Configuring an Intrusion Detection System

(CompTIA Security + SY – 601)

Objectives:

- To use an IDS sensor to monitor packets on a LAN router's interface with the outside internetwork
- To use the Security Onion Linux distribution and its bundled Snort IDS as the sensor

Resources:

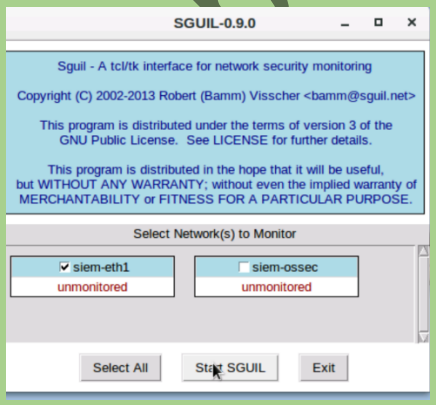
- Kali Virtual Machine (PT1-Kali)
- SIEM1 Virtual Machine
- Windows Virtual Machine (MS1)
- Security Online Linux

Instructions:

Browse IDS tool

- Log-in to SIEM1 VM
- Open **Sguil** icon on the desktop and log on with the credentials *siem* for the username and **Pa$$w0rd**

- Check the siem1-eth1 interface check box (make sure that only siem1- eth1is checked) then select Start SGUIL



- Select the PT1-Kali VM and log-in

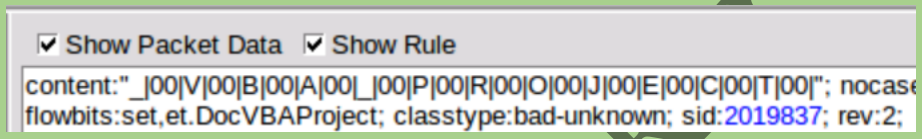
- Open a terminal and run ping 10.1.0.1 -c10

```
root@KALI:~# ping 10.1.0.1 -c10
PING 10.1.0.1 (10.1.0.1) 56(84) bytes of data.
64 bytes from 10.1.0.1: icmp_seq=1 ttl=125 time=2.29 ms
64 bytes from 10.1.0.1: icmp_seq=2 ttl=125 time=1.23 ms
64 bytes from 10.1.0.1: icmp_seq=3 ttl=125 time=1.69 ms
64 bytes from 10.1.0.1: icmp_seq=4 ttl=125 time=2.11 ms
64 bytes from 10.1.0.1: icmp_seq=5 ttl=125 time=1.57 ms
64 bytes from 10.1.0.1: icmp_seq=6 ttl=125 time=1.48 ms
64 bytes from 10.1.0.1: icmp_seq=7 ttl=125 time=1.91 ms
64 bytes from 10.1.0.1: icmp_seq=8 ttl=125 time=1.49 ms
64 bytes from 10.1.0.1: icmp_seq=9 ttl=125 time=1.60 ms
64 bytes from 10.1.0.1: icmp_seq=10 ttl=125 time=1.77 ms
```

- Switch to the **SIEM1 VM**
- The probes will be shown as new "GPL ICMP_INFO" record in the console. Note the CNT field. This shows that the rule was matched 10 times. Select the record

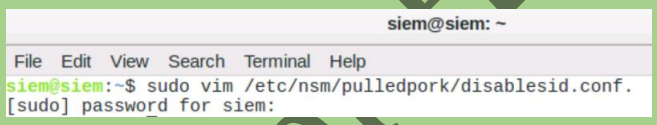
em-eth1-1	3.90	2020-03-16 13:58:13	10.246.50.2	43616	10.246.50.6	80	6	ET WEB_SERVER Possible
em-eth1-1	3.91	2020-03-16 13:58:13	10.246.50.2	43616	10.246.50.6	80	6	ET WEB_SERVER Possible
em-eth1-1	3.92	2020-03-16 13:58:13	10.246.50.6		10.246.50.2		1	GPL ICMP_INFO PING *NIX
em-eth1-1	3.95	2020-03-16 14:00:03	94.138.202.230	80	10.7.9.101	49229	6	ET WEB_CLIENT SUSPICI..

- In the panel in the bottom-right, check the **Show Packet Data** and **Show Rule** check boxes to show the packet contents and the rule that produces a signature match for this event. Record the rule SID (it appears in blue)



Configure IDS

- In the SIEM VM, minimize SGUIL and then right-click the desktop and select Open Terminal



- Run: **sudo vim/etc/nsm/pulledpork/disablesid.conf.** Enter Pa$$w0rd when prompted
- Type: **1:2100366**, using the value for the SID you recorded earlier
- Press **ESC** to exit Vim's Insert Mode
- Type **:wq** to save the close the file
- Run: **sudo rule-update** to apply the change (wait for the update to complete before moving to the next step)

```
siem@siem:~$ sudo rule-update
Wed Jul 24 13:03:15 UTC 2024
Backing up current local_rules.xml file.
Cleaning up local_rules.xml backup files older than 30 days.
Backing up current downloaded.rules file before it gets overwritten.
Cleaning up downloaded.rules backup files older than 30 days.
Backing up current local.rules file before it gets overwritten.
Cleaning up local.rules backup files older than 30 days.
LOCAL_NIDS_RULE_TUNING is enabled.
This will cause PulledPork to use the existing rules in /opt/emergingthreats/
instead of downloading new rules from the Internet.
If you want PulledPork to download new rules from the Internet,
```

- Switch to PT1-Kali VM and run **ping 10.1.0.1 -c4**

```
root@KALI:~# ping 10.1.0.1 -c4
PING 10.1.0.1 (10.1.0.1) 56(84) bytes of data.
64 bytes from 10.1.0.1: icmp_seq=1 ttl=125 time=1.43 ms
64 bytes from 10.1.0.1: icmp_seq=2 ttl=125 time=2.32 ms
64 bytes from 10.1.0.1: icmp_seq=3 ttl=125 time=2.91 ms
64 bytes from 10.1.0.1: icmp_seq=4 ttl=125 time=2.28 ms
```

- On SIEM, check the SGUIL console. Examine the CNT field-no alert should be generated and should remain at 10

ST	...	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event M
RT	6	siem-eth1-1	3.149	2020-03-16 14:00:03	10.7.9.101	49231	24.121.176.48	443	6	ET POL
RT	5	siem-eth1-1	3.32	2020-03-16 13:57:40	192.168.3.35	1032	195.2.253.92	80	6	ET USE
RT	4	siem-eth1-1	3.27	2020-03-16 13:56:51	10.42.42.253	36045	10.42.42.56	40228	17	ET SCA
RT	4	siem-eth1-1	3.31	2020-03-16 13:57:40	192.168.3.35	1032	195.2.253.92	80	6	ET TRO
RT	1	siem-eth1-1	3.19	2020-03-16 13:56:51	10.42.42.253	36020	10.42.42.56	22	6	ET SCA

Test IDS

- Select the PT1-Kali VM
- In the terminal window, run nmap 10.1.0.2 to begin a basic Nmap scan

```
root@KALI:~# nmap 10.1.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-24 06:08 PDT
Warning: File ./nmap.xsl exists, but Nmap is using /usr/bin/../share/nmap/nmap.xsl for security and consis
et NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
```

- Switch to the SIEM1 and view the alerts in Sguil
- On the PT1-Kali VM, run the following command in terminal: **hping3 -c 1000 -d.120 -S -w 64 -p 80 --flood --rand-source 10.1.0.2**

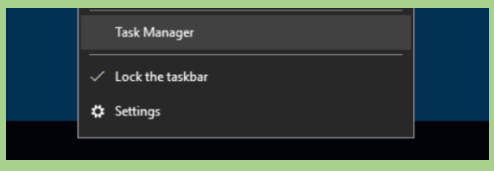
```
root@KALI:~# hping3 -c 1000 -d 120 -S -w 64 -p 80 --flood --rand-source 10.1.0.2
HPING 10.1.0.2 (eth0 10.1.0.2): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

- Let the attack proceed for a few second then press **CTRL +C** to stop it.
- Switch back to **SIEM1** and observe the rules that attack has triggered

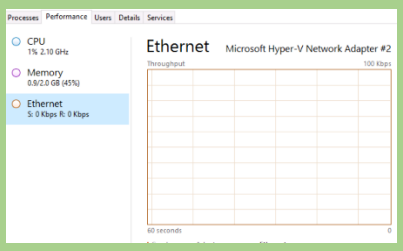
ST	...	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event M
	1	siem-eth1-1	3.279	2024-07-24 13:13:36	151.212.136.38	3655	10.1.0.2	80	6	ET DRO
	1	siem-eth1-1	3.280	2024-07-24 13:13:36	157.186.166.43	63281	10.1.0.2	80	6	ET DRO
	1	siem-eth1-1	3.281	2024-07-24 13:13:37	159.229.153.216	43652	10.1.0.2	80	6	ET DRO
	1	siem-eth1-1	3.282	2024-07-24 13:13:38	223.254.41.215	9610	10.1.0.2	80	6	ET DRO
	1	siem-eth1-1	3.283	2024-07-24 13:13:38	141.178.242.93	11617	10.1.0.2	80	6	ET DRO
	1	siem-eth1-1	3.284	2024-07-24 13:13:39	137.55.57.230	4351	10.1.0.2	80	6	ET DRO
	1	siem-eth1-1	3.285	2024-07-24 13:13:39	124.242.75.12	8485	10.1.0.2	80	6	ET DRO

Attack the MS1 Windows Server

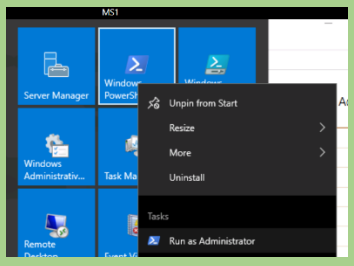
- Switch to **MS1** and sign-in
- Right-click the **Taskbar**, and select **Task Manager**



- Select the **performance** tab, and then select **Ethernet** to display network traffic (there should be a little to no traffic at the moment)



- Select **Start**, right-click **Windows Powershell** and select Run as an Administrator. Select Yes when prompted



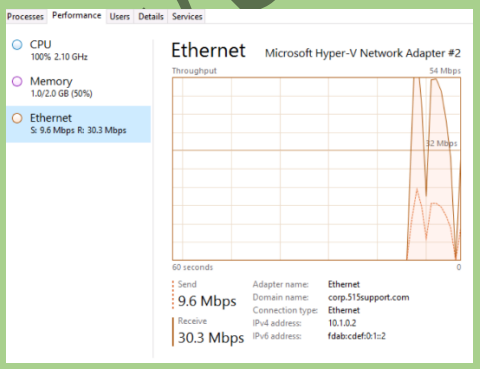
- Run: **netstat** command. You should see very few connections

```
PS C:\Windows\system32> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
```

- Organize the windows so that Task Manager is on top, with the network performance information displayed
- Switch to the **PT1-Kali** VM , and re-run the **hping3 DDos** attack

```
root@KALI:~# hping3 -c 1000 -d 120 -S -w 64 -p 80 --flood --rand-source 10.1.0.2
HPING 10.1.0.2 (eth0 10.1.0.2): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

- While the attack is running, switch to MS1, and view the network traffic in the Task Manager



- Select the Powershell window, and attempt to re-run the: **netstat** command - it may not execute during the attack

```
PS C:\Windows\system32> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
```

- Switch back to the **PT1-Kali** VM, and select Ctrl -C to halt the attack
- Switch to the **MS1** VM
- Switch to **SIEM1**, and then observe that the attack times correspond with the time you run the above commands

Observations:

- **SGUIL Configuration**: Successfully logged into SIEM1 VM, selected siem1-eth1 interface, and started SGUIL. The initial ping from PT1-Kali was detected as "GPL ICMP_INFO".
- **Rule Configuration**: Disabled the rule with SID 1:2100366 using PulledPork and verified no alerts were generated for subsequent pings.
- **Nmap Scan Detection**: Conducted a basic Nmap scan from PT1-Kali and observed alerts in SGUIL.
- **hping3 Flood Attack**: Performed a flood attack from PT1-Kali and noted the triggered alerts in SIEM1.
- **MS1 Windows Server Attack**: Observed minimal network traffic initially, increased traffic during the hping3 DDoS attack, and noted difficulty in running the netstat command during the attack.

Results:

- The IDS effectively detected and logged various types of network activities, including ICMP pings, Nmap scans, and flood attacks.
- Disabling specific IDS rules (using PulledPork) successfully prevented alerts for defined traffic patterns.
- During the DDoS attack, significant network traffic was observed on the MS1 Windows server, demonstrating the impact of the attack.

Conclusion:

The lab successfully demonstrated the configuration and effectiveness of an Intrusion Detection System (IDS) using the Security Onion Linux distribution and Snort IDS. The system accurately detected and reported different network activities and attacks, confirming its utility in monitoring and safeguarding network environments.

Future Work:

- **Automated Response**: Implement automated response mechanisms to mitigate detected threats in real-time.
- **Advanced Rule Configuration**: Develop more advanced and specific rules to detect sophisticated attack patterns.
- **Performance Optimization**: Optimize IDS performance to handle high-traffic scenarios more efficiently.
- **Integration with Other Security Tools**: Explore the integration of IDS with other security tools like firewalls and antivirus software for a comprehensive security solution.
- **User Training**: Conduct training sessions for network administrators to effectively manage and interpret IDS alerts and logs.