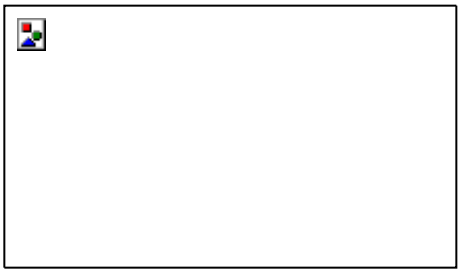

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework 02

Year and Semester

2021 -22 Spring Semester

Student Name: Raj Bhandari

London Met ID: 20049202

College ID: NP01NT4S210071

Assignment Due Date: 2022/05/05

Assignment Submission Date: 2022/05/05

Word Count (Where Required): 3300

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline 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.

Abstract

This paper focuses on understanding the term MITM (Man in the Middle) attack and how hackers can easily undertake this type of attack to acquire access to private data. This article shows how to perform an MITM attack in a virtual environment using Oracle VirtualBox to sniff and extract the victim's sensitive data when both devices are connected to the same network access point. Every step of the attack is described in detail, as are the tools used to carry out the MITM attack. This study also outlines basic countermeasures that can be used to prevent such assaults.

Table of Contents

Table of Figures

1. INTRODUCTION

The ability to transport data and information via internet using networks and servers has been a significant benefit to humanity as a whole. The availability of internet technology has vastly increased during the last few decades. Any collection of interconnecting lines reassembling a network, a network of road links, or a network of alliances has been defined as a network. A computer network is essentially a linked computer system, which is a concept that is well-suited to our goal. With the arrival of internet and current network technologies, the world is becoming more involved. Around the world, there is a tremendous amount of political, industrial, military, and government information about networking infrastructures. Because of the intellectual property that may be readily accessible through the internet, network security has become increasingly important. (Kirsch, 2019)

A MITM (Man in The Middle) attack is a popular cyber-attack in which attacker disrupt two-way communication settings by impersonating one of the parties to deceive the other. In these conditions, an intruder may listen in on the communication between the two unexpected people and obtain information. Both wired and wireless networks are vulnerable to these assaults, with the latter being more so. This type of attack happens as a result of wireless network constraints that aren't well defined. (Johnston, 2022)

1.1. Current Scenario

Cybersecurity is often regarded as one of the most serious issues, with significant organizations such as banks, IT firms, and legislators all having to consider it. Not just huge businesses, but everyone will be concerned about cybersecurity. Smaller enterprises, such as those with less than 1,000 employees, are at the highest risk. To grasp the enormity of the problem, consider that 43% of all cyberattacks target small businesses.

In the area of IT security, man-in-the-middle attacks are commonly used by black hat hackers to eavesdrop client-server conversations. This includes connections to HTTPS websites, other SSL / TLS connections, Wi-Fi, and more.

- **In 2013, information was leaked about the Quantum/Fox Acid MITM system employed by NSA to intercept TOR connections.**
- **In 2014, Lenovo installed MITM (SSL Hijacking) adware called super fish on their windows PCs.**
- **In 2015, a British couple (the Lupton's) lost £340,000 in an email eavesdropping / email hijacking MITM attack.**
  (Nidecki, 2019)

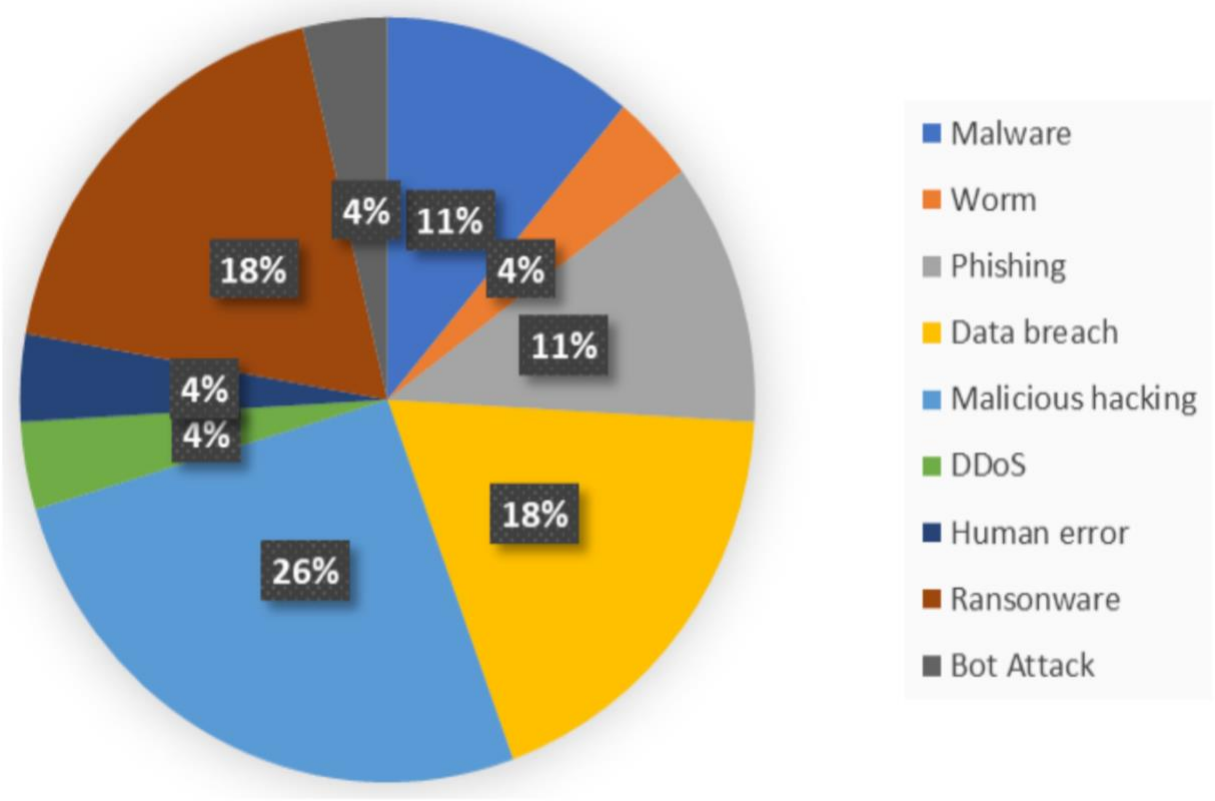

Figure 1: Top 9 cyberattacks in 2021 (Katsikas, 2022)

1.2. Problem Statement

With the widespread usage of the internet, the risk of a MITM (Man in the Middle) attack is quite high. People are unaware of such assaults and want to conduct their crucial transactions via a free public network with no limitations, making them easy targets for such attacks. As a result, the goal of this project is to show users how such assaults occur and how they be mitigated.

1.3. Aims & objective

- **Aim**

  The main goal of this project is to demonstrate how a man-in-the-middle attack including eavesdropping may be used in real-life to gain access to private information while linked to a poorly defined or unprotected network.

- **Objectives**

  The main objectives of this report are:

  a. To study about different types of vulnerabilities.
  b. To study various aspects of eavesdropping and spoofing.
  c. To demonstrate man-in-the-middle attack on a network using different tools of kali Linux.
  d. To sniff the private information of the host.
  e. To provide solutions to prevent and mitigate man-in-the-middle attack.

2. Background

2.1. Eavesdropping

An unauthorized party takes, changes, or deletes crucial information that is exchanged between two electronic devices in an eavesdropping attack, also known as sniffing or spying assault. An attacker looking for sensitive information intercepts and reads a packet sent over the network. An eavesdropping device can analyse the data acquired. Because eavesdropping is a passive attack, network surveys are difficult to detect (an attack using information without affecting resources at the system). Both wired and wireless networks can be used to carry out eavesdropping attacks. To perform network tap to sniff packets in a wired network, the eavesdropper must be in touch with the network wire. (frankenfield, 2022)

Because eavesdropping is a precondition for numerous attacks, the eavesdropping attack is a key safety threat for Wi-Fi sensor community. Traditional WSNs are made up if Wi-Fi nodes with omnidirectional antennas that emit radio indications all around the network, putting then at danger of eaves dropping.

Active eavesdropping and passive eavesdropping are the two forms of eavesdropping attacks. In active eavesdropping, attackers mimic themselves to obtain access to various personal data, whereas in a passive assault, the attacker just listens to data travelling across the network.

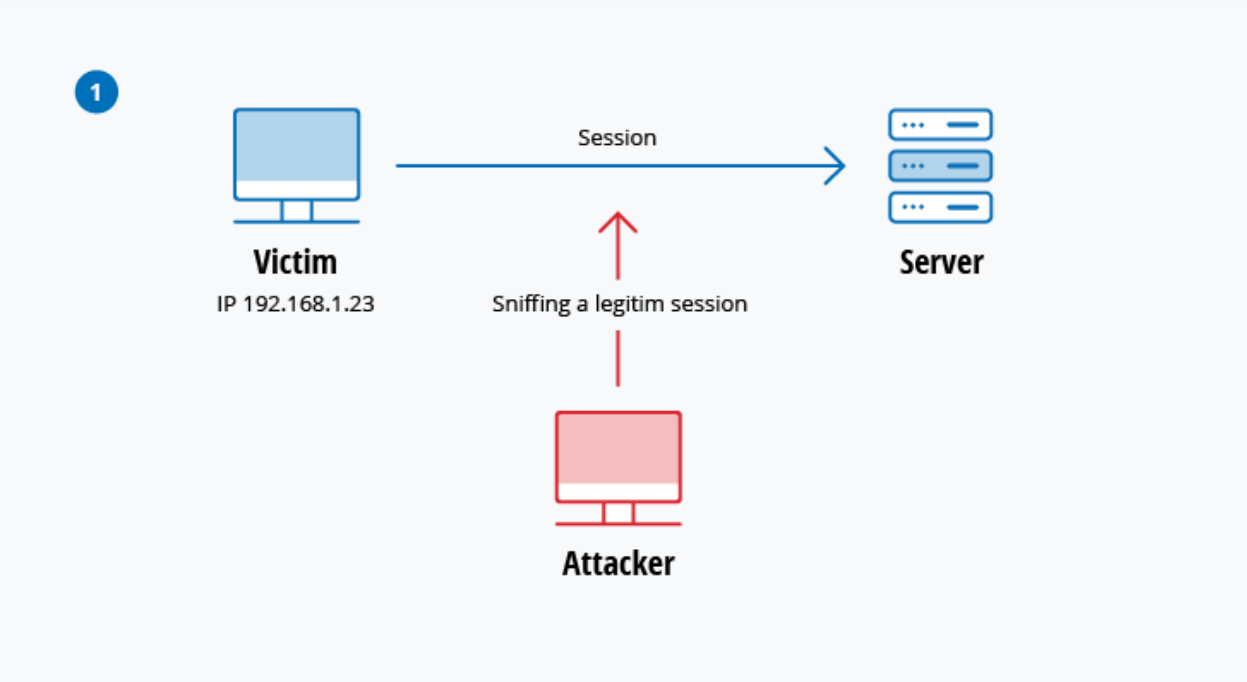

Figure 2: Eavesdropping attack

2.2. Spoofing

Spoofing, which comes from the phrase “Spying”, is one of the most used cyber-attack strategies. Spoofing is the initial stage in carrying out an MITM attack if someone desires to communicate with someone on the cryptographic network, the server broadcasts an address resolution protocol (also known as ARP) to all hosts on the same network connection if their networks are similar to an unknown MAC address. For clients who have announced the Internet Protocol, only answers with the MAC (Media Access Control) address are expected. However, because the essential authentication method is missing, cache entries can be readily created with the false ARP packets when handled dynamically.

There are three types of spoofing attacks:

2.2.1. ARP Spoofing

The Address Resolution protocol, or ARP, creates a link between a real machine address, also known as a Media Access Control or MAC, and an IP address. ARP

enables the network to discover and include the device as a structural component. In today's world, IPV4 and IPV5 are utilized to make connections more secure.

ARP spoofing is the technique of using fake ARP packets to connect an attacker's MAC address to the IP address of a victim on a specific network. Instead, the attacker receives information sent by the client to the delivery of the host IP. (Grimmick, 2021)

2.2.1.1. ARP poisoning cache

ARP poisoning is a technique for diverting network traffic so that all packets sent by the victim on a network are ignored. As a result, computers on those networks will keep updating their ARP responses until their previous cache file is reviewed. As a result, the attacker has a chance to poison the ARP cache. When communication is established, computers make an ARP request to all other computers on the network on the network, inquiring who is associated with this identifier (including IP address). And the proper machine will respond with its MAC address. To mimic the victim, the attacker's computer resolves the same MAC address to the victim's computer, and the attacker enters a listening mode where he can observe all the packet broadcast. (Gimmick, 2021)

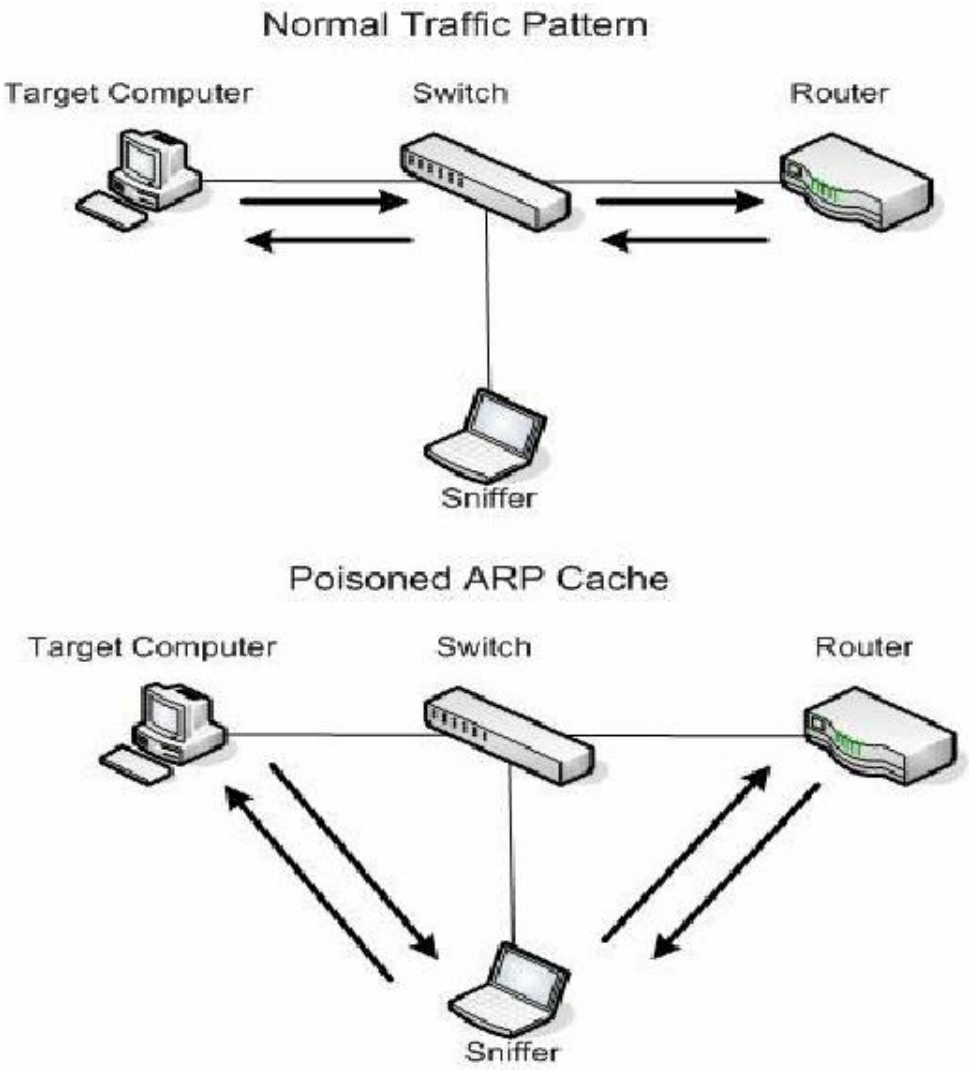

Figure 3: ARP poisoning cache

2.2.2. IP Spoofing

IP spoofing is the creation of Internet Protocol (IP) packets with a different source address in order to hie the sender's identity, mimic another computer equipment, or both. It allows cybercriminals to carry out malicious actions, often without detection. Attackers use IP spoofing to transmit packets to the victim's device with an incorrect return address in order to get victim's IP address, while the victim tries to block those packages from an unknown source. Distributed Denial of Service (DDoS) Attack, Replay and Blind spoof are some examples of IP Spoofing. (Lutkevich, 2021)

2.2.3. DNS Spoofing

The attack, also known as DNS cache poisoning, occurs when data is inserted into a domain name server and returns incorrect data to a different computer. ADNS server is typically provides by an Internet Service Provider, or by an organization, for use by a user. A network uses a dedicated DNS server to improve the response time of its resolution requests. An attacker can perform a cache poisoning attack by exploiting a vulnerability in the software used to store the results of an email. (Petcu, 2021)

2.3. Man-in-the-middle attack

Man-in-the-middle attacks are usually carried out by individuals who pretend to be a communication channel between two parties in order to steal sensitive information. The main goal of this type of attack is to obtain user's credit card number and other personal details. Information gained during such attacks can be used for illegal purposes such as unauthorized support modifications and fraud. To carry out this type of attack, the attacker must be able to intercept and inject every significant communication sent between two victims. (Swinhoe, 2022)

To carry out an MITM (man-in-the-middle) attack, the user needs a communication route. Radio frequency, Wi-Fi, LTE, GSM, UMTS, and NFC are the most often used communication routes for MITM attacks. The MITM attack is carried out in two stages:

2.3.1. Interception

The first step in carrying out an MITM attack is to get access to the communication channel that the victim is presently using so that the attacker may intercept client activity before it reaches its intended destination through the attacker's system. The following are some of the dynamic ways for dealing with MITM attacks:

- **IP Spoofing**

- **ARP Spoofing**
- **DNS Spoofing**

2.3.2. Decryption

Any two-way SSL movement intercepted should be unscrambled without notifying the client or application. The tactics for carrying out such assaults are described below.

- **HTTPS Spoofing**

  HTTPS spoofing is a typical attack tactic in which an attacker uses a domain that looks remarkably similar to the target's websites. The characters in the target domain are substituted with non-ASCII characters that seem remarkably similar. This strategy is also known as "homograph assault".
- **SSL Stripping**

  When a hacker interferes with the connection between a user and a website, this is known as SSL stripping. The Hacker sits in the midst of the connection, connecting to the HTTPS version of the site while the user connects to the HTTP version. This gives them unencrypted access to anything the user says.
- **SSL Hijacking**

  The exploitation of a legitimate session by getting unwanted access to the session key/ID information is known as SSL hijacking also known as cookie hijacking. When a user attempts to log into a web application, the server authenticates the session by placing a temporary remote cookie in the client's browser. This allows the remote server to remember the state of the client's login.
- **SSL Beast**

  Beast (Browser use against SSL/TLS) attack exploit a vulnerability in SSL 3.0 and TLS 1.0 (CVE-2011-3389). In this attack, the attacker can take advantage of a flaw in TLS 1.0's implementation of CBC (cipher block chaining). By inserting designed packets into TLS streams via MITM

methods, the attacker can decode encrypted data between two users/systems. This attack needs access to the client's (victim's) computer browser.

3. Demonstration

The following are the steps to be carried out to perform man-in-the-middle attack in a network, here all the steps are performed using VM VirtualBox.

Step 1: Creating a network

First of all, a private network is created and both the virtual machines are connected to the same network.

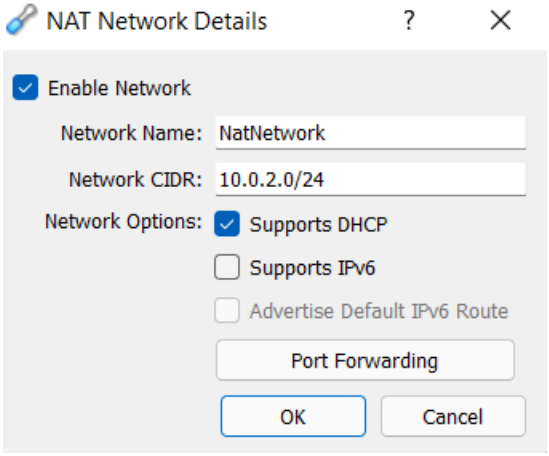

Figure 4: creating a network

Step 2: Details of attacker interface

In this step, the details of our network is shown using the command ***ifconfig:***

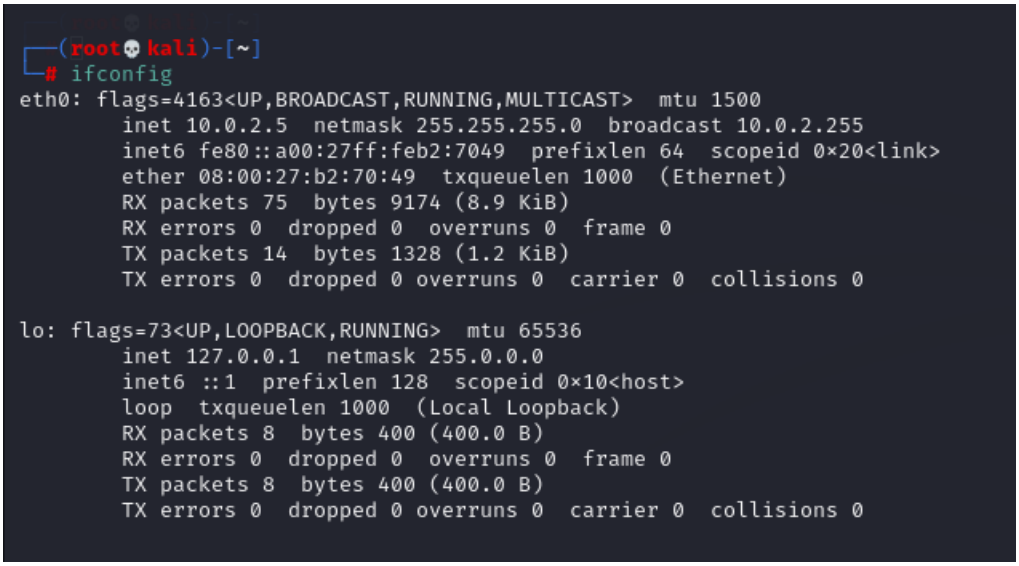

Figure 5: Details of attacker interface

We can see that our IP address is 10.0.2.5 and similarly our MAC address is 08:00:27:b2:70:49.

Step 3: Discovering IP gateway

In this step ***route -n*** command is use to IP address of the gateway.

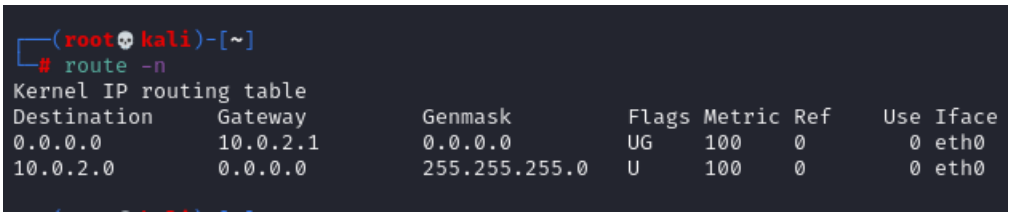

Figure 6: Discovering IP gateway

Here, we can see the IP gateway of our interface using ***route -n*** command as shown in the figure.

Step 4: Identifying IP of the victim

After finding out the gateway, all the nodes in the network are discovered using ***netdiscover -r*** command.

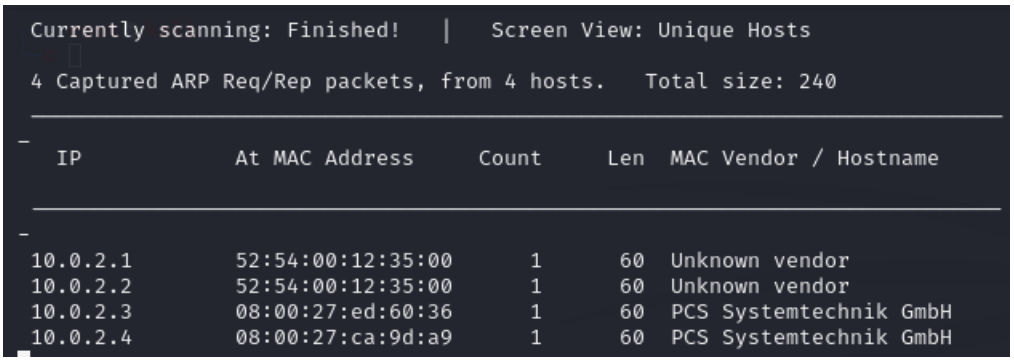

Figure 7: Identifying IP of the victim

From the figure above we can see that it captured 4 ARP requests/responses. Netdiscover sniffs the ARP traffic to discover all the nodes connected to the network. Now we know the IP addresses of the machines we want to be in between.

Step 5: IPV4 forwarding

In this step, we make sure all IPV4 traffic is forwarded so that there would be no interception while attacking the victim. ***Echo 1 > /proc/sys/net/ipv4/ip_forward*** command is used to forward ipv4 traffic as shown in the figure below.

Step 6: Redirecting HTTP to SSLStrip

After IPV4 traffic is forwarded we need to make sure all the HTTP-traffic is redirected to SSLStrip that listens to the port 10000 by default. ***Iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 10000*** command is used so that incoming HTTP-traffic (TCP on port 80) are redirected to port 10000 as shown in the figure below.

Figure 8: Redirecting HTTP to SSLStrip

Step 7: Running SSLStrip

SSLStrip is run so that we can hijack all the HTTPS-traffic on a network and match the HTTPS link with HTTP link so that we can sniff the contents of this traffic.

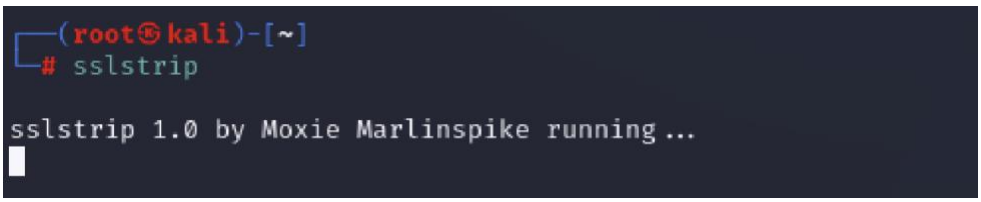

Figure 9: Running SSLStrip

Step 8: Attack with Ettercap

Ettercap is the tool for man-in-the-middle attack that sends malicious ARP to the targeted client. ***Ettercap -G*** command is used to enter the graphical interface of Ettercap, eth0 is used as primary interface and unified sniffing is done.

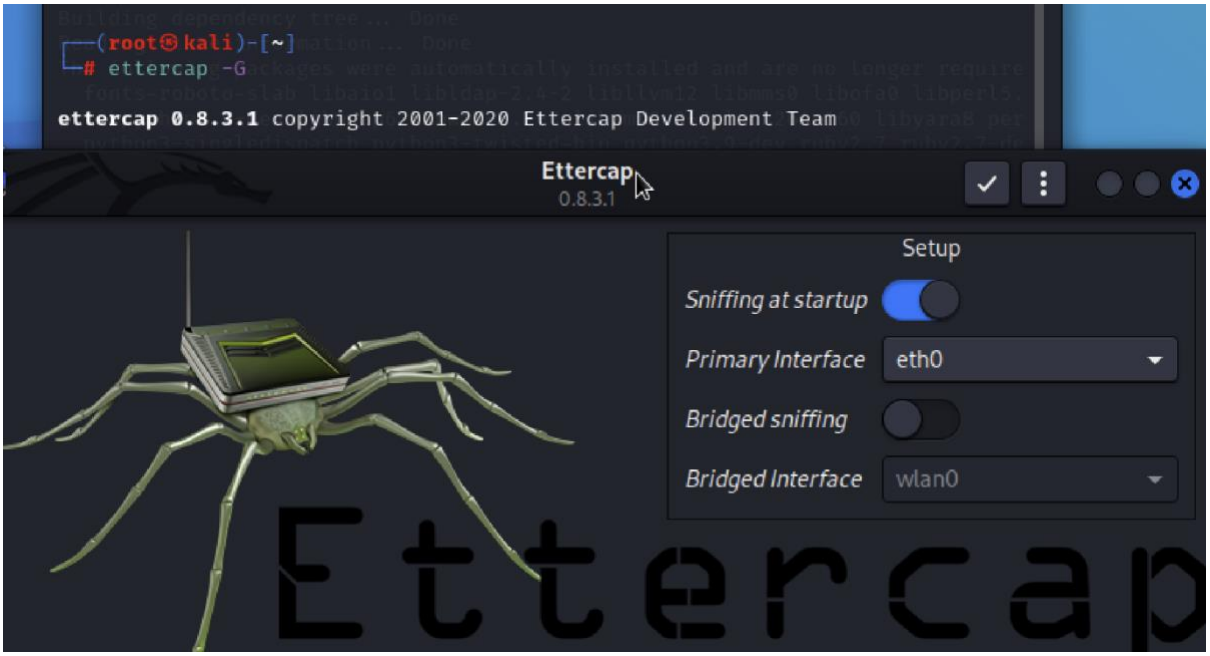

Figure 10: Attack with Ettercap

After that hosts are scanned and the host list can be displayed, and we can see both IP-address of gateway and victim.

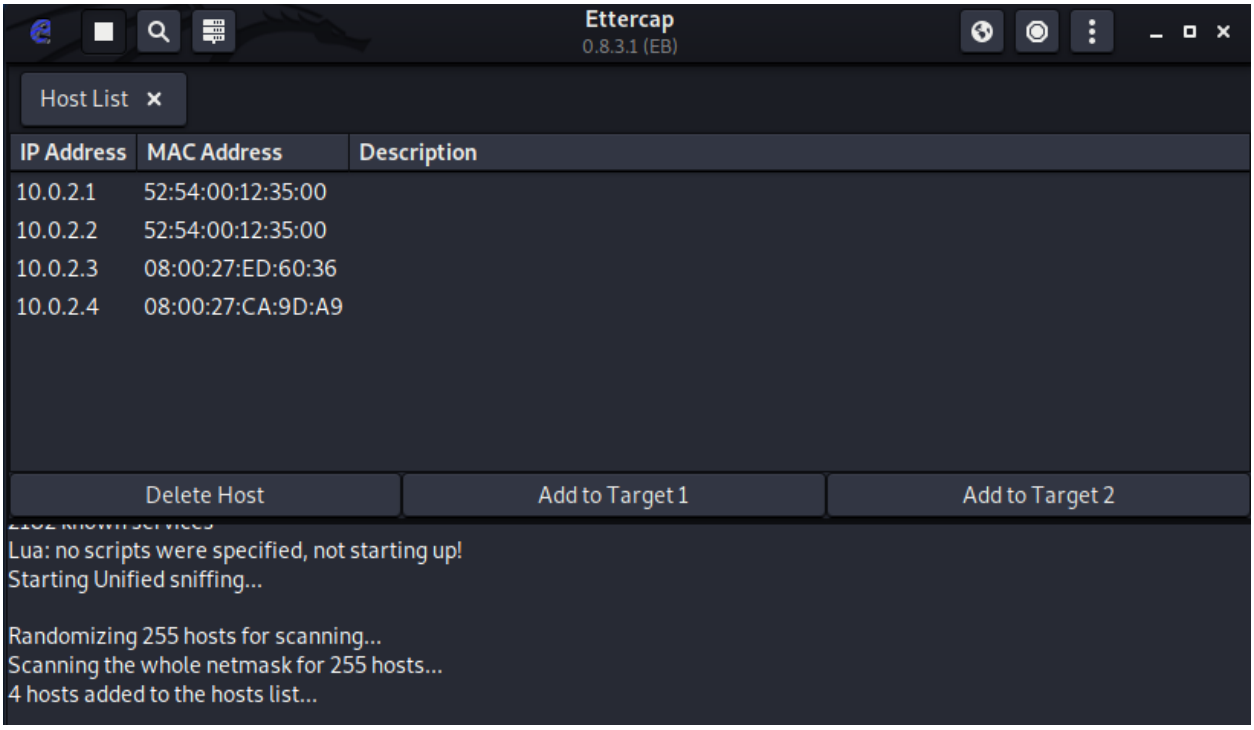

Figure 11: Ettercap host list

Now IP address of gateway is added as target 1 and the victim's IP address is added as target 2.

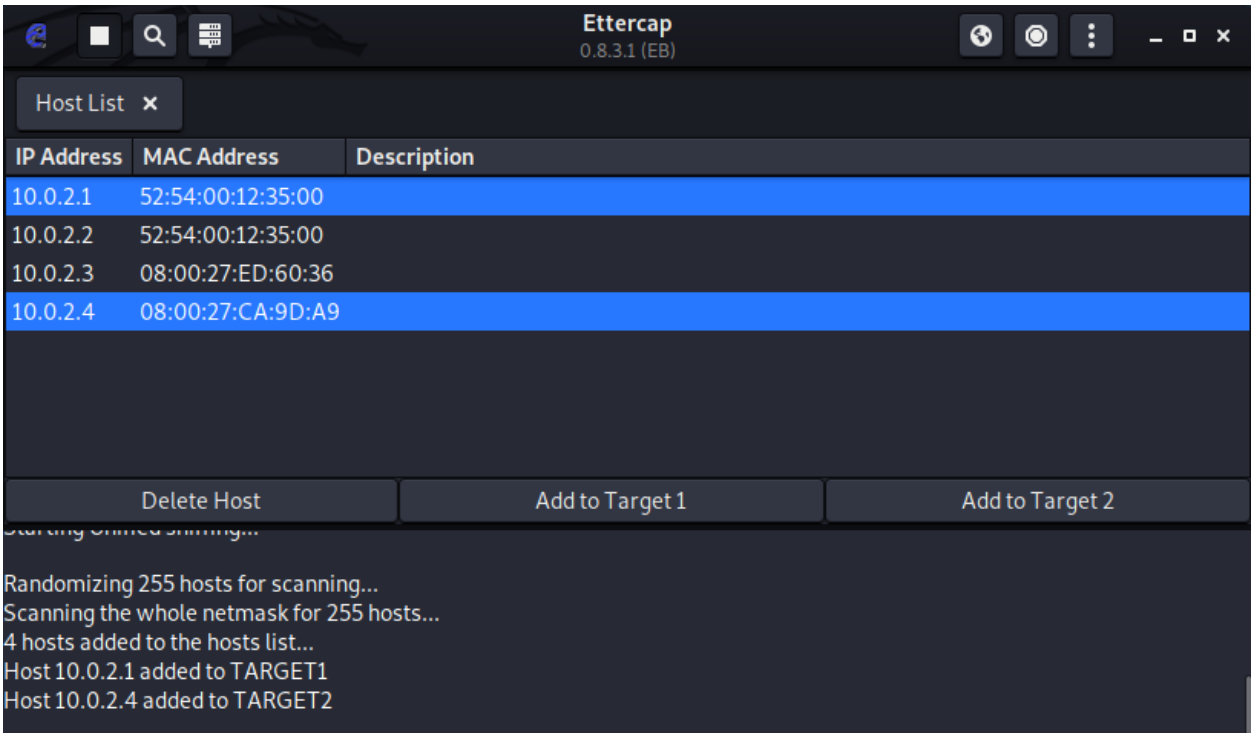

Figure 12: Adding hosts to target

After setting the targets, malicious ARP is sent to both target using ARP poisoning from the MITM menu.

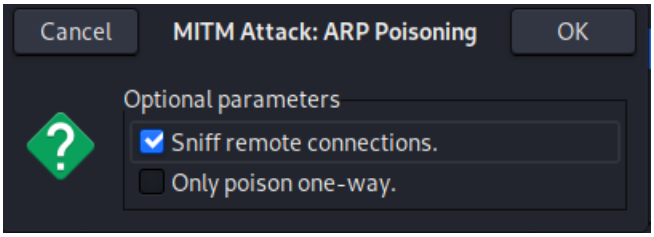

Figure 13: ARP poisoning using Ettercap

Here is the detailed figure of affected targeted group.

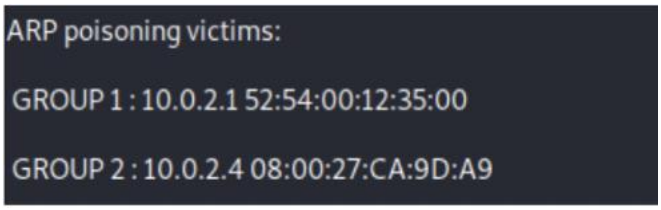

Figure 14: AR after poisoning

Step 9: ARP responses – Network traffic

In this step, Wireshark a preinstalled kali Linux tool is used to see all the ARP responses sent out to the victim and the gateway. In the figure below shows how Wireshark detects how the attackers mac address is seen linked to another machines IP address.

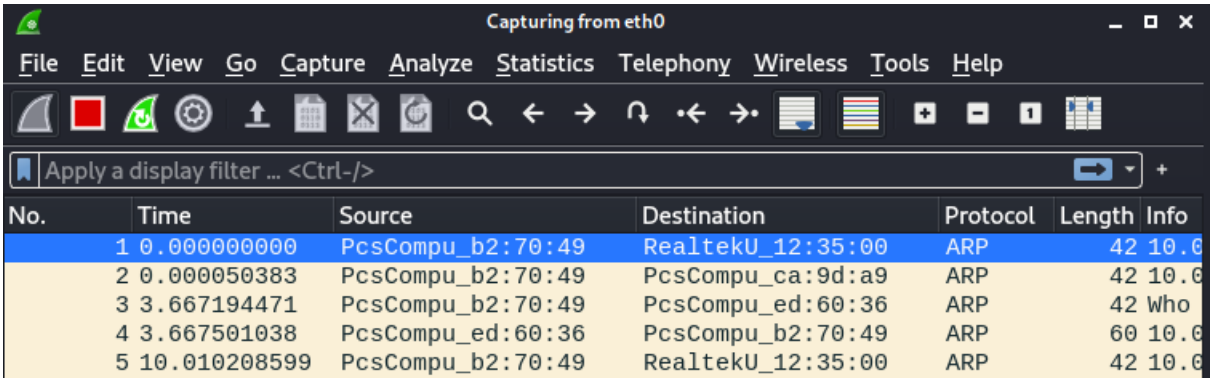

Figure 15: ARP responses - Network traffic

Step 10: ARP tables (Victim)

In this step victim's ARP table is checked using ***arp -a*** command in windows. The figure below is the arp table of the victim before arp poisoning.

```
Interface: 10.0.2.4 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-ed-60-36     dynamic
  10.0.2.67             08-00-27-b2-70-49     dynamic
  10.0.2.255            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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 16: Victim's ARP before poisoning

After ARP poisoning, we can see that, both IP addresses has been referred to attacker's MAC address. So this step clarifies the ARP poisoning was successful.

```
Interface: 10.0.2.4 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.1              08-00-27-b2-70-49     dynamic
  10.0.2.3              08-00-27-ed-60-36     dynamic
  10.0.2.5              08-00-27-b2-70-49     dynamic
  10.0.2.67             08-00-27-b2-70-49     dynamic
  10.0.2.255            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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 17: Victim's ARP after poisoning

Step 11: Browsing

After ARP poisoning was done, SSLStrip was done internet explorer was used to browse www.facebook.com. Below in the figure we can see that HTTPS was changed to HTTP and the same site will be mapped in the victim's interface. For some reason my site was blank but the HTTPS traffic was successfully hijacked and changed to HTTP traffic. With this the hacker can see all the browsing history of the victim including the login and password information from the mapped site.

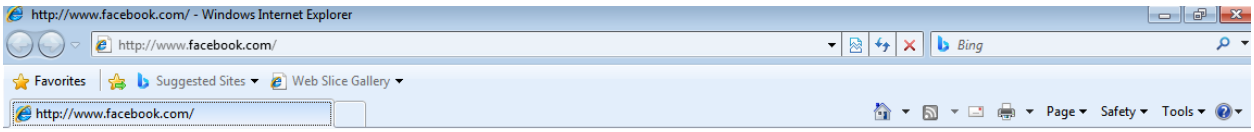

Figure 18: Browsing

4. Mitigation for MITM (Man in the Middle) Attack

4.1. Using VPN (Virtual Private Network)

Many of the sites where a MITM attack might occur will be blocked by using a VPN, but not all. It will safeguard our traffic between the user device and the VPN gateway in particular, preventing our ISP (or most governments) for launching a MITM attack against us. After using the VPN the HTTP traffic been mapped will be removed and the user can login to HTTPS traffic securely without being fear of leak of his/her privacy.

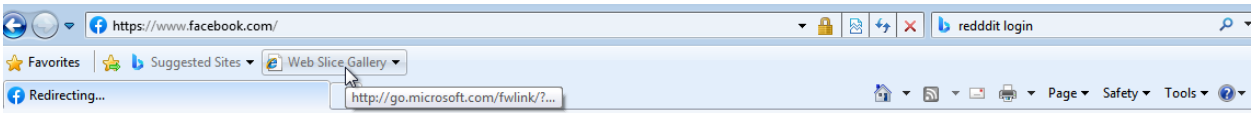

Figure 19: browsing after using VPN

In the above figure we can see that the HTTP traffic that have been mapped is been removed and changed to HTTPS traffic after the VPN was used. So, we can say that using of VPN can help us to browse safely to any website without having fear of getting attacked.

4.2. Strong WEP/WPA Encryption on Access Points

WPA (Wi-Fi Protected Access) is a security standard for computer devices that connect to the internet over a wireless connection. It was created by the Wi-Fi Alliance to provide stronger data encryption and user authentication over the original Wi-Fi security standard and wired Equivalent Privacy (WEP). With strong WEP/WPA encryption on access points makes difficult for the unauthorized users to enter the network and prevents MITM attacks. The stronger the implementation of encryption, the safer the network.

4.3. Use of HTTPS

As from the above attacks it is clear that if whenever the browsing is to be done HTTPS traffic is to be used in order to perform browsing safely. This prevents an attacker from using the data which he may intend to sniff. Users can install browser plugins to implement HTTPS on request at any time.

5. Evaluation

The use of VPN can mitigate the risk of MITM attack but the use of VPN comes with both pros and cons:

Pros:

- VPN encrypts all communications and secures data from hackers.
- Our real IP address can be covered by VPN and allow us to bypass geo-blocks.
- VPN ensures that our ISP will not be able to throttle our bandwidth.

Cons:

- VPN services costs money and the free VPNs are not too much effective.
- The use of VPN reduces the speed of the network.
- Some VPN provider ask their user to login which may threaten their privacy.

5.1. CBA (Cost Benefit Analysis)

The yearly subscription of the best VPN comes between $70 - $80. If the user carries out online transaction frequently and transfers important data using internet then the use of VPN can be considered beneficial.

6. Conclusion

When the attacker is responsible for moving along typical movement points, the MITM breaks the interface between two systems, and this phenomenon occurs. The invader is on a shared domain with the victim in both cases. An HTTP transaction does, in fact, use the TCP protocol between the client and server. The

attacker splits the TCP protocol into two channels: one between the victim and the attacker, and another between the attacker and the server.

In this coursework, a sample MITM attack was carried out in a virtual box is used to show this type of attack might be used in real life by hackers to secretly listen to your private data to use according to their desire. This report clearly demonstrates how free, unprotected networks may be extremely harmful, and why should avoid utilizing them for sensitive transactions. This also covers how to mitigate such type of assaults on one's computer using variety of tools and providing users with basic knowledge.

Works Cited

frankenfield, J. (2022, February 11). Retrieved from https://www.investopedia.com/terms/e/eavesdropping-attack.asp

Gimmick, R. (2021, April 27). *Varonis*. Retrieved from Varonis: https://www.varonis.com/blog/arp-poisoning

Grimmick, R. (2021, April 27). *Varonis*. Retrieved from Varonis: https://www.varonis.com/blog/arp-poisoning

Johnston, D. (2022, march 31). *imperva*. Retrieved from imperva: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

Katsikas, S. (2022, February 10). *MDPI*. Retrieved from MDPI: https://www.mdpi.com/2078-2489/13/3/146/htm

Kirsch, B. (2019, 10 03). *SearchITOperations*. Retrieved from techtarget: https://www.techtarget.com/searchitoperations/tip/Heed-these-cloud-security-considerations-for-SaaS-PaaS?utm_source=google&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lp03222022GOOGOTHR_GsidsITOperations_PaloAlto_Essential_IO158747_LI244289

Lutkevich, B. (2021, october). *SearchSecurity*. Retrieved from techtarget: https://www.techtarget.com/searchsecurity/definition/IP-spoofing

Nidecki, A. (2019, march 13). *Acunetix*. Retrieved from Acunetix: https://www.acunetix.com/blog/articles/man-in-the-middle-attacks/

Petcu, A. G. (2021, october 22). *heimdal security*. Retrieved from heimdal security: https://heimdalsecurity.com/blog/dns-spoofing/

Swinhoe, D. (2022, march 25). *CSO US*. Retrieved from CSO US: https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html

veracode. (n.d.). Retrieved from veracde: https://www.veracode.com/security/man-middle-attack