Swinburne University of Technology

Faculty of Science, Engineering and Technology

ASSIGNMENT AND PROJECT COVER SHEET

Unit Code: COS30015 Unit Title: IT Security

Assignment number and title:Pratical Project Due date: 21th Feburary, 2025

Tutor: Dr.Sam Nguyen Lecturer: Dr.Sam Nguyen

First Name: Lau Student ID: 104198996

Other names: Ngoc Quyen

To be completed if this is an INDIVIDUAL ASSIGNMENT
I claim that this is individual assignment and there is no collaborate amount peers during the completion of this assignment.

Signature: 

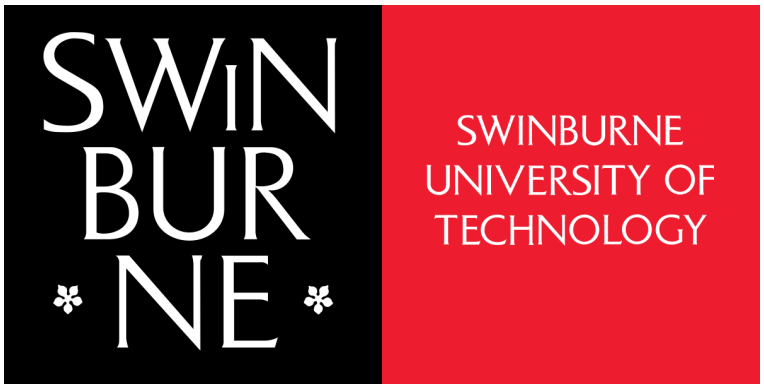
Marker's comments:

Total Mark:

Extension certification:

This assignment has been given an extension and is now due on

Signature of Convener: Date: / 2025



COS30015 - IT SECURITY

SWINBURNE UNIVERSITY OF TECHNOLOGY

Student Name:
Lau Ngoc Quyen (ID: 104198996)

Date: February 21, 2025

1. Introduction

In this assignment, I will conduct an in-depth exploration of the most prevalent cybersecurity threat **ARP spoofing and Phishing Attack**. For simulating attacks, penetration testing tools will be used to simulate the poisoning and attacks, mostly **Ettercap**, an amazing tool for redirecting victim traffic in order to alter communication between the victim and websites. Besides, **Setoolkit**, also known as "Social Engineering Toolkit", will be employed to trap users and capture sensitive information like passwords, user details, or even credit card details. On the defensive side, I will analyze and examine the incredible effectiveness of **Wireshark**, an open-source monitor and show network traffic information in real time. It is very helpful for studying network protocols, resolving network problems, and guaranteeing network security.

Background

Phishing and **ARP spoofing** are the **"evil twins"** for fraudulent practice, one for camouflage and the other for disruption. These are dangerous attack techniques in which attackers exploit weaknesses in the network protocol, sending out forged ARP responses in order to fool both the router and the victim to connect to the attacker's machine. This allows the attacker to intercept traffic meant for the targeted device, enabling sniffing or even man-in-the-middle attacks. Phishing websites are commonly used to trick users into revealing sensitive information by mimicking legitimate sites.

When combined, these techniques create an extremely powerful attack vector. **ARP spoofing** enables the hacker to redirect victim traffic to an imitation and delicate website, while **Phishing** domain expropriates sensitive information such as login credentials, credit card numbers, and most importantly, personal data.

Justification for Choosing Threat and Defensive Technique

ARP Poisoning: The primary reasons for choosing ARP spoofing and phishing are due to its widely used terms in the cybersecurity field, not only due to its high effectiveness, but also their success rates are alarmingly high. They do not require advanced technical levels but still can cause significant harm to unaware victims. *ARP (Address Resolution Protocol)* lacks authentication, making it vulnerable to threats. Attackers can intercept, alter, or even "reroute" the network traffic by manipulating updating ARP tables. Credential theft and *man-in-the-middle (MitM)* attacks are frequent usage cases. Once attackers break into the network, they can escalate privileges and steal all the unauthorized access.

Phishing: A hacking skill exploiting, and manipulating human psychology rather than technical vulnerabilities. Attackers use deceptive emails, fake websites, and malicious

attachments to steal illegal data. Even with high-security in place, users often fear urgency, which makes them panic, horrified against urgency and lead to zero self-awareness in decision-making.

Defensive Strategies: Effectively and real-time detecting phishing attempts by analyzing DNS, HTTP, and TLS traffic. Preventing ARP spoofing by monitoring ARP traffic anomalies and blocking suspicious network behavior using Virtual Private Network(VPN), which ignore the spoofed ARP packets.

Scenario Summarization

A demonstration of how attackers can use ARP spoofing and phishing to harvest personal and illegal information while showing how a security tool (Wireshark) can detect and implement changing methods to prevent such dangerous attacks.

2. Attack Tools

Setoolkit (Social Engineering Toolkit)

An open-source penetration testing tool called **Setoolkit** is used to model social engineering assaults. Web phishing is one of the many unique attack vectors available in SET that let you rapidly create a convincing assault. It will be used in this study to construct an imitation website that mirrors an authentic one in order to trick victims into revealing their login credentials..

Ettercap (ARP Spoofing and man-in-the-middle Attack)

Ettercap is a powerful network security tool designed for imp man-in-the-middle (MITM) attacks on local networks. It allows users to intercept, analyze, and modify network traffic in real time, making it a popular choice for penetration testing and security assessments, particularly through ARP spoofing techniques.

Wireshark (Threat Monitoring and Detecting)

Wireshark is a widely used network protocol analyzer that allows users to capture and inspect network traffic in real-time. Help users analyzing protocols and detect potential threats.

Running Attack Tools

To initiate the process, I began by examining the network routing table using `route-n` command to identify the default gateway.

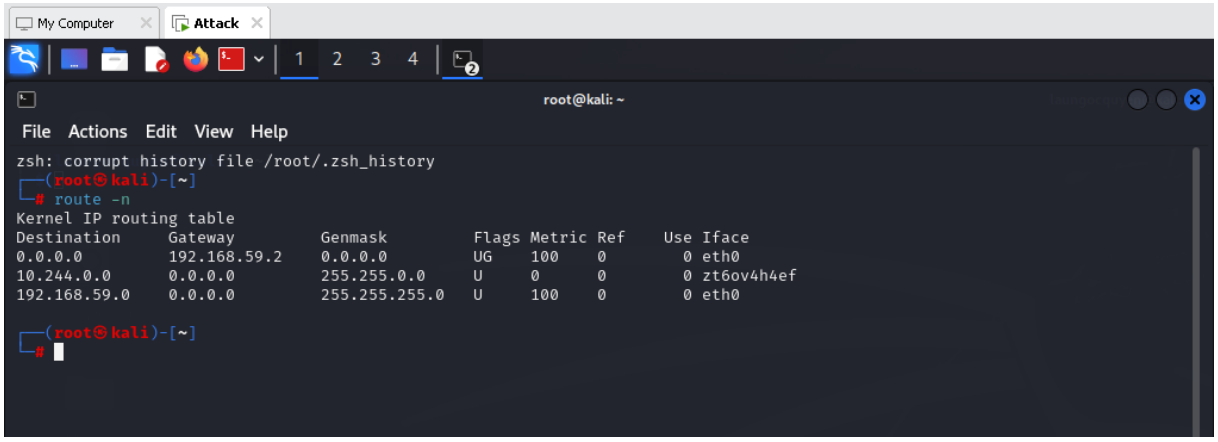


Figure 1: Checking the default gateway

This step was crucial to determine the target MAC address that the attacker is trying to mimic for spoofing. Once the default gateway was identified, I enabled IP forwarding using the command `sysctl -w net.ipv4.ip_forward=1`. When poisoning the ARP cache, A and B start sending datagrams to M that have the MAC Address of M but the IP addresses of B and A, respectively. So these datagrams are directed at M in layer 2 (Ethernet) but directed at the other device in layer 3 (IP). In order to send these datagrams out to the layer 3 recipient (according to IP address), M has to do IP forwarding for executing a Man-in-the-Middle (MITM) attack.

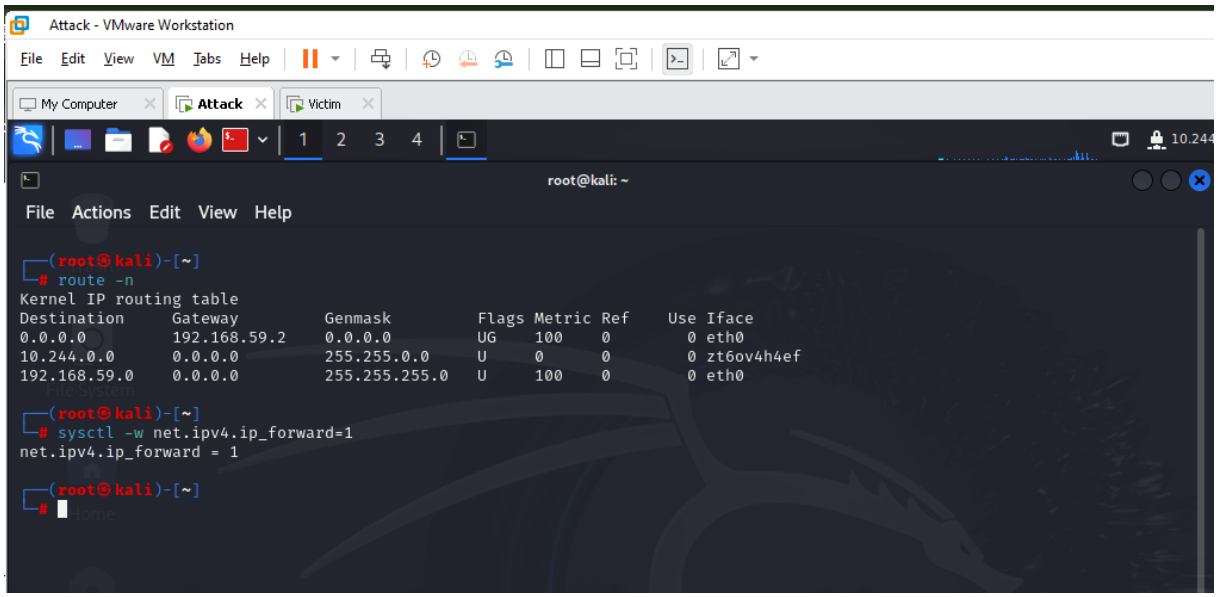


Figure 2: IP forwarding

Next, I located the directory where `etter.dns` was placed, which would allow the at-

tacker to modify the direct DNS to spoof.

Figure 3: etter.dns location and modification

Specifically, I mapped the domain `github.com` to the IP address `192.168.59.133`, which would redirect the victim's traffic to a phishing website that I will create later on.

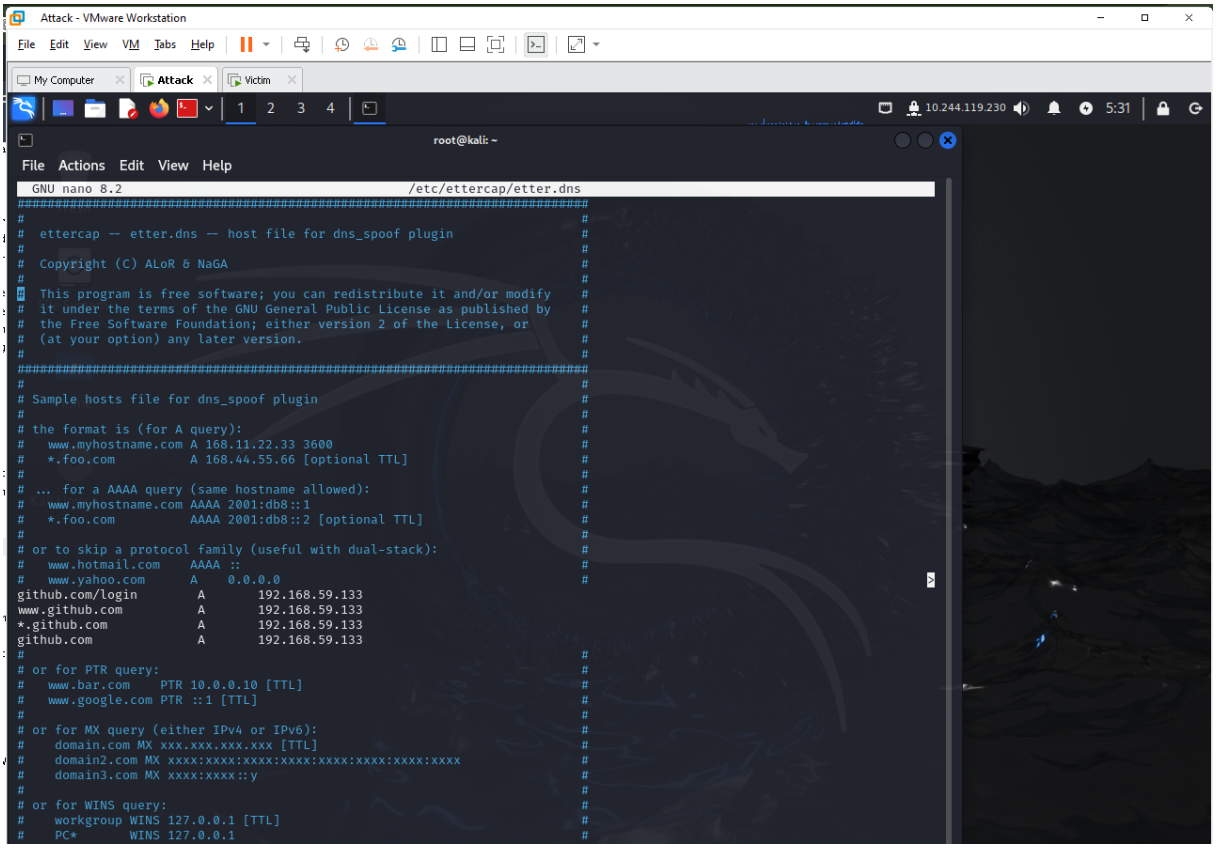


Figure 4: Mapping valid domain with phishing IP address

With the DNS setting in place, I opened the attack tool called `Ettercap` to scan the victim's host and their gateway.

Figure 5: Ettercap interface

Once the target was selected (192.168.59.132 , victim's IP address), I implemented sniffing using ARP poisoning, which allowed me to intercept and manipulate traffic between the victim's DNS queries for github.com that redirected to my phishing IP address.

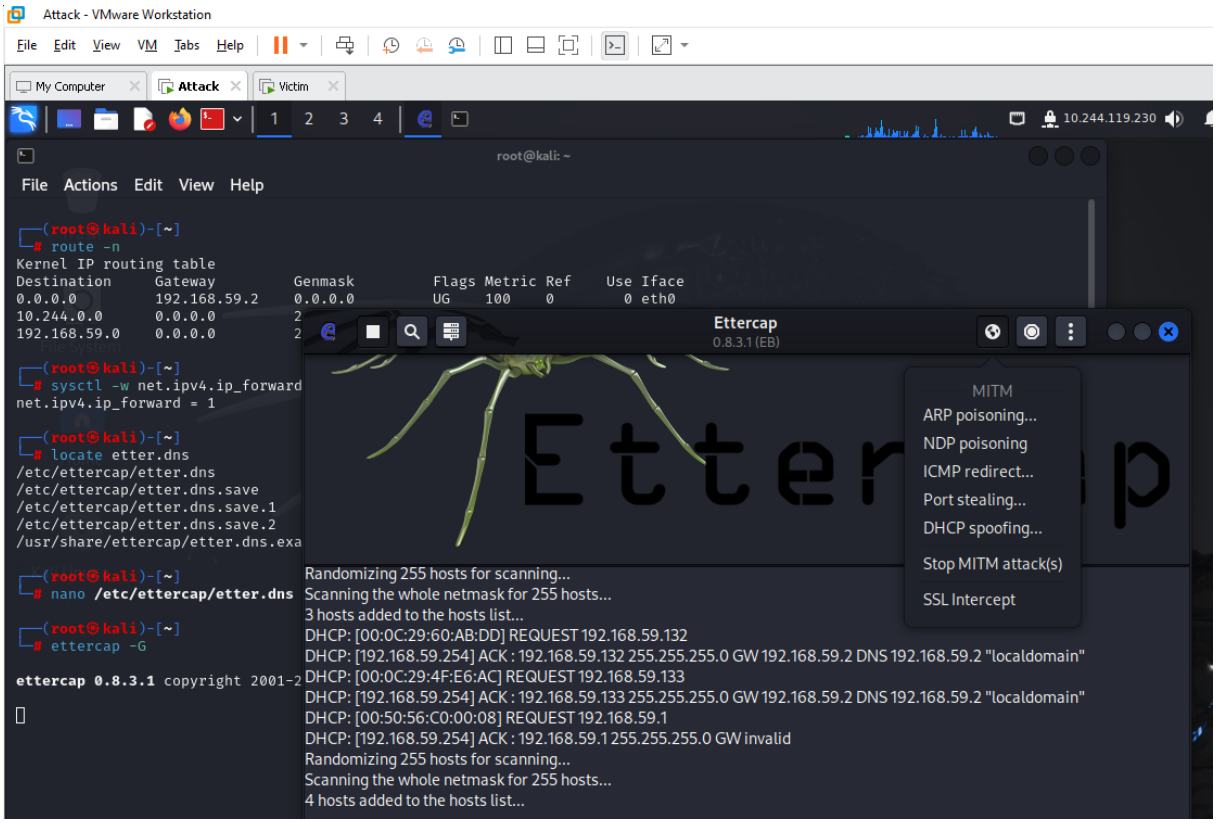


Figure 6: ARP Poisoning

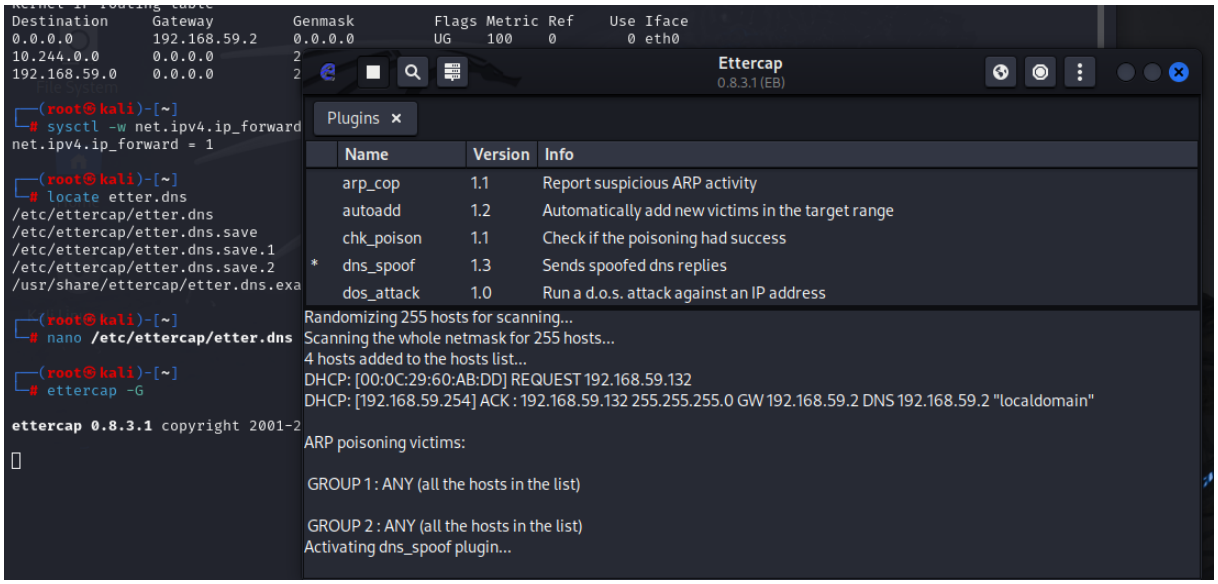


Figure 7: Activate DNS spoofing

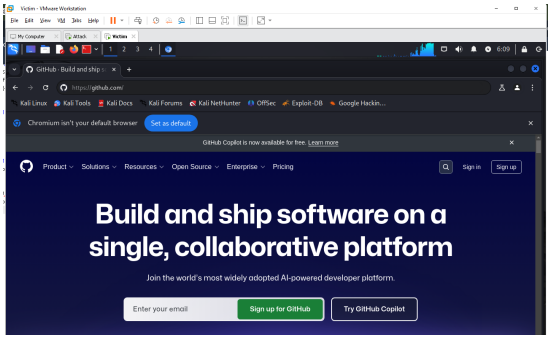


Figure 8: Before the attack

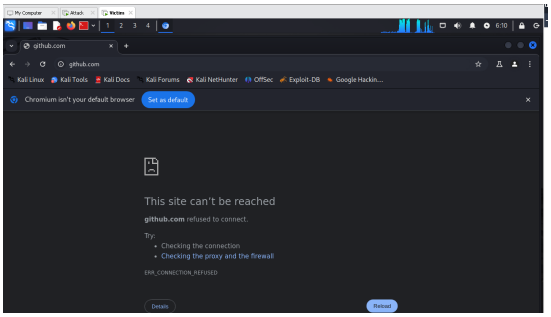


Figure 9: After the attack

To verify the successful poisoning and spoofing phase, I monitored the victim's VMware before and after being poisoned, which led to illegal information harvesting. Prior ti executing **Ettercap**, the victim was able the access `github.com` without any issue. However, after the attack was achieved succesfully, the victim's connection to the site was refused, confirming that the DNS spoofing and ARP poisoning were effective in disrupting their access.

Following this, I created a phishing website designed to mimic the legitimate GitHub login page using the **Social-Engineer Toolkit (SEToolkit)**. This replica page was hosted on my server at `192.168.59.133`, ensuring that any credentials entered by the victim would be captured. With the phishing site in place, I continued to monitor the victim's activity, waiting for them to attempt to log in to the spoofed GitHub page.

Figure 10: Setoolkit(Muti-function phishing tool)

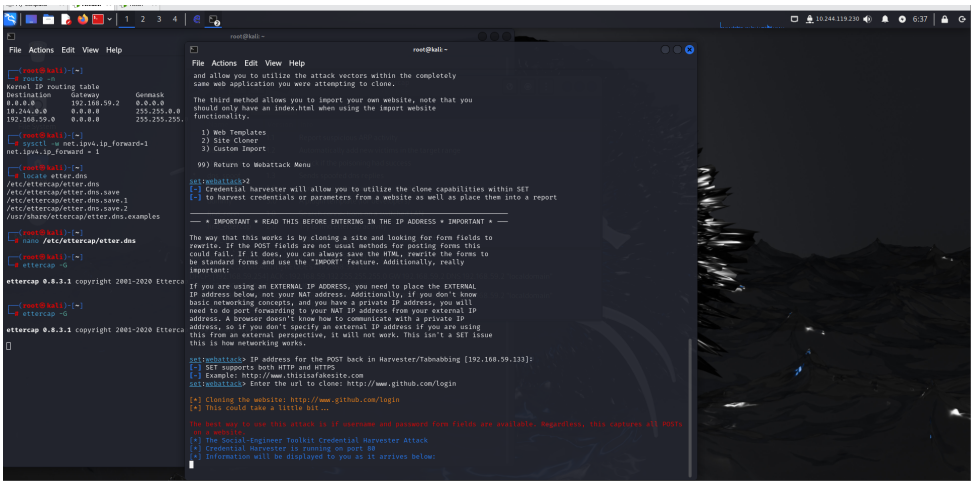


Figure 11: Fake website succesfully created

The phishing page, which were flawlessly mirrored the original `github.com` login page, prompted the victim to re-enter their login credentials

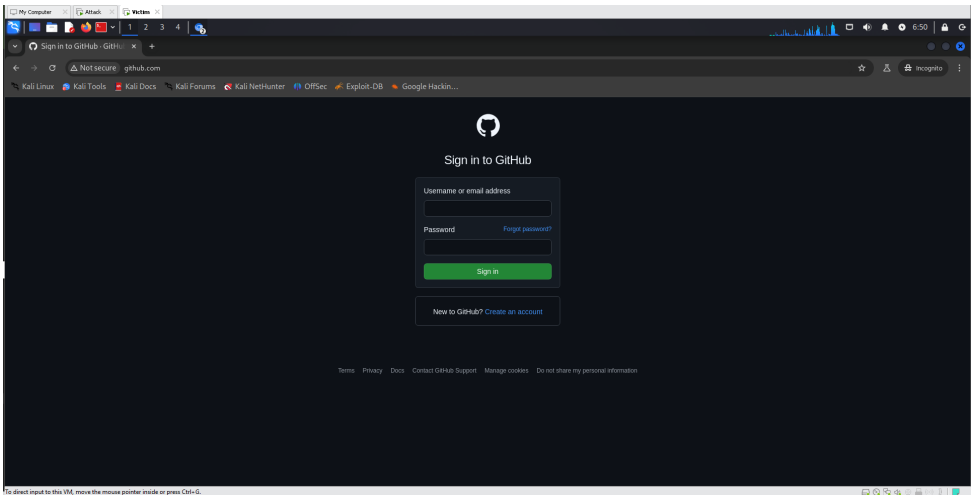


Figure 12: HTTP Phishing Github login page

Once the victim submitted their username and password, these sensitive credentials were imediately sent to my server at the IP address `192.168.59.133`, giving me fully access to the victim account and the abilities to capture all the important information.

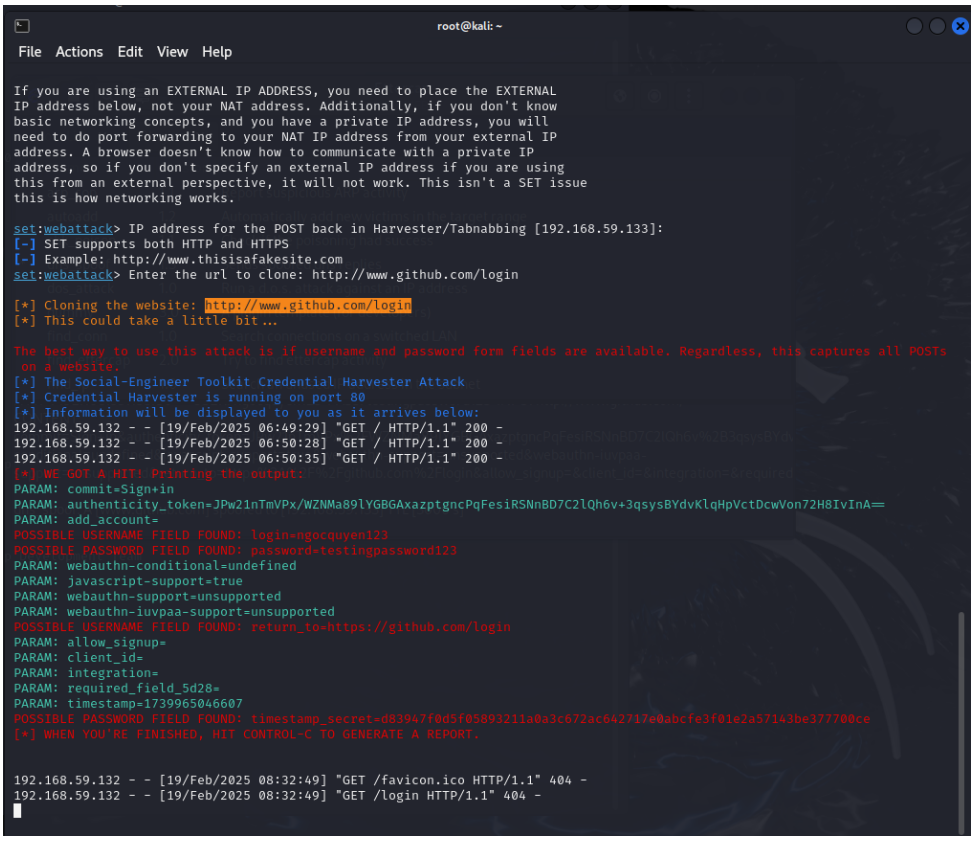


Figure 13: Login Information

Running Defense Tools

To investigate the suspicous spoof, i open `wireshark` and start capturing all the phishing packets.

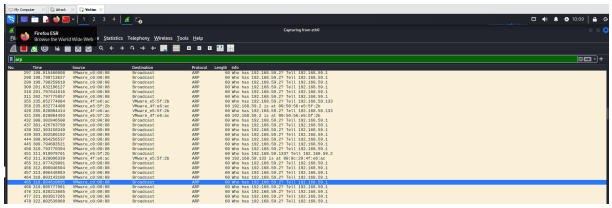


Figure 14: Before Being ARP Poisoned

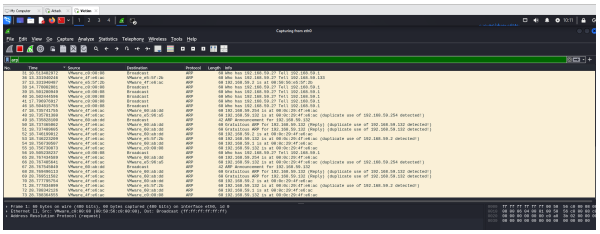


Figure 15: After Being ARP Poisoned

There appeared an aggressive duplicate conflict of ARP replies, where the routers's IP `192.168.59.1` is being associated with two different MAC addresses. One of which belongs to an unknown device. This indicates ARP spoofing. It was a legitimate request to `github.com` is being redirected to `192.168.59.133`, which is a phishing ip address that mimic as `github.com`. By manually set static ARP entries, attacker cannot manipulate ARP tables thourgh spoofing since entries do not change dynamically. Moreover, this method also ensuring that only predefined MAC addresses comunicate with specific IP address.

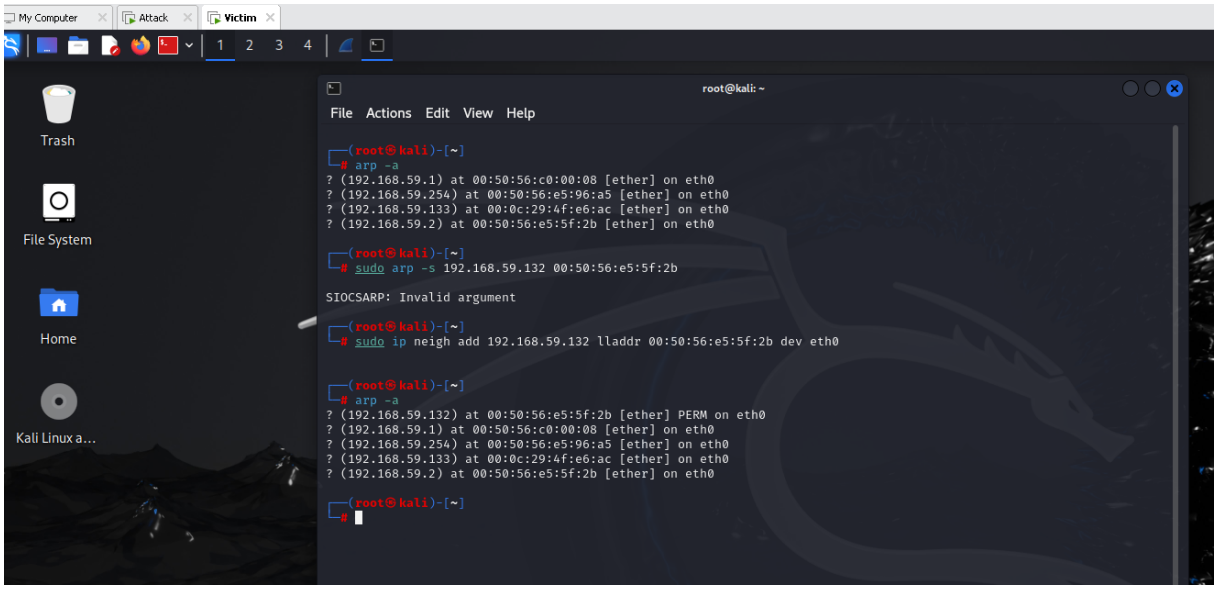


Figure 16: Static ARP Entries on Different Systems

3. Evaluation and Analysis

3.1 Attack Effectiveness

The attack illustration succcessfull in:

1. Intercepting network traffic with ARP Poisoning and DNS Spoofing
2. Redirecting victim traffic to phishing website
3. Capture login credentials from the spoofed Github clone page

Key observations:

1. ARP poisoning was effectively redirecting traffic
2. Supicous website successfully imitated the legitmate Github login page
3. Credentials harvest was achieved without victim awareness

3.2 Defense Effectiveness

The defense obseravtion and timely prevention showed varying degrees of effectiveness:

1. Successfully identified ARP spoofing packets
2. Detected suspicous MAC address conflicts
3. Real-time monitoring of network anomalies

Key observations:

1. Effectively avoided ARP table redirect
2. Blocked unauthorized MAC-IP addresses
3. Reduced the attack surface for ARP spoofing

Could been improved

1. Automatically log illustration while running.
2. Automatically analyze and block all the malicious address across the traffic.

4. Essential 8 Mitigations

Patch Applications

- Keep systems and applications manually updated
- Address known vulnerabilities

Multi-Factor Authentication

- Implement MFA for critical systems
- Reduce impact of credential theft

User Training

- Educate users about phishing threats
- Promote security awareness

Conclusion

This demontration highlighted the effectiveness of the combination of ARP spoofing and Website phishing attacks while also showing the importance of network monitoring and self-awareness against cyber-threat. The success of the attack scenario embraced the need for mutiple defense implementation, including both technicals control and user awareness enhancements.

References

[1] Imperva, "ARP Spoofing," Imperva Learning Center, 2023. [Online]. Available: https://www.imperva.com/learn/application-security/arp-spoofing/ pages

[2] J. Jaymon, "Conociendo un ataque de DNS Spoofing & Phishing," Jaymon Security, 2023. [Online]. Available: https://jaymonsecurity.com/conociendo-un-ataque-de-dns-spoofing-phishing/ pages

[3] Unix & Linux Stack Exchange, "What exactly happens when I enable net.ipv4.ip_forward=1," Stack Exchange, 2021. [Online]. Available: https://unix.stackexchange.com/questions/673573/what-exactly-happens-when-i-enable-net-ipv4-ip-forward-1 pages

[4] BKNS, "DNS Spoofing là gì?" BKNS Security, 2023. [Online]. Available: https://www.bkns.vn/dns-spoofing-la-gi.html pages

[5] Okta, "What is ARP Poisoning?" Okta Identity 101, 2023. [Online]. Available: https://www.okta.com/identity-101/arp-poisoning/ pages

[6] Offensive Security, "Social Engineering Toolkit (SET)," Kali Linux Tools, 2023. [Online]. Available: https://www.kali.org/tools/set/ pages

[7] "Social Engineering Setoolkit," StudoVN, 2023. [Online]. Available: https://www.studocu.vn/vn/document/truong-thpt-chuyen-ngoai-ngu-dai-hoc-quoc-gia-ha-noi/giao-duc-cong-dan-12/social-engineering-setoolkit/94311687 pages

[8] Ettercap Project, "Ettercap Documentation," Ettercap Project Documentation, 2023. [Online]. Available: https://www.ettercap-project.org/ pages

[9] Wireshark Foundation, "Wireshark User's Guide," Wireshark Documentation, 2023. [Online]. Available: https://www.wireshark.org/docs/ pages

[10] D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," in The Second USENIX Workshop on Electronic Commerce Proceedings, Berkeley, CA, USA, 2001. pages

[11] S. Saini and D. Soni, "Detection and Prevention of ARP Poisoning in Dynamic Networks," International Journal of Computer Networks and Applications, vol. 9, no. 2, pp. 154-165, 2022. pages

[12] Australian Cyber Security Centre, "Essential Eight Maturity Model," Australian Signals Directorate, 2023. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/essential-eight pages