Government College of Engineering, Jalgaon
(An Autonomous Institute of Govt. of Maharashtra)

Name: **PRN:**

Class: L.Y **Semester:** VII **Batch:** B

Date of Performance: _____________ **Date of Completion:** ______________

Subject: CO407U CNSL **Subject Teacher:** Ms. Shrutika Mahajan

Practical – 12

Aim: Demonstrate intrusion detection system (IDS) using any tool (snort or any other s/w)

Theory:

1. Introduction:

In today's digital world, network security has become one of the most critical aspects of any organization. With the increasing number of cyber threats, it is essential to have mechanisms that can detect and alert administrators about unauthorized access or suspicious activities.
An Intrusion Detection System (IDS) is a security mechanism designed to monitor network traffic or system activities for malicious actions, policy violations, or intrusions. When such activity is detected, the IDS generates alerts or logs the event for further investigation.
IDS plays a vital role in identifying attacks such as port scanning, Denial of Service (DoS), malware infections, and data breaches. Among the various IDS tools available, Snort is one of the most popular open-source solutions. It performs packet sniffing, real-time analysis, and rule-based attack detection, making it an excellent choice for both academic and enterprise environments.

2. Objective:

To study, configure, and demonstrate the working of an Intrusion Detection System (IDS) using a suitable tool such as Snort, in order to detect unauthorized or suspicious network traffic and generate alerts accordingly.

What is an Intrusion Detection System (IDS)?

An Intrusion Detection System is a security software or hardware that continuously monitors the system or network for malicious activities or policy violations. The primary purpose of IDS is to detect potential attacks in real time and alert the system administrator, helping them take necessary preventive actions.

Types of IDS:

Network-based Intrusion Detection System (NIDS):
Monitors and analyzes network packets transmitted within the network.
It detects suspicious traffic patterns such as port scans, malicious payloads, or protocol misuse.
Example Tools: Snort, Suricata.
Host-based Intrusion Detection System (HIDS):
Installed on individual hosts or servers to monitor file integrity, system calls, and log files.
It detects internal threats or unauthorized changes to the host system.
Example Tools: OSSEC, Tripwire.

Detection Techniques:

Signature-based Detection:
Works like an antivirus, matching network traffic against a database of known attack signatures.
Accurate for known attacks but unable to detect new or modified threats.
Anomaly-based Detection:
Establishes a baseline of normal behavior and flags any deviation from it as suspicious.
Capable of detecting unknown attacks but may generate false positives.
Hybrid Detection:
Combines both signature and anomaly detection to improve detection accuracy and reduce false alarms.

Components of an IDS:

Sensor/Agent: Captures data from the network or host.
Analyzer/Engine: Processes and compares captured data with signatures or normal behavior models.
Database: Stores signatures or rules for known threats.
Alert System: Generates notifications or logs when suspicious activity is detected.
User Interface: Allows administrators to view, analyze, and manage alerts.

Tool Used: Snort

Snort is a widely used open-source Network Intrusion Detection System (NIDS) developed by Cisco. It can analyze network packets in real time and detect a wide variety of attacks and probes. Snort uses a flexible rule-based language to describe traffic patterns and can operate in several modes.

Modes of Operation:

Sniffer Mode: Captures and displays packets in real-time from the network.

Packet Logger Mode: Logs network packets to files for offline analysis.

Network Intrusion Detection Mode: Monitors network traffic against predefined or custom rules and raises alerts on suspicious activity.

Snort Rule Structure:

A Snort rule consists of a header and options.

Syntax:
action protocol source_IP source_port -> destination_IP destination_port (options)

Example:

```
alert tcp any any -> 192.168.1.10 80 (msg:"HTTP GET Request Detected"; content:"GET";
sid:1000001;)
```

Explanation:
alert: Action to take (alert/log/drop)
tcp: Protocol to monitor
any any: Source IP and port
-> 192.168.1.10 80: Destination IP and port
msg: Message displayed in the alert
content: Pattern or string to detect
sid: Snort rule ID (unique identifier for rule)

Procedure / Working Steps:

Install Snort:
Use the following commands to install Snort on a Linux-based system (e.g., Ubuntu):

```
sudo apt update
sudo apt install snort -y
```

Configure Snort:
Edit the configuration file /etc/snort/snort.conf.
Set your local network by updating the HOME_NET variable, e.g.,

```
var HOME_NET 192.168.1.0/24
```

Include your custom rule file, typically local.rules.
Write a Custom Rule:
Open the file /etc/snort/rules/local.rules and add:

```
alert tcp any any -> 192.168.1.10 80 (msg:"HTTP GET Request Detected"; content:"GET";
sid:1000002;)
```

Run Snort in IDS Mode:
Execute the following command to start Snort in alert mode:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

Generate Test Traffic:
Use curl or nmap to generate traffic matching the rule:

```
curl http://192.168.1.10
```

or

```
nmap -sS 192.168.1.10
```

Observe Output:
When Snort detects the matching traffic, it generates an alert similar to:

```
[**] [1:1000002:1] HTTP GET Request Detected [**]
[Classification: Attempted Information Leak] [Priority: 2]
```

Advantages of IDS:

1. Provides early detection of attacks.
2. Helps in identifying vulnerabilities in the network.
3. Logs information for further forensic analysis.
4. Improves overall network security monitoring.

Applications:

1. Monitoring enterprise networks for intrusion attempts.
2. Detecting Denial of Service (DoS) attacks.
3. Protecting servers and databases from unauthorized access.
4. Supporting forensic investigation and incident response.

Conclusion:

An Intrusion Detection System (IDS) like Snort plays a crucial role in maintaining network security by continuously monitoring traffic and detecting malicious patterns based on predefined rules.

Course Teacher
Ms. Shrutika Mahajan