Name: Kunal Goyal
Reg No.: 22BCY10053
Department: CSE (Spl. in Cyber Security & Digital Forensics)
Course: Cyber Security Analyst

Project Title

Who's Watching? Simulating Man-in-the-Middle Attacks Over Public Wi-Fi

Problem Statement / Use Case

In today's digital landscape, public Wi-Fi networks are widely used but often lack proper encryption, making them vulnerable to cyber attacks. One of the most dangerous and commonly exploited threats is the Man-in-the-Middle (MITM) attack, where an attacker intercepts communication between two parties without their knowledge. This poses a significant risk to users accessing sensitive information, such as login credentials, over unsecured networks.

The objective of this project is to simulate a MITM attack in a controlled lab environment to demonstrate how attackers can intercept unencrypted HTTP traffic and retrieve sensitive data from unsuspecting users. By using tools such as Ettercap, arpspoof, and Wireshark, this simulation aims to highlight the risks associated with insecure public Wi-Fi networks and emphasize the importance of secure web protocols (HTTPS), VPNs, and user awareness as countermeasures.

Project Objective(s)

The objective of this project is to **simulate a Man-in-the-Middle (MITM) attack** on a public Wi-Fi network in a controlled environment to:

1. **Demonstrate how attackers can intercept unencrypted HTTP traffic** and capture sensitive user information such as login credentials.
2. **Use tools like Ettercap, arpspoof, and Wireshark** to perform and analyze the attack.
3. **Simulate real-world public Wi-Fi scenarios** where users unknowingly connect to insecure networks.
4. **Highlight the differences in security between HTTP and HTTPS traffic** and show how encrypted communication can prevent data interception.
5. **Raise awareness about the risks of using public Wi-Fi without proper security measures**.
6. **Showcase effective defense mechanisms**, including HTTPS, VPN usage, browser certificate validation, and MITM detection tools.

7. Provide **practical insights and security recommendations** to users and organizations to mitigate MITM risks.

Tools and Technologies

Tools Used:

1. **Kali Linux**
   A specialized Linux distribution used for penetration testing and security auditing. It includes all the required MITM tools pre-installed.
2. **Ettercap**
   A comprehensive suite for man-in-the-middle attacks on LAN. Used for sniffing live connections, performing ARP poisoning, and intercepting data.
3. **arpspoof**
   A command-line tool from the dsniff suite used to perform ARP spoofing and redirect network traffic through the attacker's machine.
4. **Wireshark**
   A powerful network protocol analyzer used to capture and inspect packets in real-time. Essential for analyzing HTTP requests and identifying captured credentials.
5. **Python HTTP Server / Apache2**
   Used to host a fake login page over HTTP, simulating insecure web services often used on public networks.
6. **Victim Machine (Windows/Linux/Android Emulator)**
   Simulates a regular user connecting to an open network and attempting to log in to an insecure website.

Techniques Applied:

1. **ARP Spoofing / Poisoning**
   A technique used to associate the attacker's MAC address with the IP address of the victim's gateway. This reroutes network traffic through the attacker.
2. **Man-in-the-Middle Attack Simulation**
   Intercepting data between the victim and the web server without the victim's knowledge, allowing sensitive data like login credentials to be captured.
3. **Traffic Sniffing and Analysis**
   Capturing HTTP packets using Wireshark to examine the structure of data being transmitted, focusing on POST requests and login information.
4. **Fake Webpage Hosting**
   A custom HTML login form is hosted to simulate a real login page, encouraging the victim to enter credentials over HTTP.
5. **Comparison Analysis (HTTP vs HTTPS)**
   Demonstrating the vulnerability of HTTP and the protection offered by HTTPS by attempting to intercept both and observing the differences in data visibility.
6. **Defense Mechanism Demonstration**
   Simulating the use of VPNs, HTTPS, and browser security features to highlight how users can protect themselves from MITM attacks.

Methodology / Approach

The project was carried out in a controlled lab setup using the following structured approach:

1. Environment Setup

- Configured two machines: one as the **attacker (Kali Linux)** and the other as the **victim**.
- Both devices were connected to the same local network to simulate a public Wi-Fi scenario.

2. Hosting a Vulnerable Web Page

- A fake **HTTP login page** was hosted using a simple Python HTTP server or Apache.
- The victim accessed this page assuming it was a legitimate site.

3. Executing the MITM Attack

- **ARP spoofing** was performed using arpspoof to redirect the victim's traffic through the attacker's machine.
- **Ettercap** and **Wireshark** were used to sniff and capture the unencrypted HTTP traffic.

4. Analyzing Captured Data

- Extracted sensitive data like **usernames and passwords** from intercepted HTTP POST requests.
- Compared results for **HTTP vs HTTPS** to show the effectiveness of encryption.

5. Demonstrating Countermeasures

- Tested the effect of **VPNs and HTTPS** in preventing MITM attacks.
- Highlighted **browser security warnings** and certificate validation as additional safeguards.

Innovation & Uniqueness

1. **Realistic Public Wi-Fi Scenario Simulation**
   The project simulates a real-world public Wi-Fi environment, such as a coffee shop or airport network. This helps demonstrate how easily users can become targets of a MITM attack when connected to unsecured networks.

2. **Complete Attack Lifecycle Demonstration**
   Rather than focusing on a single tool or step, the project covers the entire MITM process—from network setup and ARP spoofing to data interception and analysis—providing a comprehensive understanding of the threat.

3. **Comparative Analysis of Security Measures**
   The project includes a side-by-side comparison of data visibility over HTTP, HTTPS, and VPN connections. This highlights how different levels of security affect the success of a MITM attack.

4. **Custom Fake Login Page Integration**
   A dummy HTTP login page was created to simulate a real-world phishing

scenario. This shows how attackers combine social engineering with MITM to steal credentials.

5. **Emphasis on Countermeasures and User Awareness**
   The simulation is not limited to the attack itself. It also demonstrates effective defense mechanisms such as HTTPS usage, VPNs, browser certificate validation, and ARP spoofing detection techniques.

6. **Educational Focus with Visual Support**
   The project includes clear screenshots of intercepted traffic, attack flow diagrams, and packet analysis results using Wireshark. These visuals enhance understanding and make the project suitable for educational and awareness purposes.

Relevance to Cybersecurity Field

The Man-in-the-Middle (MITM) attack simulation is highly relevant to cybersecurity as it demonstrates a common and critical vulnerability in unsecured communication networks.

1. **Real-World Threat Simulation**: MITM attacks are widely used to steal sensitive data, highlighting the importance of securing communication channels.

2. **Emphasis on Secure Protocols**: By intercepting HTTP traffic, the project emphasizes the necessity of HTTPS and SSL/TLS for securing data in transit.

3. **Promotes Security Best Practices**: The simulation educates about the dangers of public Wi-Fi and the need for VPNs, encrypted communication, and network monitoring.

4. **Practical Application**: This project is valuable for penetration testers, network admins, and security professionals to understand both attack and defense strategies.

5. **Supports Cybersecurity Training**: The project serves as an effective learning tool for understanding real-world network-based attacks and defenses.

Expected Deliverables

Project Report:

A comprehensive document detailing the entire project, including:

- Introduction and background on MITM attacks.
- Step-by-step methodology of the attack simulation.
- Analysis of captured data.
- Comparison of HTTP, HTTPS, and VPN security.

Live Demonstration:

A working demonstration of the MITM attack, showcasing the interception of HTTP traffic, credential capture, and comparison of security mechanisms (HTTP, HTTPS, VPN).

Network Diagram:

A visual representation of the network setup, illustrating the attacker, victim, and communication flow during the MITM attack.

Screenshots and Packet Captures:

Screenshots from Wireshark and Ettercap showing captured HTTP credentials and other relevant network traffic.

Mitigation Recommendations:

A section outlining preventive measures against MITM attacks, including the use of HTTPS, VPNs, and user education.

Presentation Slides:

A summary of the project with key findings, diagrams, and results for presentation to an audience or evaluators.