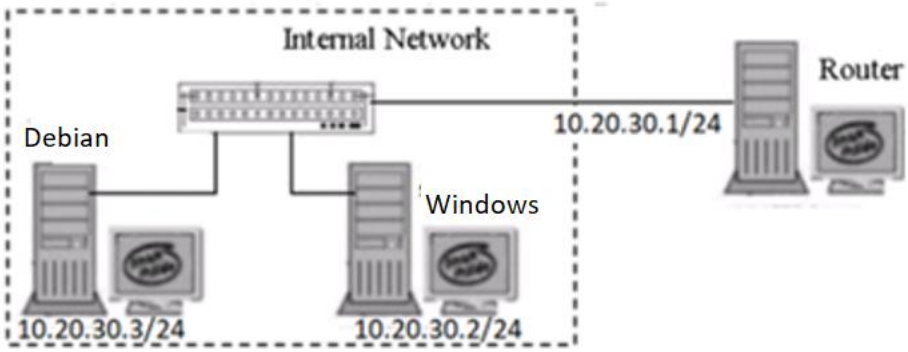
LAPORAN - JOB SHEET 5

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 kemanan host dan Server.

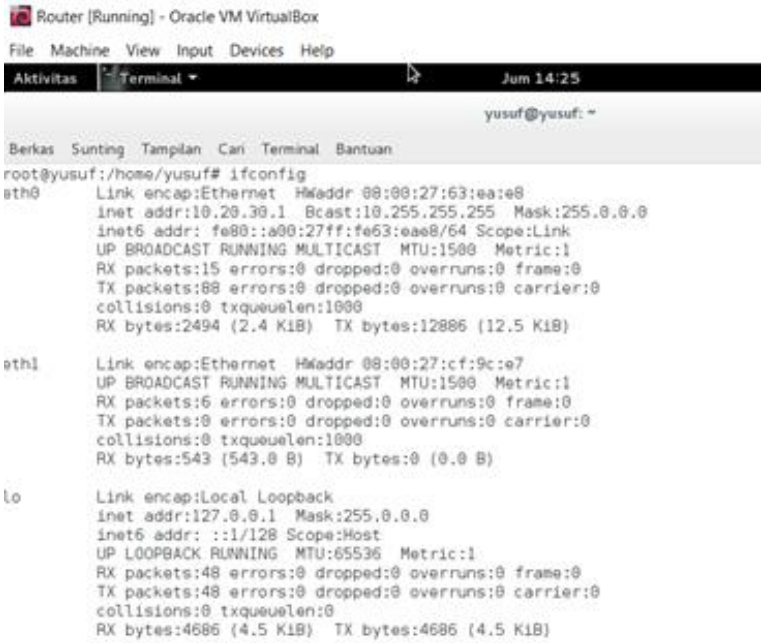
1. Bangun Topology sebagai berikut :



2. Persiapan

Router

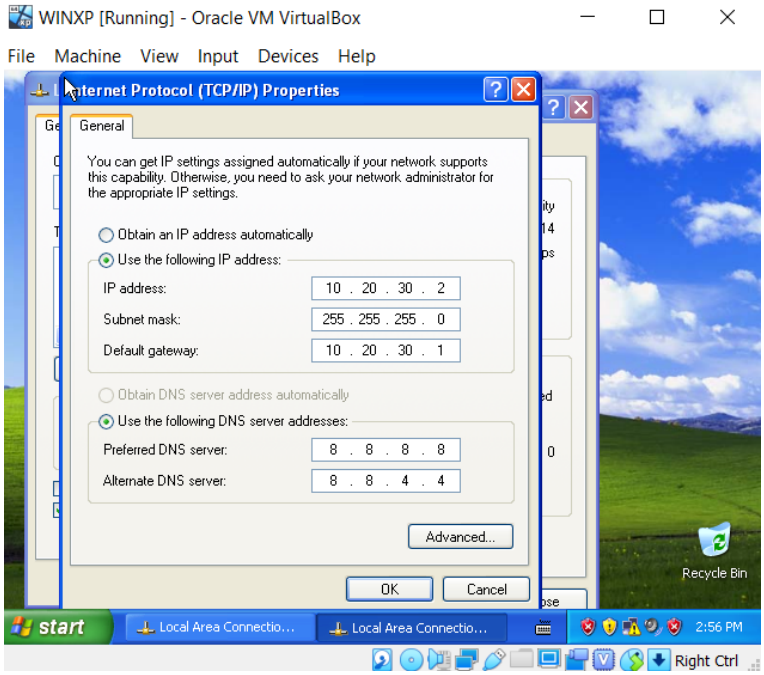
- Konfigurasi IPAddress 10.20.30.1/24



```
Router [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Aktivitas   Terminal ▾                    Jum 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:eae8/64 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)
```

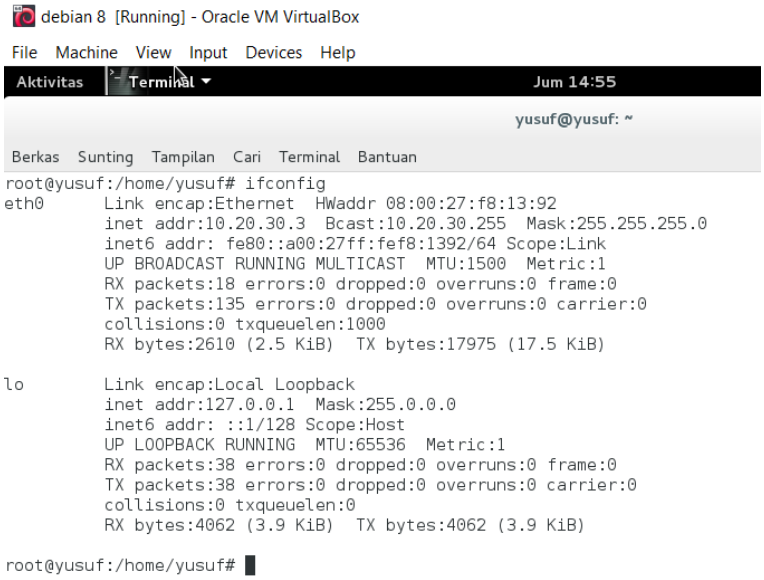
Windows

- Konfigurasi IPAddress 10.20.30.2/24



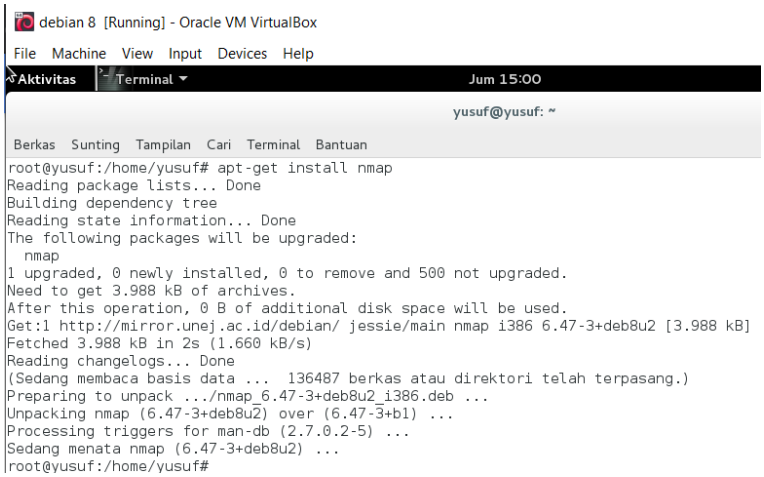
Debian

- Konfigurasi IPAddress 10.20.30.3/24



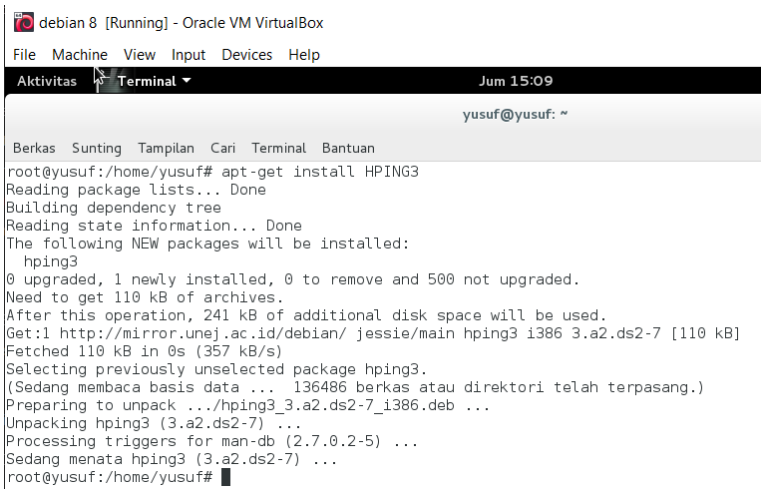
- Install Nmap

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



- Install HPING3

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

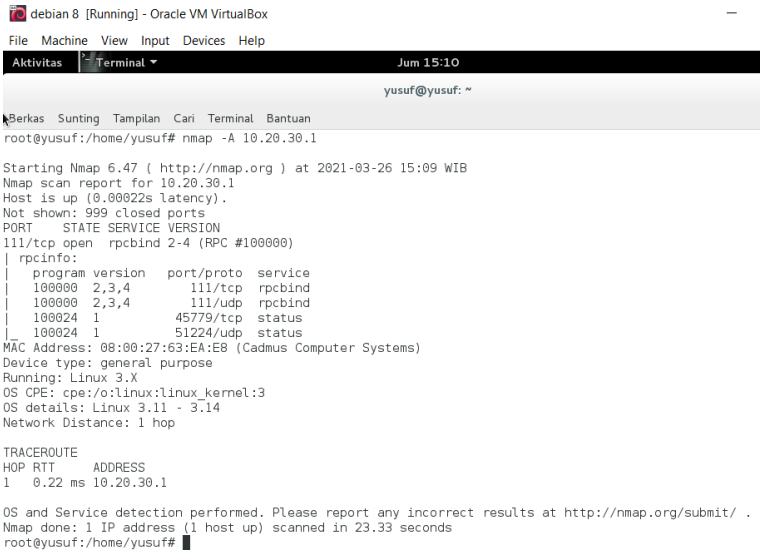


3. Lakukan Percobaan berikut dari Server-2

A. Menggunakan NMAP

- Nmap port Scaning :

```
#nmap -A 10.20.30.1
```



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:

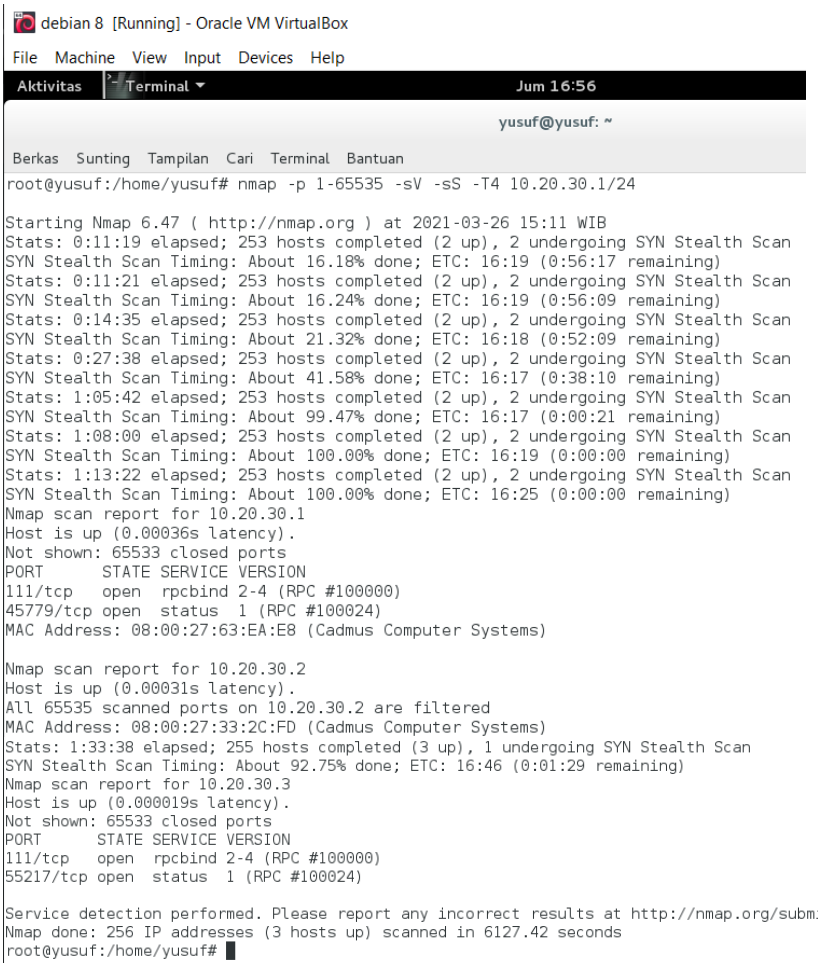
- Mac Adress
- Tipe device
- Versi linux
- OS Cpe
- OS details

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
```



```
debian 8 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Aktivitas   Terminal ▾                    Jum 16:56
                                   yusuf@yusuf: ~
Berkas  Sunting  Tampilan  Cari  Terminal  Bantuan
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:E8 (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

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

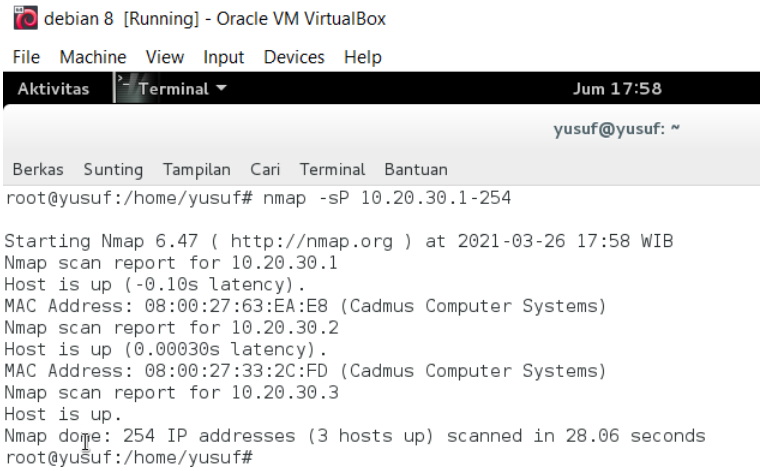
Lalu akan ada hasil deteksi dari IP 10.20.30.2/24 dengan menampilkan jumlah port yang berhasil di scan yaitu sebanyak 65535 port. Selanjutnya, hasil deteksi menampilkan MAC address dari Windows.

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
```



Hasil menunjukan bahwa,

Host yang ada dalam range 10.20.30.1-254 adatiga 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 menunjukkan 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
```

debian 8 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

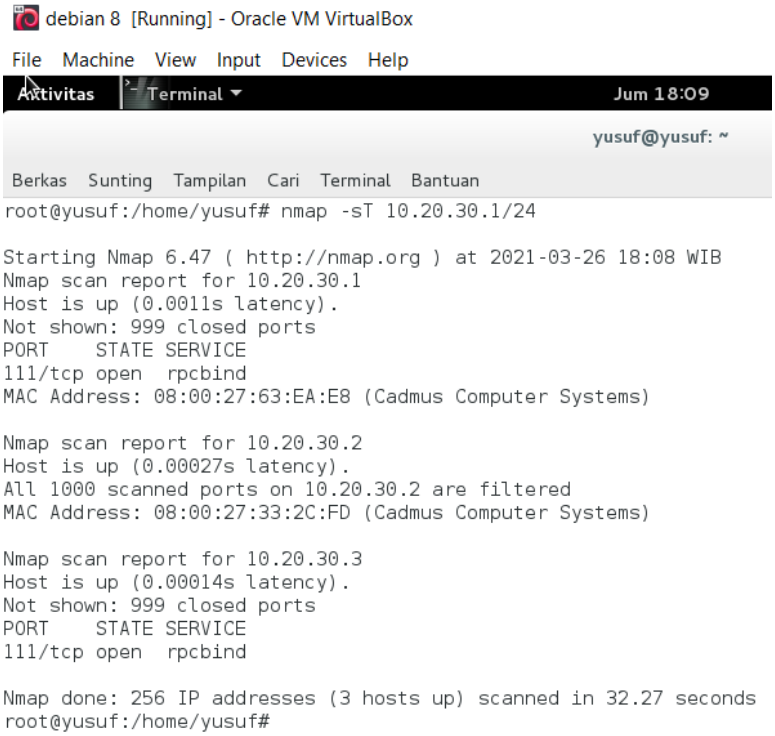
Aktivitas Terminal Jum 18:00

yusuf@yusuf: ~

Berkas Sunting Tampilan Cari Terminal Bantuan

```
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#
```

#nmap -sT 10.20.30.1/24



Hasil menunjukan bahwa,

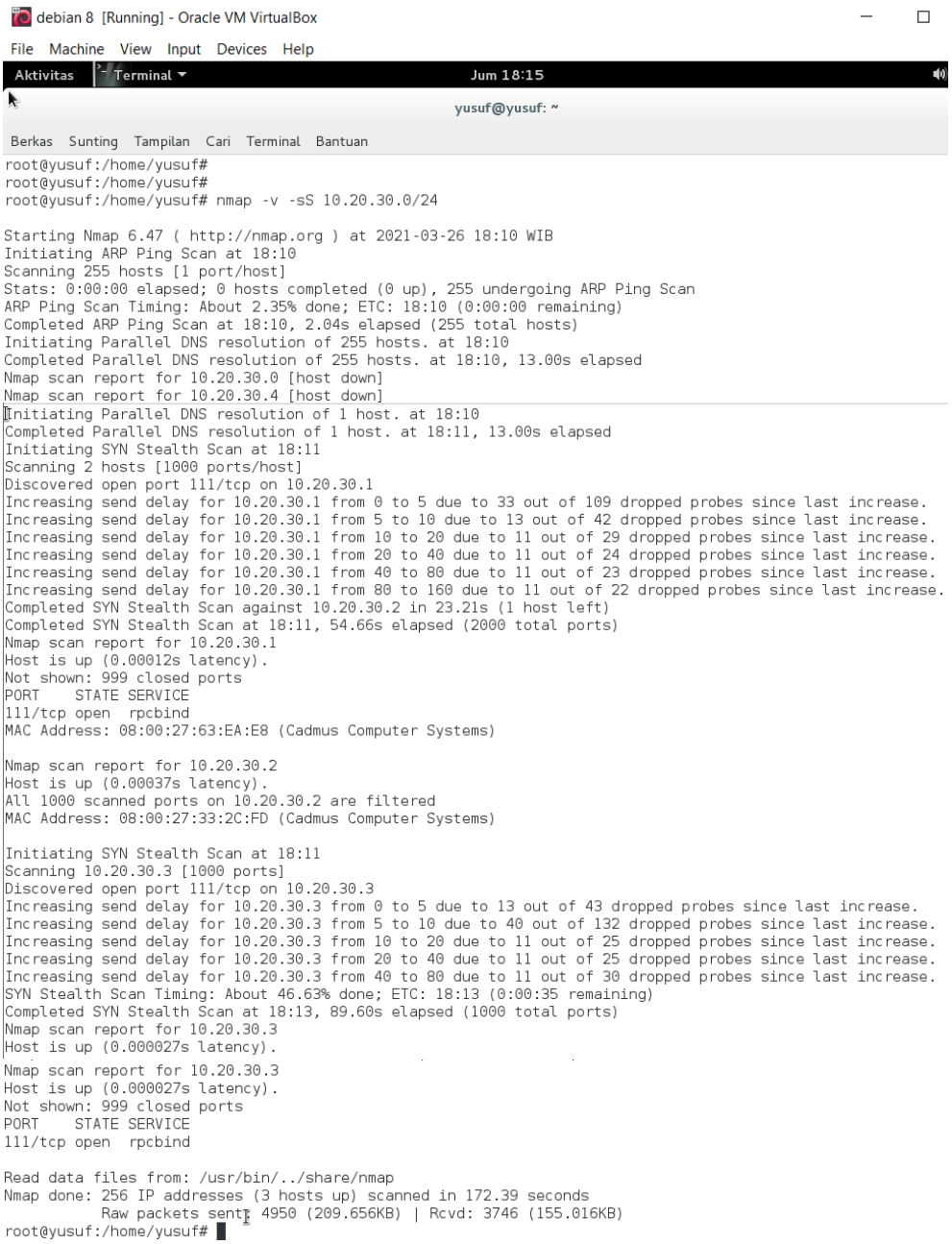
Pada pemindaian pertama yaitu dengan perintah nmap -v -sR 10.20.30.0/24 menghasilkan

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

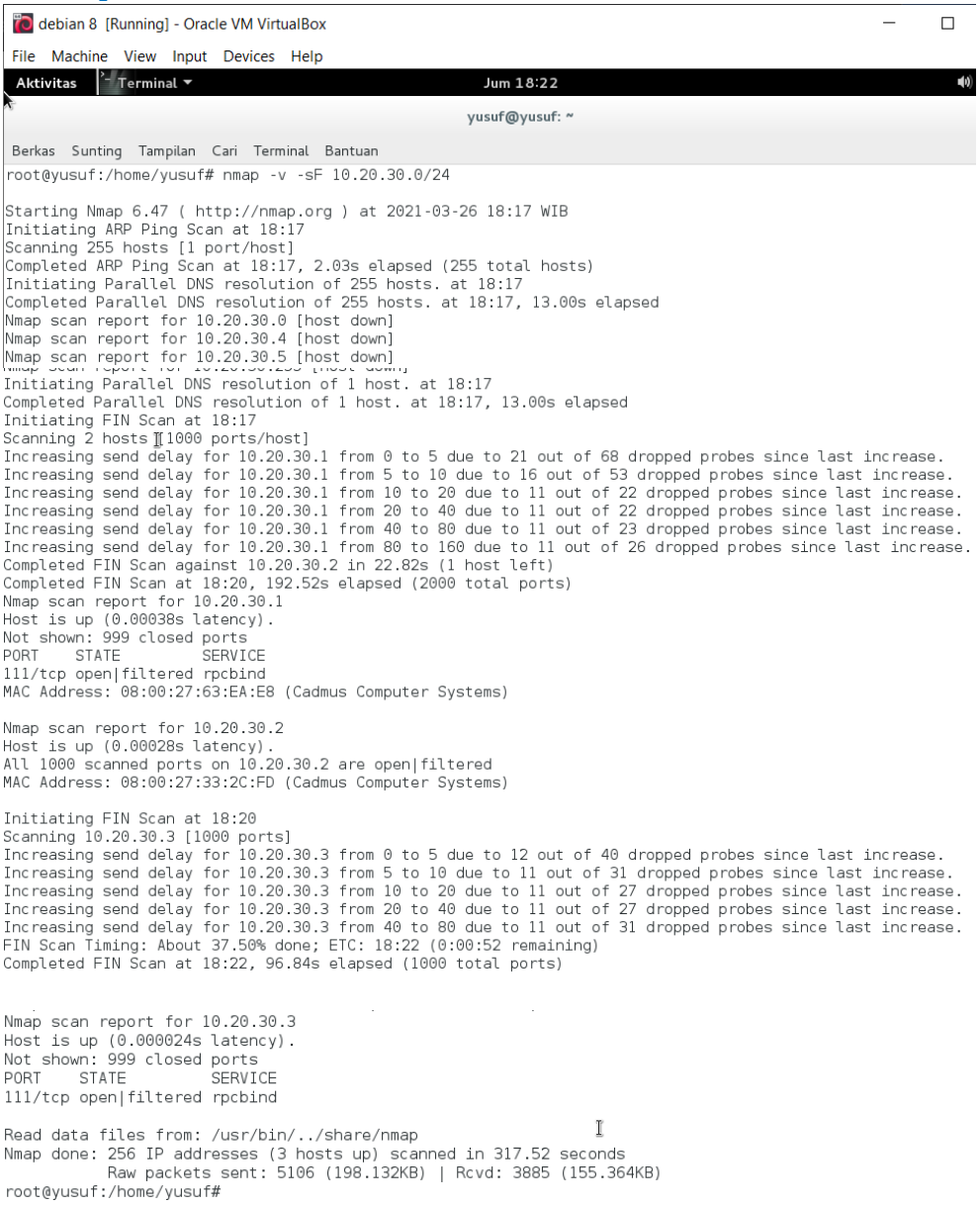
- Nmap TCP SYN (half-open) scanning

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



- Nmap TCP FIN scanning

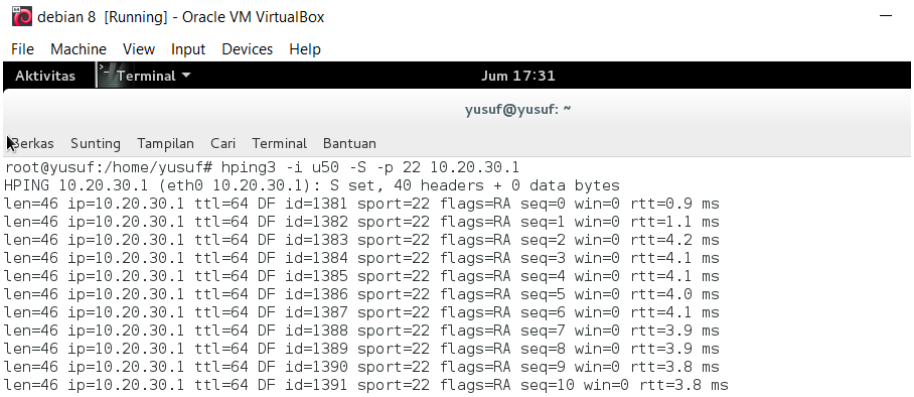
```
# nmap -v -sF 10.20.30.0/24
```



B. Menggunakan HPING

- Menyerang dengan cara SYN flood attack

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



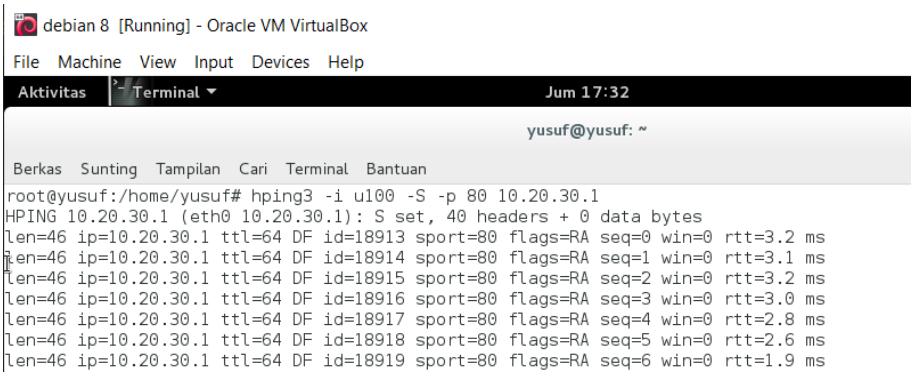
Hasil uji coba serangan tersebut, menunjukkan :

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.

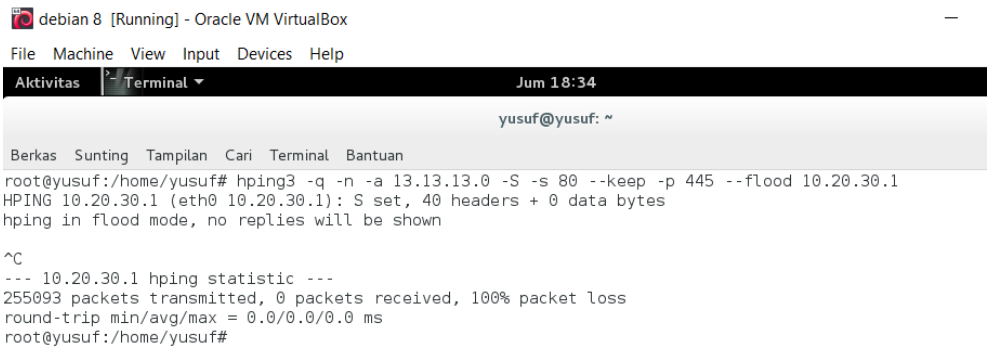
Lanjutkan untuk item selanjutnya :

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



- TCP & UDP Flood Testing

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

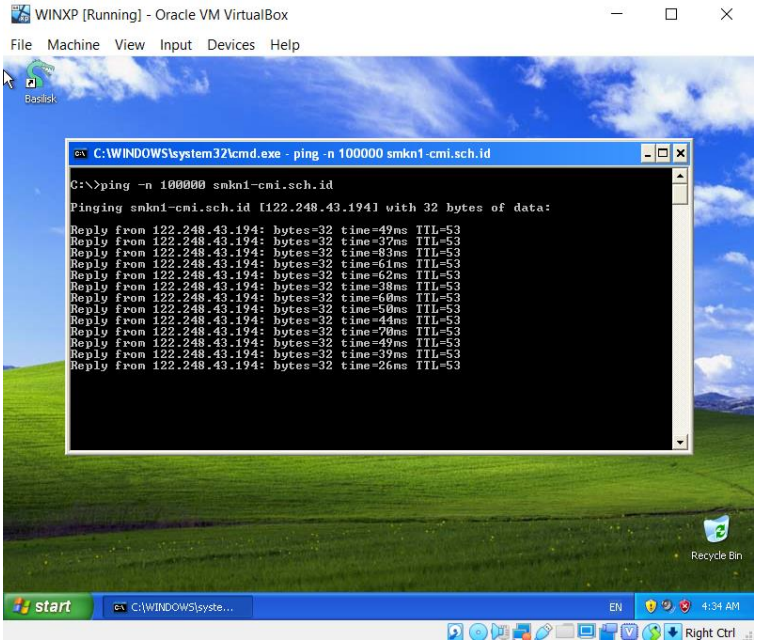


4. Melakukan dari Microsoft Windows

- ICMP Flood Testing

  Dari Windows

  c>ping -n 100000 smkn1-cmi.sch.id



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 clientnnya (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 Analisis 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