Man-in-the-Middle Attack via ARP Poisoning

Internship Project Report

Submitted by: Suhani Saini

Internship Institute: IIT Jammu

Mentor: Mr. Ankit Pulkit

Abstract

- This project demonstrates a Man-in-the-Middle (MITM) attack using ARP poisoning.
- Tools used: Kali Linux and Ettercap.
- Goal: Show how attackers intercept traffic and capture sensitive information.
- Captured credentials (username/password) show risks of insecure networks.

Introduction

- ARP maps IP addresses to MAC addresses in a network.
- It is unauthenticated and hence vulnerable to spoofing.
- In ARP poisoning, forged ARP replies trick devices into misrouting traffic.
- This allows attackers to perform MITM attacks and sniff sensitive data.

Tools & Environment Setup

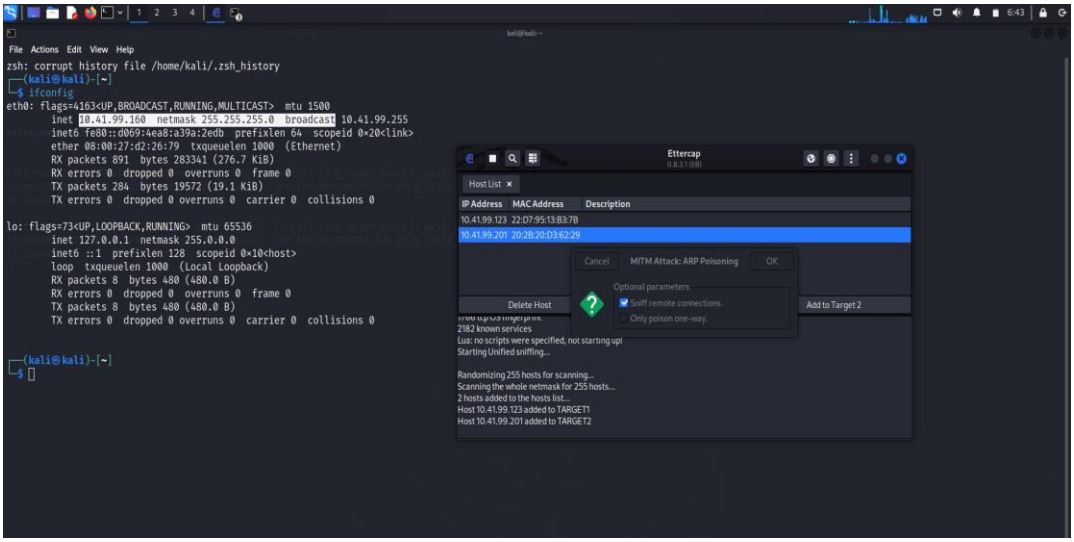
- Operating System: Kali Linux
- Tool: Ettercap (GUI mode)
- Network Interface: eth0
- Configuration: Enabled IP forwarding
- Method: Host scan, victim/gateway selection, ARP poisoning

Methodology

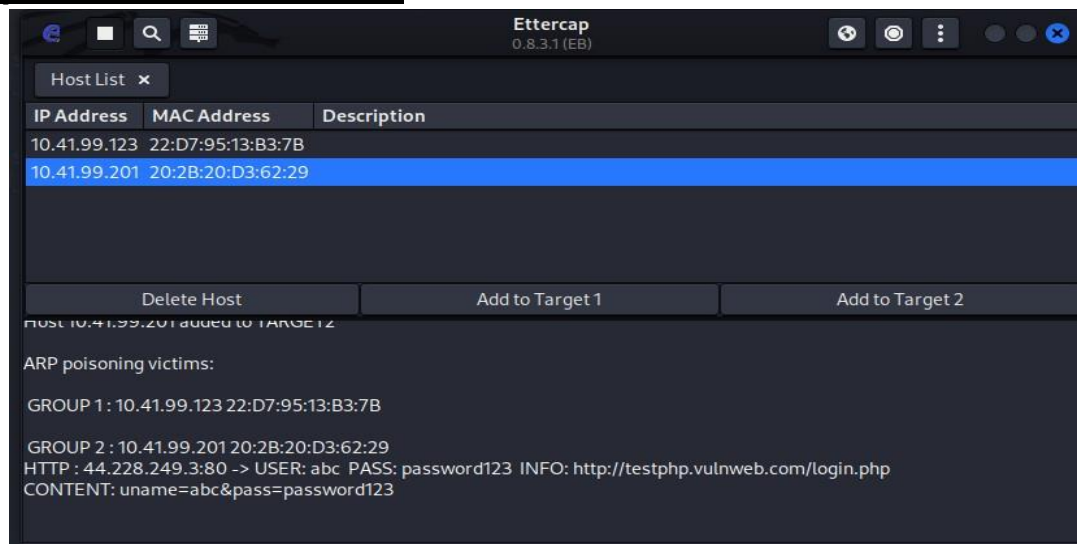
- Launch Ettercap GUI: `sudo ettercap -G`
- Select network interface (eth0).

- Scan network to discover hosts.
- Add victim to TARGET1, gateway to TARGET2.
- Start ARP poisoning with 'Sniff remote connections'.
- Capture credentials from intercepted traffic.

Experiment Screenshot 1



Experiment Screenshot 2



Results & Analysis

- ARP poisoning was successful in intercepting traffic.

- Captured sensitive login credentials over HTTP.
- Demonstrated the weakness of plaintext communications.
- Confirmed ARP's vulnerability in local networks.

Mitigation & Countermeasures

- Use HTTPS for secure communications.
- Implement static ARP entries or monitoring tools (ArpON).
- Enable client isolation in Wi-Fi networks.
- Deploy IDS/IPS to detect suspicious ARP traffic.
- Educate users about insecure networks.

Conclusion

- ARP poisoning can easily launch MITM attacks.
- Credentials transmitted over HTTP were intercepted.
- Secure protocols (HTTPS) and monitoring are crucial.
- Network admins must deploy proactive defenses.

References

- Ettercap Official Documentation
- Wikipedia: ARP Spoofing, MITM Attack
- Kali Linux Tools Documentation
- Research papers on ARP security mitigation