Lab 9 – SNORT

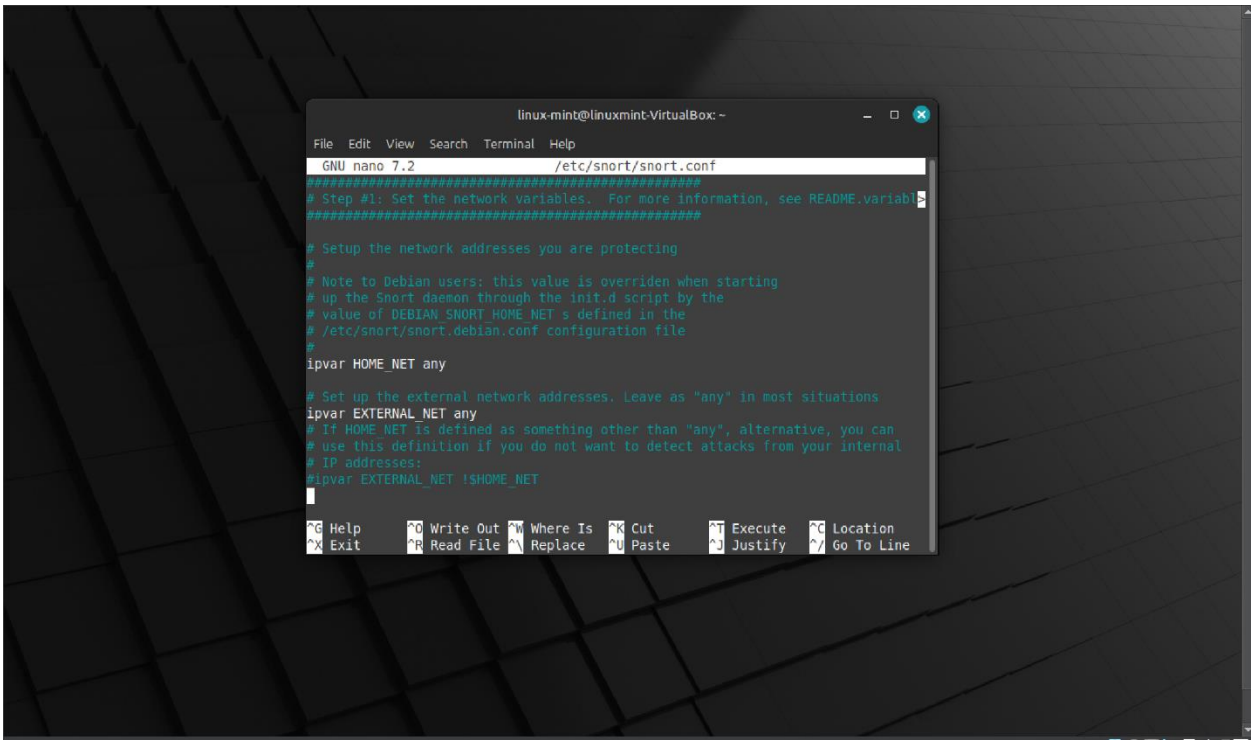
CSCI 4406_60L – Computer Networks Lab

Joshua Ludolf

- To start this lab, I installed snort (no issues 😎):

```
linux-mint@linuxmint-VirtualBox:~$ sudo apt-get install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.20-0+deb11u1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 12 not upgraded.
```

- From there, I confirmed the snort.config file (some issues, it required me to start over when I tried to change any of the include rules, so I ran this lab without changing config file after getting new linux mint image…)

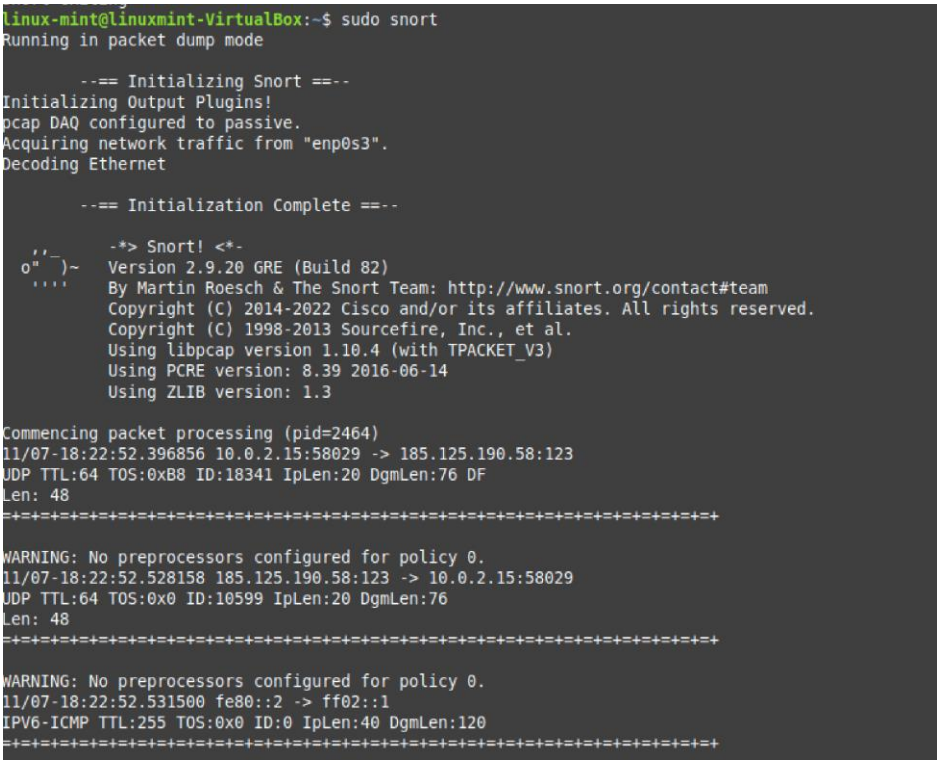


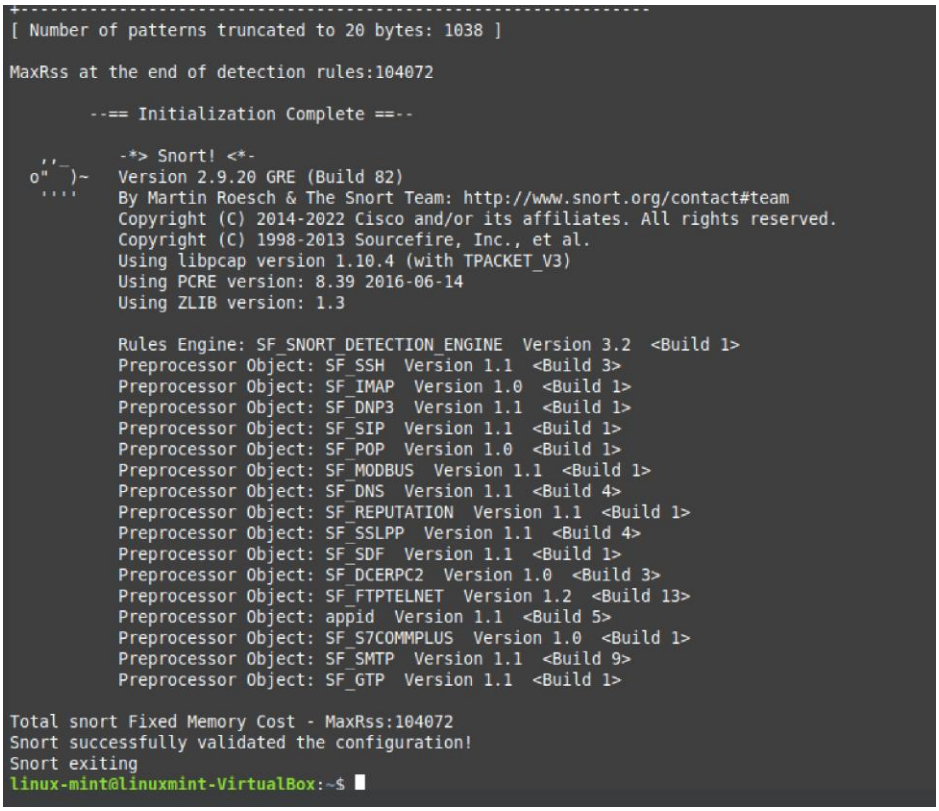
- From there, I ran snort that would "sniff" any network traffic :

```
linux-mint@linuxmint-VirtualBox:~$ sudo snort -q -A console -c /etc/snort/snort.conf
11/07-19:30:04.121310  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
11/07-19:30:05.170010  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
11/07-19:30:06.202201  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
11/07-19:30:07.218199  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
11/07-19:30:08.247346  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
11/07-19:30:09.270396  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
11/07-19:30:10.290163  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
^C*** Caught Int-Signal
11/07-19:30:11.317093  [**] [1:385:3] Joshua Ludolf - ICMP TraceRoute [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.1.1.2
```

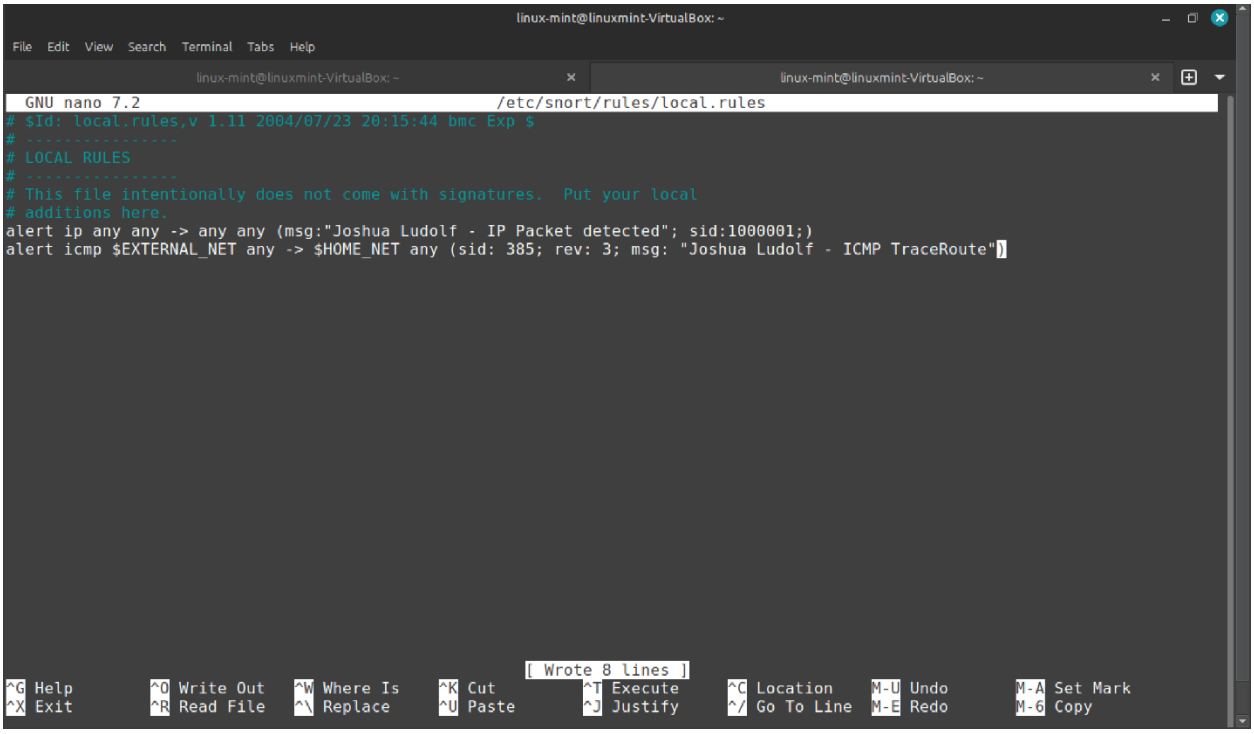
-

- Additionally, I confirmed successful installation of snort (still no issues).

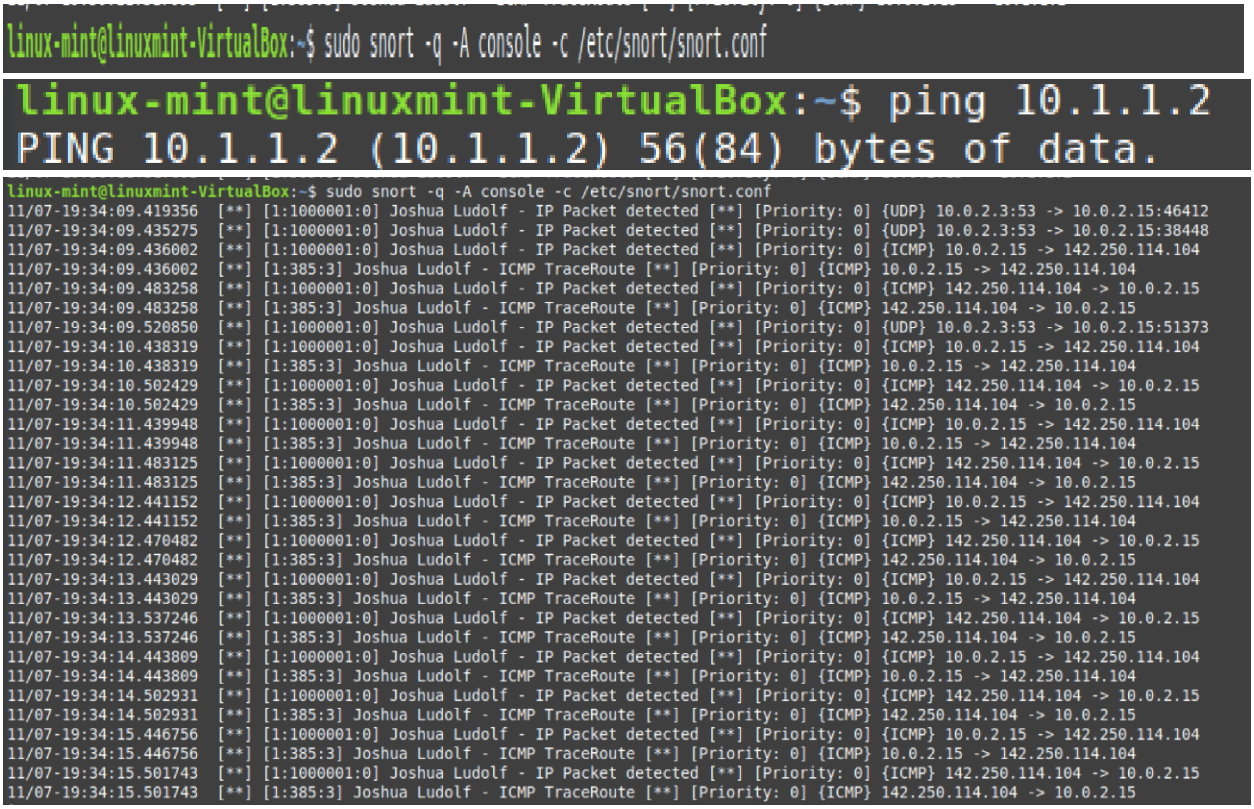




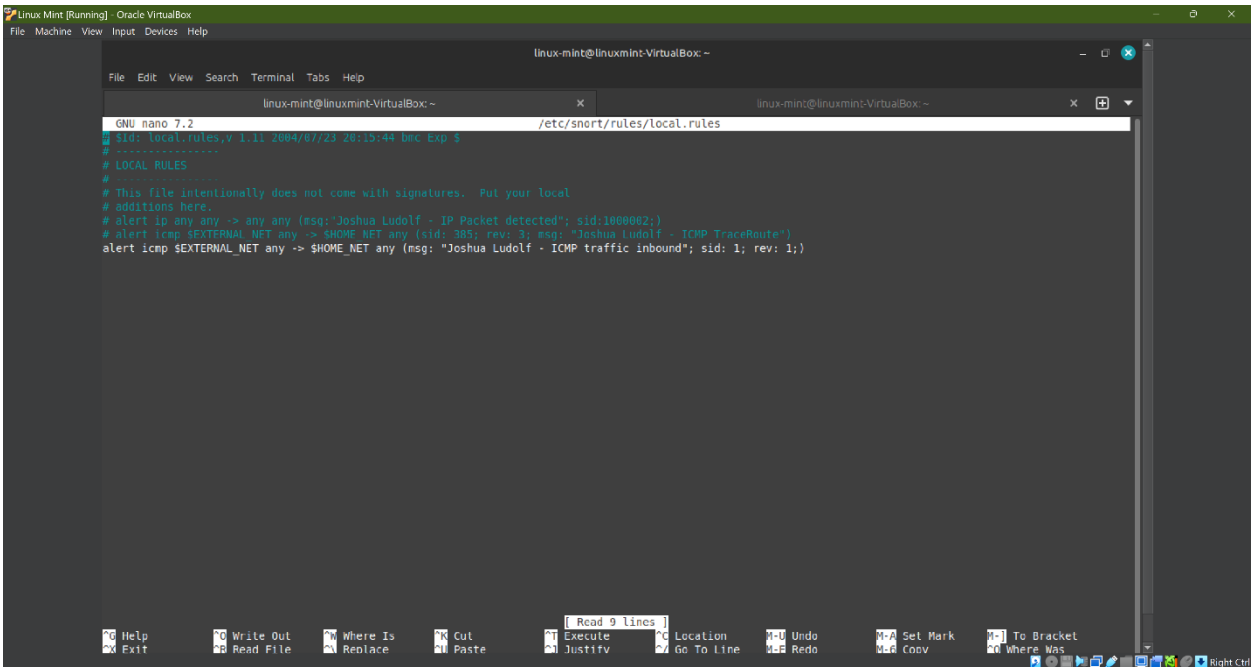
- I then added two rules as show into local.rules file:

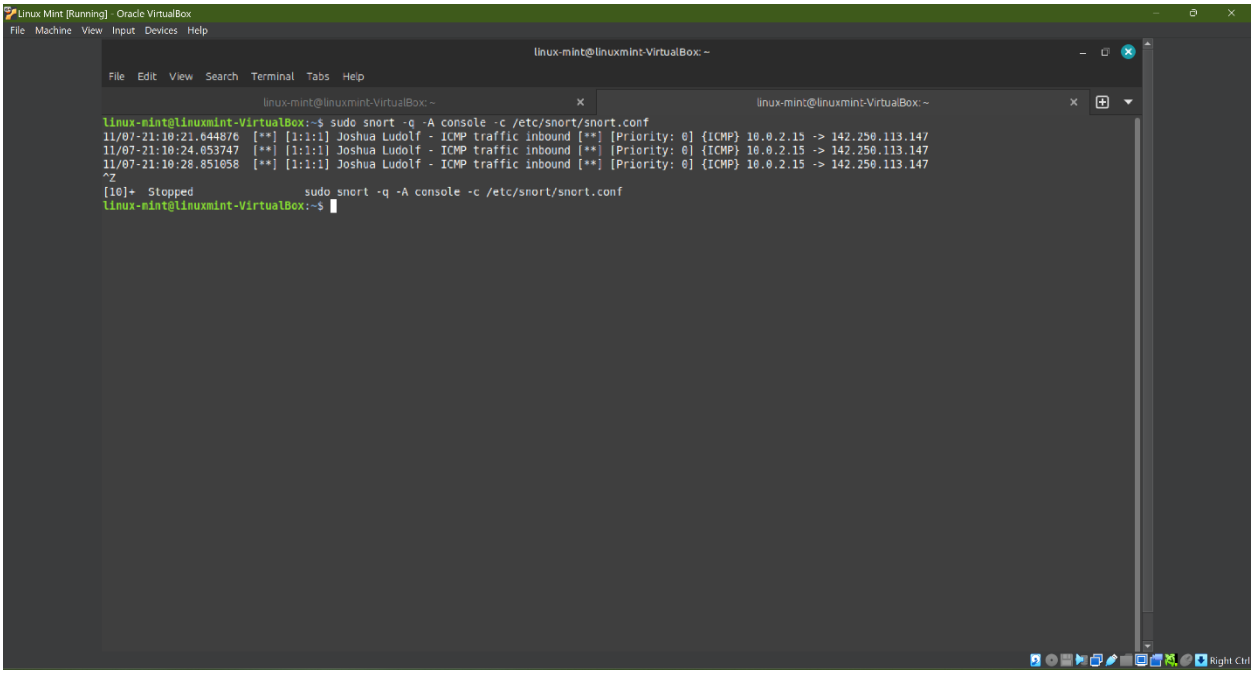


- From there I ran sudo snort -q -A console -c /etc/snort/snort.conf to see my new rules in action and additionally ping 10.1.1.2:



- After that I added another rule to the same file – alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: “Joshua Ludolf – ICMP traffic inbound”; sid: 1; rev: 1;) - (I had to comment out the other rules as it was getting confusing):





- From this lab I learned:

From this Snort lab, I gained a deeper understanding of network intrusion detection and prevention, which was incredibly insightful. Initially, I learned about Snort, a powerful tool that helps monitor and secure network traffic. Installing and configuring Snort on my Linux system gave me hands-on experience in setting up a network intrusion detection system.

Writing and customizing Snort rules was fascinating. I created a rule to detect visits to www.google.com by looking for outbound TCP traffic on port 80 that contained the pattern "www.google.com". This exercise taught me the importance of various components in a rule, such as msg, content, sid, and rev, and how they work together to trigger alerts.

Throughout the process, I encountered and resolved issues like rule duplication and deprecated keywords. These challenges taught me how to troubleshoot errors, use sudo commands, and restart services to apply changes effectively.

Checking the Snort alert logs after visiting a website and verifying that my custom rule triggered an alert was a rewarding experience. It showed me how alerts are generated and logged by Snort, providing valuable insights into network activities.

Overall, this lab equipped me with practical knowledge and hands-on experience in using Snort for network security. I now feel more confident in setting up and managing intrusion detection systems, creating custom monitoring rules, and proactively detecting and responding to potential threats. This experience has been invaluable in enhancing my skills in network security.