

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

## Network Intrusion Detection System (Snort IDS Lab)

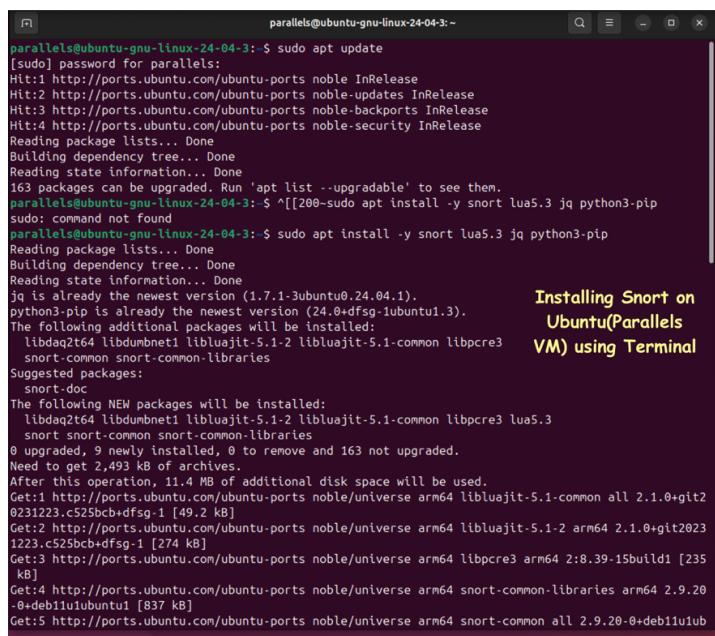
Ubuntu (Parallels VM) / Python / hping3 / Snort 2.9.20 / 2025

- 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

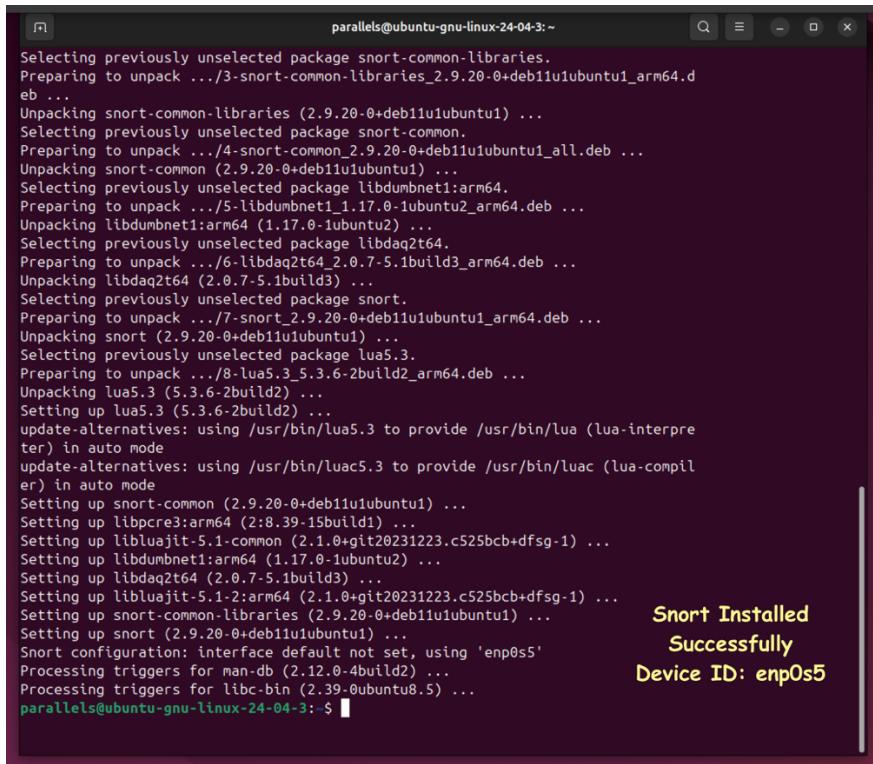
### 1. Installing Snort on Ubuntu (Parallels VM) using Terminal



The screenshot shows a terminal window titled "parallels@ubuntu-gnu-linux-24-04-3:~". The user runs several commands to update the package list and install Snort, its dependencies, and its Python interface. The terminal output includes details about package versions, dependencies like libdaq7t64, libdumbnet1, libluajit-5.1-2, libluajit-5.1-common, libpcres3, snort-common, and snort-common-libraries, and suggested packages such as snort-doc. It also lists new packages like libdaq7t64, libdumbnet1, libluajit-5.1-2, libluajit-5.1-common, libpcres3, and lua5.3. The process shows 0 upgraded, 9 newly installed, and 0 to remove. The total disk space required is 11.4 MB, and the user needs to get 2,493 kB of archives. The download progress is shown for five files from ports.ubuntu.com.

```
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:~$ ^[[200+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:
  libdaq7t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libpcres3
  snort-common snort-common-libraries
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq7t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libpcres3 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 libluajit-5.1-common all 2.1.0+git20231223.c525bc9+dfsg-1 [49.2 kB]
Get:2 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libluajit-5.1-2 arm64 2.1.0+git20231223.c525bc9+dfsg-1 [274 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libpcres3 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+deb11u1 [837 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 snort-common all 2.9.20-0+deb11u1 [837 kB]
```

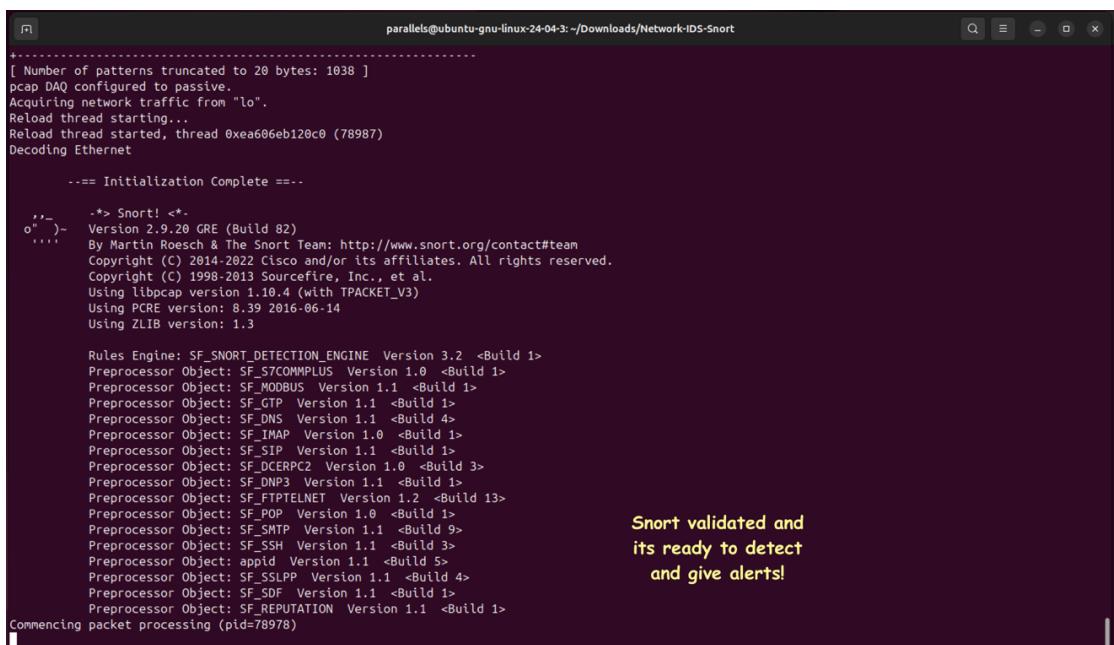
2. Snort successfully installed and configured — interface `enp0s5` identified



```
parallels@ubuntu-gnu-linux-24-04-3:~$ Selecting previously unselected package snort-common-libraries.
Preparing to unpack .../3-snort-common-libraries_2.9.20-0+deb11u1ubuntu1_arm64.d
eb ...
Unpacking snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../4-snort-common_2.9.20-0+deb11u1ubuntu1_all.deb ...
Unpacking snort-common (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package libdumbnet1:arm64.
Preparing to unpack .../5-libdumbnet1_1.17.0-1ubuntu2_arm64.deb ...
Unpacking libdumbnet1:arm64 (1.17.0-1ubuntu2) ...
Selecting previously unselected package libdaq2t64.
Preparing to unpack .../6-libdaq2t64_2.0.7-5.1build3_arm64.deb ...
Unpacking libdaq2t64 (2.0.7-5.1build3) ...
Selecting previously unselected package snort.
Preparing to unpack .../7-snort_2.9.20-0+deb11u1ubuntu1_arm64.deb ...
Unpacking snort (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package lua5.3.
Preparing to unpack .../8-lua5.3_5.3.6-2build2_arm64.deb ...
Unpacking lua5.3 (5.3.6-2build2) ...
Setting up lua5.3 (5.3.6-2build2) ...
update-alternatives: using /usr/bin/lua5.3 to provide /usr/bin/lua (lua-interpreter) in auto mode
update-alternatives: using /usr/bin/luac5.3 to provide /usr/bin/luac (lua-compiler) in auto mode
Setting up snort-common (2.9.20-0+deb11u1ubuntu1) ...
Setting up libpcap3:arm64 (2:8.39-15build1) ...
Setting up liblualjit-5.1-common (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up libdumbnet1:arm64 (1.17.0-1ubuntu2) ...
Setting up libdaq2t64 (2.0.7-5.1build3) ...
Setting up liblualjit-5.1.2:arm64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Setting up snort (2.9.20-0+deb11u1ubuntu1) ...
Snort configuration: interface default not set, using 'enp0s5'
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.5) ...
parallels@ubuntu-gnu-linux-24-04-3:~$
```

Snort Installed  
Successfully  
Device ID: `enp0s5`

3. Snort validated configuration: initialized preprocessors and detection engine



```
parallels@ubuntu-gnu-linux-24-04-3:~/Downloads/Network-ID-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 0xea606eb120c0 (78987)
Decoding Ethernet
    --- Initialization Complete ---

    => Snort! <-
  o`-- Version 2.9.20 GRE (Build 82)
  ...` By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
  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 TPACKET_V3)
  Using PCRE version: 8.39 2016-06-14
  Using ZLIB version: 1.3

  Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
  Preprocessor Object: SF_S7COMMPLUS 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_DCEPFC2 Version 1.0 <Build 3>
  Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
  Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
  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: apid 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)
```

Snort validated and  
its ready to detect  
and give alerts!

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

The screenshot shows two terminal windows side-by-side. The left terminal window displays the Snort configuration file (snort.conf) with various rules and preprocessors defined. The right terminal window shows the command `sudo hping3 -S -p 22 -c 10 10.211.55.10` being run to send TCP SYN packets to port 22 of the target host.

```
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAO configured to passive.
Acquiring network traffic from "lo".
Reload thread starting...
Reload thread started, thread 0xeaa69eb120c0 (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.  

d.  

Copyright (C) 1998-2018 Sourcefire, Inc., et al.  

Using libpcap version 1.18.4 (with TPACKET_V3)  

Using PCRE version: 8.39 2016-06-14  

Using ZLIB version: 1.3  

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <  

Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>  

Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  

Preprocessor Object: SF_SNMP Version 1.1 <Build 4>  

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 1>  

Preprocessor Object: SF_DNP3 Version 1.1 <Build 3>  

Preprocessor Object: SF_FTPTELNET Version 1.0 <Build 1>  

Preprocessor Object: SF_PPP Version 1.0 <Build 1>  

Preprocessor Object: SF_SMB Version 1.1 <Build 1>  

Preprocessor Object: SF_LSH 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)  

[]
```

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 screenshot shows two terminal windows. The left terminal window displays the Snort log output, which includes numerous alerts for "BAD-TRAFFIC same SRC/DST" (SSH brute-force test) at source IP 10.211.55.10 and destination IP 10.211.55.10. The right terminal window shows the command `sudo hping3 -S -p 22 -c 10 10.211.55.10` being run to send TCP SYN packets to port 22 of the target host. A yellow arrow points from the right terminal window to the left one, indicating that Snort successfully detected and created alerts for the simulated traffic.

```
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: 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: 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: 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: 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: 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: 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: 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: 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: 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: Potentially Bad Traffic] [Priority: 2] [TCP] 10.211.55.10:22 -> 10.211.55.10:2084
```

Snort successfully detected and  
created alerts on the left  
terminal window