



slington 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 Kumar Thakur

London Met ID: 20049203

College ID: NP01NT4S210025

Assignment Due Date: 05/05/2022

Assignment Submission Date: 05/05/2022

Word Count (Where Required):5139

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 technical paper describes an **eavesdropping attack** utilizing the **man-in-the-middle attack** approach in a virtual network environment developed in GNS3 **from Kali Linux to Windows 10**. The **Ettercap** utilities are used to perform **ARP spoofing or ARP poisoning** on Windows 10 from Kali Linux, as well as the **mitigation** procedure to prevent man-in-the-middle attacks. The approach and implementation part of this study contains a detailed description of each assault. The **mitigation technique** for each target vector is described systematically in the mitigation part, with pertinent images. Finally, in the assessment portion of this report, the implemented mitigation method is critically analysed focusing on its pros, drawbacks, and **Cost Benefit Analysis (CBA)** calculation to end the repe.

Table of Contents

1. Introduction	1
1.1 Current Scenario.....	1
1.2. Aim	3
1.3. Objectives	3
2. Background	3
3. Demonstration	9
3.1 Tools used.	9
3.1.1. Graphical Network Simulator-3 (GNS3).	9
3.1.2. Kali linux.....	10
3.1.3. Windows 10.....	12
3.1.4. VMware Workstation.	13
3.2 Setting up virtual lab in	14
3.3. Man-in-the-middle (MITM) attack on the Windows 10 from Kali linux.	15
8. Mitigation.....	25
4. Evaluation	30
4.1 Pros.	30
4.2 Cons.	30
4.3 Cost benefit analysis.....	31
5. Conclusion	34
6. References.....	35

Figure 1: Man in the Middle attack scenario.....	2
Figure 2: Active Eavesdropping attack example	4
Figure 3 Regular traffic flow between two Computers	6
Figure 4 DNS Communication between the host and the DNS Server	7
Figure 5 The attacker performs MIM attack using DNS Spoofing	7
Figure 6: GNS3	9
Figure 7: Kali Linux.....	10
Figure 8: Ettercap.....	11
Figure 9: Wireshark.....	12
Figure 10: Windows 10.....	12
Figure 11: Workstation 16 pro	13
Figure 12: Setting up virtual lab in GNS3	14
Figure 13: IP address of Kali Linux	15
Figure 14: Checking connectivity from kali linux to windows 10	15
Figure 15: IP address of Windows 10.....	16
Figure 16: Checking connectivity from windows 10 to kali Linux.....	16
Figure 17 Command to open ettercap.....	17
Figure 18: Interface of Ettercap.....	17
Figure 19: Selecting eth0	18
Figure 20: Unified sniffing has started	18
Figure 21: Scan for host	19
Figure 22: Host list	19
Figure 23: Adding target.....	20
Figure 24: MITM menu	21
Figure 25: Sniff remote connection	21
Figure 26: selecting interface eth0 in wireshark	22
Figure 27: Capturing packet on wireshark.....	22
Figure 28: Test login.....	23
Figure 29: Captured Username and Password	24
Figure 30: Search for control panel	25
Figure 31: System and Security	26
Figure 32: Windows Defender Firewall.....	26
Figure 33: Windows Defender Firewall on or off	27
Figure 34: Turn on Windows Defender Firewall	28
Figure 35: Firewall is on	28
Figure 36: Checking connectivity after firewall is on.....	29
Figure 37: Network topology of Mithila institute of technology.....	32

1. Introduction

The most significant change in human history in recent years has been huge advancement in the field of digital technologies. It has become an important element of many people's daily lives. Business, education, farming, share-marketing, and a variety of other industries may see growth in international economies far faster than they have in the past, thanks to technological advancements. However, since the amount of viruses, cyber attackers, and harmful actions increases on a regular basis, it has increased the degree of risks and risk to humankind.

Brute-force attacks, phishing and sparring assaults are some of the most common types of attacks. Hackers use a variety of attack tactics to compromise the target vector, including drive-by assaults and **man-in-the-middle (MitM) attacks or Eavesdropping technique attack**.

When a hacker intercepts, erases, or changes data sent between two or more devices, it is called an eavesdropping assault. Sniffing and eavesdropping, commonly known as network sniffing and eavesdropping, exploit unencrypted network connections to collect data in transit devices. (Fortinet, 2022)

1.1 Current Scenario

It is well known that there is a large number of individuals using the internet and this number is growing every day. As a result, it becomes vital to secure data on the internet and maintain the internet security since there are many bad guys out there who would want to reap the benefits of this and have data breaches and other types of cyberattacks without being detected.

Eavesdropping is one of the various attacks that occur these days. One type of eavesdropping attack is **man-in-the-middle (MITM)**. Wi-Fi eavesdropping, email hijacking, and IP spoofing are the most popular targets for man-in-the-middle attacks. Attackers trying MITM threats **accounted for 35% of exploitation** activity, according to IBM X- Force's Intelligence 2018 Index. (DOBRAN, 2019)

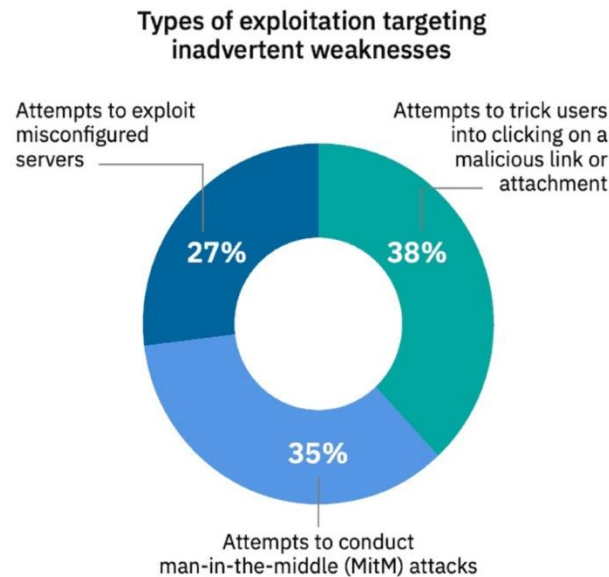


Figure 1: Man in the Middle attack scenario

After the Dutch registrar site, DigiNotar was hacked in 2011, one threat actor obtained certificates for 500 websites such as Google, Skype, and others. With access to these certificates, the attacker could impersonate genuine websites in an MITM attack, collecting data from victims after duping them into entering passwords on malicious mirror sites. As a result of the hack, DigiNotar ended up filing for bankruptcy (VERACODE, 2022).

After a data breach in 2017, credit score business Equifax had its applications pulled from Google and Apple's stores. According to the researchers, the app doesn't always use HTTPS, which allows attackers to capture data when users access their accounts. (VERACODE, 2022)

1.2. Aim

- This document is intended to provide up-to-date information on **Eavesdropping methods** and **man-in-the-middle (MITM) attacks** against information technology and systems.

1.3. Objectives

- To give in-depth information on one of the eavesdropping methods, the Man in the middle attack.
- To design network topology in Graphical Network Simulator-3 (GNS-3).
- To show the man in the middle attack from Kali Linux to Windows 10 and Router.
- To use an appropriate mitigation plan and critically analyze it by describing its benefits and downsides, as well as calculating the Cost Benefit Analysis (CBA).

2. Background

An eavesdropping attack occurs when a hacker intercepts, erases, or modifies data transferred between two or more devices. Network sniffing and Network Snooping, also known as eavesdropping, uses unprotected network connections to acquire data in transit machines (Fortinet, 2022). Network eavesdropping, such as tuning in on a conversation between two people, includes tuning in on talks across network parts like servers, PCs, cell phones, and other associated devices. (Shea, 2022)

Hackers hunt for weak connections between clients and servers in network eavesdropping attacks, such as those that are not encrypted, use out-of-date devices or software, or have malware installed via social engineering. Hackers intercept data packets transiting the network by exploiting these weak connections. A hacker can read any network, online, or email traffic that isn't encrypted.

Sniffer applications are frequently installed by hackers. Security teams frequently use legal software like Wireshark, Snort, and tcpdump to look for weaknesses and vulnerabilities in network communication by monitoring and analyzing it. However, bad actors may use these applications to identify and exploit the same vulnerabilities. Eavesdropping attacks may be divided into two categories:-

- Passive eavesdropping attack.
- Active Eavesdropping attack.

In a passive eavesdropping attack, the attacker or sniffer program just obtains data about its victim; the data has never been modified. Passive eavesdropping attacks include voice over IP (VoIP) eavesdropping. To listen in on unencrypted VoIP calls, a hacker or sniffer broke into the network using a compromised VoIP device or an element of the VoIP infrastructure, such as a switch, cable, or the internet. (Shea, 2022)

Hackers penetrate the network and pretend to be a real connection **in an active eavesdropping attack**. Hackers can inject, change, or block transmissions during active eavesdropping attacks.

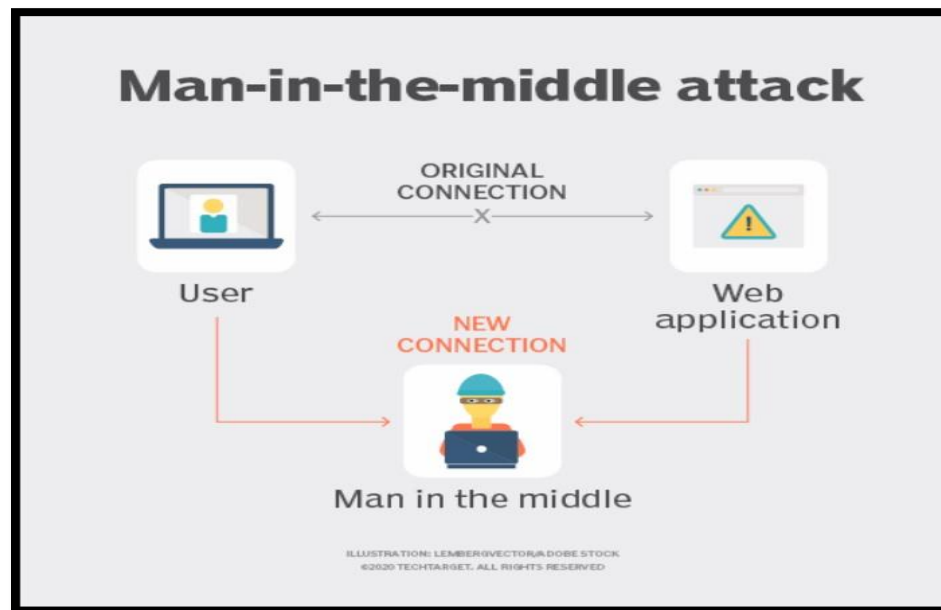


Figure 2: Active Eavesdropping attack example

Man-in-the-middle (MITM) attacks are the most widely active eavesdropping attacks. Malware or spoofing attacks, such as **Address Resolution Protocol (ARP)**, DNS, Dynamic Host Configuration Protocol, IP, or MAC address spoofing, are used to infiltrate systems in MitM attacks. By professing to be an authentic entity, attackers could catch information at any point as well as modify it and communicate it to different gadgets

and clients after gaining access to the framework through a man-in-the-middle attack. (Shea, 2022)

Interception and **decryption** are the two steps of a successful MITM attack. **Interception** occurs when an attacker disrupts a victim's genuine network by intercepting it with a fake network before it reaches its intended destination. The attacker puts oneself as the "man in the middle" during the interception phase. Attackers commonly achieve this by setting up a fake public WI-Fi hotspot that doesn't require a password. When a victim connects to the hotspot, the attacker obtains access to all of the victim's online data exchanges.

Once the attacker has successfully inserted himself between the victim and the target destination, the attacker can use a variety of tactics to prolong the attack time, including **IP spoofing**, **Address Resolution Protocol (ARP) spoofing**, and **DNS spoofing** (Panda Security, 2021).

- **IP Spoofing:-** Every computer on a network is assigned an IP address, which it uses to interact with other computers on the same network. IP addresses occur in a variety of formats; the most prevalent, known as IPv4, assigns a 32-bit identity to each machine (e.g. 192.168.34.12). The security of digital assets and applications is maintained on certain networks by defining which IP addresses have access to which resources. An IP spoofing attack occurs when a malicious actor hides their identity by impersonating a legitimate device's IP address in order to get access to resources that would otherwise be out of reach (Secret Double Octopus, 2021).

Access to a server, for example, might be restricted to a specified set or range of IP addresses. A hacker modifies network packets so that the sender's address seems to be that of a real machine. The attacker deceives the server into believing the packets are originating from a trusted source.

In **man in the middle attacks**, IP spoofing can be utilized. The attacker stands between two communication parties in this example, spoofing each of their addresses to the other. Instead than delivering their network packets to their

intended destination, each victim sends them to the attacker (Secret Double Octopus, 2021).

- **ARP Spoofing:-** The Address Resolution Protocol (**also known as ARP poisoning**) is a network communication protocol that allows network messages to reach a specified network device. ARP converts Internet Protocol (IP) addresses to Media Access Control (MAC) addresses and the other way around. ARP is most typically used by devices to communicate with the router or gateway that allows them to connect to the Internet. (Imperva, 2021)

In regular ARP, the host PC will transmit a packet containing the source and destination IP addresses and broadcast it to all devices connected to the network. The device with the destination IP address will only send an ARP reply with its MAC address, after which communication will occur. The ARP protocol is not a secure protocol, and the ARP cache lacks a failsafe mechanism, resulting in a major issue (Gangan, 2015).

The ARP reply packet is simply spoofable, and it may be forwarded to the computer that submitted the ARP request without the sender knowing that it is not the genuine machine, but rather a data breach attempt. This occurs because the ARP cache table will be modified according to the attacker's wishes, and so all network traffic will pass via the attacker, giving him complete control over the data. This is the most effective type of assault on a local area network.

Ettercap, **Dsniff**, and **Cain and Abel's** are just a few examples of ARP Cache poisoning tools available on the market (Gangan, 2015).

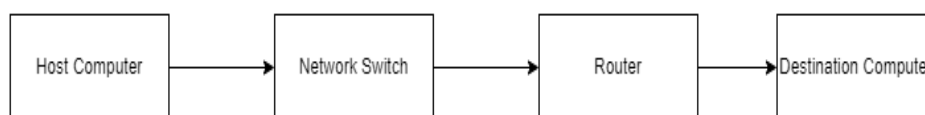


Figure 3 Regular traffic flow between two Computers

- **DNS Spoofing:-** In this situation, the target will be given false information, resulting in the loss of credentials. As previously said, this is an online MITM attack in which the attacker has constructed a false website of your bank, and when you visit your bank's website, you will be routed to the attacker's website, where the attacker will obtain access to all of your credentials. When we visit a website on our computer,

a DNS request is made to the DNS Server, and we receive a DNS response message. This is shown with the help of figure 4 (Gangan, 2015).

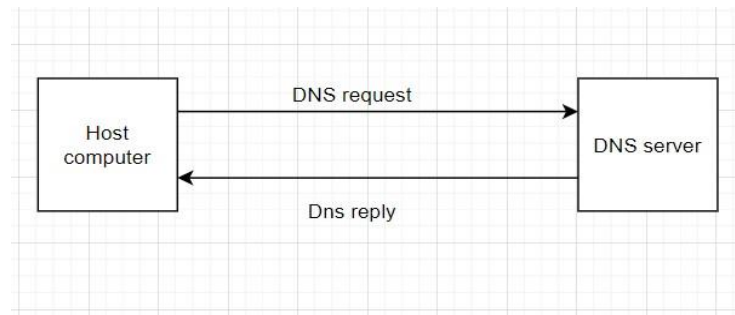


Figure 4 DNS Communication between the host and the DNS Server

This DNS request and response are linked by a unique identifier. If the attacker obtains the unique identification number, the attack can be started by disguising the victim with a corrupt packet containing the identification number. The attacker uses ARP cache poisoning to reroute the DNS request message to which the bogus reply packet is delivered, redirecting the victim to the phony website (Gangan, 2015).

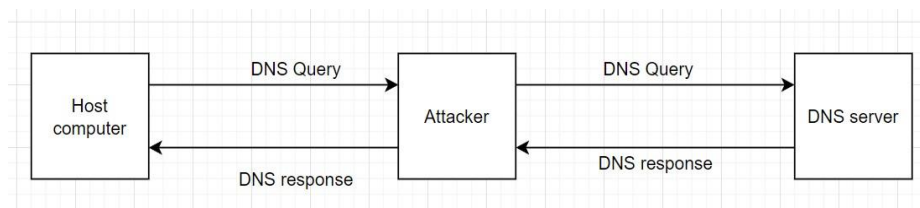


Figure 5 The attacker performs MIM attack using DNS Spoofing

When the host computer wishes to connect to a website, it sends a DNS query request to the DNS server. However, the MIM attack intercepts this DNS query and sends a bogus DNS response to the host computer. The host PC will not be able to tell if the answer is authentic or not, and it will begin connecting with the attacker's malicious website, resulting in data leaks (Gangan, 2015).

Interception is only the beginning of a man in the middle attack. Once the attacker has gained access to the victim's encrypted data, it must be **decrypted** before the attacker may read and use it. To **decrypt** the victim's data without notifying the user or program,

a variety of ways might be used, some of them are HTTPS Spoofing, SSL Hijacking and SSL Stripping (Panda Security, 2021).

- **HTTPS Spoofing:-** HTTPS spoofing is a technique for deceiving your browser into believing a website is safe and genuine when it isn't. When a victim attempts to access to a secure site, their browser receives a bogus certificate, redirecting them to the attacker's fake website. This allows the hackers to gain access to whatever information that the victim shares on the website (Panda Security, 2021).
- **SSL Hijacking:-** Your server automatically reroutes you to the secure HTTPS version of a website if you connect to an insecure website with "HTTP" in the URL. The attacker intercepts the reroute using their own computer and server, allowing them to disrupt any information transmitted between both the user's computer and the server. This grants hackers exposure to whatever sensitive data the user enters throughout their session (Panda Security, 2021).
- **SSL Stripping:-** When an attacker uses SSL stripping, he or she breaks the connection between a user and a website. This is accomplished by redirecting a user's secure HTTPS connection to the website's insecure HTTP version. This links the user to the insecure site while the attacker establishes a secure site connection, allowing the attacker to see the user's behaviour in an unencrypted form (Panda Security, 2021).

3. Demonstration

3.1 Tools used.

The tools used for this demonstration process are GNS3, and two operating system and they are Kali linux and windows 10.

3.1.1. Graphical Network Simulator-3 (GNS3).

Hundreds of thousands of network engineers throughout the world use GNS3 to mimic, setup, test, and debug virtual and real networks. GNS3 enables you to operate topologies ranging from a few devices on your laptop to numerous devices hosted on several servers or even in the cloud (Galaxy Technologies LLC, 2021). As a result, we will be able to mimic a Man-in-the-middle attack against numerous operating systems without breaching any ethical standards or employing any software illegally or improperly.

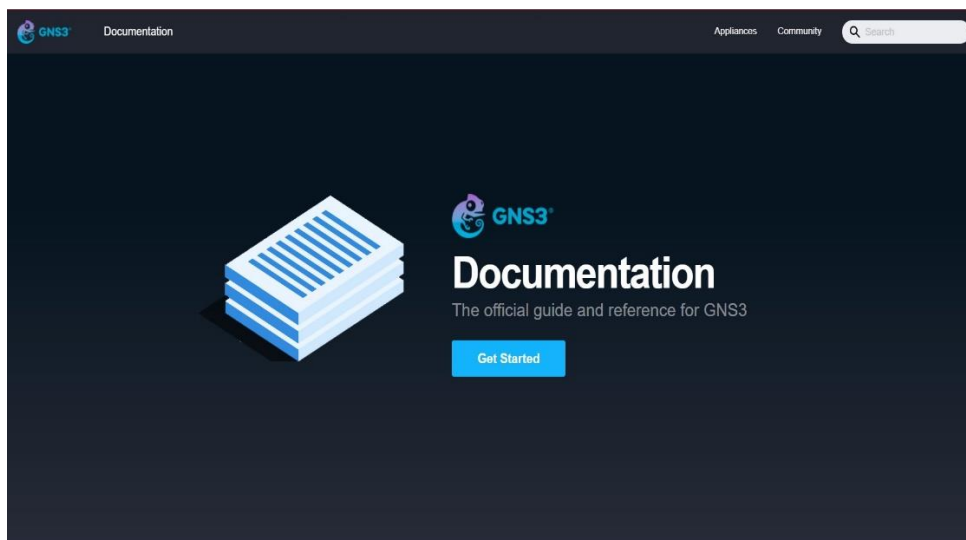


Figure 6: GNS3

3.1.2. Kali linux.

Kali Linux is a Debian-based open-source Linux system designed for sophisticated penetration testing and security auditing. Kali Linux includes hundreds of tools for diverse information security activities such as penetration testing, security research, computer forensics, and reverse engineering. Kali Linux is a multi-platform solution that is both accessible and free to information security experts and enthusiasts (OffSec Services Limited, 2022). In this scenario we will use kali linux tools, **Ettercap** and **Wireshark** to demonstrate man-in-the-middle attack on windows 10.



Figure 7: Kali Linux

3.1.2.1 Ettercap.

Ettercap supports both active and passive protocol dissection (including encrypted protocols) and provides several features for network and host investigation. Data injection in an existing connection is also conceivable, as is on-the-fly filtering (substitute or discard a packet) to maintain the connection synchronized (OffSec Services Limited, 2022).

Many sniffing modalities are included, resulting in a robust and comprehensive sniffing suite. Sniffing is supported in four modes: IP-based, MAC-based, ARP-based (full-duplex), and PublicARP-based (half-duplex). Ettercap can also identify a switched LAN and utilize OS fingerprints (active or passive) to determine the geometry of the LAN. The ettercap GUI-enabled executable is included in this package (OffSec Services Limited, 2022).



Figure 8: Ettercap

3.1.2.2 Wireshark.

Wireshark is a network "sniffer," which means it catches and analyzes packets across the connection. In this example attack, it captures packets to collect user credentials.

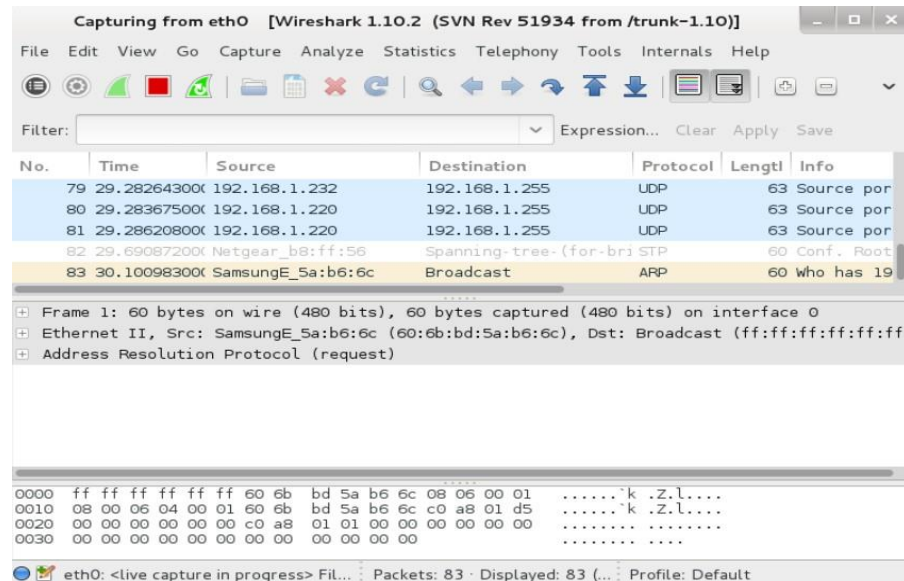


Figure 9: Wireshark

3.1.3. Windows 10.

Microsoft created the Windows operating system. A computer's operating system is what allows you to utilize it. Most new personal computers (PCs) come preinstalled with Windows, making it the biggest and most popular operating system (GCFGlobal, 2022). So, in this windows we are going to attack from kali linux.

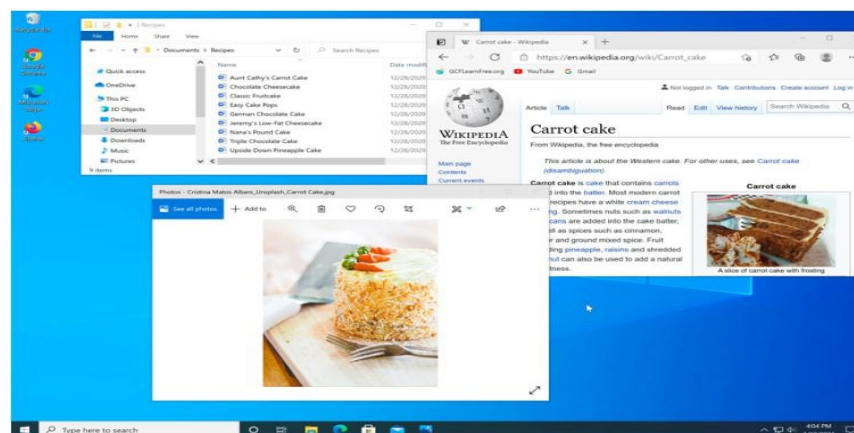


Figure 10: Windows 10

3.1.4. VMware Workstation.

VMware Workstation is a virtual machine program that allows you to run different operating systems on a single physical host computer on x86 and x86-64 machines. Each virtual machine may run a single instance of any operating system (Microsoft, Linux, etc.) concurrently. Hard drives, USB devices, and CD-ROMs are all supported by VMware Workstation, which acts as a bridge between the host and virtual system. The host computer is used to install all device drivers (techopedia, 2022). In this workstation operation system like windows 10 and Kali linux is installed to operate demonstration attack. In this demonstration process we start operation systems in workstation by using GNS3.

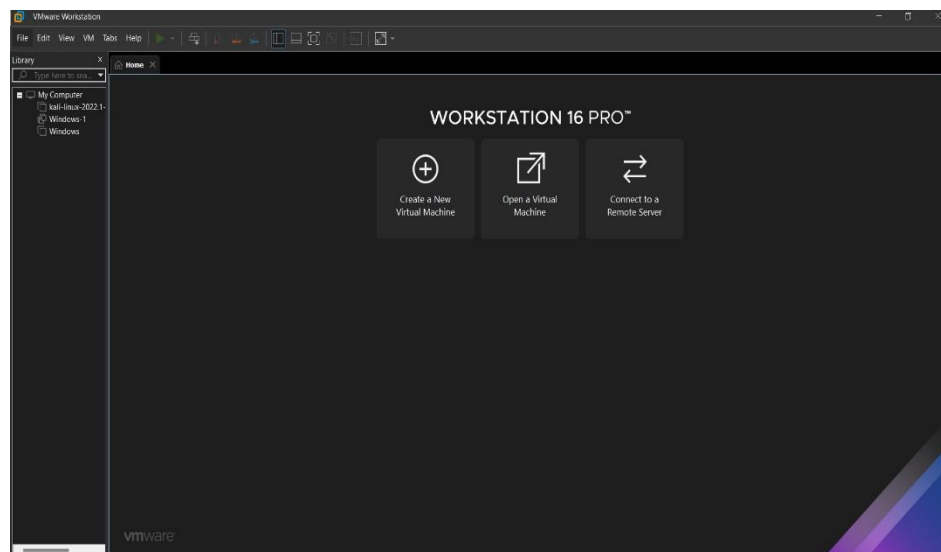


Figure 11: Workstation 16 pro

3.2 Setting up virtual lab in Graphical Network Simulator-3 (GNS3).

The **GNS3** is used for setting up virtual topology for successful attack. The GNS3 helps to simulate man-in-the-middle attack. In GNS3 there is one **Cloud for internet**, **c3725 router**, one **Ethernet switch** and **two operating system Kali-linux and windows 10**.

The kali-linux and windows 10 is connected with Ethernet switch through interface e1 and e2 respectively and the Ethernet switch is connected through e0 interface of switch to interface f0/0 with router (R1). The router R1 is connected through interface f0/1 with VMware Network Adapter VMnet 18 in cloud1. The operating system kali-linux and windows 10 are connected through **custom (VMnet17)** and **custom (VMnet19)** for communication. The router is connected through **VMnet18 on Network Address Translation (NAT)** through cloud1 for **internet connection**. The IP address of default gateway is **10.10.10.1** in interface f0/0. The IP address of kali-linux and windows 10 are **10.10.10.255** and **10.10.10.15** respectively. The IP address of f0/1 interface in router is **192.168.161.130** and **VMware Network Adapter VMnet18 IP address is 192.168.161.2**. The figure of topology is given below:-

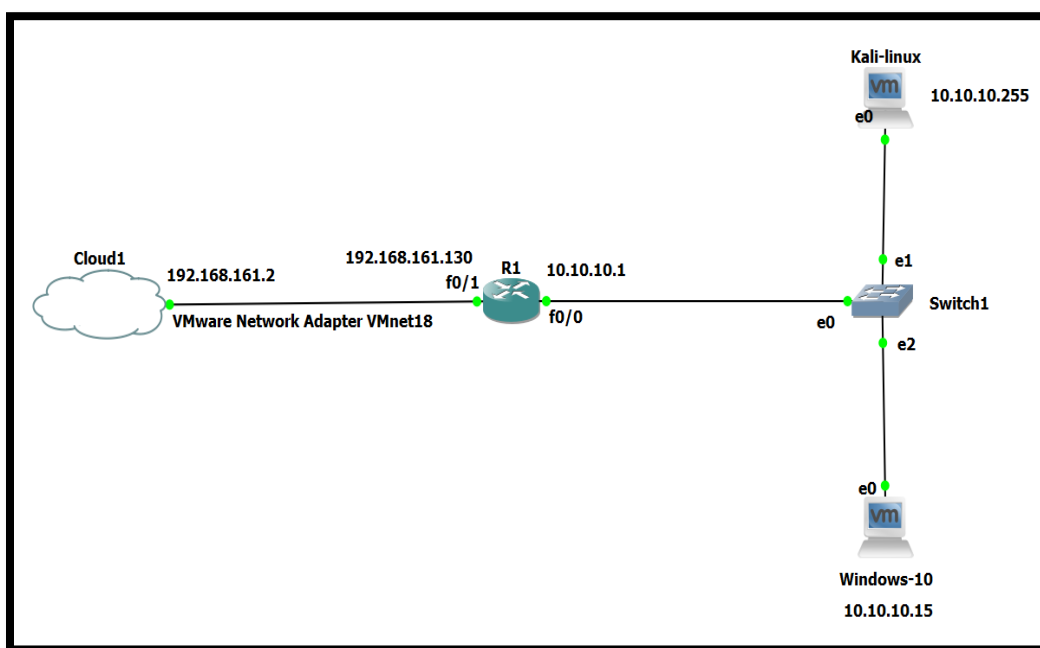
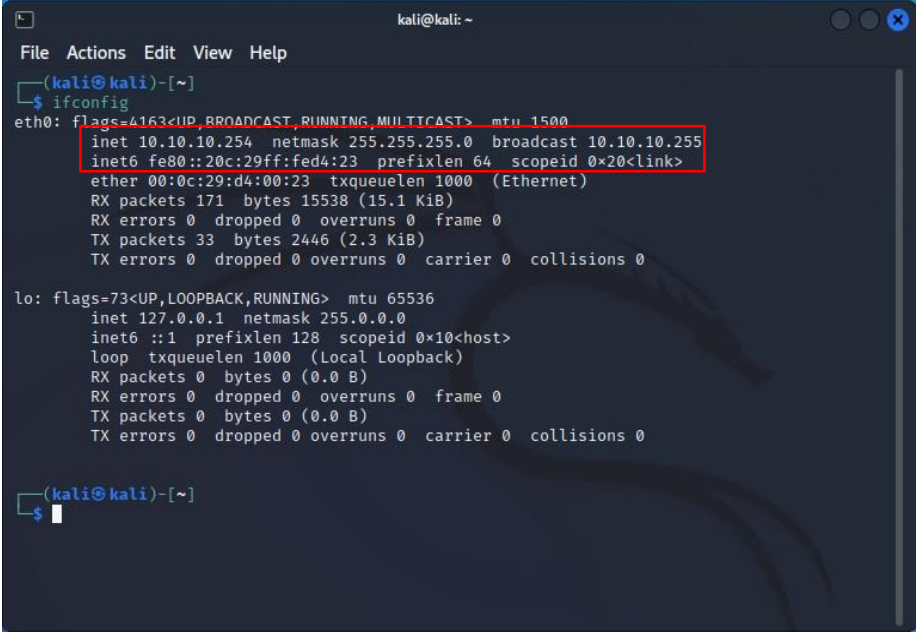


Figure 12: Setting up virtual lab in GNS3

3.3. Man-in-the-middle (MITM) attack on the Windows 10 from Kali linux.

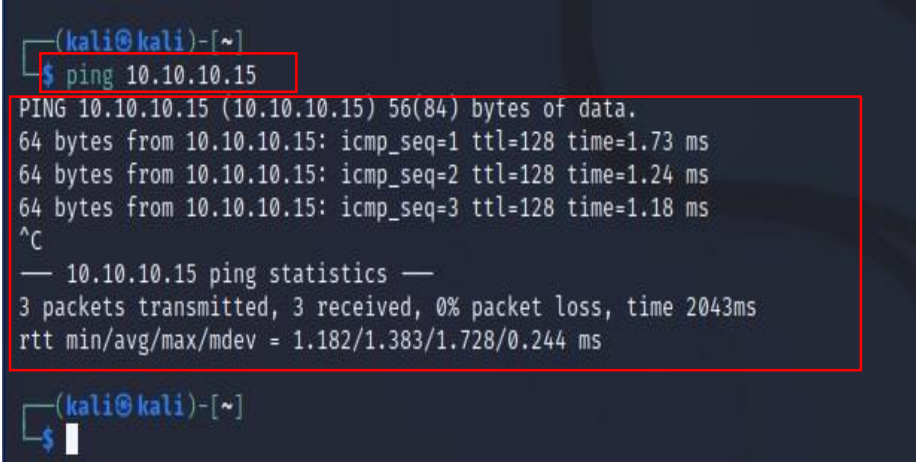
Step 01: Check for kali linux and Windows 10 connection.

Enter the ping command and the IP address of Windows 10 in kali linux to test connectivity between Kali Linux and Windows 10 .And also enter the ping command and the IP address of kali linux in windows 10 to test connectivity between windows 10 and kali linux. As indicated in figure, Kali Linux's IP address is 10.10.10.254, whereas Windows 10's IP address is 10.10.10.15.



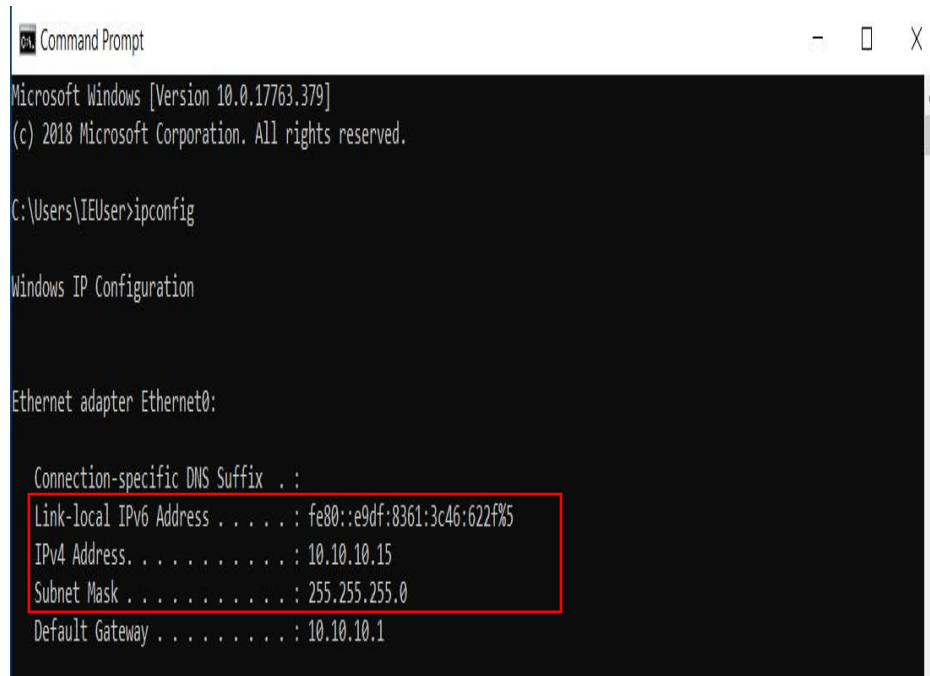
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.10.10.254 netmask 255.255.255.0 broadcast 10.10.10.255  
    inet6 fe80::20c:29ff:fed4:23 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:d4:00:23 txqueuelen 1000 (Ethernet)  
    RX packets 171 bytes 15538 (15.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 33 bytes 2446 (2.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 0 bytes 0 (0.0 B)  
    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  
  
(kali@kali)-[~]  
$
```

Figure 13: IP address of Kali Linux



```
(kali@kali)-[~]  
$ ping 10.10.10.15  
PING 10.10.10.15 (10.10.10.15) 56(84) bytes of data:  
64 bytes from 10.10.10.15: icmp_seq=1 ttl=128 time=1.73 ms  
64 bytes from 10.10.10.15: icmp_seq=2 ttl=128 time=1.24 ms  
64 bytes from 10.10.10.15: icmp_seq=3 ttl=128 time=1.18 ms  
^C  
— 10.10.10.15 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2043ms  
rtt min/avg/max/mdev = 1.182/1.383/1.728/0.244 ms  
  
(kali@kali)-[~]  
$
```

Figure 14: Checking connectivity from kali linux to windows 10

A screenshot of a Windows Command Prompt window. The title bar says "Command Prompt". The text inside shows the Windows version (10.0.17763.379) and copyright (c) 2018 Microsoft Corporation. The user has entered the command "ipconfig". The output shows the Windows IP Configuration for the Ethernet adapter Ethernet0. A red rectangle highlights the following information: Link-local IPv6 Address (fe80::e9df:8361:3c46:622f%5), IPv4 Address (10.10.10.15), Subnet Mask (255.255.255.0), and Default Gateway (10.10.10.1).

```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

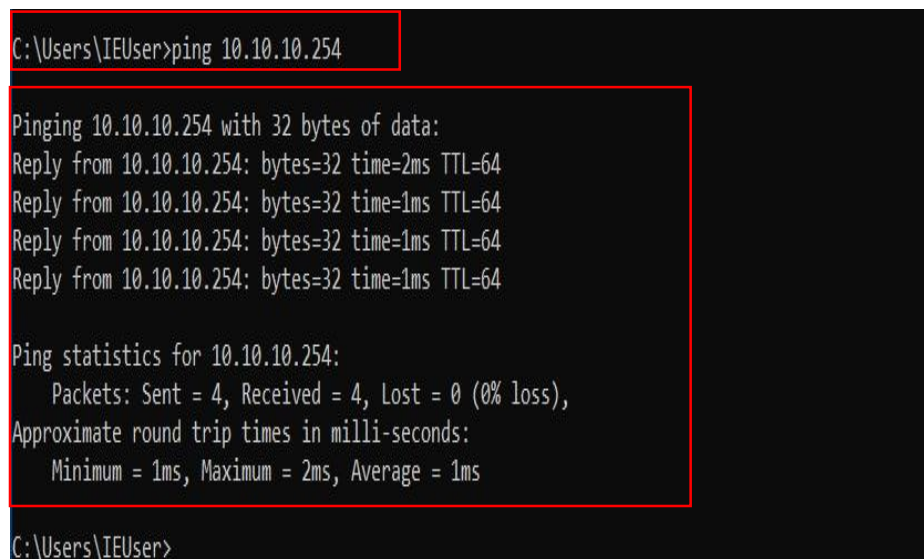
C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e9df:8361:3c46:622f%5
    IPv4 Address. . . . . : 10.10.10.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1
```

Figure 15: IP address of Windows 10

A screenshot of a Windows Command Prompt window. The user has entered the command "ping 10.10.10.254". The output shows the ping results for 10.10.10.254. A red rectangle highlights the entire output of the ping command, including the statistics. The output shows that 4 packets were sent, 4 were received, and there was 0% loss. The approximate round trip times in milliseconds are: Minimum = 1ms, Maximum = 2ms, Average = 1ms.

```
C:\Users\IEUser>ping 10.10.10.254

Pinging 10.10.10.254 with 32 bytes of data:
Reply from 10.10.10.254: bytes=32 time=2ms TTL=64
Reply from 10.10.10.254: bytes=32 time=1ms TTL=64
Reply from 10.10.10.254: bytes=32 time=1ms TTL=64
Reply from 10.10.10.254: bytes=32 time=1ms TTL=64

Ping statistics for 10.10.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\IEUser>
```

Figure 16: Checking connectivity from windows 10 to kali Linux

Step 2:- Start Ettercap.

Click on the command terminal in Kali Linux and type "sudo ettercap -G." When prompted for a password, type kali linux password. It will then launch an Ettercap window with the ominous Ettercap logo.

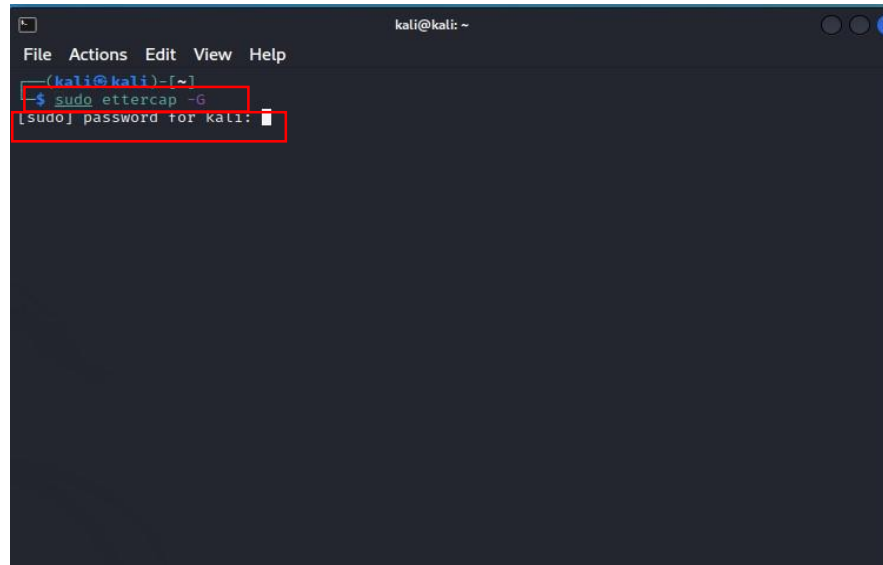


Figure 17 Command to open ettercap

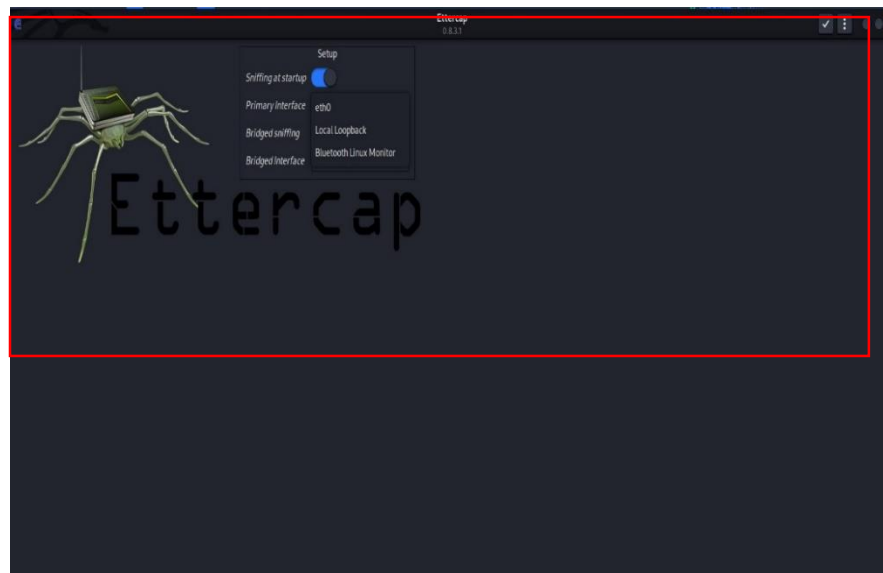


Figure 18: Interface of Ettercap

Step 3:- Select network interface for sniffing.

The primary interface may be found under setup in the Ettercap terminal. The network interface that is currently connected to the network you are attacking should be chosen. Simply set the interface to eth0.

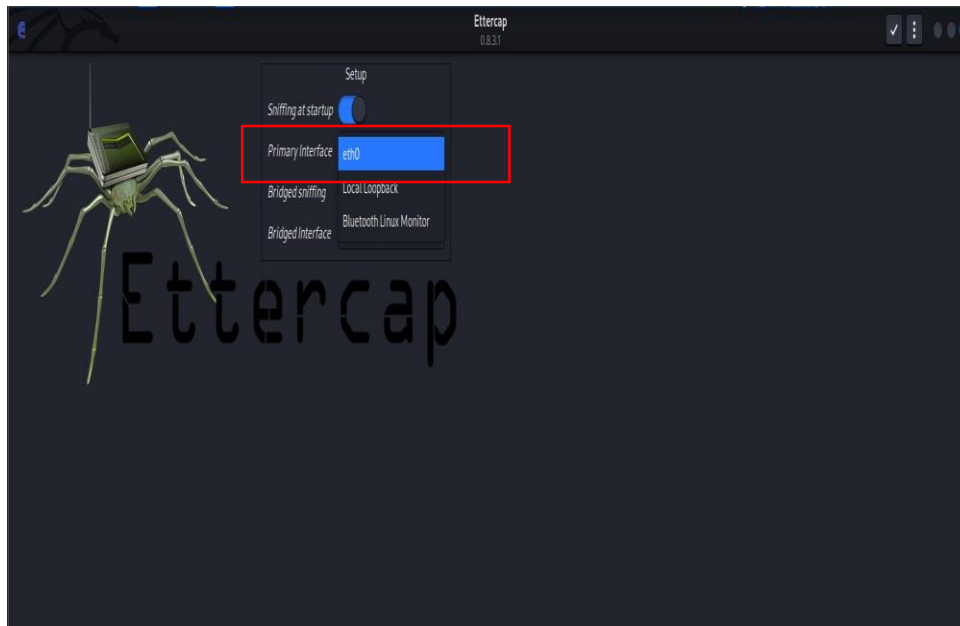


Figure 19: Selecting eth0

Now, some text confirming that unified sniffing has started.

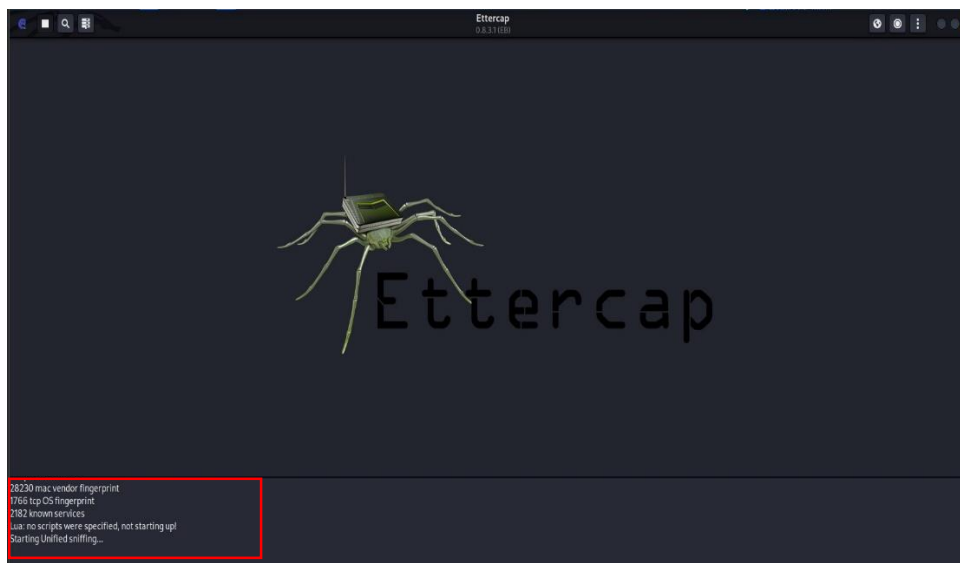


Figure 20: Unified sniffing has started

Step 4: Find the target from the host list.

Scan for hosts by clicking "Hosts," then "Scan for hosts" to discover the device to attack. There is a hosts list when the scanning is completed. After that, choose the host and add it to target1.

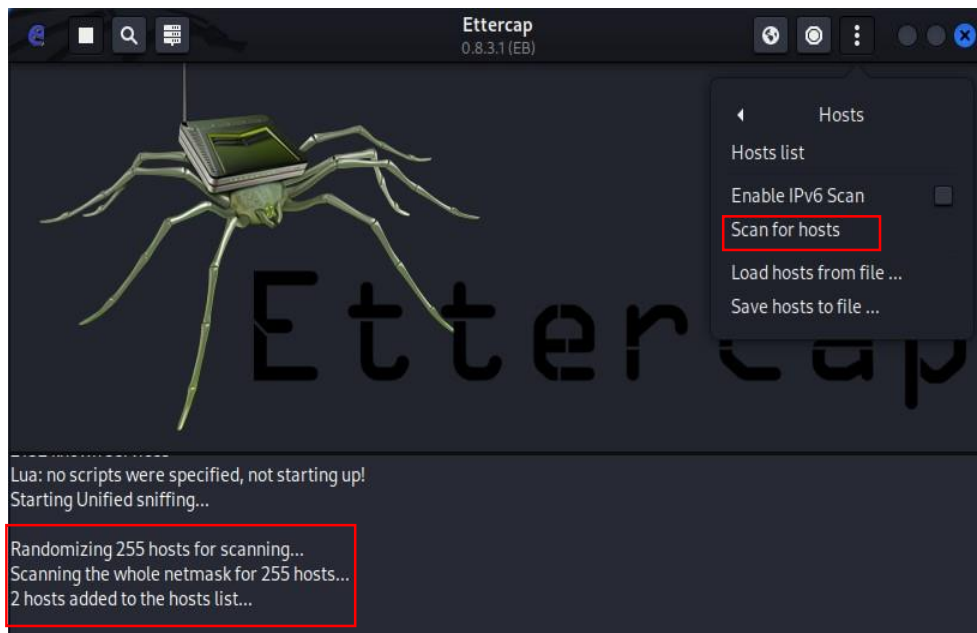


Figure 21: Scan for host

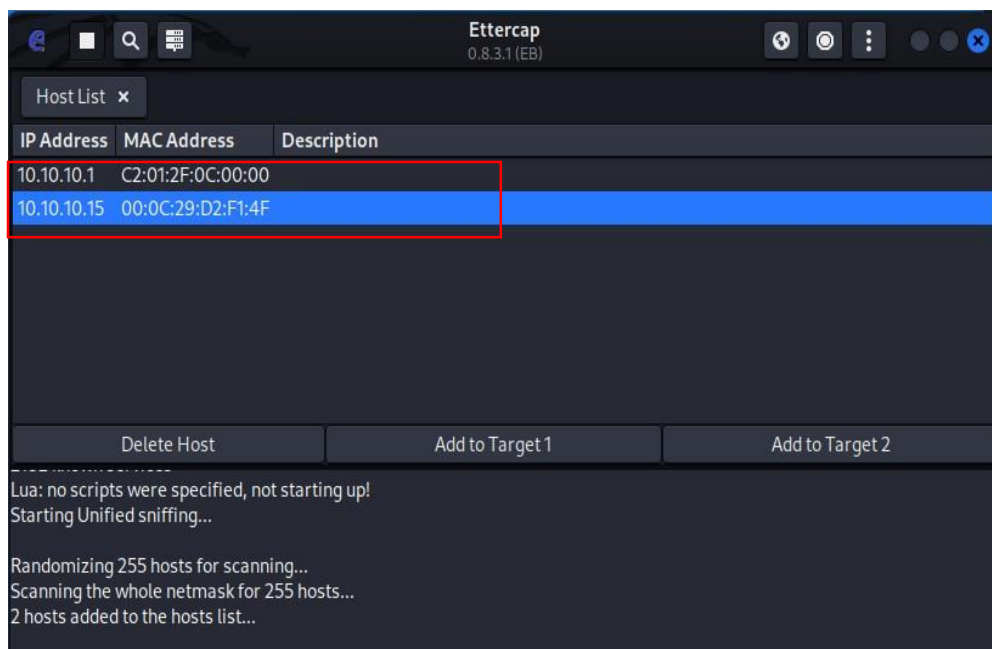


Figure 22: Host list

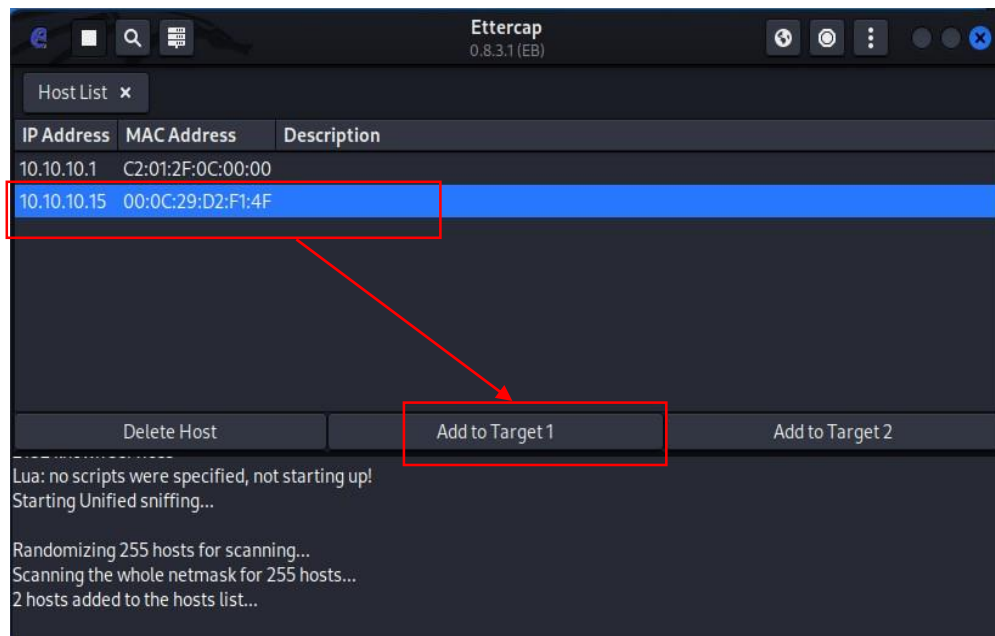


Figure 23: Adding target

Step 5:- Ready for man-in-the-middle attack on target.

Select "ARP poisoning" from the "MITM" drop-down option. To start the sniffing attack, a box will appear, and you'll pick "Sniff remote connections" and hit OK. Launch an assault with unified sniffing now.

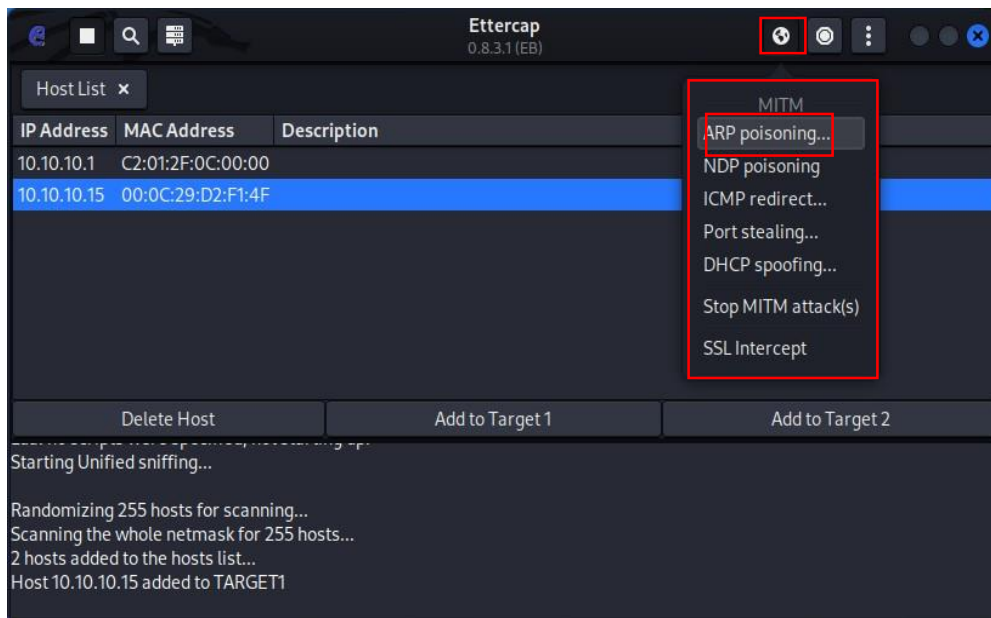


Figure 24: MITM menu

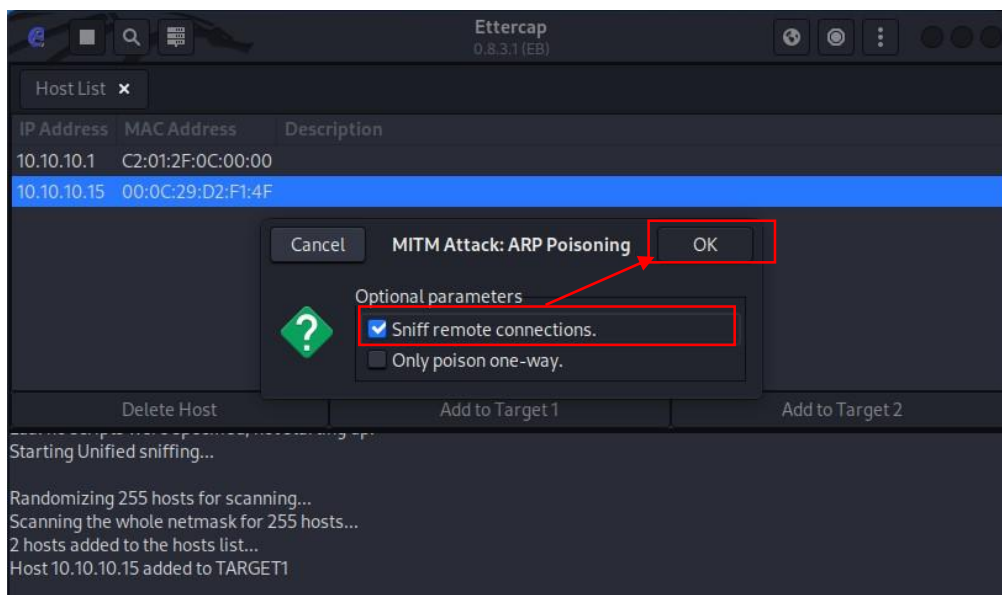


Figure 25: Sniff remote connection

Step 6:- Open Wireshark

Now type wireshark to open the wireshark terminal. Select the same network interface eth0 from the terminal. This will begin traffic monitoring. You will be able to intercept login passwords and all advanced information once the assault begins.

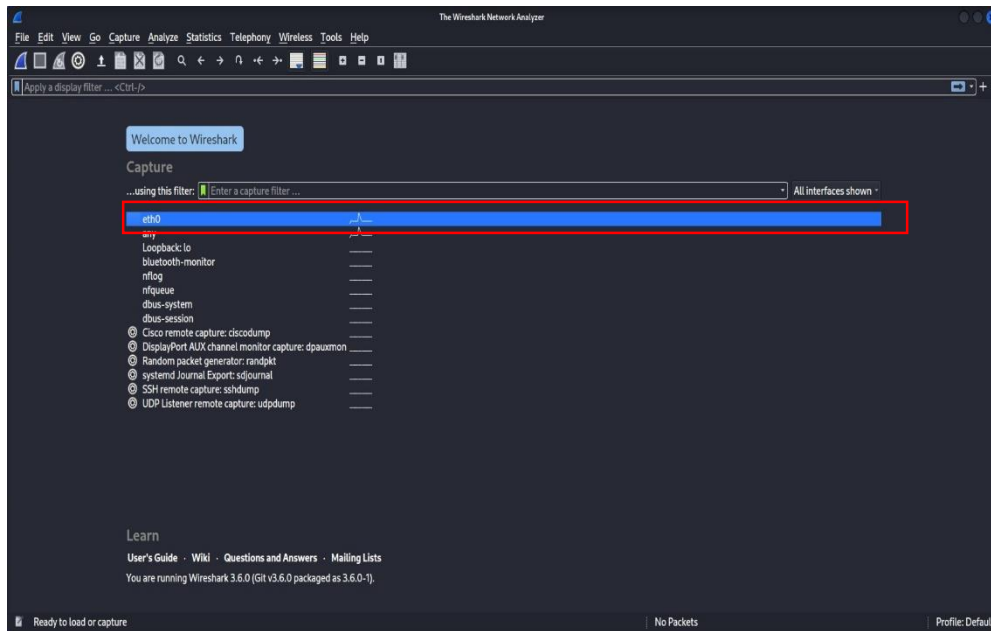


Figure 26: selecting interface eth0 in wireshark

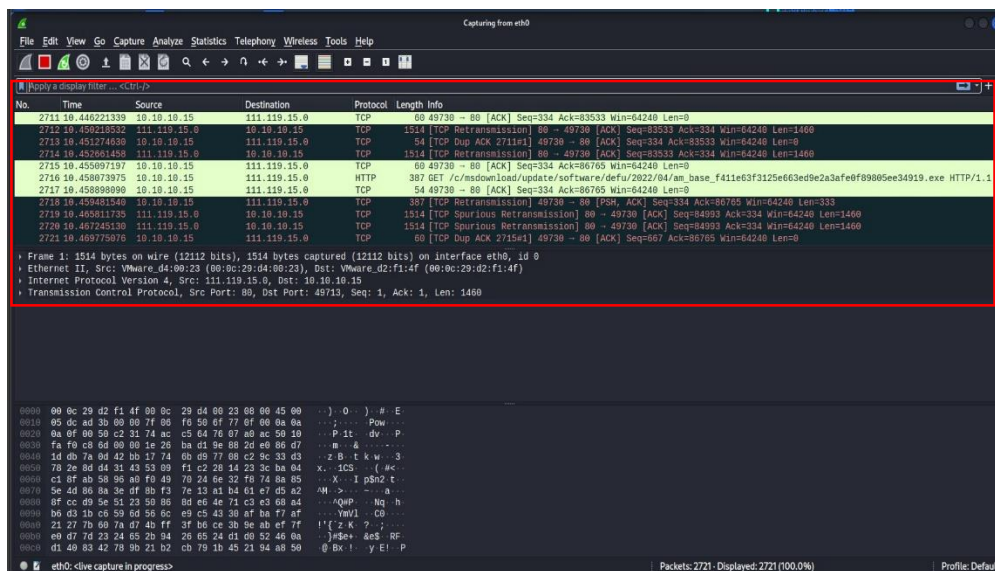


Figure 27: Capturing packet on wireshark

Step 7:- Try to intercept password.

Now, in order to practice intercepting passwords, we'll utilize a fake website with poor security so that credentials may be intercepted. Navigate to `testphp.vulnweb.com` upon this targeted system while connecting to a certain wi-fi connection. Then clicking on login and input your username (rajthakur) and password (password).

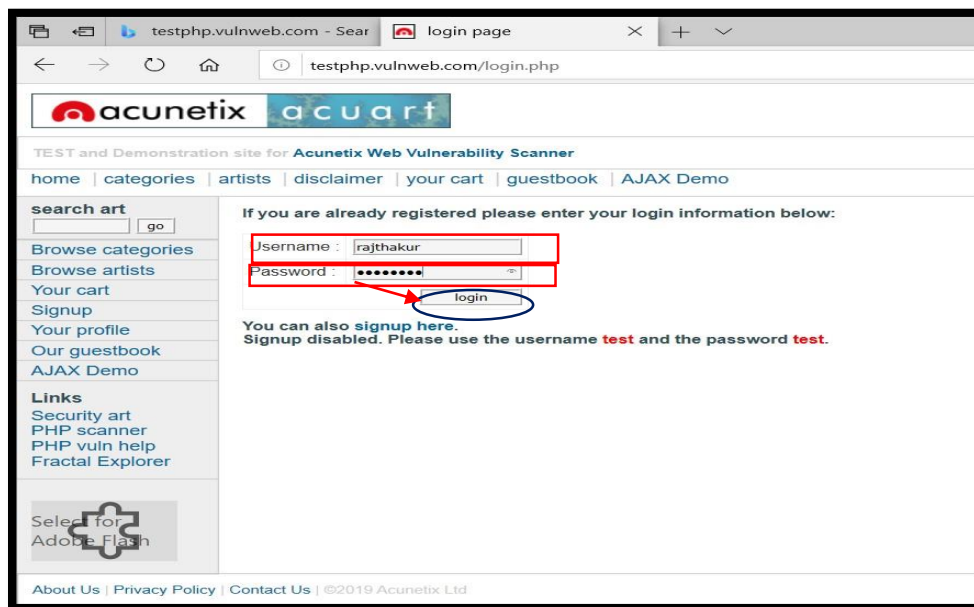


Figure 28: Test login

Step 8:- Username and password is captured.

Ettercap automatically record your username, password, and website after you've logged in. In the Wireshark terminal, you'll be able to see some detailed info.



Figure 29: Captured Username and Password

8. Mitigation

We know that IP addresses or mac addresses are responsible for communication between Windows 10 and the Internet connection, as we demonstrated in the assault section. As a result, ARP poisoning might affect an IP address or a mac address.

In a man-in-the-middle attack, the attacker may simply connect with Windows 10 through IP address or mac address. There are several options for reducing this danger. The easiest approach to stop all incoming ARP poisoning in Windows 10 is to turn on the firewall. The procedures to turn on the firewall are outlined below.

Step 01: Control Panel was found after a brief search in the search box. It was double-clicked once it appeared, as seen in the image below.

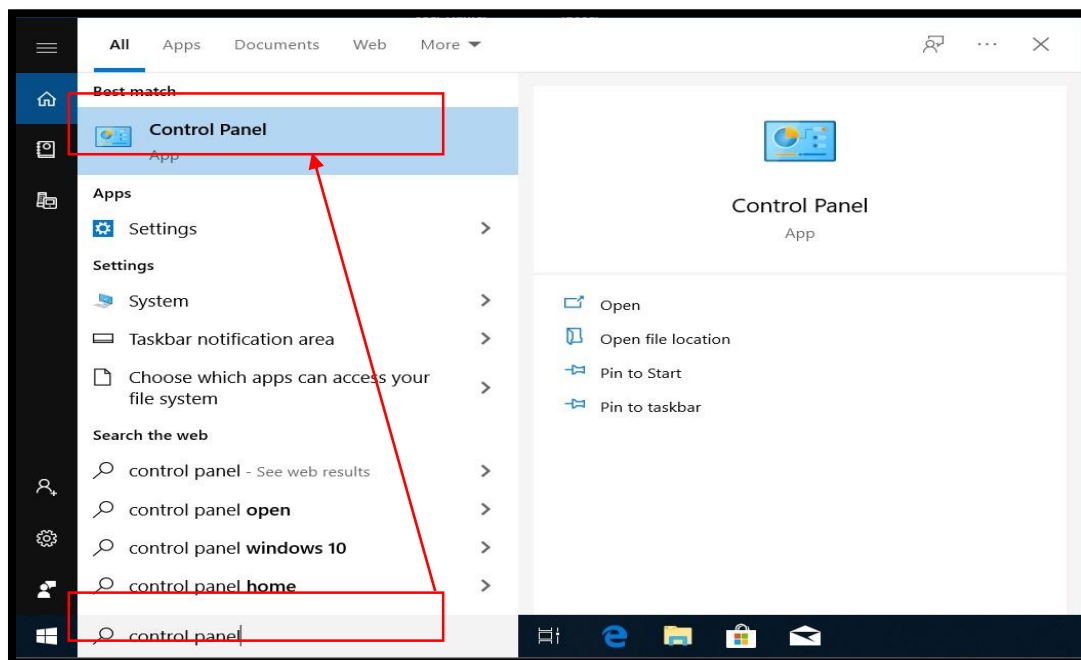


Figure 30: Search for control panel

Step 02: Double-click the "System and Security" tab in the Control panel to see the needed configuration choices.

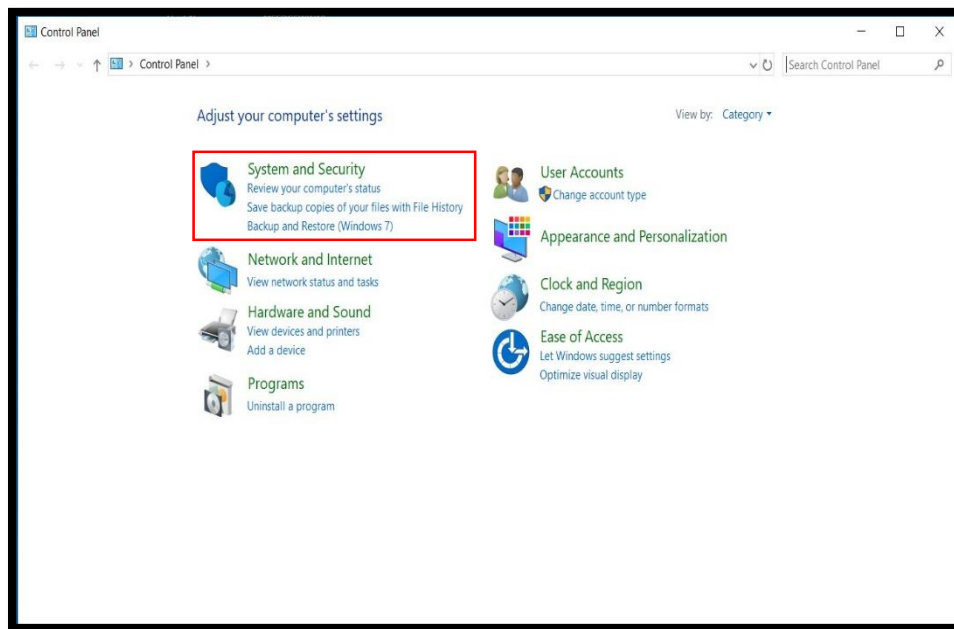


Figure 31: System and Security

Step 03: Then, to open it, double-click "Windows Defender Firewall".

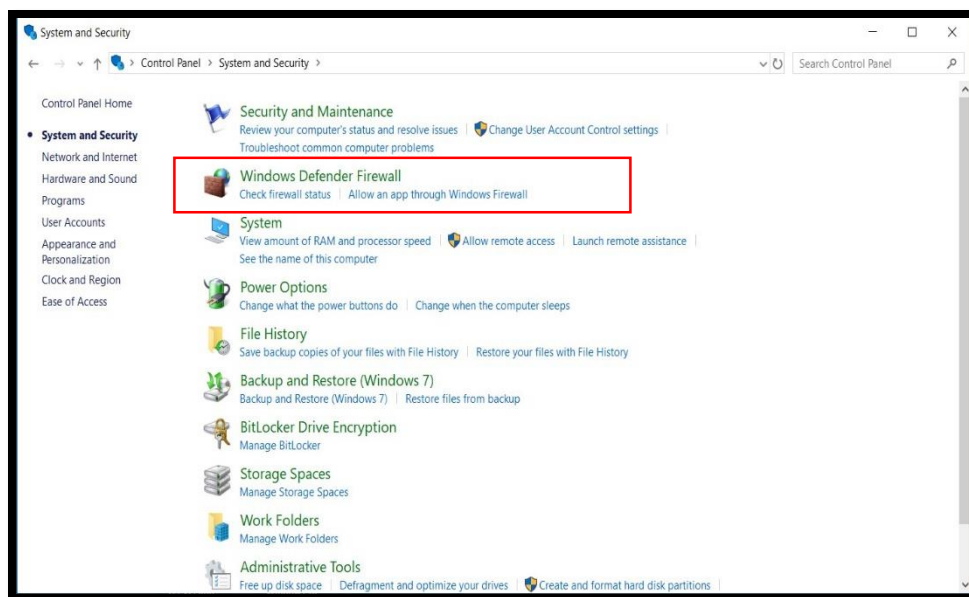


Figure 32: Windows Defender Firewall

Step 04: Then, to open it, click "Windows Defender Firewall on or off".

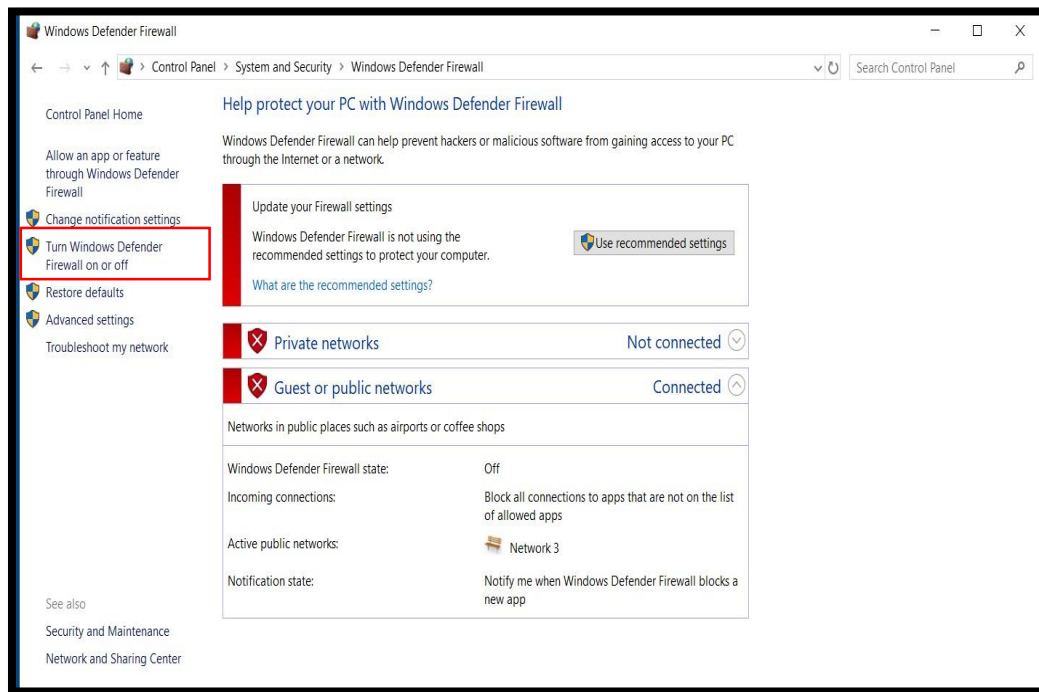


Figure 33: Windows Defender Firewall on or off

Step 05: Then "Turn on Windows Defender Firewall and check on, alert me when Windows Defender Firewall blocks a new app" for private network settings and "Turn on Windows Defender Firewall and check on, notify me when Windows Defender Firewall blocks a new app" for public network settings.

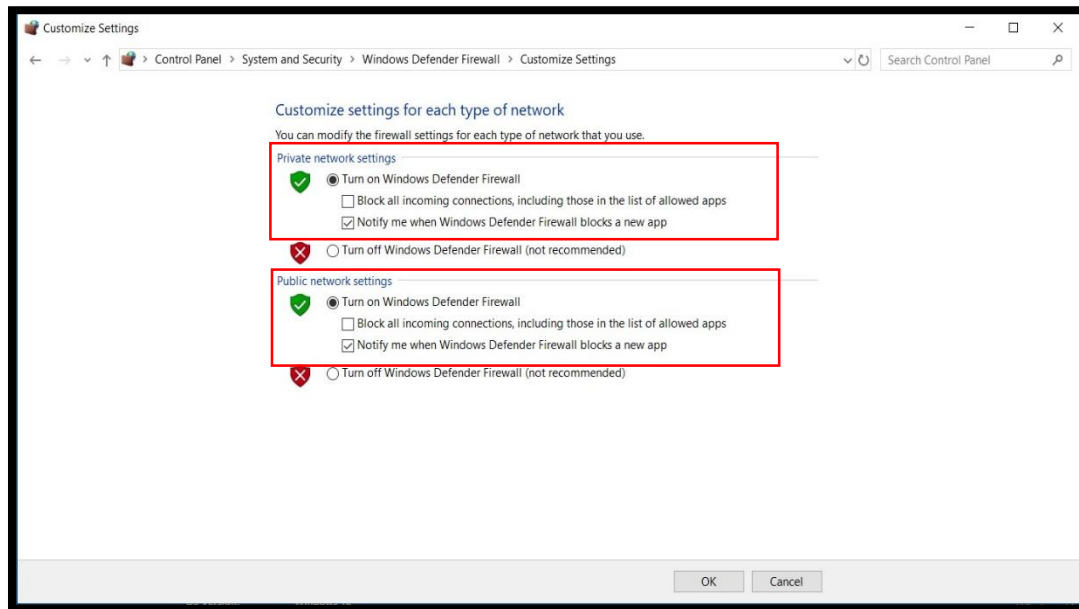


Figure 34: Turn on Windows Defender Firewall

Step 06: Now, firewall is on.

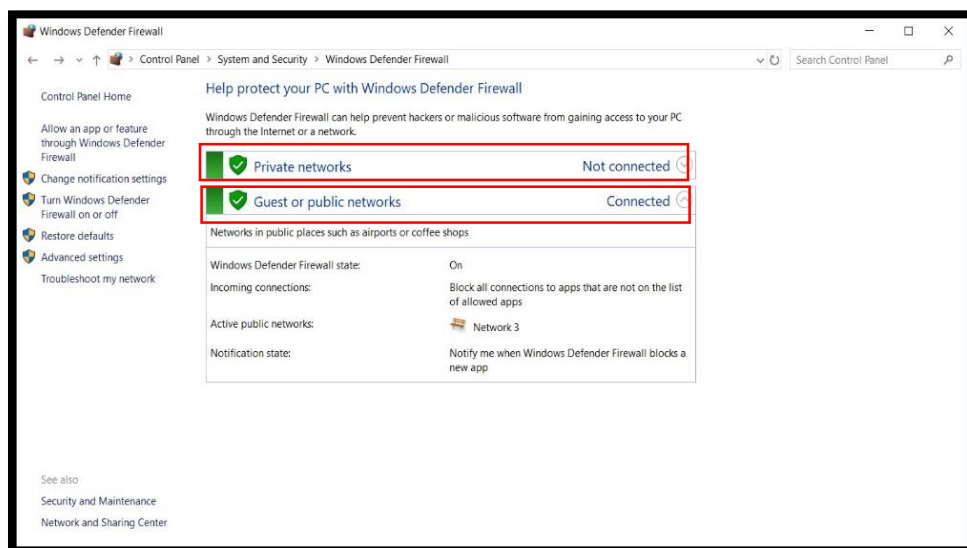
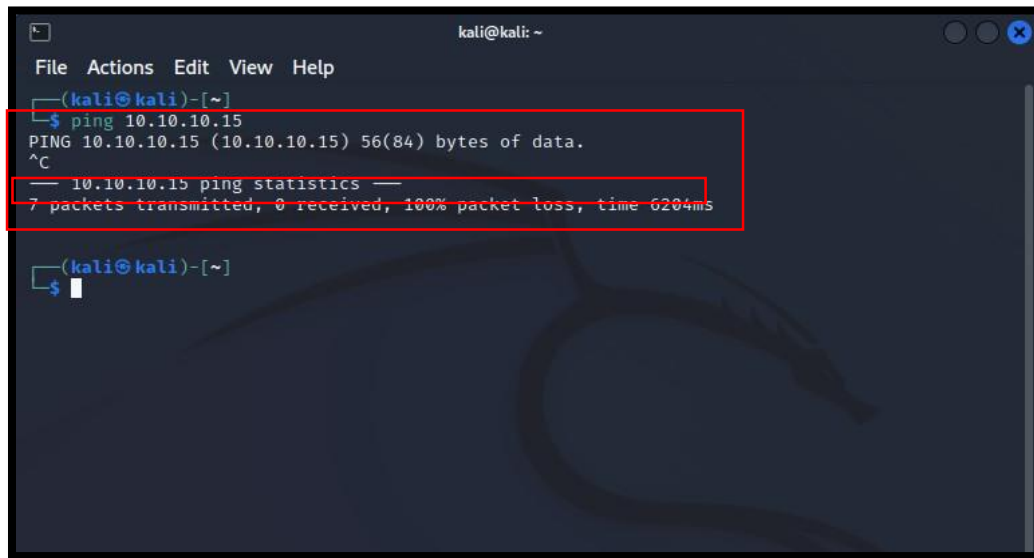


Figure 35: Firewall is on

Step 07: Now, check the connectivity using ping command, from attacker operating system that is kali linux form victim operating system Windows 10. The IP address of victim operating system windows 10 is 10.10.10.15.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a user prompt '(kali@kali)-[~]' followed by a command '\$ ping 10.10.10.15'. The output shows 'PING 10.10.10.15 (10.10.10.15) 56(84) bytes of data.' followed by a Ctrl-C interrupt '^C'. Below this, it shows '10.10.10.15 ping statistics' and '7 packets transmitted, 0 received, 100% packet loss, time 6204ms'. The terminal then returns to the user prompt '(kali@kali)-[~]' with a '\$' prompt and a cursor.

```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
$ ping 10.10.10.15  
PING 10.10.10.15 (10.10.10.15) 56(84) bytes of data.  
^C  
10.10.10.15 ping statistics  
7 packets transmitted, 0 received, 100% packet loss, time 6204ms  
~(kali@kali)-[~]  
$
```

Figure 36: Checking connectivity after firewall is on.

So, we can see clearly that kali linux is unable to ping windows 10. So, the mitigation is done successfully.

4. Evaluation

Through ARP spoofing and ARP poisoning, a man-in-the-middle attack was carried out from Kali Linux to a Windows 10 system. Those susceptible sites were fixed as well, using various mitigation measures. Although these fixes assist to keep the evaluation targets safe, they also cause service disruptions. As a result, it is evident that addressing such susceptible locations has both benefits and drawbacks. The following are some of the pro's and cons of the mitigation approach in use.

4.1 Pros.

- The implemented mitigation method does not necessitate the use of any new software or hardware, making it cost-effective.
- ARP spoofing and ARP poisoning do not allow sensitive information such as login passwords and orders to be intercepted or sniffed.
- Kali linux's Ettercap tools will never be able to hack a Windows 10 PC.

4.2 Cons.

- By modifying Kali linux static IP address, the Windows 10 firewall rule may be readily evaded.

As a result, these are some of the pro's and cons of the mitigation technique in use. Although this mitigation method has aided in the security of susceptible systems, it has also caused service disruptions. However, depending on the implemented mitigation approach, it's time to perform the cost-benefit analysis (CBA).

4.3 Cost benefit analysis

A company conducted risk assessments to determine the level of risk associated with each information asset. As the scope of the project expands, all of the hazards are overlooked. As a result, such risks are prioritized and addressed based on their severity. Before reducing any risk, it is vital to determine if the prevention technique to be used is worthwhile. As a result, Cost-Benefit Analysis comes into play (CBA).

The process of analyzing the merit of a mitigation technique to be employed for minimizing specific risk in information assets is known as cost-benefit analysis, or CBA. To put it another way, it's a method of calculating the cost and benefit. It is calculated based on the cost of risk-mitigation appliances and the advantages that may be realized after using that method. It's determined on a year-by-year basis. It can be obtained by deducting the **Annual Loss Expectancy post ($ALE_{(post)}$)** and **Annual Cost of the Safeguard (ACS)** from **Annual Loss Expectancy prior ($ALE_{(prior)}$)**. The mathematical representation of Cost Benefit Analysis is given below:-

$$\text{Cost Benefit Analysis(CBA)} = ALE_{(prior)} - ALE_{(post)} - ACS.$$

Cost-benefit analysis can have a good or negative impact. Only if the CBA value is positive does the company use the mitigation plan. The company, on the other hand, assumes the risk if the CBA value is negative. However, in this project, CBA will be used to determine which mitigation methods should be used to avoid a Man-in-the-Middle attack.

Consider the Mithila Institute of Technology, which would be comprised of a web server and a few Windows 10 computers linked to the internet through a Cisco 3275 Router. Outsiders cannot access this network because it is protected by NAT (Network Address Translation). However, if the new Kali Linux computer (attacker) is added to the current topology or LAN, the entire system may be attacked using the man-in-the-middle attack as demonstrated in the demonstration section. The organization's operational structure is presented below, with the attacker computer highlighted in red.

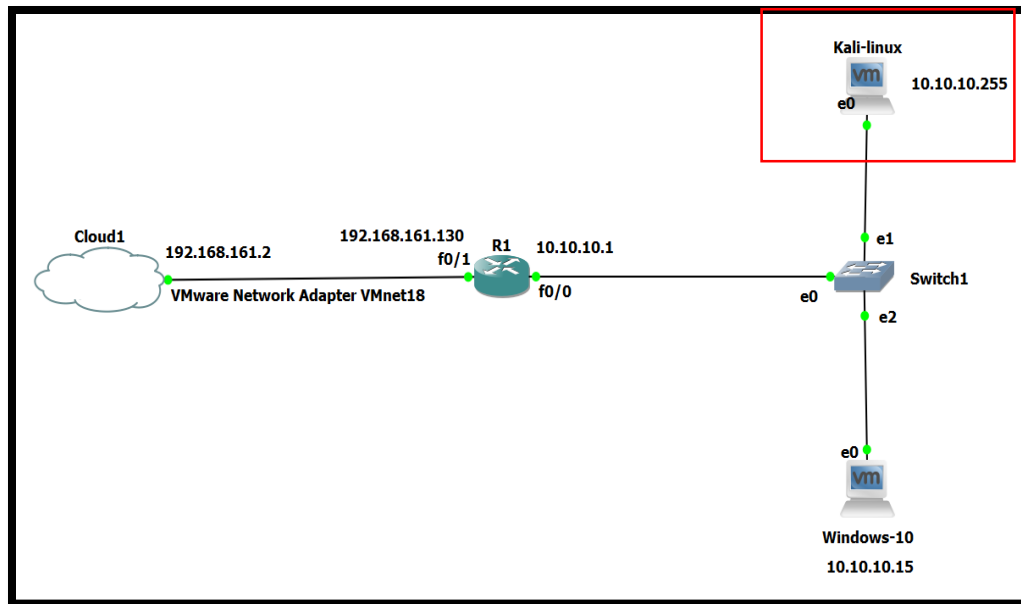


Figure 37: Network topology of Mithila institute of technology.

The whole network of Mithila institute of Technology is predicted to be hacked once every 9 months by a man-in-the-middle attack, resulting in a loss of \$120,000 every occurrence. To minimize the risk to an acceptable level, the business planned to hire a pen-tester every 9 months, which would cost them \$150000 per year. The pen-tester corrected all of the vulnerabilities linked with Brute-Force Attack without introducing any hardware or software components. As a result, the man-in-the-middle attack, Annual Loss Expectancy was decreased to \$60000. It's now time to perform a cost-benefit analysis.

Here.

Single Loss Expectancy (SLE) = \$120000

Annual Rate of Occurrence (ARO)=1 per 9 months - 2 times per annum

Annual Loss Expectancy (ALE) = SLE * ARO
 = \$120000 * 2
 =\$240000

Annual Loss Expectancy prior ($ALE_{(prior)}$) = \$240000

Annual Cost of the Safeguard (ACS) = \$150000

Annual Loss Expectancy post ($ALE_{(post)}$) = \$60000

$$\begin{aligned}\text{Cost Benefit Analysis (CBA)} &= ALE_{(prior)} - ALE_{(post)} - ACS \\ &= \$240000 - \$60000 - \$150000 \\ &= \$30000\end{aligned}$$

The expense of engaging a pen-tester on a temporary basis is less than the loss projected as a result of man-in-the-middle attack. As a result, appointing a pen-tester has a beneficial impact on the organization.

5. Conclusion

Eavesdropping attack is very common now a days. Hackers easily attack and get login credentials by **man-in-the-middle attack** by using ARP spoofing and ARP poisoning. In this, the virtual network is setup by the help of GNS3. The demonstration part of man-in-the-middle attack has been done successfully. Attack has been done from kali linux to windows 10 by **ARP spoofing and ARP poisoning** by the help tools like **Ettercap and Wireshark**. To defend the attack, the **mitigation** step has been done by turning on **firewall** and the **evaluation** of pros and cons of the mitigation step.

6. References

DOBRAN, B., 2019. *What is a Man in the Middle Attack? Types, Prevention, & Detection*. [Online]

Available at: <https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention> [Accessed 26 April 2022].

Fortinet, 2022. *What Are Eavesdropping Attacks? | Fortinet*. [Online]

Available at: <https://www.fortinet.com/resources/cyberglossary/eavesdropping> [Accessed 27 April 2022].

Galaxy Technologies LLC, 2021. *GNS3 Documentation | GNS3 Documentation*. [Online]

Available at: <https://docs.gns3.com/> [Accessed 3 May 2022].

Gangan, S., 2015. *A Review of Man-in-the-Middle Attacks*, s.l.: arXiv:1504.02115.

Gangan, S., n.d. *A Review of Man-in-the-Middle Attacks*, s.l.: s.n.

GCFGlobal, 2022. *Windows Basics: All About Windows*. [Online]

Available at: <https://edu.gcfglobal.org/en/windowsbasics/all-about-windows/1/> [Accessed 3 May 2022].

Imperva, 2021. *What is ARP Spoofing | ARP Cache Poisoning Attack Explained | Imperva*. [Online]

Available at: <https://www.imperva.com/learn/application-security/arp-spoofing/#:~:text=An%20ARP%20spoofing%2C%20also%20known%20as%20ARP%20poisoning%2C,The%20attacker%20must%20have%20access%20to%20the%20network.?msclkid=47ba8367c5e911ec8a959be8315766b0> [Accessed 27 April 2022].

OffSec Services Limited, 2022. *ettercap | Kali Linux Tools*. [Online]

Available at: <https://www.kali.org/tools/ettercap/> [Accessed 3 May 2022].

OffSec Services Limited, 2022. *What is Kali Linux? | Kali Linux Documentation*. [Online]

Available at: <https://www.kali.org/docs/introduction/what-is-kali-linux/> [Accessed 3 May 2022].

Panda Security, 2021. *What Is a Man-in-the-Middle (MITM) Attack? Definition and Prevention - Panda Security Mediacenter*. [Online]

Available at: <https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/?msclkid=2240f48ac5e211eca9397c435d8cee76> [Accessed 27 April 2022].

Secret Double Octopus, 2021. *What is IP spoofing? - Security Wiki*. [Online]

Available at: <https://doubleoctopus.com/security-wiki/threats-and-tools/ip->

[spoofing/?msclkid=cfd4d8ebc5e611eca4133d66f96bd7a7](#)

[Accessed 27 April 2022].

Shea, S., 2022. *How to prevent network eavesdropping attacks*. [Online]

Available at: <https://www.techtarget.com/searchsecurity/answer/How-to-prevent-network-sniffing-and-eavesdropping>

[Accessed 27 April 2022].

techopedia, 2022. *What is VMware Workstation? - Definition from Techopedia*. [Online]

Available at: <https://www.techopedia.com/definition/25690/vmware-workstation>

[Accessed 3 May 2022].

VERACODE, 2022. *Man in the Middle Attack: Tutorial & Examples | Veracode*. [Online]

Available at: <https://www.veracode.com/security/man-middle-attack#:~:text=A%20man%2Din%2Dthe%2Dmiddle%20attack%20is%20a%20type,to%20be%20both%20legitimate%20participants.>

[20be%20both%20legitimate%20participants.](https://www.veracode.com/security/man-middle-attack#:~:text=A%20man%2Din%2Dthe%2Dmiddle%20attack%20is%20a%20type,to%20be%20both%20legitimate%20participants.)

[Accessed 27 April 2022].