C&NS Lab Assignment 14

Onkar Santosh Gavali (2019BTECS00037)

Batch B2

# Index

Snort

* Explain Intrusion Detection System.
* Implement Intrusion Detection System using snort.

# 

# 

# Intrusion Detection System

**SNORT**

Snort is the world's foremost Open Source Intrusion Prevention System (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users. Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging or can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

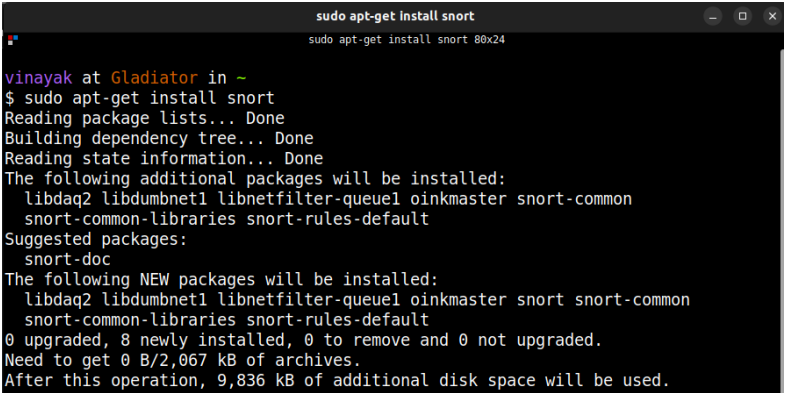
# Snort

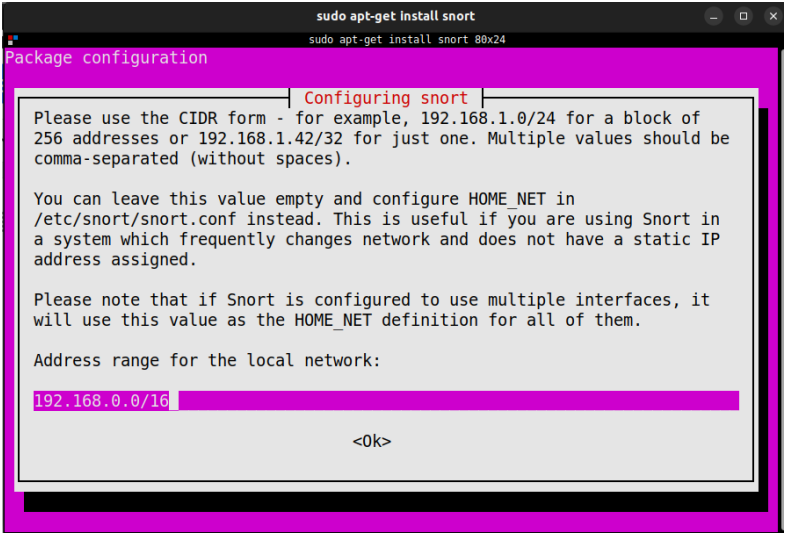
Snort is an open source and popular Intrusion Detection System (IDS). It works by actively monitoring of network traffic parsing each packet and alerting system administrator of any anomalous behavior that goes against the snort rules configured by the administrator according to the security policies of an organization.

Install snort in windows: <https://zaeemjaved10.medium.com/installing-configuring-snort-2-9-17-on-windows-10-26f73e342780>

Snort installed

# Output

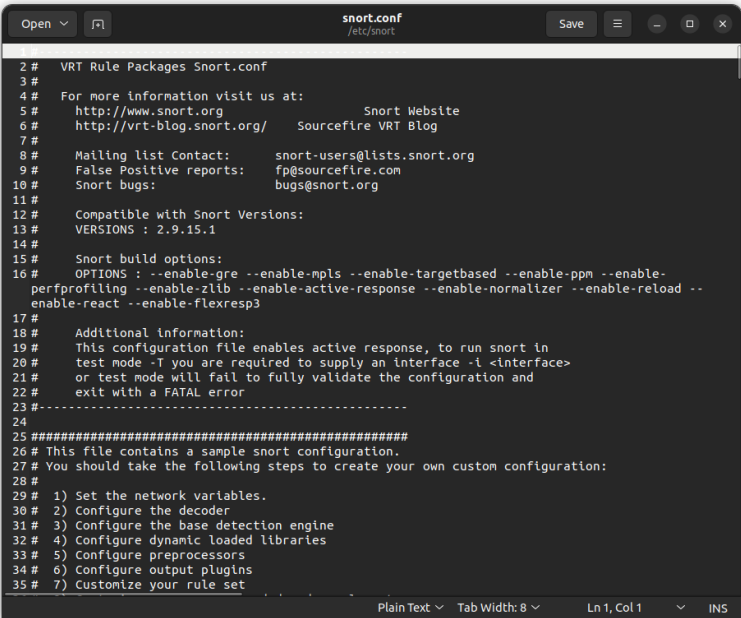




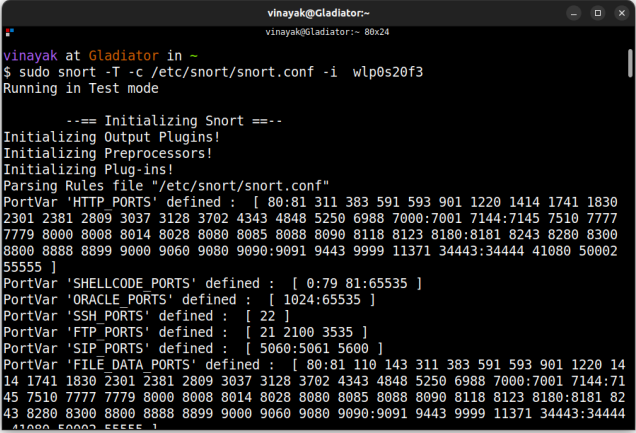


SNORT Configuration

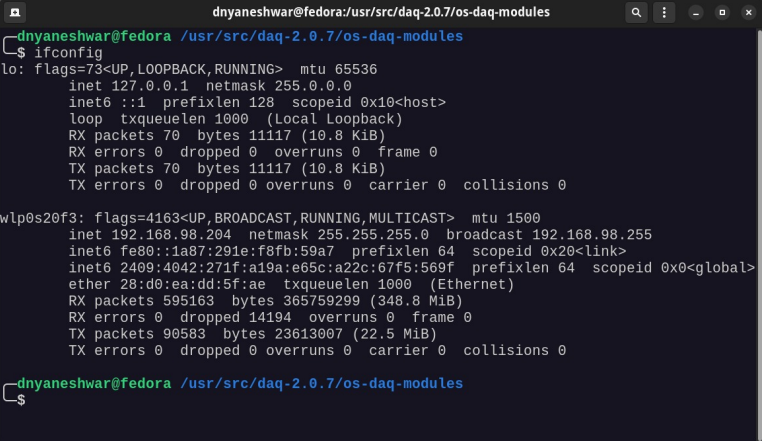




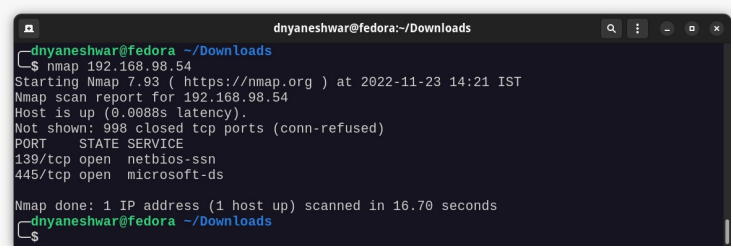
Checking configurations for the wireless interface



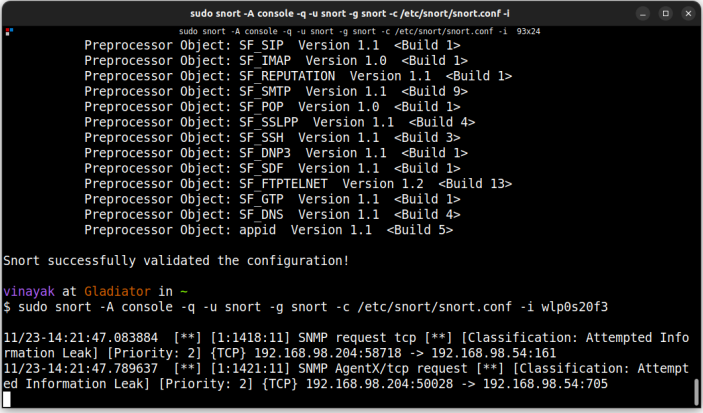
Attacking device Information:



Running NMAP from another device

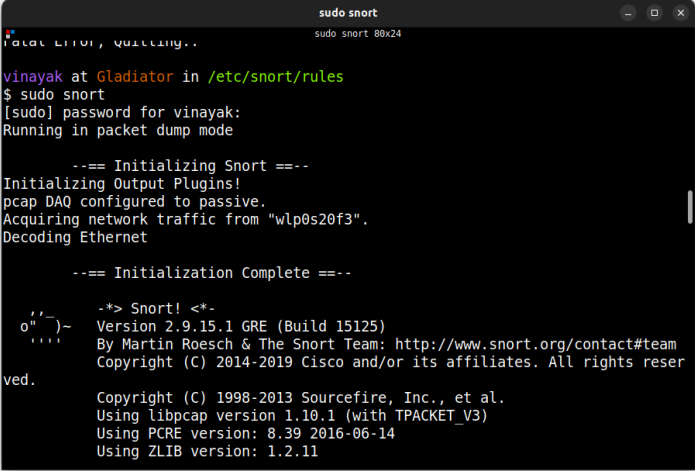


Starting SNORT in detection mode:

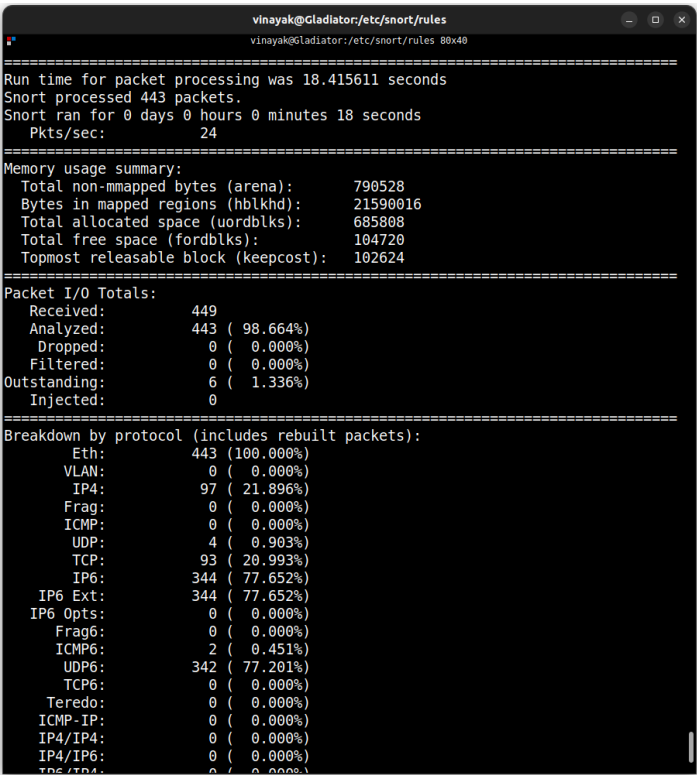


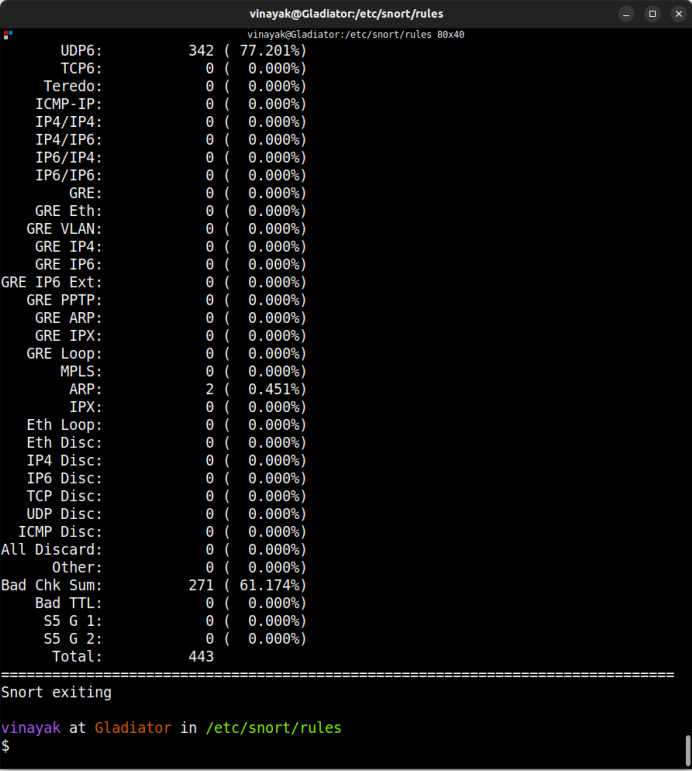
The above screenshot shows that SNORT has successfully detected the NMAP attack and an alert has been generated

Running snort in sniffing mode:



Sniffing result:





# 