Indian Institute of Technology Jodhpur

Computer Science and Engineering Department

Lab 10

CSL6010 - Cyber Security

Date:03-04-2025 **Marks: 10**

Objective: The objective of this assignment is to install, configure, and test Snort as an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) on Kali Linux.

Task 1: Snort Installation

1. Install Snort on Kali Linux.
2. Verify the installation and check the installed version.

Task 2: Configuring Snort and write Snort Rules

1. Locate and open the Snort configuration file (`snort.conf`).
2. Set the `HOME_NET` variable to match your local network.
3. Ensure that the local rules file is included in the configuration.
4. Create a custom Snort rule to detect ICMP (ping) traffic.
5. Save the rule in the `local.rules` file.

Task 3: Running Snort in IDS Mode

1. Start Snort in IDS mode and monitor network traffic.
2. Generate ICMP traffic and capture alerts in the Snort logs.
3. Verify that the alert is triggered when ICMP traffic is detected.

Task 4: Running Snort in IPS Mode

1. Modify the Snort rule to drop ICMP traffic instead of just detecting it.
2. Run Snort in inline mode to actively block malicious traffic.
3. Configure `iptables` to allow Snort to filter and drop packets.

Task 5: Testing and Logging

1. Test the IPS functionality by generating ICMP traffic.
2. Verify that the ICMP packets are being dropped.
3. View Snort logs to confirm the rule enforcement.