eLearnSecurity
Forging security professionals

SCANNING AND OS FINGERPRINTING

PENETRATION TESTING | SECTION 3 MODULE 2 | LAB #8

LAB

1. Description

In this lab you will be connected to an enterprise network with some clients and servers. You have to map the network.

2. Goals

- Run a ping scan with *fping*
- Run a ping scan with *nmap*, do you find any differences? Can you tell why?
- Perform a SYN scan against the targets. Identify clients and servers.
- Identify the version of every daemon listening on the network
- Identify, if it is possible, the operating system running on each host.

3. Tools

The best tools for this lab are:

- fping
- nmap

SOLUTIONS

Please go ahead **ONLY** if you have **COMPLETED** the lab or you are stuck! Checking the solutions before actually trying the concepts and techniques you studied in the course, will dramatically reduce the benefits of a hands-on lab!

[This page intentionally left blank]

4. Solution Steps

4.1. Find the Network Configuration

After connecting to the lab, check the network configuration of the TAP interface. Then use this information to configure your scans.

```
tap0      Link encap:Ethernet  HWaddr d6:b4:d8:c8:fe:d4
          inet addr:10.142.111.240  Bcast:10.142.111.255
Mask:255.255.255.0
          inet6 addr: fe80::d4b4:d8ff:fec8:fed4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21025 errors:0 dropped:57 overruns:0 frame:0
          TX packets:49948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:8167465 (7.7 MiB)  TX bytes:3566191 (3.4 MiB)
```

According to the netmask, the network part of the IP address is 24 bits long.

4.2. Perform a Ping Scan with Fping

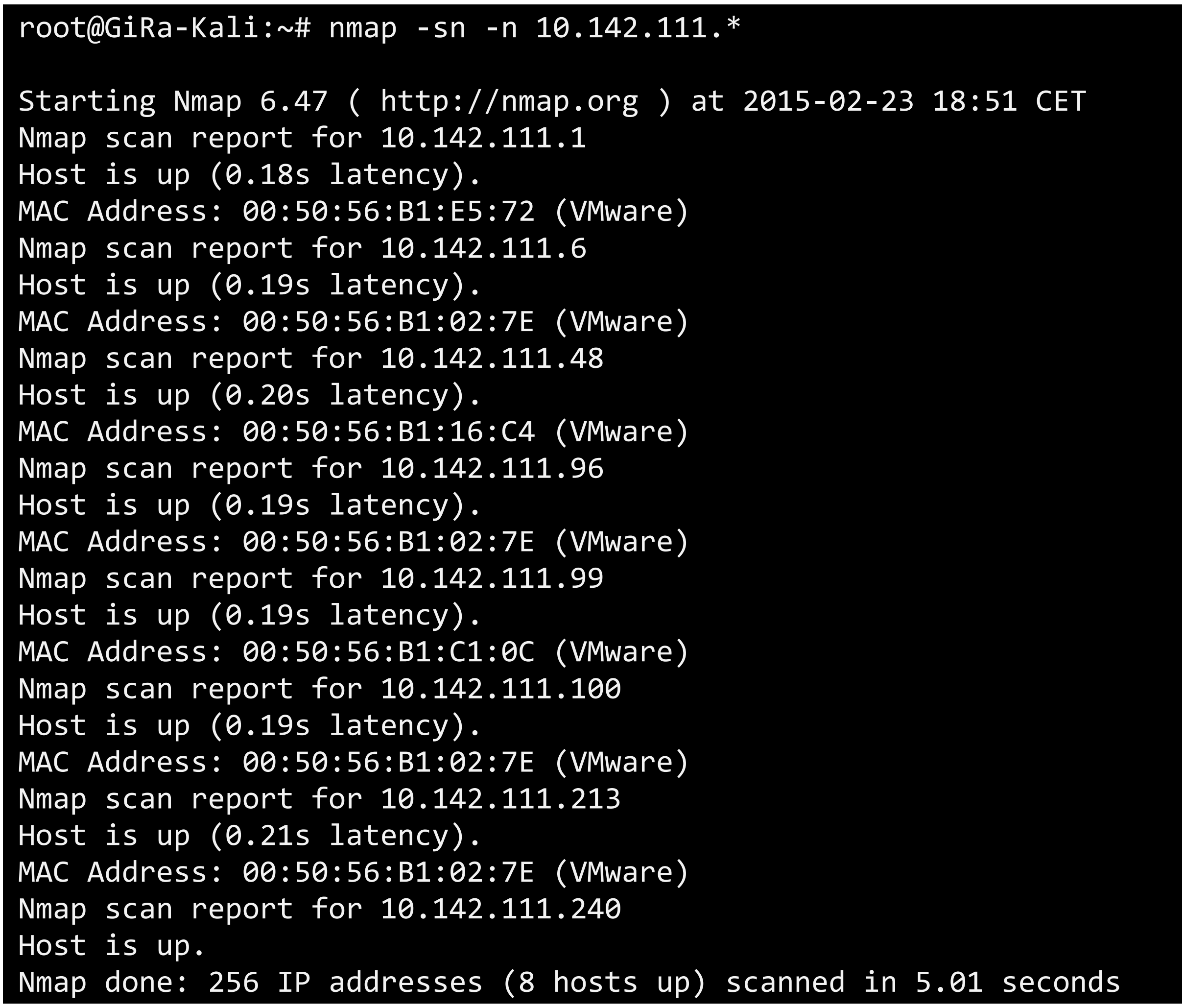
Run a ping scan on the entire network with *fping*.

```
# fping  -a -g 10.142.111.0/24 2> /dev/null
10.142.111.1
10.142.111.6
10.142.111.48
10.142.111.96
10.142.111.99
10.142.111.100
10.142.111.240
```

Fping reports 6 hosts and our attacker machine.

4.3. Run a Ping Scan with Nmap

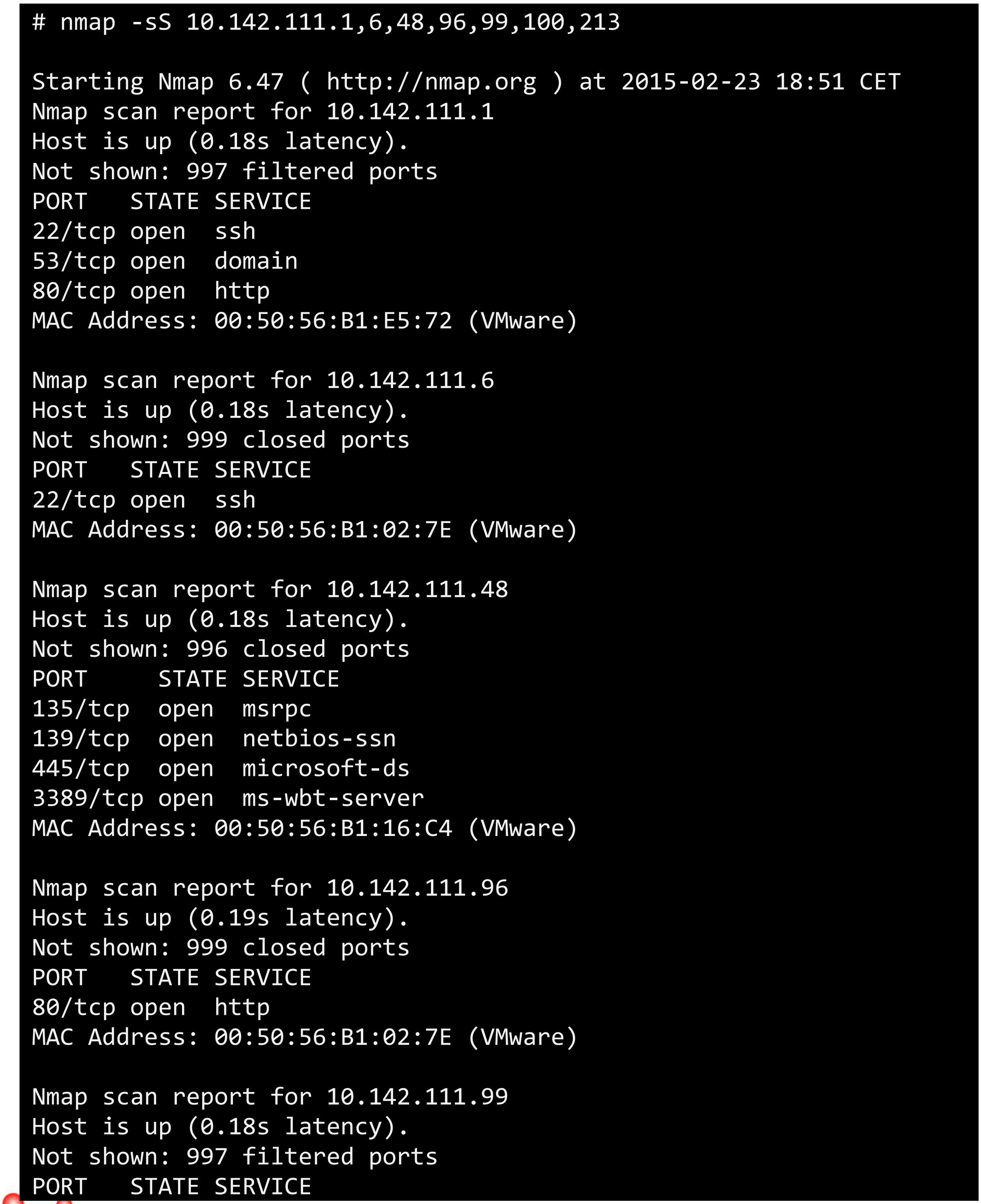
Running a ping scan with nmap reports 7 hosts. There is probably a host that does not respond to ICMP echo requests, but that has a service listening on the network.



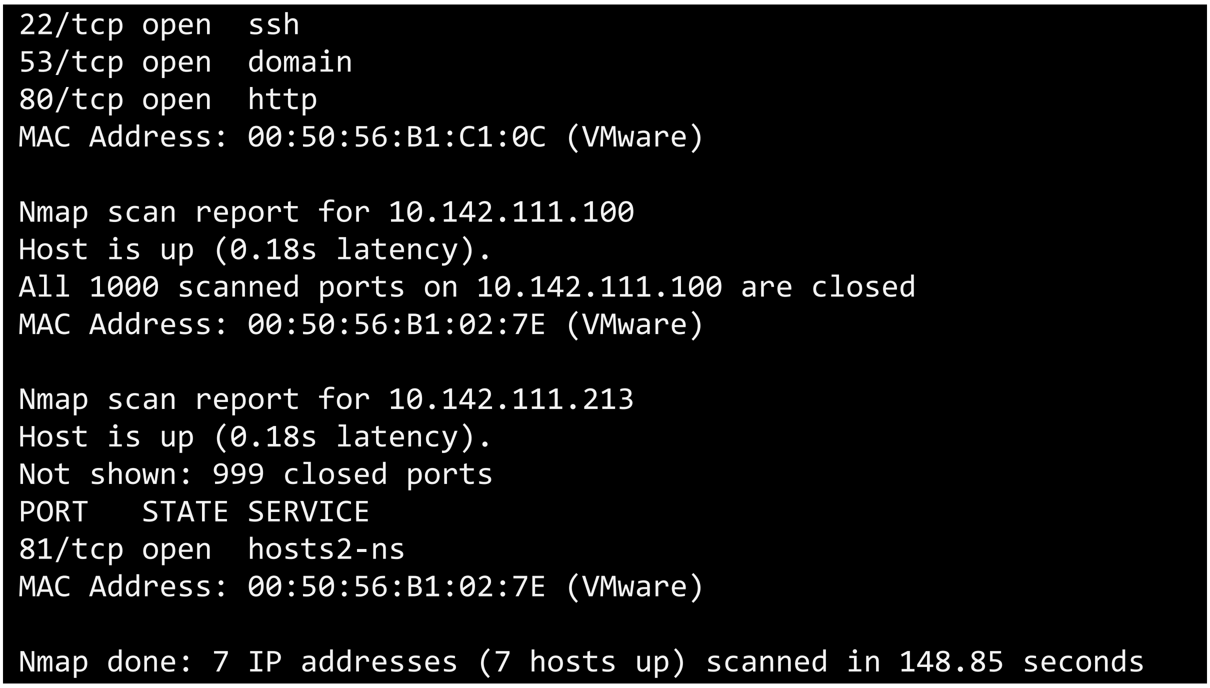
```
root@GiRa-Kali:~# nmap -sn -n 10.142.111.*

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-23 18:51 CET
Nmap scan report for 10.142.111.1
Host is up (0.18s latency).
MAC Address: 00:50:56:B1:E5:72 (VMware)
Nmap scan report for 10.142.111.6
Host is up (0.19s latency).
MAC Address: 00:50:56:B1:02:7E (VMware)
Nmap scan report for 10.142.111.48
Host is up (0.20s latency).
MAC Address: 00:50:56:B1:16:C4 (VMware)
Nmap scan report for 10.142.111.96
Host is up (0.19s latency).
MAC Address: 00:50:56:B1:02:7E (VMware)
Nmap scan report for 10.142.111.99
Host is up (0.19s latency).
MAC Address: 00:50:56:B1:C1:0C (VMware)
Nmap scan report for 10.142.111.100
Host is up (0.19s latency).
MAC Address: 00:50:56:B1:02:7E (VMware)
Nmap scan report for 10.142.111.213
Host is up (0.21s latency).
MAC Address: 00:50:56:B1:02:7E (VMware)
Nmap scan report for 10.142.111.240
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 5.01 seconds
```

4.4. Run a SYN Scan

This time run *nmap* only on the alive hosts.



```
# nmap -sS 10.142.111.1,6,48,96,99,100,213

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-23 18:51 CET
Nmap scan report for 10.142.111.1
Host is up (0.18s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:B1:E5:72 (VMware)

Nmap scan report for 10.142.111.6
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:B1:02:7E (VMware)

Nmap scan report for 10.142.111.48
Host is up (0.18s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:B1:16:C4 (VMware)

Nmap scan report for 10.142.111.96
Host is up (0.19s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:B1:02:7E (VMware)

Nmap scan report for 10.142.111.99
Host is up (0.18s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
```



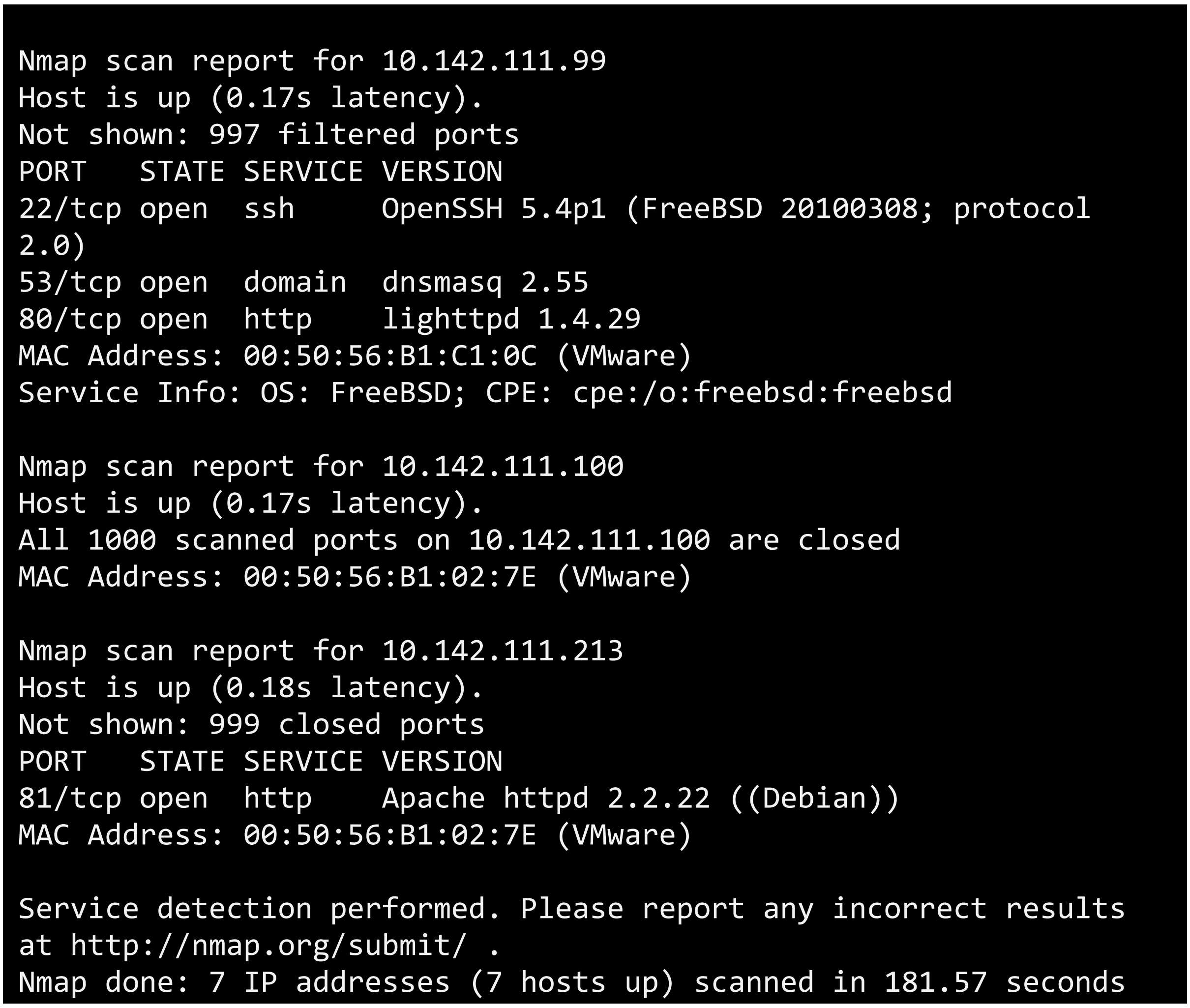
```
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:B1:C1:0C (VMware)

Nmap scan report for 10.142.111.100
Host is up (0.18s latency).
All 1000 scanned ports on 10.142.111.100 are closed
MAC Address: 00:50:56:B1:02:7E (VMware)

Nmap scan report for 10.142.111.213
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
81/tcp open  hosts2-ns
MAC Address: 00:50:56:B1:02:7E (VMware)

Nmap done: 7 IP addresses (7 hosts up) scanned in 148.85 seconds
```

10.142.111.100 is probably a client as it does not listen on the network for connections.

4.5. Version Detection Scan

Run the version detection scan and spot services running on non-conventional default ports.

```
# nmap -sV 10.142.111.1,6,48,96,99,100,213

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-23 18:56 CET
Nmap scan report for 10.142.111.1
Host is up (0.18s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.4p1 (FreeBSD 20100308; protocol
2.0)
53/tcp open  domain  dnsmasq 2.55
80/tcp open  http    lighttpd 1.4.29
MAC Address: 00:50:56:B1:E5:72 (VMware)
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Nmap scan report for 10.142.111.6
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
MAC Address: 00:50:56:B1:02:7E (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.142.111.48
Host is up (0.17s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:50:56:B1:16:C4 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.142.111.96
Host is up (0.17s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
MAC Address: 00:50:56:B1:02:7E (VMware)
```

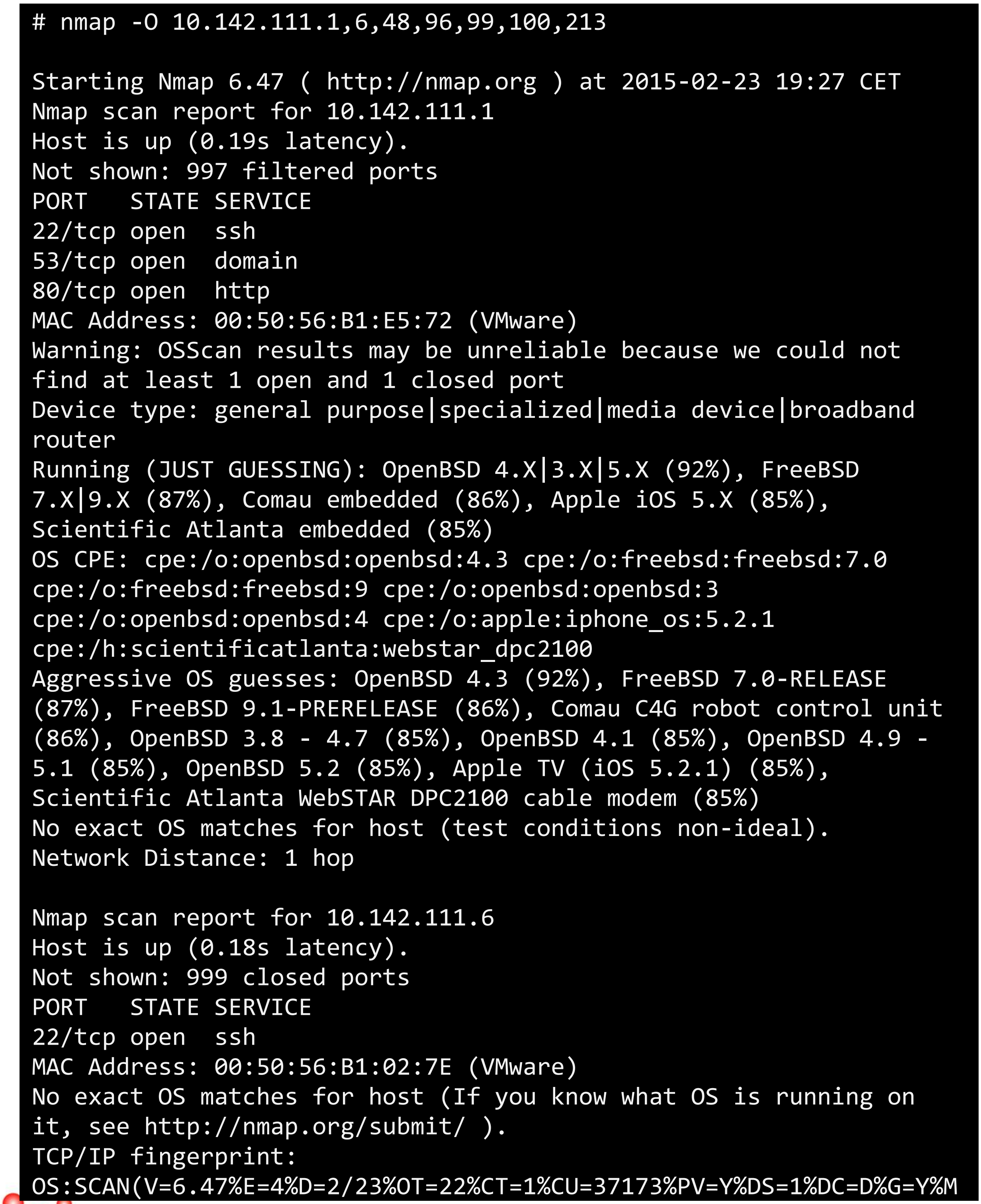


```
Nmap scan report for 10.142.111.99
Host is up (0.17s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.4p1 (FreeBSD 20100308; protocol
2.0)
53/tcp open  domain  dnsmasq 2.55
80/tcp open  http    lighttpd 1.4.29
MAC Address: 00:50:56:B1:C1:0C (VMware)
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Nmap scan report for 10.142.111.100
Host is up (0.17s latency).
All 1000 scanned ports on 10.142.111.100 are closed
MAC Address: 00:50:56:B1:02:7E (VMware)

Nmap scan report for 10.142.111.213
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
81/tcp open  http    Apache httpd 2.2.22 ((Debian))
MAC Address: 00:50:56:B1:02:7E (VMware)

Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
Nmap done: 7 IP addresses (7 hosts up) scanned in 181.57 seconds
```

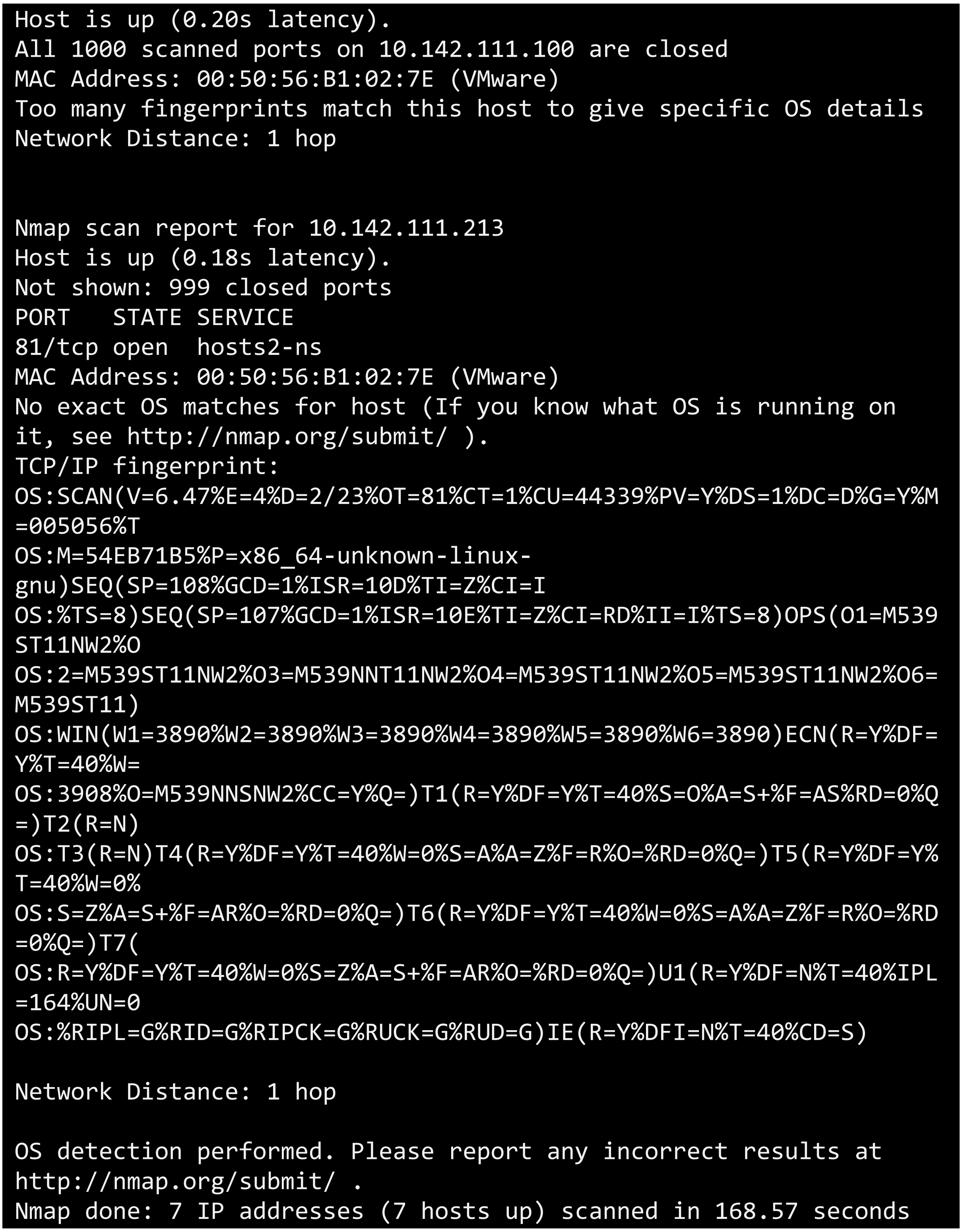
10.142.111.213 runs Apache web server on a not standard port. Please note that this is the host which does not reply to ping echo requests.

4.6. OS Fingerprinting

Fingerprint the operating systems running on the hosts with the -O *nmap* option.



```
# nmap -O 10.142.111.1,6,48,96,99,100,213

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-23 19:27 CET
Nmap scan report for 10.142.111.1
Host is up (0.19s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:B1:E5:72 (VMware)
Warning: OSScan results may be unreliable because we could not
find at least 1 open and 1 closed port
Device type: general purpose|specialized|media device|broadband
router
Running (JUST GUESSING): OpenBSD 4.X|3.X|5.X (92%), FreeBSD
7.X|9.X (87%), Comau embedded (86%), Apple iOS 5.X (85%),
Scientific Atlanta embedded (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:7.0
cpe:/o:freebsd:freebsd:9 cpe:/o:openbsd:openbsd:3
cpe:/o:openbsd:openbsd:4 cpe:/o:apple:iphone_os:5.2.1
cpe:/h:scientificatlanta:webstar_dpc2100
Aggressive OS guesses: OpenBSD 4.3 (92%), FreeBSD 7.0-RELEASE
(87%), FreeBSD 9.1-PRERELEASE (86%), Comau C4G robot control unit
(86%), OpenBSD 3.8 - 4.7 (85%), OpenBSD 4.1 (85%), OpenBSD 4.9 -
5.1 (85%), OpenBSD 5.2 (85%), Apple TV (iOS 5.2.1) (85%),
Scientific Atlanta WebSTAR DPC2100 cable modem (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.142.111.6
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:B1:02:7E (VMware)
No exact OS matches for host (If you know what OS is running on
it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=2/23%OT=22%CT=1%CU=37173%PV=Y%DS=1%DC=D%G=Y%M
=005056%T
OS:M=54EB71B5%P=x86_64-unknown-linux-
gnu)SEQ(SP=105%GCD=2%ISR=10E%TI=Z%CI=I
OS:%TS=8)SEQ(SP=105%GCD=1%ISR=10E%TI=Z%CI=I%II=I%TS=8)OPS(O1=M539S
T11NW2%O2
OS:=M539ST11NW2%O3=M539NNT11NW2%O4=M539ST11NW2%O5=M539ST11NW2%O6=M
539ST11)W
OS:IN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)ECN(R=Y%DF=Y
%T=40%W=3
OS:908%O=M539NNSNW2%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=
)T2(R=N)T
OS:3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T
=40%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
0%Q=)T7(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=
164%UN=0%
OS:RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

Nmap scan report for 10.142.111.48
Host is up (0.18s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:B1:16:C4 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop

Nmap scan report for 10.142.111.96
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:B1:02:7E (VMware)
No exact OS matches for host (If you know what OS is running on
it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=2/23%OT=80%CT=1%CU=43901%PV=Y%DS=1%DC=D%G=Y%M
=005056%T
OS:M=54EB71B5%P=x86_64-unknown-linux-
gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=I
OS:%TS=8)SEQ(SP=105%GCD=1%ISR=10E%TI=Z%CI=I%II=I%TS=8)OPS(O1=M539S
T11NW2%O2
OS:=M539ST11NW2%O3=M539NNT11NW2%O4=M539ST11NW2%O5=M539ST11NW2%O6=M
539ST11)W
OS:IN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)ECN(R=Y%DF=Y
%T=40%W=3
OS:908%O=M539NNSNW2%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=
)T2(R=N)T
OS:3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T
=40%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
0%Q=)T7(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=
164%UN=0%
OS:RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T=40%CD=S
)

Network Distance: 1 hop

Nmap scan report for 10.142.111.99
Host is up (0.20s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:B1:C1:0C (VMware)
Warning: OSScan results may be unreliable because we could not
find at least 1 open and 1 closed port
Device type: general purpose|media device
Running (JUST GUESSING): OpenBSD 4.X|3.X|5.X (92%), FreeBSD
7.X|9.X (87%), Apple iOS 5.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:7.0
cpe:/o:openbsd:openbsd:3 cpe:/o:openbsd:openbsd:4
cpe:/o:apple:iphone_os:5.2.1 cpe:/o:freebsd:freebsd:9
Aggressive OS guesses: OpenBSD 4.3 (92%), FreeBSD 7.0-RELEASE
(87%), OpenBSD 3.8 - 4.7 (85%), OpenBSD 4.9 - 5.1 (85%), OpenBSD
5.2 (85%), Apple TV (iOS 5.2.1) (85%), FreeBSD 9.1-PRERELEASE
(85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.142.111.100
```



```
Host is up (0.20s latency).
All 1000 scanned ports on 10.142.111.100 are closed
MAC Address: 00:50:56:B1:02:7E (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop


Nmap scan report for 10.142.111.213
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
81/tcp open  hosts2-ns
MAC Address: 00:50:56:B1:02:7E (VMware)
No exact OS matches for host (If you know what OS is running on
it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=2/23%OT=81%CT=1%CU=44339%PV=Y%DS=1%DC=D%G=Y%M
=005056%T
OS:M=54EB71B5%P=x86_64-unknown-linux-
gnu)SEQ(SP=108%GCD=1%ISR=10D%TI=Z%CI=I
OS:%TS=8)SEQ(SP=107%GCD=1%ISR=10E%TI=Z%CI=RD%II=I%TS=8)OPS(O1=M539
ST11NW2%O
OS:2=M539ST11NW2%O3=M539NNT11NW2%O4=M539ST11NW2%O5=M539ST11NW2%O6=
M539ST11)
OS:WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)ECN(R=Y%DF=
Y%T=40%W=
OS:3908%O=M539NNSNW2%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q
=)T2(R=N)
OS:T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%
T=40%W=0%
OS:S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
=0%Q=)T7(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL
=164%UN=0
OS:%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 7 IP addresses (7 hosts up) scanned in 168.57 seconds
```

This table summarized the results:

Host	OS	Confidence
10.142.111.1	OpenBSD	92%
	FreeBSD	87%
10.142.111.6	Unknown Linux	
10.142.111.48	Windows XP SP3	100%
10.142.111.96	Unknown Linux	
10.142.111.99	OpenBSD	92%
	FreeBSD	87%
10.142.111.100	Unknown	
10.142.111.213	Unknown Linux	

You can also use the output of the service detection phase to speculate over the OS version of some hosts:

- 10.142.111.1 and 10.142.111.99 are probably FreeBSD 20100308 and not OpenBSD. You can tell that from the SSH server banner.
- 10.142.111.6 is probably a Debian 7.1, because of the SSH server banner.
- 10.142.111.96 and 10.142.111.213 are probably some incarnation of Debian Linux. You can tell that from the Apache server banner.