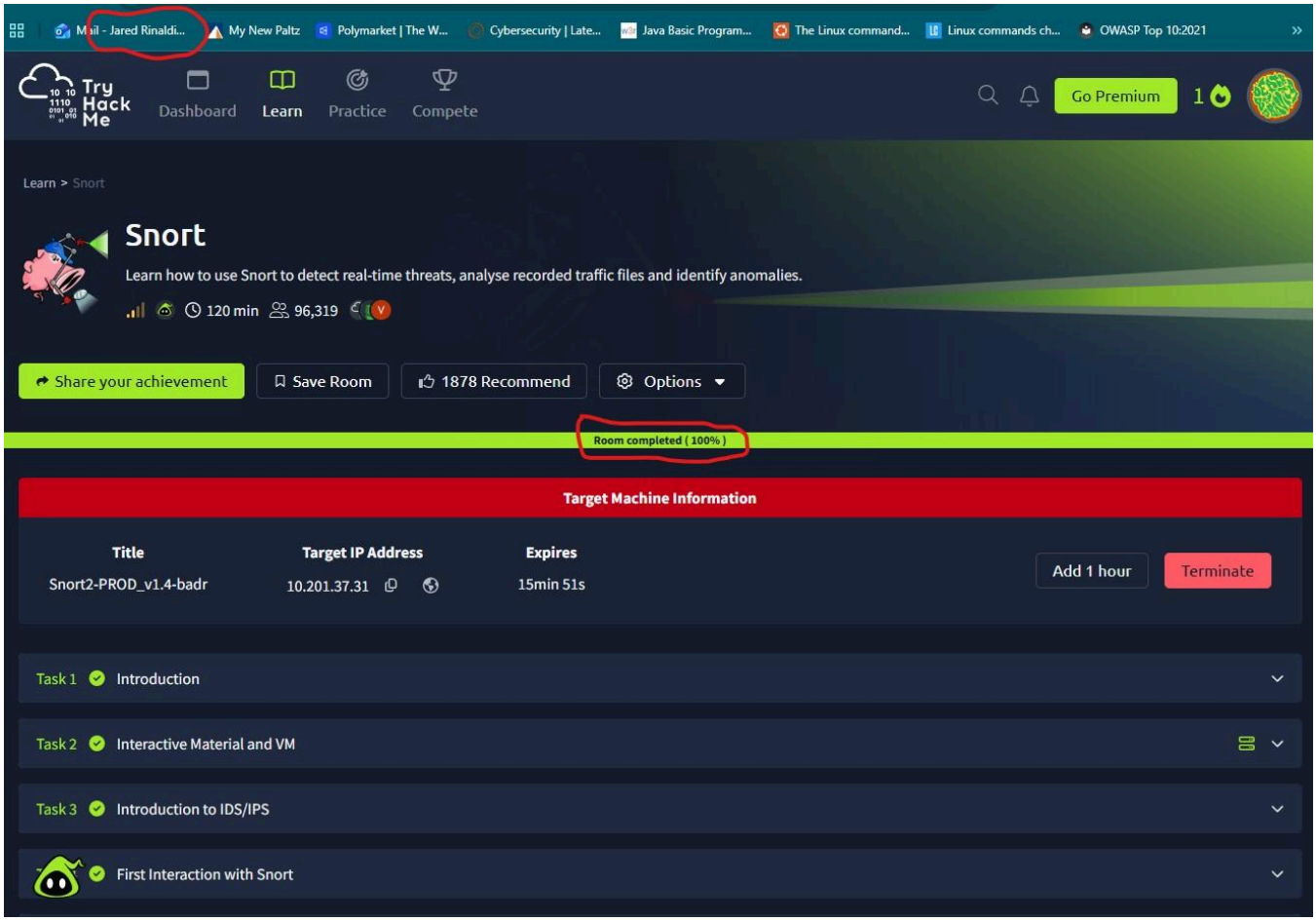
Exploring Snort Capabilities

Researcher: Jared Rinaldi
GitHub: GitHub.com/PyronicGreen
November 3, 2025

Abstract: Snort is an open source network intrusion detection and prevention system (NIDS/NIPS) made by Cisco. It is capable of performing real-time traffic analysis and packet logging on IP networks. Additionally, it can perform protocol analysis, content searching and matching, as well as detect a variety of attacks and probes. It can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging) or as a full-blown network intrusion prevention system. In this lab, I will install Snort on my Ubuntu Virtual Machine. Snort will then be used to detect my network traffic, which will be saved to a snort log file where it can be analyzed.

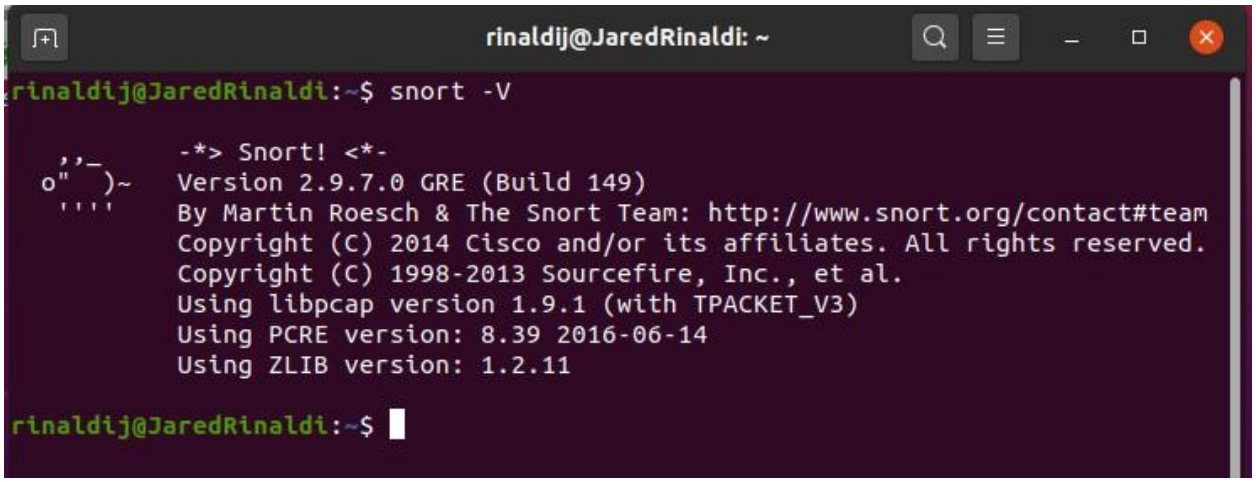
TryHackMe Snort Assignment:



Assignment 6
Snort Configuration
Step 1: Update the System

```
rinaldij@JaredRinaldi:/var/log/snort$ sudo apt update
[sudo] password for rinaldij:
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
rinaldij@JaredRinaldi:/var/log/snort$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
rinaldij@JaredRinaldi:/var/log/snort$
```

Step 2: Confirm Snort Installation



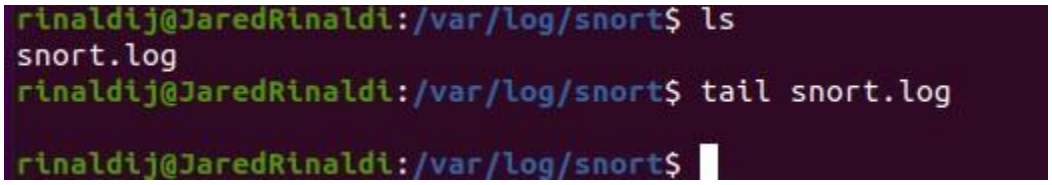
Step 5: Test Snort Configuration

```
Snort successfully validated the configuration!
Snort exiting
rinaldij@JaredRinaldi:~$
```

Steps 6 and 7: Download and View Snort Logs

I ran the command `sudo snort -c /etc/snort/snort.conf -i enp0s3`. I let the command run for around 15 seconds, and then stopped it with CTRL+c. A log file was generated called snort.log. I checked this file using the `tail` and `nano` commands,

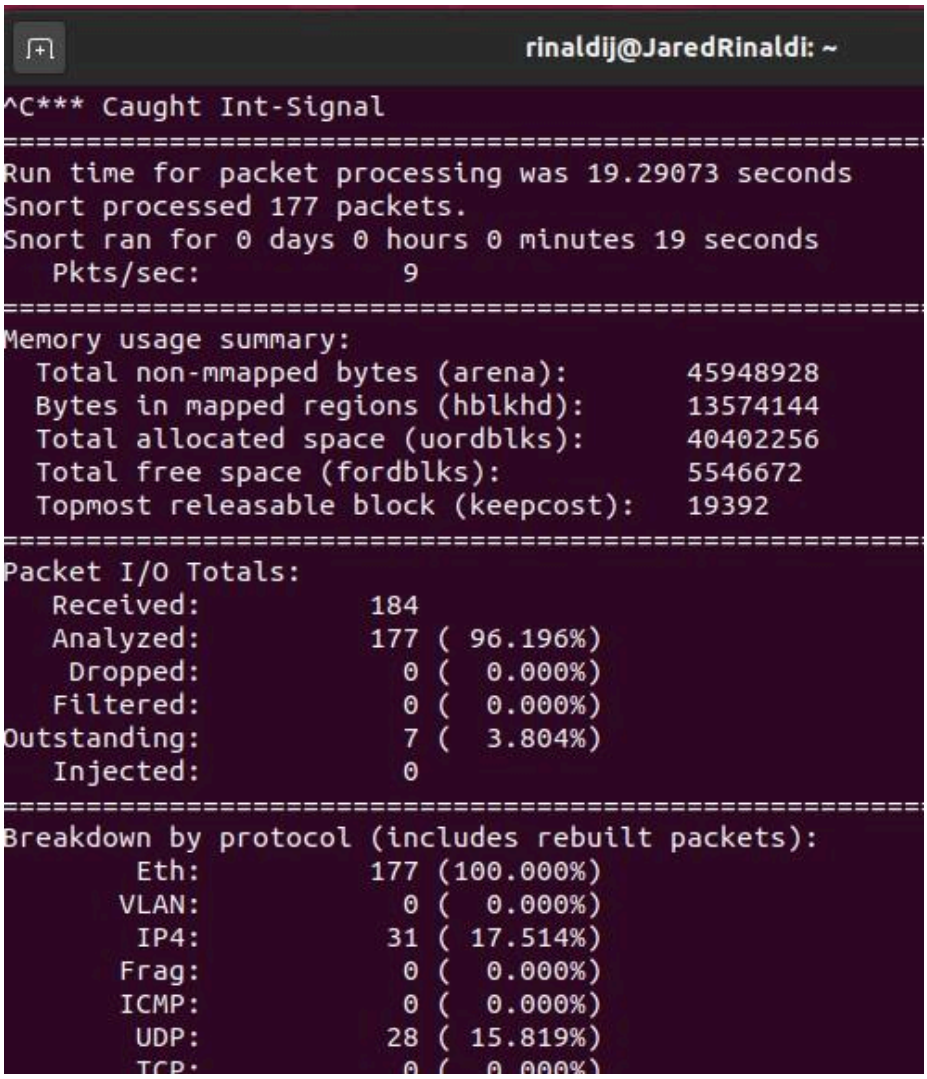
but it did not seem to contain any log entries. I believe this is due to my system being isolated from the rest of the network due to it being a virtual machine, and therefore there is no inbound network traffic.



Step 8: Running Snort as a Daemon

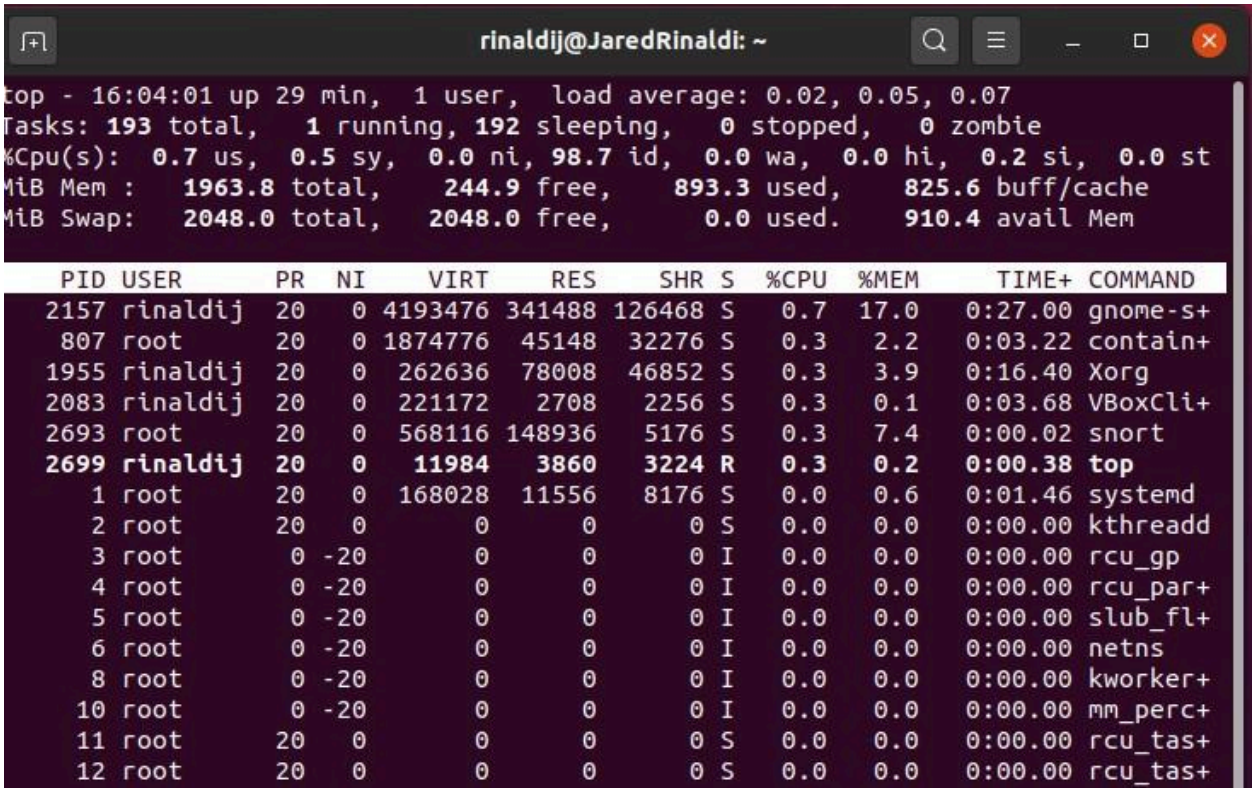
When I ran the command for this step, I did not see “Snort” running as one of the processes. As this looked to be the wrong outcome, I did a little research and discovered that VirtualBox’s default network configuration is set to NAT, which prevents the virtual host from getting any inbound traffic.

The fix was to shut down VirtualBox and switch the network type to “Bridged Connection.” After doing this and re-starting my Ubuntu machine, I went back and repeated step 6, believing that now Snort would have some network traffic to work with. This proved to be accurate. Right away, the output made it clear that Snort was analyzing packets. This meant my virtual network was no longer isolated.

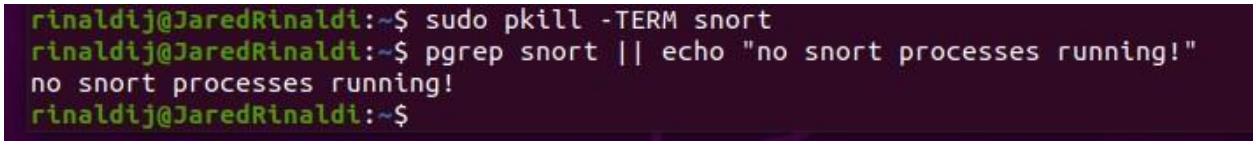


The snort.log file now contained data entries (step 7).
Returning to Step 8, the command `sudo snort -D -c /etc/snort/snort.conf -i enp0s3` was again run.

This time, “snort” did show up as a process when the `top` command was run.



To stop all snort processes from running, I ran the command `sudo pkill -TERM snort`. I used the `pgrep` command to confirm no Snort processes were running.



Conclusion: In this lab, I successfully installed Snort and used it in IDS mode to monitor traffic and log alerts. Using the "-D" option in the snort command, I was able to configure Snort to run as a background process and monitor incoming and outgoing network traffic. Snort is a useful tool and I anticipate using it for future home lab purposes.