

**LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
PERTEMUAN 6
SNORT DAN FIREWALL RULES**



DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

SNORT DAN FIREWALL RULES

A. TUJUAN

- a. Mempersiapkan Lingkungan Virtual
- b. Firewall dan Log IDS
- c. Hentikan dan Hapus Proses Mininet

B. DASAR TEORI

a. Snort

Snort adalah Network Intrusion Detection and Prevention System (NIDS/NIPS) gratis dan open source yang dapat digunakan untuk memantau dan menganalisis lalu lintas jaringan secara real time.

Snort dapat mendeteksi banyak jenis serangan dengan menganalisis lalu lintas jaringan berdasarkan aturan yang dirancang untuk mengidentifikasi pola dan perilaku tertentu.

b. Firewall Rules

Firewall rules adalah kumpulan instruksi yang menentukan bagaimana perangkat firewall mengelola lalu lintas jaringan masuk dan keluar. Aturan ini adalah mekanisme kontrol akses yang menegakkan keamanan di jaringan dengan mengizinkan atau memblokir komunikasi berdasarkan kriteria yang telah ditentukan seperti alamat IP sumber atau tujuan, port, protokol, dan layanan.

Firewall adalah perangkat keamanan jaringan yang memantau lalu lintas jaringan masuk dan keluar dan memutuskan apakah akan mengizinkan atau memblokir lalu lintas tertentu berdasarkan kumpulan aturan keamanan yang telah ditentukan. Firewall telah menjadi garis pertahanan pertama dalam keamanan jaringan selama lebih dari 25 tahun. Firewall secara cermat menganalisis lalu lintas masuk berdasarkan aturan yang telah ditentukan sebelumnya dan menyaring lalu lintas yang berasal dari sumber yang tidak aman atau mencurigakan untuk mencegah serangan.

C. ALAT DAN BAHAN

- a. Mesin virtual CyberOps Workstation
- b. Koneksi Internet

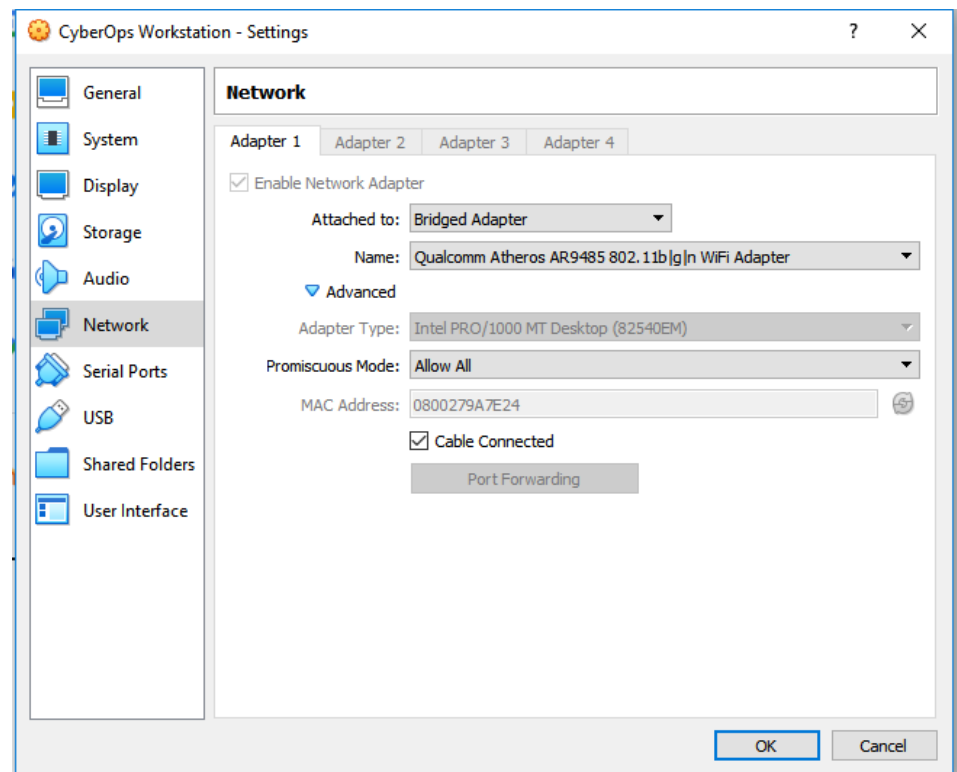
D. HASIL DAN ANALISIS

1. Bagian 1:

Mempersiapkan Lingkungan Virtual

- Luncurkan Oracle VirtualBox dan ubah CyberOps Workstation untuk mode Bridged, jika perlu. Pilih Mesin > Pengaturan > Jaringan. Di bawah

Attached To, pilih Bridged Adapter (atau jika Anda menggunakan WiFi dengan proxy, Anda mungkin memerlukan adaptor NAT) dan klik OK



- Luncurkan VM CyberOps Workstation, buka terminal dan konfigurasi jaringan dengan menjalankan skrip `configure_as_dhcp.sh`. Karena skrip memerlukan hak pengguna super, berikan kata sandi untuk user analyst

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/configure_as_dhcp.sh
[sudo] password for analyst: [analyst@secOps ~]$
```

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/configure_as_dhcp.sh
[sudo] password for analyst:
Configuring the NIC to request IP info via DHCP...
Requesting IP information...
IP Configuration successful.
```

Gunakan perintah `ifconfig` untuk memverifikasi CyberOps Workstation VM sekarang memiliki alamat IP di jaringan lokal Anda. Anda juga dapat menguji konektivitas ke server web publik dengan melakukan ping ke `www.cisco.com`. Gunakan `Ctrl+C` untuk menghentikan ping.

```
[analyst@secOps ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::a00:27ff:fe9a:7e24 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:9a:7e:24 txqueuelen 1000 (Ethernet)
    RX packets 141 bytes 14476 (14.1 KiB)
    RX errors 0 dropped 59 overruns 0 frame 0
    TX packets 36 bytes 6648 (6.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[analyst@secOps ~]$ ping www.cisco.com
PING e2867.dsca.akamaiedge.net (23.11.57.176) 56(84) bytes of data.
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=1 ttl=57 time=67.3 ms
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=2 ttl=57 time=73.1 ms
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=3 ttl=57 time=74.6 ms
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=4 ttl=57 time=54.8 ms
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=5 ttl=57 time=52.3 ms
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=6 ttl=57 time=66.7 ms
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=7 ttl=57 time=70.0 ms
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176): icmp_seq=8 ttl=57 time=65.4 ms
^C
--- e2867.dsca.akamaiedge.net ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 52.329/65.533/74.571/7.533 ms
```

2. Bagian 2: Firewall and IDS Logs

- a. Dari VM CyberOps Workstation, jalankan skrip untuk memulai mininet.mininet
- b. Dari prompt mininet, buka shell di R1 menggunakan perintah di bawah ini:

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/cyberops_extended_topo_no_fw.py
[sudo] password for analyst:
*** Adding controller
*** Add switches
*** Add hosts
*** Add links
*** Starting network
*** Configuring hosts
R1 R4 H1 H2 H3 H4 H5 H6 H7 H8 H9 H10 H11
*** Starting controllers
*** Starting switches
*** Add routes
*** Post configure switches and hosts
*** Starting CLI:
mininet> xterm R1
mininet> █
```

- c. Dari shell R1, jalankan IDS berbasis Linux, Snort..

```
[root@secOps analyst]# ./lab.support.files/scripts/start_snort.sh █
```

```

| Memory (MB)      : 13.80
| Patterns         : 0.25
| Match Lists      : 0.45
| DFA
|   1 byte states  : 0.28
|   2 byte states  : 12.63
|   4 byte states  : 0.00
+-----+
[ Number of patterns truncated to 20 bytes: 14 ]
pcap DAQ configured to passive.
Acquiring network traffic from "R1-eth0".
Reload thread starting...
Reload thread started, thread 0x7f198aa60700 (806)
Decoding Ethernet
Set gid to 29
Set uid to 29

---- Initialization Complete ----

o'')~  -*) Snort! <*-
''''   Version 2.9.11.1 GRE (Build 268)
      By Martin Roesch & The Snort Team; http://www.snort.org/contact#team
      Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.

      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.9.1 (with TPACKET_V3)
      Using PCRE version: 8.44 2020-02-12
      Using ZLIB version: 1.2.11

      Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
      Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
      Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
      Preprocessor Object: SF_GTP Version 1.1 <Build 1>
      Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
      Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
      Preprocessor Object: SF_SSH Version 1.1 <Build 3>
      Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
      Preprocessor Object: SF_SIP Version 1.1 <Build 1>
      Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
      Preprocessor Object: SF_SDF Version 1.1 <Build 1>
      Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
      Preprocessor Object: SF_DNS Version 1.1 <Build 4>
      Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
      Preprocessor Object: SF_POP Version 1.0 <Build 1>
Commencing packet processing (pid=793)
03/20-22:02:59.021144 fe80::470:ddff:fed1:3570 -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:56
+++++

```

- d. Dari prompt mininet CyberOps Workstation VM, buka shell untuk host H5 dan H10.

```

mininet> xterm H5
mininet> xterm H10

```

- e. H10 akan mensimulasikan server di Internet yang menghosting malware. Pada H10, jalankan skrip `mal_server_start.sh` untuk memulai server. f. Pada H10, gunakan `netstat` dengan opsi `-tunpa` untuk memverifikasi bahwa server web sedang berjalan. Saat digunakan seperti yang ditunjukkan di bawah ini, `netstat` mencantumkan semua port yang saat ini ditetapkan ke layanan:

Pada H5, gunakan perintah tcpdump untuk merekam peristiwa dan mengunduh file malware lagi sehingga Anda dapat merekam transaksi. Keluarkan perintah berikut di bawah ini mulai pengambilan paket:

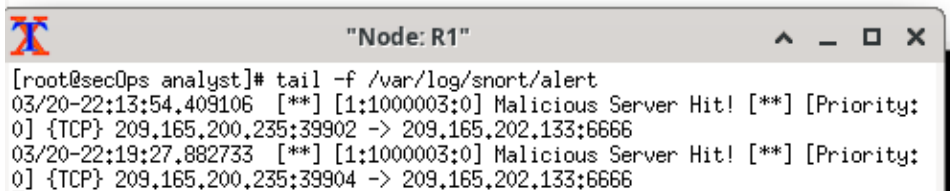
```
[root@secOps analyst]# tcpdump -i H5-eth0 -w nimda.download.pcap &
[1] 899
[root@secOps analyst]# tcpdump: listening on H5-eth0, link-type EN10MB (Ethernet
), capture size 262144 bytes
```

- i. Sekarang tcpdump menangkap paket, unduh malware lagi. Pada H5, jalankan kembali perintah atau gunakan panah atas untuk memanggilnya kembali dari fasilitas riwayat perintah.

```
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 22:19:27-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345088 (337K) [application/octet-stream]
Saving to: 'W32.Nimda.Amm.exe.2'

W32.Nimda.Amm.exe.2 100%[=====>] 337.00K --.-KB/s in 0.01s

2023-03-20 22:19:27 (23.3 MB/s) - 'W32.Nimda.Amm.exe.2' saved [345088/345088]
```



```
"Node: R1"
[root@secOps analyst]# tail -f /var/log/snort/alert
03/20-22:13:54.409106 00000003:0] Malicious Server Hit! 00000003:0] [Priority:
0] {TCP} 209.165.200.235:39902 -> 209.165.202.133:6666
03/20-22:19:27.882733 00000003:0] Malicious Server Hit! 00000003:0] [Priority:
0] {TCP} 209.165.200.235:39904 -> 209.165.202.133:6666
```

- j. Hentikan pengambilan dengan membawa tcpdump ke latar depan dengan perintah fg. Karena tcpdump adalah satu-satunya proses yang dikirim ke latar belakang, PID tidak perlu ditentukan. Hentikan proses tcpdump dengan Ctrl+C. Proses tcpdump berhenti dan menampilkan ringkasan tangkapan. Jumlah paket mungkin berbeda untuk pengambilan Anda

```
[root@secOps analyst]# fg
tcpdump -i H5-eth0 -w nimda.download.pcap
^C60 packets captured
60 packets received by filter
0 packets dropped by kernel
```

- k. Pada H5, Gunakan perintah ls untuk memverifikasi file pcap sebenarnya disimpan ke disk dan memiliki ukuran lebih besar dari nol:

```
[root@secOps analyst]# ls -l
total 1504
drwxr-xr-x 2 analyst analyst 4096 May 20 2020 Desktop
drwxr-xr-x 3 analyst analyst 4096 Feb 20 20:40 Downloads
-rw-r--r-- 1 root root 80024 Mar 1 22:47 httpdump.pcap
-rw-r--r-- 1 root root 36864 Feb 20 21:31 httpsdump.pcap
-rw-r--r-- 1 analyst analyst 51 Mar 6 21:18 lab.support
drwxr-xr-x 9 analyst analyst 4096 Jul 15 2020 lab.support.files
-rw-r--r-- 1 root root 350374 Mar 20 22:22 nimda.download.pcap
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Mar 13 21:54 W32.Nimda.Amm.exe
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe.1
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe.2
```

Menyetel Aturan Firewall Berdasarkan IDS Alerts

- a. Di VM CyberOps Workstation, mulai jendela terminal R1 ketiga.

```
mininet> xterm R1
```

- b. Di jendela terminal R1 baru, gunakan perintah iptables untuk membuat daftar rantai dan aturannya yang sedang digunakan:

```
[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
```

- c. Koneksi ke server menghasilkan paket yang harus melintasi firewall iptables di R1. Paket yang melintasi firewall ditangani oleh aturan FORWARD dan oleh karena itu, rantai itulah yang akan menerima aturan pemblokiran. Agar komputer pengguna tidak terhubung ke server yang diidentifikasi di Langkah 1, tambahkan aturan berikut ke rantai FORWARD di R1:
- d. Gunakan perintah iptables lagi untuk memastikan aturan telah ditambahkan ke rantai FORWARD. VM CyberOps Workstation mungkin memerlukan beberapa detik untuk menghasilkan output:

```
[root@secOps analyst]# iptables -I FORWARD -p tcp -d 209.165.202.133 --dport 6666 -j DROP
[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
    0    0 DROP     tcp  --  any    any    anywhere                209.165.202.133 tcp dpt:6666

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
```

- e. Pada H5, coba unduh file lagi:

```
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 22:31:02-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... failed: Connection timed out.
Retrying.

--2023-03-20 22:33:12-- (try: 2) http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... ^C
```

- f. Hentikan dan Hapus Proses Mininet


```
mininet> quit
*** Stopping 0 controllers

*** Stopping 5 terms
*** Stopping 15 links
.....
*** Stopping 3 switches
S5 S9 S10
*** Stopping 13 hosts
R1 R4 H1 H2 H3 H4 H5 H6 H7 H8 H9 H10 H11
*** Done
```

- g. Setelah keluar dari Mininet, bersihkan proses yang dimulai oleh Mininet. Masukkan kata sandi cyberops saat diminta.

```
[analyst@secOps ~]$ sudo mn -c
[sudo] password for analyst:
*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-
openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core o
vs-openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
pkill -9 -f "sudo mnexec"
*** Removing junk from /tmp
rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
*** Removing old X11 tunnels
*** Removing excess kernel datapaths
ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/nl:/'
*** Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'
ip link show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
```

PEMBAHASAN:

1. mininet> xterm R1
mininet>

Shell R1 terbuka di jendela terminal dengan teks hitam dan latar belakang putih. Pengguna apa yang masuk ke shell itu? Ini indikatornya apa?

- Pengguna root (root user). Diindikasikan dengan tanda # setelah prompt

```

2. [root@secOps analyst]# wget
209.165.202.133:6666/W32.Nimda.Amm.exe
--2017-04-28 17:00:04--
http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345088 (337K) [application/octet-stream]
Saving to: 'W32.Nimda.Amm.exe'
W32.Nimda.Amm.exe
100%[=====>] 337.00K
--.-KB/s in 0.02s
2017-04-28 17:00:04 (16.4 MB/s) - 'W32.Nimda.Amm.exe' saved
[345088/345088]
[root@secOps analyst]#

```

Port apa yang digunakan saat berkomunikasi dengan server web malware?
Apa indikatornya?

➤ Port 6666. Port ditentukan pada URL setelah : sebagai pemisah.

3. Apakah file telah diunduh sepenuhnya?

➤ Iya, file telah diunduh sepenuhnya

4. Apakah IDS menghasilkan peringatan yang terkait dengan unduhan file?

➤ Iya

5. Gambar untuk nomor 5 - 8

```

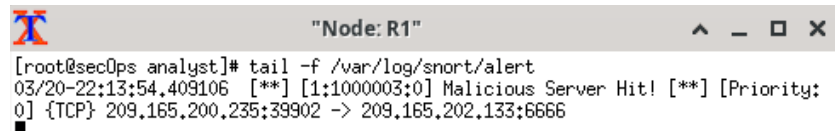
04/28-17:00:04.092153 [**] [1:1000003:0] Malicious Server
Hit! [**] [Priority: 0]

```

```

{TCP} 209.165.200.235:34484 -> 209.165.202.133:6666 (SOAL)

```



```

[root@secOps analyst]# tail -f /var/log/snort/alert
03/20-22:13:54.409106 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority:
0] {TCP} 209.165.200.235:39902 -> 209.165.202.133:6666

```

(HASIL

PRAKTIKUM)

Berdasarkan peringatan yang ditunjukkan di atas, apa alamat IPv4 sumber dan tujuan yang digunakan dalam transaksi?

➤ Source IP: 209.165.200.235

➤ Destination IP: 209.165.202.133.

6. Berdasarkan alert di atas, port sumber dan tujuan apa yang digunakan dalam transaksi?

➤ Source port: 34484 (sesuai soal); Source port: 39902 (sesuai hasil praktikum)

➤ Destination port: 6666

7. Berdasarkan peringatan yang ditunjukkan di atas, kapan pengunduhan dilakukan?

➤ 28 April 2017 sekitar pukul 17.00 pada soal. Sedangkan, 20 Maret 2023 sekitar pukul 22.19 pada hasil praktikum

8. Berdasarkan peringatan yang ditunjukkan di atas, apa pesan yang direkam IDS signature?
- “Malicious Server Hit!”
9. Bagaimana file PCAP ini berguna bagi analis keamanan?
- File PCAP berisi paket terkait lalu lintas yang terlihat oleh NIC yang meminta data. PCAP dengan sendirinya sangat berguna untuk melacak peristiwa jaringan seperti komunikasi dengan titik akhir berbahaya. Alat seperti Wireshark dapat digunakan untuk memfasilitasi analisis PCAP.
10. [root@secOps ~]# iptables -L -v
- ```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source
destination
Chain FORWARD (policy ACCEPT 6 packets, 504 bytes)
pkts bytes target prot opt in out source
destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source
destination
[root@secOps ~]#
```

Rantai apa yang saat ini digunakan oleh R1?

- INPUT, OUTPUT, dan FORWARD

11. Untuk nomor 11-12

```
[root@secOps analyst]# wget
209.165.202.133:6666/W32.Nimda.Amm.exe
--2017-05-01 14:42:37--
http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... failed: Connection
timed out.
Retrying.
--2017-05-01 14:44:47-- (try: 2)
http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... failed: Connection
timed out.
Retrying.
```

Apakah unduhan berhasil kali ini? Jelaskan.

- Tidak. Firewall sedang memblokir koneksi ke server yang meng-hosting malware.
12. Apa pendekatan yang lebih agresif tetapi juga valid saat memblokir server yang melanggar?
- Alih-alih menentukan IP, protokol, dan port, aturan tersebut dapat dengan mudah memblokir alamat IP server. Ini sepenuhnya mencegah akses ke server ini dari jaringan internal.

Setelah shell R1 terbuka di jendela terminal, maka root user akan masuk ke shell itu, diindikasikan dengan tanda # setelah prompt. Port yang digunakan saat berkomunikasi dengan server web malware adalah port 6666, dapat dilihat pada `http://209.165.202.133:6666/W32.Nimda.Amm.exe`. Terlihat pada keterangan `2023-03-20 17:00:04 (23.3 MB/s) - 'W32.Nimda.Amm.exe' saved` dengan itu maka file telah diunduh sepenuhnya. Port yang digunakan dalam transaksi ini yaitu, Source port: 39902, dan Destination port: 6666. Dapat dilihat pada {TCP} `209.165.200.235:39902 -> 209.165.202.133:6666.`

File PCAP berguna bagi analisis keamanan karena file PCAP berisi paket terkait lalu lintas yang terlihat oleh NIC yang meminta data. PCAP dengan sendirinya sangat berguna untuk melacak peristiwa jaringan seperti komunikasi dengan titik akhir berbahaya. Alat seperti Wireshark dapat digunakan untuk memfasilitasi analisis PCAP. Chain yang digunakan pada shell R1 antara lain, INPUT, OUTPUT, dan FORWARD. Chain INPUT digunakan untuk memproses trafik paket data yang masuk ke dalam router melalui interface yang ada di router dan memiliki tujuan IP Address berupa ip yang terdapat pada router. Chain OUTPUT digunakan untuk memproses trafik paket data yang keluar dari router. Chain FORWARD digunakan untuk memproses trafik paket data yang hanya melewati router. Pada saat firewall memblokir koneksi ke server yang menghosting malware maka download akan gagal. Pendekatan agresif yang dapat dilakukan saat memblokir server yang melanggar adalah dengan memblokir IP Server.

## **E. KESIMPULAN**

Sebuah file malware berhasil diunduh dengan menggunakan port 6666 pada tanggal 20 Maret 2023 (tanggal dilaksanakannya praktikum). Koneksi dilakukan melalui Source port 39902 dan Destination port 6666. File PCAP sangat berguna untuk menganalisis lalu lintas jaringan, dan dapat digunakan dengan bantuan alat seperti Wireshark. Shell R1 menggunakan chain INPUT, OUTPUT, dan FORWARD. Firewall dapat menghentikan koneksi ke server yang meng-hosting malware, yang menyebabkan unduhan gagal. Pendekatan yang agresif untuk memblokir server yang melanggar adalah dengan memblokir alamat IP server.

## F. DAFTAR PUSTAKA

Abdullahi, A. (2023, February 16). *What are Firewall Rules? Definition, Types & Best*

*Practices*. Enterprise Networking Planet. Diakses pada Maret 25, 2023, dari

<https://www.enterprisenetworkingplanet.com/security/firewall-rules/>

Cisco. (n.d.). *What Is a Firewall?* Cisco. Diakses pada Maret 25, 2023, dari

[https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.htm](https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html)

l

Tasneem, A., Kumar, A., & Sharma, S. (2018, December). Intrusion Detection

Prevention System using SNORT. *International Journal of Computer*

*Applications, Volume 181 – No. 32, 22.*

[https://www.researchgate.net/publication/329716671\\_Intrusion\\_Detection\\_Prevention\\_System\\_using\\_SNORT](https://www.researchgate.net/publication/329716671_Intrusion_Detection_Prevention_System_using_SNORT)