LOGIX ACADEMY

Lab: SNORT – Monitoring Sensitive Web Access

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

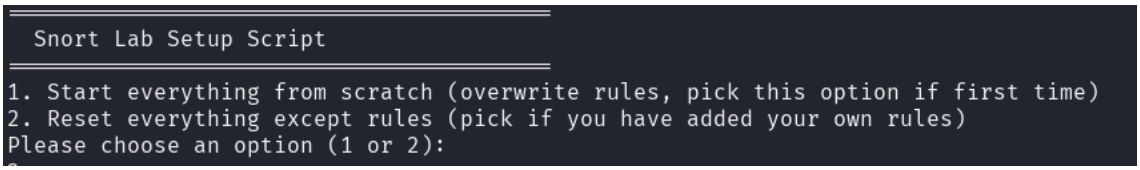
In this lab, we are going to demonstrate how SNORT, one of the most popular IDS/IPS can help us detect malicious traffic and generate alerts which are then helpful for security professionals.

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. Note that this lab is the same as the first lab, so you need to launch the same lab option. You will see the following options:



Enter 1 as choice.

Step 1: *Detect Directory Traversal Attack on /etc/passwd*

`/etc/passwd` is a well-known file on Linux systems that historically contained user account information — including hashed passwords in older systems. Some new systems store sensitive information in `/etc/shadow`, but the file `/etc/passwd` still lists usernames and is often **targeted by attackers** trying to:

- Discover user accounts
- Perform reconnaissance
- Exploit directory traversal vulnerabilities (e.g., `../../etc/passwd`)

In order to detect such an attack, we are going to use the rule:

```
alert tcp 172.17.0.1 any -> 172.17.0.2 80 (msg:"Directory Traversal Attack on /etc/passwd"; content:"etc/passwd"; sid:1000004;)
```

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 tcp 172.17.0.1 any -> 172.17.0.2 80 (msg:”Directory Traversal Attack on
/etc/passwd”; content:”etc/passwd”; 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.

Then 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 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 the following URL in a browser:

http://172.17.0.2/../etc/passwd

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

```
Commencing packet processing
++ [0] docker0
Instance 0 daq pool size: 256
Instance 0 daq batch size: 64
AppId Lua-Detector Stats: instance 0, odp detectors 0, custom detectors 0, total memor
y 50 kb
06/05-04:36:50.645896 [**] [1:1000004:0] "Directory Traversal Attack" [**] [Priority:
0] {TCP} 172.17.0.1:55416 → 172.17.0.2:80
```

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.

Your manager has asked you that they have some suspicion that some hackers have been trying to access a sensitive credentials file that is stored on the server at the URL: http://172.17.0.2/credentials.txt

This is an internal file and no one apart from authorised users should be able to view it as it contains sensitive credentials to access different servers as well as databases. However, they have the suspicion that someone has been trying to access it repeatedly and failing to do so. Your job is to write a rule that will alert on traffic coming from any ip and any port, but going to the web server on nginx container and trying to access credentials.txt file.

Note: After writing the rule, you need to relaunch the lab and then select option 2 and to trigger the rule, you need to open http://172.17.0.2/credentials.txt from a web browser.

(Solution in next lecture)