportedly affected by the following two vulnerabilities :

- An attacker may be able to cause the federated handler and daemon to crash when the federated engine issues a SHOW TABLE STATUS LIKE query by having a malicious server return a response with less than 14 columns.
(MySQL bug #29801 / CVE-2007-6304)

- It fails to update the DEFINER value of a view when that is altered, which could allow an authenticated user to gain additional access through the ALTER VIEW. (MySQL bug #29908 / CVE-2007-6303)

Description

The version of PostgreSQL installed on the remote host is 8.3.x prior to 8.3.18, and is, therefore, potentially affected by multiple vulnerabilities :

- Permissions on a function called by a trigger are not properly checked. (CVE-2012-0866)
- Line breaks in object names can be exploited to execute arbitrary SQL commands when reloading a pg_dump file.
(CVE-2012-0868)

Port-8009

This is an LFI vulnerability in AJP service. An attacker can exploit Ghostcat vulnerability and read the contents of configuration files and source code files of all webapps deployed on Tomcat.

Port -8180

Cross-Site Scripting (XSS), Directory Traversal, Denial of Service (DoS), Authentication Bypass, Remote Code Execution (RCE), SQL Injection, Session Management Flaws, Insecure Default Configurations, XML External Entity (XXE) Injection, Insecure Deserialization.

49. A suspicious service is running on an unknown port on the machine. Use Nmap to investigate and provide details about the service.

Two ports were identified as suspicious in nature; 1542 and 3632:

```
┌──(root㉿kali)-[~]
└─# nmap -sCV 192.168.0.122 -p 1524,3632 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 05:46 GMT
Nmap scan report for 192.168.0.122
Host is up (0.00032s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell
3632/tcp open  distccd   distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
```

The former indicates a root shell running on this port. The latter indicates a vulnerable service, which is susceptible to the DistCC Daemon Command Execution vulnerability.

50. Check for SSL/TLS versions and ciphers supported by services (if any) on the machine.

```
┌──(root㉿kali)-[~]
└─# sslscan 192.168.0.122:80
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 192.168.0.122

Testing SSL server 192.168.0.122 on port 80 using SNI name 192.168.0.122

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   disabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Connection failed - unable to determine TLS Fallback SCSV support

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:

  Supported Server Cipher(s):
    Unable to parse certificate
    Unable to parse certificate
    Unable to parse certificate
    Unable to parse certificate
Certificate information cannot be retrieved.
```

No SSL or TLS versions were running on the victim machine.

51. Perform an Nmap scan to identify any hidden or less commonly used ports.

```
┌──(root㉿kali)-[~]
└─# awk '/^Host:/{ip=$2} /Ports:/{gsub("/c

tcp/vsftpd , 2.3.4 22
tcp/OpenSSH Debian 4.7p1 8ubuntu1
tcp/Linux , telnetd 25
tcp/Postfix , smtpd 53
tcp/ISC 9.4.2 BIND ,
tcp/Apache 2.2.8 httpd ((Ubuntu)
tcp/2 #100000) (RPC ,
tcp/Samba 3.X smbd -
tcp/Samba 3.0.20-Debian smbd (workgroup:
tcp/netkit-rsh , rexecd 513
tcp/,  514
tcp/,  1099
tcp/GNU grmiregistry Classpath ,
tcp/Metasploitable shell root ,
tcp/2-4 #100003) (RPC ,
tcp/ProFTPD , 1.3.1 3306
tcp/MySQL , 5.0.51a-3ubuntu5 3632
tcp/distccd ((GNU) v1 4.2.4
tcp/PostgreSQL 8.3.0 DB -
tcp/VNC 3.3) (protocol ,
tcp/(access , denied) 6667
tcp/UnrealIRCd 6697 ,
tcp/UnrealIRCd 8009 ,
tcp/Apache (Protocol Jserv v1.3)
tcp/Apache JSP Tomcat|Coyote engine
tcp/Ruby RMI DRb (Ruby
tcp/1 #100024) (RPC ,
tcp/GNU grmiregistry Classpath ,
tcp/1-4 #100021) (RPC ,
tcp/1-3 #100005) (RPC
```

This is the full list of running TCP services.

52. After looking through the results of the nmap scan I have noticed all of the software versions are outdated and half are vulnerable to attacks as shown in the results above. Security measures I would suggest, to enhance the security of the machine is to firstly update all of the outdated software. Doing this is essential because older software will not be equipped to mitigate any of the newer attacks. Setting up a firewall and patching them on a regular basis is key when protecting open ports.

Port 23 allows users to login with the username and password both being ‘user’. This can be very easy for an attacker to figure out or to brute force. The best course of action for this is to create a complex password or to set up for the passwords to be changed everyday.

Port 21 allows anonymous ftp login, which will allow anyone to login without legitimate credentials and transfer any files they want. The best way to prevent this is to disable the ftp service and use protocols that support encrypted communications. If it is not possible to disable the ftp services, then ensure that there are valid credentials that are required to login.

Port 1542 has a root shell running on it that has no credentials. Which means anyone can login. The best course of action is to turn the root shell off. Root users can login via ssh.