SIGPwny

FA2024 Week 09 • 2024-10-31

Snort: Installation & Configuration, Overview & Strategy

Michael Khalaf & Sagnik Chakraborty

What is Snort?

Snort is an open-source network intrusion detection and prevention system (NIDS/NIPS) created by Martin Roesch. It is designed to monitor network traffic in real-time, detect various types of network attacks, and log or block malicious activity. Here are some key features and components of Snort:

What can we use it for?

Packet Sniffing: Snort can capture network packets in real-time and analyze them for potential threats.

Intrusion Detection: It uses predefined rules to identify suspicious traffic patterns that may indicate an intrusion or attack, such as port scans, buffer overflows, and protocol anomalies.

Intrusion Prevention: In addition to detecting threats, Snort can actively block malicious traffic when configured to do so.

Real-time Alerting: Snort can generate alerts based on specific events or activities, allowing administrators to respond quickly to potential threats.

Logging: It can log traffic data and alerts for further analysis, which is essential for incident response and forensic investigation.

Installation

1. Open Kali Linux VM

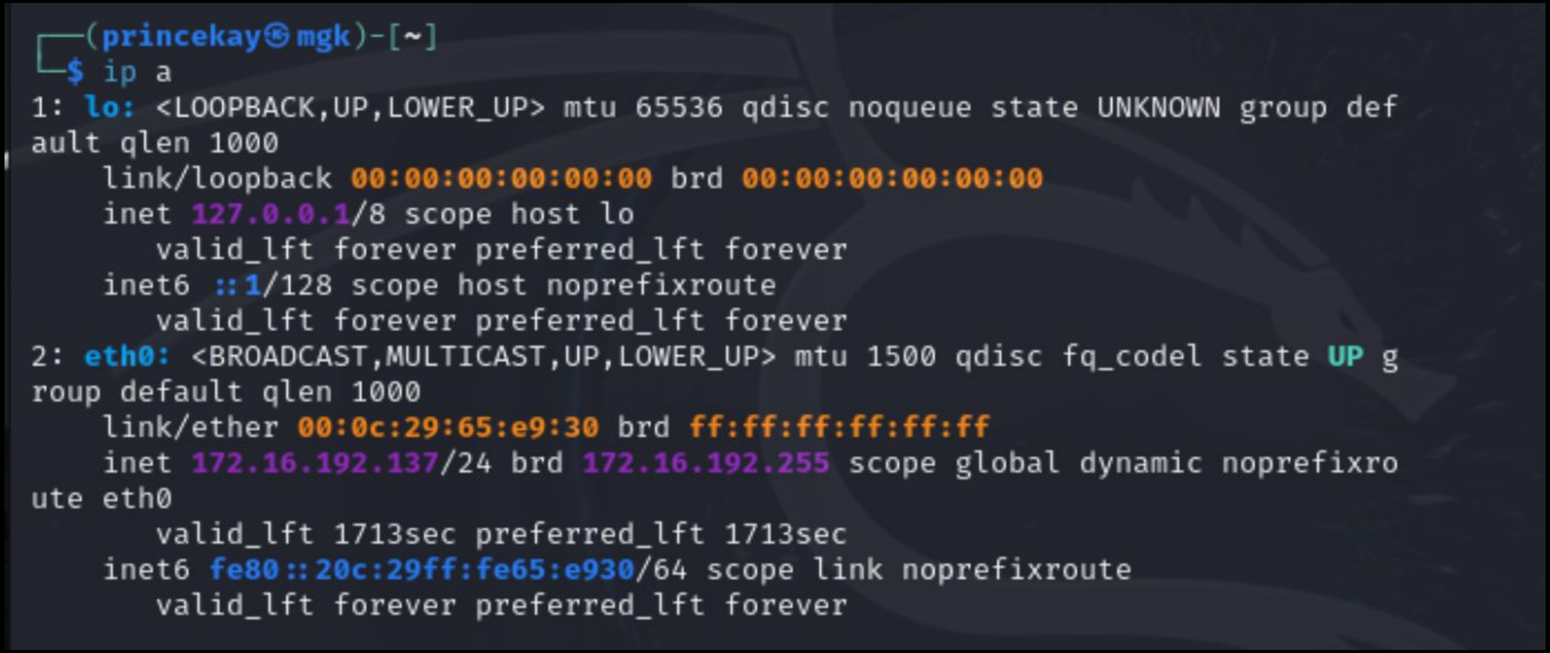
2. `sudo apt update`

3. `sudo apt install snort`

https://github.com/snort3/snort3/releases

Configure Snort

1. Command: `ip a`
2. Search for `eth0:` find your IPv4 address



```
┌──(princekay㉿mgk)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:65:e9:30 brd ff:ff:ff:ff:ff:ff
    inet 172.16.192.137/24 brd 172.16.192.255 scope global dynamic noprefixro
ute eth0
       valid_lft 1713sec preferred_lft 1713sec
    inet6 fe80::20c:29ff:fe65:e930/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Configure Snort

You could install ipcalc (to help you calculate your IP & subnet mask for snort)

```
$ sudo apt install ipcalc
```

```
$ ipcalc <your_ipv4_from_ip_a>/
```

Configure Snort

1. Open Snort configuration file:

```
$ sudo nano /etc/snort/snort.conf
```

2. Set HOME_NET variable (for your IP, include your range)

```
$ ipvar HOME_NET 172.16.192.0/24
```

3. For now, set EXTERNAL_NET to any

```
$ ipvar EXTERNAL_NET any
```

Configuration

Test the configuration file for errors at any point:

```
$ sudo snort -T -c /etc/snort/snort.conf
```

What is the idea?

Snort is open source, and it is FREE for our use.

We are encouraged to use an IDS system to our competitive advantage.

Therefore, it is allowed in CF & CCDC.

We will configure it for each VM’s IP and traverse through the 5 use case scenarios for each VM.

Implement: must add Snort to Linux & Windows system hardening checklist.

Use Case Scenarios: Packet Sniffing

→ Packet Sniffing ←

Intrusion Detection

Intrusion Prevention

Real-time Alerting

Logging

Use Case: Packet Sniffing

Capture packets & log them:

```
$ sudo snort -i eth0 -v -l /var/log/snort
```

-i eth0: Replace with your network interface.

-v: Verbose mode, displaying packet details in real-time.

-l /var/log/snort: Log the packet capture to the specified directory.

Use Case: Intrusion Detection

Packet Sniffing

→ Intrusion Detection ←

Intrusion Prevention

Real-time Alerting

Logging

Use Case: Intrusion Detection Mode

```
$ sudo snort -c /etc/snort/snort.conf -i eth0 -A console
```

-Replace eth0 with your actual network interface name (use ip a)
-A console: Output alerts to the console for real-time viewing.

-c /etc/snort/snort.conf: Use the specified configuration file.
-i eth0: Specify your network interface.
-A console: Output alerts to the console.

Use Case: Intrusion Prevention

Packet Sniffing

Intrusion Detection

→ Intrusion Prevention ←

Real-time Alerting

Logging

Use Case: Intrusion Prevention

```
$ sudo snort -Q -c /etc/snort/snort.conf -i eth0 --daq pcap --daq-var buffer_size=8388608
```

-Q: Run in inline mode to block malicious traffic.

--daq pcap: Use the packet capture DAQ (Data Acquisition) module.

--daq-var buffer_size=8388608: Set the buffer size to 8 MB (or calculate another size) for handling large traffic volumes.

Use Case: Alerts

Packet Sniffing

Intrusion Detection

Intrusion Prevention

→ Real-time Alerting ←

Logging

Use Case: Alerts

You can configure how Snort will log alerts. In the same snort.conf file, look for output configurations. For example, to log alerts to a file:

```
$ output alert_fast: /var/log/snort/alerts.log
```

→ Create the alerts.log file yourself in that /var/log/snort/ directory.

Use Case: Logging

Packet Sniffing

Intrusion Detection

Intrusion Prevention

Real-time Alerting

→ Logging ←

Use Case: Logging

```
$ sudo mkdir /var/log/snort
```

→ Ensure that a log directory exists at minimum.

```
$ chmod xxx
```

→ Ensure proper read, write, execute rules

Next Meetings

2024-11-05 • Next Tuesday

- Active Directory III with Ronan Boyarski

2024-11-07 • Next Thursday

- Splunk with Michael Khalaf & Sagnik Chakraborty