Name:Sakshi Palkar
Roll no:5863
Class:SYBSC CS-A

Task 1

Sniffing Attack

1. What is Sniffing?

A packet analyzer, also known as packet sniffer, protocol analyzer, or network analyzer, is a computer program or computer hardware such as a packet capture appliance that can analyze and log traffic that passes over a computer network or part of a network.[9] Packet capture is the process of intercepting and logging traffic. As data streams flow across the network, the analyzer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

2. Types of Sniffing Attacks

Passive Sniffing: In passive sniffing, attackers eavesdrop on network communications without altering or affecting the traffic. This type of sniffing is stealthy as it doesn't involve actively sending packets into the network.

Active Sniffing: Active sniffing involves the attacker sending specially crafted packets into the network to intercept and capture data. This can be more intrusive and detectable compared to passive sniffing.

ARP Spoofing: Address Resolution Protocol (ARP) spoofing is a type of attack where the attacker sends fake ARP messages to associate their MAC address with the IP address of a legitimate device on the network. This allows the attacker to intercept and modify network traffic.

Man-in-the-Middle (MITM) Attack: MITM attacks involve the attacker positioning themselves between the communication path of two parties, intercepting and possibly altering the data being exchanged.

3. Tools Used for Sniffing Attacks

a. Wireshark: A widely used network protocol analyzer that allows for deep inspection of network traffic.

b. Ettercap: A comprehensive suite for man-in-the-middle attacks, including sniffing

capabilities.

Name:Sakshi Palkar
Roll no:5863
Class:SYBSC CS-A

c. dsniff: A collection of tools for network auditing and penetration testing, including sniffing capabilities.