# Network Protocol Attacks and Credential Interception Using MitM Techniques

**Intern name:** Cinchana S
**Date:** 23-01-2026

## Introduction

The objective of this task was to perform network protocol attacks by intercepting traffic and abusing insecure name-resolution mechanisms. The engagement focused on Man-in-the-Middle attacks, NTLM authentication capture, and traffic analysis using Responder, Ettercap, and Wireshark. The target system was a Windows virtual machine within a controlled lab environment.

## Tools

**Wireshark** was started to monitor baseline traffic. **Ettercap** was used to identify active hosts on the local network. The **Windows system** and **gateway** were confirmed as valid targets. **Responder** was configured to listen for name-resolution and authentication requests.

**Tools initialized:**

- wireshark
- ettercap -G
- responder -I eth1

## Threat Modeling

Windows systems relying on broadcast-based name resolution protocols such as LLMNR and NBNS are vulnerable to spoofing attacks. When combined with ARP spoofing or passive listening, attackers can coerce SMB authentication attempts and capture NTLM hashes without user awareness.

## Vulnerability Analysis Log

| Attack ID | Technique | Target | Status | Outcome |
|---|---|---|---|---|
| 001 | ARP Spoofing (MitM) | Windows VM (192.168.56.101) | Success | Traffic Intercepted |
| 002 | LLMNR / NBNS Poisoning | Windows VM (192.168.56.101) | Success | NTLMv2 Hash Captured |
| 003 | SMB Authentication Abuse | Windows VM (192.168.56.101) | Success | NTLMv2 Credentials Logged |

DNS spoofing was not observed. Due to the network configuration, Windows relied on LLMNR/NBNS, which was successfully exploited instead.

## Exploitation

### Man-in-the-Middle via ARP Spoofing (Ettercap)

Steps performed (GUI):

- Sniff → Unified sniffing → eth1
- Hosts → Scan for hosts
- Hosts → Hosts list
- Targets → Target 1 → Windows IP
- Targets → Target 2 → Gateway IP
- Mitm → ARP poisoning → Sniff remote connections

**Result observed:**
ARP poisoning victims:
GROUP 1 : 192.168.56.101
GROUP 2 : 192.168.56.1
This confirmed successful MitM positioning.

### NTLM Capture via Responder (LLMNR/NBNS)

Responder was started to poison name-resolution requests and listen for authentication attempts.

Command:
*responder -I eth1*

**Observed Responder output :**

- LLMNR poisoned responses
- SMB authentication attempts
- NTLMv2 hashes captured

**Example evidence:**
[SMB] NTLMv2-SSP Username : DESKTOP-SHOKHOE\cinchu
[SMB] NTLMv2-SSP Hash : cinchu::DESKTOP-SHOKHOE:...

Multiple authentication attempts were captured, confirming successful exploitation.

## Traffic Analysis using Wireshark

Wireshark confirmed:

- Continuous ARP spoofing packets
- LLMNR and NBNS broadcast traffic
- SMB authentication packets corresponding to Responder logs

This validated the attack chain end-to-end.

## Post-Exploitation

Captured NTLMv2 hashes could be used for offline password cracking or relay attacks in real-world environments.

## Remediation Recommendations

- Disable LLMNR and NBNS on Windows systems
- Enforce secure DNS resolution
- Enable SMB signing
- Monitor for ARP spoofing activity
- Apply network segmentation and endpoint hardening

## Summary

A man-in-the-middle attack was conducted using Ettercap to intercept traffic between a Windows host and the gateway. Responder exploited LLMNR and NBNS name-resolution protocols to capture NTLMv2 hashes. Wireshark confirmed ARP spoofing and authentication traffic, demonstrating credential exposure risks