LAB: Update SNORT (IDS) and review rules

Objective: Review rules to detect cryptcurrency mining using an Intrusion Detection System, particularly installation and update of SNORT.

- In this example we are using apnictraining.net as domain name.
- # super user command
- $ normal user command
- X replace with the group number
- Username `apnic` and password `training`

Topology

The following will be the topology used for this lab. Note that the IP addresses are examples only. When working on the lab, use the actual IP addresses as indicated by the instructors. For the purpose of this guide, the IP address of 192.168.30.X or 2001:db8:1::X will refer to your Virtual Machine (VM).

```
[group1.apnictraining.net] [192.168.30.1]
[group2.apnictraining.net] [192.168.30.2]
[group3.apnictraining.net] [192.168.30.3]
.................
[group30.apnictraining.net] [192.168.30.30]
```

Lab Notes

- Confirm interface name:
    - On the VM, check the IP configuration to see the interface Name

      ```
      ifconfig
      ```

    - In this guide the interface name is `eth0` . Depending on the version of Ubuntu the interface name may be `enp0s3` or something different. Where `eth0` is used in this guide replace it with your interface name.
- Virtual Machine (Container) details
    - Ubuntu 18.04 LTS/LXC

- Hostname = groupXX.apnictraining.net
- Domain name = apnictraining.net
- IPv4 Address = 192.168.30.xx
- IPv6 Address = 2001:db8:1::xx
- xx = group ID as allocated by the instructor

Install SNORT

1. Update the list of Ubuntu repos to download resources from.

```
sudo apt-get update
```

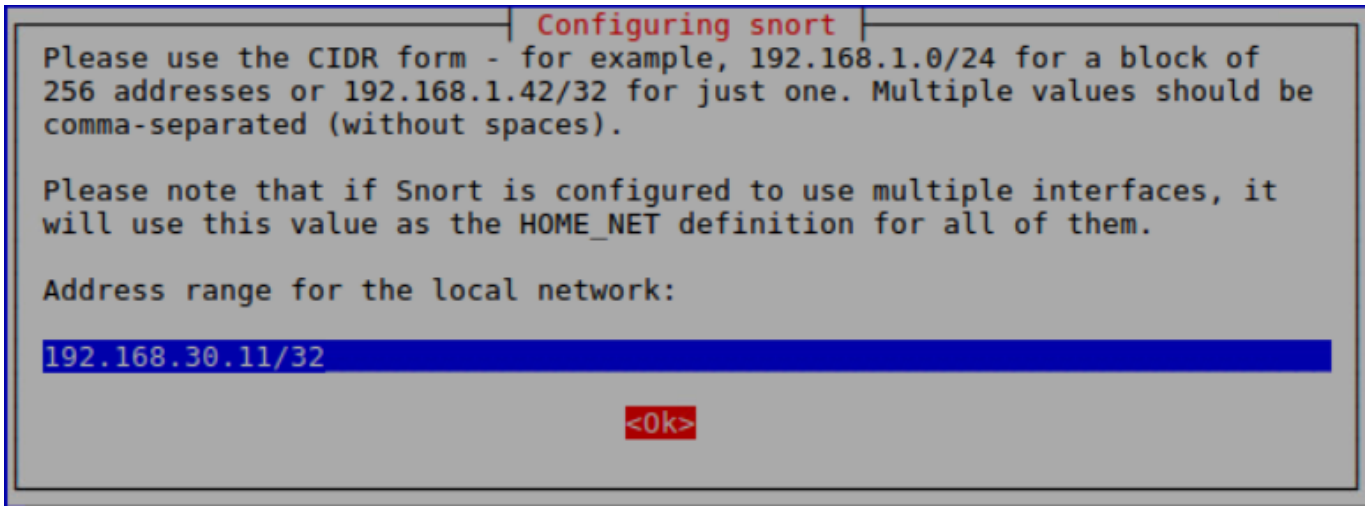
2. Install the dependencies required for snort.

```
sudo apt-get install -y ethtool build-essential libpcap-dev libpcre3-dev
sudo apt-get install -y libdumbnet-dev
sudo apt-get install -y bison flex zlib1g-dev liblzma-dev openssl libssl-dev
```

3. Install snort.

```
sudo apt-get install -y snort
```

It will ask for your HOME_NET address. For this lab define it as your host IP. Example, for group 11 it will be `192.168.30.11/32`. If required it can be changed by modifying the **snort.debian.conf** file.



4. After installation check the installation location.

```
whereis snort
```

Important file locations

- SNORT configuratiion: `/etc/snort/snort.conf`
- SNORT debian configuration: `/etc/snort/snort.debian.conf`
- SNORT rules: `/etc/snort/rules`
- SNORT executables: `/etc/sbin/snort`

5. To view the SNORT help.

```
snort -? | more
    -? display options and help
```

Update SNORT rules

1. Make a directory to store the downloaded rules

```
mkdir -p ~/Downloads/snort
cd ~/Downloads/snort
```

2. The rules file has been downloaded to a local server. Download the file

```
wget http://192.168.30.99/Exercises/snortrules-snapshot-2983.tar.gz
```

If you have an account download the rules file from https://www.snort.org/downloads

3. Extract the contents of the downloaded file:

```
tar -xvf snortrules-snapshot-2983.tar.gz
```

- -x, extract files from an archive
- -v, verbosely list files processed
- -f, use archive file or device ARCHIVE

4. Compare the updated config files with the existing configuration

```
sudo diff -y etc/snort.conf /etc/snort/snort.conf
```

- pipe symbol `|` means the files are different at that line
- less than symbol `<` means the line exists in the updated file
- greater than symbol `>` means the line exists in the current config

5. Move the updated configuration and rules to the SNORT installation directory.

```
sudo mv etc /etc/snort
sudo mv rules /etc/snort/rules
```

6. Restart SNORT.

```
sudo systemctl restart snort
```

7. Confirm SNORT is running.

```
sudo systemctl status snort
```

Review SNORT rules

Some example Snort rules used to detect crypto miners:

1. **44692**: This rule detects CoinHive mining attempts.

```
sudo grep -Hrn '44692' /etc/snort/rules
```

   - -H, print file name with output lines
   - -r, recursive
   - -n, print line number with output lines

2. **45417**: This rule detects Stratum mining protocol outbound attempts.

```
sudo grep -Hrn '45417' /etc/snort/rules
```

3. **47253**: This rule detects cryptomining javascript

```
sudo grep -Hrn '47253' /etc/snort/rules
```

4. Try doing a serach for keywords that could be used to describe the cryptomining rules:

   - crypto
   - mining
   - XMrig (try lower case as well)
   - cryptocurrency

5. Trying doing a search for rules using the Official documentation website www.snort.org/#documents

   - CVE-2019-18935 - Telerik Vulnerability
   - CVE-2017-10271 - Oracle WebLogic Server Vulnerability
   - CVE-2017-0144 - EternalBlue exploit

```
                    ***END OF EXERCISE***
```

Version: 20201105