Modular Man-In-The-Middle (MITM) Attack Guide

Overview

This document provides a step-by-step walkthrough of a Man-In-The-Middle (MITM) attack targeting inter-module traffic, based on the provided theoretical diagram and practical execution logs using Bettercap.

Phase 1: Attack Architecture & Flow

Based on the physical diagram, the attack targets **INTER-MODULE TRAFFIC** and consists of the following components:

- Module A (Sender): The legitimate source of the request.
- Module B (Receiver): The intended destination for the request.
- MITM Attacker (Interceptor Module): The rogue actor positioned between Module A and Module B.

Traffic Flow Details:

1. 1. Intercepted Request: Module A sends a request intended for Module B, but it is intercepted by the MITM Attacker (Sniffing).
2. 2. Modified/Relayed Request: The attacker alters or simply injects malicious data into the request before forwarding it to Module B.
3. 3. Original Response: Module B processes the request and sends the response back, which again goes to the attacker.
4. 4. Modified/Altered Response: The attacker modifies the response before finally relaying it to Module A.

- Key Impacts: Data Integrity is compromised, and Authentication Bypass can occur as indicated in the architecture diagram.

Phase 2: Step-by-Step Execution Using Bettercap

The following commands and steps demonstrate how to practically execute this attack on a network using Kali Linux and the Bettercap tool.

Step 1: Initialize Bettercap on the Network Interface

Launch the tool by binding it to your active wireless interface (e.g., wlan0):

Command: sudo bettercap -iface wlan0

Step 2: Network Reconnaissance (Probing)

Once inside the Bettercap interactive console, turn on network probing to discover devices on the subnet and list them:

Command: net.probe on
Command: net.show

Observation: The logs show endpoints being detected (e.g., Apple, Inc. devices and Android.local) across the 192.168.1.0/24 subnet.

Step 3: Configure ARP Spoofing Target

Specify the IP address of the target machine (Module A or B) that you wish to intercept. In the reference script, the target is 172.20.10.2 (though subnet logs show 192.168.1.x targets actively communicating).

Command: set arp.spoof.targets [TARGET_IP]

Step 4: Execute ARP Spoofing

Activate the ARP spoofing module to trick the target into sending its traffic to the attacker's machine instead of the actual gateway.

Command: arp.spoof on

Note: If the target is offline or not found, Bettercap will output a warning: "arp.spoof could not find spoof targets" as seen in the execution logs.

Step 5: Enable Traffic Sniffing

With the traffic now routing through the attacker's machine, enable the packet sniffer to capture and inspect the data in real-time.

Command: net.sniff on

Observation: The logs show active capture of mDNS traffic (Multicast DNS) and service discovery queries coming from the intercepted endpoints.

Step 6: Stop and Clean Up

To stop the spoofing and restore normal network functionality (healing the ARP tables), terminate Bettercap gracefully.

Action: Press Ctrl+C twice, then 'y' to exit.
