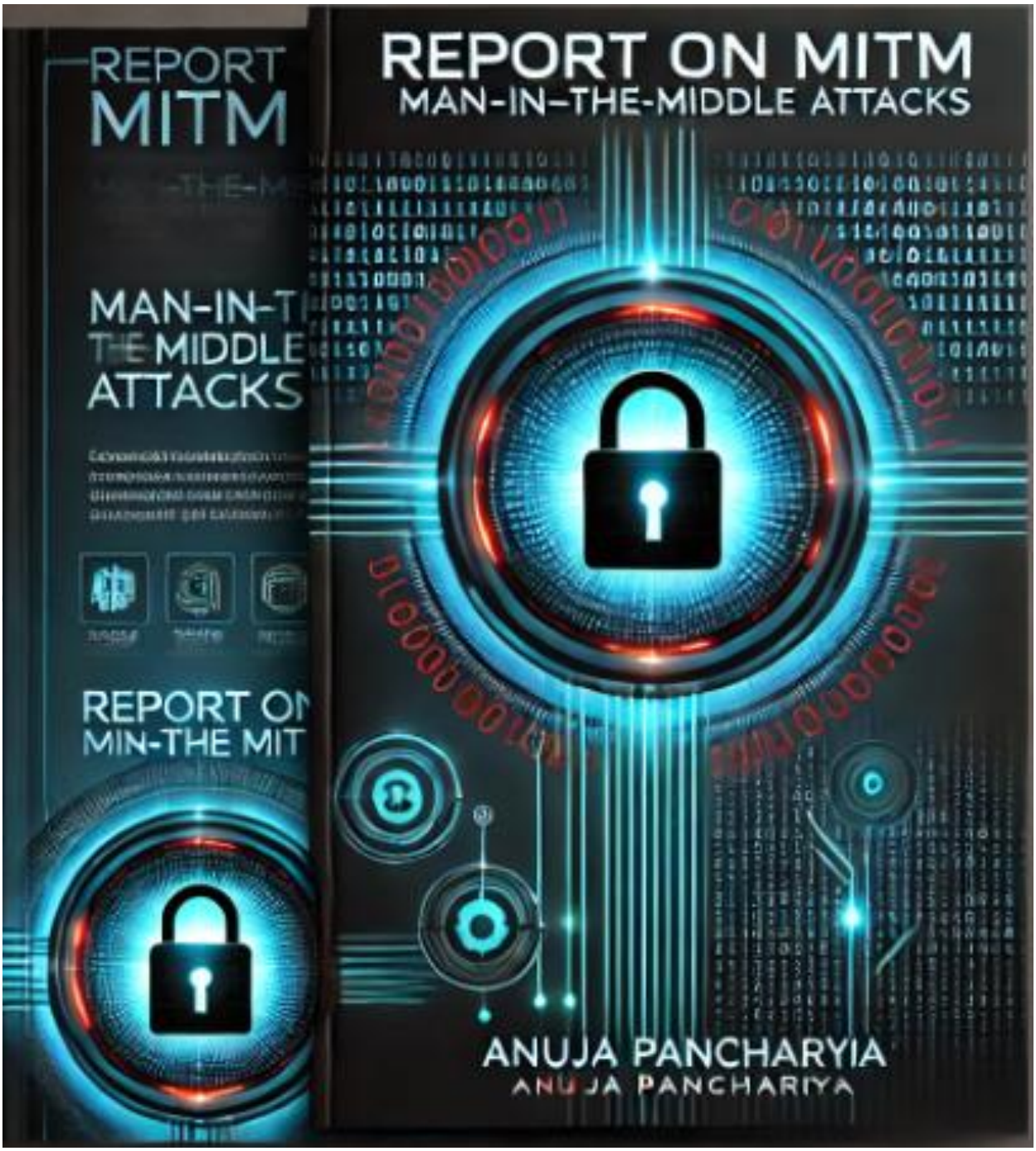
Report on MITM



Man-In-The-Middle (MITM) Attack Report

Introduction

A Man-In-The-Middle (MITM) attack is a cybersecurity threat where an attacker secretly intercepts and potentially alters communication between two parties. These attacks exploit vulnerabilities in communication channels, enabling attackers to steal sensitive information such as credentials, financial details, or confidential data. MITM attacks pose a significant risk in both personal and corporate environments.

Tool Used: Ettercap

Ettercap is a powerful network security tool designed for MITM attacks and network monitoring. It supports both active and passive dissection of numerous network protocols, providing functionalities for injecting and analyzing network traffic.

Steps Demonstrated Using Ettercap

1. Initiating Ettercap

- Ettercap was launched using the `ettercap -G` command to open the graphical interface.

2. Host Discovery:

- Ettercap scanned the network and listed available devices (hosts) along with their IP and MAC addresses. The target list was created from the identified hosts.

3. Target Selection:

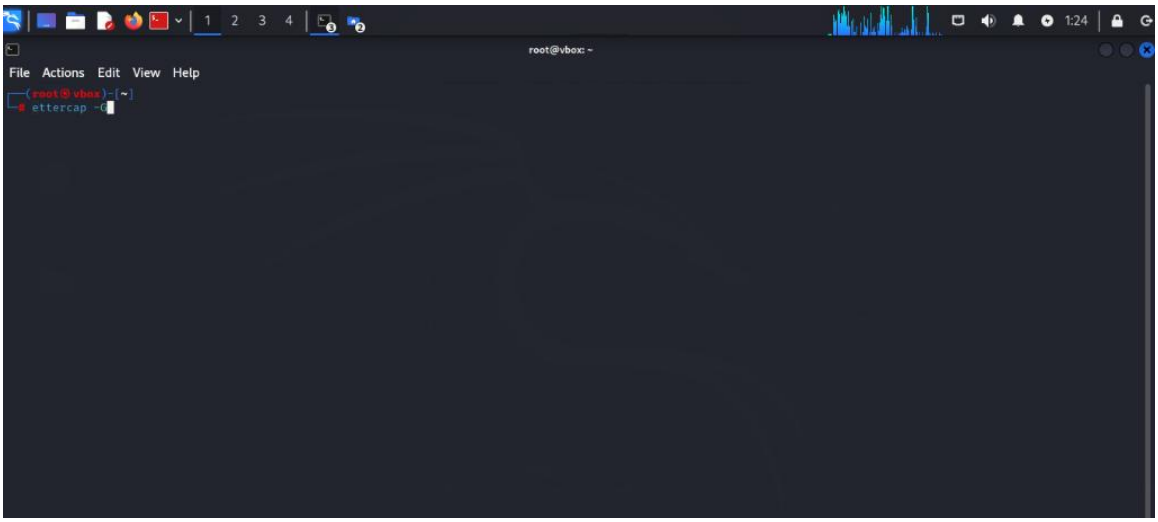
- Two groups were defined: one representing the victim and the other representing the gateway or other network users. Specific details like IP `192.168.0.102` were selected as the victim host.

4. Credential Interception:

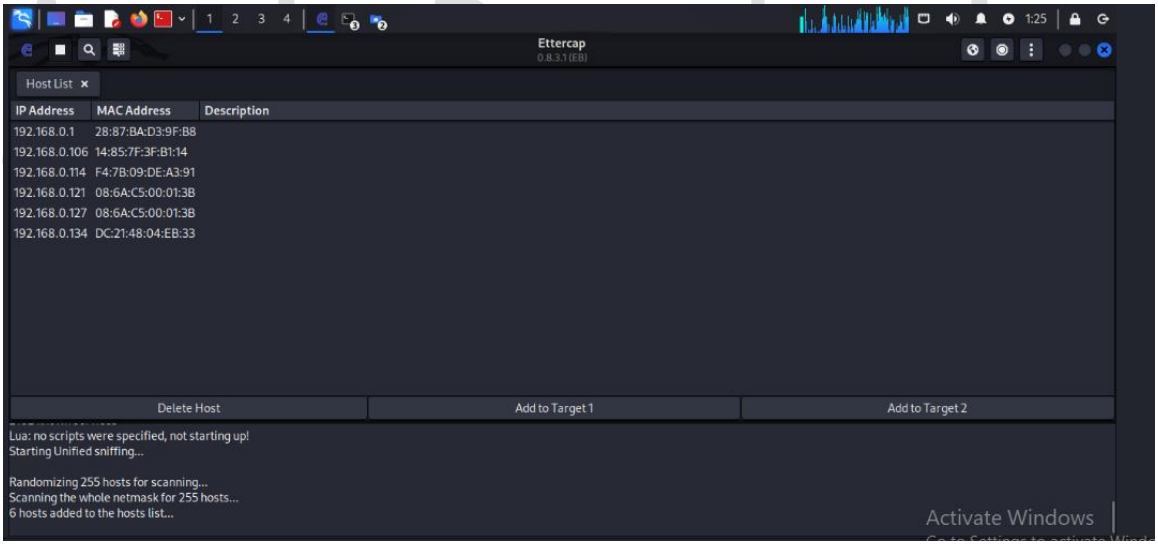
- The MITM attack successfully intercepted HTTP traffic from the victim. Credentials for a login form (`username: admin, password: admin`) were captured during the session.

Output :

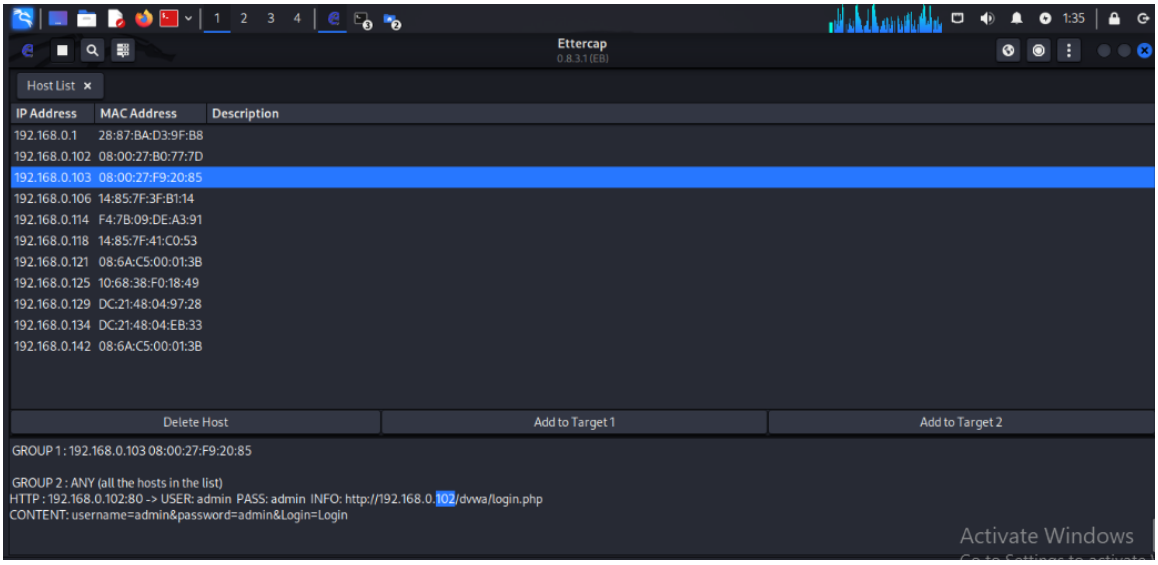
- Open Ettercap



- Scan the host



- Add the target and you have successfully done the MITM Attack



Mitigation Strategies

Organizations and individuals can defend against MITM attacks through the following methods:

1. Encryption:

- Use HTTPS for secure web communication. Encryption ensures intercepted traffic is unreadable without proper decryption keys.

2. Network Security Measures:

- Deploy secure Wi-Fi protocols (e.g., WPA3)
- Regularly monitor and audit network traffic for anomalies.

3. User Awareness:

- Educate users about phishing attacks and the importance of avoiding untrusted networks.

4. Tools and Technology:

- Utilize security tools like firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs) to protect communication.

Conclusion

The demonstration using Ettercap effectively highlights the risks associated with MITM attacks. From intercepting credentials to monitoring network activity, attackers can exploit unprotected channels to compromise sensitive data. Therefore, adopting robust cybersecurity practices is critical to safeguarding networks.

This report aims to provide a comprehensive understanding of MITM attacks and practical insights for mitigating these threats. For organizations, addressing such vulnerabilities is not just a technical necessity but a strategic imperative to ensure resilience against evolving cyber threats.