**Tutorial No. 8**

# Title: MITM

**Roll No.: 16010420075 Tutorial No.: 8**

# Aim: To execute Man In The Middle Attack

\

**Resources:** virtual box

**Theory**

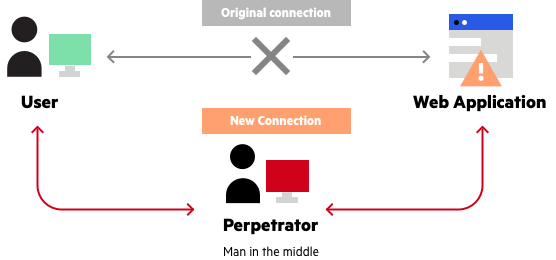
A man in the middle (MITM) attack occurs when a perpetrator inserts himself into a communication between a user and an application, either to listen in or to mimic one of the parties, making it appear as if a normal information exchange is taking place.

An attack's purpose is to steal personal data such as login credentials, account information, and credit card numbers. Users of financial apps, SaaS enterprises, e-commerce sites, and other websites that require signing in are typical targets.

Identity theft, unapproved fund transfers, and unauthorized password changes could all be possible with information gathered during an attack.

It can also be used to gain a footing inside a guarded perimeter during an advanced persistent threat (APT) assault's infiltration stage.

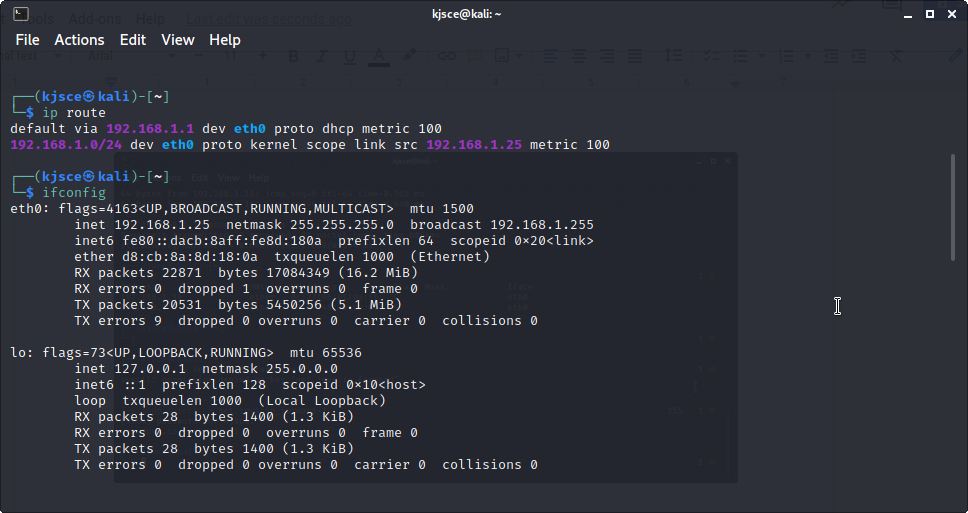
A MITM attack is essentially the same as a mailman opening your bank statement, writing down your account information, then resealing and bringing it to your door.



**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**IMPLEMENTATION AND RESULTS:**

First, we ping the IP we want to attack. Then, we use the **ip route** command to see where the IP is routing from.



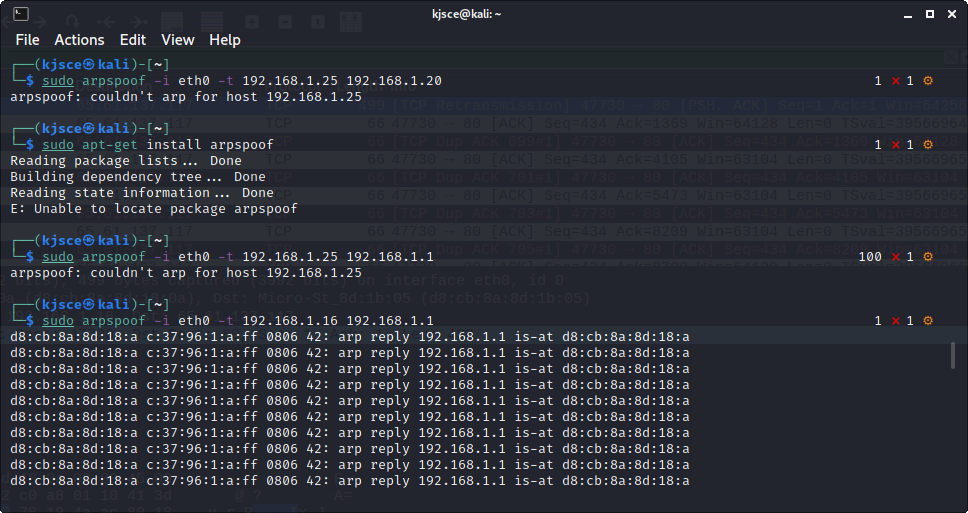
With the **arp** command, we see the devices we are connected to. We then use the

**sudo systcl -w net.ipv4.ip\_forward=1** command to allow IP forwarding in those IPs.



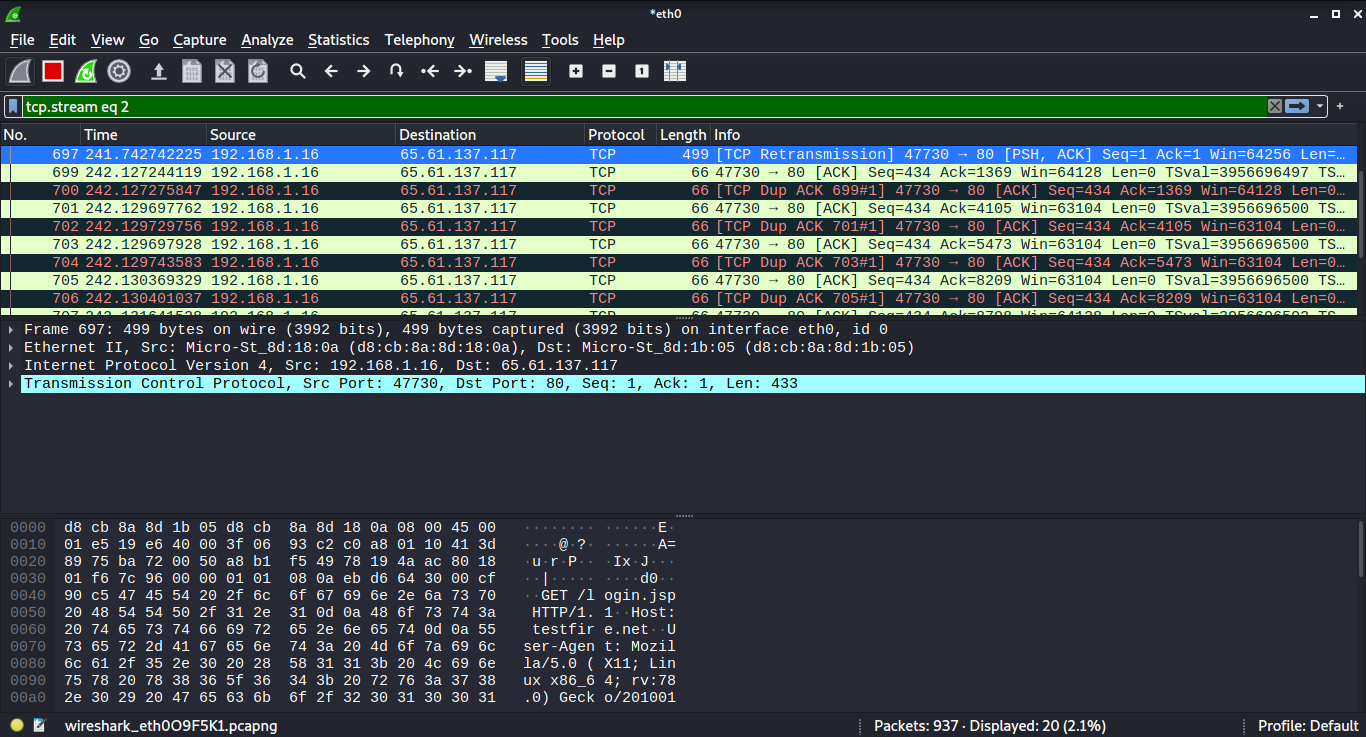
To allow TCP checking, we need to spoof the ARP using the command below.

**arpspoof -i [network interface name] -t[victim]**

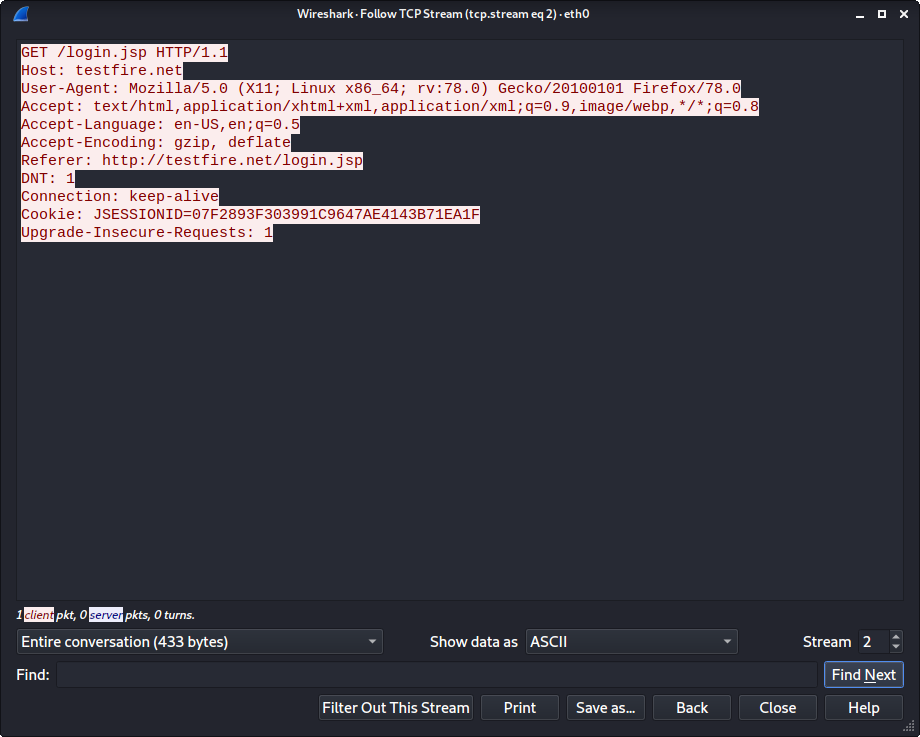


Ask the victim user to login randomly at <https://www.testfire.net>

Then open WireShark and check all the IPs that are routing in the eth0 tunnel. The activities of pinged IPs will be displayed. Right click on any of their activity and follow the TCP port.



Lastly, we see all the activities of the user as in the image displayed below.



**Outcomes:**

**CO-3:** Understand attack methodology

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

Man In The Middle attack was executed and its concept was grasped.

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**REFERENCES:**

* [www.kali.org](http://www.kali.org)