# Network Protocol Attacks Lab

Author: Harshal Harekar

Date: 30/10/2025

## Objective

* Capture NTLMv2 hashes via SMB relay attack.
* Intercept and manipulate traffic between victim and gateway using ARP Spoofing via Ettercap
* Traffic Analysis with Wireshark

## Tools

Responder, Ettercap, Wireshark

## 1. SMB Relay with Responder

### Steps

1. Start Responder on Kali:

*sudo responder -I eth0 -wd*

A screenshot of a computer

AI-generated content may be incorrect.

2. Wait for the target to initiate an SMB connection

A screenshot of a computer

AI-generated content may be incorrect.

3. Responder captures and logs NTLMv2 hashes.

A screenshot of a computer

AI-generated content may be incorrect.

## Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack ID | Technique | Target IP | Status | Outcome |
| 001 | SMB Relay | 192.168.18.132 | Success | NTLMv2 Hash |

## 2. MitM : ARP Spoofing with Ettercap

### Steps

1. Launch Ettercap in GUI or CLI:

*sudo ettercap -G*

A screenshot of a computer

AI-generated content may be incorrect.

2. Select targets: victim IP and gateway IP

A screenshot of a computer

AI-generated content may be incorrect.

3. Start ARP poisoning and Start Sniffing

4. In wireshark, we can see the source ip of windows vm

A screenshot of a computer

AI-generated content may be incorrect.

## 3. Traffic Analysis with Wireshark

### Steps

1. Open Wireshark and start capture on eth0

A screenshot of a computer

AI-generated content may be incorrect.

2. Filter for: smb / dns / http / ntlmssp / arp

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.