Republic of Iraq

Ministry of Higher Education and Scientific Research
University of Baghdad - College of Science
Department of Computer Science

Securing Networks: Advanced Attack Detection and Resilient Defense Mechanism

A Project
Submitted to College of Science, University of Baghdad in
Partial Fulfillment of the Requirements for the Degree of
B.Sc. in Computer Science

BY

Zahraa Ibrahim Khalil

Supervisor

Asst.Lect Saif Saad Shihab

2024 **1445 AH**

Acknowledgements

I am deeply grateful for the invaluable guidance and support provided by Asst.Lect Saif Saad Shihab throughout the duration of this project. His expertise, encouragement, and constructive feedback have been instrumental in shaping its development and success. From the initial stages of conceptualization to the final execution, their mentorship has not only enhanced my understanding of the subject matter but has also fostered my growth as a student and researcher.

In addition, I extend my heartfelt appreciation to my family for their unwavering encouragement and understanding during this endeavor. Their constant belief in my abilities has been a source of strength and motivation, providing me with the resilience to overcome challenges and pursue excellence. Whether offering words of encouragement or lending a listening ear during moments of doubt, their unwavering support has been a constant source of inspiration.

Furthermore, I extend my gratitude to my friends for their assistance and contributions to this project. Whether providing technical expertise, research assistance, or moral support, their contributions have played an integral role in the development and realization of this endeavor.

Zahraa

Abstract

Securing networks against advanced attacks has become a critical challenge in today's digital landscape.

This research project aims to address this challenge by focusing on advanced attack detection and the development of resilient defense mechanisms. The objective is to enhance network security by identifying and mitigating various sophisticated attack vectors, such as ICMP flood attacks, SMURF attacks, DNS attacks, SYN attacks and VLAN hopping attacks.

The research will involve comprehensive analysis of these advanced attack patterns to gain a deeper understanding of their characteristics and potential impact on network infrastructure.

Through the use of advanced detection techniques, such as anomaly detection, behavior analysis, and network traffic analysis, the project aims to develop effective mechanisms to detect and identify these attacks in real-time. Additionally, resilient defense mechanisms will be devised to minimize the impact of successful attacks and ensure network availability and integrity.

These mechanisms may include traffic filtering, rate limiting, intrusion detection and prevention systems, adaptive routing, load balancing, encryption, and adaptive response strategies. By combining advanced attack detection with resilient defense strategies, this research project aims to provide network administrators with the tools and knowledge necessary to secure their networks against a wide range of emerging and sophisticated threats.

The project will use PNET Lab to create a network scenario that simulates the attack and defense mechanisms in a realistic and controlled environment.

Table of Contents

List of Figures

CHAPTER ONE

General Introduction

1.1 Overview

In contemporary business environments, safeguarding the network infrastructure of companies assumes paramount importance. Just as physical security measures are implemented to protect tangible assets, securing the digital network serves as the primary line of defense against a myriad of cyber threats. Cyberattacks, ranging from malware infiltration to malicious hacking attempts, pose significant risks to organizational data integrity, confidentiality, and operational continuity. Recognizing the criticality of network security, our research project is dedicated to fortifying the network infrastructure of companies across various departments. By mitigating potential vulnerabilities and thwarting malicious incursions, we aim to uphold the functionality of the company's network ecosystem. This endeavor is pivotal not only for preserving sensitive information but also for sustaining operational efficacy and safeguarding organizational reputation in an increasingly interconnected digital landscape[33].

1.2 Project Problem

In the contemporary digital landscape, ensuring network security against sophisticated attacks has become increasingly challenging. Traditional security measures often fall short in addressing the complexities of these advanced attacks, leaving networks vulnerable to exploitation and compromise. As organizations become more reliant on interconnected systems and digital infrastructure, the potential ramifications of successful attacks—such as data breaches, service disruptions, and financial losses—grow more severe. Consequently, there is a pressing need for innovative approaches to effectively detect and mitigate these advanced threats. Our research project aims to tackle this problem by conducting a comprehensive examination of advanced attack vectors and developing robust defense mechanisms to safeguard network infrastructure against evolving threats.

1.3 Project Objectives

The primary objective of this research is to scrutinize security vulnerabilities across diverse network layers, with a particular focus on specific attacks. These attacks include ICMP flood and SMURF attack, both operating at Layer Three; SYN attack at Layer Four; DNS spoofing, which can occur at either Layer Three or Layer Seven; and VLAN hopping, encompassing DTP and double tagging, spanning both Layer Two and Layer Three. The aim is to gain insight into the operational dynamics of these attacks and to explore effective countermeasures. Furthermore, the study entails practical demonstrations of attack methodologies utilizing various tools, followed by the implementation of solutions designed to bolster the security of network devices across all layers susceptible to these threats.

1.4 Related Work

Intrussion detection by penetration test in an organization network[1]: This research paper discusses using penetration testing to detect intrusions in an organization's network. Penetration testing involves simulating attacks to identify vulnerabilities in a system. The authors likely evaluated the effectiveness of penetration testing for intrusion detection in a real-world network environment.

DDoS Attacks—Analysis and Prevention[2]: The paper examines DDoS attacks, which overwhelm a server's resources to disrupt services, focusing on availability in Internet applications. It discusses three defense components: detection, mitigation, and IP traceback. Detection involves identifying attacks and classifying traffic. Mitigation uses rate limits and filtering. IP traceback traces packet sources to identify true addresses. Lastly, the paper proposes a new defense mechanism for both network and application layers.

Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open-Source Tools for Instructional Use[3]: In this paper, we will discuss how the attacker performs the Man-in-the-middle (MITM) attack using the open source Ettercap tool in Kali Linux environment. Ettercap tool is a sniffing tool available in the Kali Linux operating system.

Virtual LAN Security: weaknesses and countermeasures[4] In their paper, researchers stress the significance of securing VLANs due to their susceptibility to breaches and disruptive

potential. They explore attack methods like VLAN hopping, urging for strengthened defenses. However, they caution that measures such as switch hardening could escalate administrative workload, necessitating a balance between security and operational efficiency.

1.5 Project Organization

This research consists of five chapters

1. General introduction.
2. In Chapter 2 (Theoretical Background) this chapter presents the fundamental concepts and the background information of the network, routing, network protocols, and describes the DHCP, VLANs, and discusses the importance of network protection from specific types of attacks.
3. Chapter 3 (Network Design and Implementation) is focused on designing a secure and protected network for a company campus. VMware has used to emulate different methods from devices such as windows, Linux, and most of the hacking programs that can be applied.
4. Chapter 4 (Results and discussion) is a summary of the work, and the protection that we achieve.
5. Chapter 5 (Conclusion and Future work) is a summary of the work. Recommendations and conclusions are made and possible future work.

CHAPTER TWO

Theoretical Background

2.1 Introduction

In this chapter, we delve into the theoretical underpinnings essential for understanding the intricacies of network security and attack mitigation. By exploring fundamental concepts such as routing, network protocols, and defense mechanisms, we lay the groundwork for comprehensively addressing the challenges posed by advanced cyber threats.

2.2 Routing

Routing in general refers to the process of selecting the most efficient path for data transmission between two nodes in a network. It involves determining the optimal route based on factors like delay, bandwidth, or number of hops to ensure effective communication between network devices.[5]

There are many types of routing protocols used in network communication, these are some of them:

- Static routing is a type of routing protocol in which the routing table is manually configured and does not change unless manually updated. This type of routing is best suited for small networks with a fixed topology[6].
- Dynamic routing, on the other hand, is a type of routing protocol in which the routing table is automatically updated based on network conditions. This type of routing is best suited for large networks with a dynamic topology[6].

The choice between static and dynamic routing depends on the specific network requirements and topology. Static routing is less complex and requires less processing power, but dynamic routing is more flexible and adaptable to network changes[6].

2.2.1 Routing Protocol (IS-IS)

The IS-IS (Intermediate System to Intermediate System) routing protocol is a link-state routing protocol that is commonly used in large-scale networks. It is a standardized protocol by the International Organization for Standardization (ISO) and is widely used in enterprise and service provider networks. The IS-IS protocol is designed to operate over a wide range of network types, including LANs, WANs, and MANs. It is a highly scalable protocol that can support large networks with thousands of nodes. The IS-IS protocol uses a hierarchical addressing scheme, which allows it to efficiently route traffic between different parts of the network. It also supports various features, such as traffic engineering, multi-topology routing, and graceful restart. The IS-IS protocol is often compared to the Open Shortest Path First (OSPF) protocol, which is another popular link-state routing protocol. While both protocols share some similarities, the IS-IS protocol is generally considered to be more scalable and flexible than OSPF.[7]

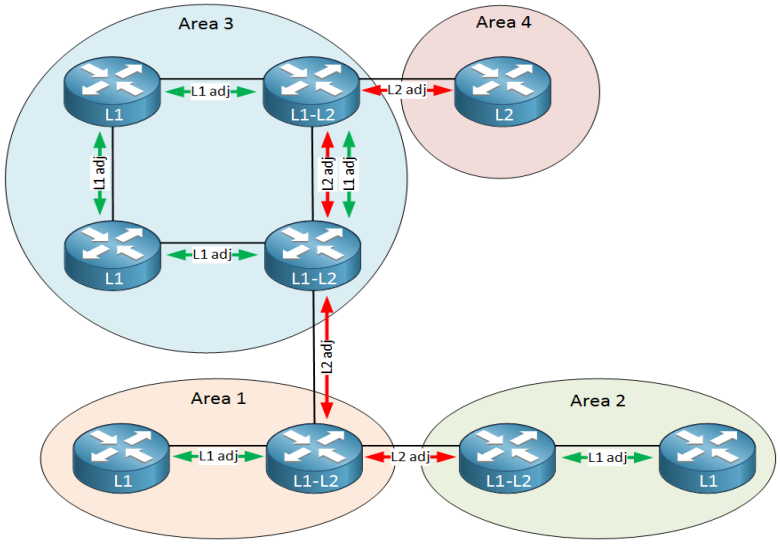


Figure (2.1): IS-IS routing protocol.[8]

2.3 ARP

ARP (Address Resolution Protocol) is a protocol used in computer networking to translate IP addresses to their corresponding MAC addresses. It is a critical component of network communication, as it allows devices to identify the physical address of another device on the same network based on its IP address. However, ARP is also susceptible to spoofing attacks, where an attacker associates its MAC address with the IP address of an intended legitimate host, allowing it to intercept and modify network traffic. This type of attack is known as an ARP spoofing-based man-in-the-middle (MITM) attack.[9]

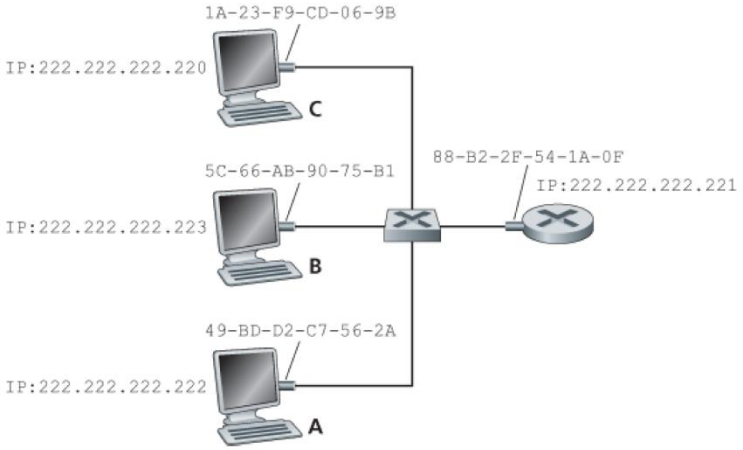


Figure (2.2): How ARP works.[10]

2.4 DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used for automatically assigning IP addresses and other network configurations to devices on a network. It is widely used in networks to simplify the process of managing IP addresses and other network configurations. However, DHCP has several vulnerabilities that can be exploited by attackers, such as a lack of authentication, confidentiality, and integrity. These vulnerabilities can result in different attacks, such as rogue DHCP server attacks, DHCP starvation attacks, or replay attacks.[11]

2.5 Virtual Local Area Networks (VLANs)

VLAN (Virtual Local Area Network) is a technology that enables the creation of logical groupings of devices within a network, even if they are not physically connected to the same network switch. VLANs are used to segment networks for security, performance, and management purposes. They allow network administrators to group devices based on factors like department, function, or security requirements, creating isolated broadcast domains within a larger network infrastructure[12].

- **Inter VLAN**

  Inter-VLAN, or Inter-Virtual LAN, refers to the communication between devices belonging to different VLANs within a network. It enables devices in separate VLANs to communicate with each other using routing devices like routers or Layer 3 switches. Inter-VLAN communication enhances network security, traffic control, and segmentation for improved network performance[13].

2.6 Network Penetration Testing

Network Penetration Testing involves assessing the security of a network infrastructure by simulating real-world attack scenarios to identify vulnerabilities and weaknesses that could be exploited by malicious actors. Examples of network penetration testing include port scanning, vulnerability scanning, exploitation of discovered vulnerabilities, DNS spoofing, VLAN hopping, SNMP attacks, and various forms of network-based attacks such as DoS (Denial-of-Service) attacks and Man-in-the-Middle (MitM) attacks. These techniques help organizations understand their security posture, improve defenses, and mitigate potential risks[14].

2.6.1 DoS (Denial-of-Service) attacks:

DoS attacks are a type of cyber-attack that aim to disrupt, deny, or degrade the availability of a target system, network, or service to legitimate users.

Here are some of the famous examples of DoS that I will cover in this project:

- **ICMP flood Attack:**

An ICMP flood attack is a type of denial-of-service (DoS) attack that aims to overwhelm a target system with a large volume of Internet Control Message Protocol (ICMP) packets. ICMP is primarily used for diagnostic or control purposes within IP networks. In an ICMP flood attack, the attacker sends a massive number of ICMP echo request (ping) packets to the target system, consuming its network bandwidth, processing capacity, or both. This flood of packets can saturate the target's network connection, making it unable to respond to legitimate traffic or causing it to slow down significantly.

The attack works by exploiting the fact that many systems respond to ICMP echo requests by default. When flooded with a high volume of these requests, the target system becomes overwhelmed, leading to a denial of service for legitimate users. Additionally, the attacker may spoof the source IP addresses of the ICMP packets, making it difficult for the target system to identify and filter out the malicious traffic[15].

- **Smurf Attack:**

Smurf attack is a type of DDoS attack that exploits the ICMP protocol. In a Smurf attack, the attacker sends a large number of ICMP echo request (ping) packets to the broadcast address of a network, spoofing the source IP address to appear as if they are coming from the victim's IP address. The broadcast address causes all devices on the network to respond to the victim's IP address with ICMP echo replies, overwhelming the victim's system with traffic and causing it to slow down or become unreachable. This amplification effect is achieved by leveraging the broadcast nature of the ICMP echo requests, making it an efficient method for conducting DDoS attacks. Smurf attacks can significantly disrupt the availability of a network or service for legitimate users[16].

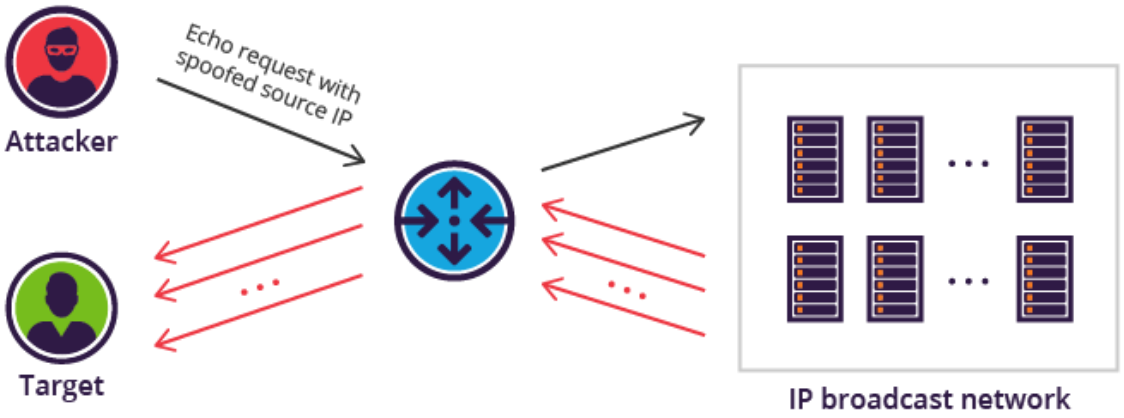


Figure (2.3):Smurf attack [17]

- **SYN Attack:**

A SYN (Synchronize) flood attack is a form of DDoS (Distributed Denial of Service) attack that targets the TCP (Transmission Control Protocol) handshake process. In a SYN flood attack, the attacker sends a large number of TCP connection requests with spoofed source IP addresses to the victim's server. These requests are part of the three-way handshake process used to establish a TCP connection.

Normally, during the TCP handshake, the client sends a SYN packet to the server, and the server responds with a SYN-ACK packet, acknowledging the SYN and indicating its own readiness to establish a connection. Finally, the client sends an ACK packet back to the server, confirming the connection establishment. However, in a SYN flood attack, the attacker sends a large number of SYN packets to the victim's server without completing the handshake process by sending the final ACK packet. As a result, the server allocates resources to maintain half-open connections, exhausting its capacity to handle legitimate connection requests and ultimately leading to a denial of service for legitimate users.

SYN flood attacks can be particularly effective because they require minimal bandwidth to initiate, yet they can overwhelm a server's resources, causing significant disruption to the availability of the targeted service. To mitigate SYN flood attacks,

various techniques such as SYN cookies, rate limiting, and SYN cache management are employed by network administrators and security professionals[16].

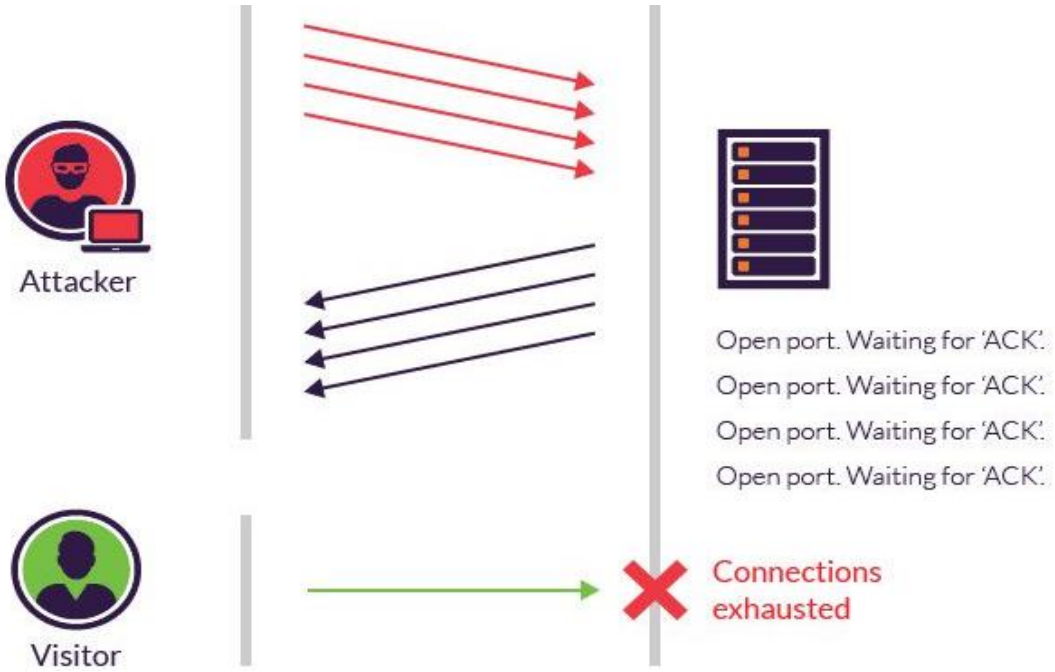


Figure (2.4): SYN attack [17].

2.6.2 Man-in-the-Middle (MitM) attacks:

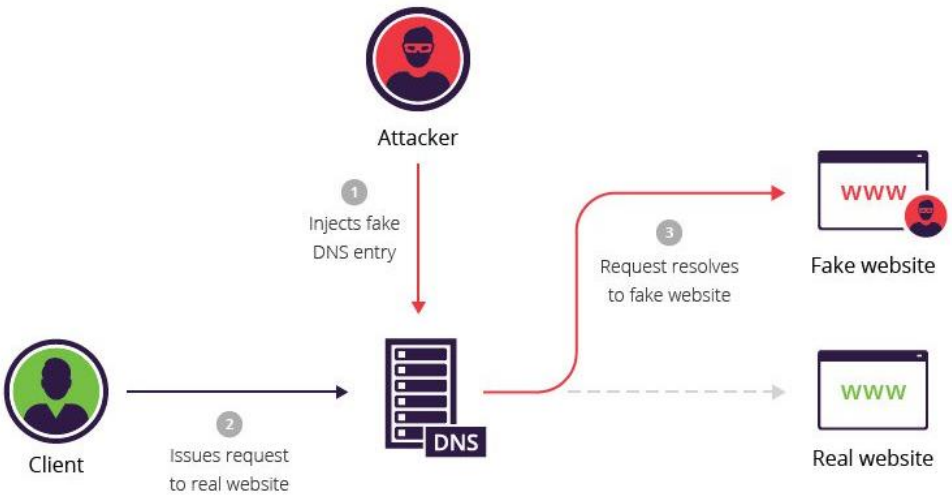
A Man-in-the-Middle (MITM) attack is a form of cyberattack where a malicious actor intercepts and potentially alters communication between two parties without their knowledge. The attacker secretly relays and possibly modifies the communication between the two parties, making them believe they are directly communicating with each other when, in fact, all the traffic is passing through the attacker's system. This allows the attacker to eavesdrop on sensitive information, such as login credentials, financial details, or private conversations, or even inject malicious content into the communication stream[18].

1) DNS Spoofing attack:

DNS spoofing, also known as DNS cache poisoning, is a cyber-attack where the attacker manipulates the Domain Name System (DNS) resolution process to redirect users to malicious

websites or servers. The DNS translates human-readable domain names (like www.example.com) into IP addresses (like 192.0.2.1) that computers use to communicate over the internet[19].

In a DNS spoofing attack, the attacker intercepts DNS queries and provides false information to the requesting system, tricking it into believing it has received the correct IP address associated with a particular domain name. This can be achieved through various methods, such as compromising DNS servers, exploiting vulnerabilities in DNS software, or poisoning the DNS cache of a victim's system or network device. Once the DNS cache is poisoned, the victim's system or network device will use the malicious IP address provided by the attacker, leading the user to unintended destinations, which could be phishing sites, malware distribution points, or other malicious servers controlled by the attacker. DNS spoofing attacks can have severe consequences, including theft of sensitive information, installation of malware, or disruption of network services[19].



Figure(2.5): DNS spoofing attack[17].

2) VLAN Hopping :

VLAN hopping is a technique used to gain unauthorized access to VLANs (Virtual Local Area Networks) by exploiting the vulnerabilities in the network infrastructure. It allows an attacker to access traffic from other VLANs, bypassing the security measures in place[20]. There are two main types of VLAN hopping attacks:

- **Switch Spoofing:** This type of VLAN hopping occurs when an attacker creates a rogue switch and connects it to the network. The rogue switch then pretends to be a legitimate switch and sends out VLAN tagged packets, allowing the attacker to access traffic from other VLANs[20][21][23].

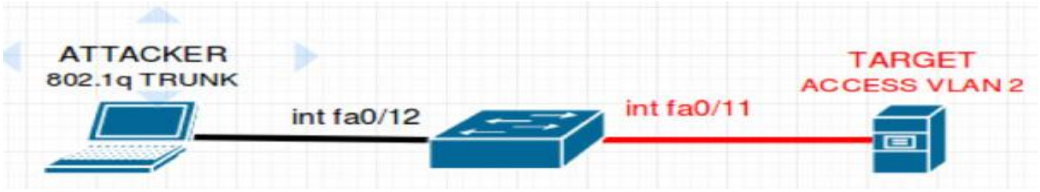


Figure (2.6): switch spoofing attack[23]

- **Double Tagging:** In this type of VLAN hopping, an attacker sends a packet with two VLAN tags, with the inner tag being the VLAN they want to access and the outer tag being the VLAN of the attacker. This technique is used to bypass the Dynamic Trunking Protocol (DTP) security features that prevent unauthorized devices from accessing the trunk port[20][21][23].

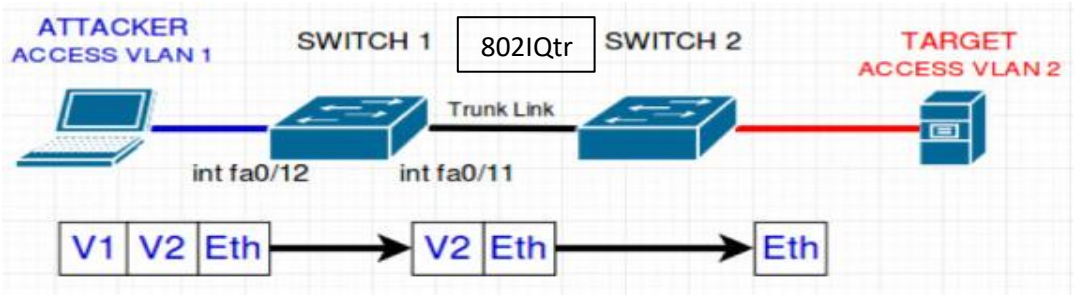


Figure (2.7): Double Tagging attack[23]

To prevent VLAN hopping attacks, network administrators should implement security measures such as:

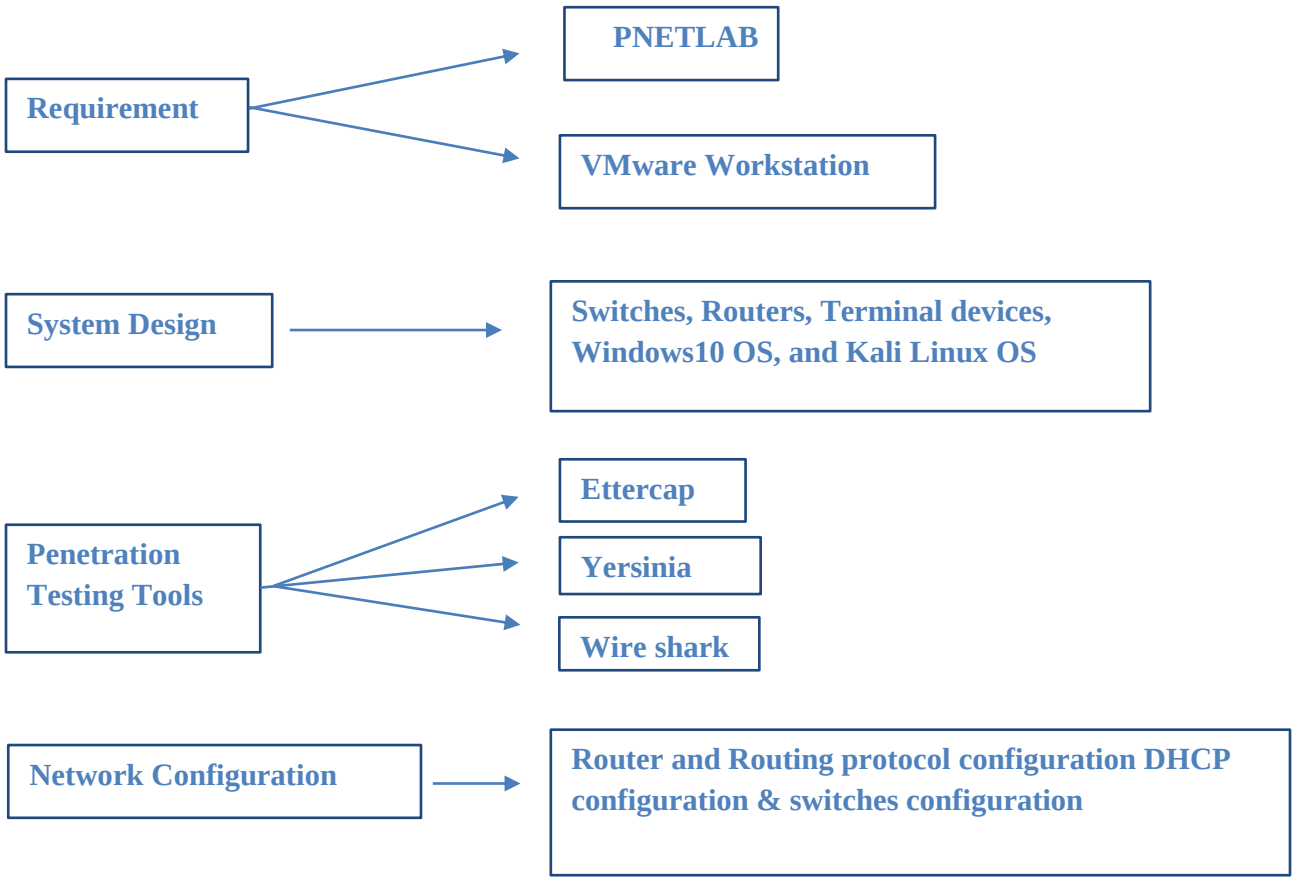
- ✓ Disabling DTP on all ports and setting them to static trunk mode.
- ✓ Using private VLANs and VLAN access control lists (VACLs) to enforce a proper trust model.
- ✓ Implementing 802.1X authentication for port-based access control.
- ✓ Regularly monitoring the network for any rogue devices or unusual traffic patterns[20][21].

CHAPTER THREE

Network Design and Implementation

3.1 Introduction

This chapter explores best practices for crafting resilient network architectures and deploying security measures to detect and mitigate cyber threats effectively. By focusing on network topology, segmentation, and the deployment of security technologies, organizations can enhance their defense posture and ensure operational continuity amidst evolving threats.

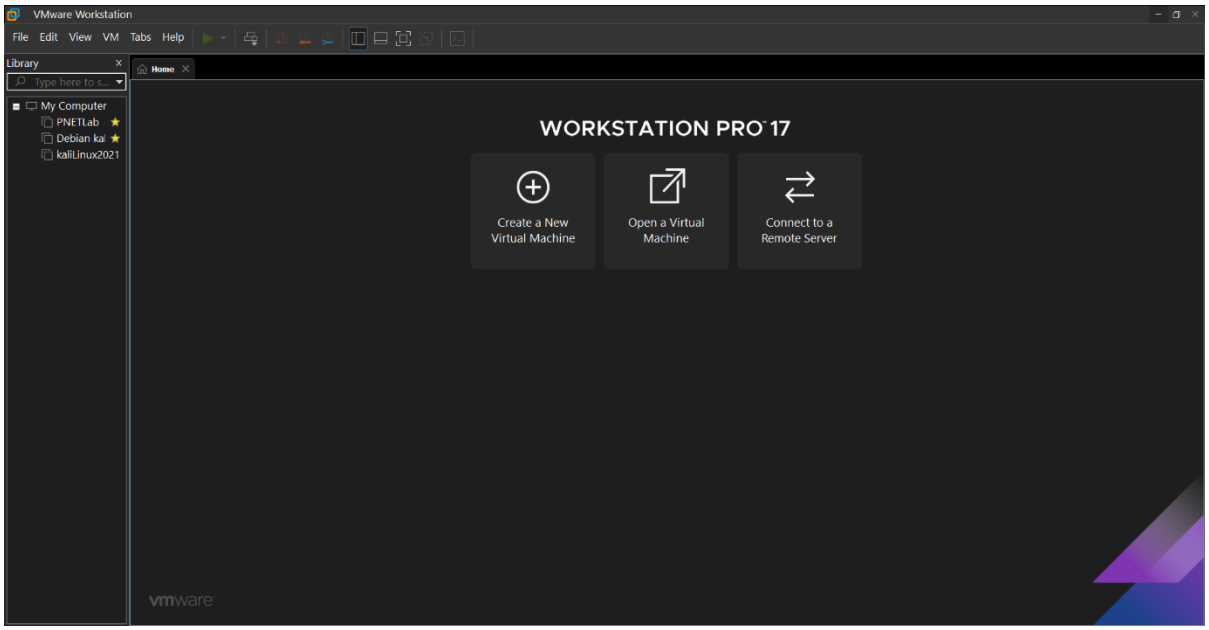


3.2 Requirements

PNET Lab represents a no-cost platform renowned for its robust capabilities in facilitating the creation, dissemination, and execution of networking laboratories involving multiple vendors. Its emulation tool empowers users to construct intricate network topologies, faithfully replicating modern computer network environments. Furthermore, PNET enjoys the backing of VMware support.

3.2.1 VMware Workstation

is a desktop virtualization software that allows users to run multiple operating systems on a single physical machine. It enables users to create and run virtual machines on their computers, providing a platform for testing software in different environments, running legacy applications, and isolating operating systems for security purposes. This software is widely used by developers, IT professionals, and businesses to streamline software development, testing, and deployment processes[21]. figure (3.1) shows the home page VMware workstation.



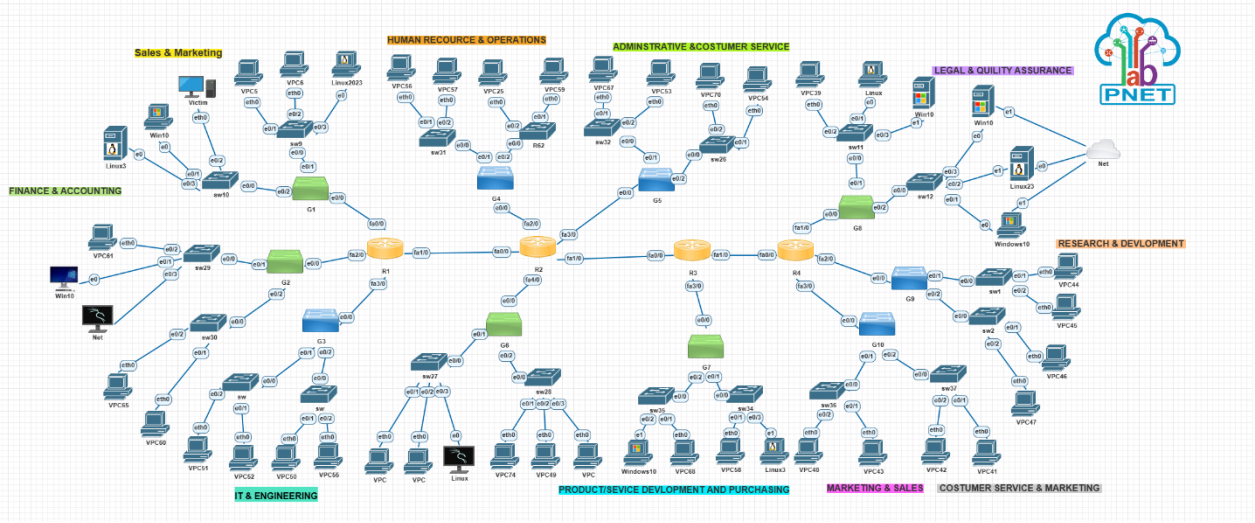
Figure(3.1): VMware workstation

3.2.2 PNET Lab

PnetLab is a virtual network platform for learning. It lets users create and experiment with virtual networks, routers, and switches on their computer, using a graphical interface. It's popular in networking courses and training programs for hands-on practice without needing physical equipment[22].

Figure(3.2): PnetLab

3.3 System Design :



Figure(3.3):system design

1. Switches: A switch is a network device that connects multiple devices within a local area network (LAN) and forwards data packets between them based on MAC addresses. It operates at the Data Link layer (Layer 2) of the OSI model[24].

One of its types that will be used in this project is a multilayer switch that operates at both Layer 2 and Layer 3 of the OSI model, combining switching and routing functionalities. It can forward traffic based on MAC addresses like a switch and route traffic based on IP addresses like a router[25].

2. Routers: A router is a networking device that forwards data packets between computer networks, typically using IP addresses. It operates at the Network layer (Layer 3) of the OSI model and makes forwarding decisions based on destination IP addresses[26].

3. Terminal device: a terminal device is an endpoint that connects to a network to send or receive data. Typically, these devices are used by end-users, running applications and handling data exchange with other devices or servers within the network, facilitating communication across the virtual network infrastructure[27].

- Kali Linux OS: Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing, equipped with numerous security tools for ethical hacking and cybersecurity testing[28].

- Windows10 OS : Windows 10 is a widely used operating system developed by Microsoft. It is one of the client operating systems used in virtual networks, along with Windows XP and Windows 7, to demonstrate the functionality of virtual machines in a virtual network setup[28].

- Virtual Personal computers: Virtual PC images are pre-configured virtual machine instances that can be used within virtualization software to emulate specific operating systems or software environments, enabling easy deployment and testing in virtual networks[29].

4. Net: translating internal IP addresses to an external IP address when accessing the internet. This setup enables multiple virtual machines to share a single external IP address for internet connectivity[25].

3.4 Penetration Testing Tools

Network penetration testing tools within the Kali Linux operating system refer to a suite of software applications specifically crafted for assessing the security posture of computer networks. These tools are designed to simulate various types of attacks, analyze network traffic, and identify potential vulnerabilities, enabling security professionals to strengthen network defenses and mitigate potential risks effectively.

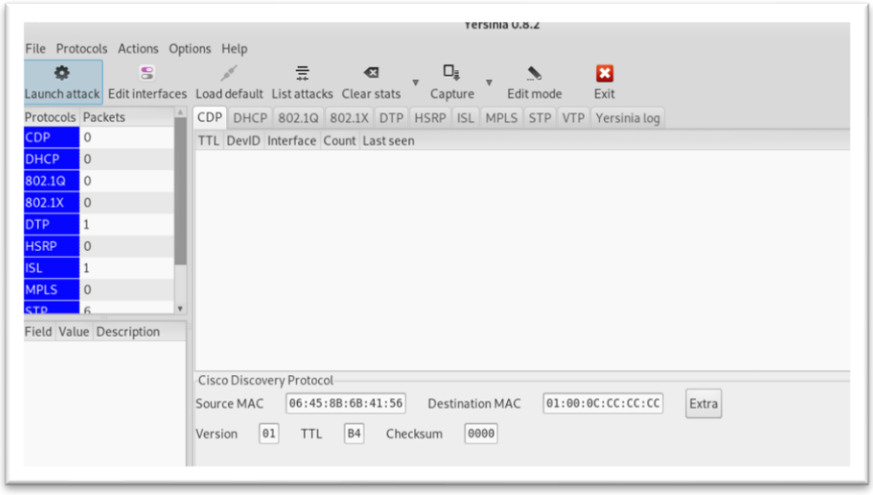
1) Ettercap

Ettercap is a comprehensive suite for man-in-the-middle attacks on LAN. It features sniffing of live connections, content filtering on the fly, and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis. Ettercap also has plugin support to extend its functionality. It is a powerful tool used for network analysis and security testing, particularly in scenarios where one needs to intercept and analyze network traffic for security assessment purposes[30].

Figure(3.4): Ettercap start window.

2) Yersinia

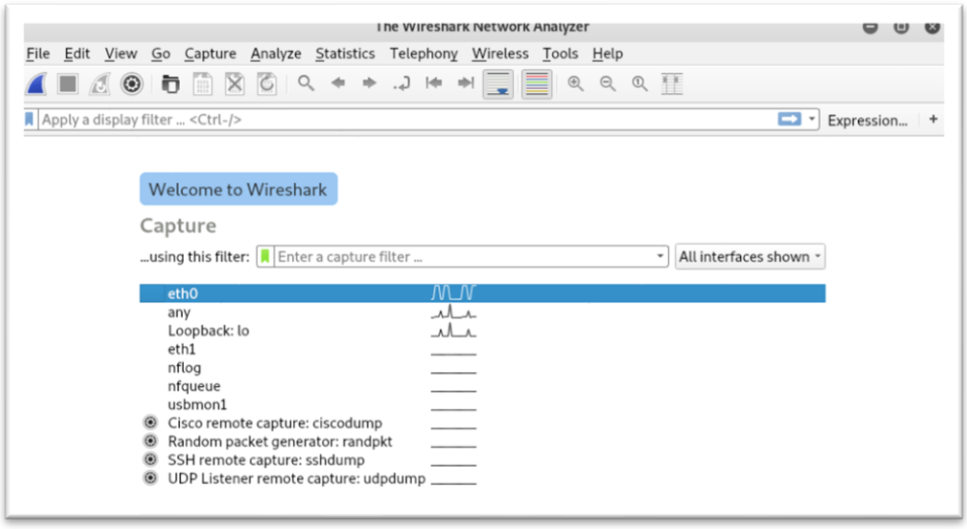
The Yersinia tool in Kali Linux is a network tool designed for network protocols analysis and security testing. It is used for various network attacks and security assessments, including Layer 2 attacks like VLAN Hopping, Spanning Tree attacks, and more. Yersinia is a versatile tool that allows users to simulate attacks on network protocols to test the security of network devices and configurations. It provides a range of functionalities for analyzing and exploiting network vulnerabilities, making it a valuable tool for network security professionals and ethical hackers[30].



Figure(3.5): Yersinia start window.

3) Wireshark

Wireshark is a network protocol analyzer tool included in the Kali Linux operating system. It is a powerful software used for network troubleshooting, analysis, and security testing. Wireshark allows users to capture and analyze network traffic in real-time, supporting a wide range of protocols. With features like live traffic capture, protocol decoding, filtering, and graphing tools, Wireshark is essential for identifying network issues, security vulnerabilities, and malicious activities. It is widely used by penetration testers and security professionals to assess network security, making it a key component of Kali Linux for advanced penetration testing and network security analysis[32].



Figure(3.6): Wire shark start window.

3.5 Network Configuration:

This section will encompass the setup and configuration procedures for each network device, encompassing routers, routing protocol switches, VLANs, and the DHCP server. These configurations are essential for the successful implementation of all experimental procedures within the network.

a) Router and Routing protocol configuration:

Each router needs to configure a its ports after turning them on by giving them ip address and a routing protocol in order to be able to reach all the networks in the topology.

The routing protocol I am using is IS-IS and here is how to configure it inside a router:

```
router isis
net 49.0010.1111.1111.1111.00

interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
ip router isis
duplex full

interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.1.1 255.255.255.0
ip router isis

interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.2.1 255.255.255.0
ip router isis

interface FastEthernet1/0
ip address 192.168.20.1 255.255.255.0
ip router isis
duplex full
```

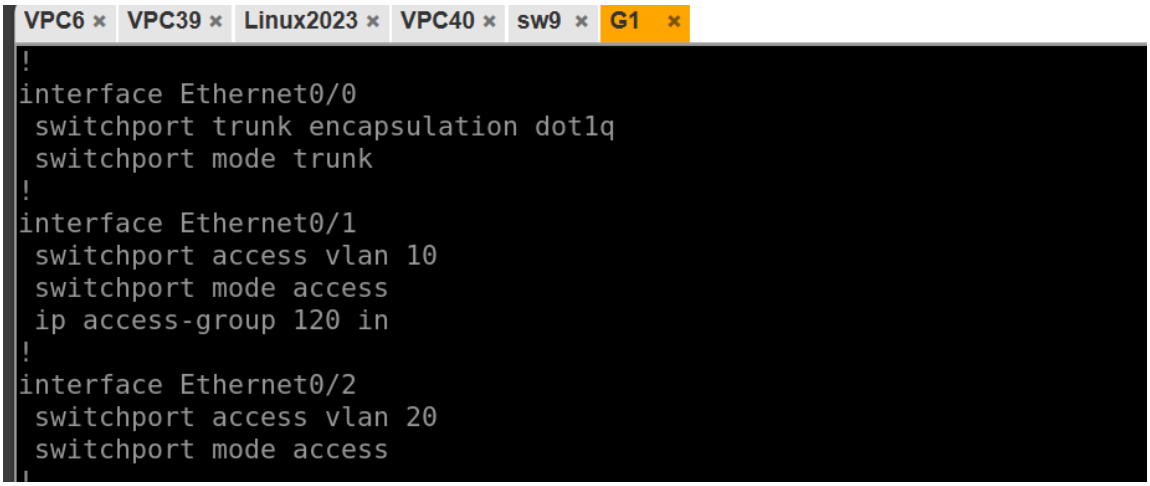
b) DHCP configuration:

In order to provide dynamic IP addresses to devices in the network, we must set up a pool for each network. This involves assigning a network IP, subnet mask, and default router IP. Additionally, for end devices to receive IP addresses dynamically, we need to configure a DHCP pool for each network, as illustrated in the example below:

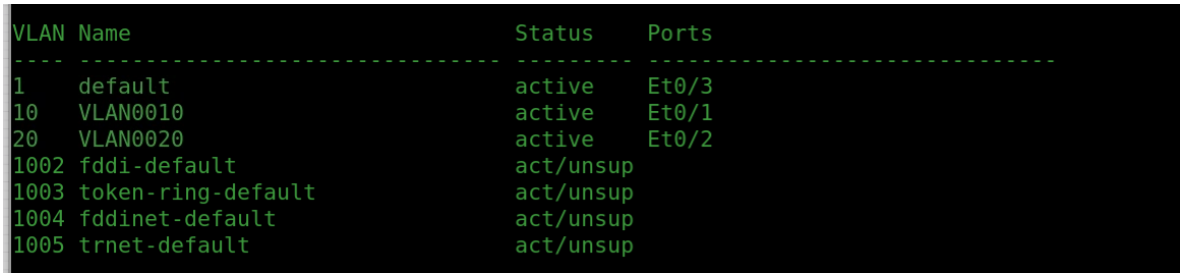
```
ip dhcp pool sales
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.1

ip dhcp pool marketing
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.2.1
```

c) VLANs and Switches Configuration

Configuring (Groups) or main switches in the topology:



Figure(3.7): VLANs and switches configuration.



Figure(3.8): Show VLANs.

CHAPTER FOUR

Results and Discussion

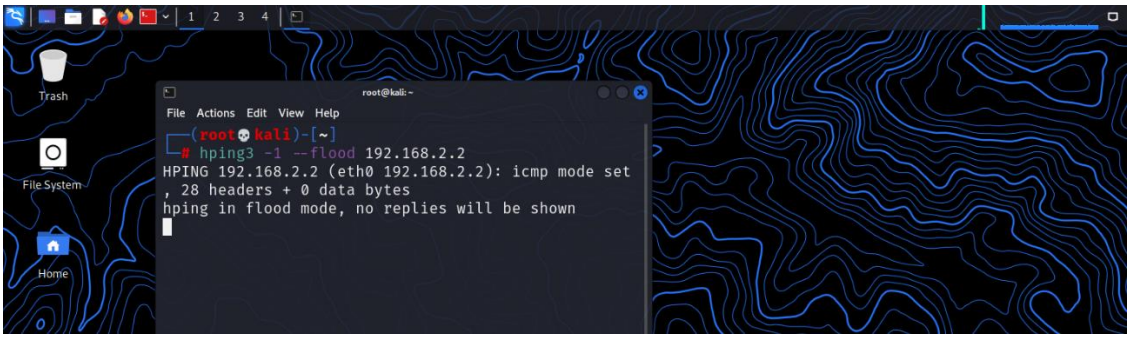
4.1 Introduction:

This chapter delves into the outcomes of the implemented methodologies and their implications. Through various experiments and tests, the effectiveness of the devised attack detection and defense mechanisms is evaluated. This chapter serves as a platform to analyze the performance of the deployed strategies in mitigating advanced cyber threats such as ICMP flood, Smurf, SYN attacks, and DNS spoofing. Additionally, discussions revolve around the observed results, potential limitations, and areas for further improvement.

4.2 DoS Experiments

1) ICMP Attack:

The ICMP flood attack can be executed using a well-known command in Kali Linux known as hping3, as illustrated in figure (3.8). The "-1" parameter designates the ICMP protocol, while "--flood" signifies the initiation of an ICMP flooding attack. Consequently, this command initiates the transmission of a substantial volume of ICMP packets directed towards the specified target, thereby inundating it. To demonstrate this, a basic ICMP attack will be conducted utilizing the hping3 utility within the Kali Linux operating system.



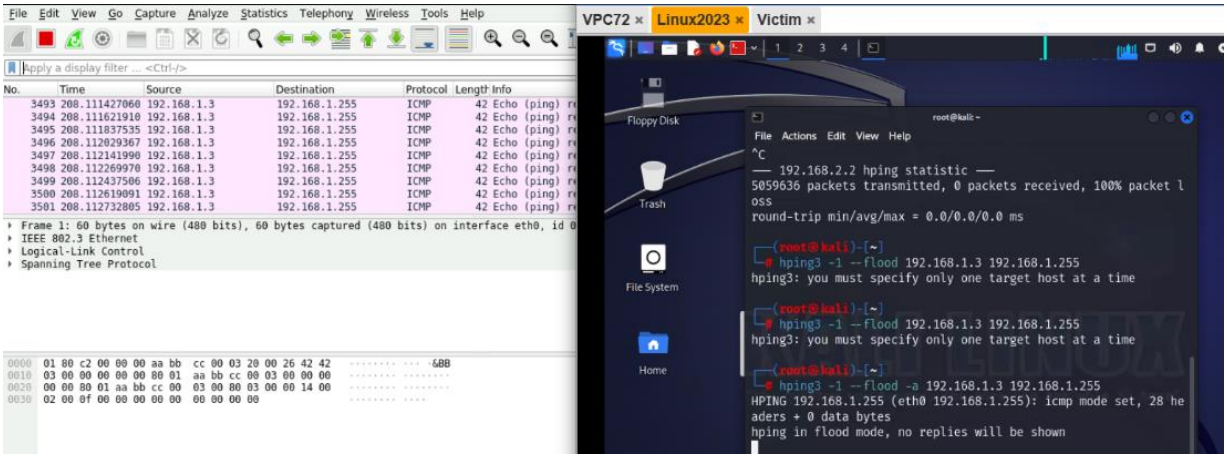
Figure(4.1): ICMP flood attack by hping3.

Figure(4.2): ICMP result on the computer of the victim.

To mitigate the attack, a Control Access List (ACL) will be implemented on the switch port connected to the attacker's PC, as depicted in Figure (3.13).

2) Smurf Attack:

To perform a Smurf attack using hping3 on Kali Linux, identify the target IP, and execute the command: “hping3 -1 --flood -a Source IP Destination IP”, as shown below:



Figure(4.3): SMURF attack by hping3.

This attack will be halted utilizing the same methodology, as it also relies on the ICMP protocol, akin to the Ping of Death Attack.

```
!
access-list 100 deny   icmp host 192.168.1.2 host 192.168.2.2
access-list 100 permit ip any any
```

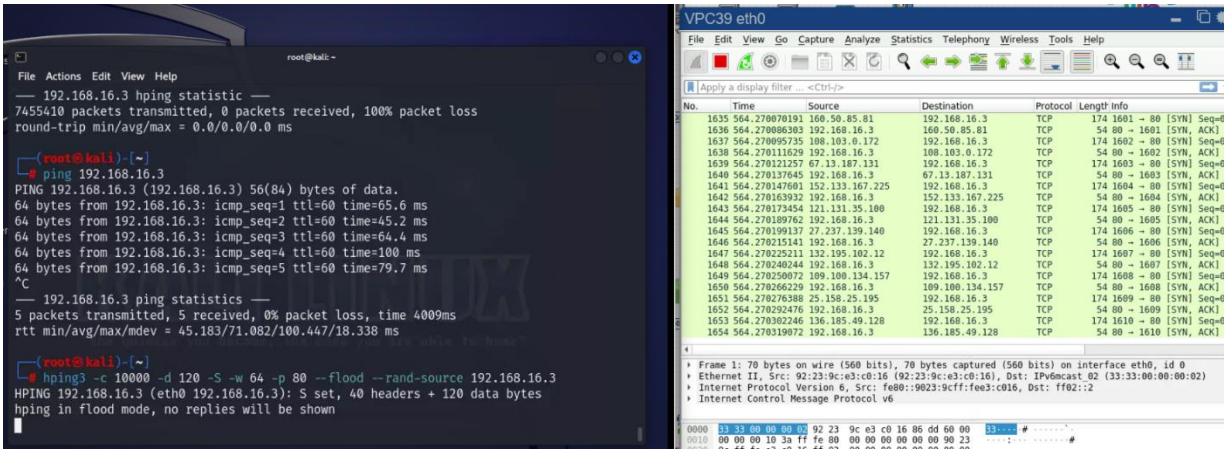
Figure(4.4): prevent ICMP and Smurf attacks.

3) SYN Attack:

To execute a SYN attack using Hping3 on Kali Linux open a terminal and input the command: "hping3 -S --flood Target IP" replacing [Target IP] with the IP address of the target system. This command initiates a SYN flood attack by sending a barrage of SYN packets to the specified port.

```
┌──(root㉿kali)-[~]
└─# hping3 -S --flood 192.168.16.3
HPING 192.168.16.3 (eth0 192.168.16.3): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure(4.5): SYN attack by hping3.



Figure(4.6): SYN result on the target shown by Wireshark.

To stop the attack, we will make a new access list that stop the TCP requests in the switch that's connected the attacker's PC, as shown below :

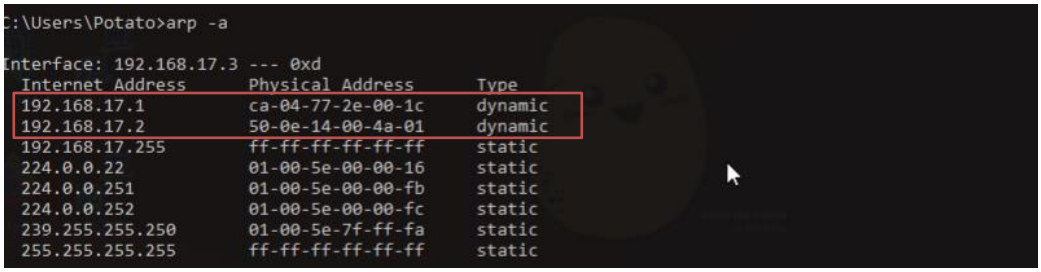
```
access-list 120 deny   tcp host 192.168.1.2 192.168.16.0 0.0.0.255
access-list 120 permit ip any any
!
```

Figure(4.7): prevent SYN attack.

4.3 MitM experiments

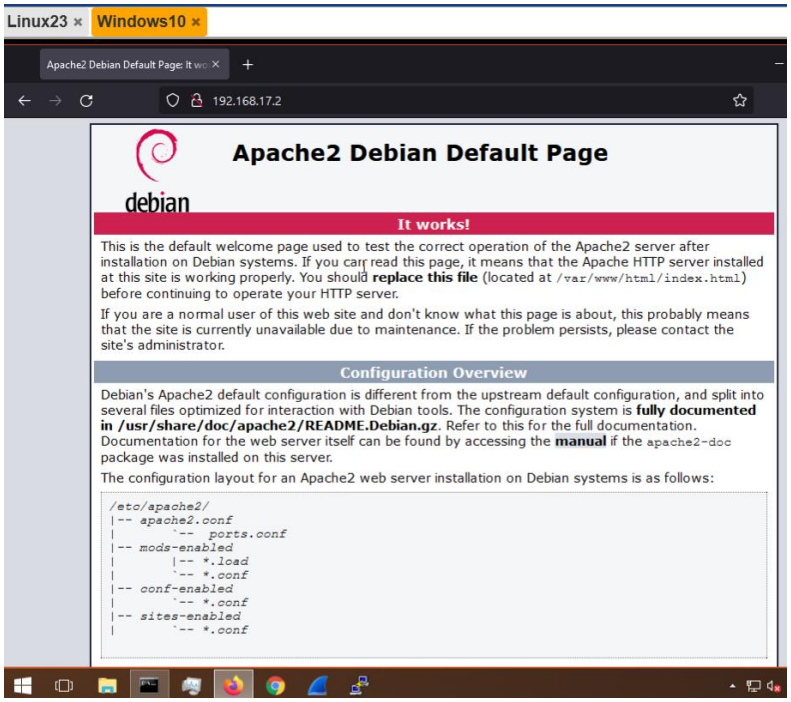
1) DNS Spoofing:

Before the attack begins, we must pay attention to the physical addresses of both the attacker and the victim to know the difference that occurs after applying the attack, as shown in the figure below:



Figure(4.8): ARP table before the dns-spoofing attack.

Initially, it is necessary to initiate the Apache Service. The Apache service in Kali Linux is the Apache HTTP Server, a popular open-source web server software used for hosting websites and conducting security testing. It enables serving both static and dynamic content over the internet[31]. Subsequently, verification will be conducted to ensure accessibility of the attacker's website from the victim's PC.



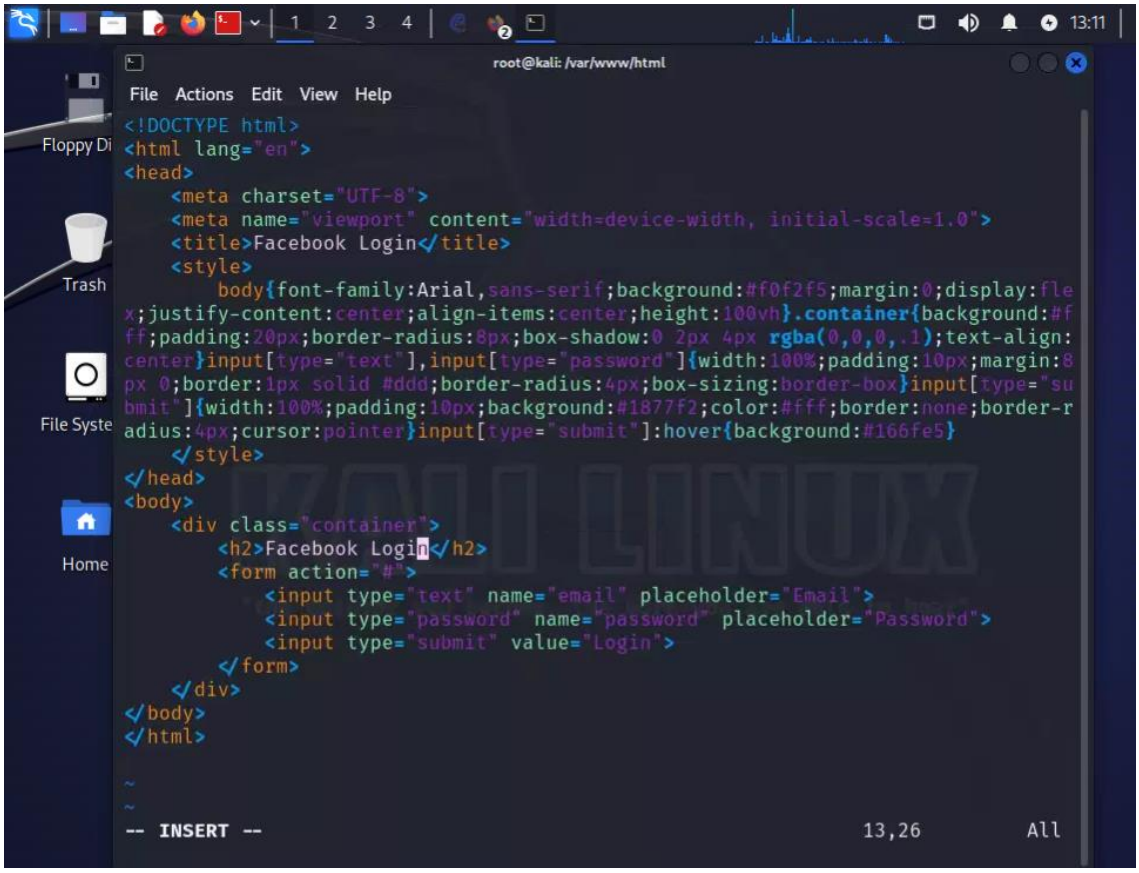
Figure(4.9): default Apache service page.

Later on, the webpage will undergo modification to resemble a Facebook login page, a process achieved by editing the "index.html" file using the Vi editor or an alternative text editor.

```
┌──(root㉿kali)-[~]
└─# sudo service apache2 start

┌──(root㉿kali)-[~]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# ls -l
total 16
-rw-r--r-- 1 root root 10701 Nov 30 11:54 index.html
-rw-r--r-- 1 root root   615 Nov 30 11:55 index.nginx-debian.html

┌──(root㉿kali)-[/var/www/html]
└─# mv index.html index-old.html

┌──(root㉿kali)-[/var/www/html]
└─# vi index.html

┌──(root㉿kali)-[/var/www/html]
└─# ls -l
total 20
-rw-r--r-- 1 root root    40 Apr  5 13:03 index.html
-rw-r--r-- 1 root root   615 Nov 30 11:55 index.nginx-debian.html
-rw-r--r-- 1 root root 10701 Nov 30 11:54 index-old.html
```

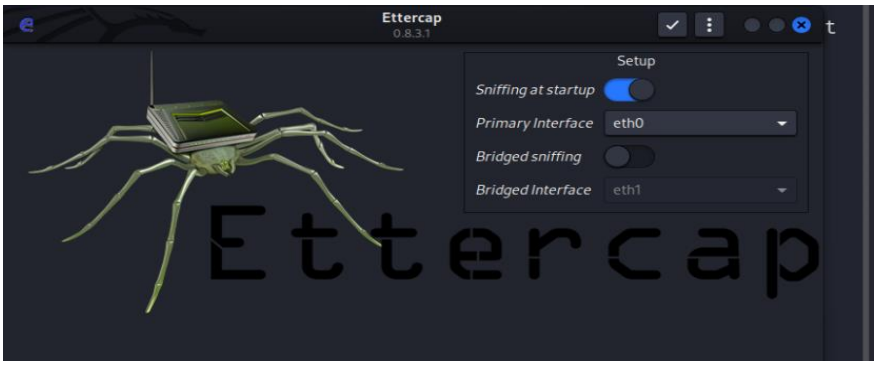
Figure(4.10): editing index.html file.

This represents the HTML code that was utilized :



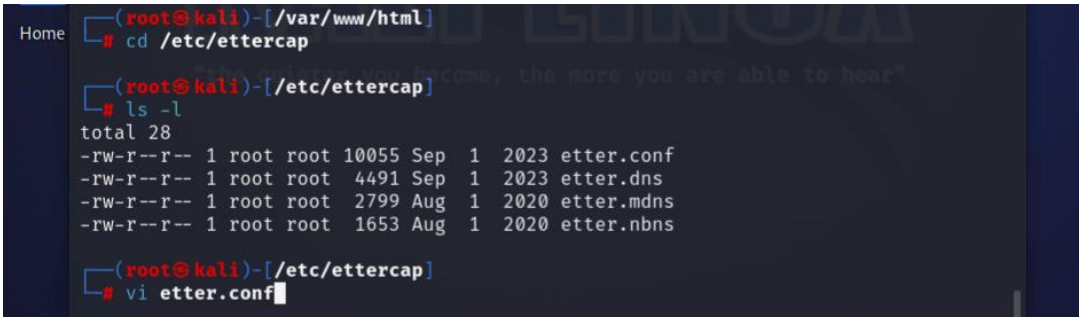
Figure(4.11): HTML code for Facebook login page.

Now in order to be able to get the victim's login information we will lunch Ettercap, Select the appropriate network interface (eth0).



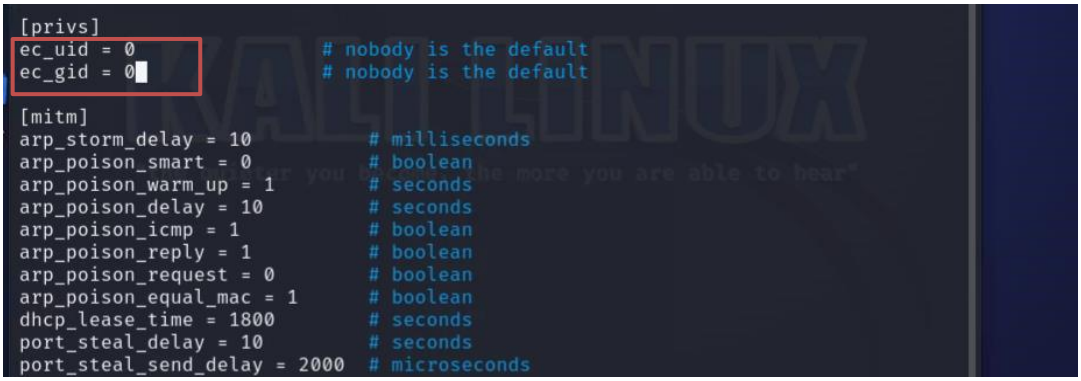
Figure(4.12): Ettercap start page.

Before utilization, it is imperative to modify certain files such as "etter.conf" and "etter.dns" to specify the target website and the IP address of the attacker.



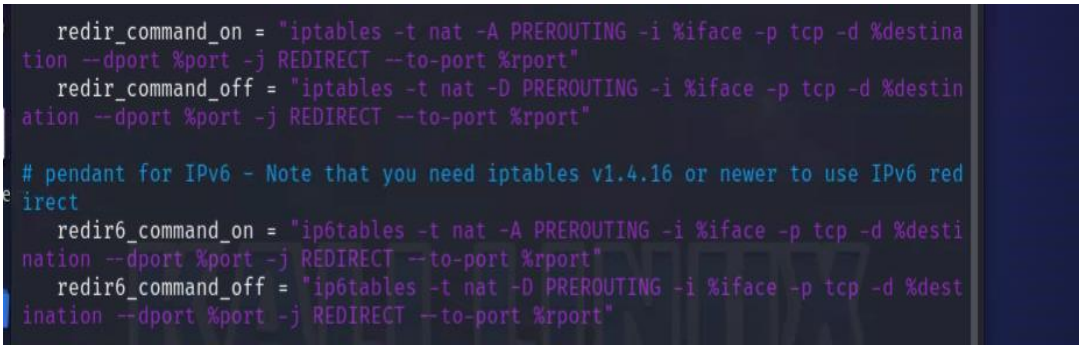
Figure(4.13): editing etter.conf file.

We need to modify both "ec_uid" and "ec_gid" values to zero, as illustrated below:



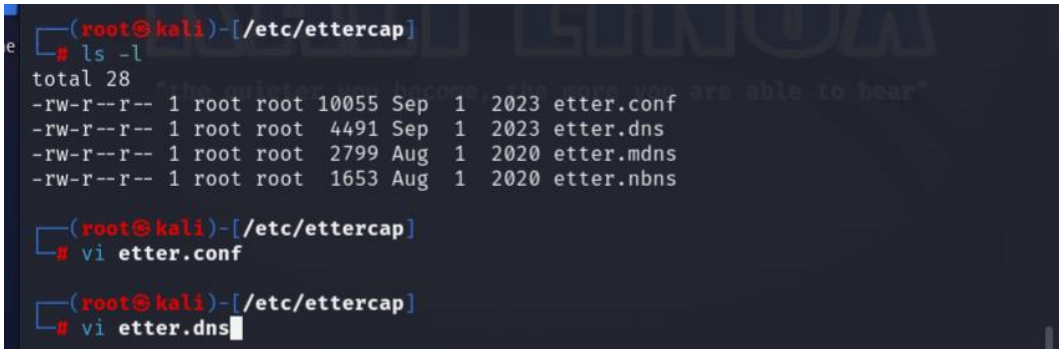
Figure(4.14): changing values in etter.conf file.

We must remove the comment markers from these lines as well.



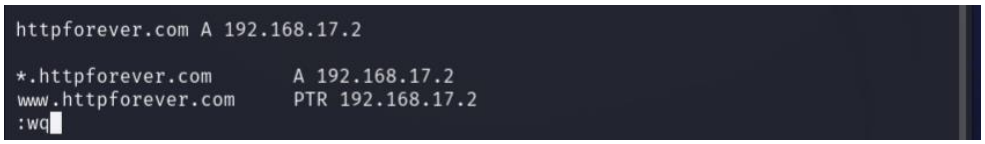
Figure(4.15): uncommenting redir and redir6 commands.

Subsequently, we exit the current session and proceed to modify the etter.dns file according to the following instructions.



Figure(4.16): editing etter.dns file.

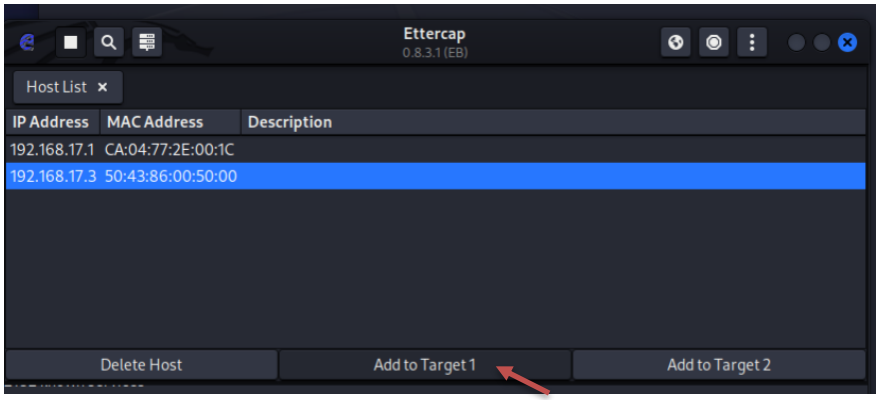
To ensure the attack targets all prefixes of the designated IP, we must insert the target website and the attacker's IP into “etter.dns” file. After making these additions, we save the changes and exit the editing session.



Figure(4.17): adding the IP address of the target website.

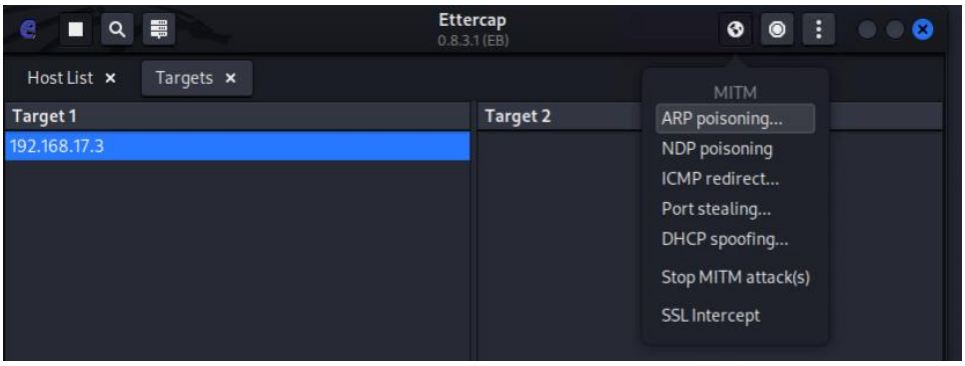
Returning to Ettercap, our initial step is to conduct a network scan to identify hosts. Following this, we select the IP address of the intended victim and add it to Target1.

Figure(4.18): Host scanning in Ettercap.



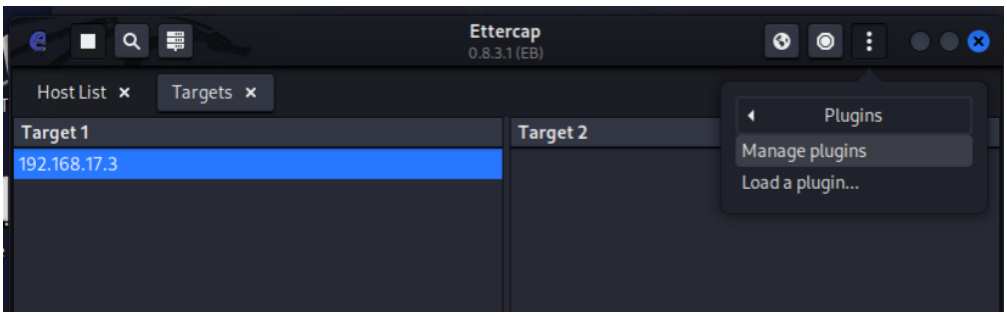
Figure(4.19): choosing The Target.

Next, we enable ARP poisoning for the selected target through the MITM menu.



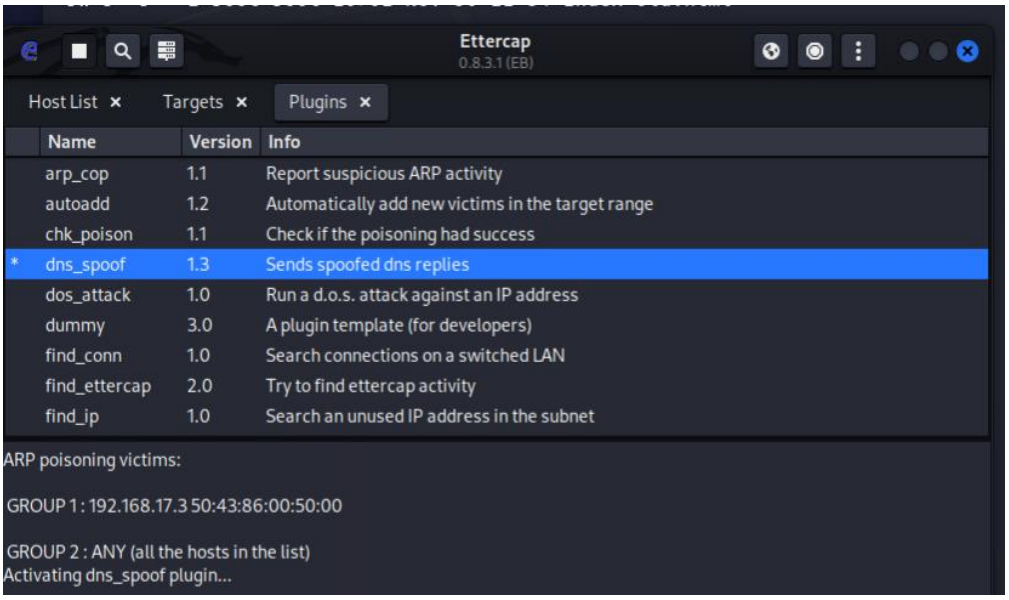
Figure(4.20): ARP poisoning.

Subsequently, we select the "Manage plugins" option within the plugins menu.



Figure(4.21): Manage plugins option.

Lastly, opt for the DNS spoof attack.



Figure(4.22): start dns-spoofing attack.

Once the victim enters their information and clicks "Login" the data will be displayed in Ettercap.

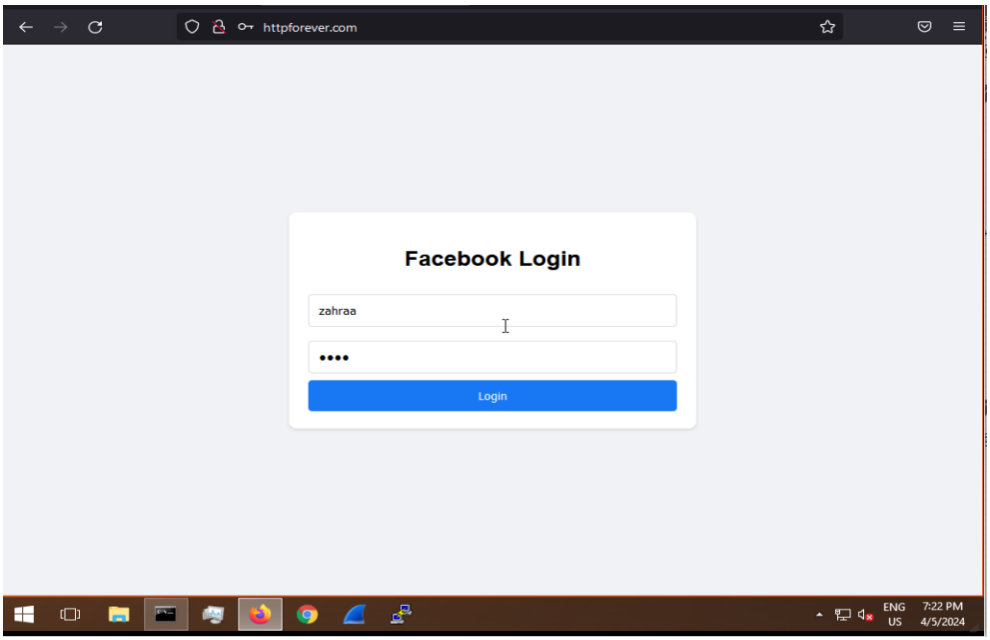
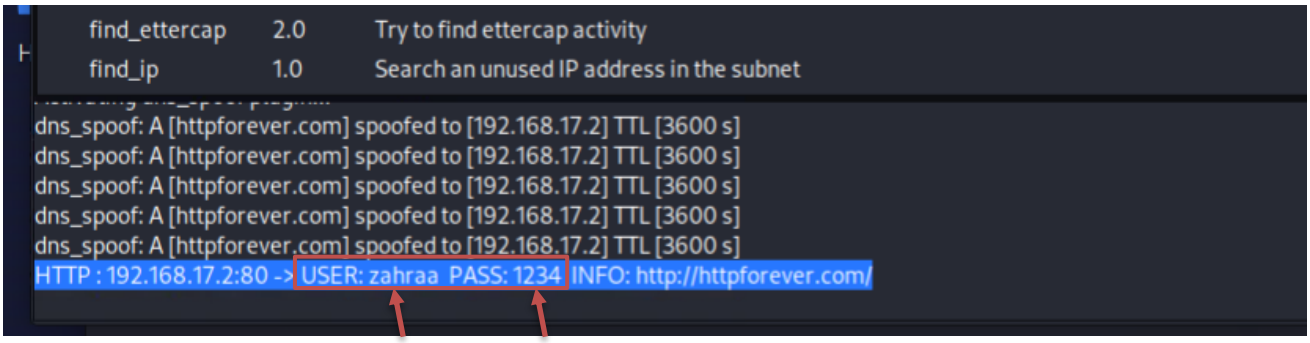


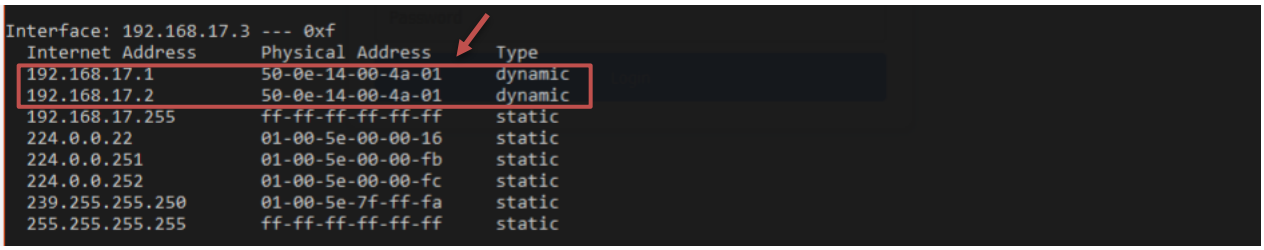
Figure (4.23): The login process.

The email field is populated with "zahraa," while the password field contains "1234."



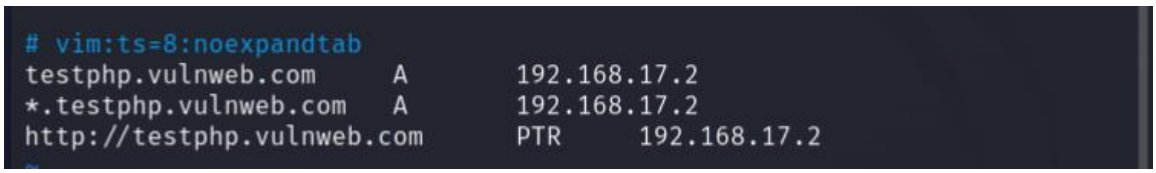
Figure(4.24): The gotten data in Ettercap.

Upon initiating the attack, the physical address of the attacker's PC is altered to resemble that of its gateway.

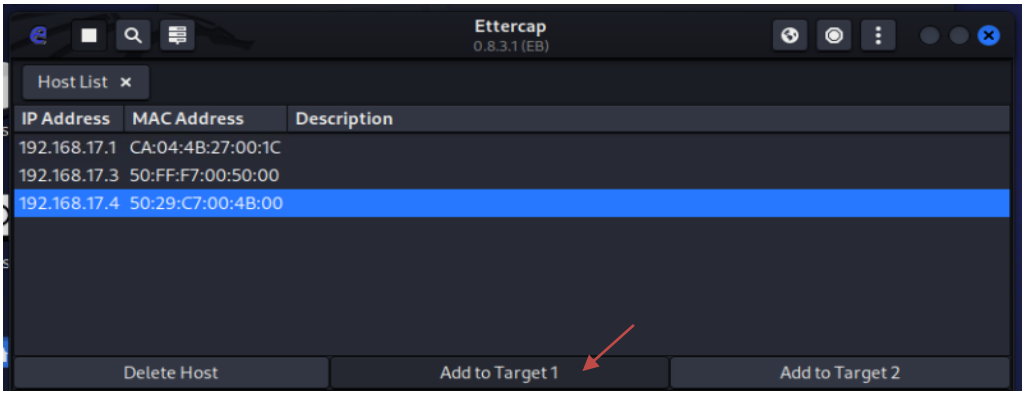


Figure(4.25): ARP table after dns-spoofing attack starts.

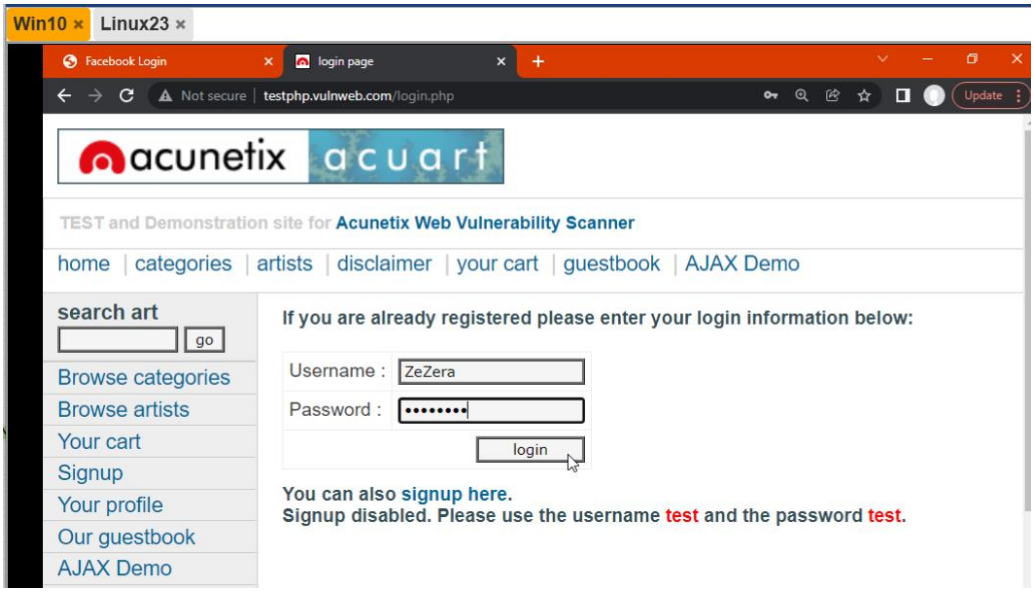
The identical procedure can be applied to web pages to pilfer user login information, as demonstrated in the given example. Let's replicate the process on another PC (192.168.17.4) utilizing the website *vulnweb.com* and its login page. Initially, we must adjust the dns.etter file by specifying the new target webpage.



Figure(4.26): Adding the IP address of the second target.



Figure(4.27): choosing the second Target.



Figure(4.28): Login to vulnweb.com.

Figure(4.29): The data of user in Ettercap.

To protect against DNS spoofing attacks we can apply ARP inspection and DHCP snooping featurs on the switch.

ARP inspection typically involves enabling ARP inspection and specifying trusted ports where legitimate ARP traffic is expected by the command "IP ARP inspection trust".

Enable DHCP snooping to monitor DHCP messages exchanged between clients and servers.

by using the "IP DHCP snooping trust" command we designate trusted ports where legitimate DHCP servers are connected

```
interface Ethernet0/0
 switchport access vlan 20
 switchport mode access
 ip arp inspection trust
 ip dhcp snooping trust
```

Figure(4.30): ip arp inspection trust and ip dhcp snooping trust.

```
Switch(config)#ip dhcp snooping vlan 20
Switch(config)#end
Switch#
*Apr 13 14:32:39.629: %SYS-5-CONFIG_I: Configured from console by console
Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
20
DHCP snooping is operational on following VLANs:
20
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.0300 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----------------------  -------    ------------    ----------------
Ethernet0/0              yes        yes             unlimited
  Custom circuit-ids:
Switch#
```

Figure(4.31): Enable dhcp snooping.

```
Switch#sh ip arp ins

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   20     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   20     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   20              0              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
   20              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   20                   0                        0                      0
Switch#
```

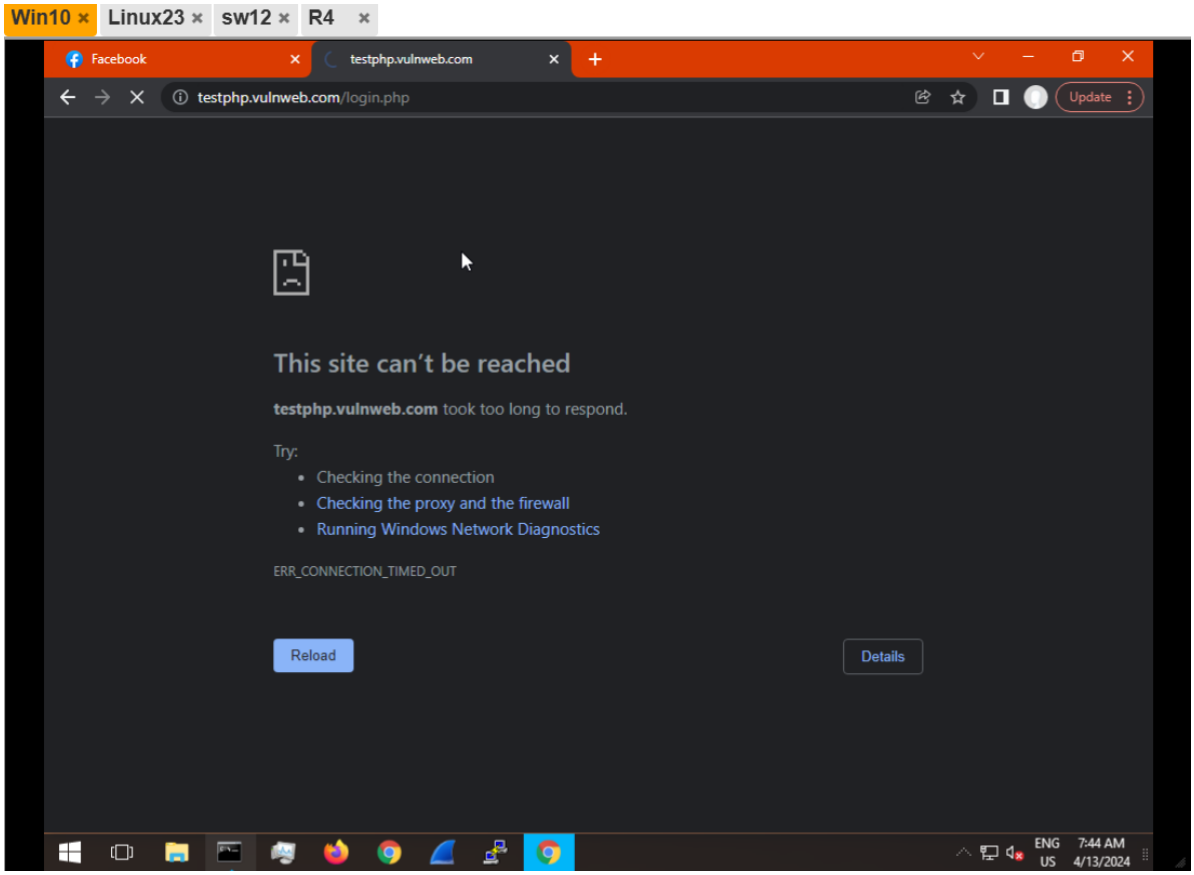
Figure(4.32): Show Ip ARP inspection.

The notifications displaying the denial process are observable in the figure depicted below.

```
Win10 × Linux23 × sw12 × R4 ×
*Apr 13 14:43:44.962: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3,
vlan 20.([5029.c700.4b00/192.168.17.4/0000.0000.0000/192.168.17.1/14:43:44 UTC Sat
Apr 13 2024])
*Apr 13 14:43:45.967: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3,
vlan 20.([5029.c700.4b00/192.168.17.4/0000.0000.0000/192.168.17.1/14:43:45 UTC Sat
Apr 13 2024])
Switch#
*Apr 13 14:43:46.967: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3,
vlan 20.([5029.c700.4b00/192.168.17.4/0000.0000.0000/192.168.17.1/14:43:46 UTC Sat
Apr 13 2024])
Switch#
Switch#
*Apr 13 14:43:48.967: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/2,
vlan 20.([500e.1400.4a01/192.168.17.1/5029.c700.4b00/192.168.17.4/14:43:48 UTC Sat
Apr 13 2024])
*Apr 13 14:43:48.967: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/2,
vlan 20.([500e.1400.4a01/192.168.17.4/ca04.64df.001c/192.168.17.1/14:43:48 UTC Sat
Apr 13 2024])
*Apr 13 14:43:48.967: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3,
vlan 20.([5029.c700.4b00/192.168.17.4/0000.0000.0000/192.168.17.1/14:43:48 UTC Sat
Apr 13 2024])
```

Figure(4.33): The denying process.

We observe that the webpage has become unreachable, indicating the cessation of the redirection process. Consequently, the attacker's ability to pilfer additional data from the victim is thwarted.



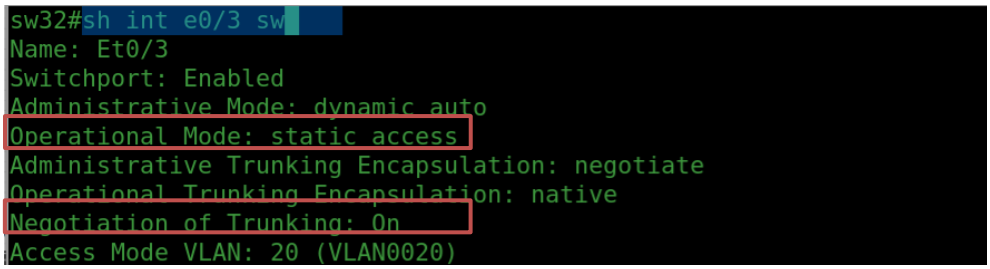
Figure(4.34): The result after stopping DNS spoofing attack.

2) VLAN Hopping:

➢ DTP attack (Dynamic Trunking Protocol)

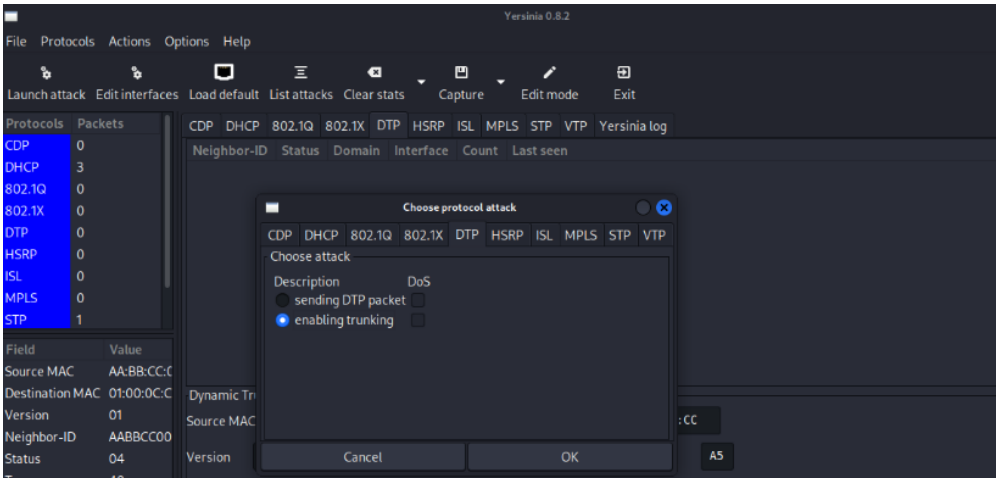
This attack occurs when the switch port mode access is disabled, enabling trunk negotiation. Consequently, the attacker may exploit this to enable trunking, potentially gaining unauthorized access to other VLANs.

It is evident that the operational mode is set to static access, and further, the Negotiation of Trunking is enabled.



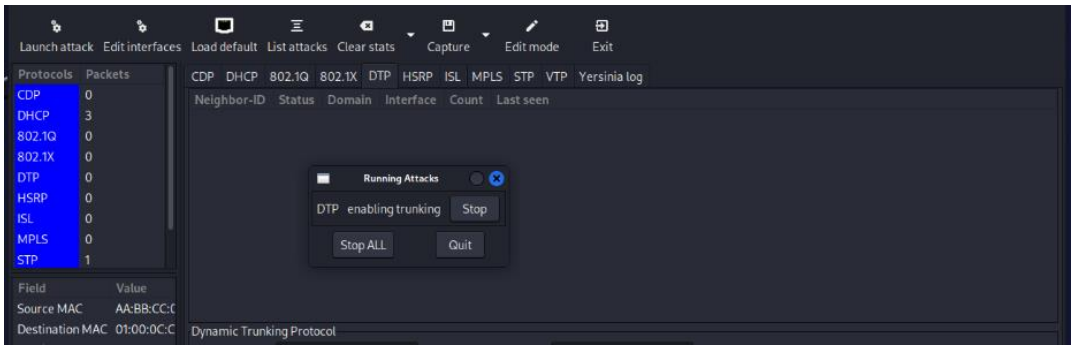
Figure(4.35): Show interface e0/3 switch before the attack

Presently, to initiate the attack, we will ascertain the protocol for the attack and opt to enable Trunking to start the process.



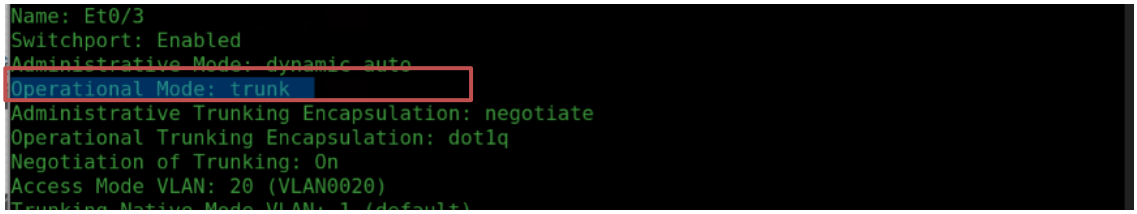
Figure(4.36): Lunching Dynamic Trunking Protocol (DTP) attack.

We may verify the successful initiation of the attack by employing the "List attacks" option, depicted in Figure (4.37), where DTP enabling Trunking is indicated as operational.



Figure(4.37): List of Running Attacks

It is apparent that the operational mode transitioned to Trunk subsequent to the implementation of the attack.

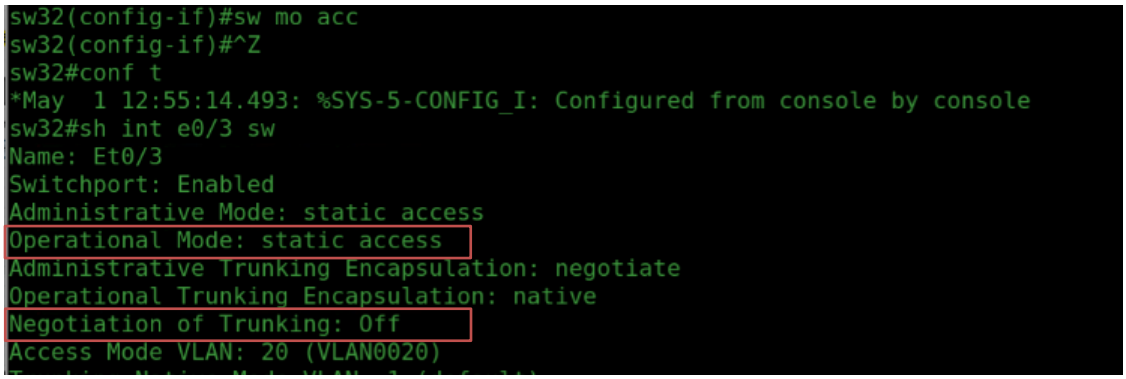


Figure(4.38): Show interface e0/3 switch after the attack

To halt or mitigate such an attack, we can readily enable switchport mode access on the identical interface, as illustrated in the accompanying figure.

Figure(4.39): enable switchport mode access on interface e0/3

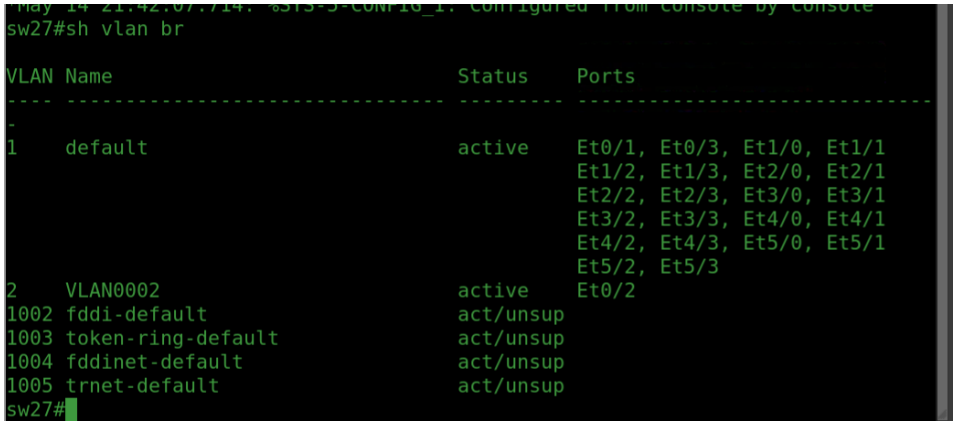
At present, the operational mode has reverted to static access, and correspondingly, the Negotiation of Trunking has been deactivated.



Figure(4.40): interface e0/3 after switchport mode access

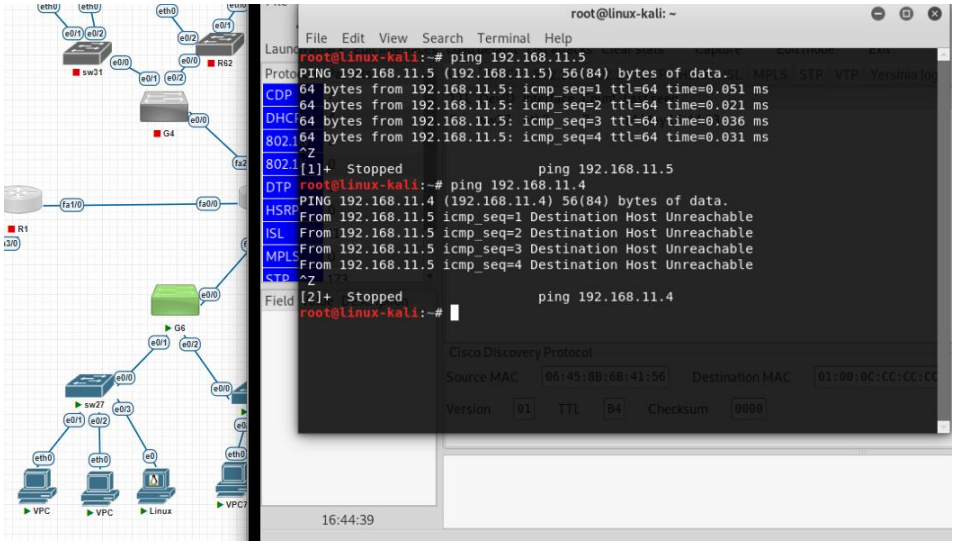
- **Double Tagging:**

In order to execute a double tagging attack, the initial step involves specifying the VLAN assignment for each individual device. Subsequently, following the establishment of the network environment, it becomes apparent that all devices contained within VLAN1 possess the ability to communicate exclusively with other devices residing within the same VLAN, with a similar arrangement observed for devices allocated to VLAN2.



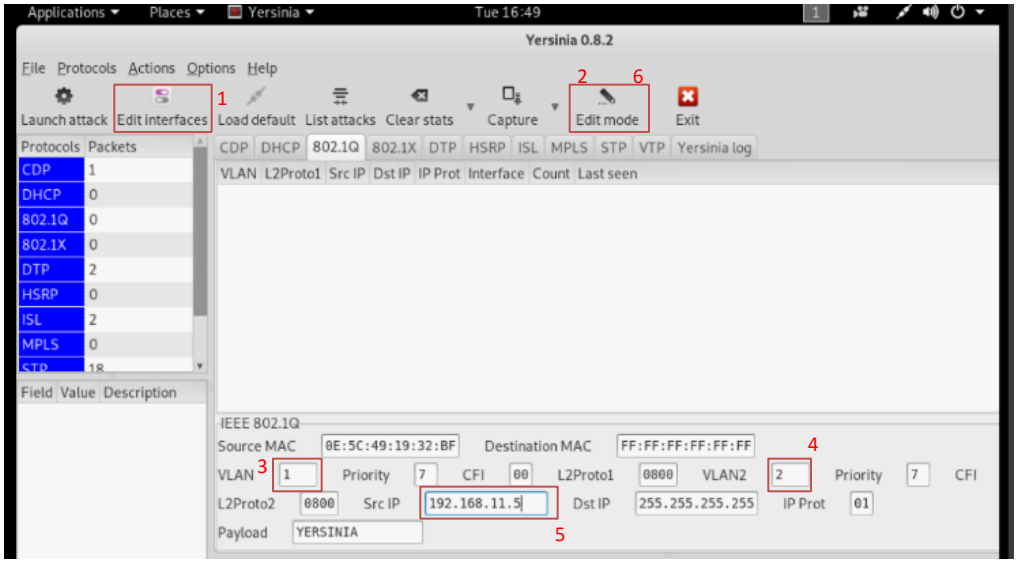
Figure(4.41): switch1 VLAN brief

However, it is imperative to note that VLAN1 is unable to establish communication with VLAN2. Such attacks are orchestrated with the explicit objective of establishing an unauthorized unidirectional connection.



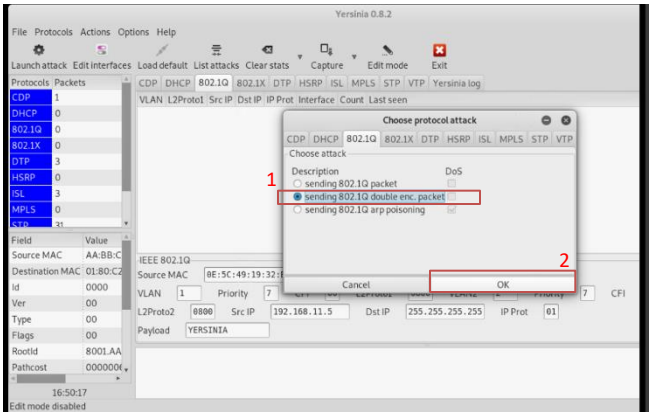
Figure(4.42): VLAN2 not reachable to VLAN1

Next, we choose Yersinia, which is packet manipulation program to help us adding two tags in ICMP packets. In Yersinia interface, firstly, we select our network interface (eth0), then switch to "Edit mode" to adjust VLAN (which VLAN the attacker is in and which the victim is in) and source IP (attacker's IP address: 192.168.56.101). Finally, don't forget to click "Edit mode" button again to exit "Edit mode". After configuring Yersinia, it is now ready to add 2 tags to every ICMP packet and send out via eth0.



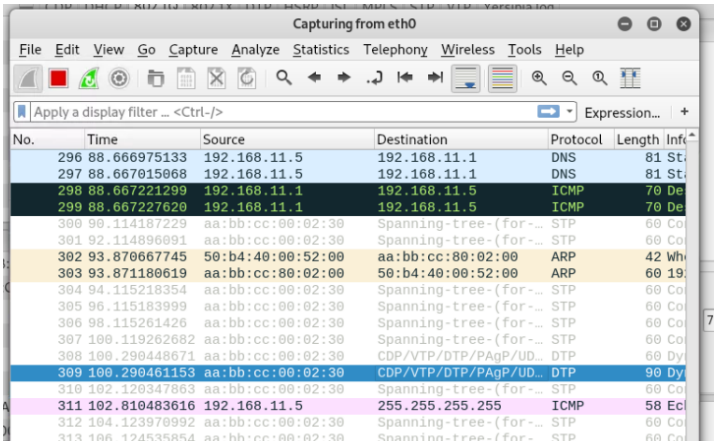
Figure(4.43): Preparing to begin the attack

Let’s launch the attack and see…



Figure(4.44): Choosing the attack type

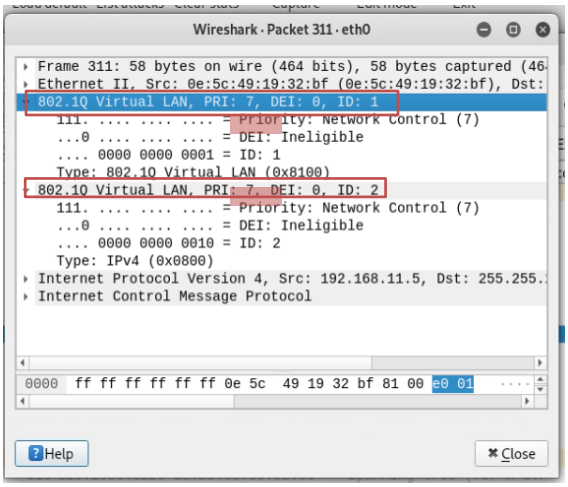
As soon as launching the attack, we’re able to see our ICMP packet is broadcasting out with the source IP address is the attacker’s IP address



Figure(4.45): The appearance of the attack

A little bit detail in our packet, there are two tags that have been added to our packet, the outer is VLAN1 (ID: 1) and the inner is VLAN2 (ID: 2).

Through this we know that the attack was carried out successfully, the figure shown below explains the process better :



Figure(4.46): The two tags of the packet

To mitigate the risk of this attack, it is imperative to modify the native VLAN from its default setting, typically VLAN1, to a less predictable value, such as VLAN 566. This can be achieved through the following command: "switchport trunk native vlan 566"

By executing this command, the switch will designate VLAN 566 as the native VLAN for trunk ports, enhancing the security posture of the network and reducing the likelihood of successful VLAN hopping attacks.

```
sw27#sh int trun

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
```

Figure(4.47): The default native VLAN

```
sw27(config)#int range e0/0-3
sw27(config-if-range)#sw tr native vlan 566
```

Figure(4.48): The new native VLAN

CHAPTER FIVE

Conclusions and Future works

5.1 Conclusion

This project has made significant strides in addressing the critical issue of internal network security. Through the development of advanced attack detection methods and resilient defense mechanisms, we have gained valuable insights into the characteristics and potential impact of complex attack vectors such as ICMP, DNS, and Smurf attacks.

By leveraging real-time detection techniques and implementing resilient defense mechanisms, we have effectively identified and mitigated these sophisticated threats.

The validation of our solutions through experiments in the PNET Lab, including the successful thwarting of attacks like ICMP floods and VLAN hopping, underscores the practical efficacy of our approach. Ultimately, this research equips network administrators with the tools and strategies needed to combat emerging threats and enhance network security.

5.2 Future Directions

The configuration and specifications outlined for the initial prototype provide a solid foundation for further development and enhancement. In our future work, we aim to expand the functionality of the prototype to improve both coverage and security. Specifically, our focus will be on devising a comprehensive framework that maximizes the utilization of all protection protocols without causing disruptions to other network components or policies.

To achieve this goal, we plan to conduct thorough testing and refinement of the framework to ensure seamless integration with existing network infrastructure. Additionally, we will explore strategies to prevent and mitigate attacks such as SNMP enumeration and NTP amplification DDoS, which pose significant threats to network security.

Furthermore, our future work will involve implementing robust monitoring mechanisms to detect and respond to any malicious activity on the network promptly. By continuously monitoring network traffic and behavior, we aim to enhance our ability to identify and mitigate potential security threats in real-time.

Overall, our future work will focus on further optimizing the prototype's configuration, expanding its functionality, and strengthening its defenses against various types of attacks. Through these efforts, we aim to contribute to the advancement of network security and safeguarding against evolving threats effectively.

References

[1] Hamisi, Ndyetabura Y., et al. "Intrussion detection by penetration test in an organization network." 2009 2nd International Conference on Adaptive Science & Technology (ICAST). IEEE, 2009.

[2] Dayanandam, G., et al. "DDoS attacks—analysis and prevention." Innovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE 2017. Springer Singapore, 2019.

[3] Pingle, Bhargav, Aakif Mairaj, and Ahmad Y. Javaid. "Real-world man-in-the-middle (MITM) attack implementation using open source tools for instructional use." 2018 IEEE International Conference on Electro/Information Technology (EIT). IEEE, 2018.

[4] Rouiller, Steve A. "Virtual LAN Security: weaknesses and countermeasures." available at uploads. askapache. com/2006/12/vlan-security-3. pdf 6 (2003).

[5] Johnson, David, Yin-chun Hu, and David Maltz. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. No. rfc4728. 2007.

[6] Abrol, Lovedeep, and Parul Gahelot. "Static and Dynamic Routing Protocols in Network Security Attacks." 2023 4th International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2023.

[7]Filsfils, Clarence, et al. "Segment routing use cases." (2013).

[8] https://networklessons.com/cisco/ccie-routing-switching-written/introduction-to-is-is

[9] Rohatgi, Vaishnavi, and Shimpy Goyal. "A detailed survey for detection and mitigation techniques against ARP spoofing." 2020 fourth international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC). IEEE, 2020.

[10] James F. Kurose and Keith W. Ross: Computer Networking: A Top-Down Approach, 7th ed.:2012.

[11] AbdulGhaffar, AbdulAziz, Sumit Kumar Paul, and Ashraf Matrawy. "An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures." 2023 Biennial Symposium on Communications (BSC). IEEE, 2023.

[12] Setiawan, Aep. "Simulasi Setting WLC berdasarkan kebijakan VLAN pada Client yang terhubung ke AP di Gedung Gamma (Administrasi) Sekolah Vokasi IPB." Prosiding Seminar Nasional Ilmu Sosial dan Teknologi (SNISTEK). Vol. 5. 2023.

[13] Hasan, Md Kamrul, and Shamim Ahammed. Design & Implementation a Corporate Network Using Inter-Vlan Routing Protocol. Diss. East West University, 2015.

[14] Jayasuryapal, G., P. Meher Pranay, and Harpreet Kaur. "A survey on network penetration testing." 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). IEEE, 2021.

[15] Harshita, Harshita. "Detection and prevention of ICMP flood DDOS attack." International Journal of New Technology and Research 3.3 (2017): 263333.

[16] Korgaonkar, Prachi, Ashish Patil, and Nilesh Khochare. "NetSHIELD: Countermeasure Tool for Network Layer Attacks." International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) 1 (2012): 91-94.

[17] Learning Center | Expertise in Cybersecurity | Imperva

[18] Pingle, Bhargav, Aakif Mairaj, and Ahmad Y. Javaid. "Real-world man-in-the-middle (MITM) attack implementation using open source tools for instructional use." 2018 IEEE International Conference on Electro/Information Technology (EIT). IEEE, 2018.

[19] Yan, Boru, et al. "Detection and defence of DNS spoofing attack." Jisuanji Gongcheng/ Computer Engineering 32.21 (2006): 130-132.

[20] Yakhlef, Sulaiman Khalifa, et al. "Simulation of Routing in NAT, PAT and Inter_VLAN Networks." Conference Title. 2014.

[21] Sundararajan, Balaji, Samar Sharma, and Yegappan Lakshmanan. "LAYER 4 THROUGH LAYER 7 SERVICE CHAINING FOR VIRTUAL NETWORK FUNCTIONS IN CLOUD ENVIRONMENT." (2018).

[22] Basile, Francesco, Ciro Carbone, and Pasquale Chiacchio. "PNetLab: a tool for the simulation, analysis and control of discrete event systems based on petri nets." IFAC Proceedings Volumes 37.18 (2004): 213-218.

[23] https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation

[24] Feltham, Joanna L., et al. "Definition of the switch surface in the solution structure of Cdc42Hs." Biochemistry 36.29 (1997): 8755-8766.

[25] Yakhlef, Sulaiman Khalifa, et al. "Simulation of Routing in NAT, PAT and Inter_VLAN Networks." Conference Title. 2014.

[26] Garrett, Aviva, Gary Drenan, and Cris Morris. Juniper networks field guide and reference. Addison-Wesley Professional, 2002.

[27] 陈家峰. “Virtual desktop implementation method, device and system and terminal.” (2014).

[28] Kaur, Gurline, and Navjot Kaur. "Penetration testing–reconnaissance with NMAP tool." International Journal of Advanced Research in Computer Science 8.3 (2017): 844-846.

[29] Joni, Joni, and Setiawan Assegaf. "Analisis Dan Perancangan Jaringan Virtual Pada Smk Negeri 2 Kota Jambi." Jurnal Manajemen Sistem Informasi 4.2 (2019): 137-146.

[30] Carranza, A., and C. DeCusatis. "Wireless network penetration testing using Kali Linux on beagleBone black." Proceedings of the 14th LACCEI International Multi-Conference for Engineering, Education, and Technology:“Engineering Innovations for Global Sustainability”, Costa Rica. 2016.

[31] Lukman, Lukman, and Melati Suci. "Analisis perbandingan kinerja snort dan Suricata sebagai intrusion detection system dalam mendeteksi serangan syn flood pada web server Apache." Respati 15.2 (2020): 6-15.

[32] Andreatos, Antonios. "An Educational Scenario for Teaching Cyber Security Using low-cost Equipment and Open Source Software." Proceedings of the ECCWS (2023).

[33] Afanasyev, Andrey, Z. Zhiming Zhao, and A. Arie Taal. "Virtual infrastructure partitioning and provisioning under nearly real-time constraints." (2018).

المستخلص

أصبح تأمين الشبكات ضد الهجمات المتقدمة تحديًا كبيرًا في المشهد الرقمي اليوم. يهدف هذا المشروع البحثي إلى معالجة هذا التحدي من خلال التركيز على الكشف المتقدم عن الهجمات وتطوير آليات دفاعية مرنة. الهدف هو تعزيز أمان الشبكة من خلال تحديد وتخفيف مختلف نواقل الهجوم المعقدة، مثل هجمات فيضاناتICMP ، وهجمات SMURF، وهجماتDNS ، وهجماتSYN ، وهجمات التنقل.VLAN

ويتضمن البحث تحليلاً شاملاً لأنماط الهجوم المتقدمة هذه للحصول على فهم أعمق لخصائصها وتأثيرها المحتمل على البنية التحتية للشبكة. ومن خلال استخدام تقنيات الكشف المتقدمة، مثل الكشف عن الحالات الشاذة، وتحليل السلوك، وتحليل حركة مرور الشبكة، يهدف المشروع إلى تطوير آليات فعالة لكشف وتحديد هذه الهجمات في الوقت الفعلي. بالإضافة إلى ذلك، سيتم تصميم آليات دفاعية مرنة لتقليل تأثير الهجمات الناجحة وضمان توافر الشبكة وسلامتها.

قد تتضمن هذه الآليات تصفية حركة المرور، وتحديد المعدل، وأنظمة كشف التسلل والوقاية منه واستراتيجيات الاستجابة التكيفية. من خلال الجمع بين الكشف المتقدم عن الهجمات واستراتيجيات الدفاع المرنة، يهدف هذا المشروع البحثي إلى تزويد مسؤولي الشبكات بالأدوات والمعرفة اللازمة لتأمين شبكاتهم ضد مجموعة واسعة من التهديدات الناشئة والمتطورة. سيستخدم المشروع مختبر PNET لإنشاء سيناريو شبكة يحاكي آليات الهجوم والدفاع في بيئة واقعية وخاضعة للرقابة.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بغداد ـ كلية العلوم
قسم علوم الحاسوب

تأمين الشبكات: الكشف المتقدم عن الهجمات وآلية الدفاع المرنة

مشروع
مقدم الى قسم علوم الحاسوب في كلية العلوم ـ جامعة بغداد
كجزء من متطلبات نيل شهادة البكالوريوس
في علوم الحاسوب

من قبل
زهراء إبراهيم خليل

بأشراف
الأستاذ سيف سعد شهاب

1445 AH 2024