Network Protocol Attacks Lab

Executive Summary

This lab focused on demonstrating how insecure network protocols can be compromised through Man-in-the-Middle (MITM) techniques. By placing the attacker between the victim and the gateway using ARP spoofing, real-time network traffic was intercepted and analyzed. The use of Responder enabled authentication poisoning and NTLM hash capture while Wireshark revealed plaintext credentials from FTP, Telnet, and HTTP sessions. DNS spoofing further redirected victim requests to attacker-controlled assets, proving how easily unencrypted protocols can be manipulated.

The experiment highlights major risks associated with legacy services and emphasizes the need for encrypted communication, secure protocol implementation, and defensive network configurations. The findings reflect real-world attack feasibility, reaffirming why modern security standards must replace outdated infrastructures.

1. Overview

This lab demonstrates the practical execution of Network Protocol Attacks focusing on MITM (Man-in-the-Middle) within a controlled environment. Using Kali Linux as the attacker and Metasploitable2 as the victim host, ARP poisoning was used to intercept and manipulate network traffic. The attack leveraged weaknesses in legacy and insecure protocols, enabling credential harvesting and authentication interception.

The experiment further validates how services such as FTP, Telnet, and HTTP transmit sensitive data in plaintext, making them highly vulnerable during real-time network interception.

2. Lab Environment

Component	**IP Address**
Attacker (Kali Linux)	192.168.0.9
Target (Metasploitable2)	192.168.0.14
Network Gateway	192.168.0.1

Local LAN environment ensured no external interference — ideal for controlled exploitation and packet-analysis tasks.

3. Tools Used

Tool	Usage in Lab
Responder	Captured NTLMv1/v2 authentication requests via LLMNR/NBT-NS poisoning
Ettercap	ARP Spoofing to enable MITM + DNS redirection
Wireshark	Packet inspection, credential extraction, protocol analysis
Telnet, FTP, HTTP Browser	Used to generate insecure traffic for sniffing
Tool	**Usage in Lab**

4. Attack Execution Walk-Through

1. **Network Scanning & Host Identification**
    - Attacker identified the victim device using nmap/network discovery.
    - Verified active IP addresses within subnet 192.168.0.0/24.
2. **Responder Deployment for Hash Capture**
    - LLMNR/NBT-NS poisoning enabled.
    - Victim broadcast requests were answered by attacker machine.
    - NTLM hashes successfully captured from SMB authentication failures.
3. **ARP Spoofing using Ettercap**
    - Attacker poisoned ARP tables of victim and gateway.
    - Network flow from victim was transparently routed through attacker.
4. **DNS Spoofing Redirection**
    - Victim DNS queries were spoofed.
    - Domain resolution forcibly redirected to Kali-hosted IP.
5. **Packet Sniffing & Credential Interception**
    - Wireshark captured **clear-text login credentials** for Telnet, FTP, and HTTP.
    - Example proof: USER msfadmin / PASS msfadmin.
    - Demonstrated real impact of insecure protocol usage.

5. Captured Evidence Summary

ID	Attack Technique	Impact
015	SMB Poisoning (Responder)	NTLM Hash captured
016	ARP MITM	Complete traffic visibility
017	DNS Spoofing	Redirected traffic to attacker asset
018	Packet Sniffing	Credentials exposed in plaintext

6. Evidence Extract (Wireshark)

USER msfadmin

PASS msfadmin

GET /dvwa/login.php HTTP/1.1

Host: 192.168.0.14

Insecure protocols leaked login information without any encryption mechanism.

7. MITM Attack Using Ettercap

In this lab, Ettercap was used to perform an ARP spoofing-based Man-in-the-Middle attack, where the attacker falsified ARP responses to position their machine between the victim and the gateway. Once the spoofing was successful, all incoming and outgoing packets from the target flowed through the attacker, enabling real-time traffic interception and monitoring. With this MITM setup, it was possible to view credentials sent over insecure services such as FTP, HTTP, and Telnet directly in plaintext using Wireshark. This attack clearly demonstrated how simple network manipulation can compromise data confidentiality when encryption is absent, making ARP spoofing one of the most practical and effective MITM techniques in unsecured networks.

8. Conclusion

During the MITM attack simulation, the attacker successfully positioned themselves between the victim and gateway using ARP spoofing. Once traffic began passing through the attacker machine, various insecure protocols were intercepted, revealing clear-text credentials, session data, and authentication attempts.

This lab highlights how legacy and unencrypted services are extremely vulnerable in a switched network environment. Even without exploiting application-level vulnerabilities, network-level interception was enough to compromise accounts and hijack communication.

In a real-world scenario, this could lead to:

- Unauthorized network access
- Credential theft and privilege escalation
- Data manipulation or redirection
- Internal reconnaissance and lateral movement
- Complete network compromise if left unchecked

The attack demonstrates that network security is only as strong as the protocols running within it, making encryption, monitoring, and network segmentation crucial.

9. Security Recommendations (Mitigation & Prevention)

To defend against attacks like MITM, ARP spoofing, and credential sniffing, organizations should implement the following:

A. Replace Insecure Protocols

❌ Disable **FTP, Telnet, and HTTP**

✔ Use **SSH, SFTP, FTPS, HTTPS** instead

B. Implement Network-Level Protections

- Enable **Dynamic ARP Inspection (DAI)** on switches
- Use **Port Security, DHCP Snooping & VLAN segmentation**
- Configure **static ARP entries** on critical servers
- Apply **802.1X network authentication**

C. Encrypt All Communication

- Force TLS/SSL for all internal and external traffic
- Deploy **HSTS + certificate pinning** where possible

D. Harden DNS & Authentication

- Use **DNSSEC** to prevent DNS spoofing
- Disable **LLMNR & NBT-NS** on Windows environments
- Implement **Kerberos or multi-factor authentication**

E. Monitoring & Detection

- Run **IDS/IPS tools** to detect spoofing attempts
- Enable **Syslog logs for authentication monitoring**
- Use **Wireshark/Tcpdump periodically for traffic audit**

F. User & Policy Controls

- Conduct employee awareness training
- Least privilege access enforcement
- Scheduled credential rotation

Final Statement

This lab reinforces that network protocol security is critical in preventing MITM attacks. With proper encryption, network segmentation, and traffic monitoring, these attacks can be stopped before exploitation. The experiment provides clear evidence of why organizations must migrate away from legacy protocols and enforce modern secure communication standards.