LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

60% Group Coursework 02

Year and Semester

2024 -25 Autumn Semester

Student Name: Bhumika Dahal London Met ID: 23056163
Student Name: Rohan Shrestha London Met ID: 23056199
Student Name: Sujita Sherpa London Met ID: 23056233

Assignment Due Date: 12/05/2025

Assignment Submission Date:12/05/2025

Word Count (Where Required): 11021

I confirm that I understand my coursework needs to be submitted online via MST 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.

23056233 Sujita Sherpa.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:95439542

Submission Date
May 12, 2025, 10:39 AM GMT+5:45

Download Date
May 12, 2025, 10:41 AM GMT+5:45

File Name
23056233 Sujita Sherpa.docx

File Size
71.7 KB

56 Pages

11,021 Words

62,042 Characters

turnitin Page 1 of 67 - Cover Page Submission ID trn:oid:::3618:95439542

16% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- **150** Not Cited or Quoted 14%
  Matches with neither in-text citation nor quotation marks
- **25** Missing Quotations 2%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

6% Internet sources
3% Publications
15% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **150** Not Cited or Quoted 14%
  Matches with neither in-text citation nor quotation marks
- **25** Missing Quotations 2%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

- 6% Internet sources
- 3% Publications
- 15% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	University of Hertfordshire on 2022-03-10 <1%
2	Submitted works	Multimedia University on 2024-02-19 <1%
3	Submitted works	Coventry University on 2023-04-04 <1%
4	Submitted works	Nottingham Trent University on 2024-03-16 <1%
5	Submitted works	Napier University on 2023-08-24 <1%
6	Submitted works	University of Westminster on 2023-09-07 <1%
7	Internet	codecomplete.jp <1%
8	Publication	Bongsik Shin. "A Practical Introduction to Enterprise Network and Security Mana... <1%
9	Submitted works	Swinburne University of Technology on 2022-06-19 <1%
10	Submitted works	Embry Riddle Aeronautical University on 2025-02-11 <1%

Abstract

In today's advanced world we rely on the internet for communication, business, and other services. However, with the advancement and use of technology it had led to more cybersecurity threats. One of the most serious threats is the Man-in-the-Middle. This report evaluates the concept, execution, and mitigation of Man-in-the-middle (MITM) attacks, while focusing on spoofing and eavesdropping techniques in the field of cybersecurity. With the advancement of digital communication and internet-based services, the threat of MITM has also increased rapidly, making MITM attacks an increasing critical concern. Through research and practical simulation, the report presents a comprehensive analysis of how attackers manipulate communication between system. The report explored into attack methodologies such as ARP Spoofing and network reconnaissance, and demonstration executed practically of the attack using tools like Kali Linux, Nmap, Ettercap, and Wireshark in a safe and controlled virtual lab environment. The report highlights each phase of attacks using the Penetration testing Execution Standard (PTES) framework, from pre-engagement to post-exploitation. Furthermore, the study also delves into effective countermeasures, including Dynamic ARP inspection, static ARP entries, encrypted communication protocols, and intrusive detection systems, aiming to mitigate these threats. The objective of this study is to understand these attacks and promote the implementation of strategies to secure network security.

Table of Contents

1. Introduction....1
1.1. Rationale....2
1.2. Current Scenario....2
1.3. Problem Statement....3
1.4. Aim....4
1.5. Objective....4
1.6. Report Structure....4
2. Background....8
2.1. Man-in-the-middle (MITM) attack....8
2.2. History Of MITM....9
2.3. ARP Protocol....10
2.4. Spoofing....10
2.4.1. Types of Spoofing....11
2.5. Eavesdropping....13
2.5.1. Types of eavesdropping Attacks....14
2.6. Penetration testing execution standard....14
2.6.1. Pre-engagement Interaction....14
2.6.1.2. Metasploitable 2....16
2.6.1.3. NAT network....16
2.6.2. Intelligence gathering....16
2.6.3. Threat modeling....17
2.6.3.1. Wireshark....17
2.6.4. Vulnerability Analysis....18
2.6.5. Exploitation....18
2.6.5.2. Ettercap....19
2.6.6. Post exploitation....19
2.6.7. Reporting....19
3. Demonstration....20
3.3. Methodology....20
3.4. Performing the Man-in-the-middle attack....20
3.4.1. Pre-Engagement Interactions....20
3.4.2. Intelligence Gathering....24
3.4.3. Threat Modeling....30
3.4.4. Exploitation....30

3.4.5. Post-Exploitation....41
4. Mitigation....52
4.1. Dynamic ARP inspection....52
4.2 Disable insecure protocols like Telnet/HTTP....53
4.3. Static ARP Cache Table....54
4.4. IDS/IPS....55
5.Evaluation....57
5.1. Pros of applied mitigation strategies....57
5.2. Cons of applied mitigation strategies....59
5.3. Application areas....60
6. Conclusion....62
7. References....63
8. Appendices....67
8.1. Setting up the environment for exploiting....67
8.1.1. Installation of virtual machines on Oracle VirtualBox....67
8.1.2. Network Adapter Configuration of Virtual Machines....67

Table of Figures

Figure 1: Prediction growth in the number of network-connected devices up to 2020 (Artem A. Maksutov, 2017) 1
Figure 2. Man-in-the-middle demonstration. (Ming-Hsing Chiu, 2011) 8
Figure 3. Message exchange in a typical MITM attack (M. Conti, 2016) 9
Figure 4: Screenshot of using Nmap to conduct a ping scan. 24
Figure 5: Screenshot of finding out the default gateway. 25
Figure 6: Screenshot of Nmap scan for 10.0.2.1. 25
Figure 7: Screenshot of Nmap scan for 10.0.2.2. 26
Figure 8: Screenshot of Nmap scan for 10.0.2.3. 26
Figure 9: Screenshot of Nmap scan for 10.0.2.6. 27
Figure 10: Screenshot of Nmap scan for 10.0.2.15. 27
Figure 11: Screenshot of Nmap scan for 10.0.2.15. 28
Figure 12: Screenshot of Nmap scan for 10.0.2.15. 28
Figure 13: Screenshot of Nmap scan for 10.0.2.15. 29
Figure 14: Screenshot of Nmap scan for 10.0.2.15. 29
Figure 15: Screenshot of Nmap scan for 10.0.2.4. 30
Figure 16: Screenshot of ARP poisoning. 31
Figure 17: Screenshot of ARP poisoning. 31
Figure 18: Screenshot of ARP poisoning. 32
Figure 19: Screenshot of packets with source ip and destination ip. 32
Figure 20: Screenshot of packets with source ip and destination ip. 33
Figure 21: Screenshot of ARP poisoning. 33
Figure 22: Screenshot of ARP poisoning. 34
Figure 23: Screenshot of packet flow with source ip and destination ip. 34
Figure 24: Screenshot of opening Wireshark. 35
Figure 25: Screenshot of selecting eth0 in Wireshark. 35
Figure 26: Screenshot of Wireshark capturing packets. 36
Figure 27: Screenshot of analysing packets from 10.0.2.6. 37
Figure 28: Screenshot of analysing packets from 10.0.2.15. 38
Figure 29: Screenshot of exploring protocols that are vulnerable. 39
Figure 30: Screenshot of exploring protocols that are vulnerable. 40
Figure 31: Screenshot of exploring protocols that are vulnerable. 41
Figure 32: Screenshot of the options for analysing the packet. 42
Figure 33: Screenshot of selecting the HTTP stream. 43
Figure 34: Screenshot of the observing the content of the packet. 44
Figure 35: Screenshot of observing the content of the packet. 44
Figure 36: Screenshot of filtering only telnet packets. 45
Figure 37: Screenshot of selecting a packet. 46
Figure 38: Screenshot of selecting the TCP stream. 47
Figure 39: Screenshot of observing the content of the packet. 47
Figure 40: Screenshot of observing the content of the packet. 48
Figure 41: Screenshot of username and password. 48
Figure 42: Screenshot of opening a new terminal. 49
Figure 43: Screenshot of establishing a telnet connection. 49
Figure 44: Screenshot of establishing a telnet connection. 50

Figure 45: Screenshot of snooping around the system. 50
Figure 46: Screenshot of accessing confidential files. 51
Figure 47: Figure explaining the algorithm. 56
Figure 48: Screenshot of how NAT adapter works in Virtual box. (Madapparambath, 2021) 67
Figure 49: Screenshot of how NAT Network adapter works in Virtual box. (Madapparambath, 2021) 68
Figure 50: Screenshot of launching Oracle VirtualBox. 69
Figure 51: Screenshot of options for tools section. 69
Figure 52: Screenshot of selecting network section. 70
Figure 53: Screenshot of creating a NAT network. 71
Figure 54: Screenshot of selecting the virtual machine. 72
Figure 55: Screenshot of opening preferences for the virtual machine. 73
Figure 56: Screenshot of changing adapter setting to NAT network. 74
Figure 57: Screenshot of setting NAT network name. 74
Figure 58: Screenshot of setting NAT network for Windows 7. 75
Figure 59: Screenshot of setting NAT network for Kali Linux. 75

1. Introduction

The integration of technology in day-to-day operations is reshaping nearly every aspect of modern life. Almost every aspect of modern life has been associated with the usage of Internet or other technology. People use online banking, online entertainment, online shopping, social networks, and so on and rely on them for day-to-day operations. These services are used for convenience stores or transfer user's sensitive information, which are a major target for hackers. Organizations have been using the internet and other technologies to improve communication and collaboration, increase efficiency, data management and analytics, remote work and flexibility. Organizations have become an even major target for hackers leading to huge economic losses as they have become more dependent on technology. (Saed & Aljuhani, 2022)

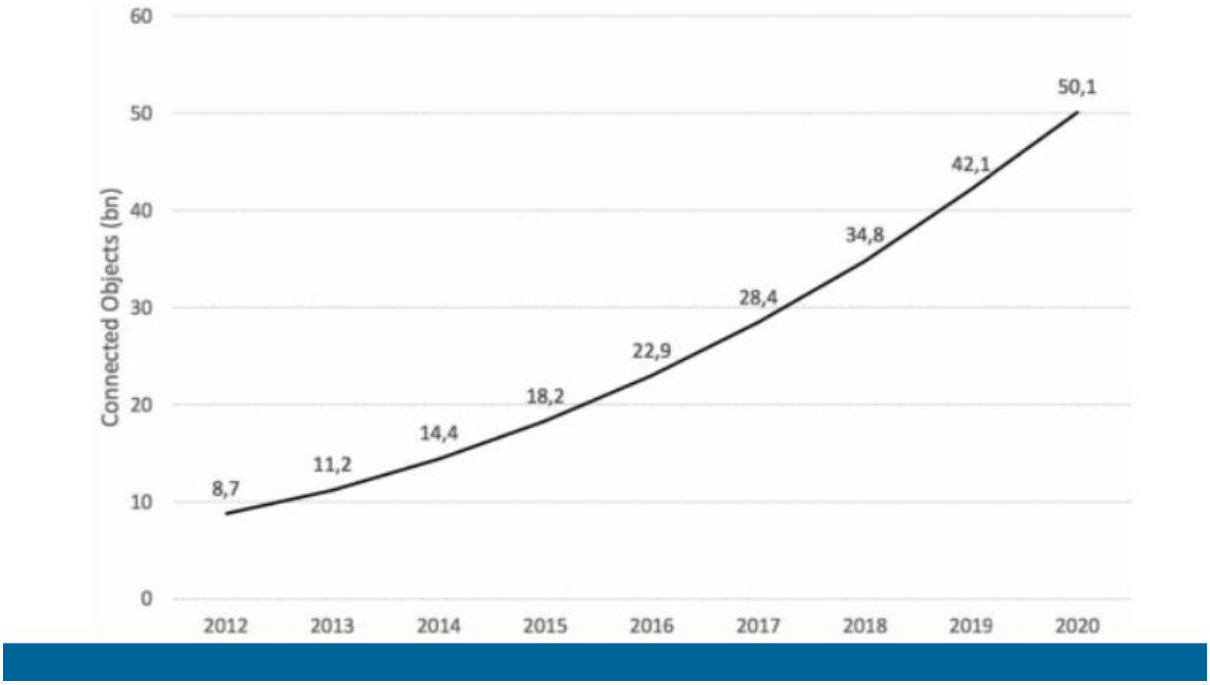

Figure 1: Prediction growth in the number of network-connected devices up to 2020 (Artem A. Maksutov, 2017)

As individuals and organizations are becoming more and more dependent on technology like the internet, hackers have been exploiting this dependency for personal gain. As individuals and organizations increasingly integrate digital systems into daily operations, hackers take advantage of security weaknesses to access sensitive information, disrupt services and commit fraud. Hackers use different attack techniques like spoofing attacks, eavesdropping attacks, Man-in-the-middle attacks, phishing attacks, malware attacks, DoS and DDoS attacks, SQL attacks, Cross-Site Scripting attacks, Zero-day exploits, and Password attacks by exploiting vulnerabilities in the systems, networks and users. These types of attacks can be used by

hackers to compromise data, disrupt operations, or gain unauthorized access which can cost an individual or organization a lot of money. The attacks that will be discussed in this report is spoofing, eavesdropping and man-in-the-middle attacks.

1.1. Rationale

As businesses, organizations, and individuals have started to heavily rely on the Internet, it has become a fundamental part of everyday life helping us to connect with billions of people worldwide. This interconnectedness has transformed the way we live, work, and interact. But the rise in online activity comes with a threat, so, securing these online data is crucial. Man-in-the-middle (MITM) attacks are a serious threat because they let attackers intercept and change private information without anyone noticing. It is important to address these attacks to keep online interactions safe and protect confidentiality, integrity, and authenticity. By understanding and mitigating MITM risks we can ensure safer and more secure digital communication and IT environment for everyone.

1.2. Current Scenario

In 2011, Cisco predicted that by 2020, there would be 50 billion devices connected to the Internet. They believed the rapid growth of the Internet would fundamentally reshape how we live, work, and interact. (Evans, 2011). New software applications emerged alongside the widespread use of the Internet. They enhanced the quality of life but also brought about a significant increase in risks. As much as it is important to build an efficient system, network or application, it is equally crucial to take the right measures to protect and offer a secure service. (Dr.Julian Fejzajb, 2021). It is easier to be interconnected with billions of people worldwide on the internet and share data simultaneously within a nanosecond. However, as data travels to its destination, it moves through multiple layers of the TCP/IP model, each posing a potential security threat. One of the major concerns is the growing reliance on cloud storage, which introduces additional vulnerabilities. This layer is especially prone to attacks, ranging from brute-force attempts on password-protected systems to even more advanced threats like Man-In-The-Middle (MITM) attacks at the session layer, potentially leading to unauthorized data modifications. (Mauro Conti, 29 March, 2016).

An MITM attack can be compared to a game of broken telephone where a message is passed from one participant to a chain of others until it reaches the last person. Often, this message is altered either intentionally or unintentionally, by the time it reaches the final person. Likewise, In an MITM attack, a third party intercepts and manipulates the communication between two

legitimate participants without their knowledge. It enables the attacker to listen in as well as modify, remove, redirect, insert, fabricate, or misdirect data. (Mauro Conti, 29 March, 2016). They aren't a new concept matter of fact they've been happening for ages. One well-known historical example is the Babington Plot of 1568. In this case, messages exchanged between Mary Stuart and her supporters about a plan to assassinate Queen Elizabeth were intercepted by a third party, Sir Francis Walsingham. Altering the contents of their messages revealed the identities of those involved leading to their execution. (Zoran Cekerevac, January 2025).

In this digital era, a lot of businesses and organizations face the threat of MITM attacks. In such attacks, hackers intercept the HTTPS traffic potentially exposing and exploiting users' credentials or even manipulating their data. Similarly, cryptographic vulnerabilities in the system allow the attackers to extract sensitive data from encrypted communications which can force mass revocation of the SSL certificates. Furthermore, Wi-fi security weakness, particularly the four-way handshake process in WPA2 allows the attackers to exploit this flaw to decrypt the wireless traffic, compromising the Confidentiality and Integrity of the data and communication within the network. (Zoran Cekerevac, January 2025). With companies increasingly dependent on digital tools, Vulnerabilities in communication systems have become prime targets for cybercriminals. In 2024, MITM attacks became a major concern in the US, particularly targeting the communication platforms that businesses use for data exchange, customer interactions, and daily operations. MITM attacks exploit these security gaps and vulnerabilities posing a serious risk to these businesses and organizations. A report by Securus Communications showed that as of May 2024, there were over 35.9 billion data breaches worldwide, with the use of advanced MITM attacks enabling the attackers/hackers to bypass even multi-factor authentication security measures. (Aijaz, 2025).

1.3. Problem Statement

Man-in-the-middle (MITM) attacks present a significant cybersecurity threat in this digital era where almost all of the data is on the internet. Here, the attacker secretly intercepts and may alter the communication between two parties by spoofing and eavesdropping. This type of attack is quite simple for hackers to execute yet can have devastating consequences if successful.

In many cases, users might unknowingly connect and communicate over insecure networks or fail to validate the authenticity of a website, apps, and even devices, which creates an opportunity for the attackers to change sensitive information such as their credentials, credit

card details, locations, mail, or even private messages. MITM attacks often occur when communication happens over unencrypted channels or weakly encrypted protocols such as HTTP or outdated versions of SSL/TLS. Common methods used in these attacks include techniques like Address Resolution Protocol spoofing (ARP Spoofing), Domain name System spoofing (DNS spoofing), and session hijacking. These methods allow attackers to intercept the data, modify communication in real time, and even impersonate the victim without any detection.

1.4. Aim

This coursework aims to explore the concepts of spoofing and eavesdropping attacks. It evaluates the risks associated with these attacks and highlights mitigation strategies to enhance security.

1.5. Objective

1. Research about concepts related to spoofing and eavesdropping attacks
2. Gather information on how the attack works, real-world examples, and why it's a cybersecurity threat.
3. Learn how to use different tools and techniques used to perform these attacks
4. Demonstrate spoofing and eavesdropping in a controlled environment.
5. Identify and discuss mitigation strategies for spoofing and eavesdropping

1.6. Report Structure

1. Introduction

This section of the report establishes the context of the report by discussing the increasing dependence on internet-based systems and the vulnerabilities this introduces. It outlines why MITM, spoofing and eavesdropping attacks are critical concerns and presents the purpose and goals of the research.

2. Background

This section builds the theoretical foundation for the Study. It explains how MITM attack functions, their historical evolution, Spoofing and Eavesdropping techniques. It also introduces the penetration testing standard used and tools selected for the attack demonstration.

3. Demonstration

This section of the report demonstrates a real MITM attack in a safe virtual environment. It demonstrates a simulated MITM attack in a virtual lab using kali Linux. It covers setting up

the environment, scanning the network, launching ARP poisoning and capturing data with Wireshark. This attack is conducted in alignment with the PTES framework ensuring a structured and methodical approach throughout the demonstration.

4. Mitigation

This section outlines multi layered defense strategies against MITM attacks. It explains how to validate ARP communications, enforce protocols like SSH and HTTPS, harden network devices with static tables and use intrusion detection/prevention systems to detect and stop malicious activities.

5. Evaluation

This section of the report assesses the strengths, effectiveness and weakness of each mitigation methods. It highlights how layered defenses, encryption and monitoring work together to reduce exposure to MITM attacks.

6. Conclusion

This section summarizes the project's overall findings. It demonstrated that Man-in-the-Middle (MITM) attacks remain a serious threat when weak or outdated security protocols are used. Sensitive data was successfully intercepted in a virtual lab environment which highlighted real-world vulnerabilities. Several mitigation strategies were reviewed, and implementation challenges were also noted. It was concluded that combining technical defenses with organizational practices is essential for effectively mitigating these risks.

7. References

A comprehensive list of academic sources, technical manuals, and online materials that support the research, attack simulation, and countermeasure discussions throughout the report.

1.7. Technical Terminologies

1. Session Hijacking

Session Hijacking is a type of cyberattack used to gain unauthorized access to an active, valid session between 2 parties. This attack often tends to target social networking sites and online banking platforms, which allows the attacker to take control of the user’s sessions and gain access to their sensitive information or services. Session hijacking is known as a common and serious threat in today’s digital environment, as this type of exploitations remain vulnerable to various websites and network. There are 3 type of session hijacking: Active, Passive and

Hybrid. In Active attacker stacks in already active session, while in passive attacker positions themselves between user and server without interrupting the session and Hybrid is combination of Active and Passive Session Hijacking. (Baitha & Vinod, 2018)

2. Zero-Day Exploit

A zero-day exploit is a type of cyberattack that takes advantage of an unpatched security vulnerability in a computer hardware, software, or firmware. The term "zero-day" refers to the fact that victim had zero day to fix the flaw before it was exploited by attackers. These vulnerabilities are dangerous because they can used to be accessed systems without warning, often before the victims are even aware of the issue. Zero-day attacks are likely to be successful of victim's ignorance and lack of patches. (Waheed, et al., 2024)

3. Brute Force Attack

A brute-force attack is a method where an attacker tries several different passwords or paraphrase hoping the guessing eventually leads to the correct combination. This process involves systematically trying all the possible combinations until the right one is found. In some cases, the attacker may also try to guess the encryption key, in which encryption usually generated through a password using a key derivation function known as an exhaust key search. (Swathi, 2022)

4. Defense-In-Depth

A Defense-In-Depth strategy, also known as security-n-depth, is cybersecurity approach that uses multiple layers of protection to secure systems and data. This layered defense model helps to reduce vulnerabilities, stop from threat's spread, and lower the overall risk. In simple words, if an attacker was to break through one layer of the security layer, the next layer can stop the attacker or slowing them down. This approach provides more secure and steady protection by ensuring that no single point of failure in the system can compromise the entire system. (Coole, 2022)

5. Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) ensures that data transmitted over the internet is protected by providing a secure channel between two machines. It helps in both securing the data in transit and verifying the identity of the machine you communicate with. SSL was originally developed to protect web traffic, especially considering data exchanges between web browsers and

servers. A known example would be while you are using the internet for banking or shopping. When “https://” is noticed at beginning of the web address and a small padlock icon is in the browser’s address bar, it means SSL is being used to secure the connection. (Agashe, et al., 2022)

2. Background

2.1. Man-in-the-middle (MITM) attack

With the advancement of technology so has the Cyberthreats. Cybercriminals are constantly finding new ways to exploit vulnerabilities in networks, applications, and communication channels. This is because, as technology has advanced, attackers have become more sophisticated. Among these threats, a Man-in-the-Middle (MITM) attack poses a significant risk. A man-in-the-middle attack is a cryptographic attack conducted by a malicious third party, where they intercept a confidential communication channel between targeted users. In this attack, the attacker can control the traffic between the victims i.e., read, modify, intercept, or replace in real-time. Doing this sort of attack protocol, the attacker leaves no clues of their interpretation becoming one of the serious concerns. The attackers target the data flowing between the two endpoints, compromising the integrity and confidentiality of the data. (Bharat Bhusan, 2017).

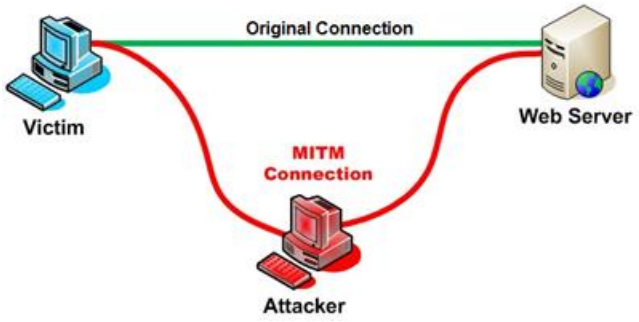

Figure 2. Man-in-the-middle demonstration. (Ming-Hsing Chiu, 2011)

To carry out a Man-in-the-Middle (MITM) attack, an attacker needs a way to communicate. The most common channels for this include GSM, UMTA, LTE, Bluetooth, Near Field Communication (NFC), Radio Frequency, and Wi-Fi (Mallik, 2018). In an MITM attack, two users become victims while a third person acts as the attacker. The attacker intercepts the communication between the two users and can change their messages. (Mauro Conti, 29 March, 2016). The MITM (Man-In-The-Middle) attack can be understood with the help of the Figure below.

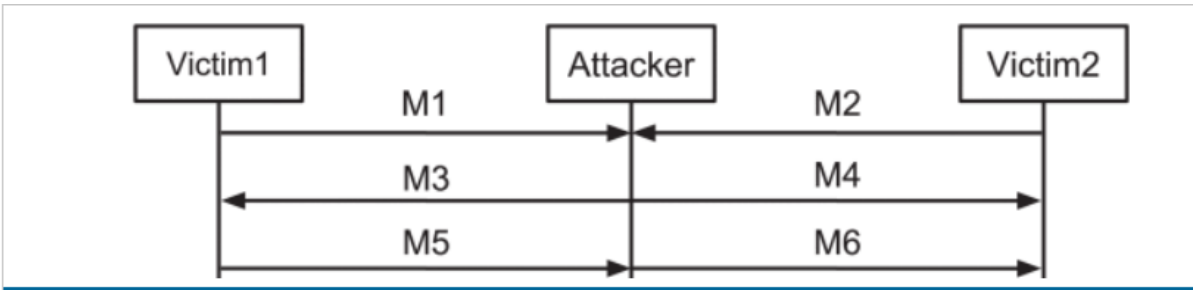

Figure 3. Message exchange in a typical MITM attack (M. Conti, 2016)

In this situation, two victims try to start a secure conversation by sharing their public keys, which are shown as messages M1 and M2. However, an attacker secretly intercepts these messages. Instead of letting the victims communicate directly, the attacker sends out its public key, labelled M3 and M4, to both victims. (M. Conti, 2016).

As the communication continues, Victim 1 is unaware of the attacker's presence. Here, the attacker encrypts a message using the attacker's public key and sends it to Victim 2, which is represented as message M5. At this point, the attacker intercepts M5 and can read it using a private key that it kept hidden. After reading the message, the attacker encrypts it again using Victim 2's public key and then sends this new message as M6. This example clearly shows how vulnerable communication can be when an attacker manipulates the exchange between two parties. (M. Conti, 2016).

2.2. History Of MITM

Leslie Lamport, an American computer scientist and mathematician, is known as the first individual to discuss "man-in-the-middle" (MITM) analysis in the context of communication security. In 1981, he published research titled "Password Authentication with Insecure Communication" in the journal "Communications of the ACM." However, evidence of his thoughts on this matter dates back to as early as 1979. (Sonia Rachel1, 2017).

Man-in-the-middle attacks have changed a lot over time, but they all follow a basic idea. An unauthorized person takes the advantage of a wired or wireless connection to intercept communication between two parties. While the idea of MITM attacks isn't new, attackers are always coming up with new methods to keep these attacks effective and relevant in our quickly evolving digital world. As people depend more on online communication, the tricks used in these attacks become more advanced. (Mallik, 2018).

2.3. ARP Protocol

Address Resolution Protocol (ARP) is a process used to connect a dynamic Internet Protocol (IP) address to a static physical machine address which is commonly known as the Media Access Control (MAC) address within a Local Area Network. It plays a crucial role in network communication as it enables devices to discover the MAC address associated with a given IP address. (Yongzhen Li, 2016).

ARP (Address Resolution Protocol) works at the data link layer of the OSI model, which organizes how networks communicate. When a device wants to send data, it first needs to find out the recipient's MAC (Media Access Control) address. To do this, the device sends out an ARP request across the Local Area Network (LAN), asking which device has a specific IP address. The device that owns that IP address then replies with an ARP response that includes its MAC address. (Ghazi Al Sukkar, 2016).

ARP requests are broadcast to all devices, while replies go directly to the requester. Devices maintain an ARP table to cache IP-to-MAC address mappings, reducing unnecessary requests. However, ARP lacks security measures, making it vulnerable to attacks. One common attack is ARP spoofing. In this method, an attacker sends fake ARP replies to trick a victim's device into linking the attacker's MAC address with the IP address of a legitimate network resource, like a default gateway or DNS server. Since ARP tables only keep the most recent response, the victim may mistakenly update its table to include the attacker's MAC address. This allows the attacker to perform a Man-in-the-Middle (MITM) attack, where they can intercept and possibly change sensitive data before it reaches its final destination. The attacker can also disrupt network access by dropping packets instead of sending them on, which stops the victim from connecting to important network resources. (Ghazi Al Sukkar, 2016).

2.4. Spoofing

In cybersecurity, spoofing is a deceptive practice where an attacker passes oneself as a trusted entity to gain unauthorized access, steal confidential information, or spread malware. In this tactic, the attacker exploits an individual and their system’s trust by falsifying data such as email addresses, IP addresses, or caller ID.

The concept of spoofing started back in the early days of computing and networking. As computer networks started to interconnect with each other, malicious actors began to discover methods to pose as reliable systems or users in order to exploit vulnerabilities. Early forms of

spoofing were relatively simple, mostly involving the manipulation of communication protocols to gain unauthorized access.

2.4.1. Types of Spoofing

2.4.1.1. IP Spoofing

One of the earliest and most common forms of spoofing is IP spoofing, which emerges as a major threat in the 1980s and 1990s. In April 1989, Steven M. Bellovin of AT&T Bell Labs mentioned in his article "Security Problems in the TCP/IP Protocol Suite" the risks associated with IP spoofing. Bellovin highlighted how Robert Tappan Morris, known for creating the infamous Internet Worm, exploited the Transmission Control Protocol (TCP) by predicting the sequence numbers and forging TCP packets. (Balaban, 2020)

The Internet Protocol (IP) serves as the fundamental protocol for data transmission across networks, encapsulating data into packets including headers with source and destination IP addresses. An Attacker uses IP spoofing to manipulate the source IP address in the packet header to appear as though the packet originates from trusted source. This deception can lead to several malicious activities, such as bypassing security measures, launching man-in-the-middle attack, or overflowing the targets with traffic in distributed denial-of-service (DDoS) attacks. (Balaban, 2020).

2.4.1.2. Email Spoofing

Then in the early 2000s email communication becoming so widely used, email spoofing emerged. Attackers started forging the sender's email address to make messages appear as if they were from a legitimate source. Email spoofing was commonly used by phishing attackers to deceive recipients into revealing confidential information or downloading malicious attachments. One of the known examples is the "ILOVEYOU" worm in 2000, which caused major global damage by spreading malware via email under the false subject line. (Pandove, et al., 2010)

In email communication, SMTP governs how messages are exchanged between servers. The email consists of several components such as the envelope, which contains the "MAIL FROM" and "RCPT TO" addresses and the header fields, which includes "From", "Reply-To" and "Sender". Attackers manipulate these fields, especially the "From" header, to mislead recipients about the emails source. Because SMTP does not automatically verify if the sending server is authorized to dispatch emails on behalf of specific domain. As a result, recipients may

receive emails that seem to be legitimate but are actually sent by malicious actors. (Pandove, et al., 2010)

2.4.1.3. Website Spoofing

As the internet and e-commerce grew in the early 2000s, website spoofing emerged as a serious threat. Cybercriminal created fake websites that resembled legitimate ones to fool users into entering private information like financial or login credentials. These fraudulent websites exploited user's trust by frequently using URLS that closely resembled legitimate websites. (Gandotra, 2020)

2.4.1.4. DNS Spoofing (Cache Poisoning)

The roots of DNS spoofing, also known as DNS cache poisoning, were found through the flaws in the DNS protocol's foundation design which was developed in the 1980s. The DNS protocol had not built–in security measures as it was primarily designed for functionality and scalability. Due to this oversight, it provided an opening for malicious activities. (Maksutov, et al., 2017)

Attackers insert malicious data in the DNS server's cache to exploit vulnerabilities in DNS software. As a result, users are redirected to a malicious website controlled by the attacker when they attempt to access a legitimate domain. This method may result in malware infection or unauthorized data collection. (Maksutov, et al., 2017)

2.4.1.5. Caller ID Spoofing

As telecommunication technologies advance, caller ID spoofing emerged where attackers manipulate caller ID information to display a trusted number. As users were being exploited with a trusted number, it increased the likelihood the recipient would answer and comply with malicious requests, such as making payments or giving out personal information. This malicious tactic raised concerns in aviation, maritime, and military operations, as it can lead to navigation errors and safety hazards. (Balaban, 2020)

Caller ID spoofing is a tactic used by attackers to exploit vulnerabilities in telephony protocols, specifically the Signalling System No. 7 (SS&) network used for call routing. The SS7 protocol was developed in the 1970s, designed with negligible security consideration, making it easy to manipulate. This technique is commonly used in social engineering attacks, phishing scams, frauds and harassment. (Balaban, 2020)

2.5. Eavesdropping

Eavesdropping can simply be defined as" listening in" on any network. It is an attack that involves unauthorized interception of private conversations with goals to gather sensitive information like login credentials, financial data, or propriety business details. This attack can be done dover wired, wireless, and digital network, exploiting vulnerabilities in communication devices or protocol.

Packet sniffing is one of the common methods of eavesdropping. This method allows the attacker to access a network, often by breaking into routers or using unsecured Wi-Fi. They record capture and analyse network traffic by using tools like Wireshark or tcpdump, extracting unencrypted data such as usernames and passwords. This attack is frequently used in Man-in-the-Middle (MITM) attacks, in which the attacker secretly relays or modifies communications between 2 ends.

Another technique used in eavesdropping is wiretapping, which involves physically tapping into communication lines to monitor voice or data transmissions. This can be accomplished on digital networks by hacking network cables or on analog lines, like telephones. Attackers can intercept and decode signals in digital environments using advanced hardware or software.

Attackers can use radio frequency (RF) eavesdropping to exploit electromagnetic waves from wireless networks, mobile devices, or RFID tags. As attackers capture unencrypted signals using RF monitoring tools, it makes wireless communication unsafe and vulnerable. Another method of eavesdropping is keylogging, in which hardware or software records every keystroke on a target device, giving hackers access to sensitive information like passwords and financial details. Malicious downloads, phishing emails, or physical access can all introduce these keyloggers. This method is especially effective in poorly secured web applications, allowing attackers to impersonate legitimate users.

Attacks such as Side-channel exploit the physical properties such as its power consumption, electromagnetic emissions, or acoustic signals to extract sensitive data. To recover encrypted keys, these attacks frequently target cryptographic systems. In order to bypass cryptographic safeguards, attackers can also use tools to observe and analyse side-channel emissions.

2.5.1. Types of eavesdropping Attacks

Eavesdropping attacks can be classified as passive or active

2.5.1.1. Passive eavesdropping:

This type of eavesdropping involves silently listening to or monitoring communication channels without altering the transmitted data. Attackers without being detected obtain information like financial data, login credentials, or confidential business communications. This technique is commonly used in network traffic analysis, where unencrypted packets are sniffed using programs like Wireshark or tcpdumb. It works efficiently when communications are not encrypted, which makes detection difficult.

2.5.1.2. Active eavesdropping:

This type of eavesdropping involves attackers who engage in active eavesdropping intercepting and altering data while it is being transmitted, frequently by impersonating one or more parties involved in communication. This method is frequently used in Man-in-the –Middle (MITM) attacks, in which attackers inject malicious content or alter messages. For example, attackers can read transmitted data by downgrading secure connections to insecure ones in HTTPS stripping attacks. Active eavesdropping can jeopardize data integrity and disrupt communications.

2.6. Penetration testing execution standard

There are seven major sections in the penetration testing execution standard. These cover every aspect of penetration testing. These cover every aspect of a penetration test, from the initial communication and reasoning behind a pen test, the intelligence gathering and threat modelling phases, where testers work behind the scenes to get better understanding of tested organization, vulnerability research, exploitation, and post exploitation, where the testers technical security expertise combines with the understanding of the engagement, and finally to the reporting, which summarizes the entire process, in an way that makes it easy for the customers to understand and provides the most value to it. (PTES, 2014).

2.6.1. Pre-engagement Interaction

The pre-engagement phase is the initial stage of a penetration test where all planning and agreements are made before any testing begins. During this phase, the goals of the test are discussed, the systems to be tested are identified, and the rules of engagement are defined.

For instance, in a Man-in-the-Middle (MITM) attack demonstration, it must be agreed that the test will be conducted only within a controlled environment such as intercepting traffic between two virtual machines ensuring that no real users or sensitive data are involved. This ensures that the penetration test is authorized, conducted safely.

According to the PTES standard, this phase involves planning, defining the scope, and preparing the tools and techniques before the testing begins. For this demonstration, a virtual lab environment was set up using Oracle Virtual Box. Three virtual machines were created: Kali Linux, Windows 7, and Metasploitable 2. The Kali Linux VM was used as the attacking machine whilst Windows 7 and Metasploitable 2 served as the targets. All the machines were connected through a NAT network, which simulated a local area network, allowing communication between the systems. This approach ensured that the testing was carried out in a safe and isolated virtual environment without affecting any live system.

2.6.1.1. Oracle VirtualBox

Oracle VM VirtualBox is a tool that lets you run different operating systems on one computer. You can create virtual machines (VMs) to use multiple systems at the same time. It supports Windows, Linux, macOS, and Oracle Solaris. VirtualBox extends a host operating system's capability without requiring additional hardware modifications. The host OS runs the VirtualBox, which allows the guest OS instances to run as virtual machines. You can deploy as many virtual machines as your host system's resources can support. (Astari, 2025).

VirtualBox is widely used in cybersecurity research and testing due to its ability to create isolated environments for controlled experiments. For example, In our case, we used VirtualBox to set up a Man-in-the-middle (MITM attack) as part of our project. We installed Kali Linux on one VM as the attacking machine and the Windows 7 VM as the target machine. Using Ettercap within Kali Linux, we performed ARP poisoning to intercept and manipulate the network traffic between the Windows 7 machine and the network. This allowed us to analyse and modify the data packets in transit, demonstrating how attackers exploit network vulnerabilities while maintaining a safe and controlled testing environment.

This approach not only helped us understand MITM attacks but also supported how VirtualBox enables cybersecurity professionals to test, learn, and experiment without compromising real systems.

2.6.1.2. Metasploitable 2

Metasploitable 2 is a deliberately vulnerable Linux virtual machine designed for security testing and ethical hacking practices. It provides a safe environment for learning penetration testing, exploiting vulnerabilities as well as analysis. It allows users to practice scanning vulnerabilities using tools like Nmap to identify misconfigurations and later exploit them using the Metasploit framework. (Mandeep Singh, 2020).

2.6.1.3. NAT network

NAT is a network function that operates at the network layer of the OSI model which is implemented on routers or firewalls to modify IP address information in packet headers as traffic passes between different networks. It works by translating private IP addresses used in a local network into a public address used on the internet and vice versa. This allows multiple devices on a private network to share a single public IP address while maintaining secure communication, often used for IP address conservation and network security. (Zhang, 2008).

2.6.2. Intelligence gathering

This section outlines the Intelligence Gathering procedure of a penetration testing. This document's main objective is to offer a standard created especially for the Pene testers performing reconnaissance against a target, usually a business, military, or similar organization. The document details the thought process and goals of pen testing reconnaissance and when used appropriately, the document assists the reader in creating a highly strategic attack plan by highlighting the objectives and thought process of pen testing reconnaissance.

This phase, as defined by the PTES focuses on collecting information about the target systems to guide further actions. In this case, Nmap was used from the Kali Linux machine to scan the network and discover active devices. Once the active hosts were identified then further scans were performed using namp -sS and nmap -A to determine which ports and services were available. Through this process IP addresses, MAC addresses and open services like Telnet and HTTP were identified forming the foundation for the later attack stages.

2.6.2.1. Nmap

Nmap is an open-source tool that is used in network mapping or finding devices on a network, checking which ports are open, and analysing security weaknesses. It helps administrators gather information about systems, such as open ports, OS details, and potential vulnerabilities, and works by sending specially crafted packets to a target system and analysing the responses to determine the status of ports and services. It uses a scanning technique called SYN scanning,

where it sends SYN packets to the target system to detect open ports. If the port is open, the target responds with a SYN/ACK. This allows the Nmap to identify the open port without completing the full TCP handshake. (HANGE, 2023).

2.6.3. Threat modelling

According to this section, a threat modelling approach is necessary for a penetration test to be carried out correctly. Instead of using a particular model, the standard calls for the model to be consistent in how threats are represented, their capabilities, their qualifications according to the organization being tested, and their ability to be applied repeatedly to subsequent tests with the same outcomes.

Assets and the attacker (threat community/agent) are the two main components of traditional threat modelling that are the focus of this standard. Each is separated into the threat communities and their capabilities, as well as business assets and business processes. Every penetration test should, at the very least, explicitly identify and document each of the four components.

As per the PTES standard, threat modelling helps identify and define the potential attack paths based on the gathered intelligence in step 2. During this phase, the data collected through Nmap was reviewed to identify the possible attack paths. From the scan results, it was clear that services like Telnet and HTTP were running without encryption. These were marked as potential targets. Wireshark was briefly used to monitor traffic and confirm that credentials and other data were being sent in plain text. This helped to confirm that MITM could be carried out effectively. The attacker was modelled as an internal user and the threat scenario was planned accordingly

Nmap- used to analyse open ports and identify insecure services

Wireshark – used to confirm unencrypted traffic was present on the network

2.6.3.1. Wireshark

Wireshark is a network analysis tool that captures and analyses data packets in real time by providing a detailed insight into network traffic. It helps to detect issues like malicious connections, network abuse, and performance problems. (Soepeno, 2023). In threat modeling, Wireshark is used to observe network traffic, identify vulnerabilities, and track attack patterns, aiding in the identification and mitigation of security risks not only this but it also supports network security by identifying threats, ensuring comprehensive traffic visibility, and helps

optimize data transmission by pinpointing bottlenecks and problematic packets. (Ndatinya, 2015).

2.6.4. Vulnerability Analysis

Finding weaknesses in applications and systems that an attacker could exploit is known as vulnerability analysis phase. These defects may include insecure application design or incorrect host and service configuration. While there are some fundamental principles that apply to the process, the method used to search for defects varies and is heavily dependent on the specific component being tested.

As per PTES, vulnerability testing is the process of identifying flaws that an attacker could exploit. Although automated vulnerability scanners were not used, possible weaknesses were identified manually through Nmap scans. Services like Telnet and HTTP which are known for lacking encryption were confirmed to be active. Metasploitable 2 a purposely vulnerable machine was used to simulate real-world misconfigurations. These findings made it clear that the systems were open to basic network-level attacks like ARP spoofing and credential interception.

Nmap - used to identify running services and confirm unprotected protocols

Metasploitable 2 - served as the target with intentionally weak configurations

2.6.5. Exploitation

The goal of a penetration test's exploitation phase is to gain access to a system or resource by evading security measures. This phase should be carefully planned and a precision strike if the vulnerability analysis phase was completed correctly. Finding the primary point of entry into the company and locating high-value target assets are the primary goals.

The exploitation phase involves taking advantage of the discovered vulnerabilities to gain unauthorized access as per the PTES standard. Once the vulnerable services were confirmed, Ettercap was used to launch an ARP spoofing attack from Kali Linux. This allowed attacker to sit in between the victim and the gateway. While the spoofing was active, Wireshark was used to capture and analyse the network traffic. Unencrypted login credentials from Telnet and HTTP sessions were intercepted, demonstrating the risk of using outdated protocols.

2.6.5.1. Kali Linux

Kali Linux is a powerful operating system based on Debian, designed for cybersecurity professionals and enthusiasts. It is an open-source platform that includes many tools for tasks

like penetration testing, ethical hacking, security research, digital forensics, and reverse engineering. It provides a versatile and highly customizable environment that helps users conduct vulnerabilities and strengthen defences across different platforms. Whether you're a beginner exploring cybersecurity or an expert conducting in-depth assessments, it provides a flexible and well documented environment to support your work. (Manasvi Sonke, 2024).

2.6.5.2. Ettercap

Ettercap is a network security tool used for packet sniffing, Man-in-the-middle (MITM) attacks, and network protocol analysis. It enables users to intercept and manipulate network traffic in real time by enabling activities like capturing data packets, extracting passwords, and modifying connections. In an MITM attack using Ettercap, the tool is exploited to intercept and modify network traffic between two devices by performing a technique called ARP poisoning. This method redirects traffic through the attacker's system, allowing them to sniff, manipulate, and inject data into the conversation. (Mohammad Daud, 2025).

2.6.6. Post exploitation

After the credentials had been successfully captured, they were used to access the victims' system using Telnet from the Kalis terminal. This proved that unauthorized access could be obtained as result of the MITM attack. This access granted the attacker full control over the victims' machine showing the severe consequences of insecure network configurations.

2.6.7. Reporting

Lastly, the final phase as recommended by PTES, involves documenting all steps, findings and recommendations in clear and structured manner. Screenshots, command outputs and analysis results were compiled into detailed report. Based on the findings recommendations and mitigation strategies were made. The report was written to explain and offer solutions in a way that could be understood by both technical and non-technical readers.

3. Demonstration

3.3. Methodology

The methodology of this attack for this report will align steps with the Penetration Testing Execution Standard (PTES) framework. The attack will be conducted step by step according to the Penetration Testing Execution Standard (PTES). Before the attack was conducted all the virtual machines were kept in local network using NAT network which also has access to the internet. The Ip address of the virtual machines are 10.0.2.4, 10.0.2.6, 10.0.2.15 and the default gateway for this network is 10.0.2.1.

Kali Linux is the machine that will be used as the attacker machine to launch the Man-in-the-middle attack. Different tools in the kali Linux distribution and techniques will be used to conduct this attack. The ip of this attacker machine is 10.0.2.4 and its MAC address is 0800279D1AF5. The tool used for intelligence gathering will be Nmap which will be used to gather information like host's ip address and ports that open. Other tools like Wireshark will be used to analyse intercepted traffic. And Ettercap will be used to do the ARP poisoning.

After a successful man in the middle connection is set up all the packets are analysed then useful packets are saved in order to be used later. The packets are analysed and are used for post exploitation like stealing credentials or gaining unauthorized access.

3.4. Performing the Man-in-the-middle attack

The attack will be done by keeping the Penetration Testing Execution Standard framework (PTES) in mind, so this includes the tools, techniques and procedures followed will be in alignment with PTES. The attack involves network reconnaissance, exploitation through ARP poisoning, packet capture for analysis, and further exploitation. The attack is designed to demonstrate how attackers perform man-in-the-middle attack in real life.

3.4.1. Pre-Engagement Interactions

In the pre-engagement interaction the target devices, network segment is declared, and the scope of test is also set. Ethical and legal considerations are also identified in this step of the PTES framework. As for ethical and legal consideration, the scope discussed with the employer is taken as the exploitable area and anything done beyond this scope will be unethical and the employer can take legal actions against the pen tester.

3.4.1.1. Terms of Reference

Terms of Reference

1. Assignment Information

Assignment title	Investigation and Demonstration of Man-in-the-Middle (MITM) Attacks
Attack type	Man in the middle
Duration	30 Days
Client	Harmony Industry Pvt. Ltd
Pen testers	Bhumika Dahal, Rohan Shrestha, Sujita Sherpa

2. Background

2.1. Introduction

Between April 1- April 30, 2025, a team of cybersecurity students conducted a controlled simulation of Man-in-the Middle (MITM) attack within a secure environment using Kali Linux and other ethical hacking tools. This report includes the methodologies that was used to perform Man-in-the-middle attack. This report also documents the analysis and mitigation techniques.

2.2. Scope

- Network traffic interception and analysis
- Tool-based demonstrations
- Virtual machine environment setup (Kali Linux, Metasploitable 2, Windows 7)

2.3. Purpose

The purpose of this project is to explore how Man-in-the-middle (MITM) attack works, its impacts, and prevention strategies of Man-in-the-Middle (MITM) attacks, including spoofing and eavesdropping techniques. By conducting these attacks in a controlled environment, the project's main goal is to help people understand these cyberattacks better by simulating these attacks in a controlled environment.

2.4. Timeline

- **Day 1–5** : Research and background writing
- **Week 3–4**: Virtual environment setup

- **Week 5**: Attack demonstration
- **Week 6**: Analysis and post-exploitation
- **Week 7**: Finalize report and references

3. Methodology

3.1. Approach

The project followed a standard approach based on the Penetration Testing Execution Standard (PTES). The methodology includes setting up virtual lab, selecting appropriate tools, conducting MITM attacks, capturing and analyzing data, and reporting the results.

3.2. Steps taken

- **Setup:** Created a virtual lab using Oracle VirtualBox with the help Kali Linux (attacker), Windows 7, and Metasploitable 2 (victims).
- **Reconnaissance:** Scanned the network and identified active hosts and open ports with the help of Nmap to scan the network and
- **Attack:** Intercept traffic between victims and gateway to execute ARP spoofing.
- **Analysis:** Extracted sensitive data, captured and analysed network packets using Wireshark.
- **Mitigation:** Explored security practices such as encryption and static ARP entries to defend against MITM

3.3. Resources Required

- Oracle VirtualBox
- Kali Linux ISO
- Metasploitable 2 VM
- Windows 7 VM
- Tools: Nmap, Wireshark, Ettercap

4. Expected output and deliverables

- Detection of network vulnerabilities
- Mitigation of network vulnerabilities

- Detailed report underlining methodologies, tools used, outcomes, and findings.
- Detailed reporting of results and mitigation steps.

5. Intellectual property

All content produced, including code, configurations, screenshots, and documentation, will be the original work of the project group. Any third-party tools or resources used will be properly credited and referenced.

6. Criteria for Evaluation of Level of Technical Compliance of Individual Contract

- Active participation in research, setup, and implementation phases
- Contribution to report writing and presentation
- Demonstrated understanding of the tools, techniques, and theory through verbal or written explanation

3.4.2. Intelligence Gathering

In this phase information is gathered about the target system. For man-in-the-middle attack a network reconnaissance is done firstly. Nmap is used in order to scan the network and identify the hosts that are active, and their IP/MAC address is collected to use for further analysis. The targets gateway is also identified, and the victim machine is also selected in this phase. The following steps were taken in order to complete the Intelligence Gathering phase:

Step 1: A ping scan is done in order to find out all the hosts that are active in the network.

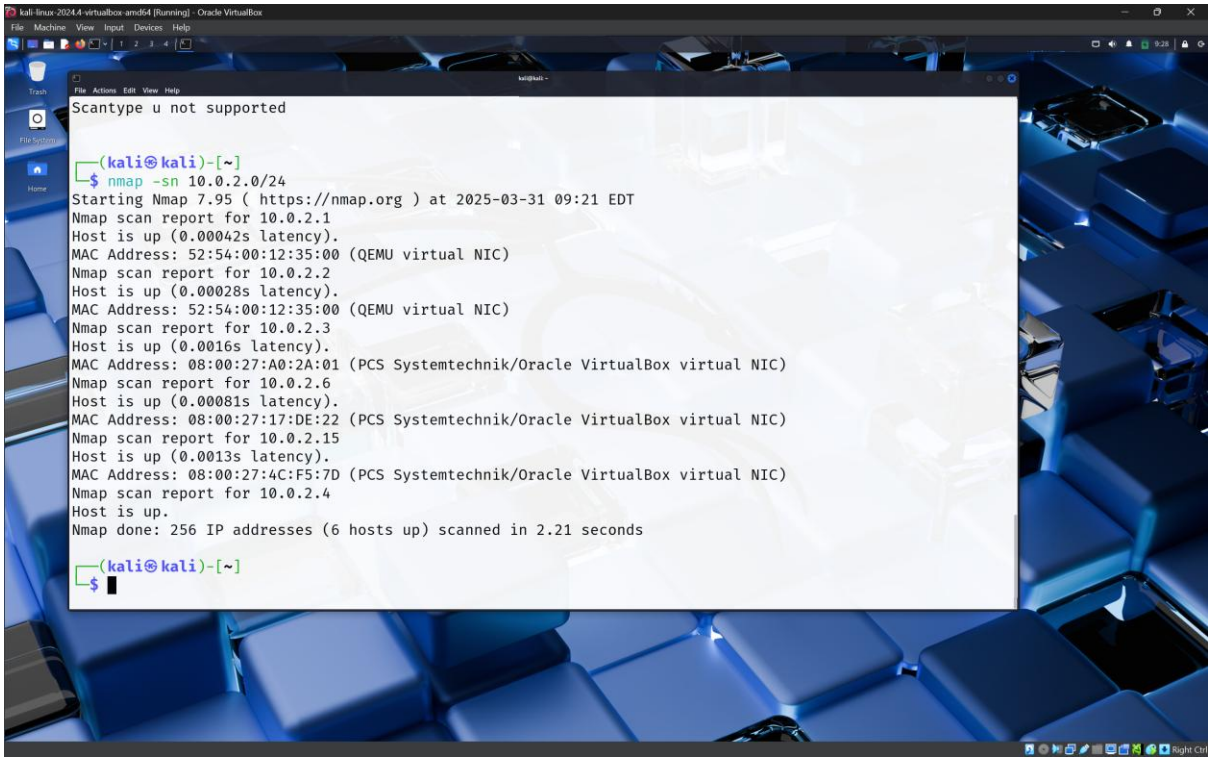

Figure 4: Screenshot of using Nmap to conduct a ping scan.

Step 2: Default gateway is found by observing where the traffic form Kali Linux is being directed to.

Figure 5: Screenshot of finding out the default gateway.

Step 3: Further scan is also done using Nmap to find possible victim/s.

Figure 6: Screenshot of Nmap scan for 10.0.2.1.

Figure 7: Screenshot of Nmap scan for 10.0.2.2.

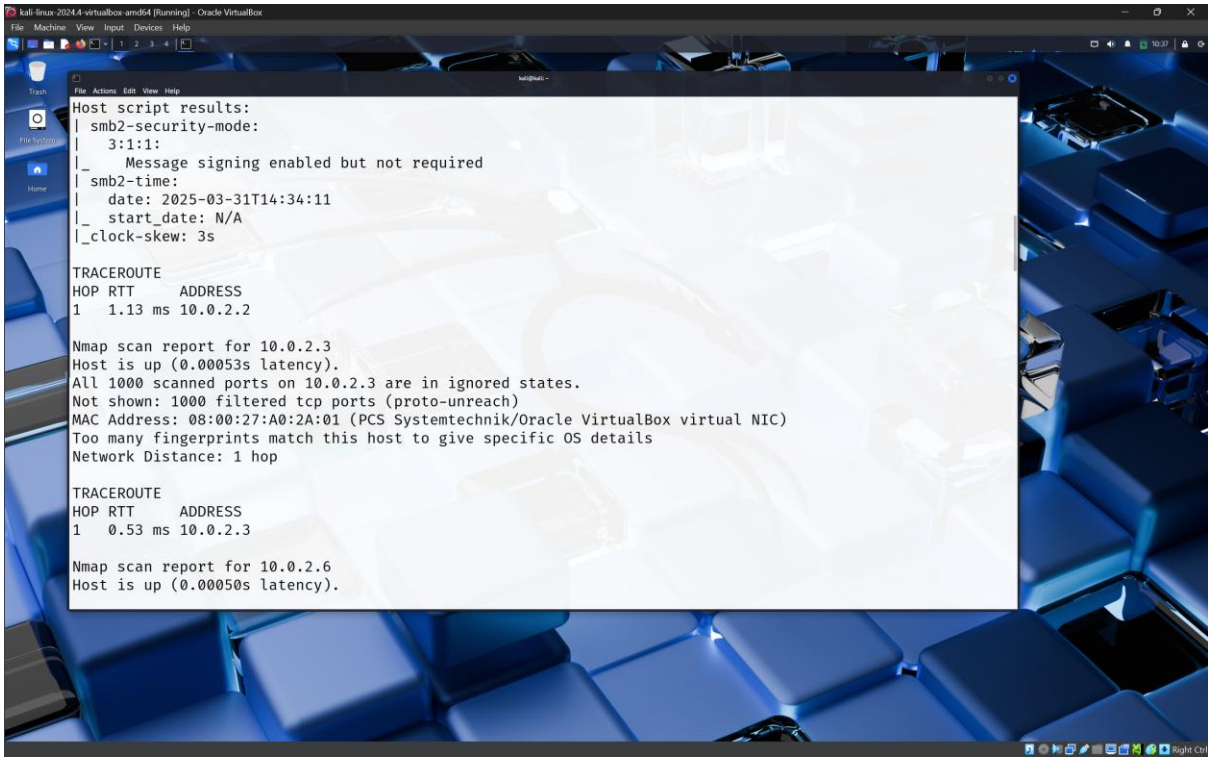

Figure 8: Screenshot of Nmap scan for 10.0.2.3.

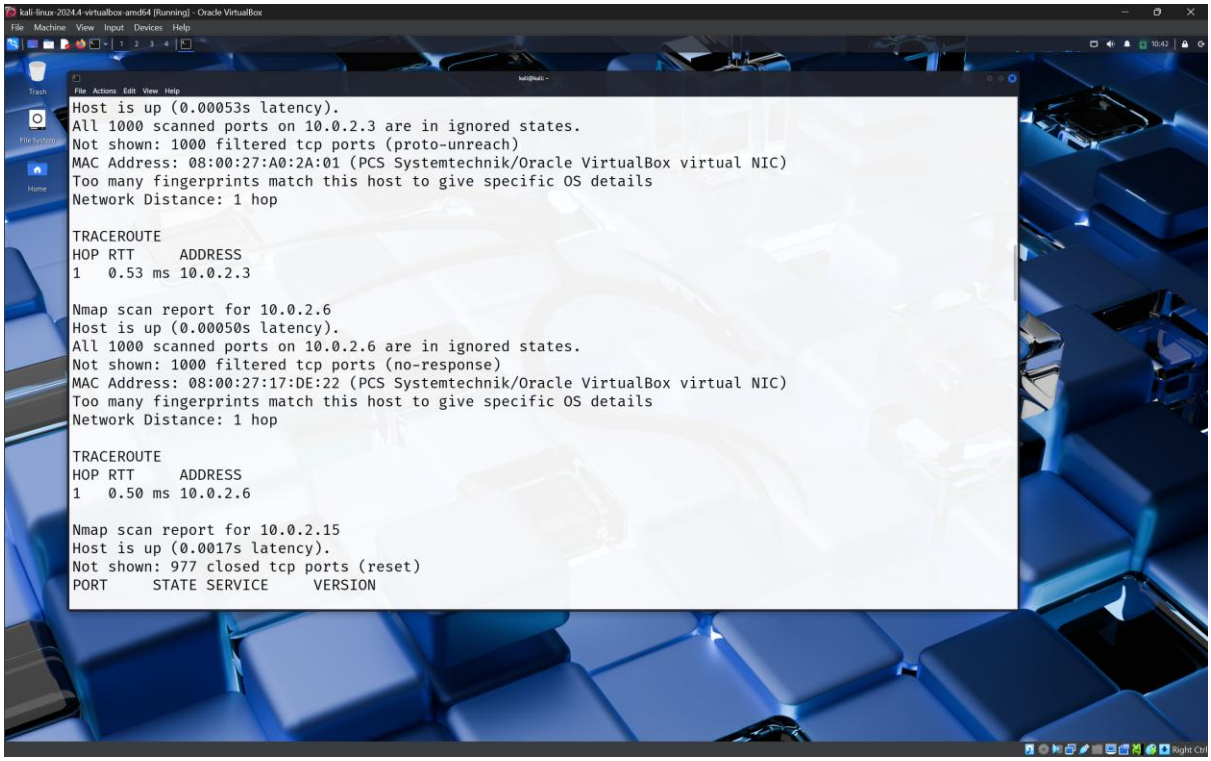

Figure 9: Screenshot of Nmap scan for 10.0.2.6.

Figure 10: Screenshot of Nmap scan for 10.0.2.15.

Figure 11: Screenshot of Nmap scan for 10.0.2.15.

Figure 12: Screenshot of Nmap scan for 10.0.2.15.

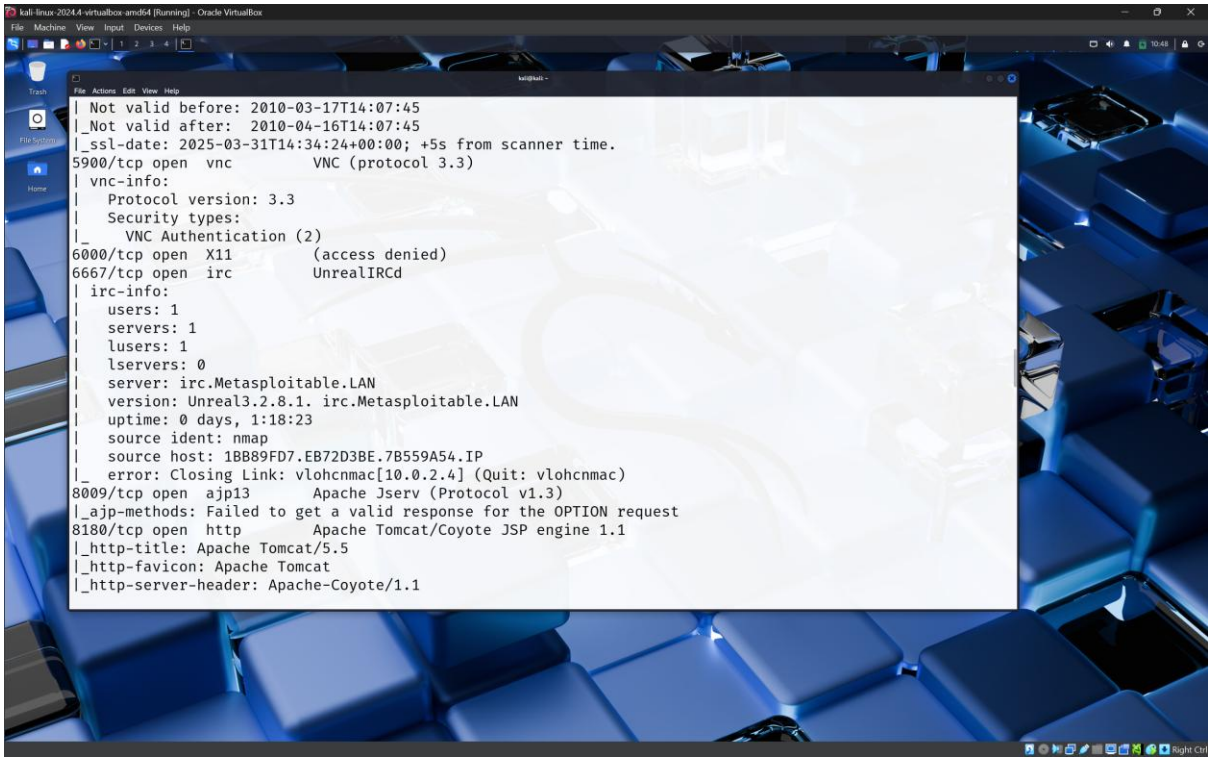

Figure 13: Screenshot of Nmap scan for 10.0.2.15.

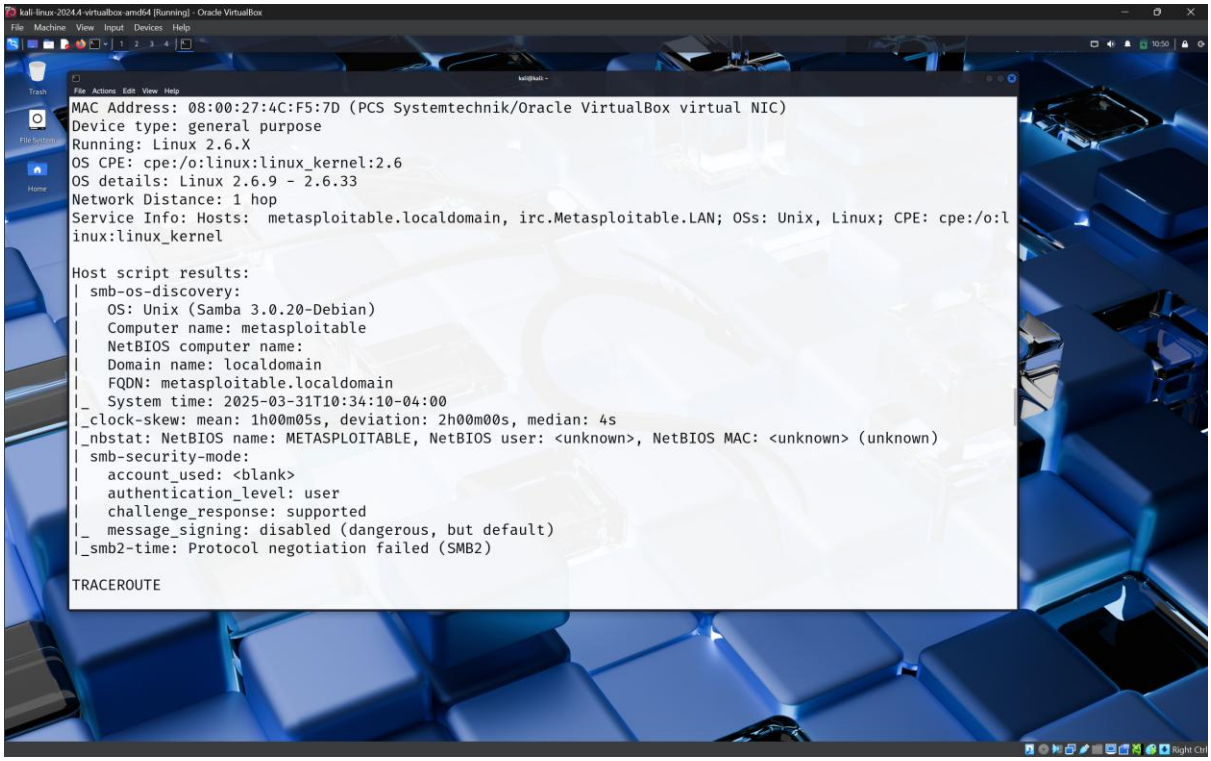

Figure 14: Screenshot of Nmap scan for 10.0.2.15.

Figure 15: Screenshot of Nmap scan for 10.0.2.4.

Step 4: The Ip 10.0.2.15 and 10.0.2.6 were selected as targets after the intelligence gathering.

3.4.3. Threat Modeling

In this step of the PTES framework vulnerabilities are assessed which are identified with the help of intelligence gathering step. Security gaps, potential risks, attack vectors are identified and the impacts they might have is also identified. The network is checked if it has ARP spoofing protection enabled, either unencrypted communication channels are used, if the network has weak segmentation and if ARP monitoring tools are used or not.

3.4.4. Exploitation

In this phase all the information gathered and analysed is used to perform the ARP poisoning attack, intercept network traffic and analyse the intercepted traffic. The intercepted network traffic can even be potentially manipulated. The three crucial pieces of information that we need in order to conduct the ARP poisoning are known because of the intelligence gathering step which are the target Ip address and the default gateway. Ettercap is used to launch the ARP poisoning with targets Ip and default gateway. To capture the packets and analyse them Wireshark is used with eth0 as the network interface as the packets pass through our interface while travelling from the target to default gateway. The steps taken to complete this phase of the attack are as follows:

Step 1: Ettercap is launched in text only mode without SSL on interface eth0 with mode arp:remote on the default gateway Ip and first target machines Ip.

Figure 16: Screenshot of ARP poisoning.

Figure 17: Screenshot of ARP poisoning.

Figure 18: Screenshot of ARP poisoning.

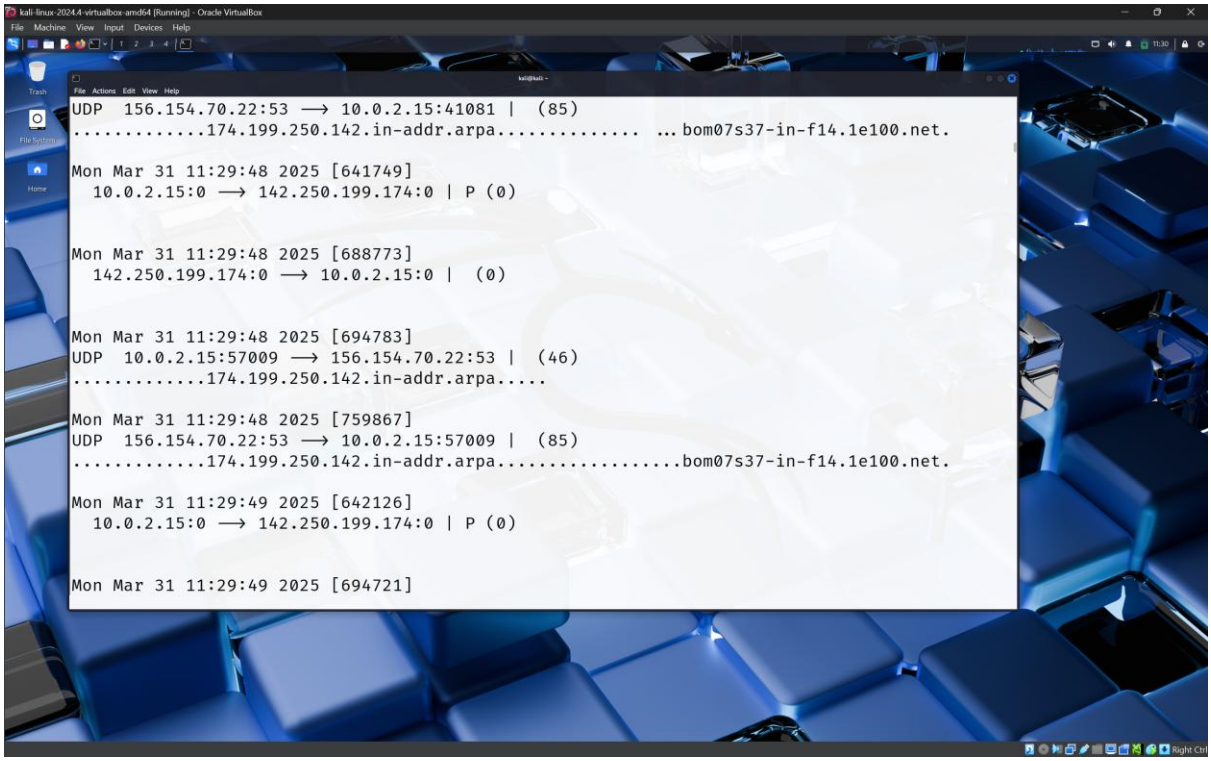

Figure 19: Screenshot of packets with source ip and destination ip.

Figure 20: Screenshot of packets with source Ip and destination Ip.

Step 2: Ettercap is launched in text only mode without SSL on interface eth0 with mode arp:remote on the default gateway Ip and second target machines Ip.

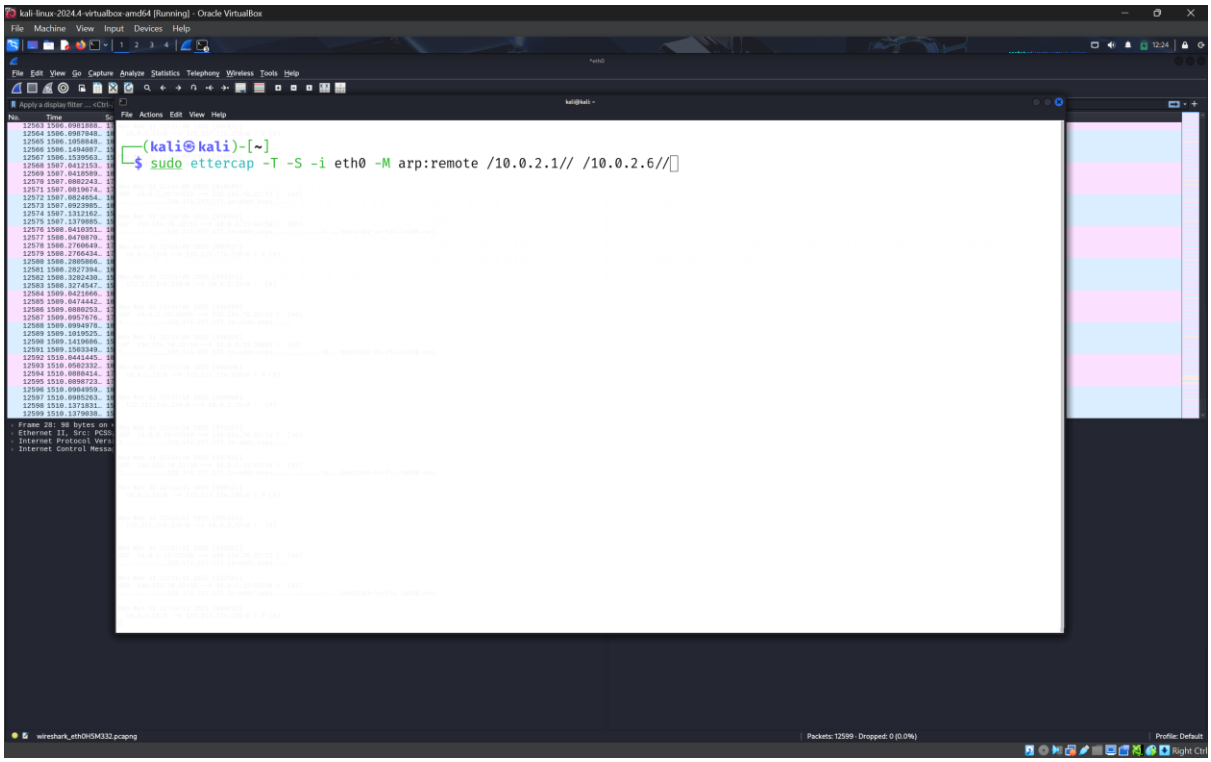

Figure 21: Screenshot of ARP poisoning.

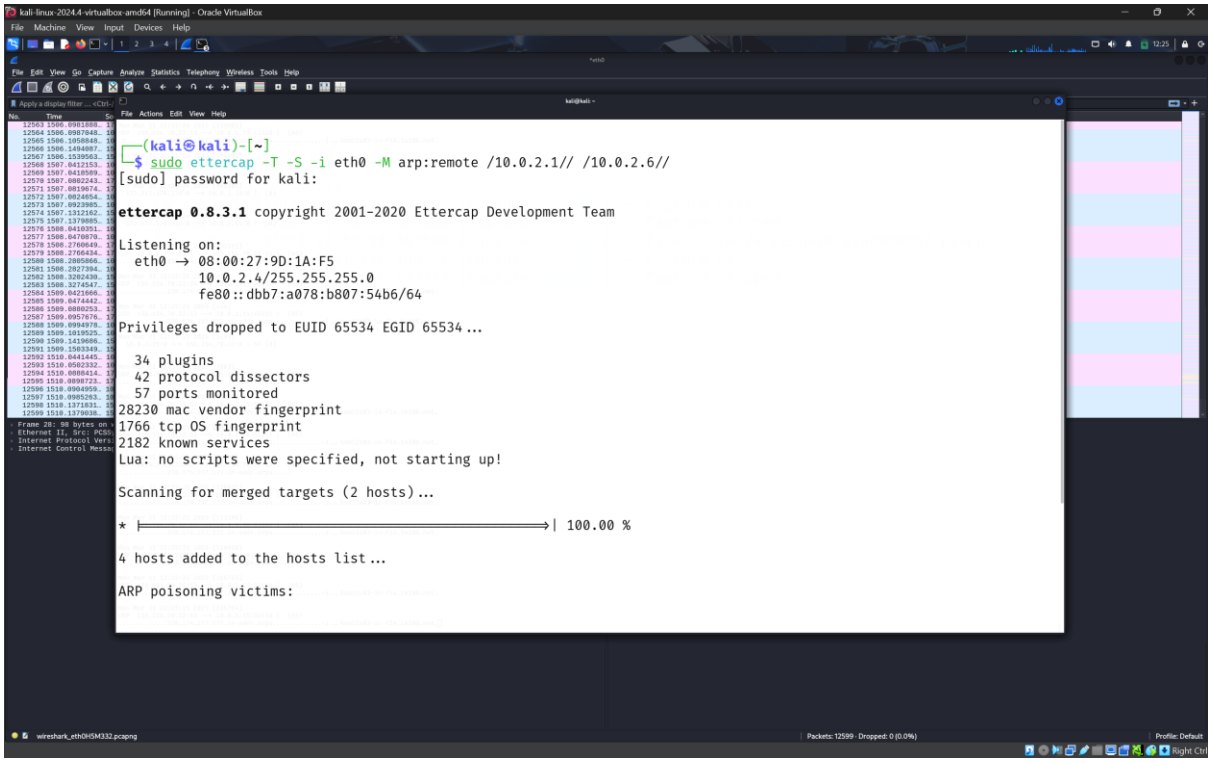

Figure 22: Screenshot of ARP poisoning.

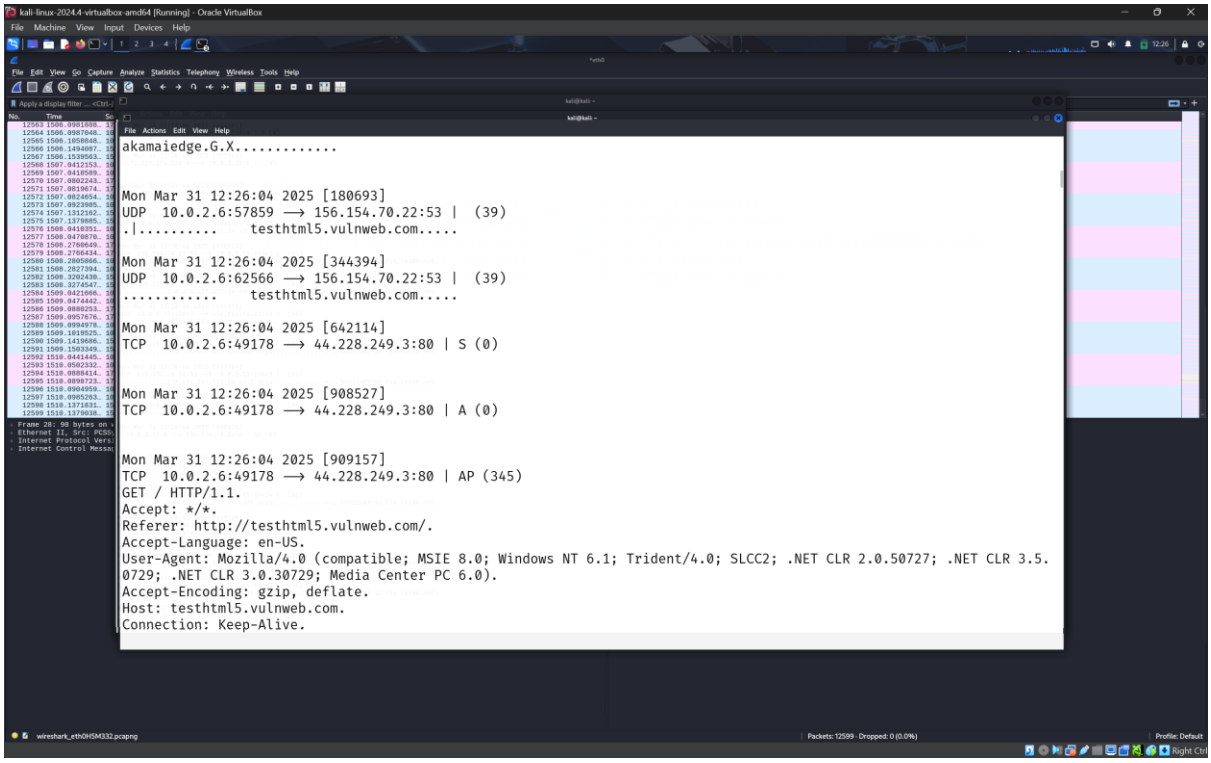

Figure 23: Screenshot of packet flow with source Ip and destination Ip.

Step 3: Wireshark is opened to capture and analyse packets that pass through eth0. The packets now travel through the Kali Linux's interface eth0 making it the man in the middle.

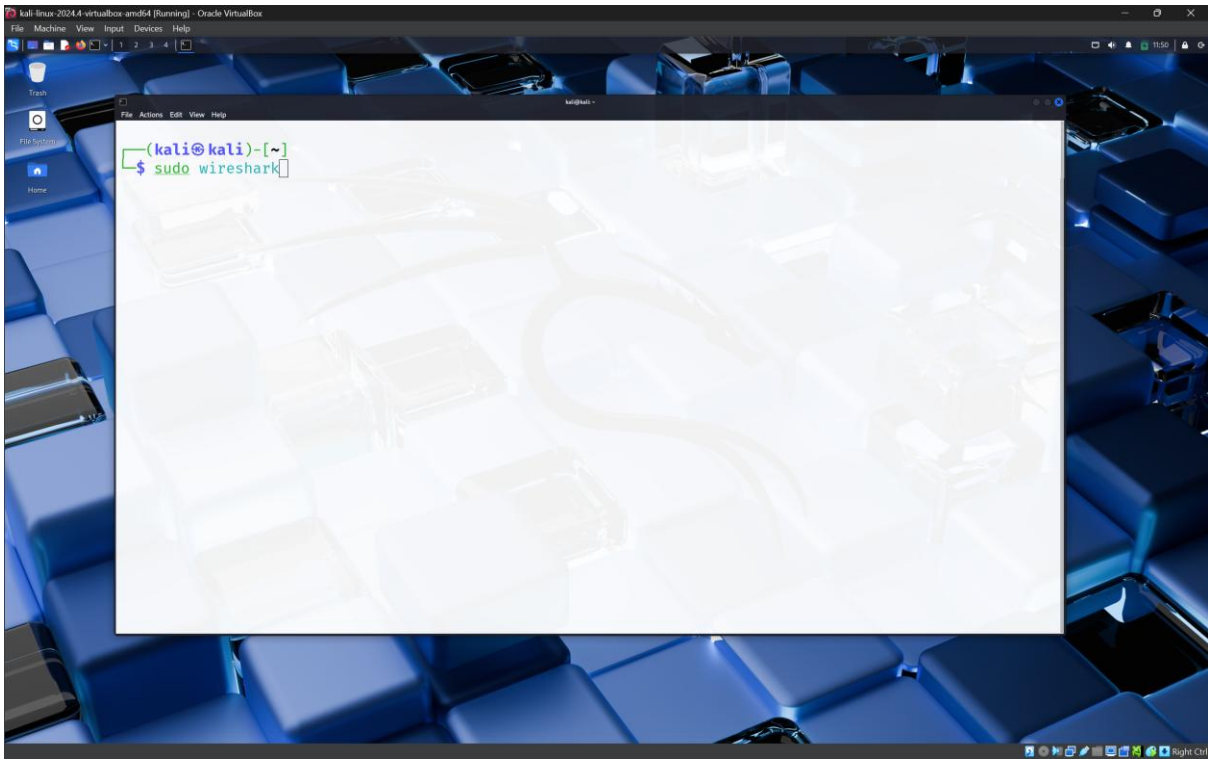

Figure 24: Screenshot of opening Wireshark.

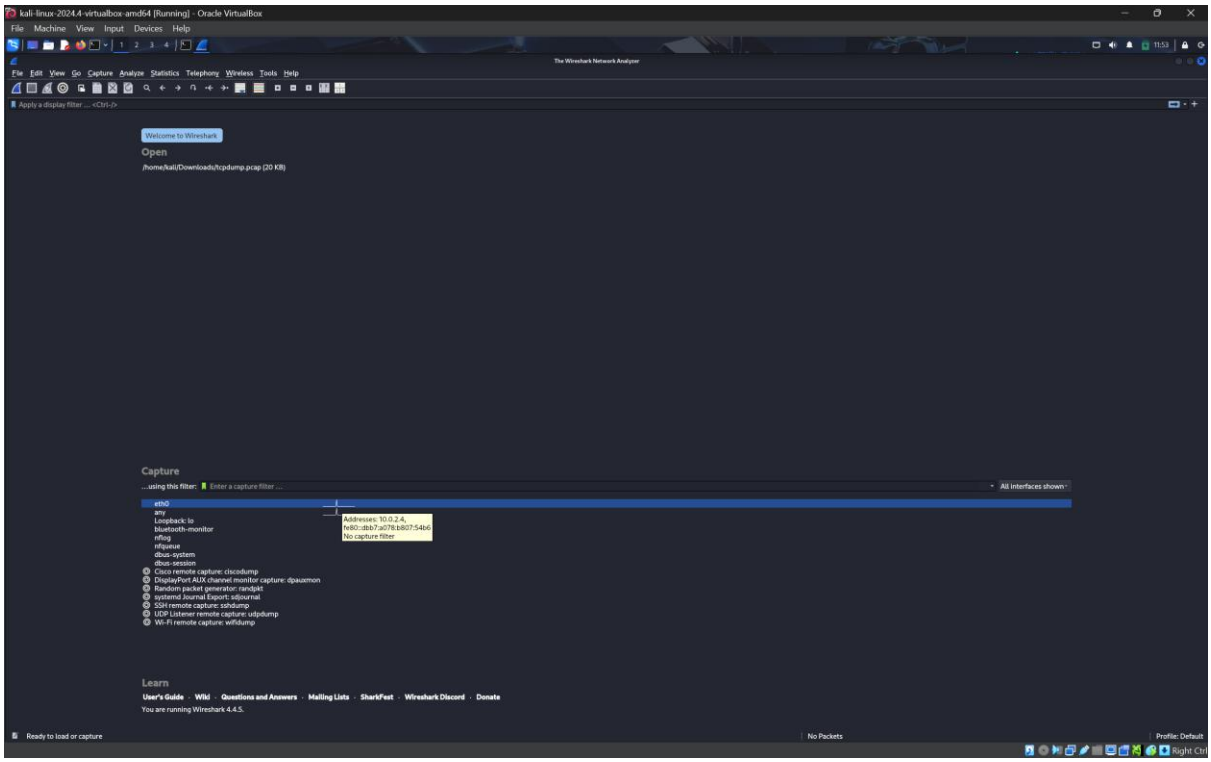

Figure 25: Screenshot of selecting eth0 in Wireshark.

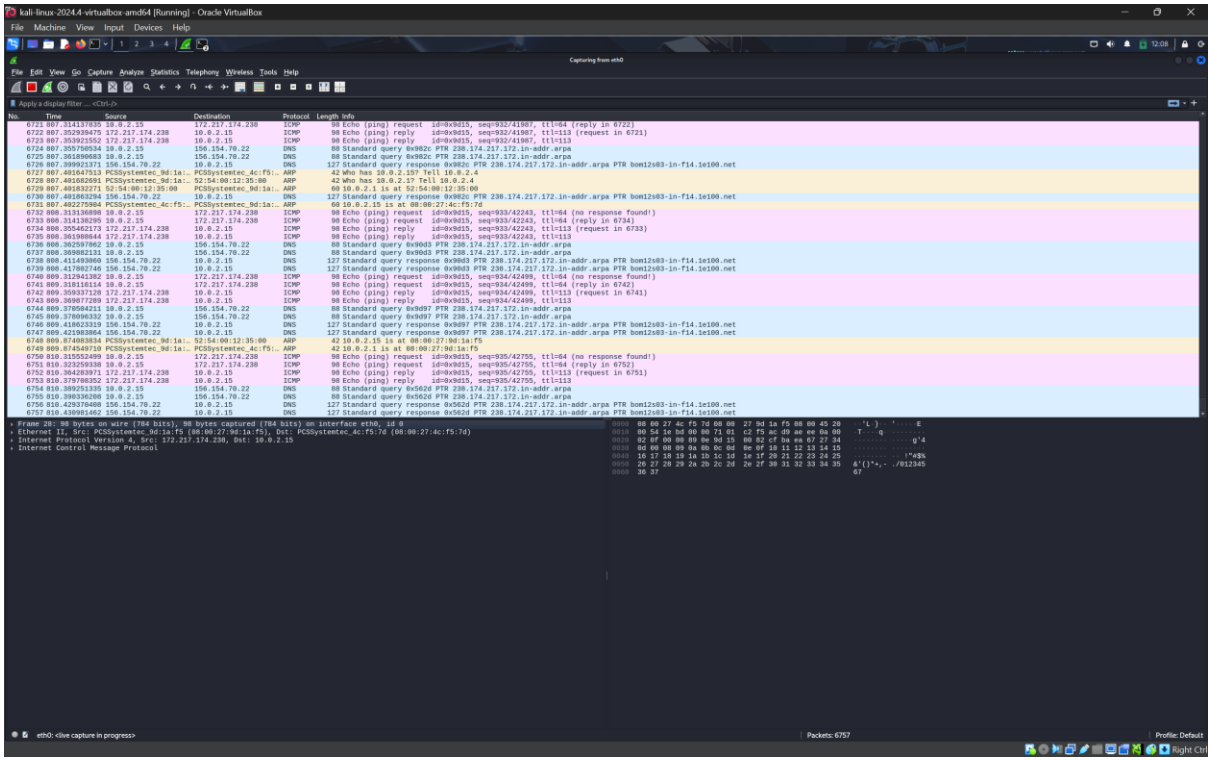

Figure 26: Screenshot of Wireshark capturing packets.

Step 4: A filter is applied to the filter tab so that packets from the first target to and from the default gateway are only seen.

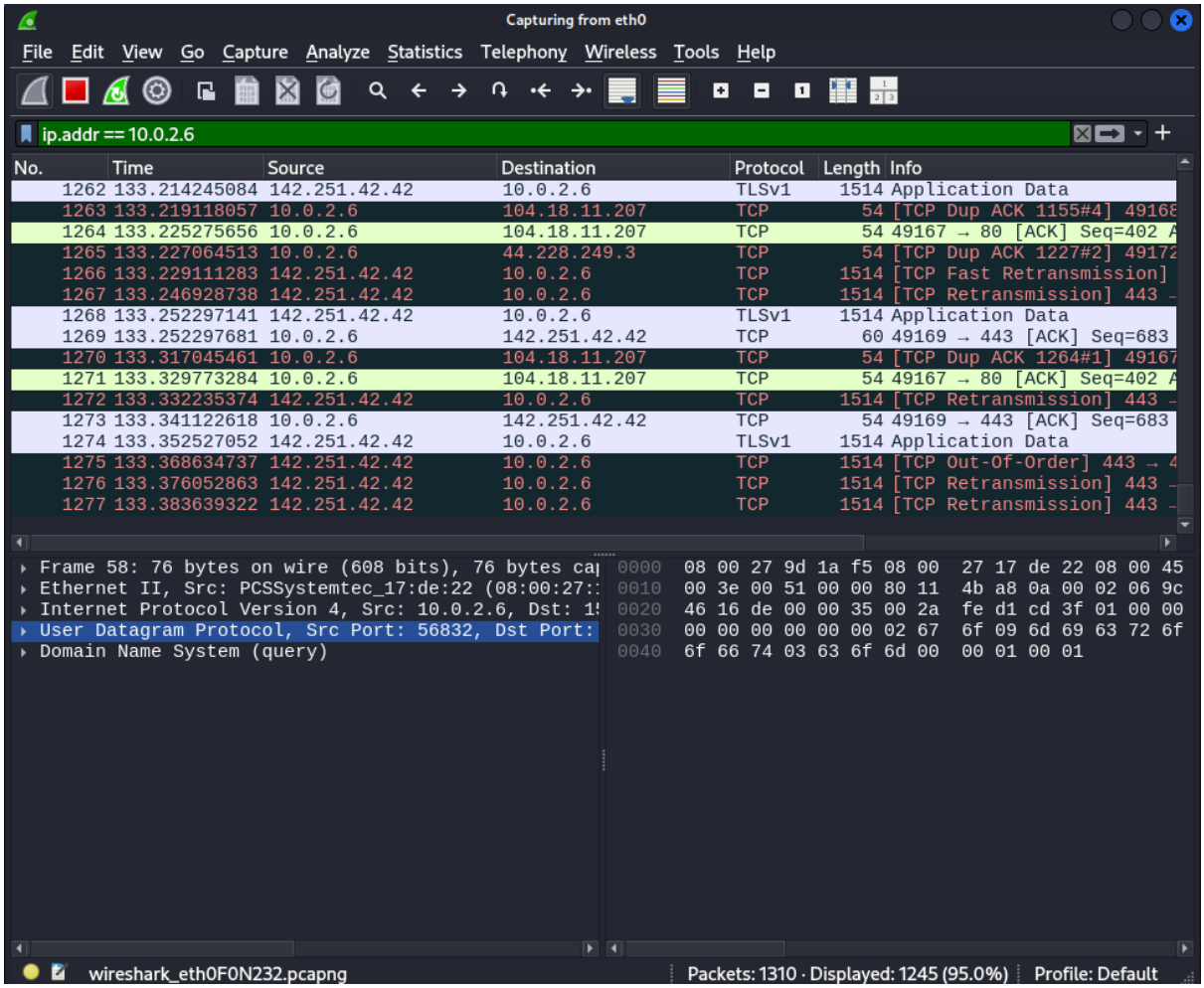

Figure 27: Screenshot of analysing packets from 10.0.2.6.

Step 5: A filter is applied to the filter tab so that packets from the second target to and from the default gateway are only seen.

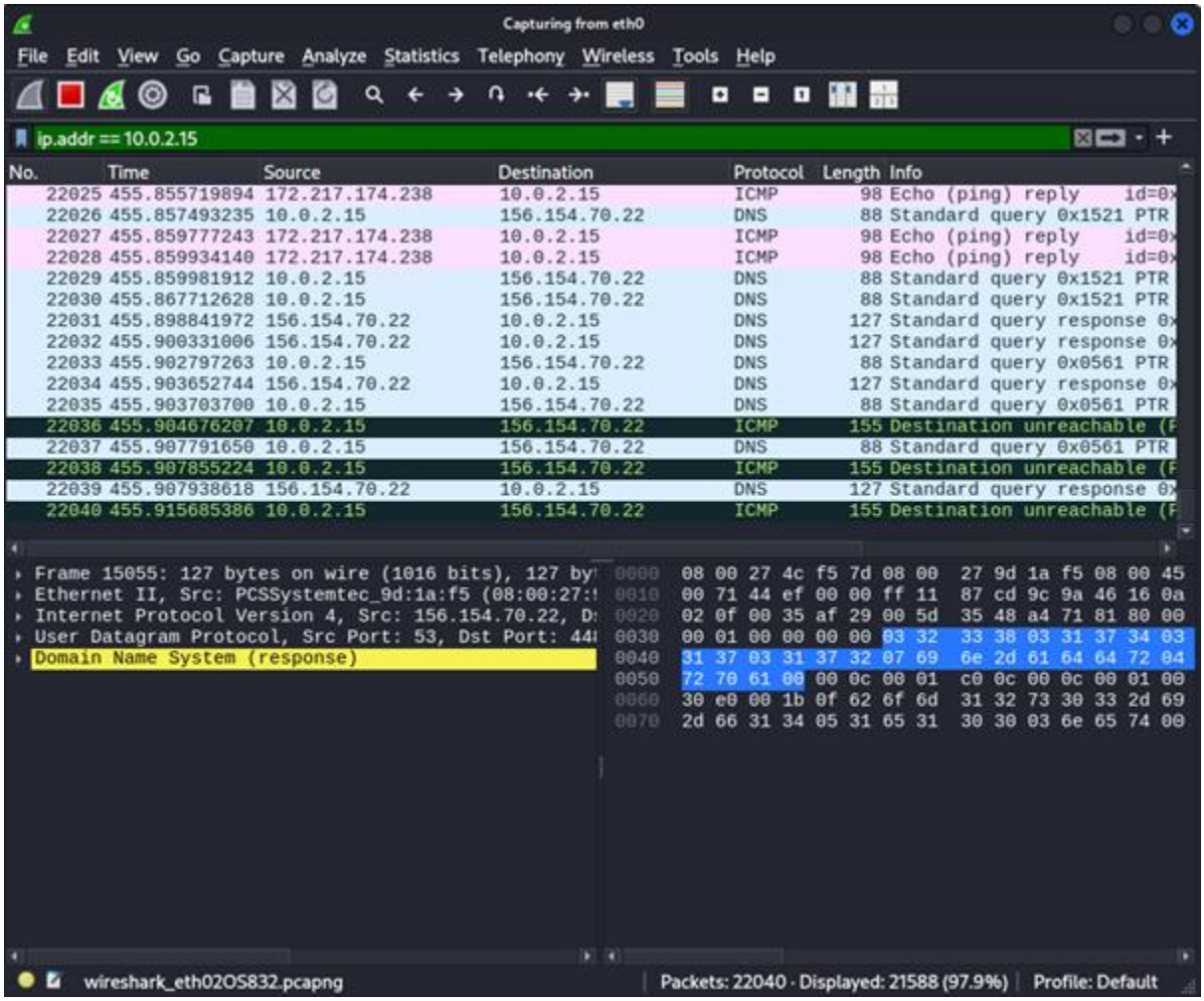

Figure 28: Screenshot of analysing packets from 10.0.2.15.

Step 6: Useful packets are analysed and saved for further use. Vulnerable protocols are set in the filter tab to further exploit the machine.

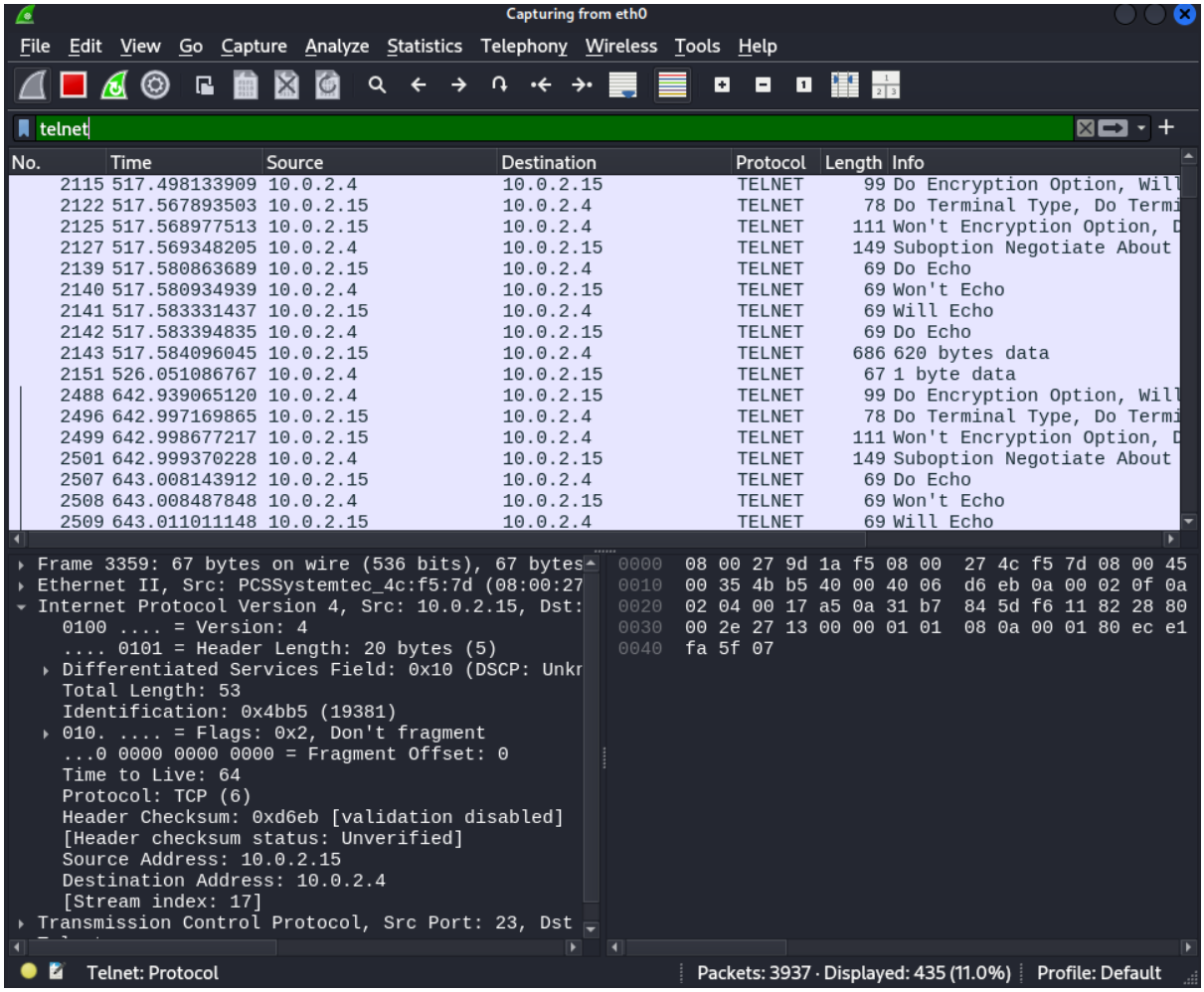

Figure 29: Screenshot of exploring protocols that are vulnerable.

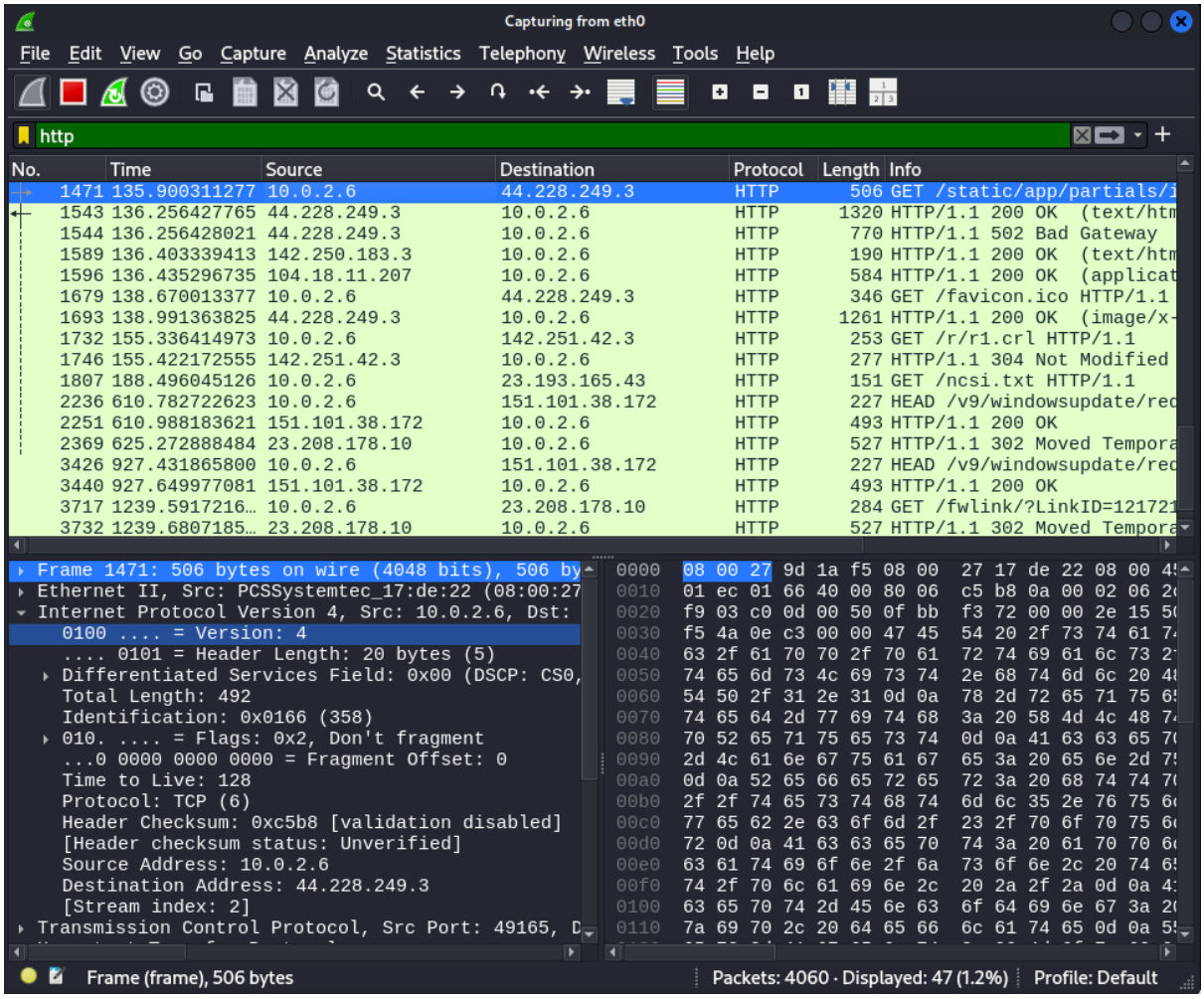

Figure 30: Screenshot of exploring protocols that are vulnerable.

3.4.5. Post-Exploitation

Step 1: The packets that use vulnerable protocols are loaded and then is analysed individually.

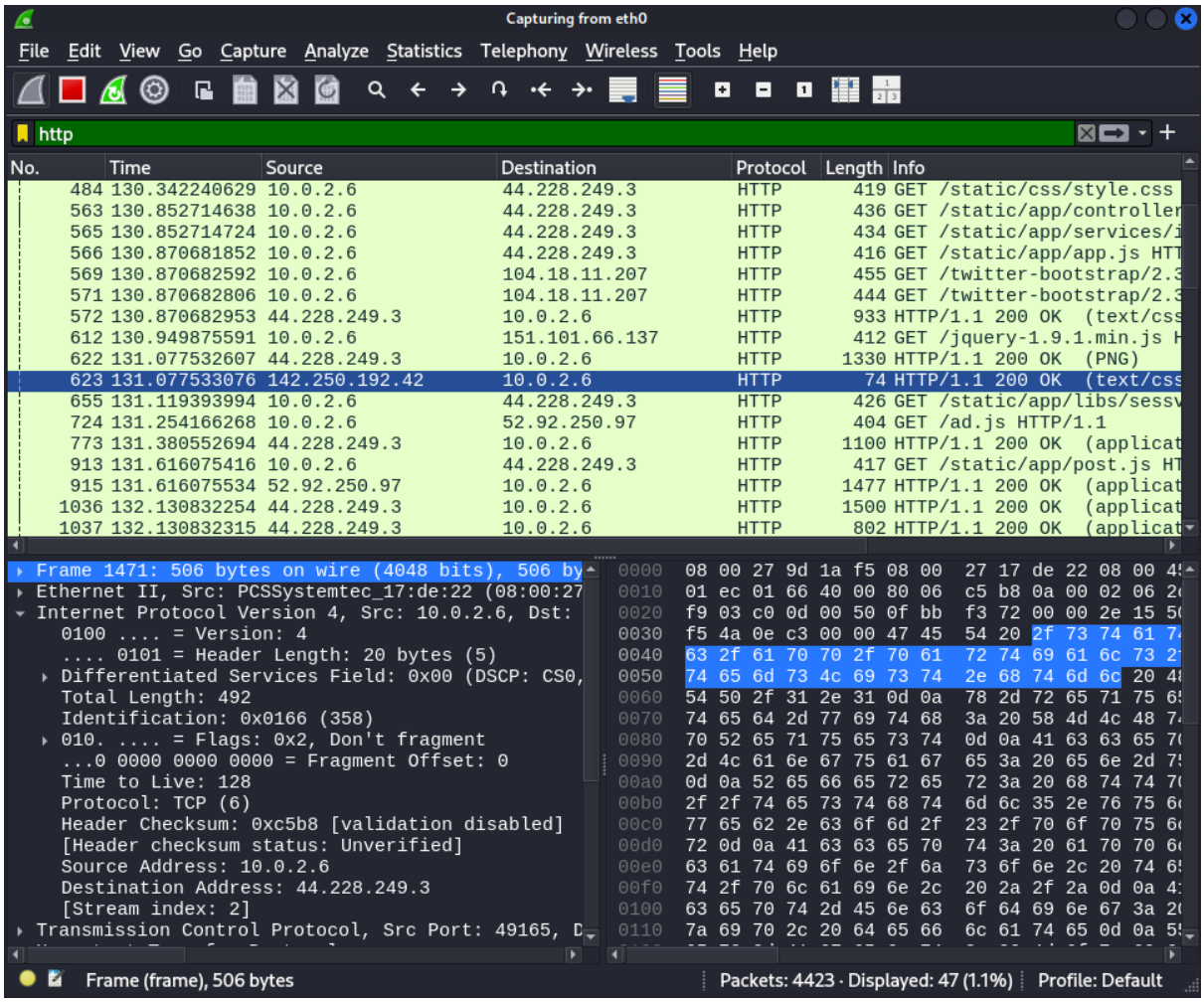

Figure 31: Screenshot of exploring protocols that are vulnerable.

Step 2: One of the packets is selected and clicked to show options.

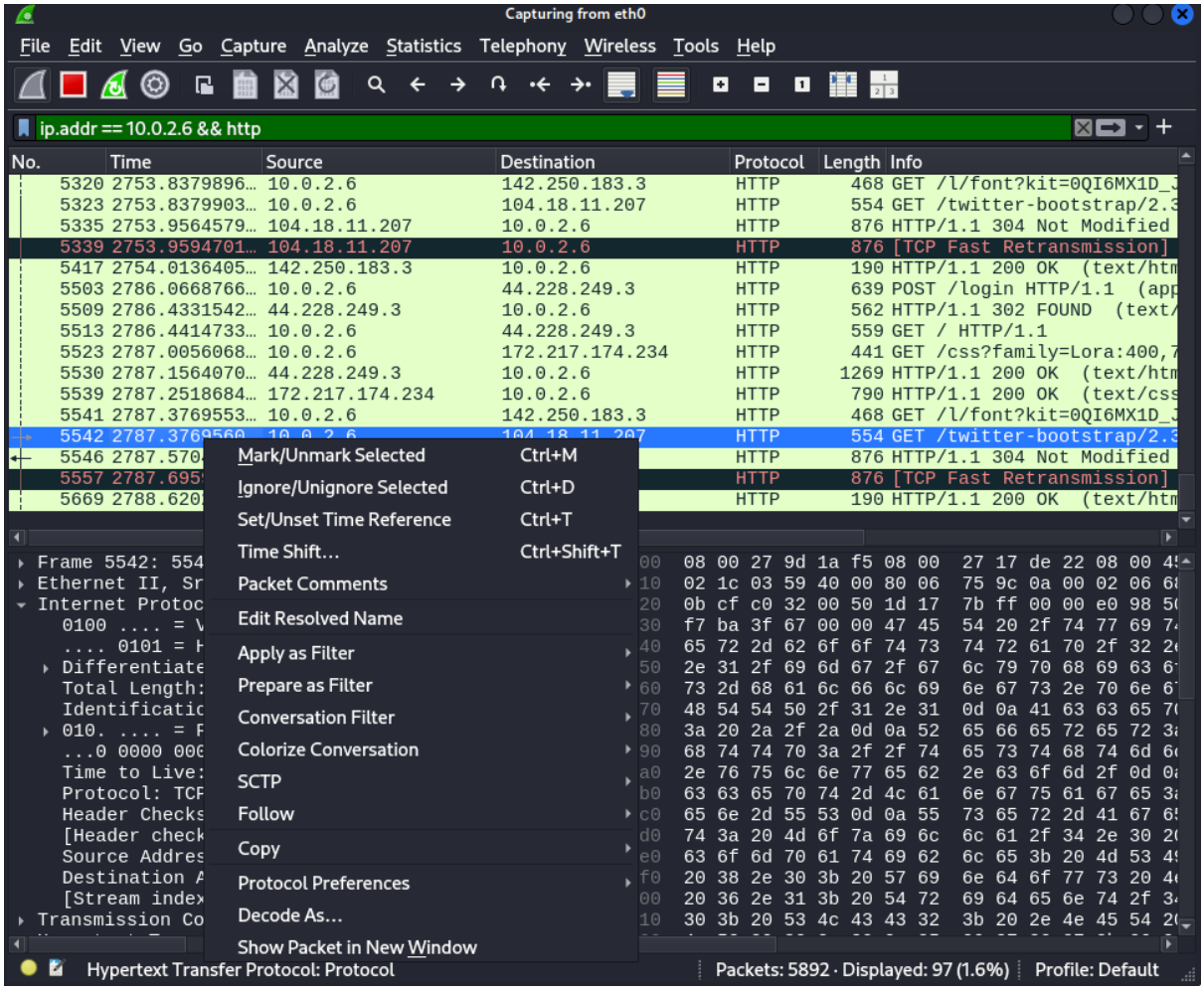

Figure 32: Screenshot of the options for analysing the packet.

Step 3: Then the HTTP stream is selected under the follow option.

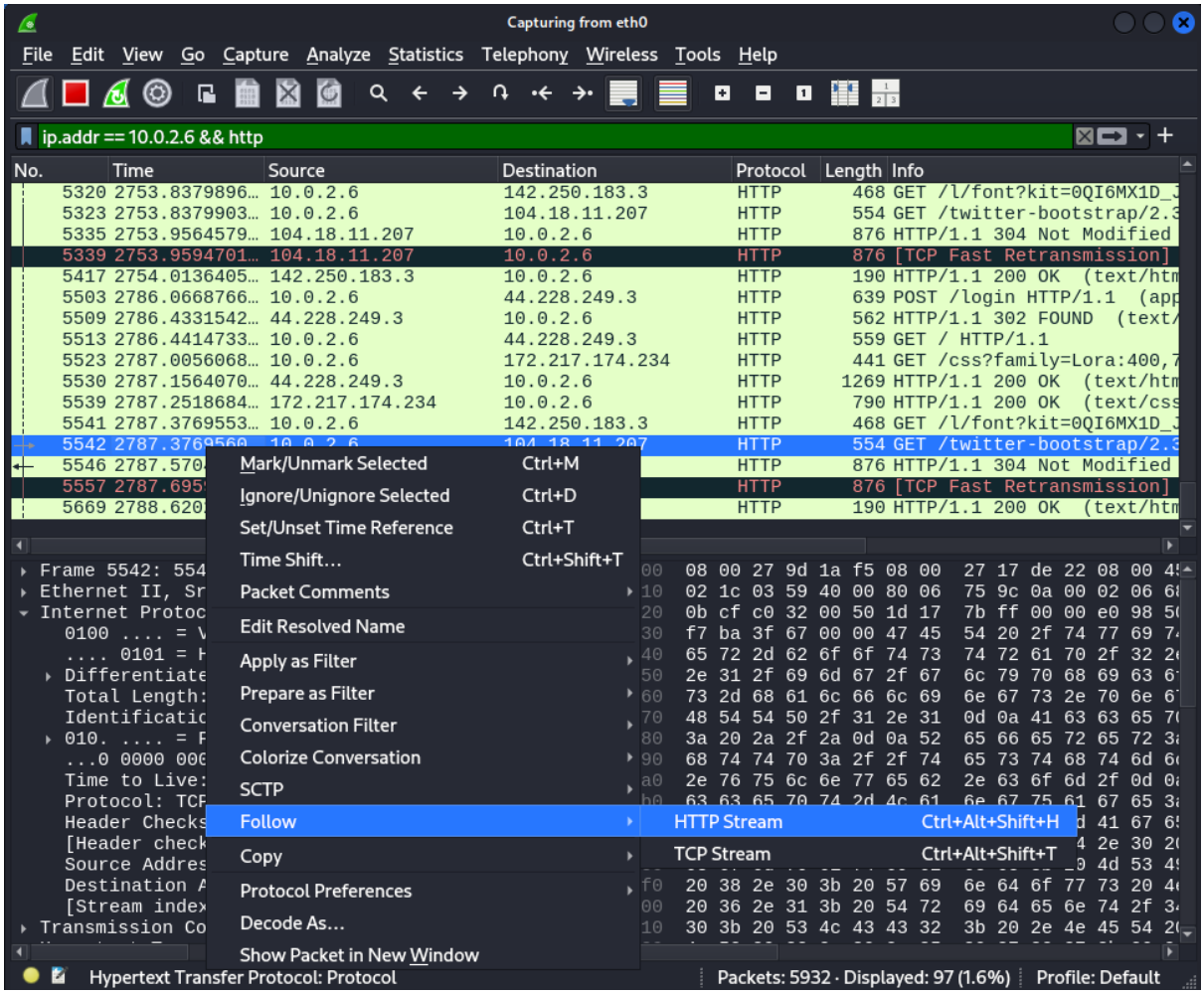

Figure 33: Screenshot of selecting the HTTP stream.

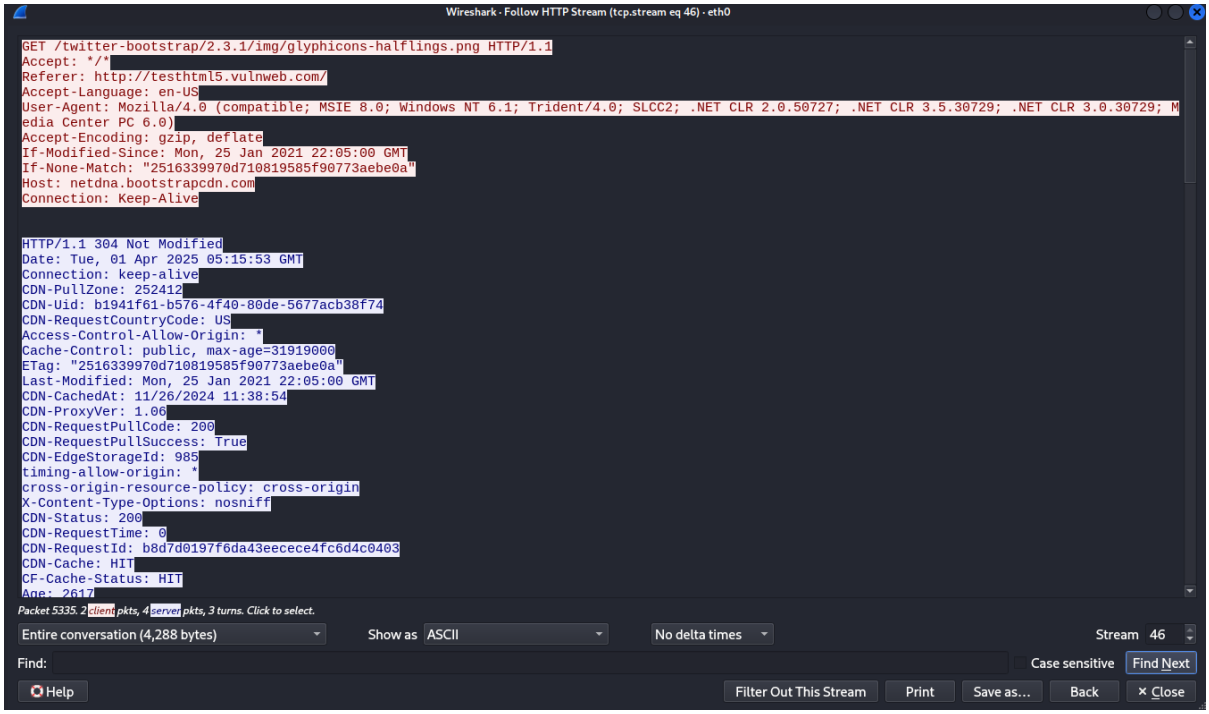

Figure 34: Screenshot of the observing the content of the packet.

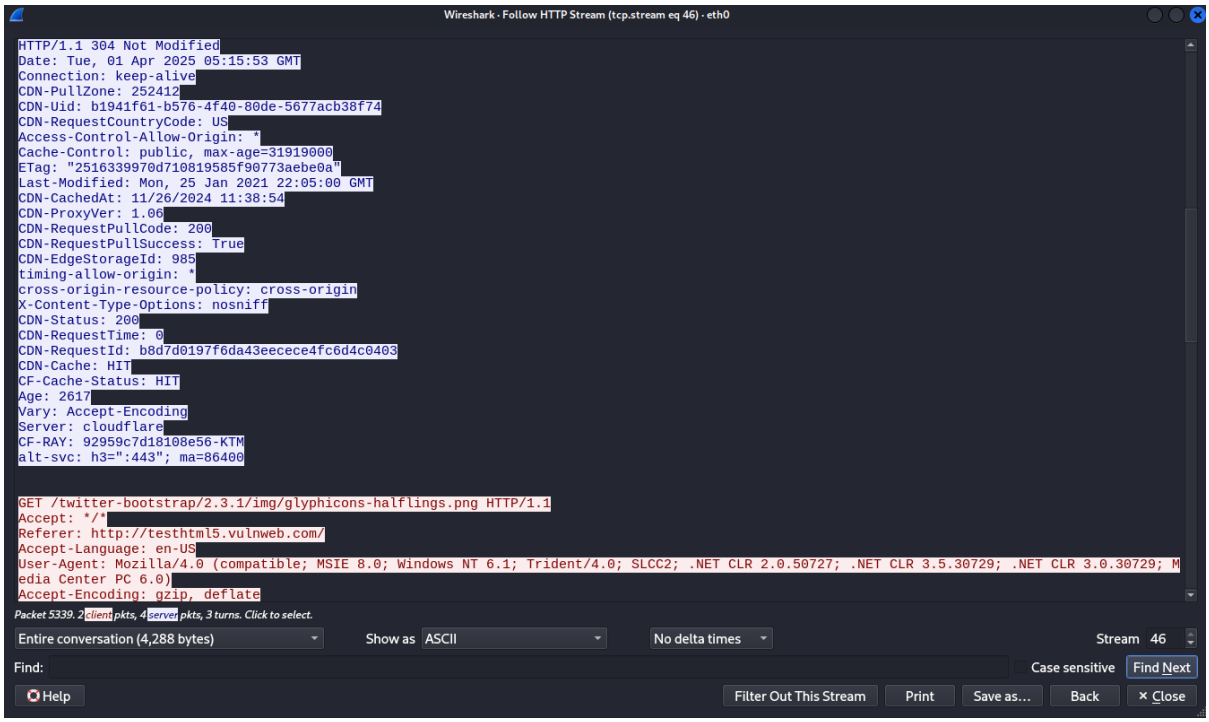

Figure 35: Screenshot of observing the content of the packet.

Step 4: Telnet packets are filtered by using the filter tab.

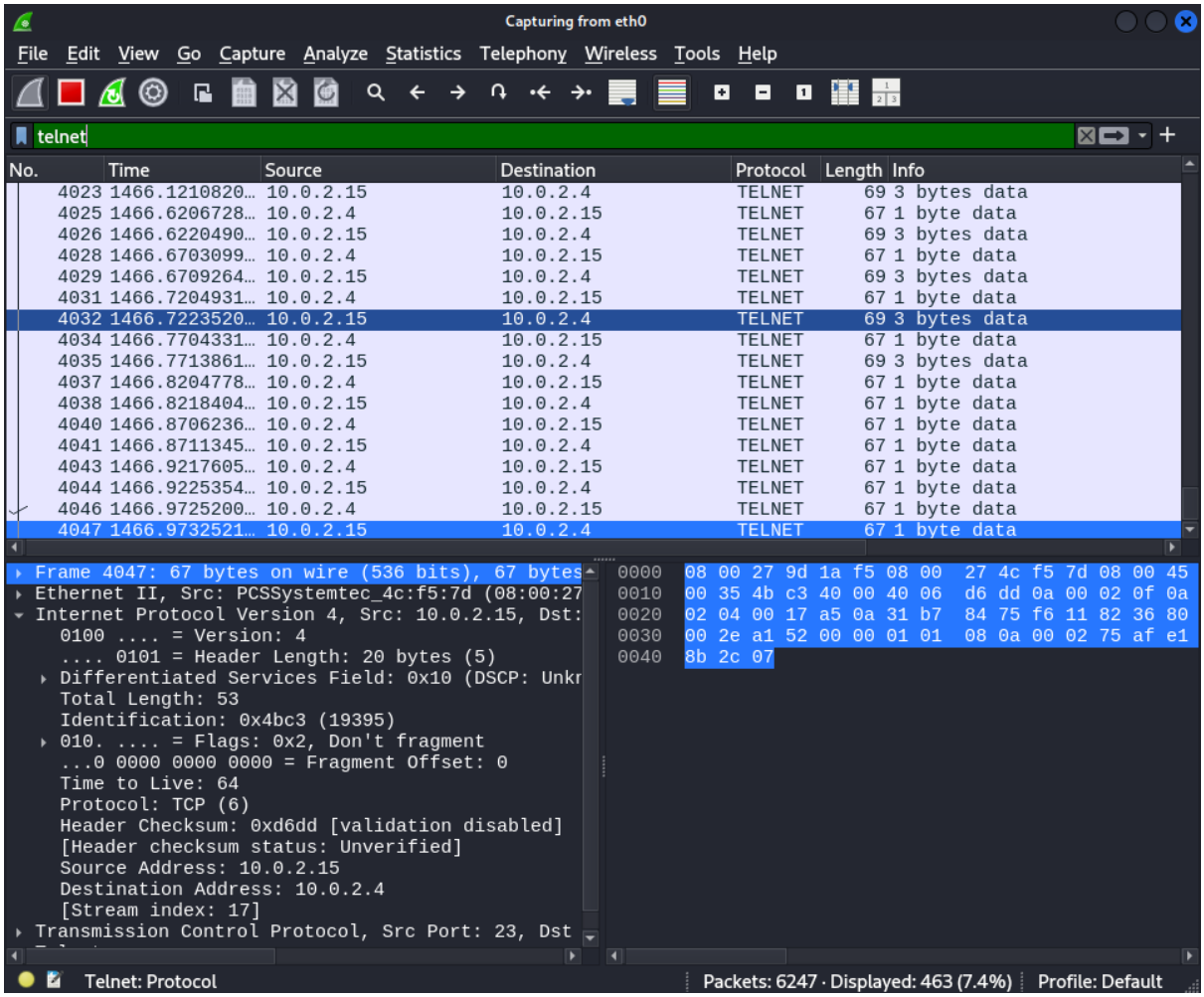

Figure 36: Screenshot of filtering only telnet packets.

Step 5: One of the packets is selected and clicked to show the options.

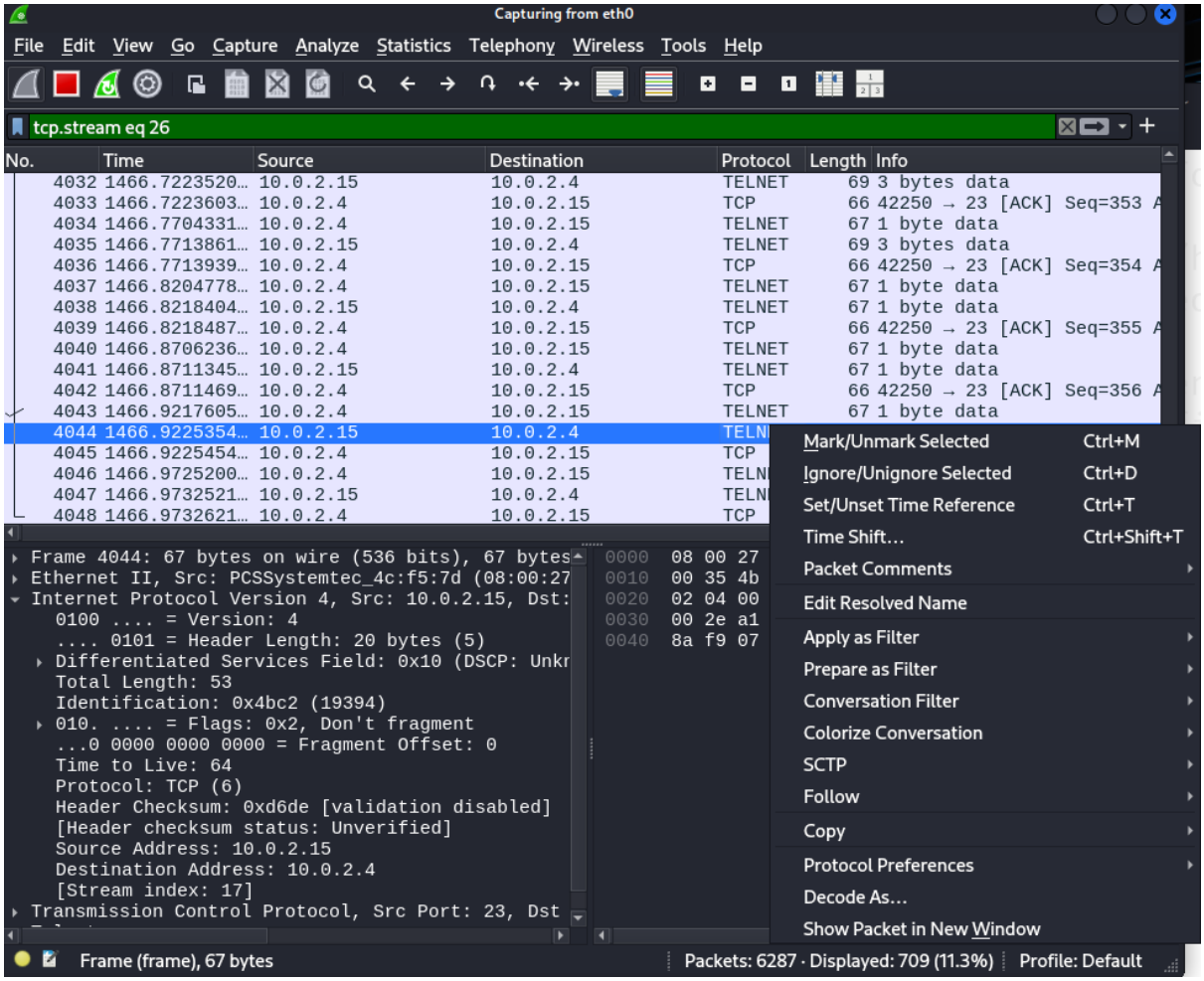

Figure 37: Screenshot of selecting a packet.

Step 6: TCP stream is selected under the follow option.

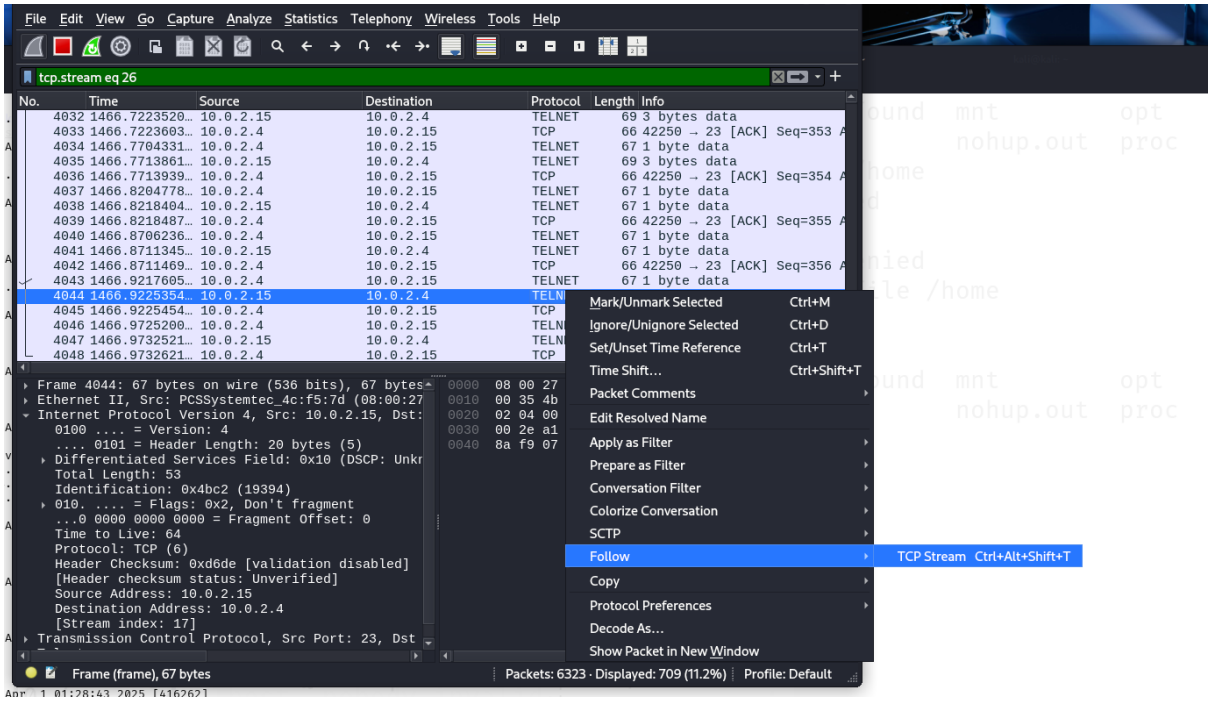

Figure 38: Screenshot of selecting the TCP stream.

Step 7: The content of the packets is observed.

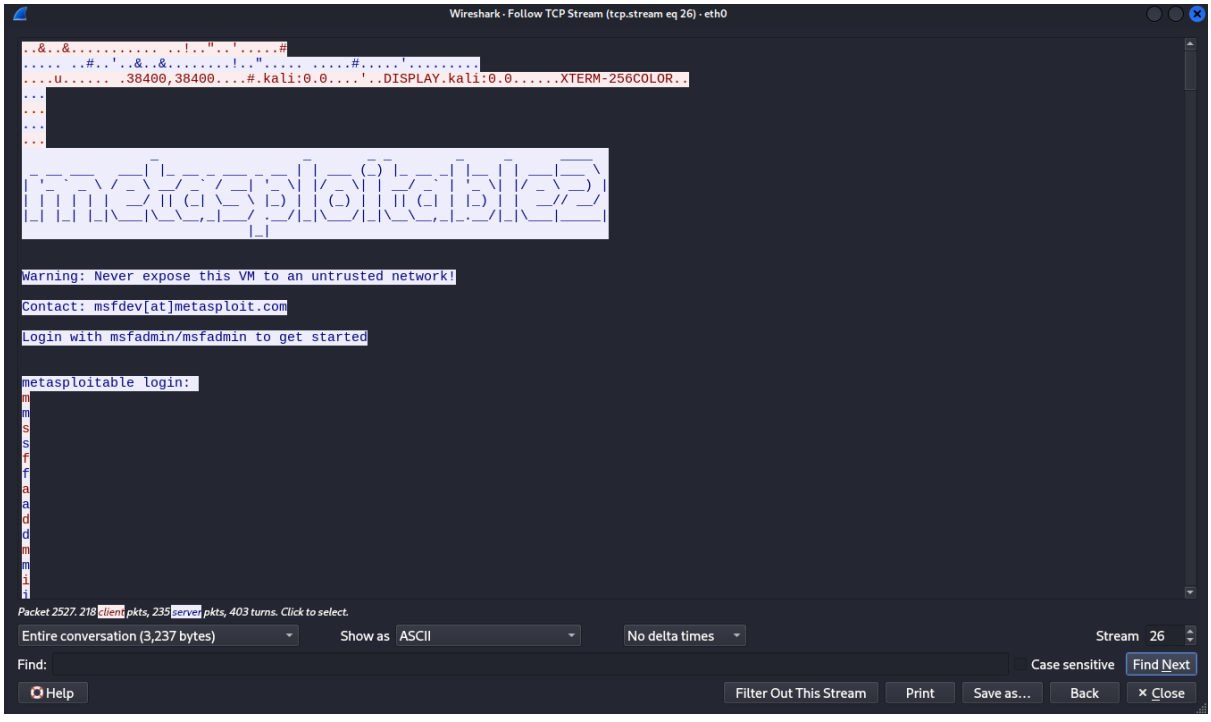

Figure 39: Screenshot of observing the content of the packet.

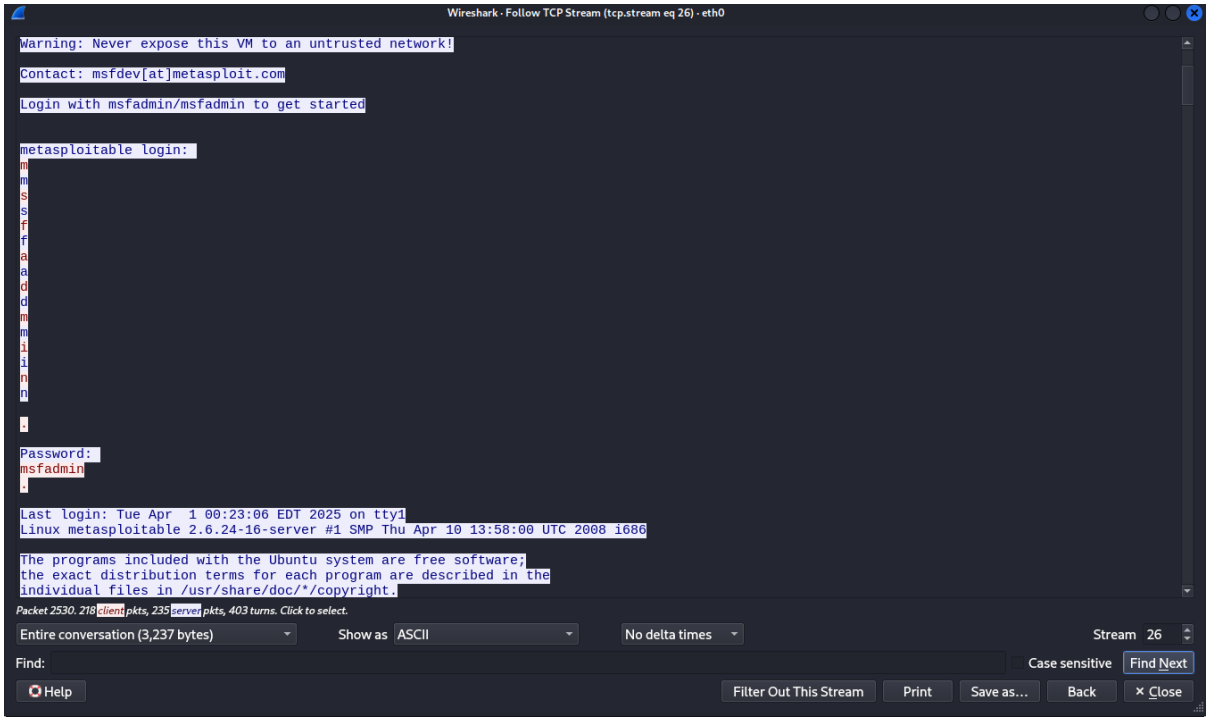

Figure 40: Screenshot of observing the content of the packet.

Step 8: A username and password for telnet is observed and is saved for later use.

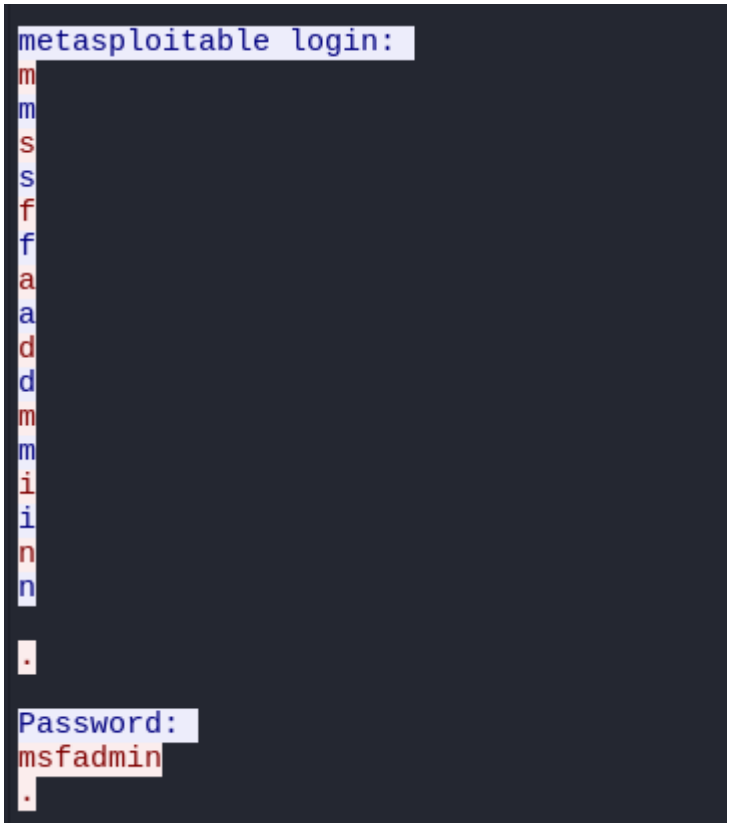

Figure 41: Screenshot of username and password.

Step 9: A new terminal is opened to start a telnet connection.

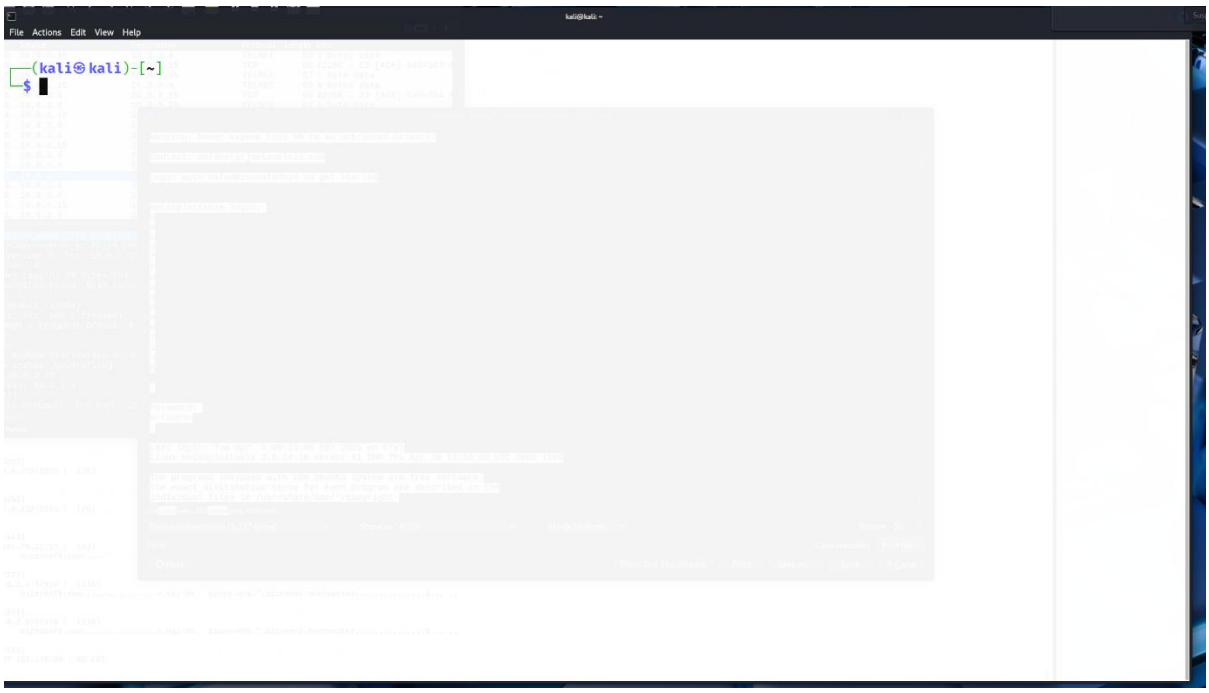

Figure 42: Screenshot of opening a new terminal.

Step 10: The above observed username and password is used to establish a telnet connection to the target.

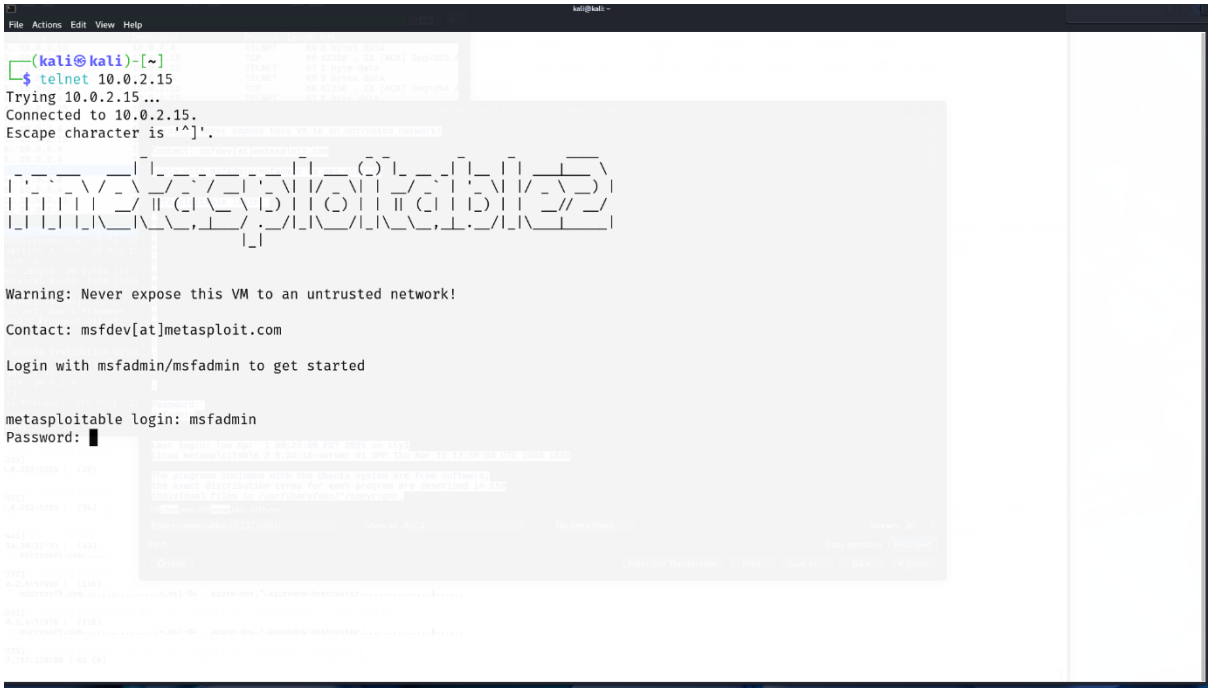

Figure 43: Screenshot of establishing a telnet connection.

Figure 44: Screenshot of establishing a telnet connection.

Step 11: A successful telnet connection is established with the target machine.

Step 12: Further snooping is done in order to find out files that could be exploited.

Figure 45: Screenshot of snooping around the system.

Step 13: Secret files are viewed and kept for further exploitation.

Figure 46: Screenshot of accessing confidential files.

4. Mitigation

4.1. Dynamic ARP inspection

Address Resolution Protocol (ARP) plays a vital role in LAN communication by mapping the IP addresses from the network layer to MAC addresses at the data link layer. This conversion is important as data frames within a LAN requires a destination MAC address for transmission. To make this process more efficient and reduce the unnecessary broadcasts each device keeps an ARP cache that stores IP and MAC pairs. The ARP protocol is used to resolve the MAC address associated with an IP address to ensure proper communication between devices on the same network. (Sabah M. Morsy, 2022).

Despite its functionality, ARP lacks in built-in security mechanisms due to its stateless design. This vulnerability exposes it to ARP spoofing a type of MITM attack. As a result, ARP spoofing poses a significant threat to data integrity and confidentiality in unsecured LAN environments. (Sabah M. Morsy, 2022). This is where Dynamic ARP Inspection comes into play. Dynamic ARP inspection functions as a security mechanism within a network that protects against ARP spoofing attacks. Since ARP lacks authentication features it is vulnerable to malicious activities where attackers can impersonate as a legitimate device. DAI addresses this vulnerability by verifying ARP messages against a trusted database of MAC-to IP-address bindings which is maintained in a DHCP binding table. This allows only valid ARP responses that match the verified entries/users. (Fauzan Prasetyo Eka Putra, 2024).

DAI is implemented on network switches so when it is enabled the switch becomes more selective about which ARP messages it accepts. It checks the senders MAC and IP addresses in its trusted records and if it doesn't match up it drops/discards the message. This helps to prevent the attackers from tricking the network. (Cisco, Jan 14, 2025). DAI closely monitors the ports connected to user devices allowing only ARP messages that pass the validation check. Each switch port is classified as either trusted or untrusted. The trusted ports connected to other switches can freely send ARP messages while untrusted ports are monitored more closely and carefully. If an ARP message on an untrusted port doesn't match the information in the DHCP snooping table then the switch drops the packet and prevents it from being added on the ARP cache. (Sabah M. Morsy, 2022). This process is effective at stopping ARP spoofing because fake ARP messages won't pass the switch's verification checks. But DAI doesn't just help prevent attacks but it's also useful for troubleshooting. It keeps a log of ARP traffic which can

help identify devices with connection problems or spot misconfigured settings on the network. (C & Francis, 2023).

4.2 Disable insecure protocols like Telnet/HTTP

One of the most effective mitigation strategies is disabling insecure communication protocols such as Telnet and HTTP which were successfully exploited during the MITM attack demonstration. These protocols transmit data including sensitive credentials in plain text making it easy for attackers to intercept and read the information using packet sniffing tools like Wireshark (Pandey, 2011). In the demonstration, attackers were able to capture a username and password over Telnet and gain unauthorized access to the victim's machine. This clearly illustrates the risks posed by unencrypted communication.

It is essential to use encrypted protocols to secure both remote administrative access and the transmission of sensitive information in everyday application. To enhance security organizations should replace Telnet with Secure Shell (SSH) which provides encrypted terminal sessions and use HTTPS instead of HTTP for web traffic to ensure the confidentiality and integrity. These protocols not only safeguard data transmission but also increases the difficulty for the attackers attempting threats like MITM attacks .This added complexity serves as a strong deterrent and contributes to an overall defense-in-depth strategy where multiple layers of protection are used to reduce the likelihood of a successful breach. (Medium, 2024).

The importance of encrypted protocols becomes even more evident when considering Man-in-the-Middle (MITM) attacks. These attacks exploit vulnerabilities in unprotected communication channels to eavesdrop on or alter traffic between two parties. If the communication isn't protected, then the attacker can easily read or even change the information being sent. However, when strong encryption is in place things get a lot harder for the attacker. Even if they manage to intercept the traffic, they can't actually understand it without the proper decryption keys. It's like trying to open a locked safe without the combination. Modern encryption standards such as TLS 1.3 are designed to be incredibly secure making it nearly impossible to break the code. (Muneer Alwazzeh, 2020). It's not just about grabbing the data anymore, but the attacker also has to figure out how to crack the encryption which is extremely difficult. This extra layer of protection acts as a strong guard and is a key part of a "defense-in-depth" approach where multiple security measures work together to make systems more secure and reduce the chances of a successful attack. (Prowell, 2010).

4.3. Static ARP Cache Table

Static ARP Cache Table is another mitigation method for ARP poisoning. ARP request spoofing works by tricking the victim device by sending deceptive ARP request packets which will update the ARP table according to the attacker's request making MITM possible. The Static ARP Cache table method involves making a static ARP table which makes sure that spoofed ARP request packet does not affect the ARP table entries. Most OS like Linux and Windows provide features that enable users to create static records for ARP tables which can be managed by manually adding permanent ARP entries. This technique can also be automated by using the capabilities of certain python scripts. (Data, 2018)

Static ARP Cache Table can be incorporated with the help of dedicated software for ARP spoofing detection or can be incorporated through custom Python code by Scapy library. These dedicated software makes it harder to perform IP spoofing as they increase the complexity, requiring valid MAC addresses to be associated with IP addresses and incorporating ARP spoofing detection. The software also looks for unusual patterns and monitors packet transmissions making ARP spoofing harder to execute. "During data transmissions, the system monitors ARP packets, extracting the true physical address of the gateway based on the provided IP. A comparison is made between this gateway MAC address and the one found in the ARP packet's response. If a discrepancy exists between the two MAC addresses, an error message is generated and displayed, while the suspicious packet is discarded. This outcome signifies the recognition of an ARP spoof attack, issuing alerts and highlighting the initial physical address, accompanied by the presentation of a simulated MAC address." (Thomas, et al., 2024)

Since all the entries in the ARP cache table will remain fixed it would most definitely provide a strong mitigation measure against ARP spoofing. And as the ARP cache table is static impersonation and unauthorized access of the ARP operations is quite impossible. Modification attempts which want to change the ARP cache table will be blocked by the above-mentioned dedicated software. Only one fixed entry is established for each IP address to a MAC address, so all network devices linked to that address stops initiating any ARP response requests. A highly defensive mechanism is achieved that not only disables ARP spoofing attempts but also improves overall network security by this mitigation method. (Thomas, et al., 2024)

4.4. IDS/IPS

ARP spoofing involves sending corrupt or abnormal ARP packets to the target hosts and manipulating them into changing the ARP cache table. But this type of attack also creates a DoS situation as it sends abnormal amount of ARP packets. Also, some MAC addresses and IP address in the corrupt ARP packets are very abnormal. So, an IDS/IPS with optimal ARP Spoofing Detection Algorithm would be a great mitigation technique for ARP spoofing. (Al-Hemairy, et al., 2009)

IDS such as Snort are also used to detect ARP attacks and generate an alert to inform administrators. It can help administrators detect attacks early which can help them to launch a countermeasure as soon as possible. Snort inspects packets based on an ARP cache table provided by the administrators. Any ARP packets and ethernet frame being relayed in the network will be inspected and the IDS will read source IP addresses on this list and compare it with corresponding MAC address from the ARP cache table. When inconsistency is detected, a warning is issued which can be read by the administrators. (Demuth & Leitner, 2005)

An Optimal ARP spoofing Detection Algorithm should be used in the IDS/IPS system to make the most out of it. A report written by Al-Hemaiary, Amin, Trabelsi demonstrates a algorithm for optimal ARP spoofing detection which performs cross-layer ARP inspection, performs stateful inspection, detects non expected IP and MAC addresses, detects ARP storm, detects ARP scanning and manually or atomically builds a IP-MAC table to detect invalid IP-MAC pairs. The algorithm created by the above-mentioned authors is shown below. (Al-Hemairy, et al., 2009).

```
Abnormal_Arp_Packet_Detection (Ethernet_header,
ARP_header, IP_MAC_Mapping_Table)
{ /* ARP request packet */
if (ARP_Operation = "request"):
{ Unicast_ARP_request (Ethernet_MAC_Destination);   /* for
detecting packet P#3 */

Unexpected_IP_MAC_Addresses_in_ARP_Request
(Ethernet_MAC_Source, Ethernet_MAC_Destination,
ARP_IP_Source, ARP_MAC_Source, ARP_IP_Destination,
ARP_MAC_Destination); /* for detecting packet P#4 */

Cross_Layer_Inspection_ARP_Request
(Ethernet_MAC_Source, ARP_MAC_Source) /* for detecting
packet P#2 */

IP_to_MAC_Address_Mappings_ARP_Request
(ARP_IP_Source, ARP_MAC_Source,
IP_MAC_Mapping_Table )  /* for detecting packet P#1  */ }

/* ARP reply packet */
if (ARP_Operation = "reply"):
{ Broadcast_ARP_reply (Ethernet_MAC_Destination)   /* for
detecting packet P#9 */

Unexpected_IP_MAC_Addresses_in_ARP_Reply
(Ethernet_MAC_Source, Ethernet_MAC_Destination,
ARP_IP_Source, ARP_MAC_Source, ARP_IP_Destination,
ARP_MAC_Destination); /* for detecting packet P#10 */
Cross_Layer_Inspection_ARP_Reply (Ethernet_MAC_Source,
ARP_MAC_Source, Ethernet_MAC_Destination,
ARP_MAC_Destination )   /* for detecting packets P#6 and
P#8 */

IP_to_MAC_Address_Mappings_ARP_Reply
(ARP_IP_Source, ARP_MAC_Source, ARP_IP_Destination,
ARP_MAC_Destination, IP_MAC_Mapping_Table )   /* for
detecting packets P#5 and P#7 */
}}
```

Figure 47: Figure explaining the algorithm.

5.Evaluation

5.1. Pros of applied mitigation strategies

In evaluating the effectiveness of the mitigation measures, several key advantages stand out supporting its role in overall network security and resilience against ARP-based threats.

1. Dynamic ARP Inspection

A critical evaluation of Dynamic ARP Inspection reveals multiple strengths to mitigate ARP-related threats through precise verification mechanisms. Dynamic ARP Inspection offers a robust defense mechanism against ARP-based attacks by verifying the integrity of the ARP packets before they are processed. One of its key strengths is its ability to detect and drop ARP packets containing invalid IP and MAC address bindings. This verification is made possible through the use of a trusted database built using DHCP snooping which maintains accurate IP-to-MAC mappings. then by cross-checking the ARP traffic against this database. By doing so DAI effectively mitigates ARP spoofing and poisoning attacks. (Abad & Bonilla, 2007).DAI allows the switches to differentiate between the trusted and untrusted ports which enforces stricter security on potentially vulnerable edge ports (Sabah M. Morsy, 2022).DAI logs suspicious ARP traffic and provides insight into device behaviour which helps administrators troubleshoot misconfigurations and track down malicious activity. (C & Francis, 2023).

2. Disabling Insecure Protocols

The use of insecure communication protocols such as Telnet and HTTP is widely recognized as a significant vulnerability in network environments. Disabling these protocols strengthens security by replacing them with encrypted alternatives like SSH and HTTPS. Telnet transmits credentials in plaintext which makes them easy to intercept but if replaced with SSH the terminal sessions are encrypted, thereby reducing the risk of credential theft and man-in-the-middle (MITM) attacks. Similarly, replacing HTTP with HTTPS ensures that web traffic is encrypted during transmission, thereby protecting data from unauthorized access and improving its confidentiality and integrity. These strategies reinforce a defense-in-depth strategy by providing encrypted communication that adds an extra layer of protection and makes it more difficult for attackers to access sensitive data. (Medium, 2024).

3. Static ARP Cache Table

Implementing a static ARP cache table offers key security and performance advantages, especially in fixed or tightly controlled network environments. Static ARP cache tables

enhance network security by preventing ARP spoofing, as manually configured IP-MAC bindings cannot be altered by spoofed packets. These entries do not expire or get overridden, ensuring consistent communication and protecting against man-in-the-middle attacks. This ensures consistent communication and reduces the risk of unexpected disruptions caused by ARP table updates. When combined with ARP monitoring tools, it further strengthens overall network protection. (Huawei, 2023).

4. IDS and IPS

IDS/IPS systems provide significant benefits in mitigating ARP spoofing by detecting suspicious ARP traffic and alerting administrators when unexpected behaviours such as IP-MAC mismatches are identified. These systems use smart ARP spoofing detection algorithms to track anomalies like MAC-IP mismatches, ARP storms, and other abnormal patterns. This constant monitoring allows network administrators to respond quickly to potential threats helping to stop attacks before they grow worse. As a result, the systems play a crucial role in protecting the network from serious damage over time, ensuring the safety of important data and keeping everything running smoothly. (Abbas, et al., 2023).

5.2. Cons of applied mitigation strategies

1. Dynamic ARP Inspection

Another mitigation measure discussed above is Dynamic ARP inspection. It is a new feature which is included in high end Cisco switches, and it allows the switch to drop questionable and fake IP, MAC binds. Its major disadvantage is that it is a feature available in high-cost switches, so in order to implement this mitigation strategy a company must buy the expensive cisco switches which is not feasible for everyone. Its dependency on DHCP server and network makes it so that some ARP packets might not be possible to be validated. (Abad & Bonilla, 2007).

2. Disabling Insecure Protocols

The last mitigating method explained in the Mitigation section is using secure protocols, while this might be valid for new and updated devices it is not feasible for legacy devices as they might not be compatible with the new secure protocols. (Abad & Bonilla, 2007).

3. Static ARP Cache Table

One of the mitigation measures mentioned above is Static ARP table which establishes a ARP table that has IP and MAC bind permanently unless manually changed. One of the major drawbacks for this mitigation strategy is that it does not work in an environment where devices are dynamically assigned IP addresses. If DHCP service is enabled, then it is very tough to maintain this strategy as the administrator must manually update the ARP cache every time a new device connects the network. Also, this mitigation strategy is not very scalable because the administrator again has to deploy and update tables throughout the network. (Abad & Bonilla, 2007).

4. IDS and IPS

Intrusion Detection System (IDS) works by detecting anomalies and sending alerts, while IDS usually do detect ARP attacks and send alerts the administrator, but the main drawback of this applied mitigation strategy is that it tends to generate a lot of false alarms as many of the alerts don’t turn out be actual attacks. An organization must assign a person who must oversee the IDS for it to be effective. Also, while some IDS might be able to detect all forms of ARP attack most cannot, so it is also one of the cons for this mitigation strategy. (Abad & Bonilla, 2007).

5.3. Application areas

1. Dynamic ARP Inspection

DIA is a feature in cisco switches that lets network administrators to intercept, log and discard ARP packets with invalid MAC-IP pairs. It helps protect the LAN network from MITM attacks. One of the major application areas for DIA is where network is accessible and open to many people. An example where DIA could be used is educational institutions where Wi-Fi networks are open and accessible to anyone. Attackers could leverage the accessibility of the network to many users to launch MITM attacks. DIA can help maintain accurate MAC-IP binding table which will help prevent malicious redirection of traffic in such environment. (Cisco, 2016)

2. Disabling Insecure Protocols

Using insecure protocols like HTTP and telnet transmits all the packets in the network in plain text, during MITM attack the attacker could easily steal information that is being transmitted over. Disabling insecure protocols is very crucial in environment where sensitive data is transmitted and must be protected from eavesdropping and interception. A major application area for this mitigation strategy could be in financial institutions as they need to be complaint with data protection regulations and the data and information transmitted in the financial institutions are sensitive and must be encrypted. (Medium, 2024)

3. Static ARP Cache Table

Static ARP Cache Table helps avoid ARP poisoning attacks by creating an unchanged ARP Cache Table which will have static IP-MAC mapping. It might not be feasible where device configuration is unpredictable. But when it comes to IoT networks it will thrive, and pre-configured ARP entries could prevent spoofing attacks effectively. Since the IoT devices do not need to change Ip addresses at all or move across networks, Static ARP entries would enhance security without requiring constant monitoring or dynamic learning systems. (Thomas, et al., 2024)

4. IDS and IPS

Intrusion Detection and Prevention System (IDS/IPS) could not only used for ARP Spoofing detection, but it could also be used across different areas to detect, monitor and mitigate other cyber threats in real time. It is a very versatile security solution that could identify, monitor and mitigate a wide range of cyber threats. The major application area for this mitigation strategy would be Corporate Enterprise Networks as it would help prevent MITM from insider threats

as well as malware propagation or other types of suspicious activities in the network. It could also be used in Data centres and ISPs because of its versatility. It would help in keeping logs and scan for all the traffic entering and leaving the premises.

6. Conclusion

This report highlights the risks of Man-in-the-Middle (MITM) attacks and the importance of strong cybersecurity in networks. By using tools in virtual lab, we demonstrated how attackers can easily take advantage of any loopholes such as ARP spoofing and unprotected communication protocols. We were also able to study sensitive information like username and passwords, which proved that old or weak security methods are not enough.

The report studies different ways to mitigate these attacks. Using secure communication, fixed ARP settings, stronger protocols, and applying systems that can detect unusual behaviour can improve network security. However, each of these solutions comes with its own challenges such as setup costs, management difficulties, and issues with older systems. And that is why, the best defense includes a combination of technical tools and organizational practices like regular system updates, employee training, continuous monitoring, and clear security policies.

The report follows the Penetration Testing Execution Standard (PTES), that helps to make sure the testing is done in a structured and ethical way in a secure environment. The process involves steps such as planning, gathering information, modelling threats, attacking, and analysing results. In the test done, the attack prove dhow weak protocols like telnet ad HTTP can be used to steal username an passwords.

Beside finding these weaknesses, the report also looks at different ways to protect networks. Some of these include using Dynamic ARP Inspection (DAI), setting up static ARP, using secure protocols like SSH and HTTPS, and using Intrusion Detection Prevention System (IDS/IPS). The report also highlights how important and easy it is to use these tools.

In conclusion, the finding of this project features the importance of security measure in preventing and mitigating MITM attacks. By simulating a real-world attack scenario and studying the outcomes, the report provides valuable insights about both offensive and defensive aspects of cybersecurity. This report serves as a reminder that while the technologies advances, awareness, preparedness, and strategic mitigation helps to reduce an organization’s vulnerability to such attacks.

7. References

Abad, C. L. & Bonilla, R., 2007. *An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks.* Toronto, Canada, IEEE.

Abbas, S., Abbas , A. & Naser Khuder, W. a., 2023. Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). *Global Journal of Engineering and Technology Advances,* 14(02), pp. 155-158.

Agashe, R. et al., 2022. Secure Socket Layer in the Network and Web Security. *International Journal of Advanced Research in Computer and Communication Engineering,* 11(5), p. 638–643.

Aijaz, D., 2025. *purewl.* [Online] Available at: https://www.purewl.com/man-in-the-middle-attacks-in-the-us-in-2024/ [Accessed 28 03 2025].

Al-Hemairy, M., Amin, S. & Trabelsi, Z., 2009. *Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks.* Dubai, IEEE.

Artem A. Maksutov, I. A. C. M. S. A., 2017. *Detection and prevention of DNS spoofing attacks.* Novosibirsk, Russia, IEEE.

Astari, H., 2025. *spiceworks.* [Online] Available at: https://www.spiceworks.com/tech/cloud/articles/what-is-virtualbox/ [Accessed 31 03 2025].

Baitha, A. K. & Vinod, S., 2018. *Research Gate.* [Online] Available at: https://www.researchgate.net/publication/325117343_Session_Hijacking_and_Prevention_Technique
[Accessed 9 May 2025].

Balaban, D., 2020. *Security.* [Online] Available at: https://www.securitymagazine.com/articles/91980-types-of-spoofing-attacks-every-security-professional-should-know-about
[Accessed 5 April 2025].

Bharat Bhusan, A. K. R. ,. G. S., 2017. *Man-in-the-middle attack in wireless and computer networking — A review.* Dehradun,India , IEEE.

C, E. & Francis, 2023. *Medium.* [Online] Available at: https://edgarcf.medium.com/what-is-dai-dynamic-arp-inspection-4d150059d89b [Accessed 19 04 2025].

Cisco, 2016. *Configuring Dynamic ARP Inspection.* [Online] Available at: https://www.static-cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380-configuration/dynarp.pdf
[Accessed 10 May 2025].

Cisco, Jan 14, 2025. *Cisco Meraki.* [Online] Available at: https://documentation.meraki.com/MS/Other_Topics/Dynamic_ARP_Inspection [Accessed 19 04 2025].

Coole, M., 2022. *Research Gate.* [Online] Available at: https://www.researchgate.net/publication/280571067_Defence_in_depth_protection_in_depth_and_security_in_depth_A_comparative_analysis_towards_a_common_usage_language [Accessed 10 May 2025].

Data, M., 2018. *The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table.* Malang, IEEE.

Demuth, T. & Leitner, A., 2005. ARP spoofing and poisoning traffic tricks. *Linux magazine,* 56(1), pp. 26-31.

Dr.Julian Fejzajb, E. Y., 2021. *Man in the Middle: Attack and Protection.* Tirana,Albania, CEUR Workshop Proceedings (CEUR-WS.org).

Evans, D., 2011. *The Internet of Things, How the next Evolution of the Internet is Changing Everything ,* San Jose, CA: Cisco Internet Business Solutions Group(IBSG).

Fauzan Prasetyo Eka Putra, U. U. A. B. T. R. W. E., 2024. Implementation And Simulation Of Dynamic Arp Inspection In Cisco Packet Tracer For Network Security. *Brilliance Research of Artificial Intelligence ,* 4(1), pp. 2807-9035.

Gandotra, E. a. G. D., 2020. Improving Spoofed Website Detection Using Machine Learning. *Cybernetics and Systems,* p. 169–190.

Ghazi Al Sukkar, R. S. S. K. M. M. I. J., 2016. *Address Resolution Protocol (ARP): Spoofing Attack and Proposed DefenseGhazi Al Sukkar, Ramzi Saifan, Sufian Khwalde3, Mahmoud Maqableh, Iyad Jafar.* Jordan, Cretivecommons.

HANGE, Y. M., 2023. A REVIEW ON NMAP AND ITS FEATURES. *International Research Journal of Engineering and Technology (IRJET),* 10(5), pp. 2395-0072.

Huawei, 2023. *Huawei.* [Online] Available at: https://support.huawei.com/enterprise/en/doc/EDOC1100278756/1fe67885/understanding-arp#EN-US_CONCEPT_0172353405 [Accessed 21 04 2025].

M. Conti, N. D. a. V. L., 2016. A Survey of Man in the middle attacks. *IEEE,* 18(3), pp. 2027-2051.

Madapparambath, G., 2021. *How To Create And Use NAT Network In VirtualBox.* [Online] Available at: https://www.techbeatly.com/how-to-create-and-use-natnetwork-in-virtualbox/ [Accessed 22 April 2025].

Maksutov, A. A., Cherepanov, I. A. & Alekseev, M. S., 2017. *Detection and prevention of DNS spoofing attacks,* Novosibirsk: IEEE.

Mallik, A., 2018. MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. *Cyberspace: Jurnal Pendidikan Teknologi Informas,* 2(2), pp. 109-134.

Manasvi Sonke, P. T. B. H. R. K., 2024. Kali Linux for Cyber Security. *International Journal of Research Publication and Reviews,* 5(8), pp. 4248-4258.

Mandeep Singh, S. K. T. G. N. P., 2020. Penetration Testing on Metasploitable 2. *International Journal Of Engineering And Computer Science,* 9(04), pp. 25014-25022.

Mauro Conti, N. D. ,. V. L., 29 March, 2016. A Survey of Man In The Middle Attacks. *IEEE,* 18(3), pp. 2027-2051.

Medium, 2024. *Networking Secure Protocols | Cyber Security 101 (THM).* [Online] Available at: https://medium.com/@Z3pH7/tryhackme-networking-secure-protocols-cyber-security-101-thm-67356d1b8b69
[Accessed 10 May 2025].

Ming-Hsing Chiu, K.-P. Y. R. M. a. T. K., 2011. *Analysis of a Man-in-the-Middle Experiment with Wireshark,* Lousiana: Louisiana University.

Mohammad Daud, S. S. B. F. S., 2025. Detection of ARP Spoofing Attack by using ETTERCAP. *Advances in Nonlinear Variational Inequalities,* 28(4), pp. 1092-910.

Muneer Alwazzeh, S. K. M. N. S., 2020. Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat. *Journal of Cyber Security and Mobility,* 9(3), pp. 449-468.

Ndatinya, V. &. X. Z. &. M. V. &. M. K. &. X. Y., 2015. Network forensics analysis using Wireshark. *International Journal of Security and Networks,* 10(2).

Pandey, S., 2011. MODERN NETWORK SECURITY: ISSUES AND CHALLENGES. *International Journal of Engineering Science and Technology* , 3(5), pp. 0975-5462.

Pandove, K., Jindal, A. & Kumar, R., 2010. *International Journal of Computer Applications.* [Online]
Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f7d5f70bad4358cb9e7472108d01b0e6d474b9b6
[Accessed 5 April 2025].

Prowell, S. K. R. a. B. M., 2010. *Man-in-the-Middle.* Burlington: Syngress.

PTES, 2014. *The Penetration Testing Execution Standard.* [Online] Available at: http://www.pentest-standard.org/index.php/Main_Page
[Accessed 10 May 2025].

Sabah M. Morsy, D. N., 2022. D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing. *IEEE,* Volume 10, pp. 46142-48153.

Saed, M. & Aljuhani, A., 2022. *Detection of Man in The Middle Attack using Machine learning.* Tabuk, IEEE.

Soepeno, W. A. E. T. f. A. f. t. c. A. A. P., 2023. *Wireshark: An Effective Tool forNetwork Analysis,* Arizona: The University of Arizona.

Sonia Rachel1, S. S., 2017. *An Overview of the Man-In-The-Middle Attack,* Bangalore: National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS).

Swathi, K., 2022. Brute Force Attack on Real World Passwords. *International Journal of Research Publication and Reviews,* 3(11), p. 552–558.

Thomas, D. R. et al., 2024. *Detection and Prevention of Poisoning Targets with ARP Cache using Scapy*. Bangalore, IEEE.

Waheed, A., Seegolam, B. & Jowaheer, M. F., 2024. *Research Gate.* [Online] Available at: https://www.researchgate.net/publication/382734105_Zero-Day_Exploits_in_Cybersecurity_Case_Studies_and_Countermeasure
[Accessed 10 May 2025].

Yongzhen Li, J. L., 2016. *The Research on ARP Protocol Based Authentication.* China, Atlantis Press.

Zhang, L., 2008. A retrospective view of network address translation. *IEEE,* 22(5), pp. 8-12.

Zoran Cekerevac, P. C. ,. L. P. F. A.-N., January 2025. SECURITY RISKS FROM THE MODERN MAN-IN-THE-MIDDLE-ATTACK. *MEST Journal,* 13(1), pp. 34-51.

8. Appendices

8.1. Setting up the environment for exploiting

8.1.1. Installation of virtual machines on Oracle VirtualBox

The attack was performed safely in a controlled environment in order to avoid ethical or legal issues. The virtual environment that was used to conduct the attack is Oracle VirtualBox. 3 virtual machines were created, 1 virtual machine hosts Kali Linux which will act as the attacker machine, and the other virtual machines will host windows 7 and metaspoitable 2 which are the victim machines and their connection with each other and to the internet is eavesdropped and further exploited.

8.1.2. Network Adapter Configuration of Virtual Machines

By default, Oracle VirtualBox sets the virtual machines network adapter to NAT which lets the virtual machines access the internet. But it does not allow the machines to access or build a connection with other virtual machines hosted in the same system. The virtual machines must be connected to a virtual switch in order to establish connection between the machines that we have hosted on the virtual box.

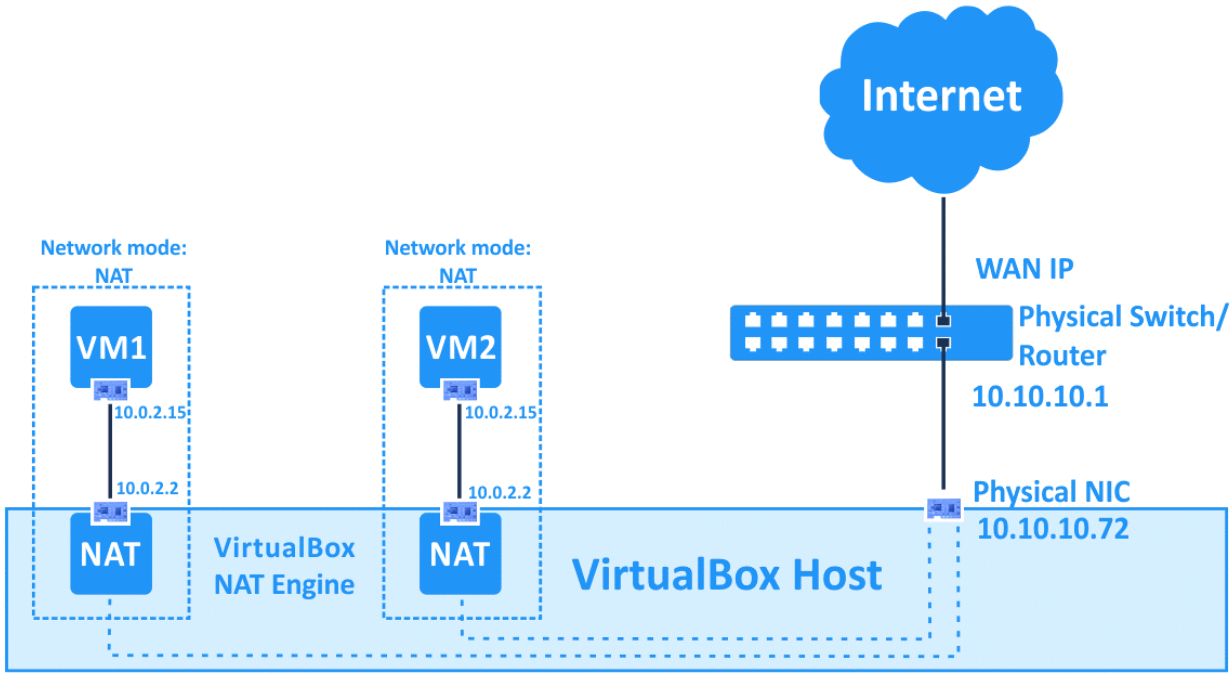

Figure 48: Screenshot of how NAT adapter works in Virtual box. (Madapparambath, 2021)

A NAT network creates a virtual switch where all the hosts in the same NAT network are connected to this virtual switch. The virtual switch lets network connection between the different virtual machines that we created possible. A NAT network was created so that all the

machines are in the same network, it is done so to establish a connection between the attacker machine and victim machine. Without a network connection the attack would not be possible to conduct.

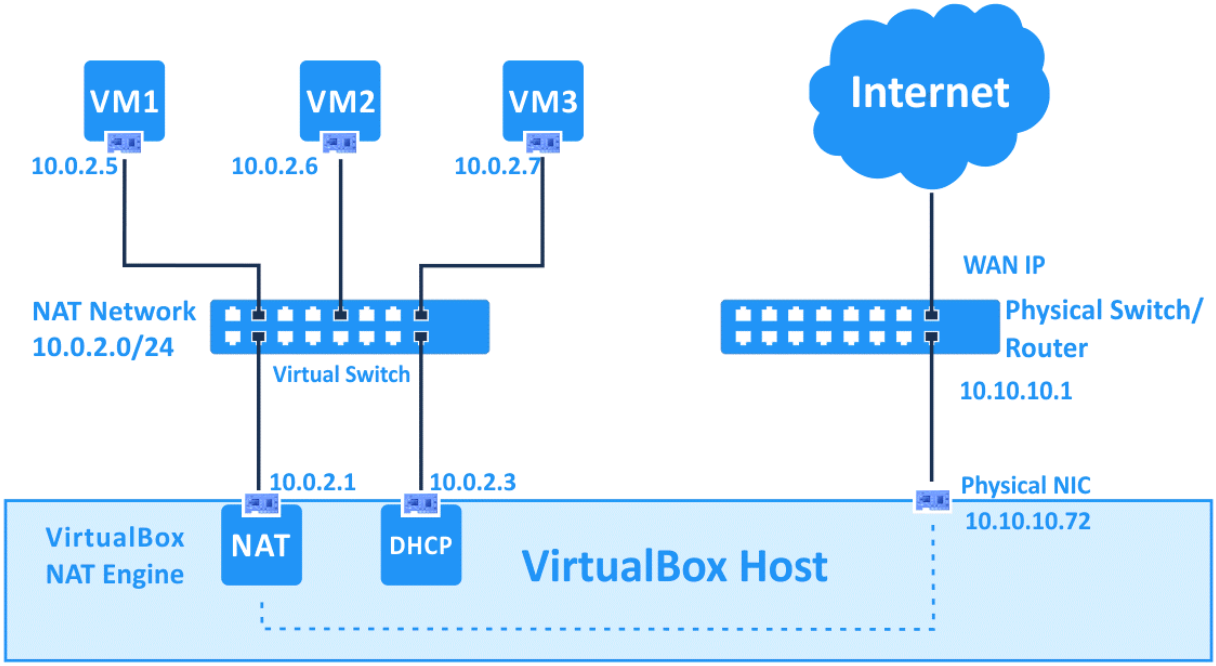

Figure 49: Screenshot of how NAT Network adapter works in Virtual box. (Madapparambath, 2021)

8.1.2.1. Setting up NAT network

Step 1: First of all, Oracle VirtualBox is launched.

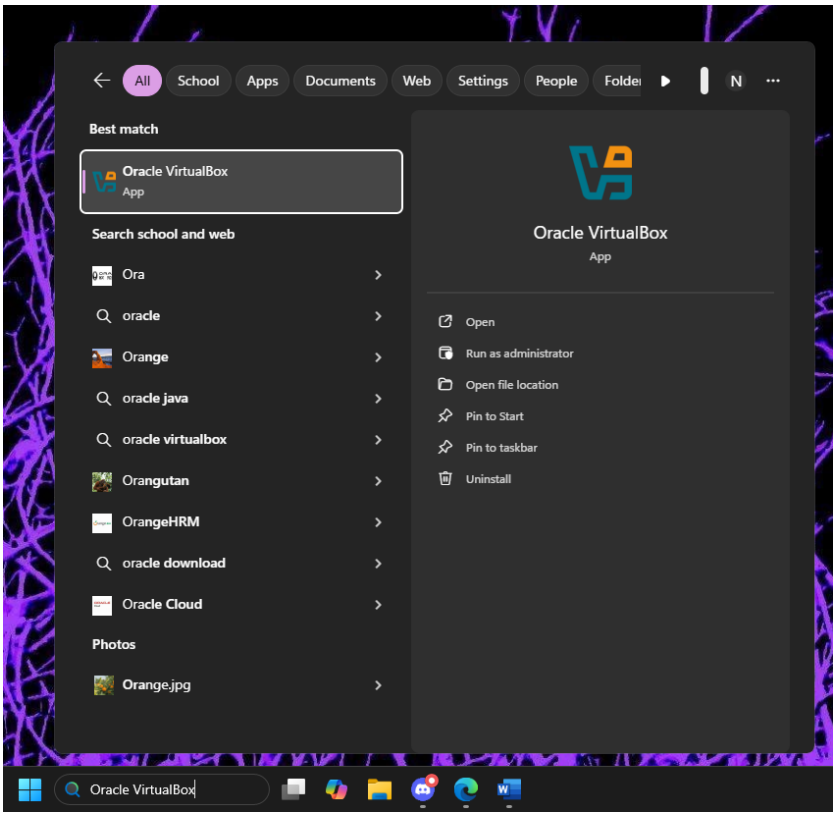

Figure 50: Screenshot of launching Oracle VirtualBox.

Step 2: The option button for tools is clicked.

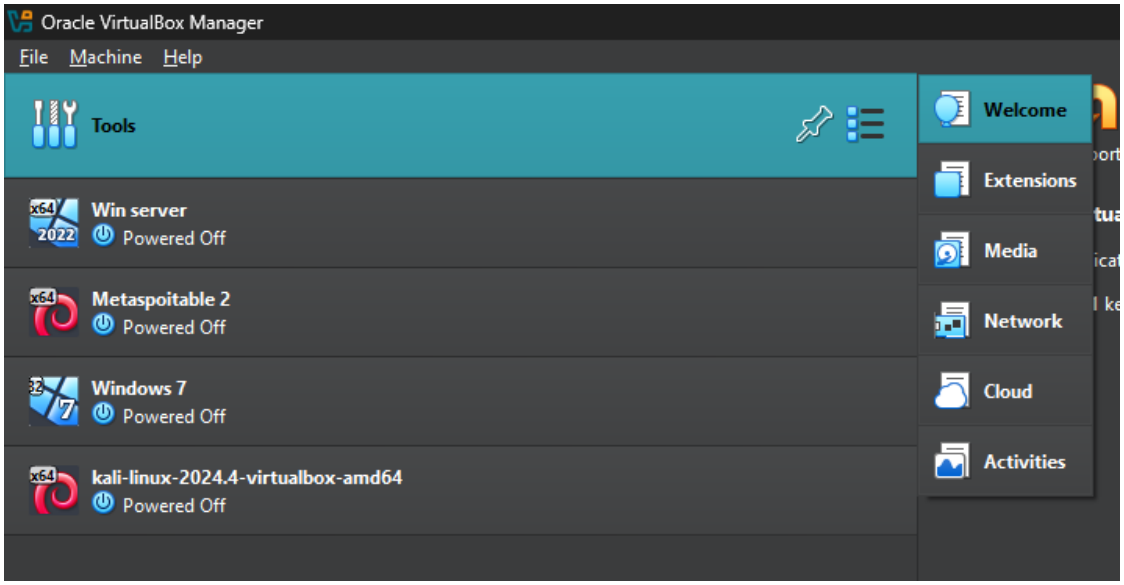

Figure 51: Screenshot of options for tools section.

Step 3: Then the Network section is selected.

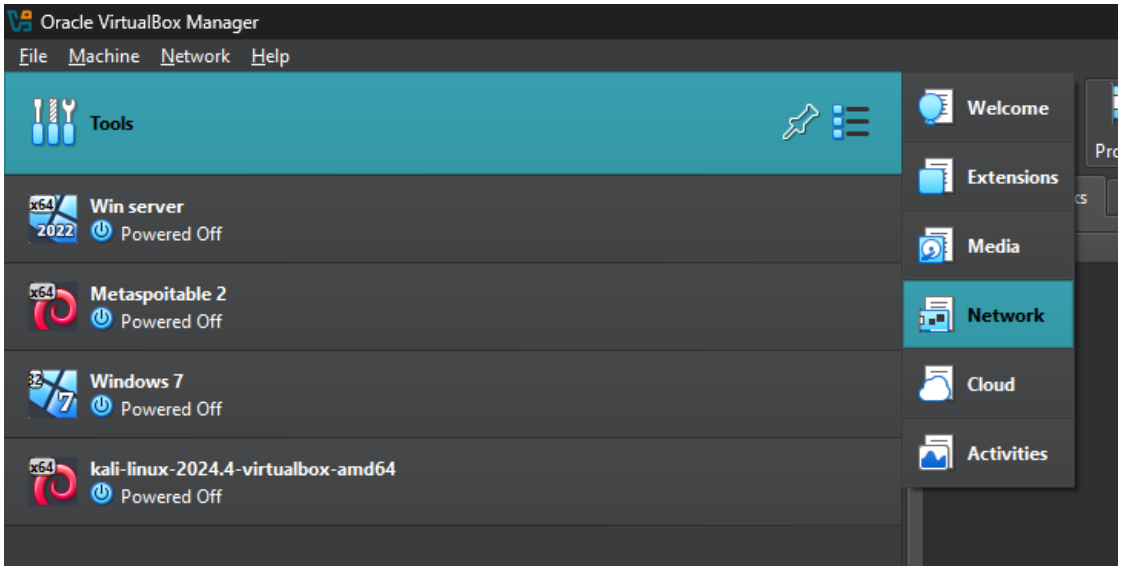

Figure 52: Screenshot of selecting network section.

Step 4: Then a NAT network is created by going to the NAT network tab and clicking the "Create" button on top.

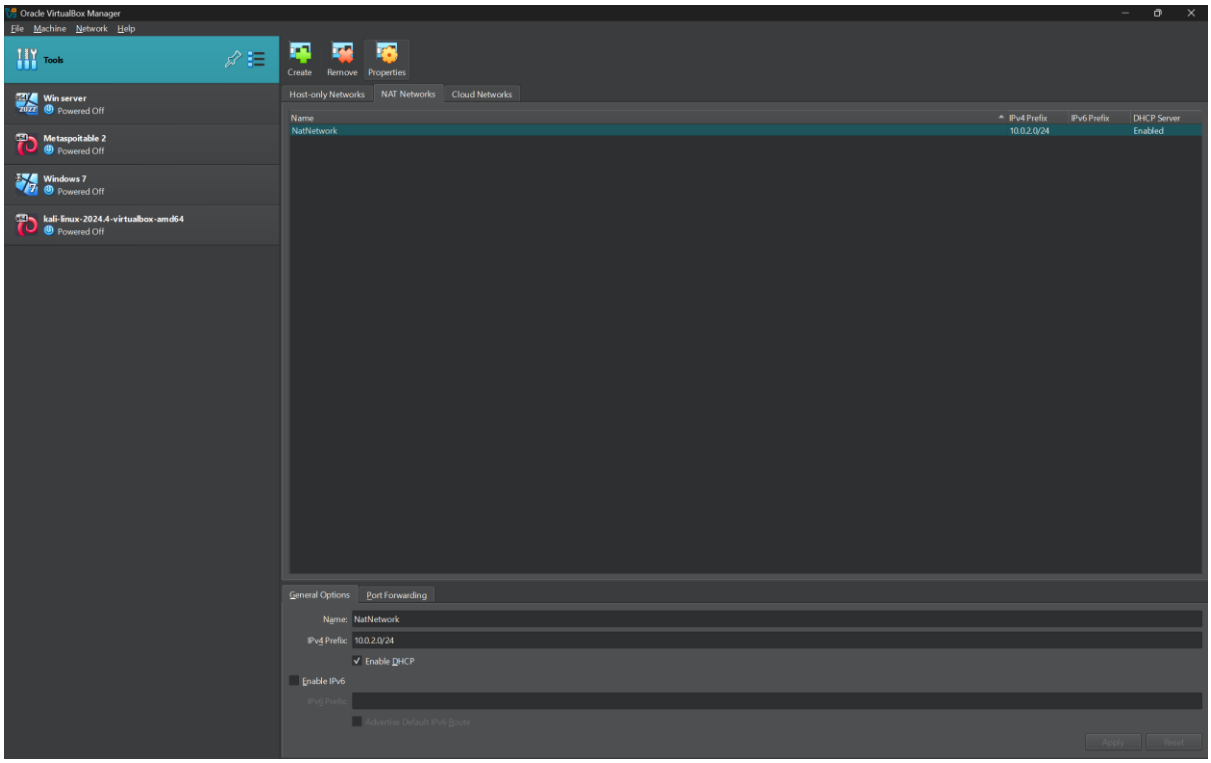

Figure 53: Screenshot of creating a NAT network.

A NAT network is created with the name 'NatNework' is created with IPv4 prefix 10.0.2.0/24 and DHCP is enabled too. The IPv4 prefix can be edited but it won't be changed for this lab environment and DHCP is kept enabled as the other virtual machine that will be connected to this NAT network will need ip assigned automatically.

8.1.2.2. Setting NAT network in virtual machines

Step 1: The Machine that needs to be assigned to the NAT network made above is selected by clicking them in the virtual machine list.

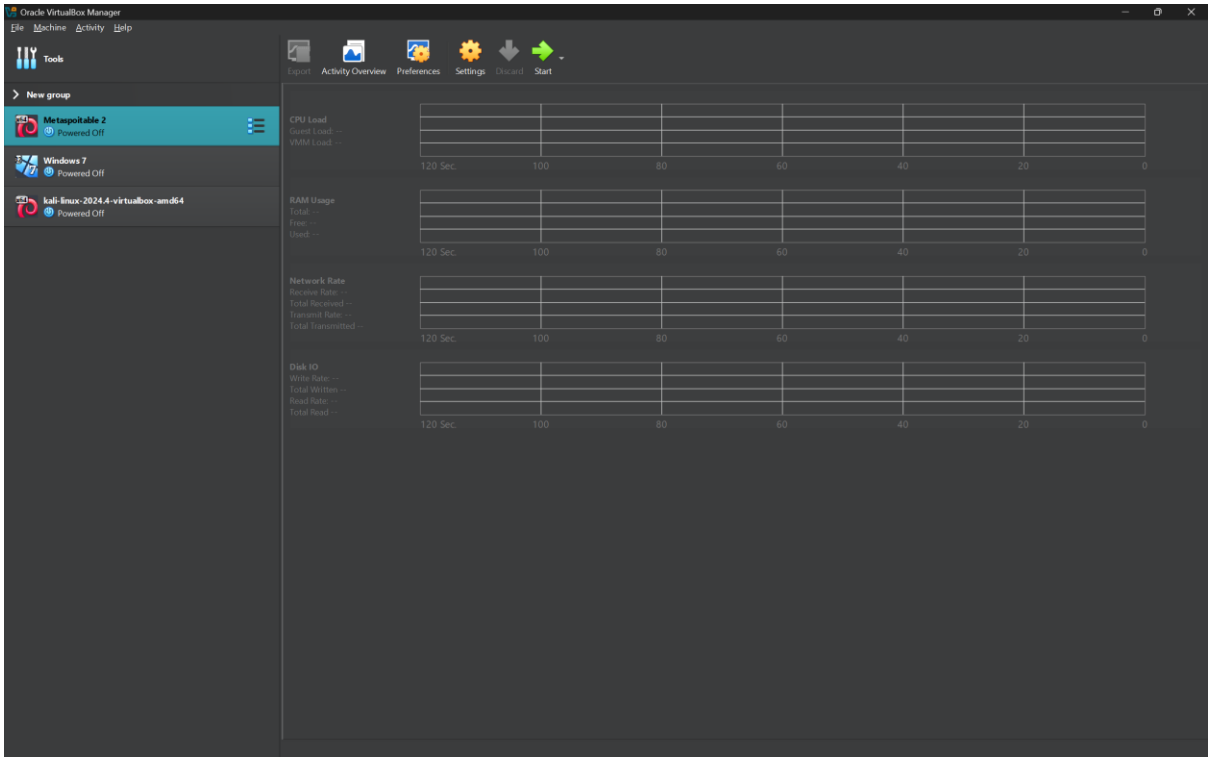

Figure 54: Screenshot of selecting the virtual machine.

Step 2: Then Setting button from the top tab is clicked which will open the preferences for the virtual machine.

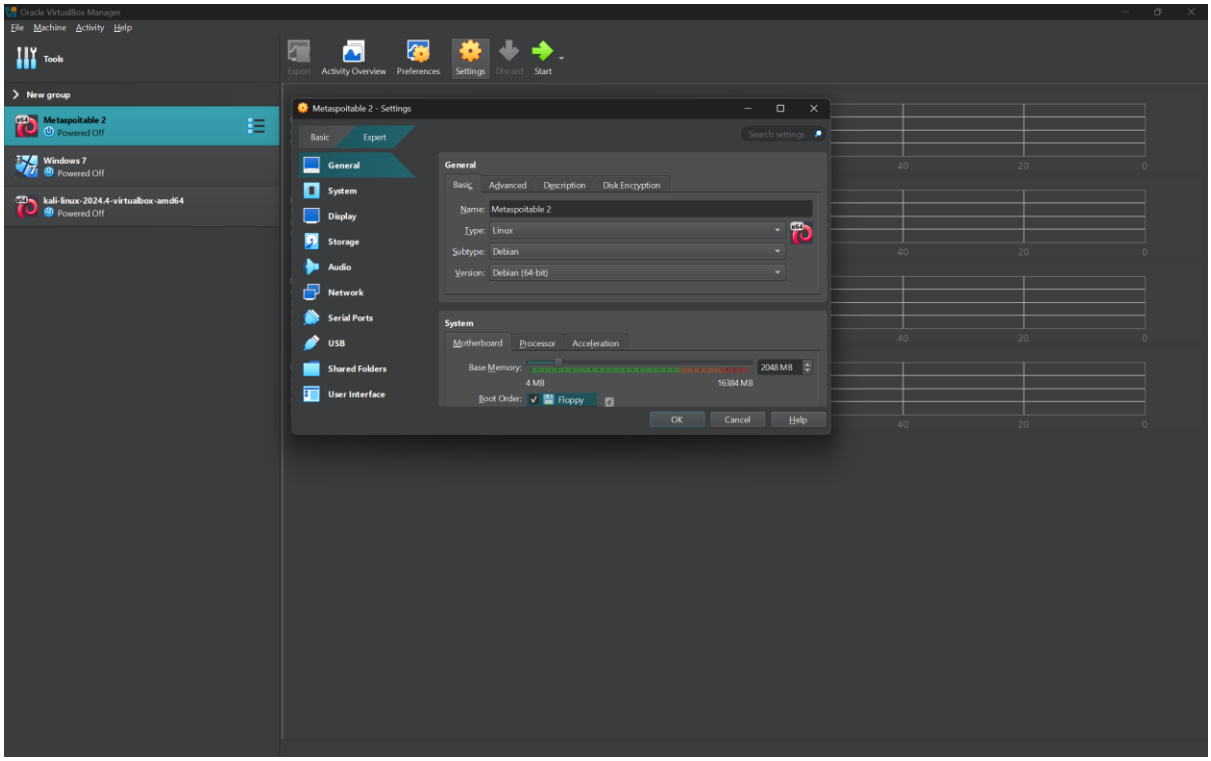

Figure 55: Screenshot of opening preferences for the virtual machine.

Step 3: Then the network tab is clicked, and the adapter setting is changed from NAT to NAT network in ‘Attached to:’ section and the NAT network name is set to the NAT network that was made earlier.

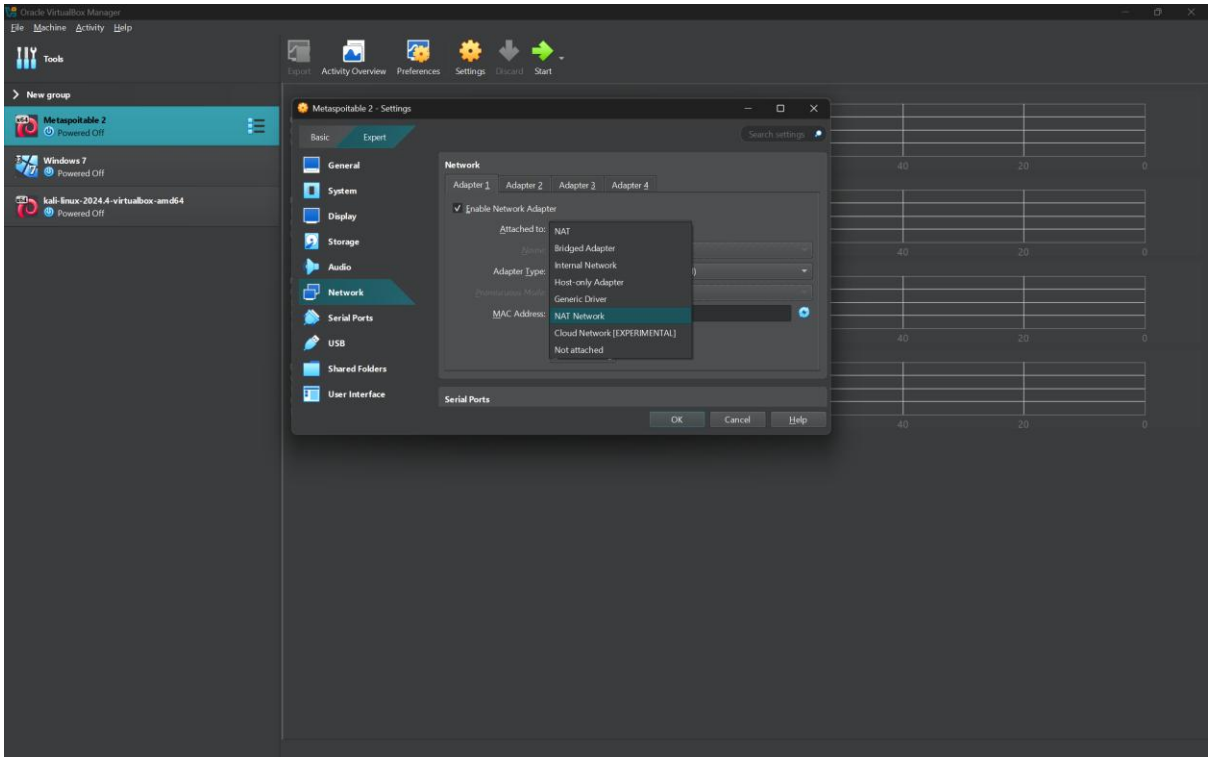

Figure 56: Screenshot of changing adapter setting to NAT network.

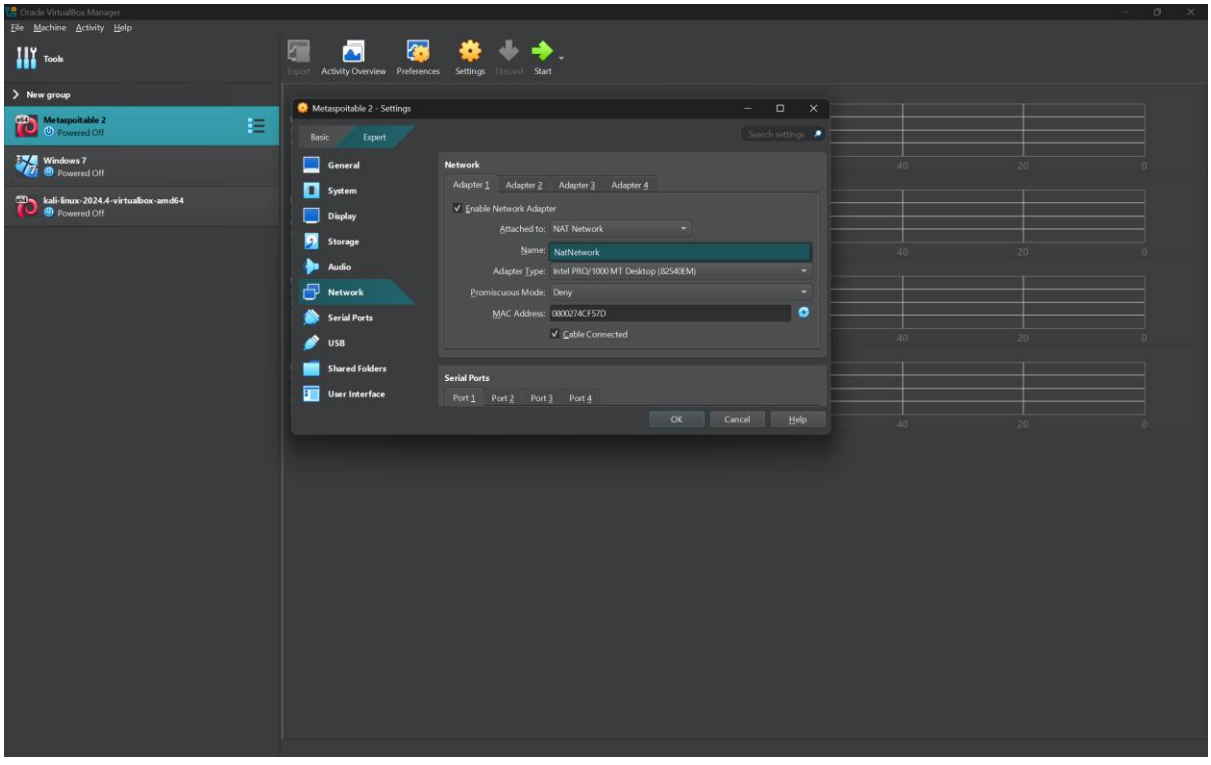

Figure 57: Screenshot of setting NAT network name.

Step 4: The same steps are done to Windows 7 and Kali Linux, and the NAT Network name is set to the NAT network that was made earlier.

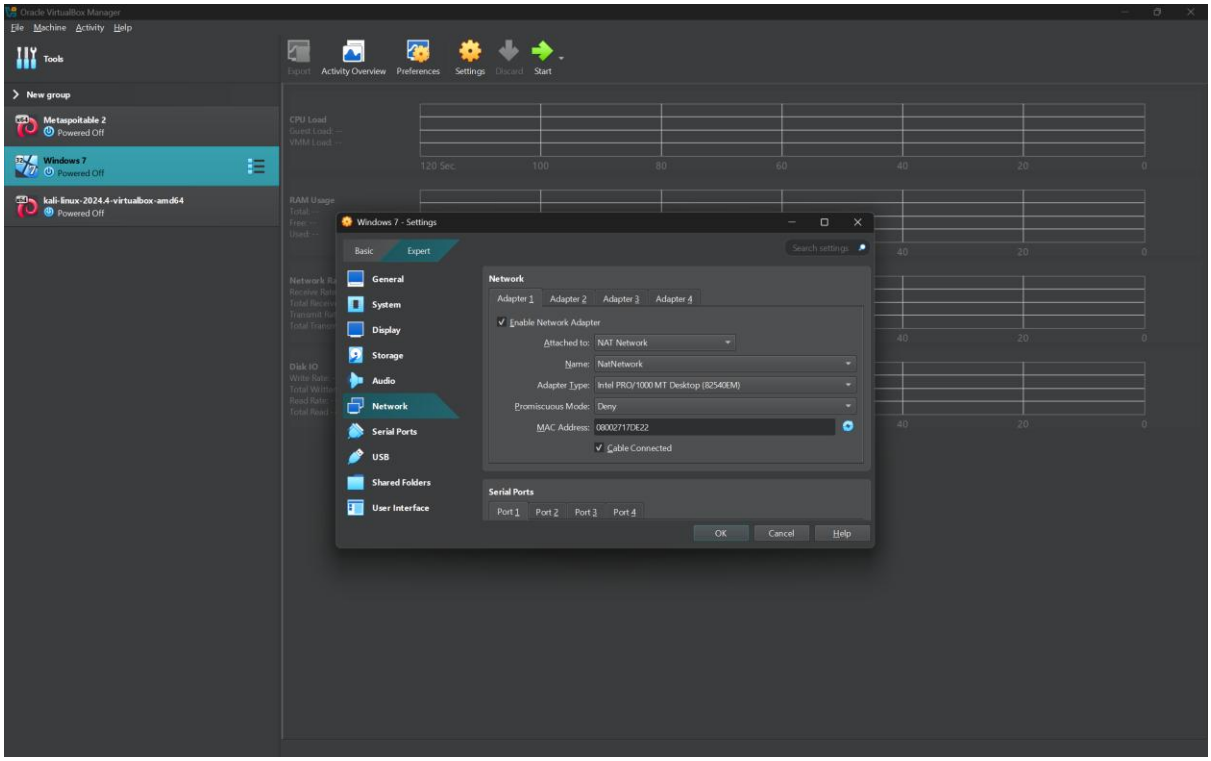

Figure 58: Screenshot of setting NAT network for Windows 7.

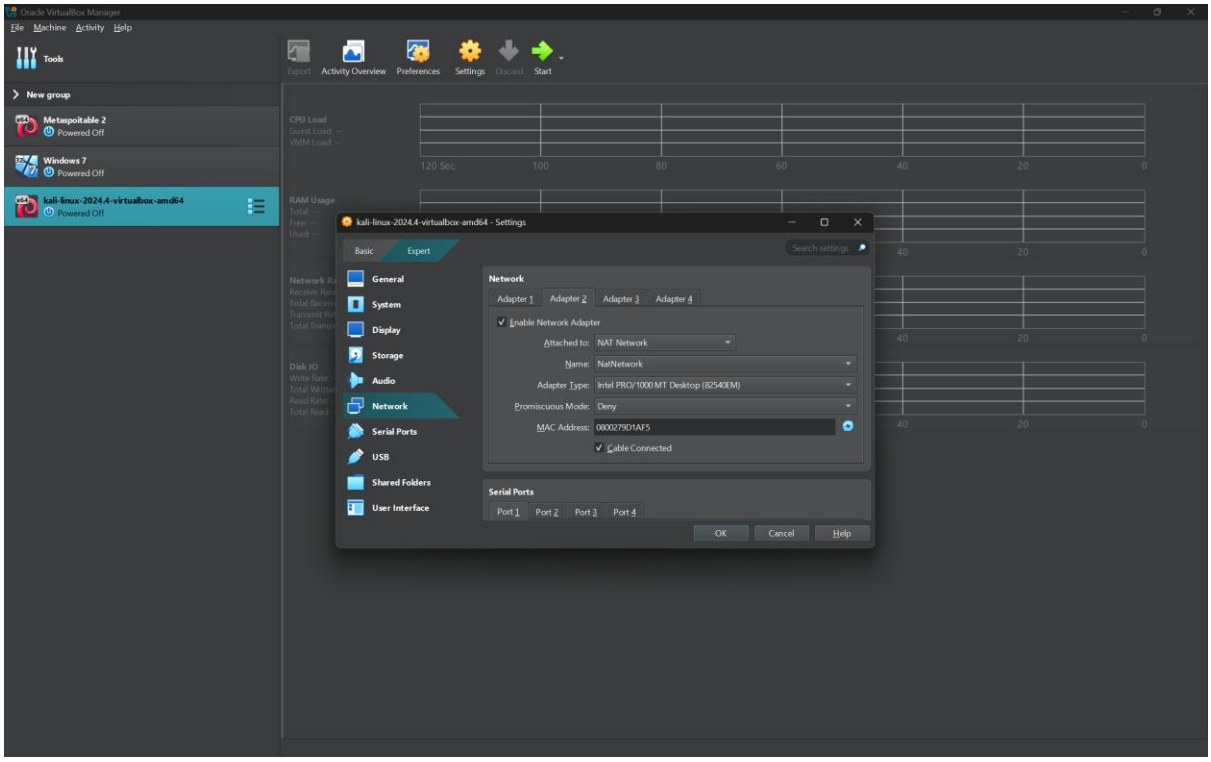

Figure 59: Screenshot of setting NAT network for Kali Linux.