Investigation Stage/Research

Intrusion Detection System setup and Tuning of Snort is the foremost open-source intrusion prevention system in the world. It uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generate alerts for users. Snort can be deployed to inline stop these packets as well. It has three primary uses. The first is a packet sniffer like tcpdump, a packet logger, which helps network traffic debugging and the last is a full-blown network intrusion prevention system. This one source can be configured for personal and business alike. (Snort)

T

IDS Planning Stage:

My plan is to install snort on a ubuntu system, reason for this is it is an operating system I have never used, and a command line based. I challenges I will uncover are lack of knowledge of the operating system and lack of knowledge on snort. To solve these problems, I will rely on the internet, YouTube, and my instructor.

* Create a Virtual Machine
* Chosen operating system Ubuntu.
* Configure Ubuntu system setup.
* Install Snort
* Create rules for ping, internet, and DOS.
* Attempts Nmap scan.
* Attempts DOS attack.
* Attempt ping.
* Attempt internet.
* Face problems with rules and find solutions.

# Works Cited

*Snort*. n.d. snort.org. 03 08 2024.