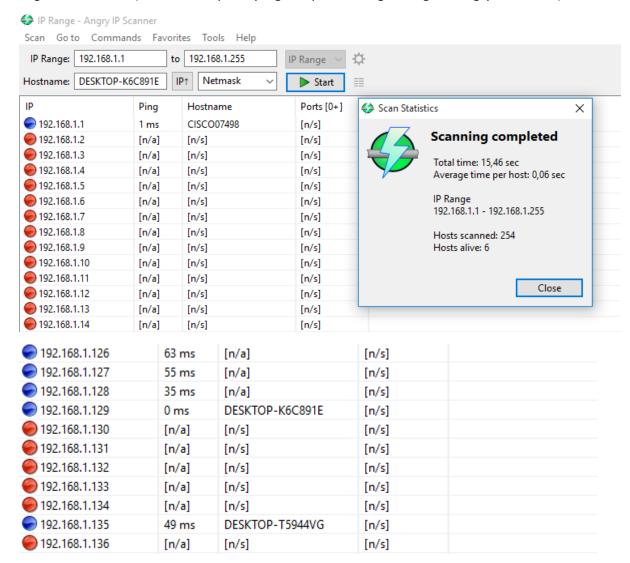# MODUL 2

SCANNING

Wyne Habsari/L200160080

---

1. Tugas Percobaan 1 (Mencari komputer yang hidup/aktif dengan Program Angry IP Scanner)

2. Tugas Percobaan 2 (Mencari Port yang Terbuka)
   Website UMS

```
C:\Users\Asus-X453S>nslookup www.ums.ac.id
Server:  UnKnown
Address: 10.1.1.17

Non-authoritative answer:
Name:    www.ums.ac.id
Address: 103.226.174.220


C:\Users\Asus-X453S>nmap -sS 103.226.174.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:53 SE Asia Standard Time
Nmap scan report for 103.226.174.220
Host is up (0.096s latency).
Not shown: 983 filtered ports
PORT       STATE   SERVICE
20/tcp     closed ftp-data
21/tcp     open    ftp
22/tcp     open    ssh
53/tcp     open    domain
80/tcp     open    http
161/tcp    closed snmp
443/tcp    open    https
465/tcp    closed smtps
587/tcp    closed submission
3306/tcp   open    mysql
8080/tcp   closed http-proxy
8081/tcp   closed blackice-icecap
50000/tcp closed ibm-db2
50001/tcp closed unknown
50002/tcp closed iiimsf
50003/tcp closed unknown
50006/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 24.98 seconds
```

```
C:\Users\Asus-X453S>nmap -sT 103.226.174.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:58 SE Asia Standard Time
Nmap scan report for 103.226.174.220
Host is up (0.000077s latency).
Not shown: 985 filtered ports
PORT       STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
25/tcp     open  smtp
53/tcp     open  domain
80/tcp     open  http
110/tcp    open  pop3
119/tcp    open  nntp
143/tcp    open  imap
443/tcp    open  https
465/tcp    open  smtps
563/tcp    open  snews
587/tcp    open  submission
993/tcp    open  imaps
995/tcp    open  pop3s
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 51.00 seconds
```

Website Detik.com

```
C:\Users\Asus-X453S>nslookup www.detik.com
Server:  UnKnown
Address:  10.1.1.17

Non-authoritative answer:
Name:    detik.com
Addresses:  203.190.242.211
          103.49.221.211
Aliases:  www.detik.com


C:\Users\Asus-X453S>nmap -sS 203.190.242.211
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:52 SE Asia Standard Time
Nmap scan report for s2-211-242.190.203.detik.com (203.190.242.211)
Host is up (0.019s latency).
Not shown: 995 closed ports
PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   open       https
1720/tcp  filtered   h323q931
5666/tcp  open       nrpe
5678/tcp  filtered   rrac

Nmap done: 1 IP address (1 host up) scanned in 16.69 seconds
```

```
C:\Users\Asus-X453S>nmap -sT 203.190.242.211
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:59 SE Asia Standard Time
Nmap scan report for s2-211-242.190.203.detik.com (203.190.242.211)
Host is up (1.2s latency).
Not shown: 986 closed ports
PORT      STATE      SERVICE
25/tcp    open       smtp
80/tcp    open       http
110/tcp   open       pop3
119/tcp   open       nntp
143/tcp   open       imap
443/tcp   open       https
465/tcp   open       smtps
563/tcp   open       snews
587/tcp   open       submission
993/tcp   open       imaps
995/tcp   open       pop3s
1720/tcp  filtered   h323q931
5666/tcp  open       nrpe
5678/tcp  filtered   rrac

Nmap done: 1 IP address (1 host up) scanned in 300.98 seconds
```

Website female.com

```
C:\Users\Asus-X453S>nslookup www.female.com
Server:  UnKnown
Address:  10.1.1.17

Non-authoritative answer:
Name:    www.female.com
Addresses:  146.112.61.106
          146.112.61.106


C:\Users\Asus-X453S>nmap -sS 146.112.61.106
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:56 SE Asia Standard Time
Nmap scan report for hit-adult.opendns.com (146.112.61.106)
Host is up (0.096s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 20.76 seconds
```

```
C:\Users\Asus-X453S>nmap -sT 146.112.61.106
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:02 SE Asia Standard Time
Nmap scan report for hit-adult.opendns.com (146.112.61.106)
Host is up (0.00074s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
119/tcp  open  nntp
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
563/tcp  open  snews
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 61.39 seconds
```

Scanning port lebih dari 1 target

```
C:\Users\Asus-X453S>nmap -sS 192.168.1.1-255
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:44 SE Asia Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
80/tcp open   http
MAC Address: 20:AA:4B:44:84:CD (Cisco-Linksys)

Nmap scan report for 192.168.1.125
Host is up (0.081s latency).
All 1000 scanned ports on 192.168.1.125 are filtered
MAC Address: 70:4D:7B:56:B9:5C (Asustek Computer)

Nmap scan report for 192.168.1.126
Host is up (0.12s latency).
All 1000 scanned ports on 192.168.1.126 are closed
MAC Address: 20:5E:F7:28:72:04 (Samsung Electronics)

Nmap scan report for 192.168.1.127
Host is up (0.050s latency).
All 1000 scanned ports on 192.168.1.127 are closed
MAC Address: 74:23:44:28:D9:5A (Xiaomi Communications)

Nmap scan report for 192.168.1.128
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.1.128 are closed
MAC Address: 4C:ED:FB:21:6B:3D (Unknown)

Nmap scan report for 192.168.1.131
Host is up (0.029s latency).
All 1000 scanned ports on 192.168.1.131 are filtered (828) or closed (172)
MAC Address: 20:5E:F7:6B:1F:F8 (Samsung Electronics)

Nmap scan report for 192.168.1.132
Host is up (0.095s latency).
All 1000 scanned ports on 192.168.1.132 are filtered
MAC Address: 74:C6:3B:CE:9F:F1 (AzureWave Technology)

Nmap scan report for 192.168.1.134
Host is up (0.084s latency).
All 1000 scanned ports on 192.168.1.134 are filtered
MAC Address: A0:A4:C5:BA:B4:59 (Unknown)
```

```
Nmap scan report for 192.168.1.135
Host is up (0.042s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1500/tcp  open  vlsi-lm
3306/tcp  open  mysql
MAC Address: 74:C6:3B:F8:E4:E3 (AzureWave Technology)

Nmap scan report for 192.168.1.129
Host is up (0.00s latency).
Not shown: 979 closed ports
PORT        STATE      SERVICE
25/tcp      filtered   smtp
110/tcp     filtered   pop3
119/tcp     filtered   nntp
125/tcp     filtered   locus-map
135/tcp     open       msrpc
139/tcp     open       netbios-ssn
143/tcp     filtered   imap
445/tcp     open       microsoft-ds
465/tcp     filtered   smtps
548/tcp     filtered   afp
554/tcp     open       rtsp
563/tcp     filtered   snews
587/tcp     filtered   submission
800/tcp     filtered   mdbs_daemon
903/tcp     filtered   iss-console-mgr
993/tcp     filtered   imaps
995/tcp     filtered   pop3s
1433/tcp    filtered   ms-sql-s
2869/tcp    open       icslap
5357/tcp    open       wsdapi
10243/tcp   open       unknown

Nmap done: 255 IP addresses (10 hosts up) scanned in 232.71 seconds
```

3. Tugas Percobaan 3 (Scanning Port dengan Netcat)

```
C:\Users\Asus-X453S\Desktop\netcat>nc -v -z -w2 192.168.1.1 1-255
CISCO07498 [192.168.1.1] 143 (imap) open
CISCO07498 [192.168.1.1] 119 (nntp) open
CISCO07498 [192.168.1.1] 110 (pop3) open
CISCO07498 [192.168.1.1] 80 (http) open
CISCO07498 [192.168.1.1] 25 (smtp) open

C:\Users\Asus-X453S\Desktop\netcat>nc -u -v -z -w2 192.168.1.1 1-255
CISCO07498 [192.168.1.1] 255 (?) open
CISCO07498 [192.168.1.1] 254 (?) open
CISCO07498 [192.168.1.1] 253 (?) open
CISCO07498 [192.168.1.1] 252 (?) open
CISCO07498 [192.168.1.1] 251 (?) open
CISCO07498 [192.168.1.1] 250 (?) open
CISCO07498 [192.168.1.1] 249 (?) open
CISCO07498 [192.168.1.1] 248 (?) open
CISCO07498 [192.168.1.1] 247 (?) open
CISCO07498 [192.168.1.1] 246 (?) open
CISCO07498 [192.168.1.1] 245 (?) open
CISCO07498 [192.168.1.1] 244 (?) open
CISCO07498 [192.168.1.1] 243 (?) open
CISCO07498 [192.168.1.1] 242 (?) open
CISCO07498 [192.168.1.1] 241 (?) open
CISCO07498 [192.168.1.1] 240 (?) open
CISCO07498 [192.168.1.1] 239 (?) open
CISCO07498 [192.168.1.1] 238 (?) open
CISCO07498 [192.168.1.1] 237 (?) open
CISCO07498 [192.168.1.1] 236 (?) open
CISCO07498 [192.168.1.1] 235 (?) open
CISCO07498 [192.168.1.1] 234 (?) open
CISCO07498 [192.168.1.1] 233 (?) open
CISCO07498 [192.168.1.1] 232 (?) open
CISCO07498 [192.168.1.1] 231 (?) open
CISCO07498 [192.168.1.1] 230 (?) open
CISCO07498 [192.168.1.1] 229 (?) open
CISCO07498 [192.168.1.1] 228 (?) open
CISCO07498 [192.168.1.1] 227 (?) open
```

Website UMS

```
C:\Users\Asus-X453S\Desktop\netcat>nc -v -z -w2 103.226.174.220 20-25
220.174.226.103.in-addr.arpa [103.226.174.220] 25 (smtp) open
220.174.226.103.in-addr.arpa [103.226.174.220] 24 (?): TIMEDOUT
220.174.226.103.in-addr.arpa [103.226.174.220] 23 (telnet): TIMEDOUT
220.174.226.103.in-addr.arpa [103.226.174.220] 22 (ssh) open
220.174.226.103.in-addr.arpa [103.226.174.220] 21 (ftp) open

C:\Users\Asus-X453S\Desktop\netcat>nc -u -v -z -w2 103.226.174.220 20-25
220.174.226.103.in-addr.arpa [103.226.174.220] 25 (?) open
220.174.226.103.in-addr.arpa [103.226.174.220] 24 (?) open
220.174.226.103.in-addr.arpa [103.226.174.220] 23 (?) open
220.174.226.103.in-addr.arpa [103.226.174.220] 22 (?) open
220.174.226.103.in-addr.arpa [103.226.174.220] 21 (?) open
220.174.226.103.in-addr.arpa [103.226.174.220] 20 (?) open
```

Website Detik.com

```
C:\Users\Asus-X453S\Desktop\netcat>nc -v -z -w2 203.190.242.211 20-25
s2-211-242.190.203.detik.com [203.190.242.211] 25 (smtp) open

C:\Users\Asus-X453S\Desktop\netcat>nc -u -v -z -w2 203.190.242.211 20-25
s2-211-242.190.203.detik.com [203.190.242.211] 25 (?) open
s2-211-242.190.203.detik.com [203.190.242.211] 24 (?) open
s2-211-242.190.203.detik.com [203.190.242.211] 23 (?) open
s2-211-242.190.203.detik.com [203.190.242.211] 22 (?) open
s2-211-242.190.203.detik.com [203.190.242.211] 21 (?) open
s2-211-242.190.203.detik.com [203.190.242.211] 20 (?) open
```

Website Female.com

```
C:\Users\Asus-X453S\Desktop\netcat>nc -v -z -w2 146.112.61.106 20-25
hit-adult.opendns.com [146.112.61.106] 25 (smtp) open
hit-adult.opendns.com [146.112.61.106] 24 (?): TIMEDOUT
hit-adult.opendns.com [146.112.61.106] 23 (telnet): TIMEDOUT
hit-adult.opendns.com [146.112.61.106] 22 (ssh): TIMEDOUT
hit-adult.opendns.com [146.112.61.106] 21 (ftp): TIMEDOUT
hit-adult.opendns.com [146.112.61.106] 20 (ftp-data): TIMEDOUT

C:\Users\Asus-X453S\Desktop\netcat>nc -u -v -z -w2 146.112.61.106 20-25
hit-adult.opendns.com [146.112.61.106] 25 (?) open
hit-adult.opendns.com [146.112.61.106] 24 (?) open
hit-adult.opendns.com [146.112.61.106] 23 (?) open
hit-adult.opendns.com [146.112.61.106] 22 (?) open
hit-adult.opendns.com [146.112.61.106] 21 (?) open
hit-adult.opendns.com [146.112.61.106] 20 (?) open
```

4. Tugas Percobaan 4 (Mendeteksi Sistem Operasi Target dengan Nmap)

```
C:\Users\Asus-X453S>nmap -O 192.168.1.135
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:07 SE Asia Standard Time
Nmap scan report for 192.168.1.135
Host is up (0.27s latency).
Not shown: 993 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1500/tcp open  vlsi-lm
3306/tcp open  mysql
MAC Address: 74:C6:3B:F8:E4:E3 (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_20
rosoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Se
indows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.15 seconds
```

```
C:\Users\Asus-X453S>nmap -p80 -O 192.168.1.135
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:17 SE Asia Standard Time
Nmap scan report for 192.168.1.135
Host is up (0.032s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 74:C6:3B:F8:E4:E3 (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|XP (86%)
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:micro
p2
Aggressive OS guesses: Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (86%), Microsoft Wi

No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

Website ums.ac.id

```
C:\Users\Asus-X453S>nmap -O 103.226.174.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:20 SE Asia Standard Time
Nmap scan report for 103.226.174.220
Host is up (0.024s latency).
Not shown: 984 filtered ports
PORT        STATE   SERVICE
20/tcp      closed  ftp-data
21/tcp      open    ftp
22/tcp      open    ssh
53/tcp      open    domain
80/tcp      open    http
161/tcp     closed  snmp
443/tcp     open    https
465/tcp     closed  smtps
587/tcp     closed  submission
3306/tcp    open    mysql
8080/tcp    closed  http-proxy
8081/tcp    closed  blackice-icecap
50000/tcp   closed  ibm-db2
50001/tcp   closed  unknown
50003/tcp   closed  unknown
50006/tcp   closed  unknown
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.20 seconds
```

```
C:\Users\Asus-X453S>nmap -p80 -O 103.226.174.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:22 SE Asia Standard Time
Nmap scan report for 103.226.174.220
Host is up (0.041s latency).

PORT    STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.81 seconds

C:\Users\Asus-X453S>nmap -p80 -O 103.226.174.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:24 SE Asia Standard Time
Nmap scan report for 103.226.174.220
Host is up (0.0081s latency).

PORT    STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.16 seconds
```

Website Detik.com

```
C:\Users\Asus-X453S>nmap -O 203.190.242.211
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 15:49 SE Asia Standard Time
Nmap scan report for s2-211-242.190.203.detik.com (203.190.242.211)
Host is up (0.0078s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
80/tcp   open     http
443/tcp  open     https
5666/tcp open     nrpe
5678/tcp filtered rrac
Device type: specialized|router|printer|load balancer
Running (JUST GUESSING): AVtech embedded (86%), HP embedded (85%), Ricoh embedded (
OS CPE: cpe:/h:hp:procurve_7102dl cpe:/h:ricoh:aficio_sp_c240sf cpe:/o:f5:tmos:11.6
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (86%), HP ProCur
Traffic Manager load balancer (TMOS 11.6) (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/sub
Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds

C:\Users\Asus-X453S>nmap -p80 -O 203.190.242.211
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 15:52 SE Asia Standard Time
Nmap scan report for s2-211-242.190.203.detik.com (203.190.242.211)
Host is up (0.0093s latency).

PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 oper
Aggressive OS guesses: Vodavi XTS-IP PBX (93%), Crestron XPanel control system (92%
 5.3 (90%), HP 170X print server or Inkjet 3000 printer (89%), HP LaserJet 4250 pri
tendo Wii game console (88%), Brother MFC-7820N printer (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/sub
Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds
```

Website Female.com

```
C:\Users\Asus-X453S>nmap -O 146.112.61.106
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:30 SE Asia Standard Time
Nmap scan report for hit-adult.opendns.com (146.112.61.106)
Host is up (0.15s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (94%), Linux 3.16 (90%), Crestron XPanel control system (90%), Linux 2
 ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%), Linux 2.6.32 - 3.10 (87%)
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 32.01 seconds

C:\Users\Asus-X453S>nmap -p80 -O 146.112.61.106
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:32 SE Asia Standard Time
Nmap scan report for hit-adult.opendns.com (146.112.61.106)
Host is up (0.091s latency).

PORT    STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (94%), Linux 3.16 (90%), Crestron XPanel control system (90%), Linux 4
 3.2 - 3.8 (88%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%)
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 14.59 seconds
```