LOGIX ACADEMY

Lab: SNORT

Important!

Please note that we have recently updated the VMs in the Network security section along with video instructions on how to install on Windows and MacOS systems. Please make sure that you are using the newer Kali Linux VMs that we have recently added to the Network Section. Easiest way to identify is by checking if you have the `Labs` folder on the Desktop which contains `main_script.sh` then you are on the right VM.

Purpose

In this lab, we are going to demonstrate how SNORT, one of the most popular IDS/IPS can help us detect malicious traffic and generate alerts which are then helpful for security professionals.

Pre-Requisite:

Before you can start the lab, you need to run the lab script which will setup everything. Open the **Labs** folder on Desktop then right-click and "Open Terminal Here". Or open a terminal and cd to Desktop/Labs folder, then issue the command:

```
sudo ./main_script.sh
```

Select **SNORT IDS Lab** option from the lab menu.

The you will see the following options:

```
═══════════════════════════════
  Snort Lab Setup Script
═══════════════════════════════
1. Start everything from scratch (overwrite rules, pick this option if first time)
2. Reset everything except rules (pick if you have added your own rules)
Please choose an option (1 or 2):
```

Enter 1 as choice.

Step 1: *Check if existing rule for alerting on nmap scan of port 21 is working*

We first need to check if the FTP scan alert rule that comes with the lab is indeed working.
Open a **new** tab of terminal, and run the following command which is basically kali Linux doing a port 21 scan of the vulnerable nginx web container:

```
nmap -p 21 172.17.0.2
```

You should see the following alert in the other tab (after a few seconds):

```
05/27-05:36:04.019065 [**] [1:1000003:0] "NMAP Scan to FTP(21) Port Detected" [**] [Priority: 0
] {TCP} 172.17.0.1:34454 → 172.17.0.2:21
```

Step 2: *Add a new rule to detect ping sweep and generate alert*

Open a new terminal tab, then run the following command:

```
sudo vi /etc/snort/rules/local.rules
```

Go to the new line at the end of current rule, then press **i**

Then please type the rule:

```
alert icmp any any -> 172.17.0.2 any (msg: "Ping sweep detected"; sid:1000004;)
```

press Escape key then **:wq** and press enter.

Run the following command and see if the output shows the rules correctly:

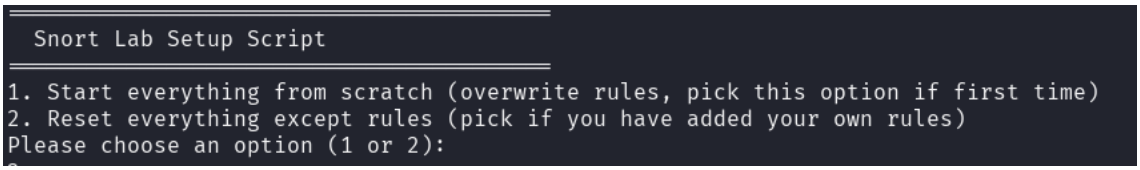
```
sudo cat /etc/snort/rules/local.rules
```

Close the old snort tab. Open a new tab and now please re-launch the lab but this time we will go with option 2 within snort lab options (remember within SNORT lab there are two options).

```
sudo ./main_script.sh
```

Select **SNORT IDS Lab** option from the lab menu.

The you will see the following options:

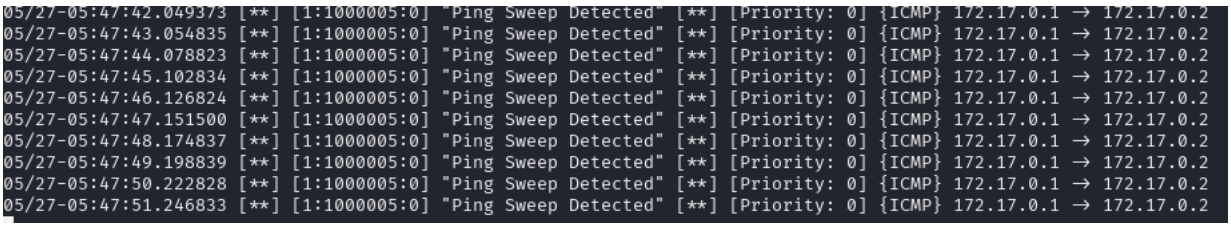


Enter 2 as choice (because we don't the script to overwrite the rule that we just added)

Now check if your alert is working or not by opening a new terminal tab and issuing:

```
ping 172.17.0.2
```

You should see the following alert:



Press Ctrl + C to stop the ping.

LOGIX ACADEMY

Challenge

Note: For the following, you need to follow the same steps as at the start of the lab for editing, saving the file and then relaunching the lab but with option 2 in the second step.

It is recommended to complete both the rules in one go then relaunch the lab.

1. Write a rule that:
    - Will alert on a nmap port scan of SSH (port 22) of the Nginx Web Server container (172.17.0.2)
    - It should display the message *ALERT: NMAP scan detected on SSH (22).*
    - You need to provide a different *Sid* in the rule (1000003 and 1000004 are used so maybe use 1000004). Note five zeros.

2. Write a rule that:
    - Will alert on the **ping reply** not the ping request, so when we do `ping 172.17.0.2` Kali Linux pings the Nginx container and we already detect that, but now we want an alert on the automatic reply that is coming from the container to Kali Linux for the same ping command. Keep in mind, for every ping request, the destination responds with a ping reply and we want an alert on that
    - It should display the message *ALERT: Ping reply detected*
    - You need to provide a unique *Sid* in the rule (e.g., use 1000005). Note five zeros.

You can check if your rules are working by issuing the following commands:

```
nmap -p 22 172.17.0.2
```

```
ping 172.17.0.2
```

(Solution in next lecture)