Indian Institute of Technology Jodhpur

Computer Science and Engineering Department

Lab 7

CSL6010 - Cyber Security

Date: 06-03-2025 **Marks: 10**

Aim: Replay Attack

Objective: How to perform a Replay Attack, analyze its effects, and understand how to prevent it.

Requirements

- **Software**: Kali Linux / Ubuntu, Wireshark, Python (Scapy)
- **Tools**: Wireshark, Scapy (Python Library)
- **Networking**: Two networked systems (attacker & victim) or localhost

Overview: A Replay Attack is a type of network attack where an attacker captures valid data packets and resends (replays) them to trick the receiver into believing it's a legitimate message.

Task 1: Understanding Replay Attacks

Task 2: Lab Setup
Install and configure the required software: Wireshark, Python, and Scapy. Set up a testing environment where network packets can be captured and analyzed.

Task 3: Capturing Network Packets
Start Wireshark and capture live network traffic. Generate ICMP packets by using the **ping** command and save the captured packets for further analysis.

Task 4: Performing a Replay Attack
Use Scapy to replay the captured ICMP packets and analyze the impact. Observe how the replayed packets appear in Wireshark and identify any abnormalities.

Task 5: Detecting a Replay Attack
Analyze the Wireshark capture to identify duplicate packets. Write a Python script using Scapy to detect replayed packets by checking for repeated timestamps, sequence numbers, or identical payloads.

Task 6: Preventing Replay Attacks
Research and implement measures to prevent replay attacks. Discuss methods such as timestamps, nonces, and encryption techniques. Modify the replay detection script to log suspicious activity.

Task 7: Submission Requirements

- Screenshots of captured packets in Wireshark.
- Python scripts used for packet replay and detection.
- A report summarizing observations, findings, and suggested preventive measures.