EXPERIMENT NUMBER 8

Name of Student: Sangeet Agrawal	PRN: 21070122140	Section: CS-B3

Title: Study of Intrusion Detection System (IDS)

Aim: Study and understand Snort IDS

Objective: To make students understand IDS and current research in IDS

Theory:

The goal of the Intrusion Detection Analyst is to find possible attacks against a network. Recent years have witnessed a significant increase in Distributed Denial-of-Service (DDoS) attacks on the Internet, making network security a great concern. Analysts search for possible attacks by examining IDS logs and packet captures and corroborating them with firewall logs, known vulnerabilities, and general trending data from the Internet. IDS attacks are becoming more sophisticated; automatically reasoning the attack scenarios in real-time, and categorizing them has become a critical challenge. These processes result in huge amounts of data, which analysts must examine to detect a pattern. However, the overwhelming flow of events generated by IDS sensors make it difficult for security administrators to uncover hidden attack plans.

To become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSs, IDSs, malicious network activity, and log information.

Overview of Intrusion Detection Systems

Intrusion detection systems are highly useful as they monitor both the inbound and outbound traffic of the network and continuously inspects the data for suspicious activities that may indicate a network or system security breach. The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is detected. It can be categorized into active and passive, depending on its functionality: an IDS is generally passive and is used to detect intrusions, while an intrusion prevention system (IPS) is considered as an active IDS, as it is not only used to detect the intrusion on the network, but also prevent them.

Main Functions of IDS:

- Gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy
- Also referred to as a “packet-sniffer,” which intercepts packets traveling along various communication mediums and protocols
- Evaluates traffic for suspected intrusions and signals an alarm after detection

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. 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 generate 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 it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

Detect Intrusions using Snort: Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching and is used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic to collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

Uses of Snort:

- Straight packet sniffer such as tcpdump
- Packet logger (useful for network traffic debugging, etc.)
- Network intrusion prevention system

Tools for Study:

1) Snort
2) HoneyBOT

Reference web links:

1) https://www.snort.org/
2) https://download.cnet.com/Intrusion-Detection-System-SAX2/3000-18510_4-10886064.html
3) https://honeybot.software.informer.com/

Conclusion:

Theory question:

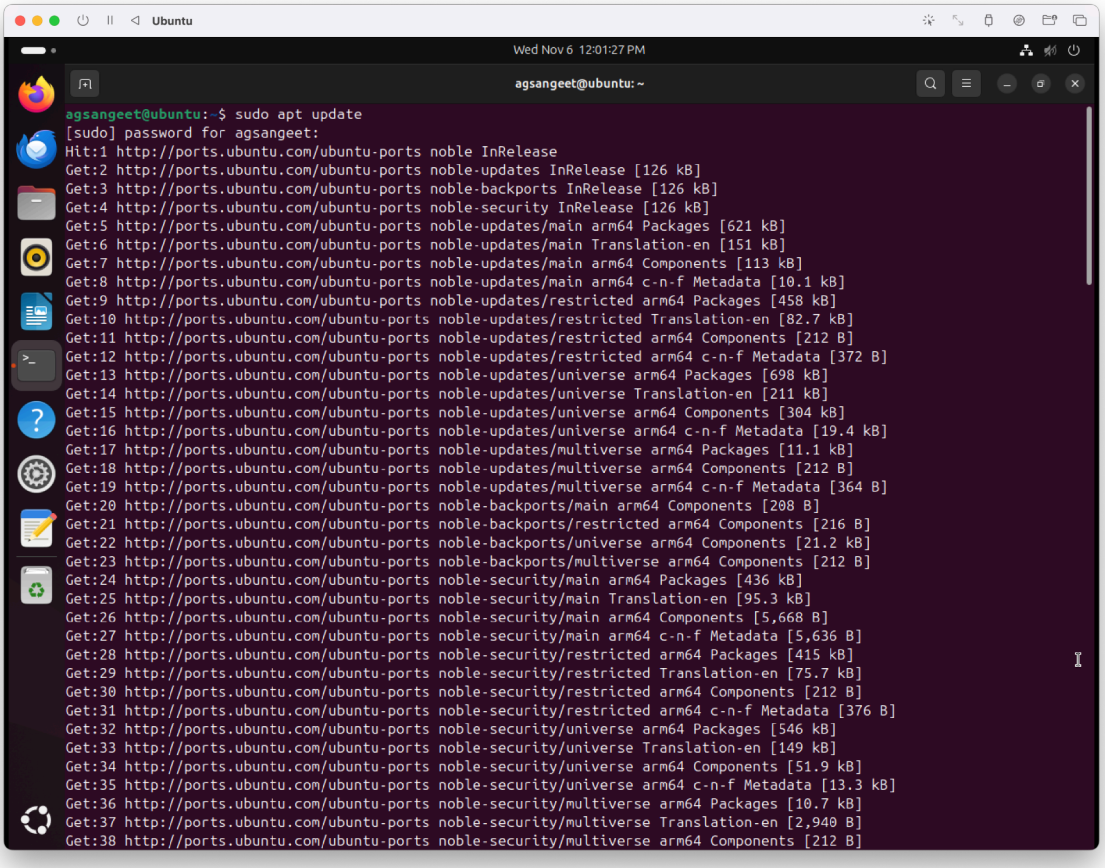
1) What do you mean by Intrusion prevention system (IPS)? How IDS is different than IPS?

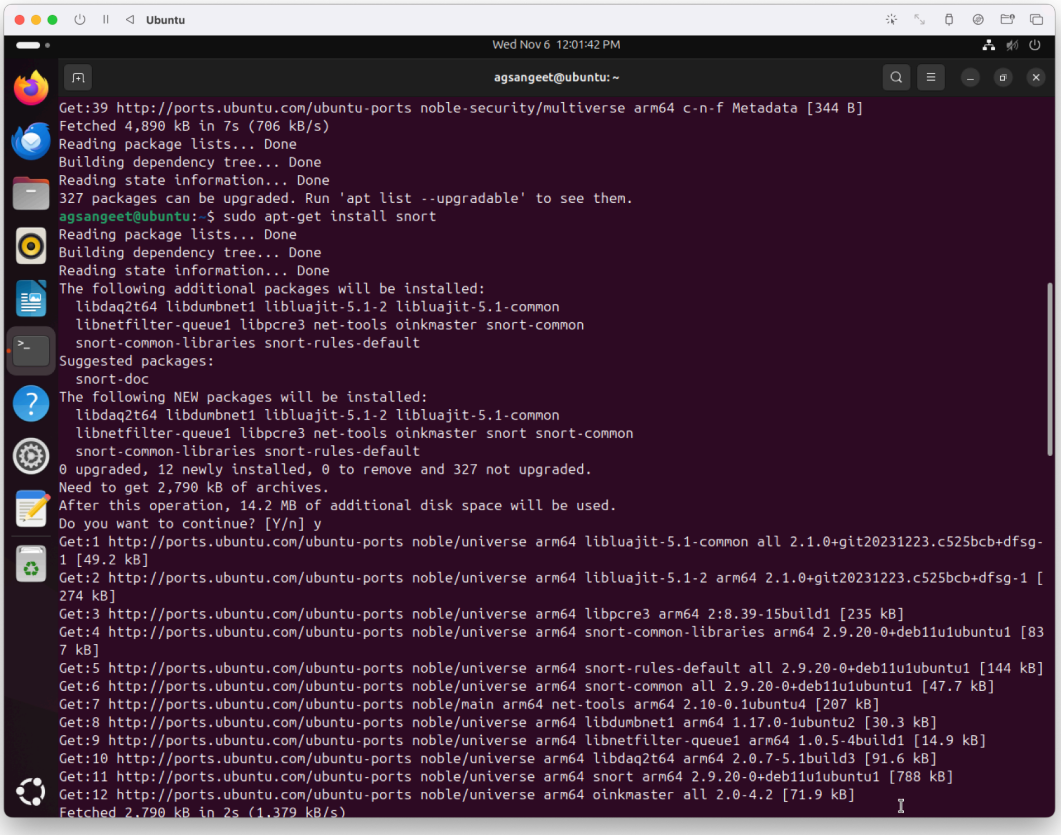
Answer) An Intrusion Prevention System (IPS) is a network security tool designed to detect and prevent potential threats by monitoring traffic and taking action to block attacks in real-time. It actively stops malicious activities by enforcing security policies.

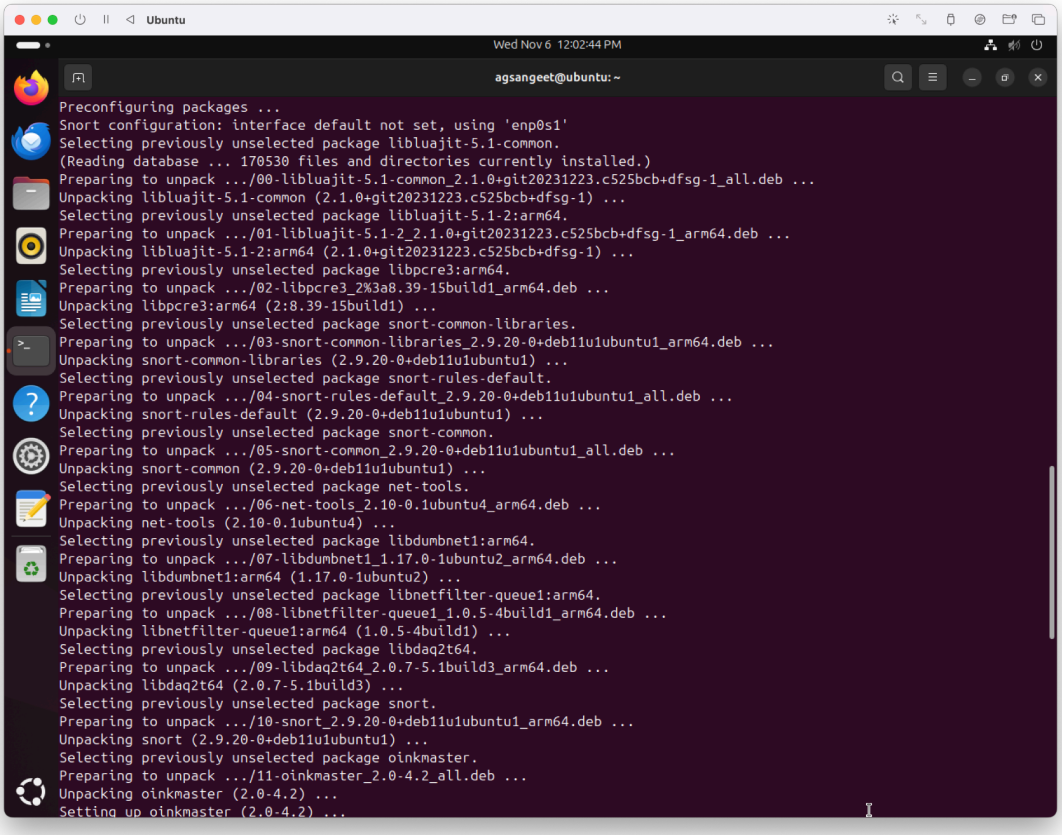
In contrast, an Intrusion Detection System (IDS) only monitors network traffic and alerts administrators to potential threats but does not take direct action to prevent them. IDS is passive, while IPS is proactive in its response to threats.

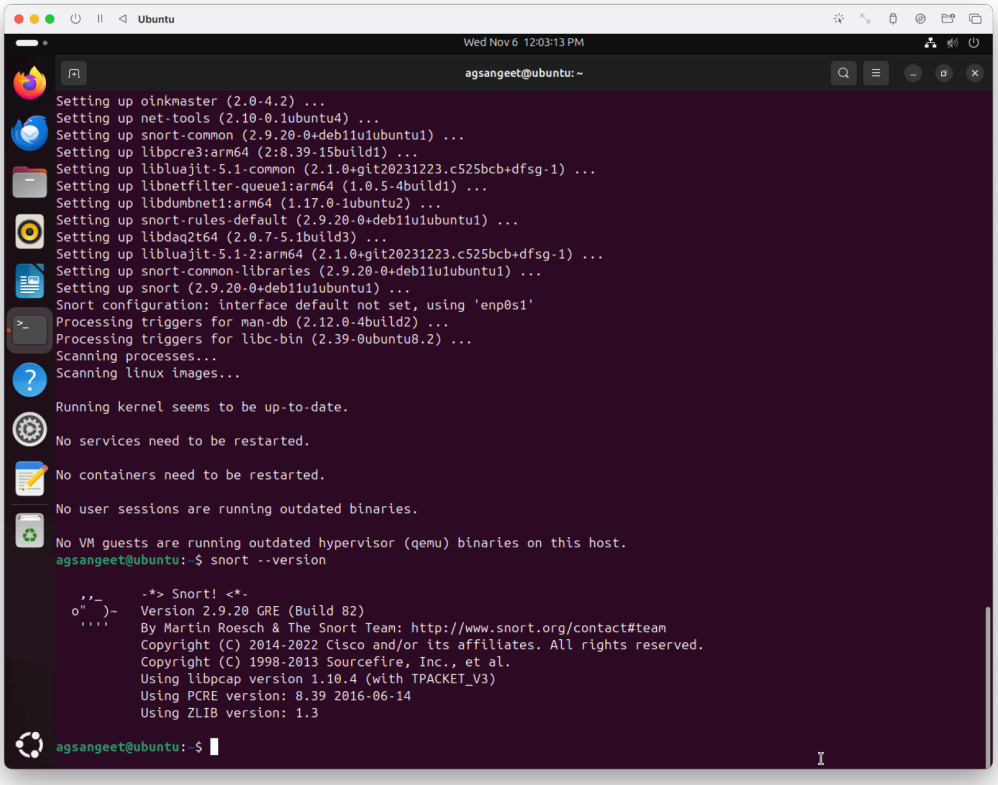
Feature	**IDS (Intrusion Detection System)**	**IDS (Intrusion Detection System)**
Action	Detects and alerts	Detects and blocks
Response	Passive (no direct action)	Active (automatically prevents)
Position in Network	Monitors traffic	Inline with network traffic
Impact on Traffic	No effect on traffic flow	Can impact traffic by blocking threats
Main Purpose	Alert administrators of suspicious activity	Prevent attacks in real-time

2) Configuration and demonstration of Snort

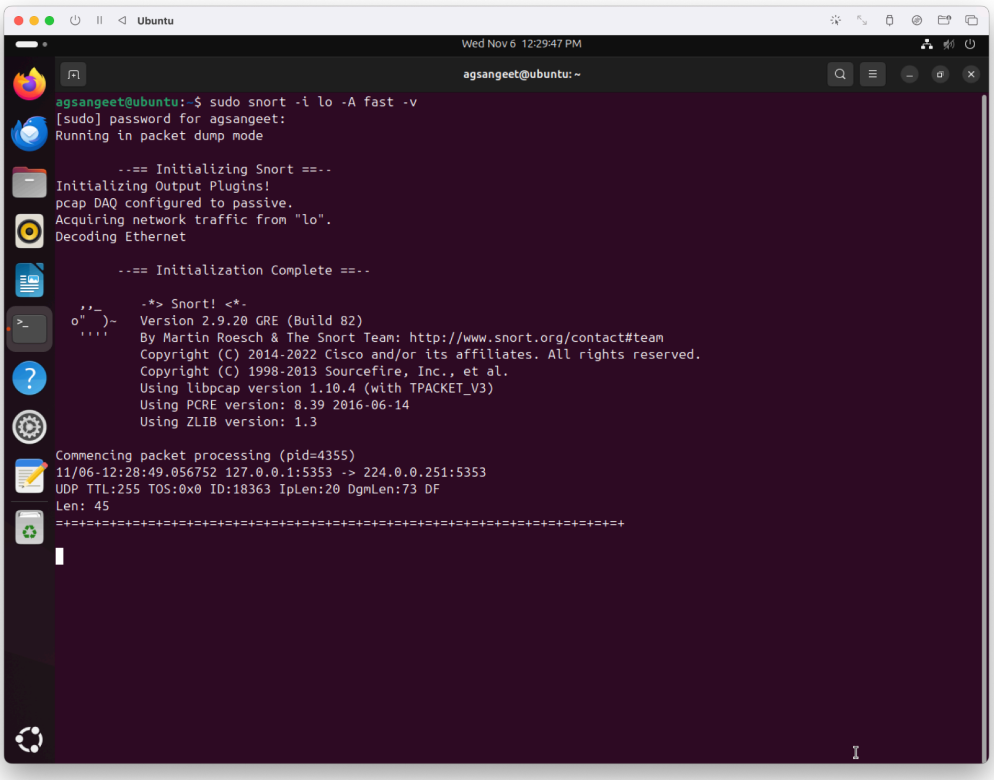



Ubuntu
Wed Nov 6 12:01:42 PM
agsangeet@ubuntu: ~
Get:39 http://ports.ubuntu.com/ubuntu-ports noble-security/multiverse arm64 c-n-f Metadata [344 B]
Fetched 4,890 kB in 7s (706 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
327 packages can be upgraded. Run 'apt list --upgradable' to see them.
agsangeet@ubuntu:~$ sudo apt-get install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
libnetfilter-queue1 libpcre3 net-tools oinkmaster snort-common
snort-common-libraries snort-rules-default
Suggested packages:
snort-doc
The following NEW packages will be installed:
libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
libnetfilter-queue1 libpcre3 net-tools oinkmaster snort snort-common
snort-common-libraries snort-rules-default
0 upgraded, 12 newly installed, 0 to remove and 327 not upgraded.
Need to get 2,790 kB of archives.
After this operation, 14.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libluajit-5.1-common all 2.1.0+git20231223.c525bcb+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.c525bcb+dfsg-1 [274 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libpcre3 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+deb11u1ubuntu1 [837 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 snort-rules-default all 2.9.20-0+deb11u1ubuntu1 [144 kB]
Get:6 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 snort-common all 2.9.20-0+deb11u1ubuntu1 [47.7 kB]
Get:7 http://ports.ubuntu.com/ubuntu-ports noble/main arm64 net-tools arm64 2.10-0.1ubuntu4 [207 kB]
Get:8 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libdumbnet1 arm64 1.17.0-1ubuntu2 [30.3 kB]
Get:9 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libnetfilter-queue1 arm64 1.0.5-4build1 [14.9 kB]
Get:10 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 libdaq2t64 arm64 2.0.7-5.1build3 [91.6 kB]
Get:11 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 snort arm64 2.9.20-0+deb11u1ubuntu1 [788 kB]
Get:12 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 oinkmaster all 2.0-4.2 [71.9 kB]
Fetched 2,790 kB in 2s (1,379 kB/s)


Ubuntu
Wed Nov 6 12:02:44 PM
agsangeet@ubuntu: ~
Preconfiguring packages ...
Snort configuration: interface default not set, using 'enp0s1'
Selecting previously unselected package libluajit-5.1-common.
(Reading database ... 170530 files and directories currently installed.)
Preparing to unpack .../00-libluajit-5.1-common_2.1.0+git20231223.c525bcb+dfsg-1_all.deb ...
Unpacking libluajit-5.1-common (2.1.0+git20231223.c525bcb+dfsg-1) ...
Selecting previously unselected package libluajit-5.1-2:arm64.
Preparing to unpack .../01-libluajit-5.1-2_2.1.0+git20231223.c525bcb+dfsg-1_arm64.deb ...
Unpacking libluajit-5.1-2:arm64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
Selecting previously unselected package libpcre3:arm64.
Preparing to unpack .../02-libpcre3_2%3a8.39-15build1_arm64.deb ...
Unpacking libpcre3:arm64 (2:8.39-15build1) ...
Selecting previously unselected package snort-common-libraries.
Preparing to unpack .../03-snort-common-libraries_2.9.20-0+deb11u1ubuntu1_arm64.deb ...
Unpacking snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../04-snort-rules-default_2.9.20-0+deb11u1ubuntu1_all.deb ...
Unpacking snort-rules-default (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../05-snort-common_2.9.20-0+deb11u1ubuntu1_all.deb ...
Unpacking snort-common (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package net-tools.
Preparing to unpack .../06-net-tools_2.10-0.1ubuntu4_arm64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4) ...
Selecting previously unselected package libdumbnet1:arm64.
Preparing to unpack .../07-libdumbnet1_1.17.0-1ubuntu2_arm64.deb ...
Unpacking libdumbnet1:arm64 (1.17.0-1ubuntu2) ...
Selecting previously unselected package libnetfilter-queue1:arm64.
Preparing to unpack .../08-libnetfilter-queue1_1.0.5-4build1_arm64.deb ...
Unpacking libnetfilter-queue1:arm64 (1.0.5-4build1) ...
Selecting previously unselected package libdaq2t64.
Preparing to unpack .../09-libdaq2t64_2.0.7-5.1build3_arm64.deb ...
Unpacking libdaq2t64 (2.0.7-5.1build3) ...
Selecting previously unselected package snort.
Preparing to unpack .../10-snort_2.9.20-0+deb11u1ubuntu1_arm64.deb ...
Unpacking snort (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../11-oinkmaster_2.0-4.2_all.deb ...
Unpacking oinkmaster (2.0-4.2) ...
Setting up oinkmaster (2.0-4.2) ...



To quickly capture packets and alert on suspicious behaviour: (The process is slow)



Note: Students are suggested to use Linux OS-based tools or free Windows OS-based tools.