

LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1

PERTEMUAN 6

Snort & Firewall Rule



DISUSUN OLEH

Nama : Muhamad Alan Dharma Saputro S
NIM : 21/481348/SV/19761
Hari, Tanggal : Selasa, 21 Maret 2023
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Kelas : RI4AA

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

A. Tujuan

1. Mempersiapkan Lingkungan Virtual
2. Firewall dan Log IDS
3. Hentikan dan Hapus Proses Mininet

B. Latar Belakang

Snort dan SGUIL

Snort adalah IDS yang bergantung pada aturan yang telah ditentukan sebelumnya untuk semua kejadian yang berbahaya. Snort melihat ke semua bagian dari paket jaringan (header dan payload), mencari pola yang ditentukan dalam aturannya. Saat Snort mengambil tindakan yang ditentukan dalam aturan yang sama.

SGUIL menyediakan antarmuka grafis untuk log dan peringatan Snort, memungkinkan analisis keamanan untuk beralih dari SGUIL ke alat lain untuk informasi lebih lanjut. Misalnya, jika paket yang berpotensi berbahaya dikirim ke server web dan Snort memunculkan peringatan, SGUIL akan peringatan itu. Analis kemudian dapat mengklik kanan peringatan itu untuk mencari database ELSA atau Bro untuk pemahaman yang lebih baik tentang acara tersebut

Firewall rule (aturan firewall) merupakan instruksi yang mengontrol bagaimana perangkat firewall menangani lalu lintas masuk dan keluar. Aturan ini merupakan mekanisme control akses yang menegakkan keamanan dalam jaringan dengan memblokir atau mengizinkan komunikasi berdasarkan kriteria yang telah ditentukan.

Firewall mengevaluasi setiap paket data yang masuk dan keluar terhadap aturan firewall. Jika paket cocok dengan salah satu aturan, firewall mengizinkan paket tersebut untuk melintas ke tujuannya. Jika tidak, firewall akan menolak dan melaporkannya. Aturan firewall dikonfigurasi sebagai Access Control Lists (ACL), yang merupakan daftar urutan izin yang mendefinisikan lalu lintas yang diizinkan atau ditolak. ACL yang umum mencakup tindakan (mengizinkan, menolak, atau menolak) diikuti dengan kondisi atau parameter yang harus dipenuhi lalu lintas sebelum tindakan diterapkan.

C. Alat dan Bahan

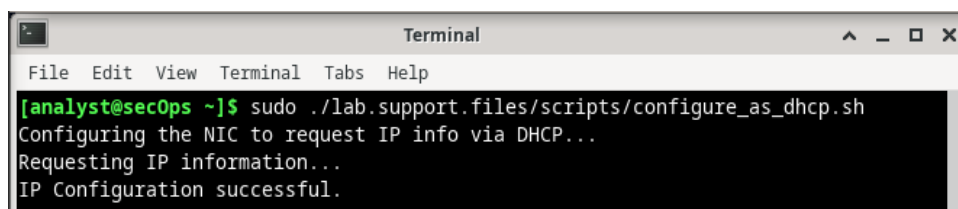
- Access Internet
- Mesin Virtual CyberOps Workstation

D. Intruksi Kerja

Bagian 1 : Mempersiapkan Lingkungan Virtual

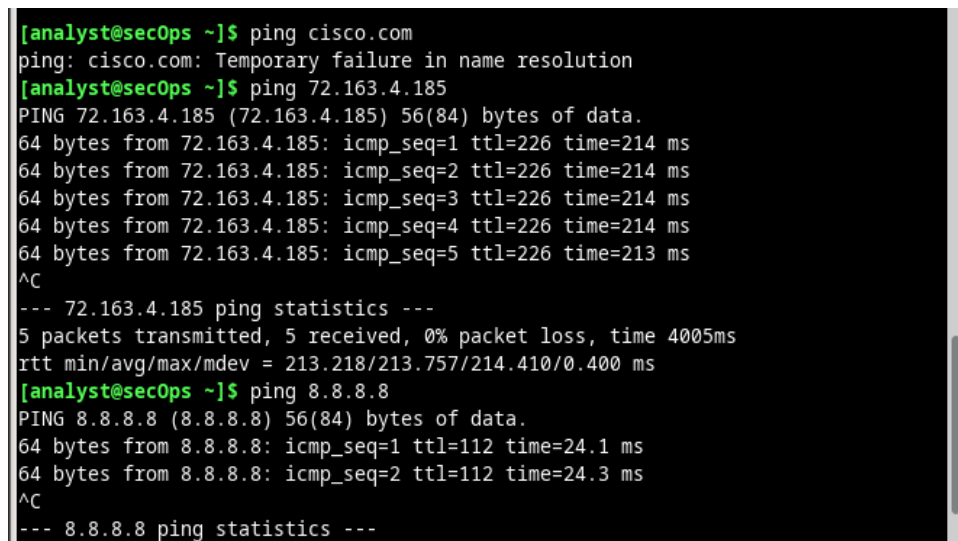
1. Luncurkan Oracle VirtualBox dan ubah CyberOps Workstation untuk mode Bridged, jika perlu. Pilih Mesin > Pengaturan > Jaringan. Di bawah Attached To, pilih Bridged Adapter (atau jika Anda menggunakan WiFi dengan proxy, Anda mungkin memerlukan adaptor NAT) dan klik OK.
2. Luncurkan VM CyberOps Workstation, buka terminal dan konfigurasi jaringannya dengan menjalankan skrip `configure_as_dhcp.sh`.

Karena skrip memerlukan hak pengguna super, berikan kata sandi untuk user analyst.



```
Terminal
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/configure_as_dhcp.sh
Configuring the NIC to request IP info via DHCP...
Requesting IP information...
IP Configuration successful.
```

3. 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 ~]$ ping cisco.com
ping: cisco.com: Temporary failure in name resolution
[analyst@secOps ~]$ ping 72.163.4.185
PING 72.163.4.185 (72.163.4.185) 56(84) bytes of data.
64 bytes from 72.163.4.185: icmp_seq=1 ttl=226 time=214 ms
64 bytes from 72.163.4.185: icmp_seq=2 ttl=226 time=214 ms
64 bytes from 72.163.4.185: icmp_seq=3 ttl=226 time=214 ms
64 bytes from 72.163.4.185: icmp_seq=4 ttl=226 time=214 ms
64 bytes from 72.163.4.185: icmp_seq=5 ttl=226 time=213 ms
^C
--- 72.163.4.185 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 213.218/213.757/214.410/0.400 ms
[analyst@secOps ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=24.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=24.3 ms
^C
--- 8.8.8.8 ping statistics ---
```

Bagian 2 : Firewall dan IDS Logs

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

```
[analyst@sec0ps ~]$ sudo ./lab.support.files/scripts/cyberops_extended_topo_no_f
w.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 di bawah ini:



The screenshot shows a terminal window with the following text:

```

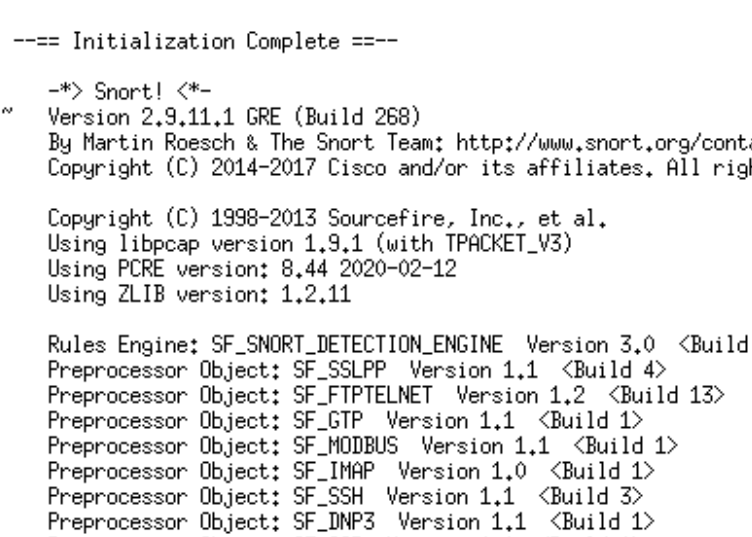
*** Add links
*** Starting network
*** Configuring hosts
R1 R4 H1 H2 H3 H4 H5 H6 H7
*** Starting controllers
*** Starting switches
*** Add routes
*** Post configure switch
*** Starting CLI:
mininet> xterm R1
mininet>

```

Overlaid on the terminal is a window titled "Node: R1" with a terminal icon. The prompt in this window is `[root@sec0ps analyst]#`.

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

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



```

Node: R1

--- Initialization Complete ---

--*) 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>

```

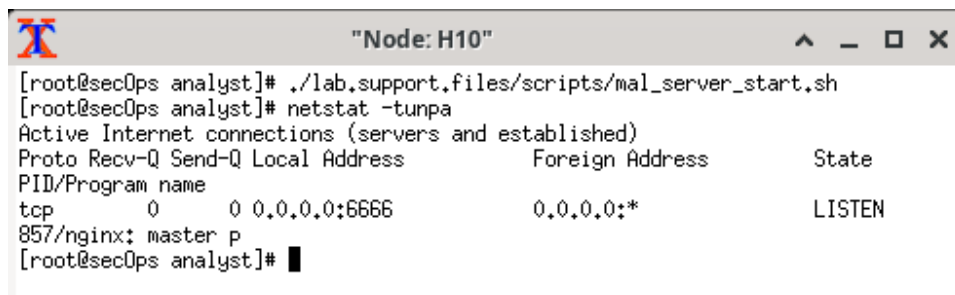
4. Dari prompt mininet CyberOps Workstation VM, buka shell untuk host H5 dan H10.

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



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

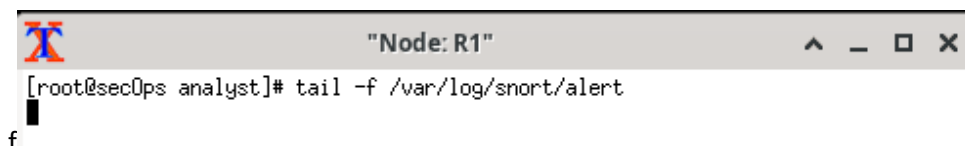
6. Pada H10, gunakan `netstat` dengan opsi `-tunpa` untuk memverifikasi bahwa server web sedang berjalan. Saat digunakan seperti yang ditunjukkan di bawah ini, `netstat` mencantumkan semua port yang saat ini ditetapkan ke layanan:



```
[root@secOps analyst]# ./lab.support.files/scripts/mal_server_start.sh
[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
857/nginx: master p
[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.
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.



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

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 21:53:55-- 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 21:53:55 (28.9 MB/s) - 'W32.Nimda.Amm.exe.1' saved [345088/345088]

[root@secOps analyst]#
```

Port apa yang digunakan saat berkomunikasi dengan server web malware?

Apa indikatornya?

Apakah file telah diunduh sepenuhnya?

Apakah IDS menghasilkan peringatan yang terkait dengan unduhan file?

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:

```
"Node: R1"
[root@secOps analyst]# tail -f /var/log/snort/alert
03/20-21:53:55.322150  [**] [1:1000003:0] Malicious Server Hit! [**] [Priority:
0] {TCP} 209.165.200.235:42528 -> 209.165.202.133:6666
```

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

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

Berdasarkan peringatan yang ditunjukkan di atas, kapan pengunduhan dilakukan?

Berdasarkan peringatan yang ditunjukkan di atas, apa pesan yang direkam IDS signature?

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:

```
"Node: H5"
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 21:53:55-- 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 21:53:55 (28.9 MB/s) - 'W32.Nimda.Amm.exe.1' saved [345088/345088]

[root@secOps analyst]# tcpdump -i H5-eth0 -w nimda.download.pcap &
[1] 890
[root@secOps analyst]# tcpdump: listening on H5-eth0, link-type EN10MB (Ethernet
), capture size 262144 bytes
```

11. Perintah di atas menginstruksikan tcpdump untuk menangkap paket pada antarmuka H5-eth0 dan menyimpan tangkapan ke file bernama nimda.download.pcap.
12. Tekan ENTER beberapa kali untuk mendapatkan kembali kendali atas shell saat tcpdump berjalan di latar belakang.
13. Sekarang tcpdump menangkap paket, unduh malware lagi. Pada H5, jalankan kembali perintah atau gunakan panah atas untuk memanggilnya kembali dari fasilitas riwayat perintah.

```
"Node: H5"
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 21:53:55 (28.9 MB/s) - 'W32.Nimda.Amm.exe.1' saved [345088/345088]

[root@secOps analyst]# tcpdump -i H5-eth0 -w nimda.download.pcap &
[1] 890
[root@secOps analyst]# tcpdump: listening on H5-eth0, link-type EN10MB (Ethernet
), capture size 262144 bytes

[root@secOps analyst]#
[root@secOps analyst]#
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 21:56:57-- 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 21:56:57 (25.4 MB/s) - 'W32.Nimda.Amm.exe.2' saved [345088/345088]

[root@secOps analyst]#
```

14. 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.

```
"Node: H5"
[root@secOps analyst]# fg
tcpdump -i H5-eth0 -w nimda.download.pcap
^C52 packets captured
52 packets received by filter
0 packets dropped by kernel
```

15. 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 11132
drwxr-xr-x 2 analyst analyst 4096 Mar 13 21:30 Desktop
drwxr-xr-x 4 analyst analyst 4096 Mar 6 21:50 Downloads
-rw-r--r-- 1 root root 183149 Feb 20 21:23 httpdump.pcap
-rw-r--r-- 1 root root 9801728 Feb 20 21:32 httpsdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Jul 15 2020 lab.support.files
-rw-r--r-- 1 root root 349718 Mar 20 21:59 nimda.download.pcap
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Mar 13 21:46 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
[root@secOps analyst]#
```

Bagaimana file PCAP ini berguna bagi analis keamanan?

Bagian 3 : Menyetel Aturan Berdasarkan IDS Alerts

1. Di VM CyberOps Workstation, mulai jendela terminal R1 ketiga.
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
[root@secOps analyst]#
```

Rantai apa yang saat ini 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:


```
Try 'iptables -h' or 'iptables --help' for more information.
[root@secOps analyst]# iptables -I FORWARD -p tcp -d 209.165.202.133 --dport 66
66 -j DROP
```

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

```
Try 'iptables -h' or 'iptables --help' for more information.
[root@secOps analyst]# iptables -I FORWARD -p tcp -d 209.165.202.133 --dport 66
66 -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

[root@secOps analyst]#
```

- Pada H5, coba unduh file lagi:

```
-rw-r--r-- 1 root    root      349718 Mar 20 21:59 nimda.download.pcap
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst    345088 Mar 13 21:46 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
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 22:06:27-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... ^C
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2023-03-20 22:07:10-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... █
```

Apakah unduhan berhasil kali ini? jelaskan.

Apa pendekatan yang lebih agresif tetapi juga valid saat memblokir server yang melanggar?

- Hentikan dan Hapus Proses Mininet. Arahkan ke terminal yang digunakan untuk memulai Mininet. Hentikan Mininet dengan memasukkan quit di jendela terminal VM CyberOps utama.

```
Terminal
File Edit View Terminal Tabs Help
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> xterm H5
mininet> xterm H10
mininet> xterm R1
mininet> xterm R1
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.

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

E. Pembahasan

Pada praktikum pertemuan ini melakukan pengamatan pada aktifitas jaringan komputer yang bertujuan untuk memahami firewall rule dan IDS Signature menggunakan linux (snort). Dengan menggunakan snort dapat melihat semua bagian dari paket jaringan dan mencari pola yang ditentukan. Peringatan jaringan yang dihasilkan oleh berbagai jenis perangkat antara lain peralatan keamanan, firewall, perangkat IPS, router, switch, server. Tool yang digunakan yaitu menggunakan VM CyberOps Workstation.

Pertama buka terminal dan konfigurasi jaringan dengan menjalankan perintah **sudo ./lab.support.files/scripts/configure_as_dhcp.sh** yang berfungsi untuk konfigurasi jaringan agar mendapatkan IP dhcp. Untuk mengeceknya dapat menggunakan website cisco, namun jika langsung ping pada websitenya tidak bisa maka gunakan IP website tersebut yaitu **72.163.4.185**. Selanjutnya memonitoring lalu lintas jaringan pada firewall, dengan mencocokkan lalu lintas masuk dengan aturan administrative menggunakan IDS. IDS ini mampu memberikan peringatan kepada administrator apabila terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.

Jalankan perintah untuk memulai mininet yaitu **sudo ./lab.support.files/scripts/cyberops_extended_topo_no_fw.py**, terdapat beberapa node yang digunakan antara lain 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. Perintah **./lab.support.files/scripts/mal_server_start.sh** digunakan untuk memulai server pada H10. Perintah **netstat -tunpa** berfungsi untuk melihat semua port yang digunakan layanan server tersebut. Pada H5 gunakan perintah **wget** untuk mengunduh file bernama **W32.Nimda.Amm.exe** yang merupakan malware, lalu terminal akan memeriksa muatan dalam paket tersebut engan menggunakan perintah **tcdump**.

Lalu lintas yang memasuki firewall dan ditujukan ke perangkat firewall itu sendiri ditangani oleh rantai INPUT. Contoh lalu lintas ini adalah paket ping yang datang dari perangkat lain di jaringan apa pun dan dikirim ke salah satu antarmuka firewall. Lalu lintas yang berasal dari perangkat firewall itu sendiri dan ditujukan ke tempat lain, ditangani oleh rantai OUTPUT. Contoh lalu lintas ini adalah respons ping yang dihasilkan oleh perangkat firewall itu sendiri. Lalu lintas berasal dari tempat lain

dan melewati perangkat firewall ditangani oleh rantai FORWARD. Contoh lalu lintas ini adalah paket yang dirutekan oleh firewall.

Setiap rantai dapat memiliki seperangkat aturan independennya sendiri yang menentukan bagaimana lalu lintas akan difilter untuk rantai tersebut. Sebuah rantai dapat memiliki hampir sejumlah aturan, termasuk tidak ada aturan sama sekali. **Chain** yang digunakan adalah Forward dengan **IP, port, dan protokol** yang sebelumnya diidentifikasi pada R1. Untuk dapat memblokir file jahat lainnya di server menggunakan pendekatan yang lebih agresif dan valid dengan memblokir server IP target tanpa menentukan alamat IP, port, dan protokol. Ini sepenuhnya memutus akses ke server target, sehingga host tidak dapat mengakses apa pun di server yang diblokir.

F. Kesimpulan

Kesimpulan yang didapatkan dari praktikum kali ini yaitu:

1. Dengan menggunakan snort dapat melihat semua bagian dari paket jaringan dan mencari pola yang ditentukan.
2. IDS mampu memberikan peringatan kepada administrator apabila terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.
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 protocol yang digunakan.

G. Daftar Pustaka

- Abdullahi, A. (2023) What are firewall rules? definition, types & best practices, Enterprise Networking Planet. Available at: <https://www.enterprisenetworkingplanet.com/security/firewall-rules/#:~:text=Firewall%20rules%20are%20instructions%20that,communication%20based%20on%20predetermined%20criteria>. (Accessed: March 24, 2023).
- Huda, N. (2022) APA ITU Intrusion Detection System (IDS)? Jenis Dan Cara Kerjanya, Blog Dewaweb. Available at: <https://www.dewaweb.com/blog/ids-adalah/> (Accessed: March 27, 2023).
- Gaffari, D. (2018) APA ITU Snort ???, corat_coret. Available at: <https://tangankecill.wordpress.com/2015/01/19/apa-itu-snort/> (Accessed: March 27, 2023).