Pip commands
sudo pip install scapy

Man-in-the-middle (MITM) attack is a type of cyber attack where the attacker intercepts and alters communication between two parties without their knowledge or consent.

Arp poisoning is one of the commonly used techniques to perform MITM is ARP poisoning, where the attacker sends fake Address Resolution Protocol (ARP) messages to a local network to link their MAC address with the IP address of another device on the network. This allows the attacker to intercept network traffic and monitor, modify, or inject malicious code into the communication between the two devices.

arp_poisning.py is a Python script that implements ARP poisoning to perform a MITM attack on a local network. The script uses Scapy, a powerful packet manipulation tool for network engineering and security, to send fake ARP messages to the network to associate the MAC address of the attacker's device with the IP address of the target device.

The script requires the following arguments to run:

target_ip: IP address of the target device on the local network
host_ip: IP address of the attacker's device on the local network
The script has two main functions:

_enable_linux_iproute() and **_enable_windows_iproute():** These functions enable IP forwarding in the operating system so that the attacker's device can forward network traffic between the target device and the internet.

spoof(target_ip, host_ip, verbose=True): This function sends fake ARP messages to the target device to associate the MAC address of the attacker's device with the IP address of the target device. This allows the attacker to intercept and modify network traffic between the target device and the internet.

pseudocode for arp_poisning.py:

```
function _enable_linux_iproute():
    // Enables IP route ( IP Forward ) in linux-based distro

function _enable_windows_iproute():
    // Enables IP route (IP Forwarding) in Windows

function enable_ip_route(verbose=True):
    // Enables IP forwarding

function get_mac(ip):
    // Returns MAC address of any device connected to the network
```

```
    // If ip is down, returns None instead

function spoof(target_ip, host_ip, verbose=True):
    // Spoofs `target_ip` saying that we are `host_ip`.
    // It is accomplished by changing the ARP cache of the target (poisoning)
    // Sends the fake ARP message
    // Prints the status message if verbose=True
```

http_pkts.py is another Python script that uses Scapy to capture and display HTTP packets in real-time. It can be used in combination with arp_poisning.py to intercept and monitor HTTP traffic between the target device and the internet.

To run http_pkts.py, simply execute the script in a terminal:

python http_pkts.py

pseudocode for http_pkts.py:

```
function packet_callback(packet):
    // Callback function to process the captured packet
    // If the packet has a TCP layer and payload
    // Decode the payload as UTF-8 and print the contents

try:
    // Start capturing packets that match the filter criteria
    sniff(prn=packet_callback, filter="tcp and port 80")
except KeyboardInterrupt:
    // Exit gracefully if the user interrupts the program
    print("\nExiting...")
```

To perform a man-in-the-middle attack using arp_poisoning.py and http_pkts.py, you can follow these steps:

1. **RUN arp -a**

```
mubeen@mubeen:~/mitm$ arp -a
asa-met-ghrko.uni-koblenz.de (141.26.64.20) at 00:1f:9e:50:63:de [ether] on ens3
tk-ucware.uni-koblenz.de (141.26.64.152) at ea:72:2f:70:5e:29 [ether] on ens3
cachens.uni-koblenz.de (141.26.64.60) at 9e:69:75:c9:75:5a [ether] on ens3
printhost.uni-koblenz.de (141.26.64.118) at ae:b4:46:b5:b4:c1 [ether] on ens3
printhost12.uni-koblenz.de (141.26.64.113) at 36:71:ab:2c:ae:76 [ether] on ens3
sparci-test-guestvm4.uni-koblenz.de (141.26.70.79) at 1e:00:f5:00:00:04 [ether] on ens3
sparci-test-guestvm14.uni-koblenz.de (141.26.68.159) at 1e:00:26:00:00:1d [ether] on ens3
cachens1.uni-koblenz.de (141.26.67.191) at 9e:69:75:c9:75:5a [ether] on ens3
ascent.uni-koblenz.de (141.26.67.181) at a6:da:5d:67:f0:2d [ether] on ens3
winroute.uni-koblenz.de (141.26.64.9) at 00:00:5e:00:01:2a [ether] on ens3
? (141.26.68.0) at <incomplete> on ens3
printers.uni-koblenz.de (141.26.64.84) at 0e:df:6e:d0:5e:89 [ether] on ens3
```

2. **Note down the host is dns is**
   winroute.uni-koblenz.de (141.26.64.9) at 00:00:5e:00:01:2a [ether] on ens3

3. **Now let suppose the target if is**
   sparci-test-guestvm14.uni-koblenz.de (141.26.68.159) at 1e:00:26:00:00:1d [ether] on ens3

4. **Now run the command**

   Sudo python3 arp_poisning.py 141.26.68.159 141.26.64.9 –verbose

```
mubeen@mubeen:~/mitm$ sudo python3 arp_poisning.py 141.26.68.159 141.26.64.9 --verbose
[!] Enabling IP Routing...
[!] IP Routing enabled.
[+] Sent to 141.26.68.159 : 141.26.64.9 is-at 1e:00:9b:00:00:1c
[+] Sent to 141.26.64.9 : 141.26.68.159 is-at 1e:00:9b:00:00:1c
[+] Sent to 141.26.68.159 : 141.26.64.9 is-at 1e:00:9b:00:00:1c
[+] Sent to 141.26.64.9 : 141.26.68.159 is-at 1e:00:9b:00:00:1c
[+] Sent to 141.26.68.159 : 141.26.64.9 is-at 1e:00:9b:00:00:1c
[+] Sent to 141.26.64.9 : 141.26.68.159 is-at 1e:00:9b:00:00:1c
```

5. Open an other terminal and run http_pkts.py in another terminal window. This script listens for and intercepts HTTP packets being sent between the victim and the router. When a packet is intercepted, it prints out the contents of the packet.

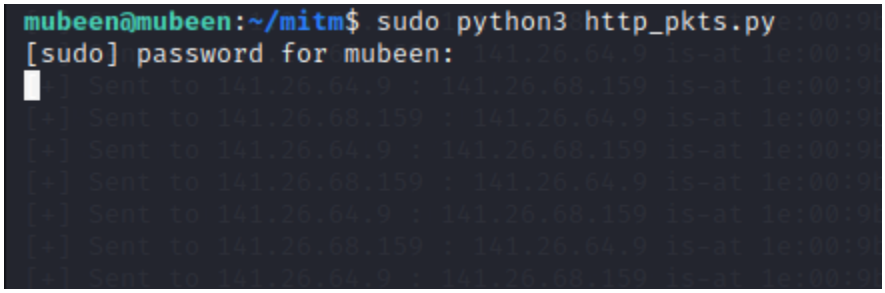
6. **The command should look something like this:**
   sudo python3 http_pkts.py

7. Once both scripts are running, any HTTP traffic sent between the victim and the router will be intercepted and printed out in the http_pkts.py terminal window. This includes any login credentials or other sensitive information sent over HTTP.

VPN Helps in preventing MITM Attacks

Regarding the security of performing a man-in-the-middle attack through a VPN, using a VPN can provide some level of protection against MITM attacks, as it encrypts the traffic between the

client and the VPN server, making it more difficult for an attacker to intercept and read the traffic. However, if the VPN server itself is compromised, the attacker could still intercept the traffic. After running the http_pkts.py you have noticed there is no packets captured.



Attack Status:

- Mitm, attack failed
- During the security assessment of the target system, we attempted to launch a man-in-the-middle (MitM) attack on the network traffic. The purpose of this attack was to intercept and analyze the traffic passing through the network to gain unauthorized access to sensitive information.

- However, our attempt at launching a MitM attack was unsuccessful. We did not find any vulnerabilities or weaknesses that could be exploited to launch such an attack. Our analysis suggests that the network traffic is secured because of VPN, which encrypts the data transmitted over the network and makes it difficult to intercept or eavesdrop.

- In conclusion, the MitM attack failed due to the secure nature of the VPN. We recommend the target system to continue using the VPN to secure their network traffic and prevent unauthorized access to sensitive information. Further assessments and testing can be performed to identify any other potential security weaknesses and improve the overall security of the system.

To secure Apache Cloud from MITM attacks, there are several measures you can take, including:

- Using SSL/TLS to encrypt web traffic
- Implementing certificate pinning to prevent attackers from using fake certificates
- Implementing HTTP strict transport security (HSTS) to ensure that web browsers only use HTTPS connections to communicate with the server
- Regularly updating and patching the server and software to address known security vulnerabilities
- These measures can help prevent attackers from intercepting and reading web traffic on the Apache Cloud server.

References:

https://en.wikipedia.org/wiki/Man-in-the-middle_attack
https://www.cloudflare.com/learning/ssl/what-is-ssl-encryption/
https://www.owasp.org/index.php/Certificate_pinning
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

To run codes
ssh mubeen@141.26.68.158 -p 22
password 12345

cd mitm
ls