Nama : Aulia Rachmawati

NIM : L200160015

Kelas : A

-MODUL 8-

#Karena praktikum harus pakai 2 laptop dan saya praktikum sendiri di rumah jadi saya memakai virtual box, dengan ubuntu sebagai server dan kali linux sebagai Client.

Ip client

```
root@hacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.8.8.52  netmask 255.255.255.0  broadcast 10.8.8.255
        inet6 fe80::a00:27ff:fe57:e584  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:57:e5:84  txqueuelen 1000  (Ethernet)
        RX packets 7007  bytes 1481977 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1213  bytes 78071 (76.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ip server

```
aulia@aulia-VirtualBox:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:af:40:7c
          inet addr:10.8.8.53  Bcast:10.8.8.255  Mask:255.255.255.0
          inet6 addr: fe80::c219:9b5d:8a21:8281/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54073 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23231 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:79003586 (79.0 MB)  TX bytes:1900593 (1.9 MB)
```

Client ping server

```
root@hacker:~# ping 10.8.8.53
PING 10.8.8.53 (10.8.8.53) 56(84) bytes of data.
64 bytes from 10.8.8.53: icmp_seq=1 ttl=64 time=1.37 ms
64 bytes from 10.8.8.53: icmp_seq=2 ttl=64 time=0.481 ms
64 bytes from 10.8.8.53: icmp_seq=3 ttl=64 time=0.588 ms
64 bytes from 10.8.8.53: icmp_seq=4 ttl=64 time=0.642 ms
64 bytes from 10.8.8.53: icmp_seq=5 ttl=64 time=0.318 ms
```

Server ping client

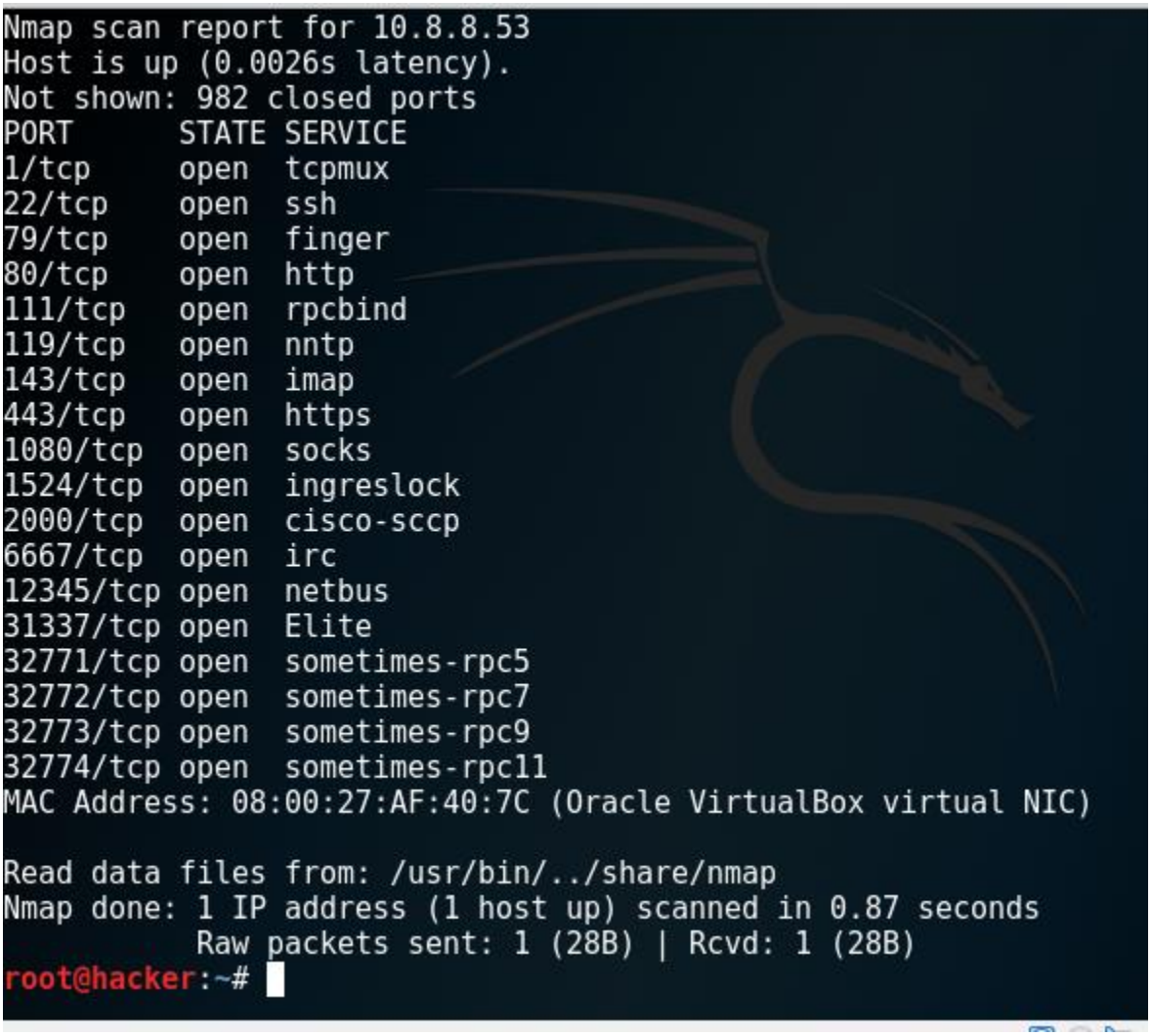
```
aulia@aulia-VirtualBox:~$ ping 10.8.8.52
PING 10.8.8.52 (10.8.8.52) 56(84) bytes of data.
64 bytes from 10.8.8.52: icmp_seq=1 ttl=64 time=0.355 ms
64 bytes from 10.8.8.52: icmp_seq=2 ttl=64 time=0.513 ms
64 bytes from 10.8.8.52: icmp_seq=3 ttl=64 time=0.505 ms
64 bytes from 10.8.8.52: icmp_seq=4 ttl=64 time=0.492 ms
```

Install portsentry

```
aulia@aulia-VirtualBox:~$ sudo apt-get install portsentry
[sudo] password for aulia:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  logcheck
The following NEW packages will be installed:
  portsentry
0 upgraded, 1 newly installed, 0 to remove and 252 not upgraded.
Need to get 0 B/64,5 kB of archives.
After this operation, 228 kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously unselected package portsentry.
(Reading database ... 183601 files and directories currently installed.)
Preparing to unpack .../portsentry_1.2-14_amd64.deb ...
Unpacking portsentry (1.2-14) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu21.21) ...
Processing triggers for ureadahead (0.100.0-19) ...
Setting up portsentry (1.2-14) ...
Processing triggers for systemd (229-4ubuntu21.21) ...
Processing triggers for ureadahead (0.100.0-19) ...
aulia@aulia-VirtualBox:~$
```

Scanning port server

Nmap -sT -v 10.8.8.53



Edit file portsentry.conf

Nano /etc/portsentry/portsentry.conf

Ubah “BLOCK_TCP=’0’” dan “BLOCK_UDP=’0’” menjadi “BLOCK_TCP=’1’” dan “BLOCK_UDP=’1’”.

```
  GNU nano 2.5.3       File: /etc/portsentry/portsentry.conf          Modified

# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"
```

Kemudian hilangkan tanda ‘#’ pada kalimat “KILL_HOSTS_DENY=”ALL: $TARGET$”. Kemudian simpan file.

```
  GNU nano 2.5.3       File: /etc/portsentry/portsentry.conf          Modified

################
# TCP Wrappers#
################
# This text will be dropped into the hosts.deny file for wrappers
# to use. There are two formats for TCP wrappers:
#
# Format One: Old Style - The default when extended host processing
# options are not enabled.
#
KILL_HOSTS_DENY="ALL: $TARGET$"
```

Edit default portsentry

Nano /etc/default/portsentry/

Ubah TCP_MODE = “tcp” menjadi TCP_MODE = “atcp” dan UDP_MODE = “udp” menjadi UDP_MODE = “audp”. Kemudian simpan file

```
  GNU nano 2.5.3         File: /etc/default/portsentry                Modified

# /etc/default/portsentry
#
# This file is read by /etc/init.d/portsentry. See the portsentry.8
# manpage for details.
#
# The options in this file refer to commandline arguments (all in lowercase)
# of portsentry. Use only one tcp and udp mode at a time.
#
TCP_MODE="atcp"
UDP_MODE="audp"
```

Edit file portsentry.ignore.static

Nano /etc/portsentry/portsentry.ignore.static

Tambahkan IP Address dari IP client. Kemudian simpan file

```
  GNU nano 2.5.3    File: /etc/portsentry/portsentry.ignore.static    Modified

# PortSentry can support full netmasks for networks as well. Format is:
#
# <IP Address>/<Netmask>
#
# Example:
#
# 192.168.2.0/24
# 192.168.0.0/16
# 192.168.2.1/32
# Etc.
#
# If you don't supply a netmask it is assumed to be 32 bits.
#
#
127.0.0.1/32
0.0.0.0

10.8.8.52/255.255.255.0
```

Restart portsentry

/etc/init.d/portsentry restart

```
root@aulia-VirtualBox:/home/aulia# /etc/init.d/portsentry restart
[ ok ] Restarting portsentry (via systemctl): portsentry.service.
root@aulia-VirtualBox:/home/aulia#
```

Membaca log portsentry terakhir

tail -f /var/log/syslog

```
sentry...
May 21 09:30:21 aulia-VirtualBox portsentry[5461]: adminalert: PortSentry 1.2 is
 starting.
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced mode wil
l monitor first 1024 ports
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced mode wil
l manually exclude port: 113
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced mode wil
l manually exclude port: 139
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced Stealth
scan detection mode activated. Ignored TCP port: 22
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced Stealth
scan detection mode activated. Ignored TCP port: 53
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced Stealth
scan detection mode activated. Ignored TCP port: 80
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced Stealth
scan detection mode activated. Ignored TCP port: 443
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced Stealth
scan detection mode activated. Ignored TCP port: 631
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced Stealth
scan detection mode activated. Ignored TCP port: 113
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: Advanced Stealth
scan detection mode activated. Ignored TCP port: 139
May 21 09:30:21 aulia-VirtualBox portsentry[5462]: adminalert: PortSentry is now
```

Scanning port server

```
root@hacker:~# nmap -sT -v 10.8.8.53

Starting Nmap 7.40 ( https://nmap.org ) at 2019-05-20 22:40 EDT
Initiating ARP Ping Scan at 22:40
Scanning 10.8.8.53 [1 port]
Completed ARP Ping Scan at 22:40, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:40
Completed Parallel DNS resolution of 1 host. at 22:40, 2.56s elapsed
Initiating Connect Scan at 22:40
Scanning 10.8.8.53 [1000 ports]
Discovered open port 80/tcp on 10.8.8.53
Discovered open port 22/tcp on 10.8.8.53
Discovered open port 443/tcp on 10.8.8.53
Connect Scan Timing: About 40.25% done; ETC: 22:41 (0:00:46 remaining)
Connect Scan Timing: About 49.80% done; ETC: 22:42 (0:01:01 remaining)
Connect Scan Timing: About 53.20% done; ETC: 22:43 (0:01:20 remaining)
```

Cek log portsentry

```
can from host: 10.8.8.52/10.8.8.52 to TCP port: 808
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: Host: 10.8.8.52/
10.8.8.52 is already blocked Ignoring
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: TCP SYN/Normal s
can from host: 10.8.8.52/10.8.8.52 to TCP port: 264
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: Host: 10.8.8.52/
10.8.8.52 is already blocked Ignoring
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: TCP SYN/Normal s
can from host: 10.8.8.52/10.8.8.52 to TCP port: 119
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: Host: 10.8.8.52/
10.8.8.52 is already blocked Ignoring
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: TCP SYN/Normal s
can from host: 10.8.8.52/10.8.8.52 to TCP port: 222
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: Host: 10.8.8.52/
10.8.8.52 is already blocked Ignoring
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: TCP SYN/Normal s
can from host: 10.8.8.52/10.8.8.52 to TCP port: 666
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: Host: 10.8.8.52/
10.8.8.52 is already blocked Ignoring
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: TCP SYN/Normal s
can from host: 10.8.8.52/10.8.8.52 to TCP port: 880
May 21 09:40:38 aulia-VirtualBox portsentry[5462]: attackalert: Host: 10.8.8.52/
10.8.8.52 is already blocked Ignoring
root@aulia-VirtualBox:/home/aulia#
```

Cek blocked tcp

```
  GNU nano 2.5.3         File: portsentry.blocked.atcp

1558405837 - 05/21/2019 09:30:37 Host: 10.8.8.214/10.8.8.214 Port: 445 TCP Bloc$
1558405883 - 05/21/2019 09:31:23 Host: 10.8.8.139/10.8.8.139 Port: 445 TCP Bloc$
1558406438 - 05/21/2019 09:40:38 Host: 10.8.8.52/10.8.8.52 Port: 995 TCP Blocked
```

Cek host deny

```
  GNU nano 2.5.3            File: /etc/hosts.deny

# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

#ALL: 192.168.100.109 : DENY
#ALL: 192.168.100.109 : DENY
ALL: 172.20.1.33 : DENY
ALL: 172.20.0.133 : DENY
ALL: 192.168.1.132 : DENY
ALL: 10.10.28.65 : DENY
ALL: 10.10.28.65 : DENY
ALL: 10.8.8.214
ALL: 10.8.8.139
ALL: 10.8.8.52
```

Cek Portsentry.history

```
  GNU nano 2.5.3    File: /var/lib/portsentry/portsentry.history

1558404536 - 05/21/2019 09:08:56 Host: 10.8.8.41/10.8.8.41 Port: 161 UDP Blocked
1558404631 - 05/21/2019 09:10:31 Host: 10.8.8.52/10.8.8.52 Port: 111 TCP Blocked
1558405837 - 05/21/2019 09:30:37 Host: 10.8.8.214/10.8.8.214 Port: 445 TCP Bloc$
1558405883 - 05/21/2019 09:31:23 Host: 10.8.8.139/10.8.8.139 Port: 445 TCP Bloc$
1558406438 - 05/21/2019 09:40:38 Host: 10.8.8.52/10.8.8.52 Port: 995 TCP Blocked
```

Cek Route

```
root@aulia-VirtualBox:/var/lib/portsentry# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.8.8.1        0.0.0.0         UG    100    0        0 enp0s3
10.8.8.0        *               255.255.255.0   U     100    0        0 enp0s3
10.8.8.52       -               255.255.255.255 !H    0      -        0 -
10.8.8.139      -               255.255.255.255 !H    0      -        0 -
10.8.8.214      -               255.255.255.255 !H    0      -        0 -
link-local      *               255.255.0.0     U     1000   0        0 enp0s3
root@aulia-VirtualBox:/var/lib/portsentry#
```

Ping server

```
root@hacker:~# ping 10.8.8.53
PING 10.8.8.53 (10.8.8.53) 56(84) bytes of data.
From 10.8.8.52 icmp_seq=1 Destination Host Unreachable
From 10.8.8.52 icmp_seq=2 Destination Host Unreachable
From 10.8.8.52 icmp_seq=3 Destination Host Unreachable
From 10.8.8.52 icmp_seq=4 Destination Host Unreachable
From 10.8.8.52 icmp_seq=5 Destination Host Unreachable
From 10.8.8.52 icmp_seq=6 Destination Host Unreachable
```

Cek hosts.deny

```
  GNU nano 2.5.3            File: /etc/hosts.deny

# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

#ALL: 192.168.100.109 : DENY
#ALL: 192.168.100.109 : DENY
ALL: 172.20.1.33 : DENY
ALL: 172.20.0.133 : DENY
ALL: 192.168.1.132 : DENY
ALL: 10.10.28.65 : DENY
ALL: 10.10.28.65 : DENY
ALL: 10.8.8.214
ALL: 10.8.8.139
ALL: 10.8.8.52
```

Hapus host 10.8.8.52

```
root@aulia-VirtualBox:/var/lib/portsentry# route del -host 10.8.8.52 reject
root@aulia-VirtualBox:/var/lib/portsentry# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.8.8.1        0.0.0.0         UG    100    0        0 enp0s3
10.8.8.0        *               255.255.255.0   U     100    0        0 enp0s3
10.8.8.139      -               255.255.255.255 !H    0      -        0 -
10.8.8.214      -               255.255.255.255 !H    0      -        0 -
link-local      *               255.255.0.0     U     1000   0        0 enp0s3
root@aulia-VirtualBox:/var/lib/portsentry#
```

Ping server

```
root@hacker:~# ping 10.8.8.53
PING 10.8.8.53 (10.8.8.53) 56(84) bytes of data.
64 bytes from 10.8.8.53: icmp_seq=1 ttl=64 time=0.330 ms
64 bytes from 10.8.8.53: icmp_seq=2 ttl=64 time=0.408 ms
64 bytes from 10.8.8.53: icmp_seq=3 ttl=64 time=0.464 ms
64 bytes from 10.8.8.53: icmp_seq=4 ttl=64 time=0.474 ms
64 bytes from 10.8.8.53: icmp_seq=5 ttl=64 time=0.699 ms
64 bytes from 10.8.8.53: icmp_seq=6 ttl=64 time=0.310 ms
64 bytes from 10.8.8.53: icmp_seq=7 ttl=64 time=0.531 ms
```

Nmap server

```
root@hacker:~# nmap -sT -v 10.8.8.53

Starting Nmap 7.40 ( https://nmap.org ) at 2019-05-20 22:54 EDT
Initiating ARP Ping Scan at 22:54
Scanning 10.8.8.53 [1 port]
Completed ARP Ping Scan at 22:54, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:54
Completed Parallel DNS resolution of 1 host. at 22:54, 0.02s elapsed
Initiating Connect Scan at 22:54
Scanning 10.8.8.53 [1000 ports]
Discovered open port 22/tcp on 10.8.8.53
Discovered open port 80/tcp on 10.8.8.53
Discovered open port 443/tcp on 10.8.8.53
Completed Connect Scan at 22:54, 0.11s elapsed (1000 total ports)
Nmap scan report for 10.8.8.53
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:AF:40:7C (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
root@hacker:~#
```