

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
Snort & Firewall Rules



DI SUSUN OLEH

Nama : M Abdul Aziz
NIM : 21/474516/SV/18951
Hari, Tanggal : Selasa, 21 Maret 2023
Kelas : RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

Praktikum Keamanan Informasi 1

Snort & Firewall Rules

I. Tujuan

- Mendeteksi penyalahgunaan pada jaringan menggunakan *Snort*
- Melakukan *block* terhadap penyalahgunaan pada jaringan menggunakan *Firewall Rules*

II. Landasan Teori

Snort adalah sebuah software ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer. Snort dapat digunakan sebagai suatu *Network Intrusion Detection System* (NIDS) yang berskala ringan (*lightweight*), dan software ini menggunakan sistem peraturan-peraturan (*rules system*) yang relatif mudah dipelajari untuk melakukan deteksi dan pencatatan (*logging*) terhadap berbagai macam serangan terhadap jaringan komputer. Dengan membuat berbagai rules untuk mendeteksi ciri-ciri khas (*signature*) dari berbagai macam serangan, maka *Snort* dapat mendeteksi dan melakukan *logging* terhadap serangan-serangan tersebut. Software ini bersifat *opensource* berdasarkan GNU *General Public License* [GNU89], sehingga boleh digunakan dengan bebas secara gratis, dan kode sumber (*source code*) untuk Snort juga bisa didapatkan dan dimodifikasi sendiri bila perlu.

Firewall adalah sistem keamanan untuk mengelola dan memantau trafik masuk dan keluar berdasarkan aturan keamanan (*security rules*) yang sudah ditentukan. Firewall berfungsi mencegah akses yang tidak diinginkan dari atau ke dalam jaringan atau server. Salah satu jenis *firewall* adalah *iptables*. *Iptables* adalah salah satu tools firewall pada sistem operasi Linux. Fungsi *iptables* adalah mengamankan jaringan dengan melakukan penyaringan trafik pada server VPS tanpa panel. Dengan *iptables*, kita dapat mengatur lalu lintas jaringan, termasuk mengizinkan atau memblokir koneksi yang masuk, keluar, atau sekedar melewati server. *Iptables* bekerja dengan membandingkan lalu lintas jaringan dengan serangkaian aturan yang telah dibuat. Jadi, semua paket dalam lalu lintas jaringan akan dicek.

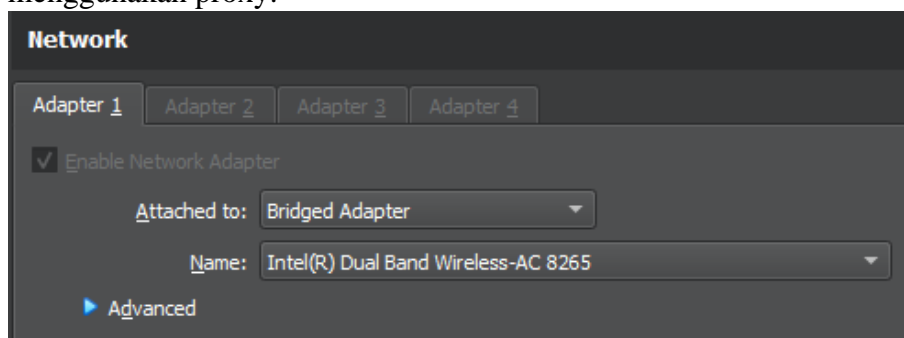
III. Alat & Bahan

- PC/Laptop
- CyberOps Workstation VM
- Koneksi internet

IV. Instruksi Kerja

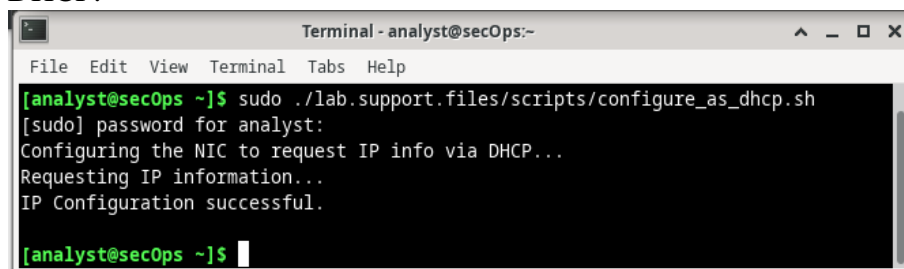
A. Mempersiapkan *Virtual Machine*

1. Jalankan VM CyberOps Workstation. Ubah mode koneksi menjadi *bridged* jika jaringan WiFi tidak menggunakan proxy atau NAT jika jaringan WiFi menggunakan proxy.

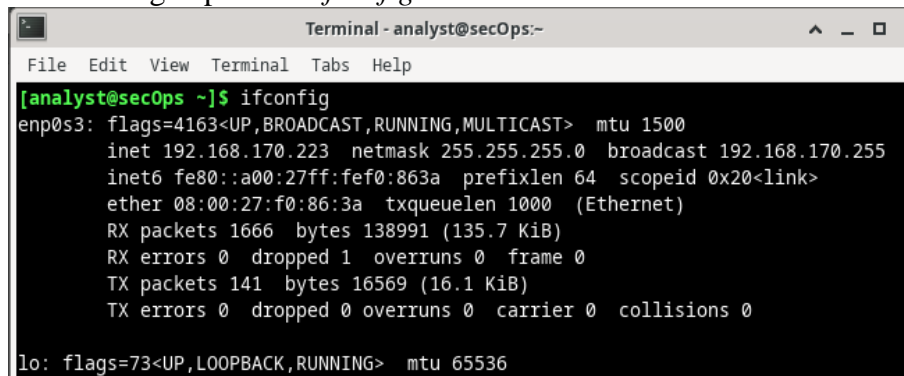


Karena menggunakan jaringan Hotspot pribadi, maka gunakan mode *Bridged Adapter*.

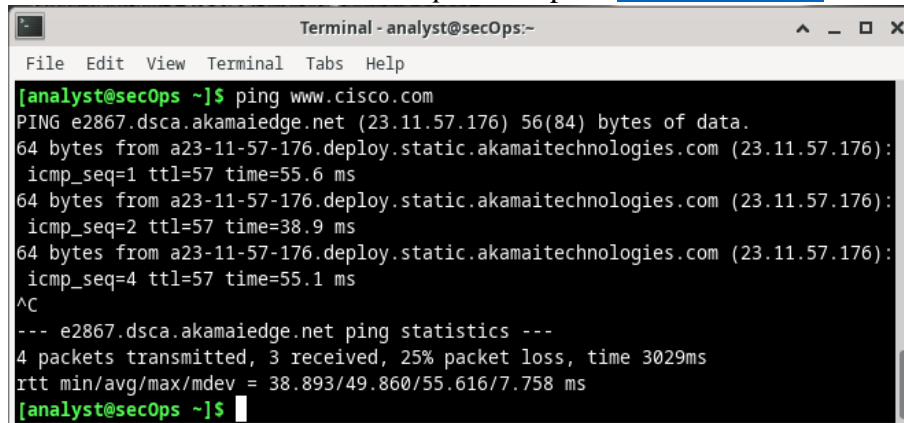
2. Konfigurasi agar mendapatkan IP secara otomatis, lakukan konfigurasi DHCP.



Cek IP dengan perintah *ifconfig*.



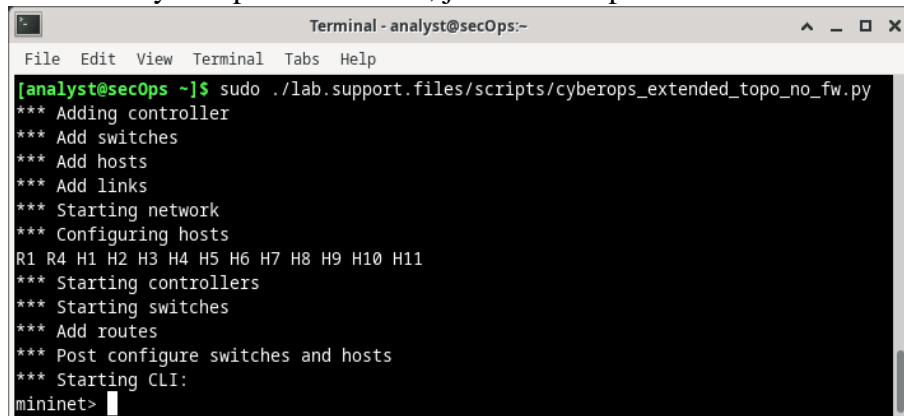
Cek koneksi PING ke *webserver public* seperti www.cisco.com.



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[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=55.6 ms  
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176):  
icmp_seq=2 ttl=57 time=38.9 ms  
64 bytes from a23-11-57-176.deploy.static.akamaitechnologies.com (23.11.57.176):  
icmp_seq=4 ttl=57 time=55.1 ms  
^C  
--- e2867.dsca.akamaiedge.net ping statistics ---  
4 packets transmitted, 3 received, 25% packet loss, time 3029ms  
rtt min/avg/max/mdev = 38.893/49.860/55.616/7.758 ms  
[analyst@secOps ~]$
```

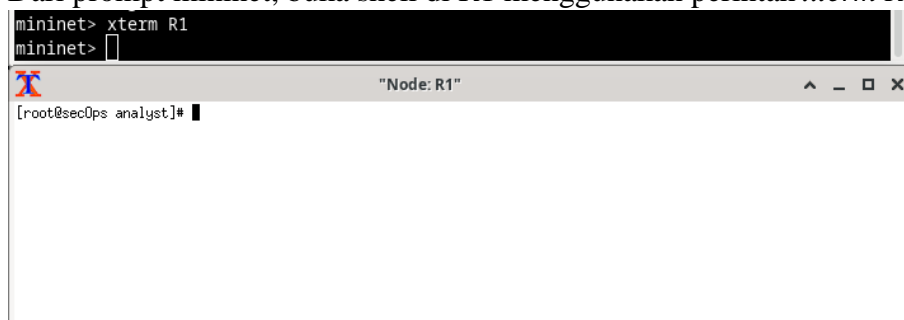
B. Firewall & IDS Logs

1. Dari VM CyberOps Workstation, jalankan skrip untuk memulai **mininet**.



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/cyberops_extended_topo_no_fw.py  
*** 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>
```

2. Dari prompt mininet, buka shell di R1 menggunakan perintah *xterm R1*

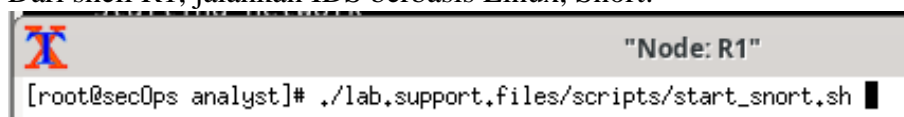


```
mininet> xterm R1  
mininet>  
"Node: R1"  
[root@secOps analyst]#
```

Maka akan muncul

Maka akan muncul jendela *Shell R1* yang masuk sebagai Super User dengan indikator *root* pada *username* yang digunakan.

3. Dari shell R1, jalankan IDS berbasis Linux, Snort.



```
"Node: R1"  
[root@secOps analyst]# ./lab.support.files/scripts/start_snort.sh
```

```
"Node: R1"

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=1279)
```

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

```
mininet> xterm H5
mininet> xterm H10
mininet> █
```

5. H10 akan mensimulasikan server di Internet yang menghosting malware. Pada H10, jalankan skrip mal_server_start.sh untuk memulai server

```
"Node: H10"
[root@secOps analyst]# ./lab.support.files/scripts/mal_server_start.sh
[root@secOps analyst]# █
```

6. 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:

```
"Node: H10"
[root@secOps analyst]# netstat -tunpa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:6666             0.0.0.0:*               LISTEN
1318/nginx: master
[root@secOps analyst]# █
```

Seperti yang terlihat pada output di atas, nginx server web ringan sedang berjalan pada koneksi pada port TCP 6666

7. Di jendela terminal R1, sebuah instance dari Snort sedang berjalan. Untuk memasukkan lebih banyak perintah di R1, buka terminal R1 lain dengan memasukkan xterm R1 lagi di jendela terminal VM CyberOps Workstation.

Anda mungkin juga ingin mengatur jendela terminal sehingga Anda dapat melihat dan berinteraksi dengan setiap perangkat..

```
mininet> xterm R1
mininet>

"Node: R1"
[root@secOps analyst]#

"Node: R1"
=====
03/20-22:21:47.482732 fe80::4802:61ff:fe4d:aaa8 -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:56
=====
03/20-22:22:55.750260 fe80::caa:93ff:feae:e98b -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:56
=====
```

8. Di tab terminal R1 baru, jalankan perintah tail dengan opsi -f untuk memantau file /var/log/snort/alert secara real-time. File ini adalah tempat snort dikonfigurasi untuk merekam peringatan.

```
"Node: R1"
[root@secOps analyst]# tail -f /var/log/snort/alert
```

9. Dari H5, gunakan perintah wget untuk mengunduh file bernama W32.Nimda.Amm.exe. Dirancang untuk mengunduh konten melalui HTTP, wget adalah alat yang hebat untuk mengunduh file dari server web langsung dari baris perintah.

```
"Node: H5"
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 22:33:55-- 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.1'

W32.Nimda.Amm.exe.1 100%[=====>] 337,00K --.-KB/s in 0.01s

2023-03-20 22:33:55 (32,5 MB/s) - 'W32.Nimda.Amm.exe.1' saved [345088/345088]

[root@secOps analyst]#

"Node: R1"
[root@secOps analyst]# tail -f /var/log/snort/alert
03/20-22:33:55.494324 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0]
{TCP} 209.165.200.235:41032 -> 209.165.202.133:6666
```

```

***A***F Seq: 0x3469EFD2 Ack: 0x55567E55 Win: 0x55 TcpLen: 32
TCP Options (3) => NOP NOP TS: 2182331305 127748973
=====

03/20-22:33:55.520026 209.165.200.235:41032 -> 209.165.202.133:6666
TCP TTL:63 TOS:0x0 ID:65120 IpLen:20 DgmLen:52 DF
***A*** Seq: 0x55567E55 Ack: 0x3469EFD3 Win: 0x36C TcpLen: 32
TCP Options (3) => NOP NOP TS: 127748974 2182331305
=====

```

- Port yang digunakan adalah 6666 dengan indikator :6666 setelah Ip Address dari webserver
- File diunduh sepenuhnya dengan indikator 100%
- IDS memberikan peringatan dengan ditandai dengan *alert* pada jendela Node R1 yang kedua

10. Saat file berbahaya sedang transit R1, IDS, Snort, dapat memeriksa muatannya. Payload cocok dengan setidaknya satu tanda tangan yang dikonfigurasi di Snort dan memicu peringatan di jendela terminal R1 kedua (tab tempat tail -f berjalan). Entri peringatan ditunjukkan di bawah ini. Stempel waktu Anda akan berbeda:

```

[root@secOps analyst]# tail -f /var/log/snort/alert
03/20-22:33:55.494324 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0]
{TCP} 209.165.200.235:41032 -> 209.165.202.133:6666

```

- Alamat Ipv4 sumber dan tujuan yang digunakan dalam transaksi adalah 209.165.200.235 dan 209.165.202.133
- Berdasarkan Alert. Port sumber dan tujuan yang digunakan dalam transaksi adalah 41032 dan 6666
- Berdasarkan peringatan yang ditunjukkan, pengunduhan dilakukan pada tanggal 20 Maret 2023 Pukul 22:33:55
- Berdasarkan peringatan yang ditunjukkan pesan yang direkam adalah Malicious Server Hit

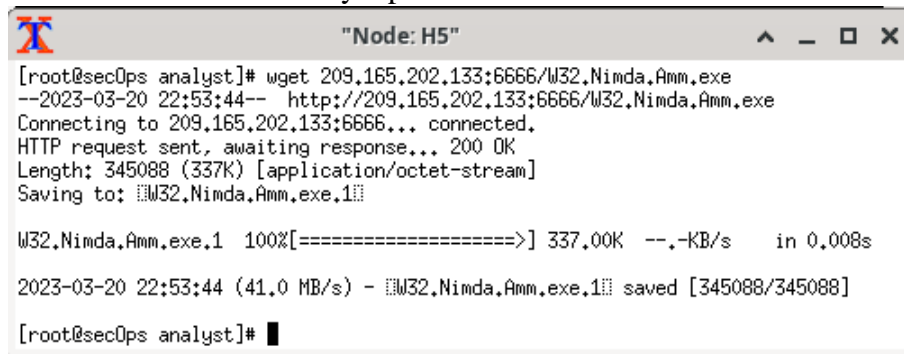
11. Pada H5, gunakan perintah tcpdump untuk merekam peristiwa dan mengunduh file malware lagi sehingga Anda dapat merekam transaksi. Keluarkan perintah berikut di bawah ini mulai pengambilan paket:

```

[root@secOps analyst]# tcpdump -i H5-eth0 -w nimda.download.pcap &
[1] 1454
[root@secOps analyst]# tcpdump; listening on H5-eth0, link-type EN10MB (Ethernet),
capture size 262144 bytes
[root@secOps analyst]#

```

12. Perintah di atas menginstruksikan tcpdump untuk menangkap paket pada antarmuka H5-eth0 dan menyimpan tangkapan ke file bernama nimda.download.pcap. Simbol & di bagian akhir memberitahu shell untuk mengeksekusi tcpdump di latar belakang. Tanpa simbol ini, tcpdump akan membuat terminal tidak dapat digunakan saat sedang berjalan. Perhatikan [1] 5633; itu menunjukkan satu proses dikirim ke latar belakang dan ID prosesnya (PID) adalah 5366. PID Anda kemungkinan besar akan berbeda.
13. Tekan ENTER beberapa kali untuk mendapatkan kembali kendali atas shell saat tcpdump berjalan di latar belakang.
14. Sekarang tcpdump menangkap paket, unduh malware lagi. Pada H5, jalankan kembali perintah atau gunakan panah atas untuk memanggilnya kembali dari fasilitas riwayat perintah.



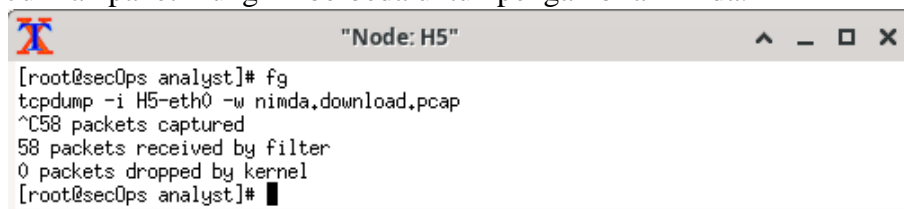
```
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 22:53:44-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345088 (337K) [application/octet-stream]
Saving to: 'W32.Nimda.Amm.exe.1'

W32.Nimda.Amm.exe.1 100%[=====>] 337,00K --.-KB/s in 0,008s

2023-03-20 22:53:44 (41,0 MB/s) - 'W32.Nimda.Amm.exe.1' saved [345088/345088]

[root@secOps analyst]#
```

15. 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
^C58 packets captured
58 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

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


```
"Node: H5"
[root@secOps analyst]# ls -l
total 1720
drwxr-xr-x 2 analyst analyst 4096 Mar 6 22:03 Desktop
drwxr-xr-x 3 analyst analyst 4096 Feb 20 20:37 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jul 15 2020 lab.support.files
-rw-r--r-- 1 root root 1400832 Mar 20 22:56 nimda.download.pcap
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe.1
[root@secOps analyst]#
```

C. Menyetel Aturan Firewall Berdasarkan IDS Alerts

1. Di VM CyberOps Workstation, mulai jendela terminal R1 ketiga.

```
mininet> xterm R1
mininet>

"Node: R1"
[root@secOps analyst]#
```

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

```
"Node: R1"
[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
```

Saat ini belum ada *chain* yang digunakan oleh R1

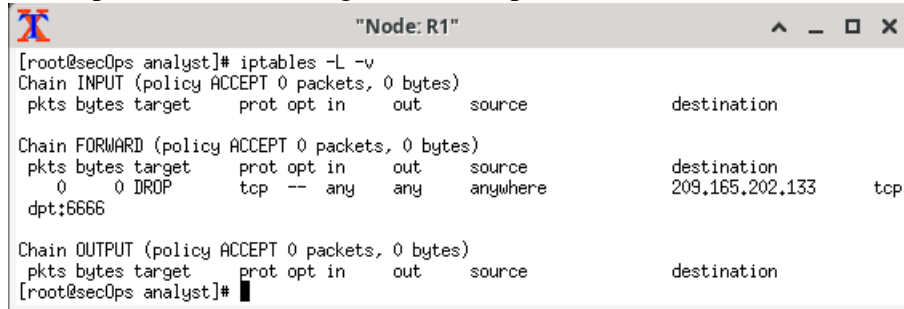
3. Koneksi ke server menghasilkan paket yang harus melintasi firewall iptables di R1. Paket yang melintasi firewall ditangani oleh aturan FORWARD dan oleh karena itu, rantai itulah yang akan menerima aturan pemblokiran. Agar komputer pengguna tidak terhubung ke server yang diidentifikasi di Langkah 1, tambahkan aturan berikut ke rantai FORWARD di R1:

```
"Node: R1"
[root@secOps analyst]# iptables -I FORWARD -p tcp -d 209.165.202.133 --dport 6666 -j DROP
[root@secOps analyst]#
```

Di mana:

- a) -I FORWARD: menyisipkan aturan baru dalam rantai FORWARD.
- b) -p tcp: menentukan protokol TCP.
- c) -d 209.165.202.133: menentukan tujuan paket
- d) --dport 6666: menentukan port tujuan
- e) -j DROP: atur aksi ke drop.

4. Gunakan perintah iptables lagi untuk memastikan aturan telah ditambahkan ke rantai FORWARD. VM CyberOps Workstation mungkin memerlukan beberapa detik untuk menghasilkan output:

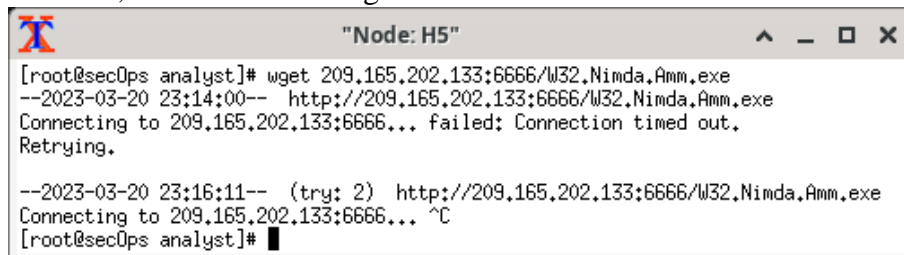


```
[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination

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
[root@secOps analyst]#
```

5. Pada H5, coba unduh file lagi:

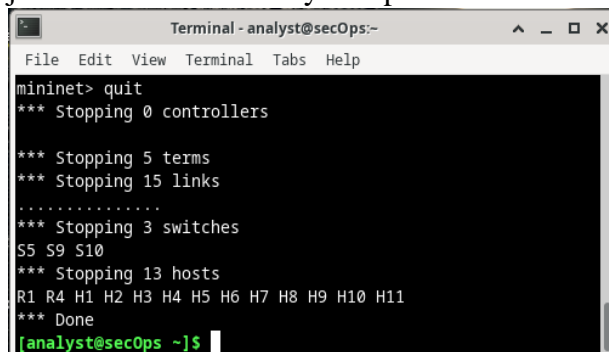


```
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 23:14:00-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... failed: Connection timed out.
Retrying.

--2023-03-20 23:16:11-- (try: 2) http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... ^C
[root@secOps analyst]#
```

- Unduhan tidak berhasil karena terdapat *firewall* yang akan melakukan *DROP* paket yang telah ditentukan, dalam hal ini adalah paket dengan tujuan ke 209.165.202.133 dengan port 6666.
- Kita dapat melakukan *block* terhadap IP Server tujuan. Hal ini dapat sepenuhnya memotong akses ke server tujuan dari jaringan internal, sehingga kita tidak perlu menentukan IP, Port, maupun protokol dalam sebuah server.

6. Hentikan proses *mininet* dengan mengarahkan ke terminal yang digunakan untuk memulai Mininet. Hentikan Mininet dengan memasukkan quit di jendela terminal VM CyberOps utama.



```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
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
[analyst@secOps ~]$
```

7. 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/n
ull
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs 2> /de
v/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 '([a-z0-9:]+)-eth[0-9]+'
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.
[analyst@secOps ~]$
```

V. Pembahasan

Pada praktikum ini, mahasiswa akan melakukan pengamatan terhadap aktivitas dalam suatu jaringan komputer menggunakan IDS berbasis linux (*snort*). Dalam praktikum ini, terdapat tools emulator jaringan komputer yaitu mininet. Ketika mininet dijalankan, kita dapat membuat suatu simulasi jaringan komputer lengkap berisi switch, router, dan host yang realistis serta dapat berinteraksi dengan real kernel dan program lainnya.

Dalam praktikum ini terdapat beberapa *node* yang digunakan, diantaranya adalah R1, H5, dan H10. R1 diatur sebagai router yang menjalankan *snort* serta *Firewall*, H10 digunakan sebagai *webserver*, dan H5 digunakan sebagai host yang akan menjadi *client* dari *webserver*. Dalam *webserver*, terdapat file berbahaya bernama W32.Nimda.Amm.exe. Ketika *host* H5 melakukan pengunduhan terhadap file tersebut, maka *snort* pada R1 akan memeriksa muatan dalam paket yang diunduh. Adanya *payload* cocok dengan setidaknya satu *signature* memicu *alert* pada R1. *Alert* yang ditampilkan dari hasil praktikum adalah berupa *signature Malicious Server Hit* dengan alamat sumbernya yaitu 209.165.200.235 dengan port 41032 serta alamat tujuannya yaitu 209.165.202.133 dengan port 6666. Dari *alert* tersebut ditampilkan juga waktu pengunduhan file tersebut, yaitu tanggal 20 Maret 2023 pukul 22:33:55.

Untuk pencegahan terhadap ancaman berikutnya dapat dilakukan dengan membuat aturan *Firewall* sesuai dengan IDS *alert*. Caranya adalah membuat aturan *firewall* yang akan melakukan DROP paket yang melewati router ke suatu jaringan

luar yang telah terindikasi berbahaya, dalam hal ini adalah sumber dari file W32.Nimda.Amm.exe. *Chain* yang digunakan adalah *Forward* dengan IP, port, serta protokol yang sebelumnya telah terdeteksi pada R1. Untuk mencegah terdapat file berbahaya lain dalam server tersebut, kita dapat juga melakukan pendekatan yang lebih agresif dan valid dengan melakukan *block* terhadap IP Server tujuan tanpa menentukan IP, Port, serta protokol yang digunakan. Dengan hal tersebut, akses ke server tujuan akan sepenuhnya terpotong, sehingga host tidak akan dapat mengakses semua hal yang ada pada server yang telah di *block*.

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

1. IDS akan memberikan peringatan jika setidaknya terdapat 1 *signature* yang cocok dengan *payload*.
2. Untuk pencegahan, kita dapat menetapkan aturan *firewall* sesuai dengan peringatan yang telah didapatkan sebelumnya.
3. Untuk mencegah file berbahaya lain diunduh dari server yang telah terindikasi terdapat file berbahaya, kita dapat melakukan *block* terhadap IP Server tujuan secara penuh tanpa menentukan spesifikasi IP, Port, serta protokol yang digunakan.
4. Pemblokiran terhadap IP Server akan memotong sepenuhnya jalur ke server tujuan.

VII. Daftar Pustaka

- Gaffari, D. (January 19, 2015). Apa Itu Snort???. Retrieved March 22, 2022, from <https://tangankecill.wordpress.com/2015/01/19/apa-itu-snort/>
- Triyadi. (April 25, 2019). Apa itu Firewall? Pengertian, Fungsi dan Cara Kerja. Retrieved March 23, 2022, from <https://www.rumahweb.com/journal/apa-itu-firewall/#:~:text=Firewall%20adalah%20sistem%20keamanan%20untuk,k%20dalam%20jaringan%20atau%20server.>
- Regita, N. (October 19, 2021). Iptables: Pengertian, Fungsi dan Cara Menggunakannya. Retrieved March 23, 2022, from [https://www.niagahoster.co.id/blog/tutorial-iptables/#Apa Itu Iptables](https://www.niagahoster.co.id/blog/tutorial-iptables/#Apa%20Itu%20Iptables)