

Mahmudur Rahman
Snort Lab Updated (11-05-2025)

Network Intrusion Detection System (Snort IDS Lab)

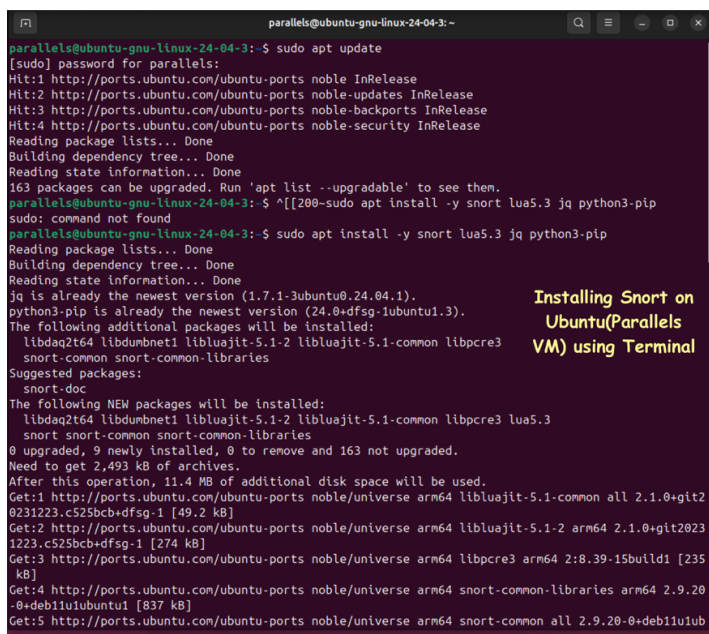
Ubuntu (Parallels VM) / Python / hping3 / Snort 2.9.20 / 2025

- Deployed and configured **Snort IDS** on Ubuntu within a virtualized Parallels environment to detect malicious traffic and perform network-level threat analysis.
- Wrote and tuned **custom local.rules** for detecting SSH brute force and port-scanning attempts with detection filters and unique SIDs.
- Used **hping3** to simulate attack traffic and validate detection logic on loopback and enp0s5 interfaces.
- Captured, analyzed, and visualized Snort alerts to confirm detection accuracy for both inbound and outbound scans.
- Created a self-contained test lab with **Python automation scripts** (generate_scan.py, generate_ssh_bruteforce.py) and alert-parsing utilities for reproducible IDS testing.
- Verified Snort's **rule engine initialization**, preprocessor configuration, and packet decoding pipeline, confirming successful packet capture and live alert generation.

Key Skills: Intrusion Detection Systems (IDS), Snort, Network Security, Packet Analysis, Python Automation, hping3, Linux Administration, Cyber Defense Lab Setup

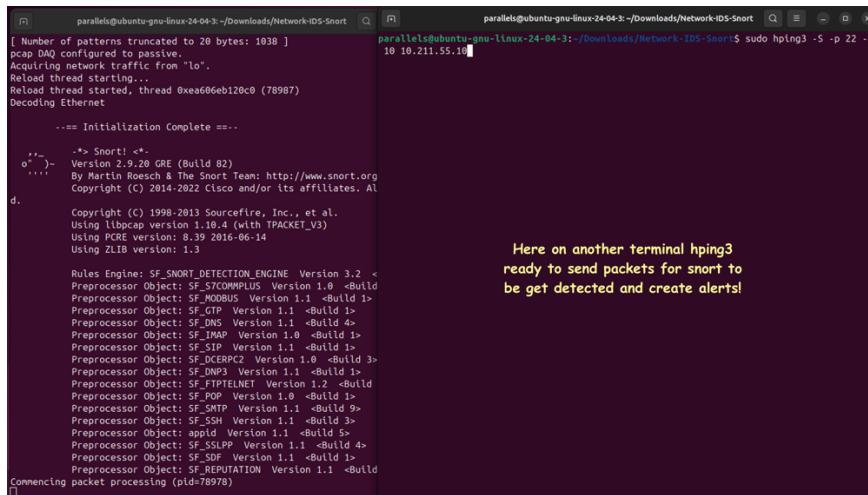
Screenshots Showcase

1. *Installing Snort on Ubuntu (Parallels VM) using Terminal*



```
parallels@ubuntu-gnu-linux-24-04-3:~$ sudo apt update
[sudo] password for parallels:
Hit:1 http://ports.ubuntu.com/ubuntu-ports noble InRelease
Hit:2 http://ports.ubuntu.com/ubuntu-ports noble-updates InRelease
Hit:3 http://ports.ubuntu.com/ubuntu-ports noble-backports InRelease
Hit:4 http://ports.ubuntu.com/ubuntu-ports noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
163 packages can be upgraded. Run 'apt list --upgradable' to see them.
parallels@ubuntu-gnu-linux-24-04-3:~$ sudo apt install -y snort lua5.3 jq python3-pip
sudo: command not found
parallels@ubuntu-gnu-linux-24-04-3:~$ sudo apt install -y snort lua5.3 jq python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
jq is already the newest version (1.7.1-3ubuntu0.24.04.1).
python3-pip is already the newest version (24.0+dfsg-1ubuntu1.3).
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 liblua5.1-2 liblua5.1-common libpcrc3
  snort-common snort-common-libraries
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 liblua5.1-2 liblua5.1-common libpcrc3 lua5.3
  snort snort-common snort-common-libraries
0 upgraded, 9 newly installed, 0 to remove and 163 not upgraded.
Need to get 2,493 kB of archives.
After this operation, 11.4 MB of additional disk space will be used.
Get:1 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 liblua5.1-common all 2.1.0+git20231223.c525bcb+dfsg-1 [49.2 kB]
Get:2 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 liblua5.1-2 arm64 2.1.0+git20231223.c525bcb+dfsg-1 [274 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libpcrc3 arm64 2:8.39-15build1 [235 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 snort-common-libraries arm64 2.9.20-0+deb11u1ubuntu1 [837 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 snort-common all 2.9.20-0+deb11u1
```


4. Running Snort on loopback interface — ready to detect and generate alerts



The image shows two terminal windows. The left window displays the Snort initialization process, including loading rules and preprocessors. The right window shows the execution of the hping3 command to send packets to the loopback interface.

```
parallels@ubuntu-gnu-linux-24-04-3: ~/Downloads/Network-IDS-Snort
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "lo".
Reload thread starting...
Reload thread started, thread 0xae60eb12b0 (78987)
Decoding Ethernet
...== Initialization Complete ==...

--* Snort! *--
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with PACKET_V3)
Using PCRE version: 8.39 2019-06-14
Using ZLIB version: 1.3

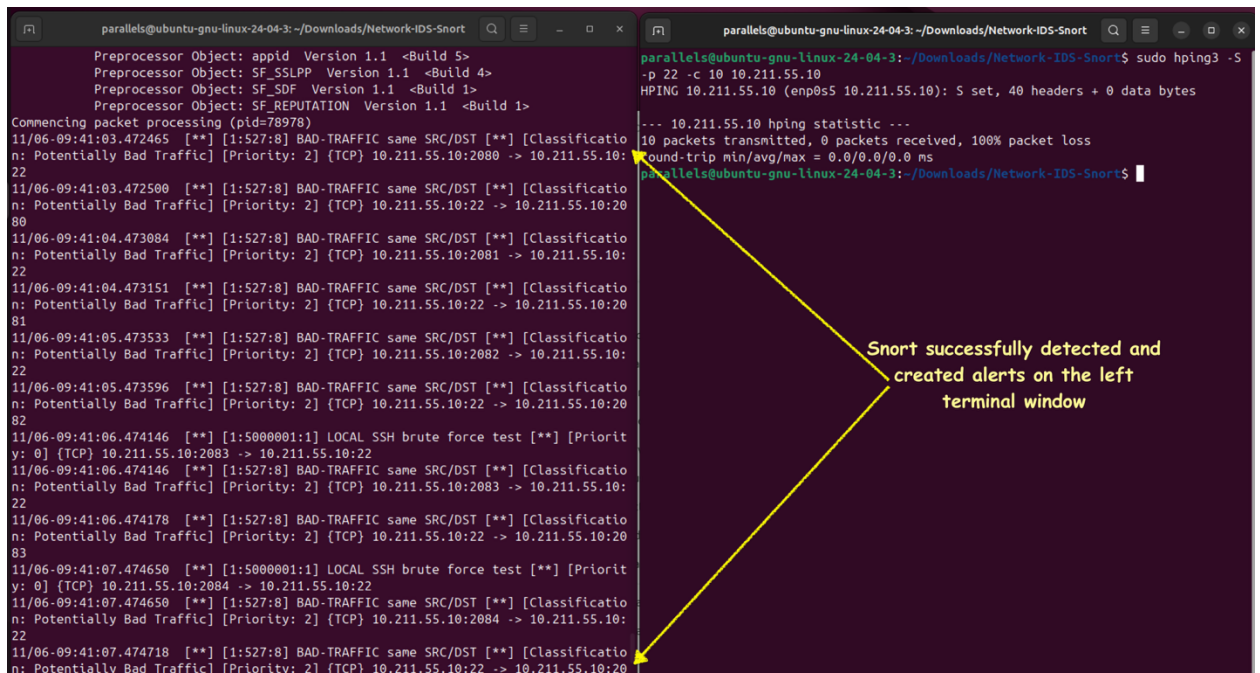
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SXCOMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_FTPNET Version 1.2 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>

Commencing packet processing (pid=78978)

parallels@ubuntu-gnu-linux-24-04-3: ~/Downloads/Network-IDS-Snort$ sudo hping3 -S -p 22 -c 10 10.211.55.10
```

Here on another terminal hping3 ready to send packets for snort to be get detected and create alerts!

5. Simulated SSH brute-force traffic with hping3 scripts; Snort generated real-time alerts in console view



The image shows two terminal windows. The left window displays Snort alerts for simulated SSH brute-force traffic. The right window shows the execution of the hping3 command to send packets to the loopback interface.

```
parallels@ubuntu-gnu-linux-24-04-3: ~/Downloads/Network-IDS-Snort
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Commencing packet processing (pid=78978)
11/06-09:41:03.472465 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:2080 -> 10.211.55.10:22
11/06-09:41:03.472500 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:22 -> 10.211.55.10:2080
11/06-09:41:04.473084 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:2081 -> 10.211.55.10:22
11/06-09:41:04.473151 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:22 -> 10.211.55.10:2081
11/06-09:41:05.473533 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:2082 -> 10.211.55.10:22
11/06-09:41:05.473596 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:22 -> 10.211.55.10:2082
11/06-09:41:06.474146 [**] [1:5000001:1] LOCAL SSH brute force test [**] [Priority: 0] (TCP) 10.211.55.10:2083 -> 10.211.55.10:22
11/06-09:41:06.474146 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:2083 -> 10.211.55.10:22
11/06-09:41:06.474178 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:22 -> 10.211.55.10:2083
11/06-09:41:07.474650 [**] [1:5000001:1] LOCAL SSH brute force test [**] [Priority: 0] (TCP) 10.211.55.10:2084 -> 10.211.55.10:22
11/06-09:41:07.474650 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:2084 -> 10.211.55.10:22
11/06-09:41:07.474718 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: n: Potentially Bad Traffic] [Priority: 2] (TCP) 10.211.55.10:22 -> 10.211.55.10:2084

parallels@ubuntu-gnu-linux-24-04-3: ~/Downloads/Network-IDS-Snort$ sudo hping3 -S -p 22 -c 10 10.211.55.10
HPING 10.211.55.10 (enp0s5 10.211.55.10): S set, 40 headers + 0 data bytes
--- 10.211.55.10 hping statistic ---
10 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
parallels@ubuntu-gnu-linux-24-04-3: ~/Downloads/Network-IDS-Snort$
```

Snort successfully detected and created alerts on the left terminal window