

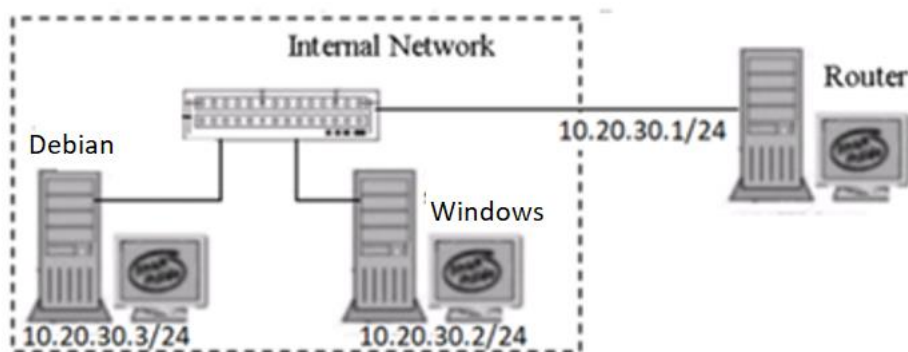
LAPORAN - JOB SHEET 5

Praktikum Network Security Menguji Keamanan Jaringan, Host Dan Server

NAMA : YUSUF ISCHAK MAULANA
ASAL SEKOLAH : SMKN 1 CIMAHI
KELAS : XII SIJA A

Dalam kegiatan ini peserta diklat akan menerapkan langkah-langkah menguji keamanan host dan Server.

1. Bangun Topology sebagai berikut :



2. Persiapan

Router

- Konfigurasi IPAddress 10.20.30.1/24

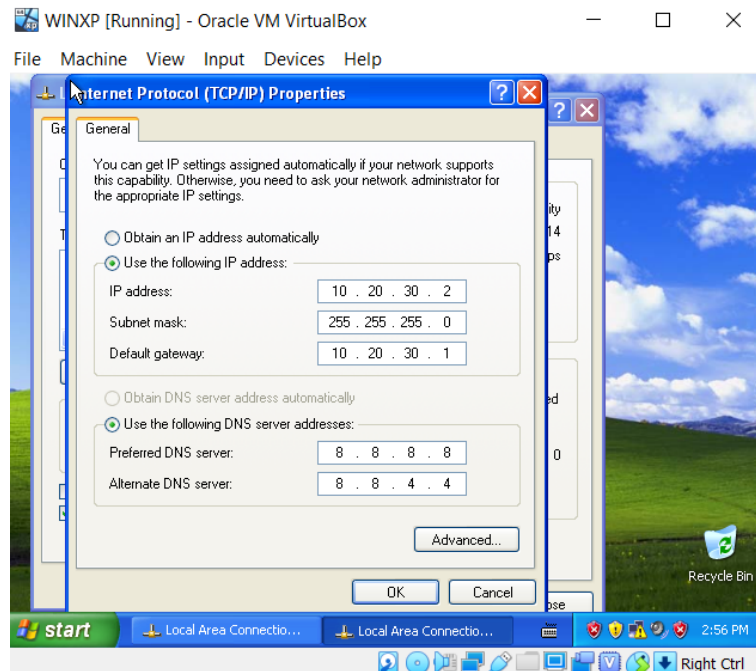
```
Router [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal Jun 14:25
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:63:ea:e8
          inet addr:10.20.30.1  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fe63:ea:e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2494 (2.4 KiB)  TX bytes:12886 (12.5 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:cf:9c:e7
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:543 (543.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4686 (4.5 KiB)  TX bytes:4686 (4.5 KiB)
```

Windows

- Konfigurasi IPAddress 10.20.30.2/24



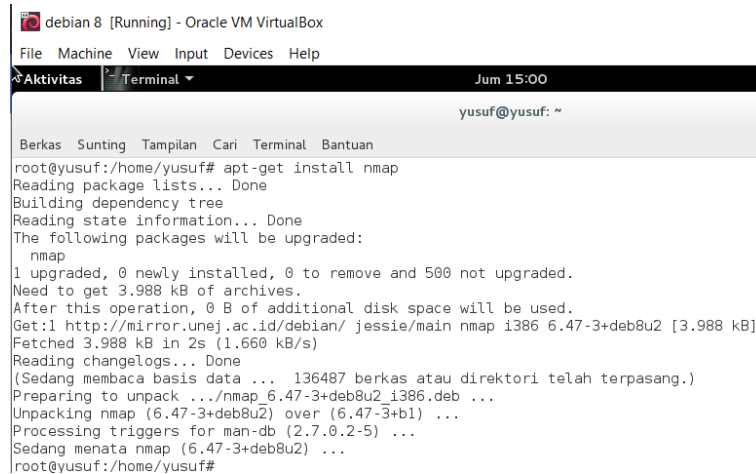
Debian

- Konfigurasi IPAddress 10.20.30.3/24



- Install Nmap

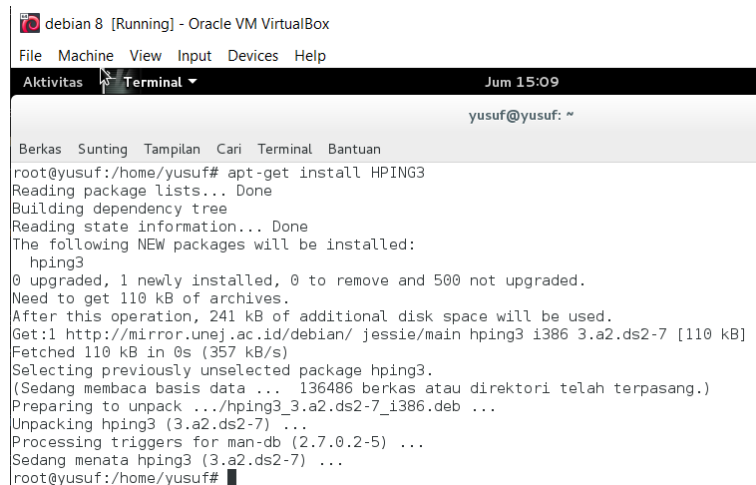
```
#apt-get install nmap
```



```
debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal Jum 15:00
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf# apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  nmap
1 upgraded, 0 newly installed, 0 to remove and 500 not upgraded.
Need to get 3.988 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://mirror.unej.ac.id/debian/ jessie/main nmap i386 6.47-3+deb8u2 [3.988 kB]
Fetched 3.988 kB in 2s (1.660 kB/s)
Reading changelogs... Done
(Sedang membaca basis data ... 136487 berkas atau direktori telah terpasang.)
Preparing to unpack .../nmap_6.47-3+deb8u2_i386.deb ...
Unpacking nmap (6.47-3+deb8u2) over (6.47-3+b1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Sedang menata nmap (6.47-3+deb8u2) ...
root@yusuf:/home/yusuf#
```

- Install HPING3

```
#apt-get install hping3
```



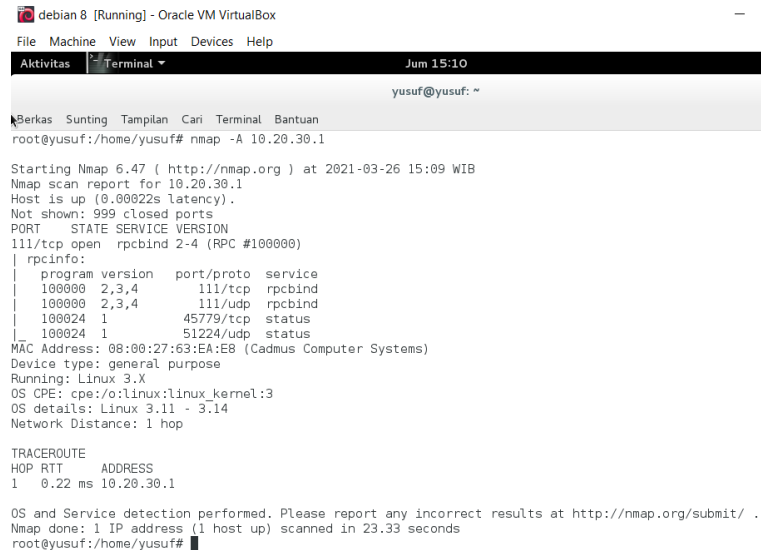
```
debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal Jum 15:09
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf# apt-get install HPING3
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  hping3
0 upgraded, 1 newly installed, 0 to remove and 500 not upgraded.
Need to get 110 kB of archives.
After this operation, 241 kB of additional disk space will be used.
Get:1 http://mirror.unej.ac.id/debian/ jessie/main hping3 i386 3.a2.ds2-7 [110 kB]
Fetched 110 kB in 0s (357 kB/s)
Selecting previously unselected package hping3.
(Sedang membaca basis data ... 136486 berkas atau direktori telah terpasang.)
Preparing to unpack .../hping3_3.a2.ds2-7_i386.deb ...
Unpacking hping3 (3.a2.ds2-7) ...
Processing triggers for man-db (2.7.0.2-5) ...
Sedang menata hping3 (3.a2.ds2-7) ...
root@yusuf:/home/yusuf#
```

3. Lakukan Percobaan berikut dari Server-2

A. Menggunakan NMAP

➤ Nmap port Scanning :

```
#nmap -A 10.20.30.1
```



```
root@yusuf:/home/yusuf# nmap -A 10.20.30.1

Starting Nmap 6.47 ( http://nmap.org ) at 2021-03-26 15:09 WIB
Nmap scan report for 10.20.30.1
Host is up (0.00022s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2-4 (RPC #100000)
|_ rpcinfo:
|_  program version  port/proto  service
|_  100000  2,3,4      111/tcp    rpcbind
|_  100000  2,3,4      111/udp    rpcbind
|_  100024  1          45779/tcp  status
|_  100024  1          51224/udp  status
MAC Address: 08:00:27:63:EA:E8 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.11 - 3.14
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1 0.22 ms 10.20.30.1

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.33 seconds
root@yusuf:/home/yusuf#
```

Hasil diatas, menunjukkan hasil penelusuran jumlah port tertutup sebanyak 999 port. Kemudian, terdapat port yang aktif yaitu port 111/tcp yang melayani service rpcbind. Dibawahnya terdapat rpcinfo yang menampilkan informasi 4 buah port, yaitu 111/tcp, 111/udp, 45779/tcp, dan 51224/udp. Lalu ada keterangan mengenai komputer router berupa:

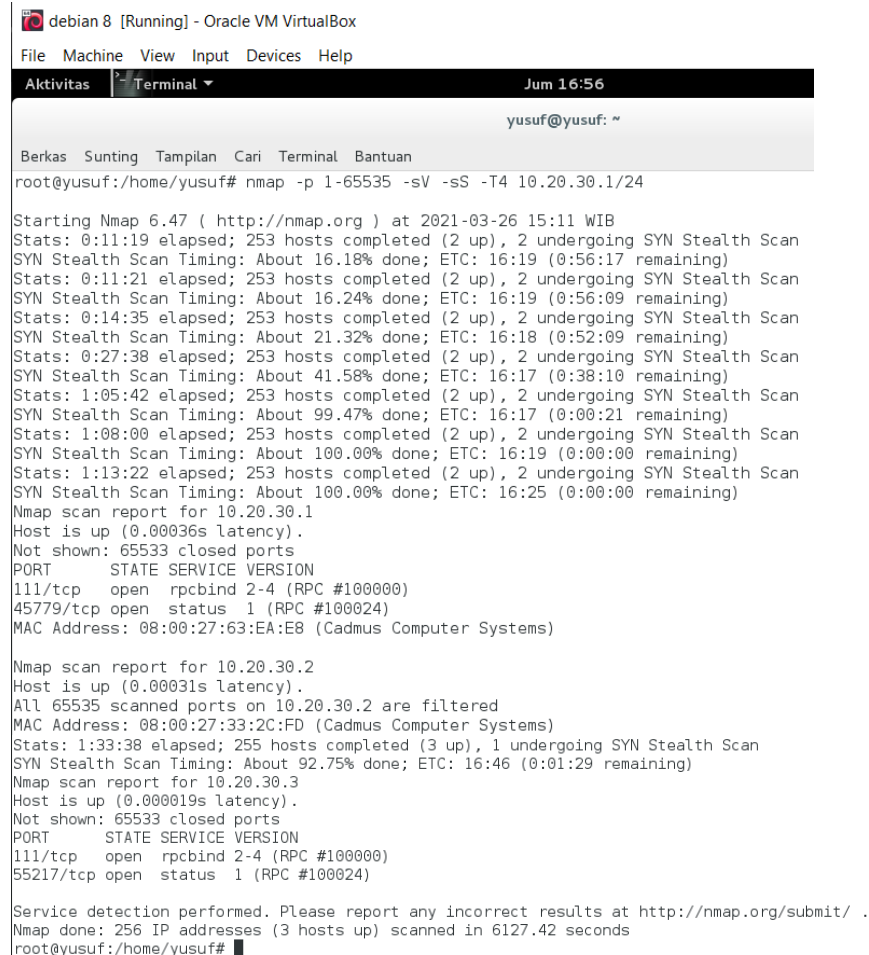
- Mac Adress
- Tipe device
- Versi linux
- OS Cpe
- OS details

Dan terakhir adalah jarak hop yang digunakan untuk melakukan proses nmap yaitu 1 hop, serta dijelaskan pada bagian Traceroute

Lanjutkan untuk item selanjutnya :

- Mendeteksi service TCP portscan dan version

```
#nmap -p 1-65535 -sV -sS -T4 10.20.30.1/24
```



```
root@yusuf:/home/yusuf# nmap -p 1-65535 -sV -sS -T4 10.20.30.1/24

Starting Nmap 6.47 ( http://nmap.org ) at 2021-03-26 15:11 WIB
Stats: 0:11:19 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.18% done; ETC: 16:19 (0:56:17 remaining)
Stats: 0:11:21 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.24% done; ETC: 16:19 (0:56:09 remaining)
Stats: 0:14:35 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.32% done; ETC: 16:18 (0:52:09 remaining)
Stats: 0:27:38 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.58% done; ETC: 16:17 (0:38:10 remaining)
Stats: 1:05:42 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.47% done; ETC: 16:17 (0:00:21 remaining)
Stats: 1:08:00 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 16:19 (0:00:00 remaining)
Stats: 1:13:22 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 16:25 (0:00:00 remaining)
Nmap scan report for 10.20.30.1
Host is up (0.00036s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2-4 (RPC #100000)
45779/tcp  open  status  1 (RPC #100024)
MAC Address: 08:00:27:63:EA:EB (Cadmus Computer Systems)

Nmap scan report for 10.20.30.2
Host is up (0.00031s latency).
All 65535 scanned ports on 10.20.30.2 are filtered
MAC Address: 08:00:27:33:2C:FD (Cadmus Computer Systems)
Stats: 1:33:38 elapsed; 255 hosts completed (3 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.75% done; ETC: 16:46 (0:01:29 remaining)
Nmap scan report for 10.20.30.3
Host is up (0.000019s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2-4 (RPC #100000)
55217/tcp  open  status  1 (RPC #100024)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 6127.42 seconds
root@yusuf:/home/yusuf#
```

Hasil diatas, menunjukan bahwa,

Proses scanning mendeteksi semua host yang ada pada subnet ip 10.20.30.1/24, dimana mendeteksi menggunakan paket SYN menghasilkan pada alamat 10.20.30.1/24

- o berupa nomor port :
 - port 111/tcp yang merupakan rpcbind, dan
 - port 45779/tcp dengan layanan status.
- o Dibawah akan ada MAC address dari server 10.20.30.1/24

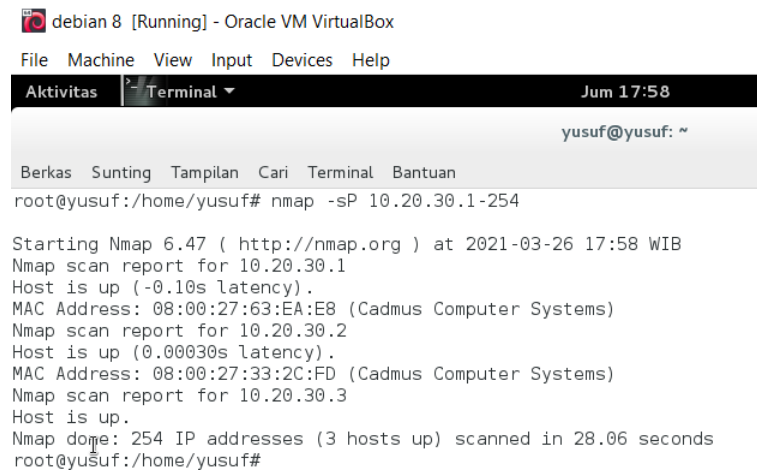
Lalu akan ada hasil deteksi dari IP 10.20.30.2/24 dengan menampilkan jumlah port yang berhasil di scan yaitu sebanyak 65535 port. Selanjutnya, hasil deteksi menampilkan MAC address dari Windows.

Hasil terakhir menampilkan hasil deteksi dari IP 10.20.30.3 dengan laporan jumlah port tertutup sebanyak 65533 port. Terdapat juga

informasi port yang aktif sebanyak 2 port yaitu port 111/tcp yang melayani rpcbind, dan port 55217/tcp yang melayani status.

➤ Mendapatkan daftar port tertentu yang sedang terbuka

```
# nmap -sP 10.20.30.1-254
```



The screenshot shows a terminal window titled "debian 8 [Running] - Oracle VM VirtualBox". The terminal displays the command `nmap -sP 10.20.30.1-254` and its output. The output indicates that three hosts are up in the range 10.20.30.1-254: 10.20.30.1, 10.20.30.2, and 10.20.30.3. It also provides MAC addresses for each host and states that 254 IP addresses were scanned in 28.06 seconds.

```
root@yusuf:/home/yusuf# nmap -sP 10.20.30.1-254

Starting Nmap 6.47 ( http://nmap.org ) at 2021-03-26 17:58 WIB
Nmap scan report for 10.20.30.1
Host is up (-0.10s latency).
MAC Address: 08:00:27:63:EA:E8 (Cadmus Computer Systems)
Nmap scan report for 10.20.30.2
Host is up (0.00030s latency).
MAC Address: 08:00:27:33:2C:FD (Cadmus Computer Systems)
Nmap scan report for 10.20.30.3
Host is up.
Nmap done: 254 IP addresses (3 hosts up) scanned in 28.06 seconds
root@yusuf:/home/yusuf#
```

Hasil menunjukan bahwa,

Host yang ada dalam range 10.20.30.1-254 adatingga buah host yang terdeteksi yaitu :

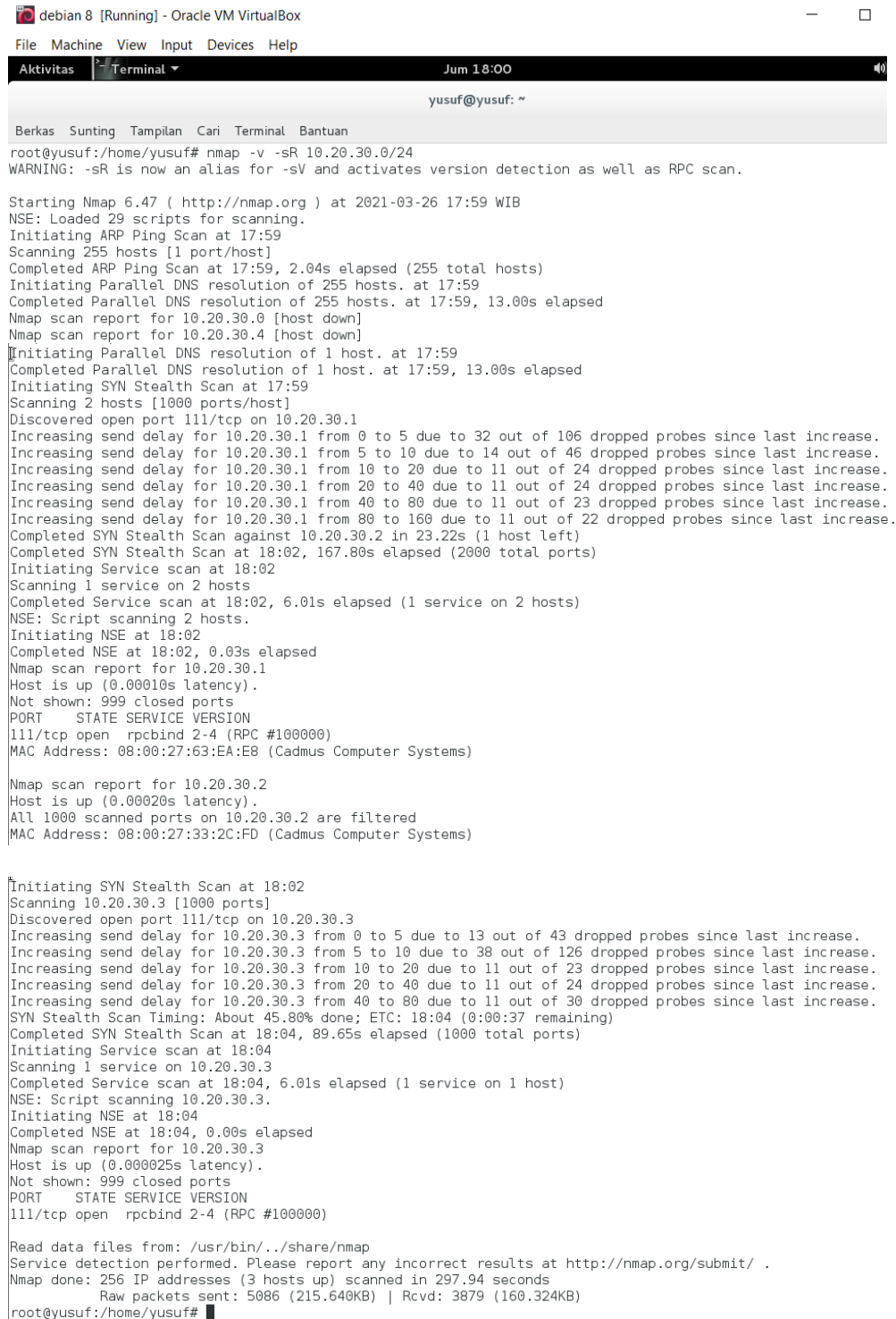
- 10.20.30.1,
- 10.20.30.2, dan
- 10.20.30.3

Dengan keterangan "host is up" yang artinya adalah host tersedia atau dalam keadaan nyala dan memiliki latensi sesuai yang tercantum.

Informasi berikutnya yang dicantumkan yaitu MAC address dari setiap host. Di bagian akhir menunjukan total IP address sebanyak 254 dengan tiga host menyala dengan durasi pindai selama 28.06 detik.

- Nmap TCP RPC scanning, untuk menemukan aplikasi yang menggunakan remote call procedure pada target

```
#nmap -v -sR 10.20.30.0/24
```



```
root@yusuf:/home/yusuf# nmap -v -sR 10.20.30.0/24
WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.

Starting Nmap 6.47 ( http://nmap.org ) at 2021-03-26 17:59 WIB
NSE: Loaded 29 scripts for scanning.
Initiating ARP Ping Scan at 17:59
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 17:59, 2.04s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 17:59
Completed Parallel DNS resolution of 255 hosts. at 17:59, 13.00s elapsed
Nmap scan report for 10.20.30.0 [host down]
Nmap scan report for 10.20.30.4 [host down]
Initiating Parallel DNS resolution of 1 host. at 17:59
Completed Parallel DNS resolution of 1 host. at 17:59, 13.00s elapsed
Initiating SYN Stealth Scan at 17:59
Scanning 2 hosts [1000 ports/host]
Discovered open port 111/tcp on 10.20.30.1
Increasing send delay for 10.20.30.1 from 0 to 5 due to 32 out of 106 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 5 to 10 due to 14 out of 46 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 10 to 20 due to 11 out of 24 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 20 to 40 due to 11 out of 24 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 40 to 80 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 80 to 160 due to 11 out of 22 dropped probes since last increase.
Completed SYN Stealth Scan against 10.20.30.2 in 23.22s (1 host left)
Completed SYN Stealth Scan at 18:02, 167.80s elapsed (2000 total ports)
Initiating Service scan at 18:02
Scanning 1 service on 2 hosts
Completed Service scan at 18:02, 6.01s elapsed (1 service on 2 hosts)
NSE: Script scanning 2 hosts.
Initiating NSE at 18:02
Completed NSE at 18:02, 0.03s elapsed
Nmap scan report for 10.20.30.1
Host is up (0.00010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2-4 (RPC #100000)
MAC Address: 08:00:27:63:EA:E8 (Cadmus Computer Systems)

Nmap scan report for 10.20.30.2
Host is up (0.00020s latency).
All 1000 scanned ports on 10.20.30.2 are filtered
MAC Address: 08:00:27:33:2C:FD (Cadmus Computer Systems)

Initiating SYN Stealth Scan at 18:02
Scanning 10.20.30.3 [1000 ports]
Discovered open port 111/tcp on 10.20.30.3
Increasing send delay for 10.20.30.3 from 0 to 5 due to 13 out of 43 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 5 to 10 due to 38 out of 126 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 10 to 20 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 20 to 40 due to 11 out of 24 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 40 to 80 due to 11 out of 30 dropped probes since last increase.
SYN Stealth Scan Timing: About 45.80% done; ETC: 18:04 (0:00:37 remaining)
Completed SYN Stealth Scan at 18:04, 89.65s elapsed (1000 total ports)
Initiating Service scan at 18:04
Scanning 1 service on 10.20.30.3
Completed Service scan at 18:04, 6.01s elapsed (1 service on 1 host)
NSE: Script scanning 10.20.30.3.
Initiating NSE at 18:04
Completed NSE at 18:04, 0.00s elapsed
Nmap scan report for 10.20.30.3
Host is up (0.000025s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2-4 (RPC #100000)

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 297.94 seconds
Raw packets sent: 5086 (215.640KB) | Rcvd: 3879 (160.324KB)
root@yusuf:/home/yusuf#
```

```

debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal
Jum 18:09
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf# nmap -sT 10.20.30.1/24

Starting Nmap 6.47 ( http://nmap.org ) at 2021-03-26 18:08 WIB
Nmap scan report for 10.20.30.1
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind
MAC Address: 08:00:27:63:EA:E8 (Cadmus Computer Systems)

Nmap scan report for 10.20.30.2
Host is up (0.00027s latency).
All 1000 scanned ports on 10.20.30.2 are filtered
MAC Address: 08:00:27:33:2C:FD (Cadmus Computer Systems)

Nmap scan report for 10.20.30.3
Host is up (0.00014s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind

Nmap done: 256 IP addresses (3 hosts up) scanned in 32.27 seconds
root@yusuf:/home/yusuf#

```

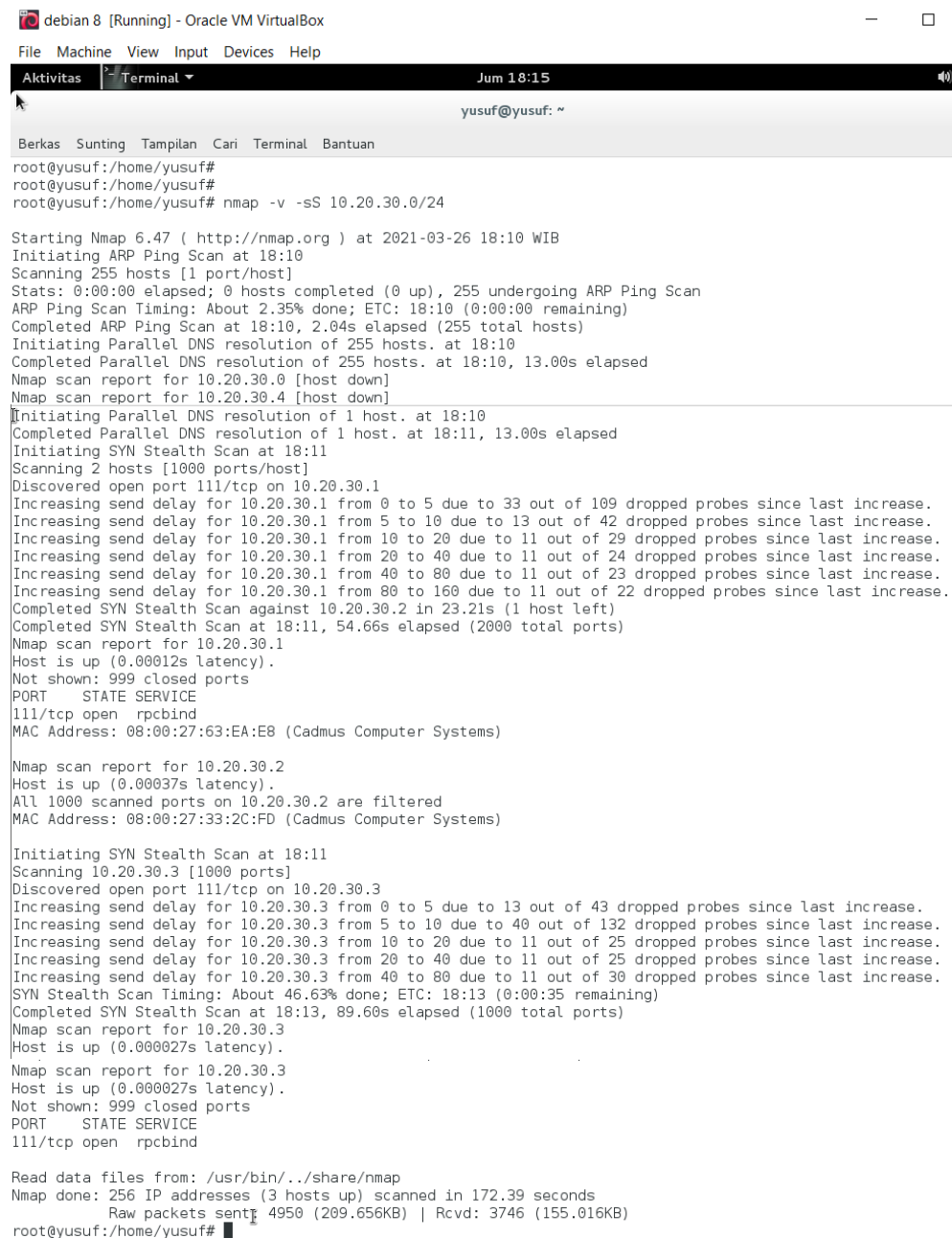
Pada pemindaian pertama yaitu dengan perintah `nmap -v -sR 10.20.30.0/24` menghasilkan

- Semua host dari nmap scan yang sedang tidak aktif (Host Down),
- Info tentang 10.20.30.1
 - o Menyatakan "host is up" atau sedang aktif
 - o Port yang tertutup sebanyak 999 port
 - o Port yang berjalan 111/tcp yang merupakan rpcbind, dan
 - o Mac Address
- Info tentang 10.20.30.2
 - o Menyatakan "host is up" atau sedang aktif
 - o Semua 1000 port yang sudah di scan terfilter, dan
 - o Mac Address
- Info tentang 10.20.30.3
 - o Menyatakan "host is up" atau sedang aktif
 - o Port yang berjalan 111/tcp yang merupakan rpcbind

Perintah berikutnya dengan perintah `nmap -sT 10.20.30.1/24` menghasilkan berbagai koneksi TCP yang terdeteksi oleh NMAP. Terdapat beberapa port dari setiap host yang terdeteksi oleh perintah ini dengan protokol yang sama yaitu TCP. Sebagai contoh pada host 10.20.30.1 terdeteksi terdapat sebuah port yaitu 111 dimana merupakan protokol TCP.

➤ Nmap TCP SYN (half-open) scanning

```
# nmap -v -sS 10.20.30.0/24
```



```
debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal Jum 18:15
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf#
root@yusuf:/home/yusuf#
root@yusuf:/home/yusuf# nmap -v -sS 10.20.30.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2021-03-26 18:10 WIB
Initiating ARP Ping Scan at 18:10
Scanning 255 hosts [1 port/host]
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 2.35% done; ETC: 18:10 (0:00:00 remaining)
Completed ARP Ping Scan at 18:10, 2.04s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 18:10
Completed Parallel DNS resolution of 255 hosts. at 18:10, 13.00s elapsed
Nmap scan report for 10.20.30.0 [host down]
Nmap scan report for 10.20.30.4 [host down]
Initiating Parallel DNS resolution of 1 host. at 18:10
Completed Parallel DNS resolution of 1 host. at 18:11, 13.00s elapsed
Initiating SYN Stealth Scan at 18:11
Scanning 2 hosts [1000 ports/host]
Discovered open port 111/tcp on 10.20.30.1
Increasing send delay for 10.20.30.1 from 0 to 5 due to 33 out of 109 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 5 to 10 due to 13 out of 42 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 10 to 20 due to 11 out of 29 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 20 to 40 due to 11 out of 24 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 40 to 80 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 10.20.30.1 from 80 to 160 due to 11 out of 22 dropped probes since last increase.
Completed SYN Stealth Scan against 10.20.30.2 in 23.21s (1 host left)
Completed SYN Stealth Scan at 18:11, 54.66s elapsed (2000 total ports)
Nmap scan report for 10.20.30.1
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind
MAC Address: 08:00:27:63:EA:E8 (Cadmus Computer Systems)

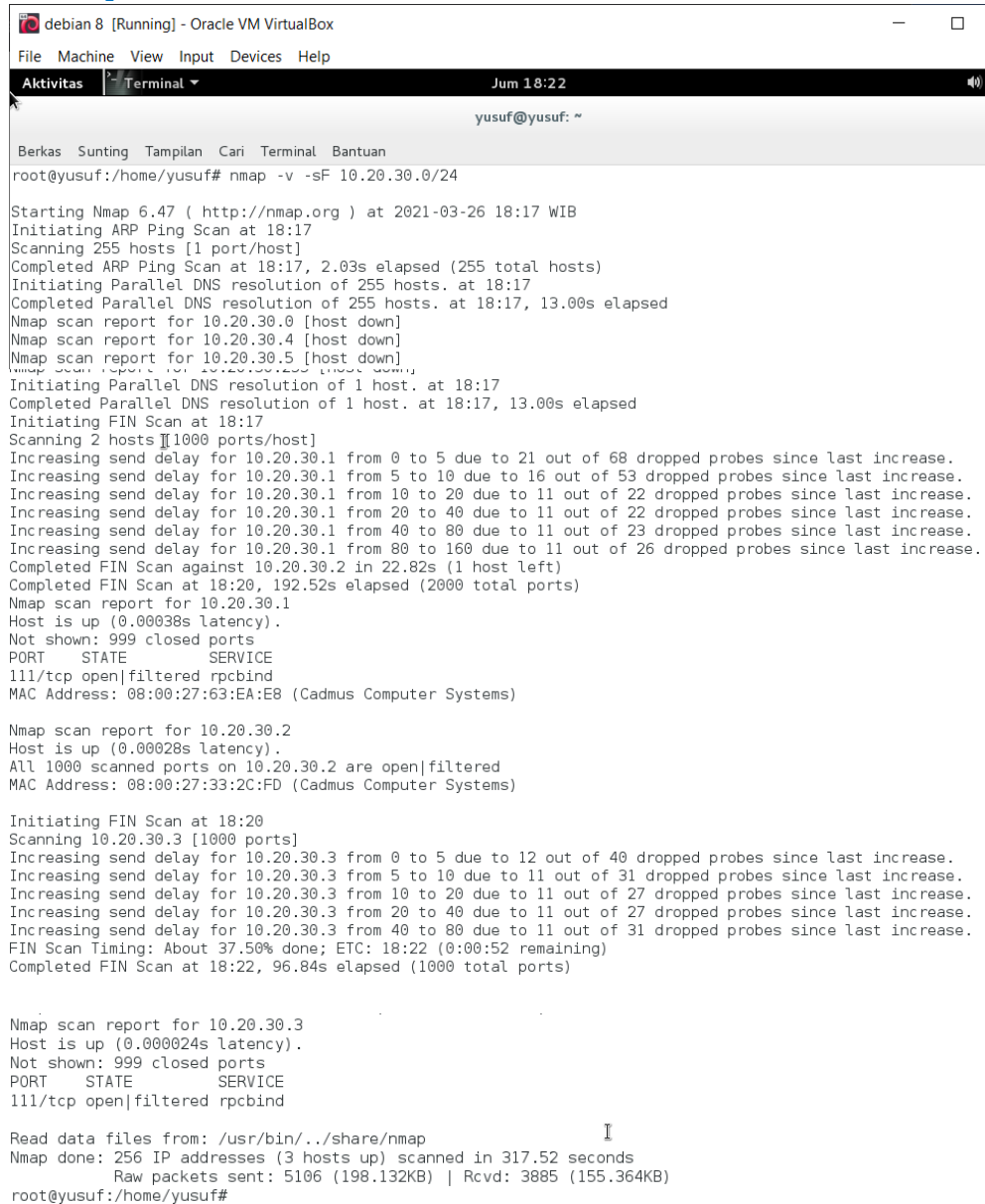
Nmap scan report for 10.20.30.2
Host is up (0.00037s latency).
All 1000 scanned ports on 10.20.30.2 are filtered
MAC Address: 08:00:27:33:2C:FD (Cadmus Computer Systems)

Initiating SYN Stealth Scan at 18:11
Scanning 10.20.30.3 [1000 ports]
Discovered open port 111/tcp on 10.20.30.3
Increasing send delay for 10.20.30.3 from 0 to 5 due to 13 out of 43 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 5 to 10 due to 40 out of 132 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 10 to 20 due to 11 out of 25 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 20 to 40 due to 11 out of 25 dropped probes since last increase.
Increasing send delay for 10.20.30.3 from 40 to 80 due to 11 out of 30 dropped probes since last increase.
SYN Stealth Scan Timing: About 46.63% done; ETC: 18:13 (0:00:35 remaining)
Completed SYN Stealth Scan at 18:13, 89.60s elapsed (1000 total ports)
Nmap scan report for 10.20.30.3
Host is up (0.000027s latency).
Nmap scan report for 10.20.30.3
Host is up (0.000027s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind

Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 172.39 seconds
Raw packets sent: 4950 (209.656KB) | Rcvd: 3746 (155.016KB)
root@yusuf:/home/yusuf#
```

➤ Nmap TCP FIN scanning

```
# nmap -v -sF 10.20.30.0/24
```



The screenshot shows a terminal window titled "debian 8 [Running] - Oracle VM VirtualBox". The terminal displays the output of the command `nmap -v -sF 10.20.30.0/24`. The output includes the following information:

- Starting Nmap 6.47 (<http://nmap.org>) at 2021-03-26 18:17 WIB
- Initiating ARP Ping Scan at 18:17
- Scanning 255 hosts [1 port/host]
- Completed ARP Ping Scan at 18:17, 2.03s elapsed (255 total hosts)
- Initiating Parallel DNS resolution of 255 hosts. at 18:17
- Completed Parallel DNS resolution of 255 hosts. at 18:17, 13.00s elapsed
- Nmap scan report for 10.20.30.0 [host down]
- Nmap scan report for 10.20.30.4 [host down]
- Nmap scan report for 10.20.30.5 [host down]
- Nmap scan report for 10.20.30.200 [host down]
- Initiating Parallel DNS resolution of 1 host. at 18:17
- Completed Parallel DNS resolution of 1 host. at 18:17, 13.00s elapsed
- Initiating FIN Scan at 18:17
- Scanning 2 hosts [1000 ports/host]
- Increasing send delay for 10.20.30.1 from 0 to 5 due to 21 out of 68 dropped probes since last increase.
- Increasing send delay for 10.20.30.1 from 5 to 10 due to 16 out of 53 dropped probes since last increase.
- Increasing send delay for 10.20.30.1 from 10 to 20 due to 11 out of 22 dropped probes since last increase.
- Increasing send delay for 10.20.30.1 from 20 to 40 due to 11 out of 22 dropped probes since last increase.
- Increasing send delay for 10.20.30.1 from 40 to 80 due to 11 out of 23 dropped probes since last increase.
- Increasing send delay for 10.20.30.1 from 80 to 160 due to 11 out of 26 dropped probes since last increase.
- Completed FIN Scan against 10.20.30.2 in 22.82s (1 host left)
- Completed FIN Scan at 18:20, 192.52s elapsed (2000 total ports)
- Nmap scan report for 10.20.30.1
- Host is up (0.00038s latency).
- Not shown: 999 closed ports
- PORT STATE SERVICE
- 111/tcp open|filtered rpcbind
- MAC Address: 08:00:27:63:EA:E8 (Cadmus Computer Systems)
- Nmap scan report for 10.20.30.2
- Host is up (0.00028s latency).
- All 1000 scanned ports on 10.20.30.2 are open|filtered
- MAC Address: 08:00:27:33:2C:FD (Cadmus Computer Systems)
- Initiating FIN Scan at 18:20
- Scanning 10.20.30.3 [1000 ports]
- Increasing send delay for 10.20.30.3 from 0 to 5 due to 12 out of 40 dropped probes since last increase.
- Increasing send delay for 10.20.30.3 from 5 to 10 due to 11 out of 31 dropped probes since last increase.
- Increasing send delay for 10.20.30.3 from 10 to 20 due to 11 out of 27 dropped probes since last increase.
- Increasing send delay for 10.20.30.3 from 20 to 40 due to 11 out of 27 dropped probes since last increase.
- Increasing send delay for 10.20.30.3 from 40 to 80 due to 11 out of 31 dropped probes since last increase.
- FIN Scan Timing: About 37.50% done; ETC: 18:22 (0:00:52 remaining)
- Completed FIN Scan at 18:22, 96.84s elapsed (1000 total ports)
- Nmap scan report for 10.20.30.3
- Host is up (0.00024s latency).
- Not shown: 999 closed ports
- PORT STATE SERVICE
- 111/tcp open|filtered rpcbind
- Read data files from: /usr/bin/./share/nmap
- Nmap done: 256 IP addresses (3 hosts up) scanned in 317.52 seconds
- Raw packets sent: 5106 (198.132KB) | Rcvd: 3885 (155.364KB)
- root@yusuf:/home/yusuf#

B. Menggunakan HPING

➤ Menyerang dengan cara SYN flood attack

```
#hping -I u50 -S -p 22 10.20.30.1
```

```
debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal Jum 17:31
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf# hping3 -i u50 -S -p 22 10.20.30.1
HPING 10.20.30.1 (eth0 10.20.30.1): S set, 40 headers + 0 data bytes
len=46 ip=10.20.30.1 ttl=64 DF id=1381 sport=22 flags=RA seq=0 win=0 rtt=0.9 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1382 sport=22 flags=RA seq=1 win=0 rtt=1.1 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1383 sport=22 flags=RA seq=2 win=0 rtt=4.2 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1384 sport=22 flags=RA seq=3 win=0 rtt=4.1 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1385 sport=22 flags=RA seq=4 win=0 rtt=4.1 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1386 sport=22 flags=RA seq=5 win=0 rtt=4.0 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1387 sport=22 flags=RA seq=6 win=0 rtt=4.1 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1388 sport=22 flags=RA seq=7 win=0 rtt=3.9 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1389 sport=22 flags=RA seq=8 win=0 rtt=3.9 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1390 sport=22 flags=RA seq=9 win=0 rtt=3.8 ms
len=46 ip=10.20.30.1 ttl=64 DF id=1391 sport=22 flags=RA seq=10 win=0 rtt=3.8 ms
```

Hasil uji coba serangan tersebut, menunjukkan :

Menunjukkan SYN flood attack yang merupakan metode ddos attack dengan mengirimkan paket SYN ke target dan kita tidak menerima paket syn+ack dari target.

SYN flood attack yang dilakukan oleh server 2 (debian 8) yang berupa TCP SYN Scan, dan akan memindai port 22, dengan hasil flag RA yang menunjukkan port tertutup. Sedangkan jika flag berupa SA (SYN dan ACK) menunjukkan port terbuka.

Lanjutkan untuk item selanjutnya :

```
#hping3 -i u100 -S -p 80 10.20.30.1
```

```
debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal Jum 17:32
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf# hping3 -i u100 -S -p 80 10.20.30.1
HPING 10.20.30.1 (eth0 10.20.30.1): S set, 40 headers + 0 data bytes
len=46 ip=10.20.30.1 ttl=64 DF id=18913 sport=80 flags=RA seq=0 win=0 rtt=3.2 ms
len=46 ip=10.20.30.1 ttl=64 DF id=18914 sport=80 flags=RA seq=1 win=0 rtt=3.1 ms
len=46 ip=10.20.30.1 ttl=64 DF id=18915 sport=80 flags=RA seq=2 win=0 rtt=3.2 ms
len=46 ip=10.20.30.1 ttl=64 DF id=18916 sport=80 flags=RA seq=3 win=0 rtt=3.0 ms
len=46 ip=10.20.30.1 ttl=64 DF id=18917 sport=80 flags=RA seq=4 win=0 rtt=2.8 ms
len=46 ip=10.20.30.1 ttl=64 DF id=18918 sport=80 flags=RA seq=5 win=0 rtt=2.6 ms
len=46 ip=10.20.30.1 ttl=64 DF id=18919 sport=80 flags=RA seq=6 win=0 rtt=1.9 ms
```

➤ TCP & UDP Flood Testing

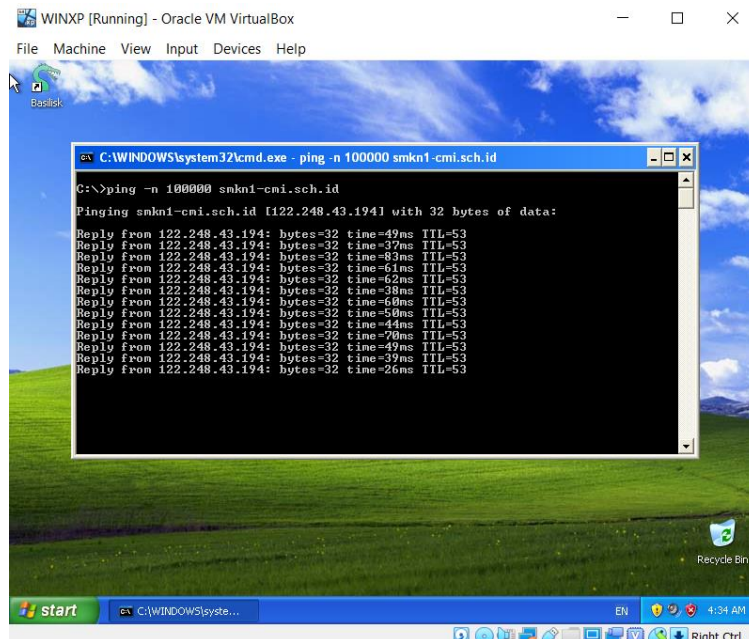
```
#hping -q -n -a 13.13.13.0 -S -s 80 -keep -p 445 -flood 10.20.30.1
```

```
debian 8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aktivitas Terminal Jum 18:34
yusuf@yusuf: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@yusuf:/home/yusuf# hping3 -q -n -a 13.13.13.0 -S -s 80 --keep -p 445 --flood 10.20.30.1
HPING 10.20.30.1 (eth0 10.20.30.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

^C
--- 10.20.30.1 hping statistic ---
255093 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@yusuf:/home/yusuf#
```

4. Melakukan dari Microsoft Windows

- ICMP Flood Testing
Dari Windows
c>ping -n 100000 smkn1-cmi.sch.id



```
WINXP [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Basisk
C:\WINDOWS\system32\cmd.exe - ping -n 100000 smkn1-cmi.sch.id
C:\>ping -n 100000 smkn1-cmi.sch.id
Pinging smkn1-cmi.sch.id [122.248.43.194] with 32 bytes of data:
Reply from 122.248.43.194: bytes=32 time=49ms TTL=53
Reply from 122.248.43.194: bytes=32 time=37ms TTL=53
Reply from 122.248.43.194: bytes=32 time=83ms TTL=53
Reply from 122.248.43.194: bytes=32 time=61ms TTL=53
Reply from 122.248.43.194: bytes=32 time=52ms TTL=53
Reply from 122.248.43.194: bytes=32 time=38ms TTL=53
Reply from 122.248.43.194: bytes=32 time=60ms TTL=53
Reply from 122.248.43.194: bytes=32 time=50ms TTL=53
Reply from 122.248.43.194: bytes=32 time=44ms TTL=53
Reply from 122.248.43.194: bytes=32 time=70ms TTL=53
Reply from 122.248.43.194: bytes=32 time=47ms TTL=53
Reply from 122.248.43.194: bytes=32 time=39ms TTL=53
Reply from 122.248.43.194: bytes=32 time=26ms TTL=53
```

KESIMPULAN

Sangatlah penting dalam PENETRATION TESTING melaksanakan langkah-langkah sebagai berikut :

1. Reconnaissance (Pengumpulan Informasi)

Reconnaissance adalah langkah awal dari Penetration Testing yang dimulai dengan menentukan target pengujian berdasarkan scope pengerjaan. Setelah target ditentukan, research dilakukan untuk mengumpulkan informasi pada target seperti: ports apa yang digunakan untuk komunikasi, dimana lokasinya, tipe services yang diberikan kepada clientnya (web,database,dll). Data-data ini dibutuhkan untuk langkah selanjutnya yang akan dilakukan untuk penetration testing. Deliverable dari langkah reconnaissance harus mencakup list dari semua

asset yang dimiliki target, aplikasi yang terkait dengan asset, services yang digunakan, dan pemilik aset.

Information Gathering difokuskan untuk dapat mengumpulkan informasi secukupnya mengenai sistem target. proses pengumpulan informasi sendiri terbagi menjadi dua, yaitu passive information gathering dan active information gathering. Pengumpulan informasi menggunakan teknik passive information gathering dapat menggunakan service WHOIS, DNS, Search Engine (Google), Website Analysis Security (netcraft) dan tools seperti Maltego, metagofil dan tracerout. Sedangkan untuk prosedur active information gathering biasanya hacker menggunakan teknik Port Scanning, Banner Grab, Fingerprinting, Network Mapping dan ARP Poisoning.

2. Target Evaluasi

Tujuan dari langkah Target Evaluation adalah melakukan evaluasi data yang telah didapatkan dan mengklasifikasikannya menjadi beberapa bagian, yaitu:

- Kemungkinan-kemungkinan kelemahan target
- Identifikasi dan penentuan prioritas kerentanan pada sistem target
- Pemetaan kelemahan sistem terhadap pemilik asset
- Menemukan dokumen-dokumen

3. Exploitation

Pada langkah ini eksploitasi mulai dilakukan pada target dengan cara mencoba berbagai serangan yang sudah disesuaikan dengan data-data yang sebelumnya diperoleh. Tujuan dari kegiatan eksploitasi adalah sebagai berikut :

- Melakukan eksploitasi terhadap vulnerabilities (kerentanan)
- Memperoleh foothold (pijakan) pada sistem target
- Pengambilan data (service atau user) pada system
- Social engineering
- Serangan pada sistem atau aplikasi lain yang ada pada target menemukan dokumen - dokumen

4. Privilege Excalation (Pengambilan Akses)

Privilege Excalation mencakup kegiatan identifikasi dan password cracking terhadap akun user, dan ruang pada sistem yang lainnya. Sebuah contoh adalah mendapatkan akses user, identifikasi shadow file yang berisi user login administrator, memperoleh password administrator melalui password cracking, dan memasuki sistem aplikasi internal dengan hak akses administrator. Tujuan dari kegiatan privelege excalation adalah sebagai berikut :

- Memperoleh level akses yang tinggi ke sistem dan network target
- Memperoleh informasi akun user lain pada system
- Memperoleh akses sistem lain dengan hak yang tinggi

5. Maintaining a Foothold (Pengamanan Akses)

Pada langkah ini hal penting yang dilakukan adalah menghapus semua jejak kegiatan penetration test yang telah dilakukan. Penghapusan bukti mencakup beberapa hal seperti menghapus user logs, menggunakan saluran yang telah dimasking, dan menghapus pesan error yang mungkin di sebabkan oleh kegiatan penetration testing. Tujuan dari kegiatan maintaining foothold adalah sebagai berikut:

- Menetapkan beberapa metode akses terhadap target

- Menghilangkan bukti adanya akses yang tidak diizinkan
- Memperbaiki sistem dari dampak eksploitasi
- Mengamankan akses pada target