



---

## Network Protocol Attacks Lab

**Intern:** Radha Singh

**Assessment date:** 27/2/2026

**Environment:** Kali VM (192.168.75.128) attacking Metasploitable2 VM (192.168.75.129)

---

### 1. Executive Summary

This lab demonstrates practical exploitation of insecure network protocols through **Man-in-the-Middle (MitM)** techniques. Using **Responder**, **Ettcap**, and **Wireshark**, the attacker successfully intercepted authentication traffic, relayed SMB credentials, and analyzed sensitive network packets. The exercise highlights how weak protocol configurations and trust assumptions can lead to credential disclosure and session compromise.

---

### 2. Objective

The primary objective of this lab was to simulate real-world network-level attacks by abusing legacy authentication mechanisms and insecure traffic flows. The goals included:

- Capturing NTLM hashes via SMB relay
  - Performing ARP spoofing to establish MitM positioning
  - Intercepting and analyzing live traffic for sensitive data leakage
  - Documenting technical findings and security implications
- 

### 3. Tools & Methodology

Tool	Purpose
<b>Responder</b>	Capture NTLM hashes via SMB/LLMNR/NBT-NS poisoning
<b>Ettcap</b>	Conduct ARP spoofing and traffic interception
<b>Wireshark</b>	Deep packet inspection and protocol analysis

---

### 4. Attack Simulation – SMB Relay using Responder

#### Attack Overview

SMB relay attacks exploit the **NTLM authentication protocol**, which relies on challenge-response mechanisms rather than mutual authentication. By poisoning name resolution traffic, the attacker tricks the victim into authenticating against a rogue SMB server.

#### Execution Steps

1. Responder was launched on the Kali VM interface connected to the target network.
  2. LLMNR and NBT-NS poisoning were enabled.
  3. The victim system attempted SMB authentication.
  4. NTLM credentials were captured successfully.
-



1.  $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

To kill this script hit CTRL-C

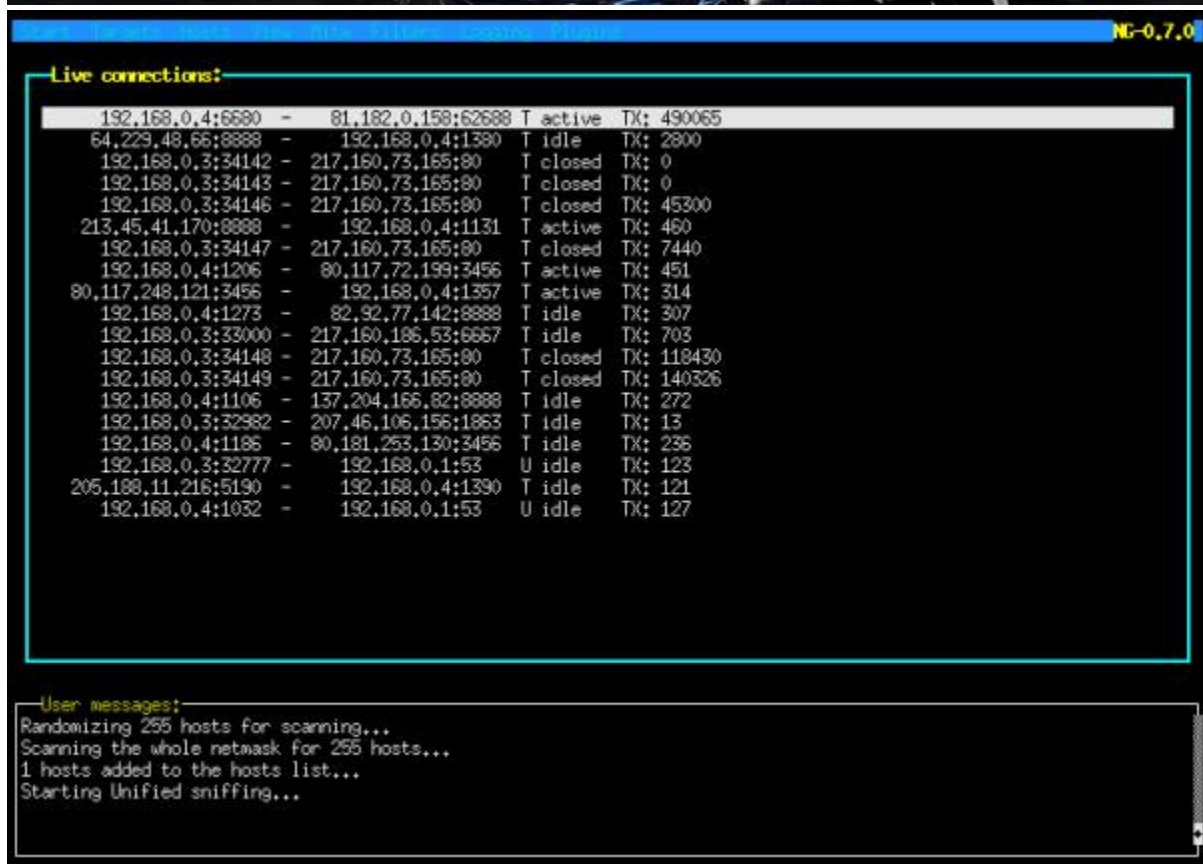
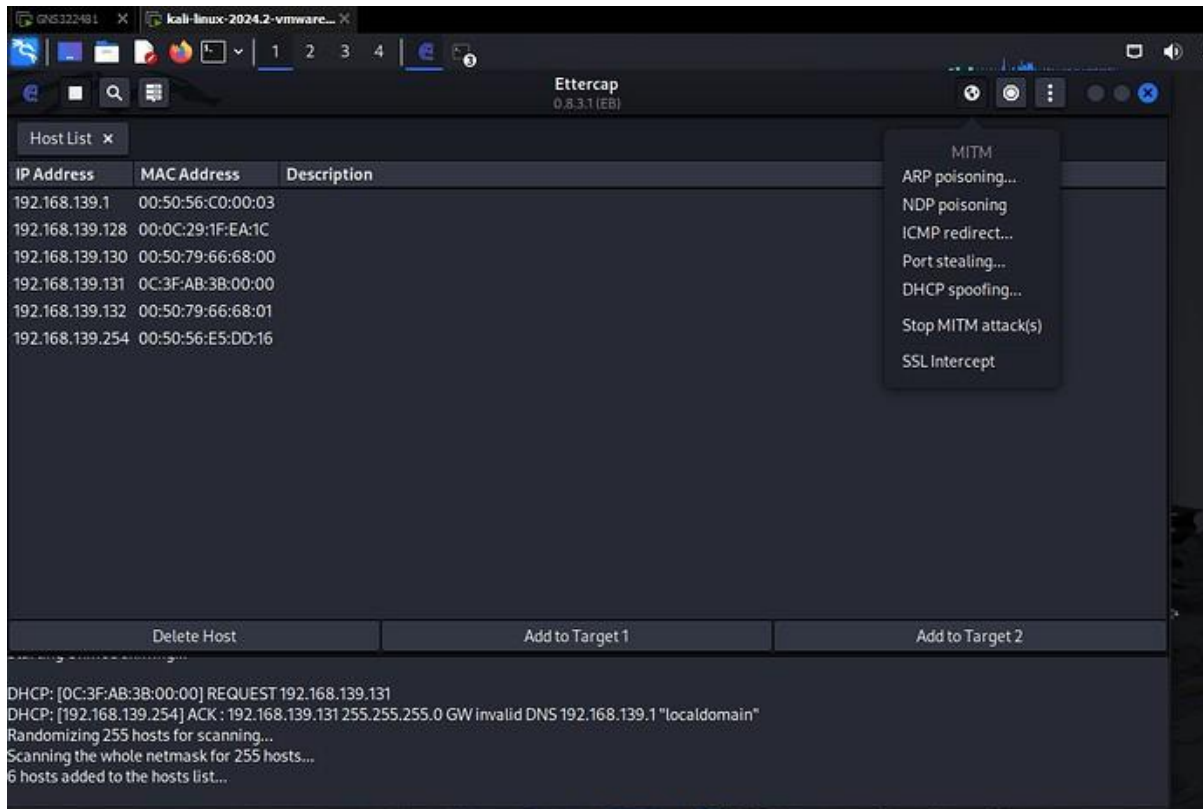
```
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [ON]
```

```
HTTP server      [OFF]
HTTPS server     [ON]
WPAD proxy       [ON]
Auth proxy       [ON]
SMB server       [OFF]
Kerberos server  [ON]
SQL server       [ON]
```

[illegible]



1. Ettercap was launched in unified sniffing mode.
2. ARP poisoning was initiated between the victim and the gateway.
3. Bidirectional traffic interception was achieved.





Ethercap was used to perform ARP spoofing between the victim and gateway, establishing a Man-in-the-Middle position. This allowed interception of live traffic, session data, and protocol exchanges. The attack demonstrates how lack of ARP protection enables silent network compromise and data exposure.

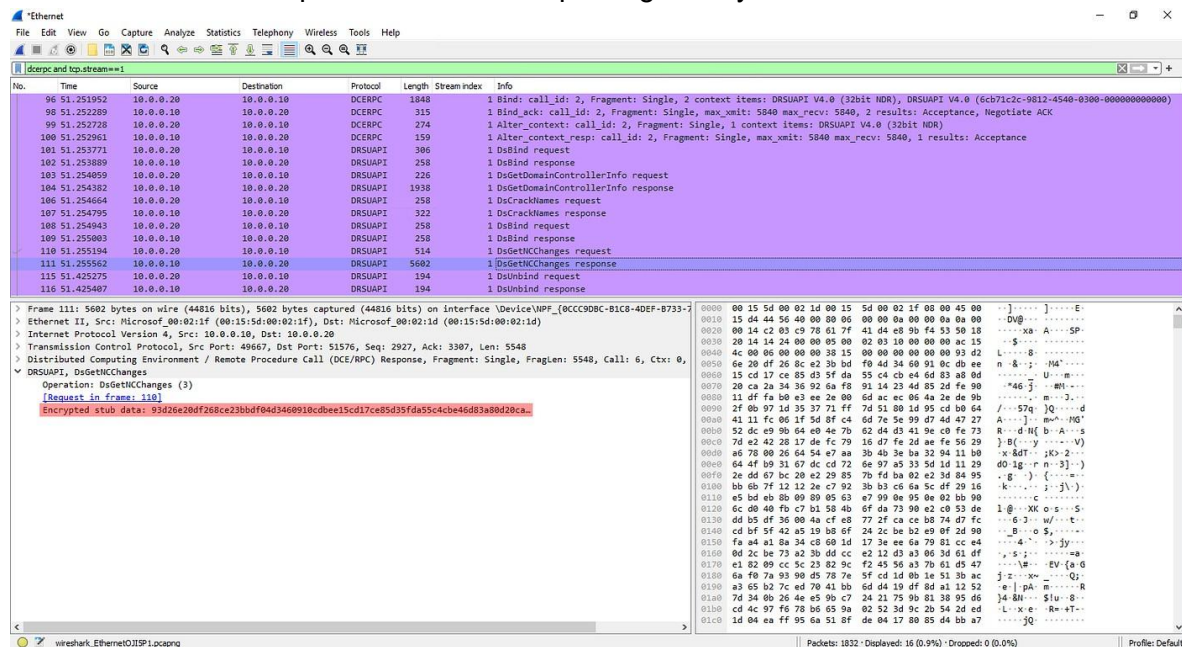
## 6. Traffic Analysis – Wireshark

### Analysis Overview

With MitM positioning established, Wireshark was used to inspect captured packets. Several insecure protocols transmitted data in cleartext, revealing authentication attempts and session metadata.

### Key Observations

- SMB and HTTP traffic visible in plaintext
- NTLM authentication exchanges identified
- DNS and ARP packets confirmed spoofing activity





arp.src.hw_mac == de:ad:be:ef:de:ad						
No.	Time	Source	Destination	Protocol	Length	Info
13	7.371348	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
14	7.371358	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
15	7.371474	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
16	7.371480	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
40	22.372398	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
41	22.372411	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
42	22.372582	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
43	22.372592	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: de:ad:be:ef:de:ad (de:ad:be:ef:de:ad), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
[Duplicate IP address detected for 192.168.112.1 (de:ad:be:ef:de:ad) - also in use by e4:8d:8c:bd:1e:63 (frame 4)]  
[Frame showing earlier use of IP address: 4]  
[Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.112.1)]  
[Duplicate IP address configured (192.168.112.1)]  
[Severity Level: Warning]  
[Group: Sequence]  
[Seconds since earlier frame seen: 4]  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: de:ad:be:ef:de:ad (de:ad:be:ef:de:ad)  
Sender IP address: 192.168.112.1  
Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
Target IP address: 192.168.112.11

http.request.method=="POST"						
No.	Time	Source	Destination	Protocol	Length	Info
1034	8.148165	172.99.96.253	160.153.129.234	HTTP	617	POST /sign
[Full request URI: http://www.sababank.com/signin.php]						
[HTTP request 1/1]						
[Response in frame: 1129]						
File Data: 53 bytes						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "username" = "Ibrahim_Diyeb"						
Form item: "password" = "yemen_123"						
Form item: "actn" = "signin"						
01a0	63 6f 64 65 64 0d 0a 43	6f 6e 74 65 6e 74 2d 4c	coded..Content-L			
01b0	65 6e 67 74 68 3a 20 35	33 0d 0a 43 6f 6f 6b 69	ength: 53..Cooki			
01c0	65 3a 20 50 48 50 53 45	53 53 49 44 3d 34 31 32	e: PHPSESSID=412			
01d0	33 35 34 31 32 30 63 35	36 37 34 35 61 63 66 34	354120c5 6745acf4			
01e0	31 62 38 65 32 39 36 34	63 32 62 65 35 3b 20 6c	1b8e2964 c2be5; l			
01f0	61 6e 67 3d 61 72 61 62	69 63 0d 0a 43 6f 6e 6e	ang=arabic..Conn			
0200	65 63 74 69 6f 6e 3a 20	6b 65 65 70 2d 61 6c 69	ection: keep-ali			
0210	76 65 0d 0a 55 70 67 72	61 64 65 2d 49 6e 73 65	ve..Upgrade-Inse			
0220	63 75 72 65 2d 52 65 71	75 65 73 74 73 3a 20 31	cure-Requests: 1			
0230	0d 0a 0d 0a 75 73 65 72	6e 61 6d 65 3d 49 62 72	....user name=Ibr			
0240	61 68 69 6d 5f 44 69 79	65 62 26 70 61 73 73 77	ahim_Diyeb&passw			

## Impact

An attacker can reconstruct sessions, steal credentials, and map internal network behavior, leading to full network compromise.

## 7. Security Impact Analysis

Area	Risk
Authentication	NTLM hashes exposed
Confidentiality	Sensitive data intercepted
Network Trust	ARP poisoning breaks trust model

**Area****Risk**

Lateral Movement High potential

---

## 9. Remediation & Defensive Measures

- Disable LLMNR and NBT-NS across the network
  - Enforce SMB signing to prevent relay attacks
  - Replace NTLM with Kerberos authentication
  - Implement Dynamic ARP Inspection (DAI)
  - Use encrypted protocols (HTTPS, SMBv3)
- 

## 10. Conclusion

This lab clearly demonstrates how outdated authentication protocols and unsecured network designs expose organizations to credential theft and silent interception attacks. Through SMB relay and MitM exploitation, the attacker gained unauthorized access without exploiting software vulnerabilities—highlighting the critical importance of protocol hardening and network monitoring.