Network and System Security

Security Testing and Report (ca2) Securing the Network

Prepared by: Primrose Mncube

Student number: 2022179

Date:

07/05/2025

Table of Contents

Introduction

On this assignment the main goal is to evaluate the security posture for the Jones Café & Bakery who are now on 15 locations by using security testing techniques in a virtual lab environment. I am being tasked with evaluating, testing and suggesting enhancements to the client's current network as a recently appointed security consultant at ISC

To complete the task, I am using sandbox lab setup that will include a few virtual machines that being kali Linux, Metasploitable2, Ubuntu server 24.04 and windows 2016 additionally the tools I will use is Nmap, Metasploit, Wireshark and my lecturers favourite Nessus to look out for vulnerabilities. This report will present findings across a arrange of security tests.

Recommendations to Harden the Network

Patch management

Unpatched Vulnerabilities are a leading cause for a lot of security breaches so ensure that all systems, web server software's, and any installed applications are fully updated. Unpatched vulnerabilities are what attackers usually exploit. (Essex, 2023) So a patch management process would likely be put in place.

Web application Firewall

A web application firewall can help filter and block HHTP traffic to and from the web application, it will protect against common attacks such as SQL injection and XSS by filtering malicious HTTP requests (OWASP,2021). This provides good protection for the new site.

Disable unused ports

Any unnecessary open ports on the server provide potential entry points for attackers as a result the web sever should be reviewed using tools like Nmap to identify and disable unused ports especially if they are not required. Firewalls should be configured to allow only required traffic.

Stronger User Authentication

User account security is very important especially for accounts where there are administrative privileges, I would suggest that they disable shared user accounts additionally enforce strong password policies (minimum length, expiry and complication of the password) (NIST, 2017). The Administrator accounts should be limited and given at role base.

Implement Security logging and monitoring

Enable security logs and keep an eye out for indications of unwanted access. IP addresses that repeatedly fail to log in can automatically banned with tools like Fail2Ban. Furthermore, real-time network traffic monitoring and notifications regarding suspicious activity are possible with intrusion detection systems (IDS) such as Snort (Ward, 2025).

OWASP REPORT

Chosen risk: INJECTION(A03:2025)

Injection vulnerabilities occur when user supplied data is not validated, filtered by the program, leaving it open to threats and allowing malicious input to be executed within the interpreter. Furthermore, malicious data is directly used into SQL statements, commands or stored procedures that then embedding harmful content within queries and increasing the risk of unauthorized access (OWASP, 2021)

How Jones Café and Bakery could be Vulnerable

With Jones café now launching a new online platform that will now allow customers to order through a website connected to an internal database. There is a significant chance of SQL injection if the team has not properly cleaned user inputs such as names, shipping addresses or payment information for example if a user enters malicious SQL code and the back end uses raw queries without validation this could easily give the attacker access to modify the sensitive data

Attack Scenario Diagram

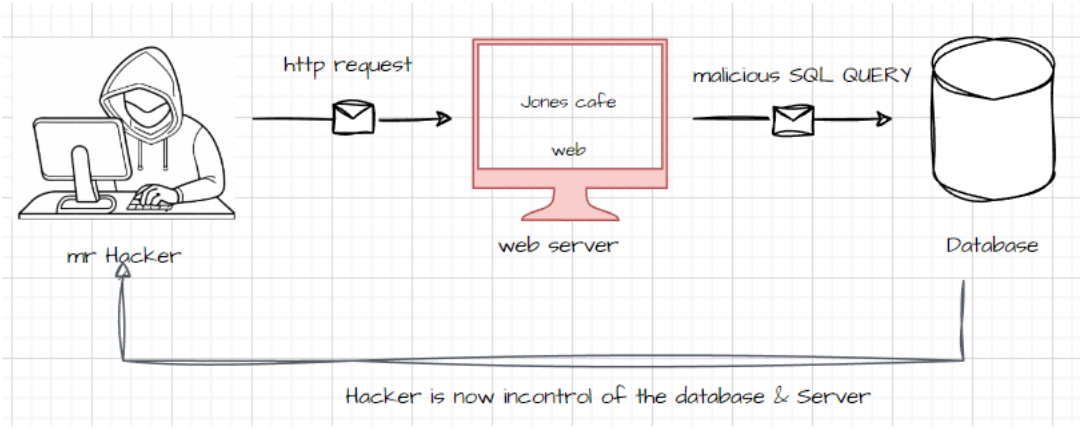

Fig 1: a Flow showing a user submitting a logging, and because the server hasn't been properly cleaned the attacker has gained access

Q2: Attacking a vulnerable Machine

The first step was to let the machines Ping each other to make sure they are reachable

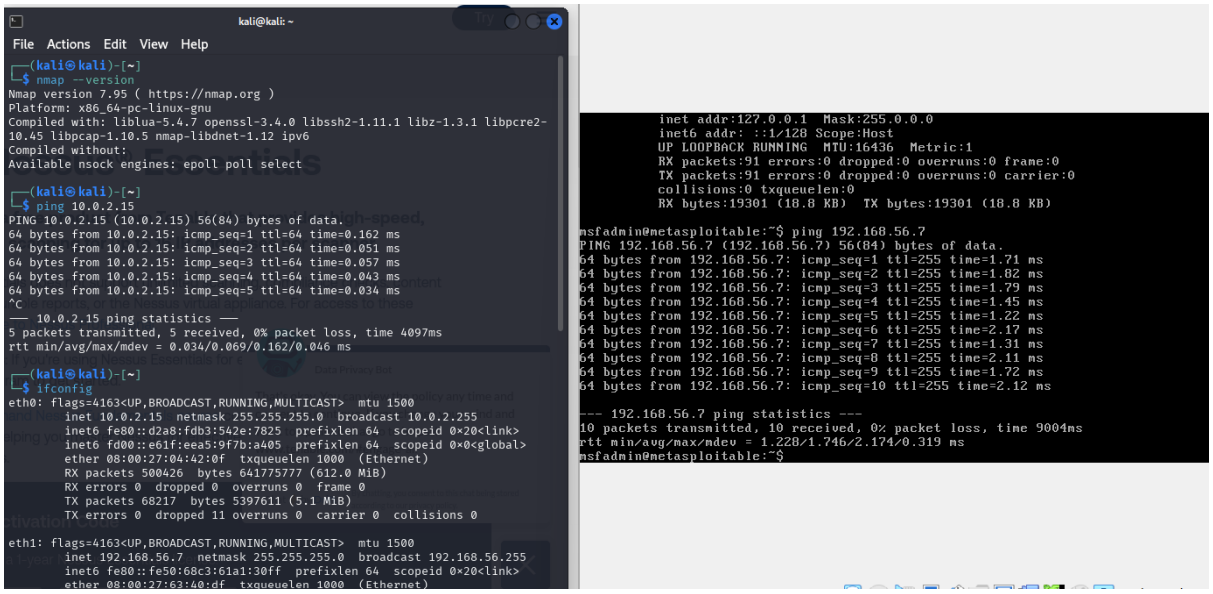

Fig1: Machines can ping one another and I have also just checked tosee the version on Nmap I have on my PC.

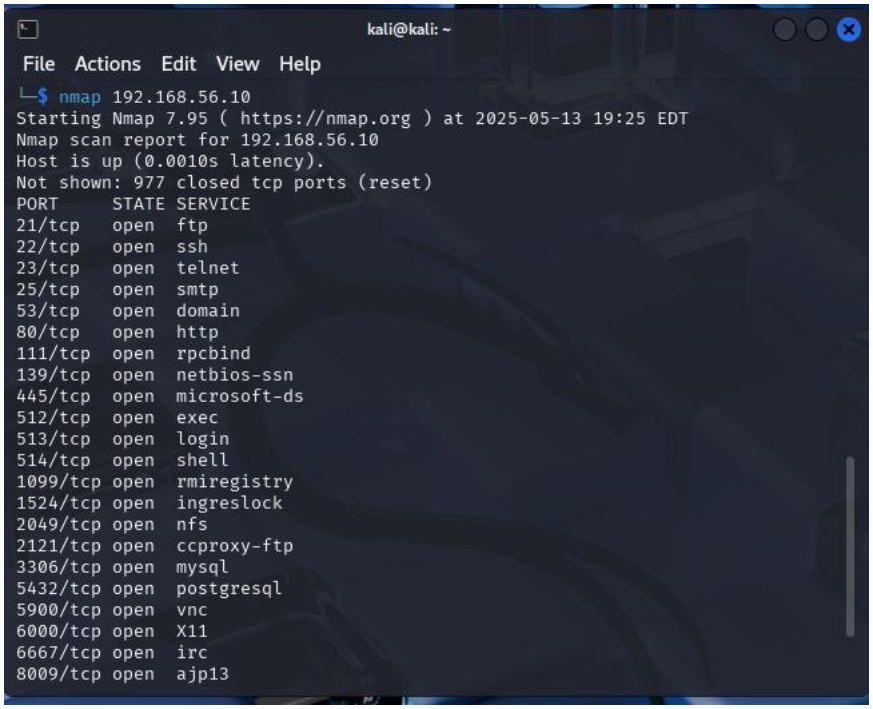

Fig 2: Scanning to see how many ports are open

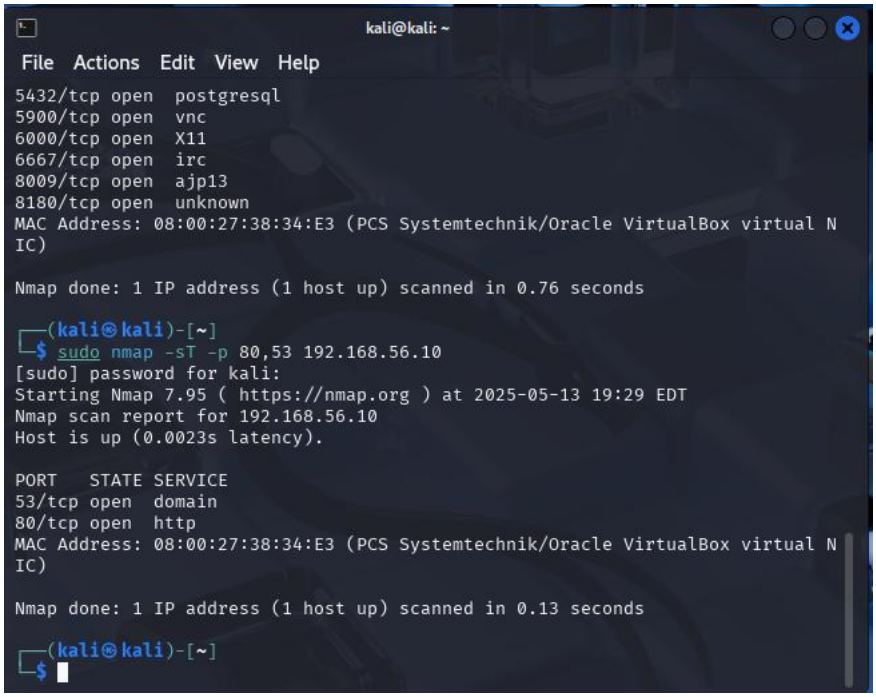

Fig3: Scanning for open ports on all active network hosts, as you'll see its open

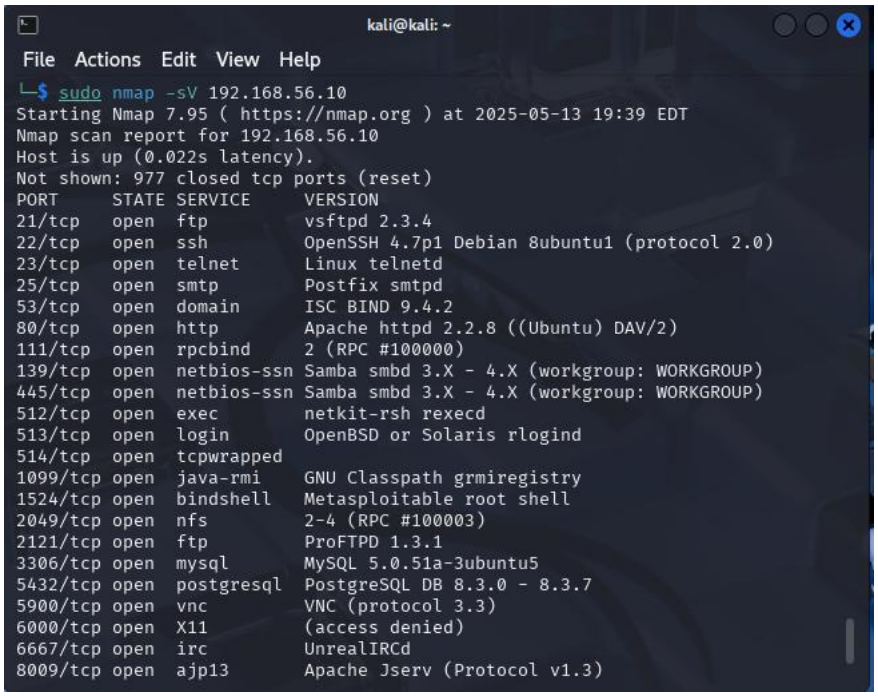

Fig 4: this shows what services, and their versions are running on the ports

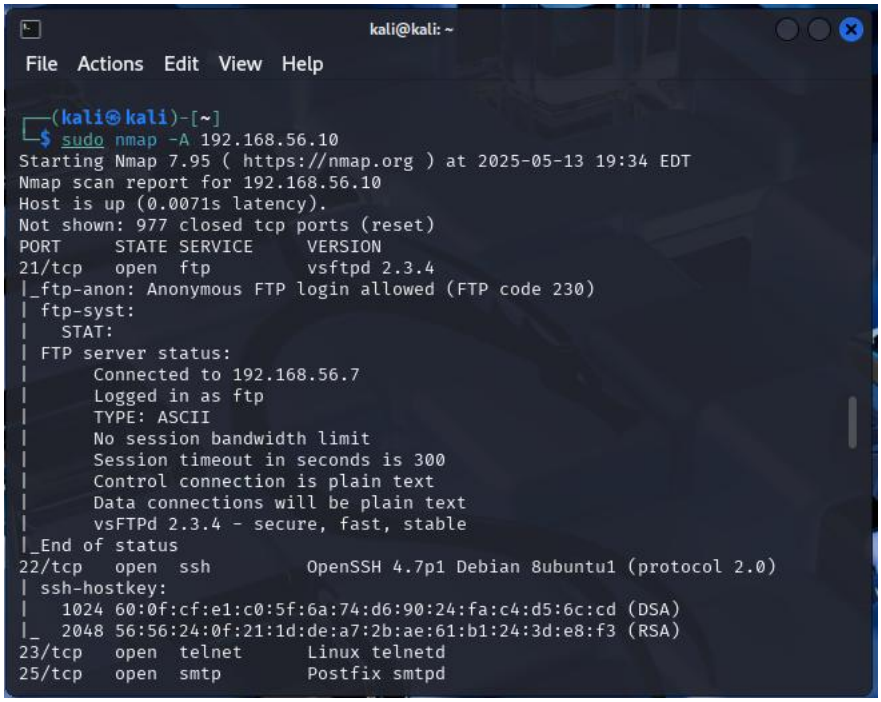

Fig 5: Aggression Scan

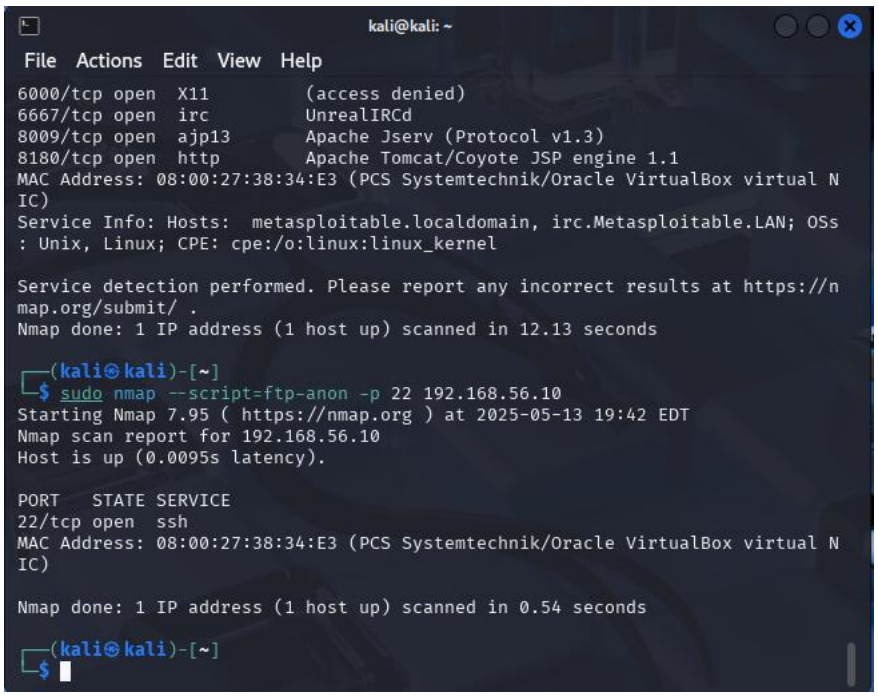

Fig 5: This is to check for any anonymous logins on SSH

Q3b. Demonstrate a Brute Force attack using Kali Linux against a vulnerable VM Metasploit-able Linux

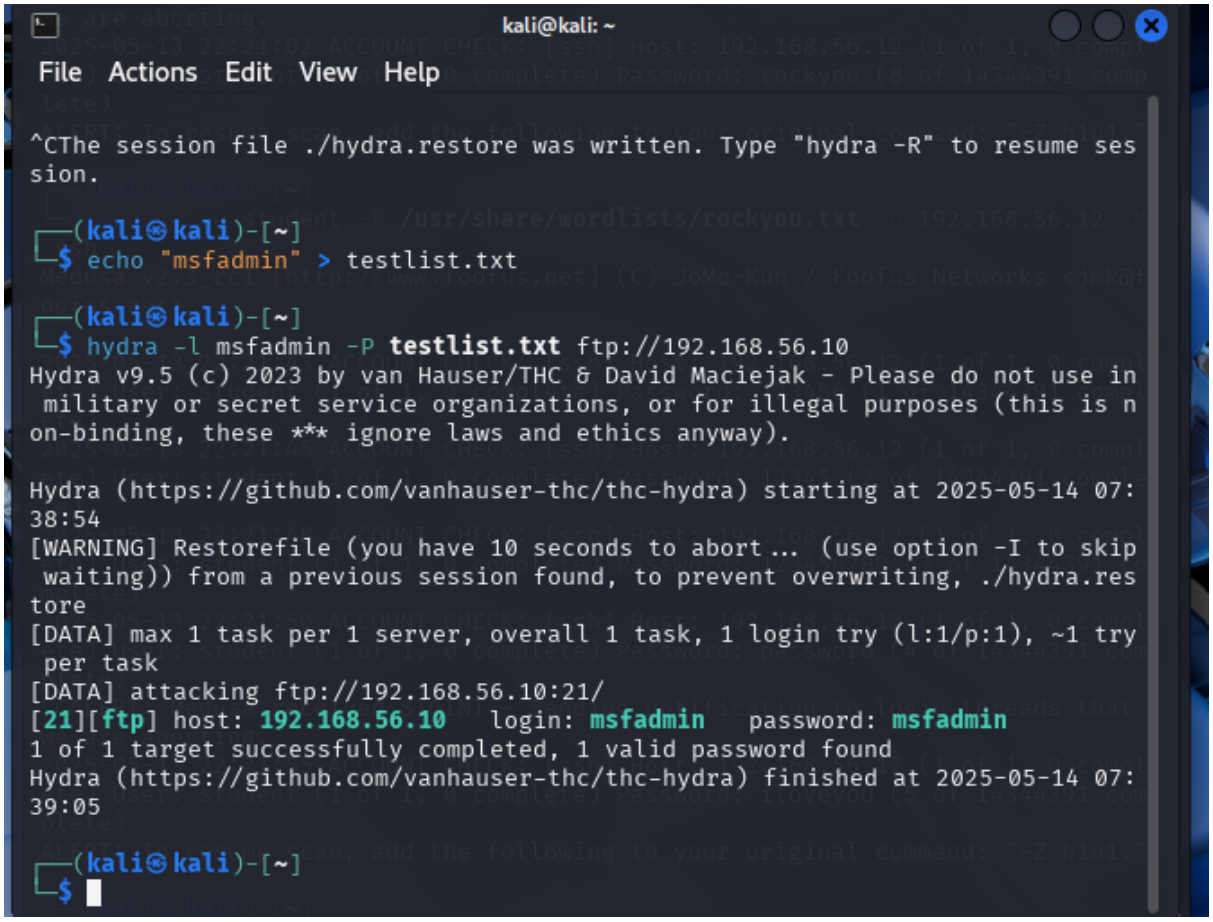

Fig 1: I used Hydra to brute force the FTP login on the Metasploit-able VM. It was initially too slow because the rock you file is large, so I narrowed it to a shorter test list the Hydra proved that the system is vulnerable to simple brute-force attacks (Shivanandhan, 2022)

Q4. Installation and use of Tenable's Nessus Vulnerability scanner.

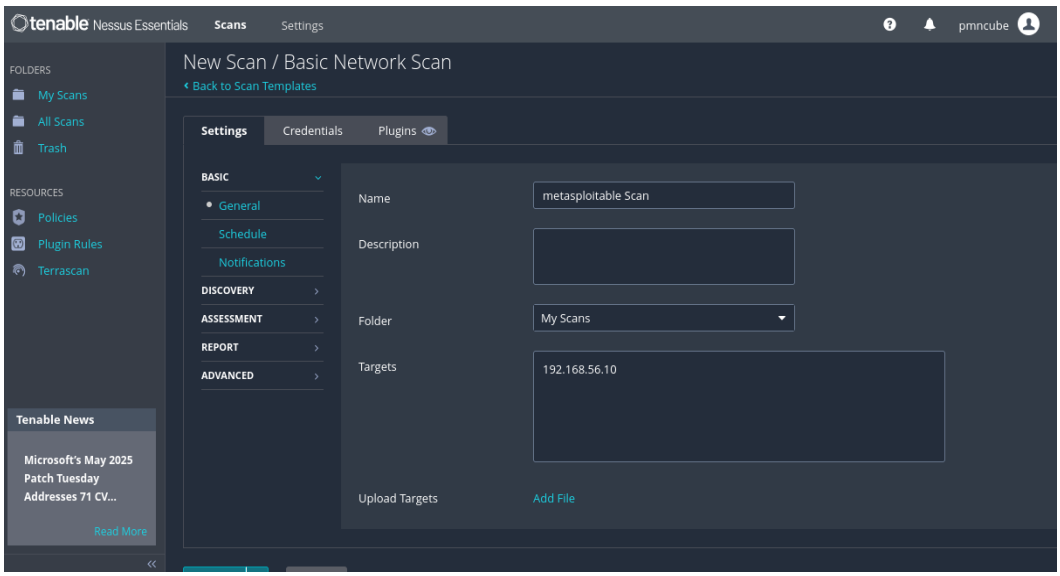

Fig 1: new Scan with the Metasploit-able IP address

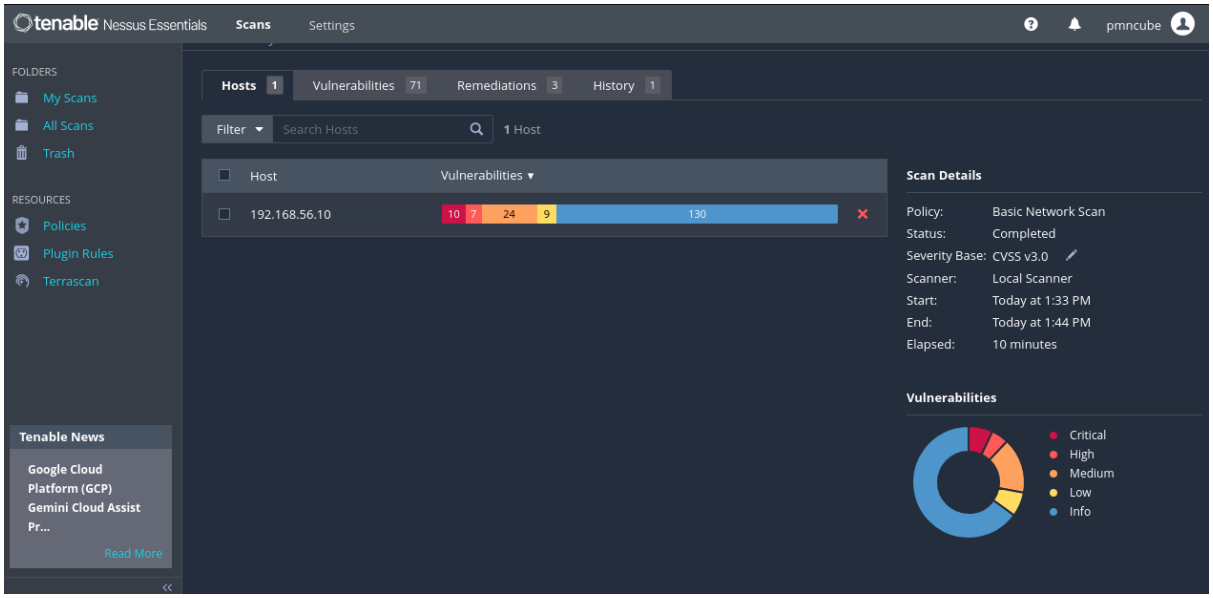

Fig2: view of all the vulnerabilities

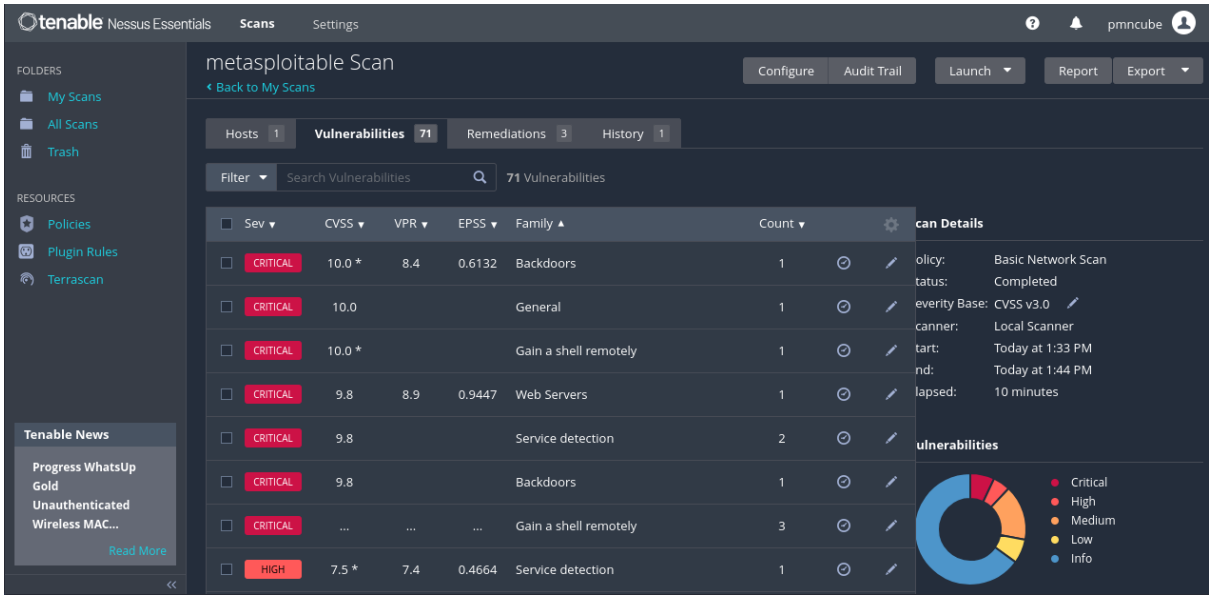

Fig 3: clicked on vulnerabilities

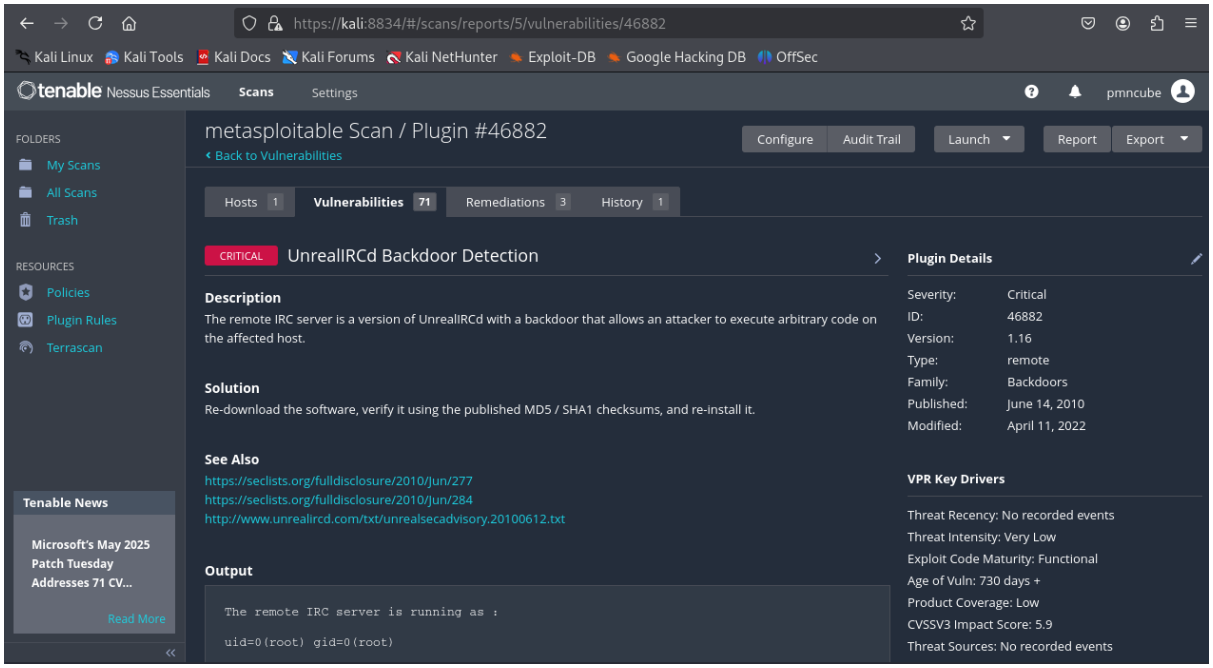

Fig 4: clicked on one critical vulnerability to read more on it

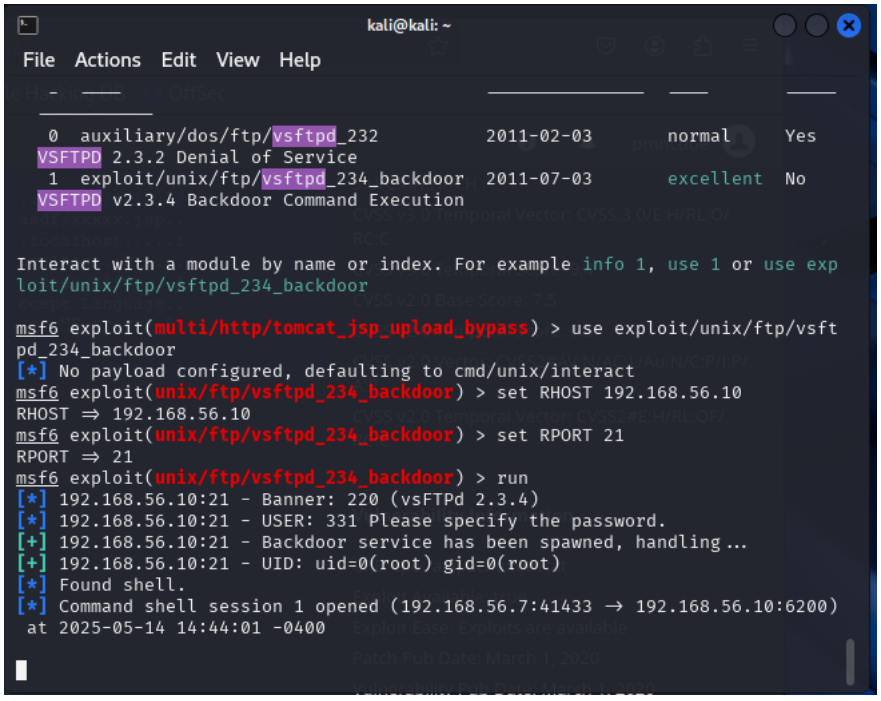

Fig 5: Using Metasploit, I explored vsftpd 234 backdoor vulnerability which was identified by Nessus as a vulnerability.

Q5. Mitre ATT&CK Framework research

What is the Mitre ATT&CK

The Mitre ATT&CK known as (Adversarial Tactics, Techniques and Common Knowledge) for enterprises is a very important resource in cybersecurity as well as its presentation as a kanban

board-style diagram. It describes how attackers work using 14 techniques, each of them representing a distinct stage of the attack lifecycle such as initial access, execution, persistence and Exfiltration, hundreds of techniques e.g. phishing, credential dumping (mitre, 2025).

Why is it so important

Think of the MITRE ATT&CK framework like a common language for cybersecurity folks. It helps the good guys (blue teams), the simulated bad guys (red teams), and the detectives (analysts) all understand each other better when talking about how attacks happen. It also makes it easier for the good guys to figure out where they can't see what's going on in their systems and set up better alarms to catch attackers. Plus, it helps connect the dots between how a new attack looks and how known hacking groups like APT29 or FIN7 usually operate, so companies can react quicker and even guess what might happen next (MITRE,2024). Finally, it's a big help in training people and running practice attack drills to make sure everyone's ready for the real thing

The Real-life examples

Phishing

A bunch of hackers known as APT28 tried to break into a bunch of European government computers. They sent out emails that looked important, like they were from someone you'd trust. But these emails had an infected Microsoft Word file. If someone opened one of those files, it was like leaving the back door wide open for the hackers to sneak into the government's computer systems. (Mitre.org., 2024)

LSASS Memory

During that big SolarWinds hack, the bad guys were able to sneak in and use special tools, kind of like lock-picking software (like Mimikatz), to grab those secret keys right out of the computer's memory. Once they had those keys, it was like having a master key to move around to other computers in the system without needing to log in again. That's what "lateral movement" means – hopping from one computer to another inside the network. (www.youtube.com, n.d.)

Persistence- Registry Run keys

Software that is sly, such as Trick Bot. Even after you turn your computer off and back on, it may remain on it. It essentially adds its name to a list of items that start up automatically each time your computer boots up. It achieves this by writing its own small instruction in a certain location within your machine's settings. The Windows Registry is this unique location, and these instructions are like "Run Keys." Trick Bot is therefore extremely persistent because it has a free license that allows it to wake and begin causing issues every time your computer is turned on.

Q6. Perform a Man in the Middle (MiTM) Attack on the Windows VM (required: Kali Linux and Windows or Linux VM).

Part 1: Performing ARP Poisoning with Ettercap

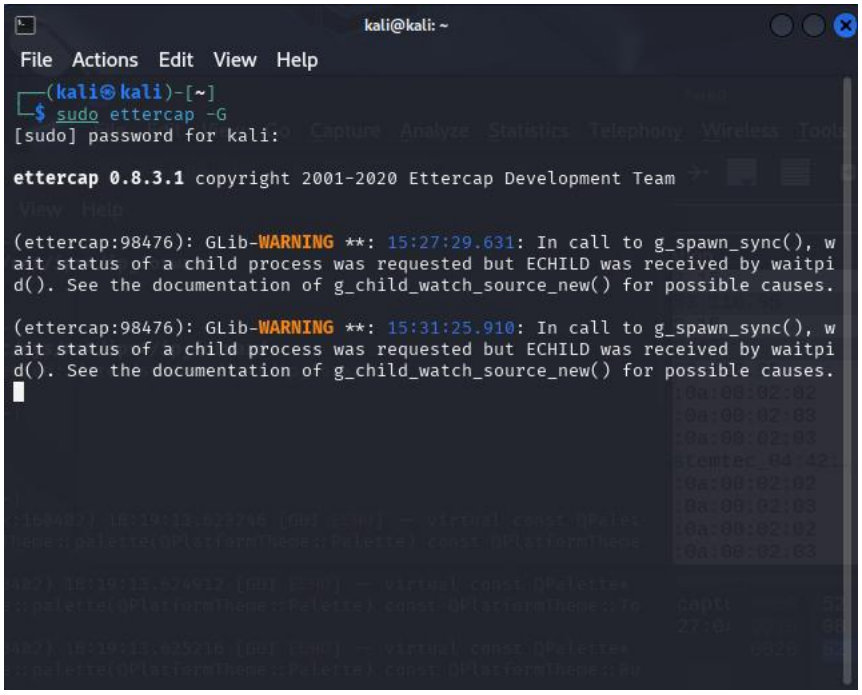

Fig1: This opens the Ettercap GUI

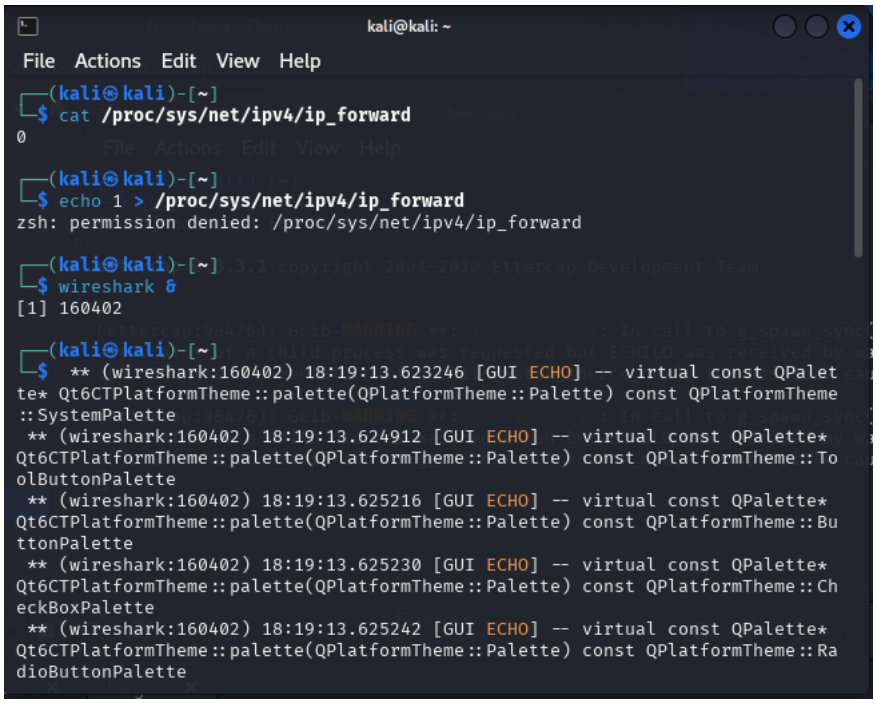

Fig2: the cat command was to change how I can investigate traffic. the default value was 0 so I attempted to change that, however that wasn't successful by the echo 1. Followed by running Wireshark at the same time with Ettercap.

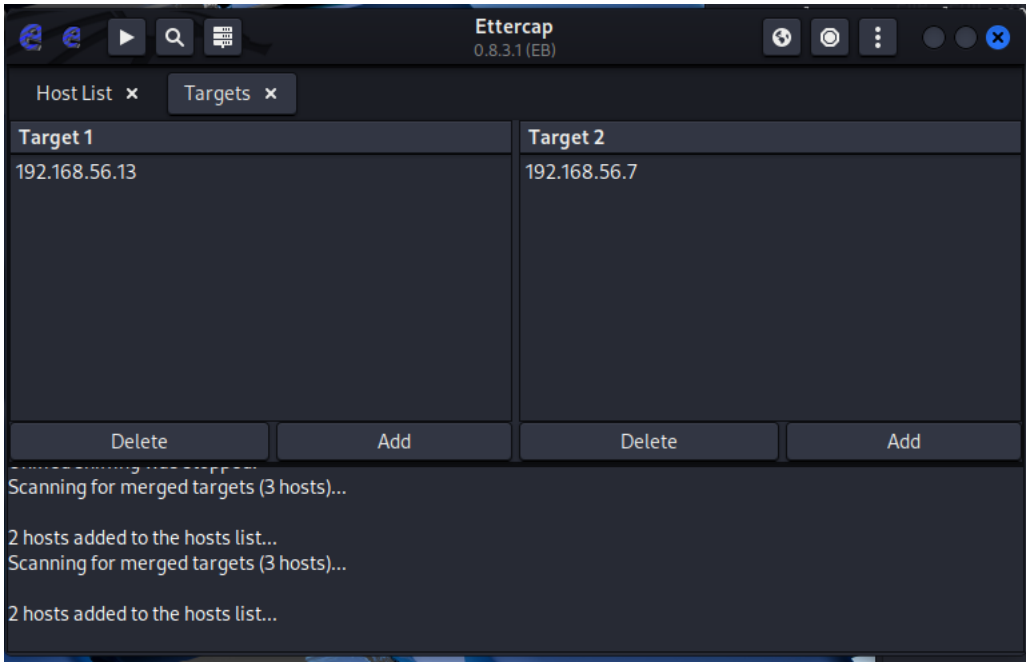

Fig3 : I have set 2 targeted IP address, the one IP address belongs to the windows machine

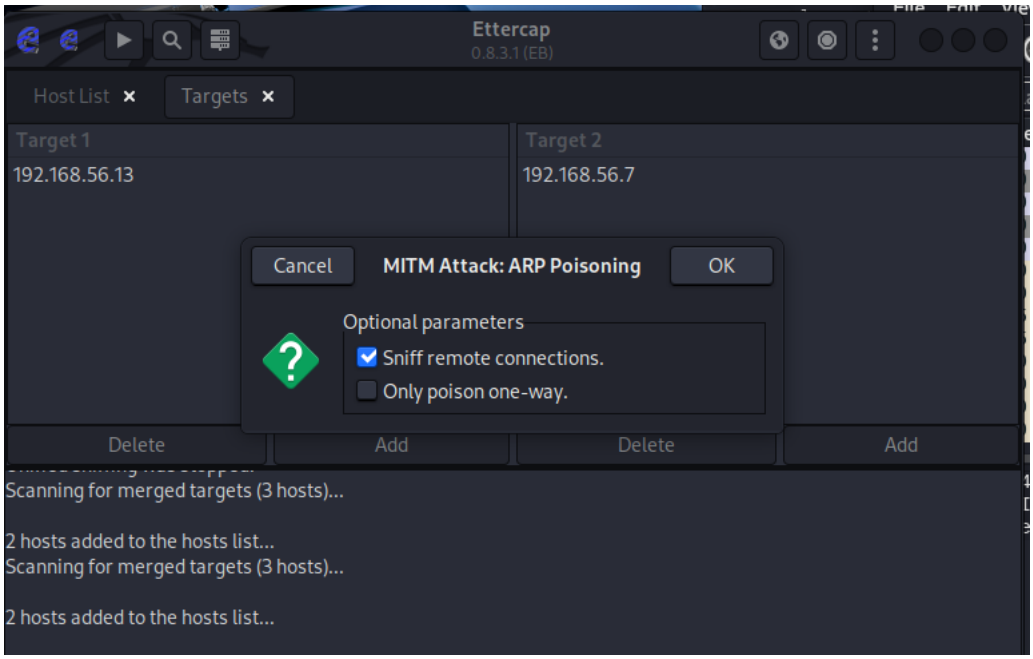

Fig 4: starting the ARP poisoning

Part 2: showing evidence and the traffic capture

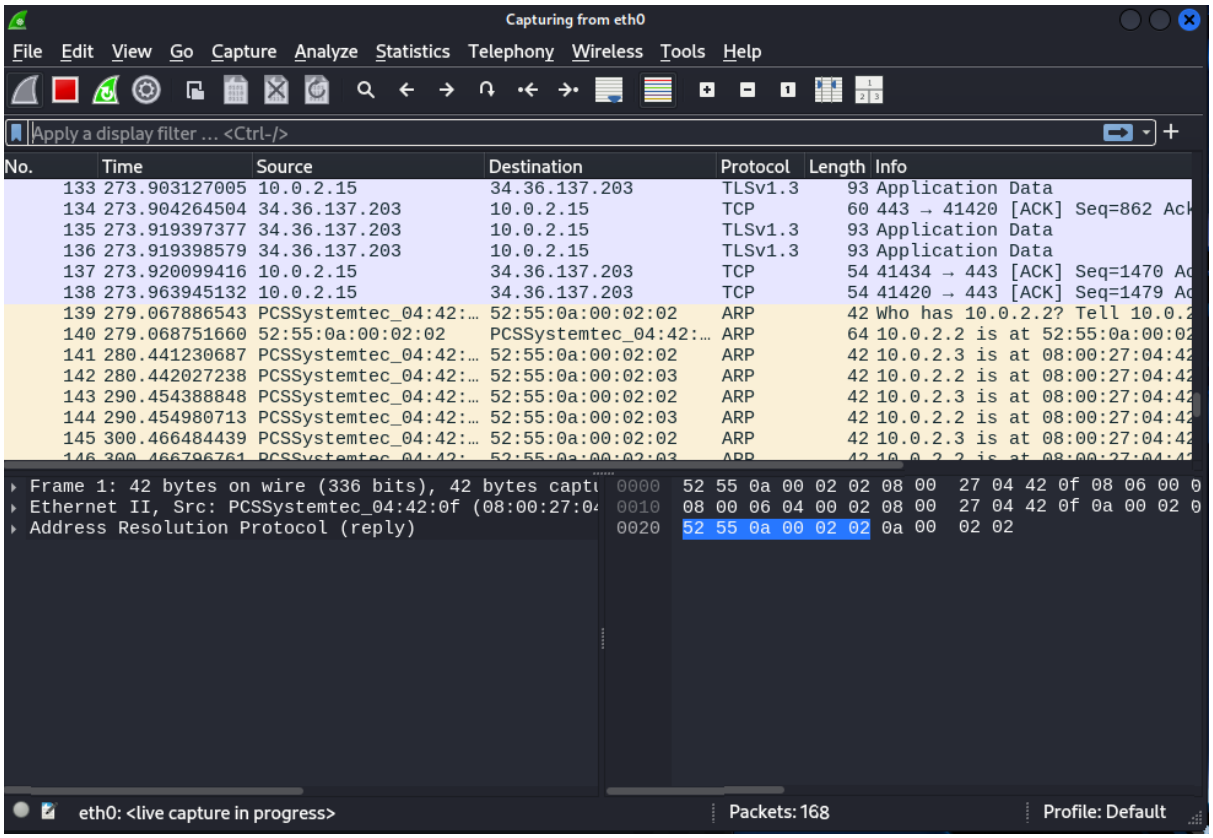

Fig5: Started capturing the traffic on Wireshark as you can see there ARP information is being sent out in the environment to confuse the different IP addresses. The ARP cache of these machines is being messed with

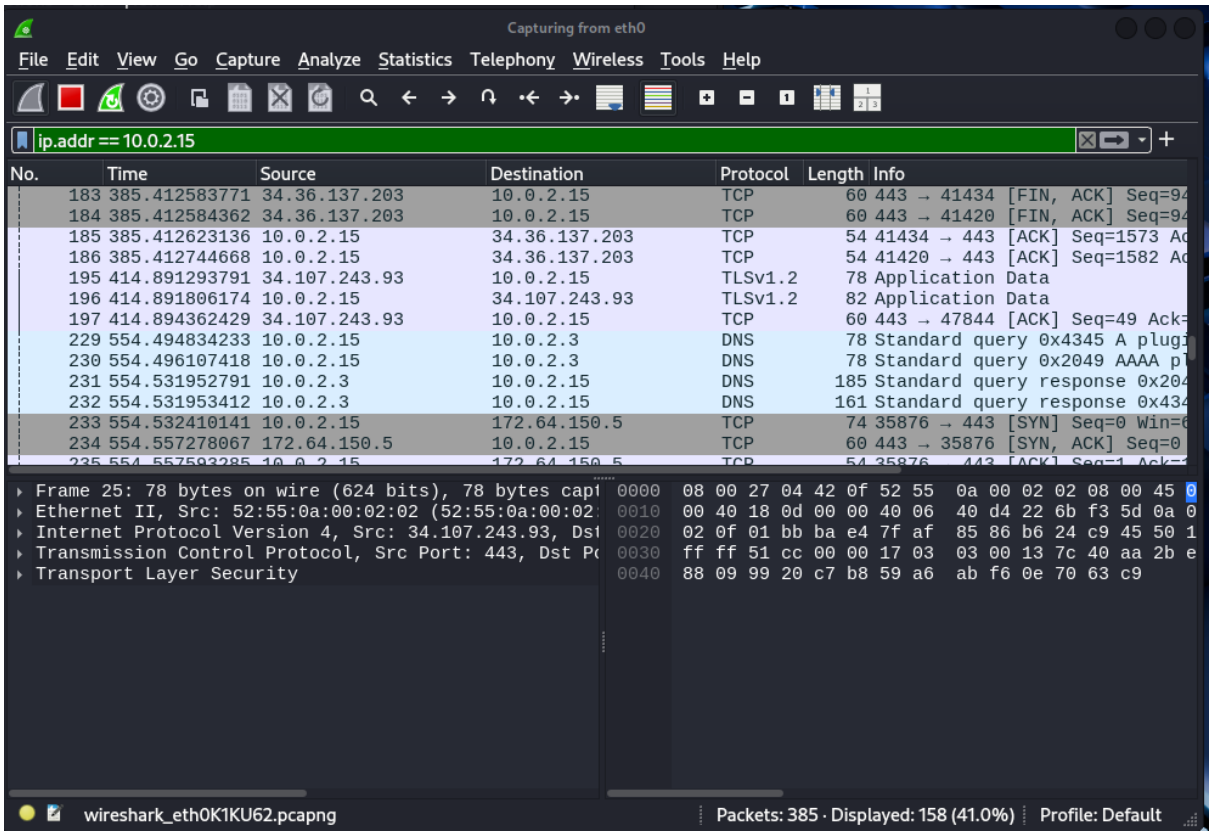

Fig 6: I have now filtered to show all packets to and from the victim, this confirms if the MiTM attack is working.

Part 3 -ARP command to confirm

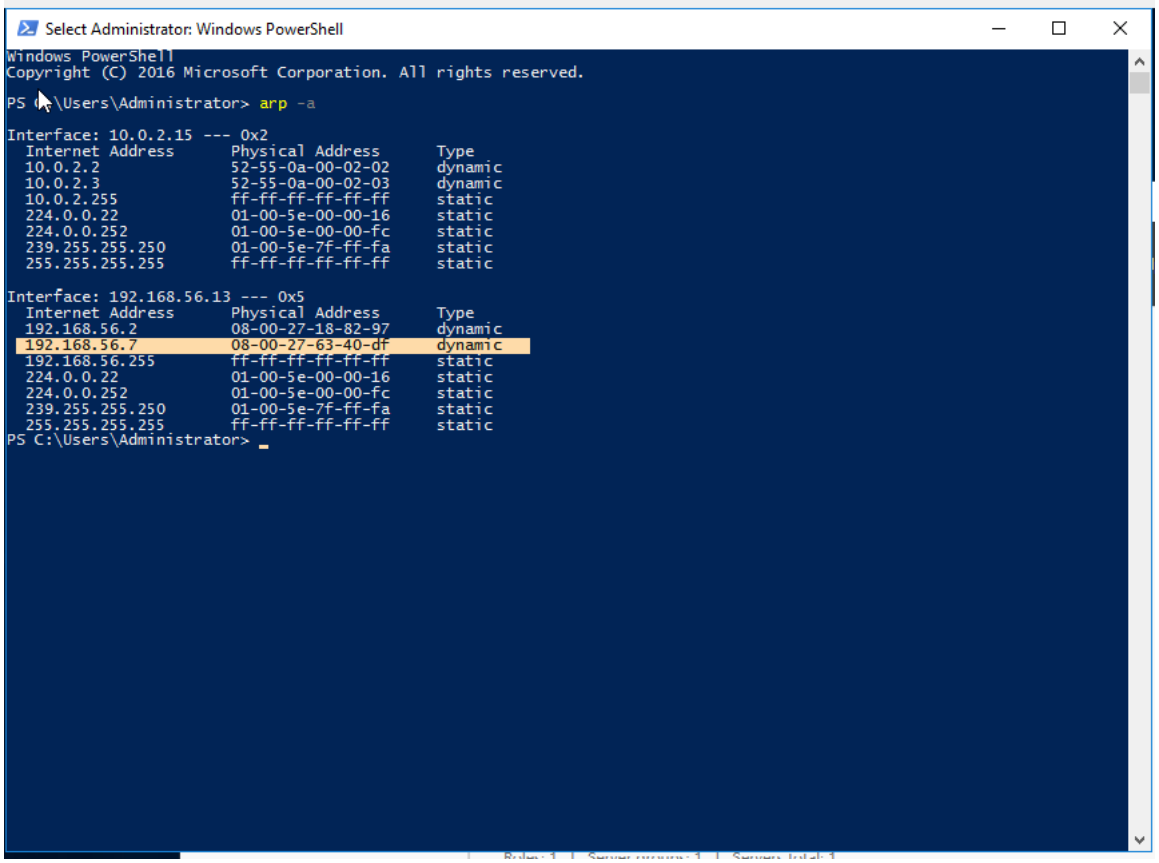

Fig 7: as you can see on the imagine above, I now can see the kali machines Mac and Ip address too, this is proof the ARP poisoning

Part 4: Mitigation Method

The use of static ARP Entries

Using static ARP entries is a good way to counteract Man-in-the-Middle (MiTM) attacks, including ARP poisoning. Using this method, network devices' fixed MAC addresses are manually assigned to their matching IP addresses. It stops attackers from faking ARP answers and redirecting traffic through a malicious system by creating these static associations. This method's main disadvantage is that only of scalability, even if it works very well in tiny, controlled settings like labs or secure internal segments. Because of the administrative burden and possibility of setup problems, it is not feasible to maintain static ARP tables across large networks. (www.juniper.net, n.d.)

Implementing Network divisions and VlANs

Using network division and VLANs (Virtual Local Area Networks) is a second, more scalable approach. Communication channels are limited by segmenting the network into separate parts and allocating systems to various VLANs. An attacker's ability to spy on or manipulate traffic between devices on different segments is limited by this isolation. An attacker would not be able to readily capture or change traffic from another VLAN, even if they were able to access one. When put together, these two tactics greatly reduce the attack surface and make it more difficult for attackers to carry out MiTM attacks on a network. (Basan, 2024)

REFERENCES

- Essex, D. (2023). *What is Patch Management and Why is it Important?* [online] SearchEnterpriseDesktop. Available at: https://www.techtarget.com/searchenterprisedesktop/definition/patch-management.
- OWASP (n.d.). *Web Application Firewall | OWASP*. [online] owasp.org. Available at: https://owasp.org/www-community/Web_Application_Firewall.
- NIST (2023). *NIST Special Publication 800-63B*. [online] Nist.gov. Available at: https://pages.nist.gov/800-63-3/sp800-63b.html.
- Ward, T. (2025). *The Importance of Security Monitoring and Logging - Spyrus*. [online] Spyrus. Available at: https://spyrus.com/the-importance-of-security-monitoring-and-logging/.
- OWASP (2021). *A03 Injection - OWASP Top 10:2021*. [online] owasp.org. Available at: https://owasp.org/Top10/A03_2021-Injection/.
- Shivanandhan, M. (2022). *How to Use Hydra to Hack Passwords – Penetration Testing Tutorial*. [online] freeCodeCamp.org. Available at: https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/.
- MITRE (2025). *MITRE ATT&CK*. [online] Mitre.org. Available at: https://attack.mitre.org/.
- MITRE (2024). *MITRE ATT&CK®*. [online] attack.mitre.org. Available at: https://attack.mitre.org.
- www.youtube.com. (n.d.). - *YouTube*. [online] Available at: https://www.youtube.com/watch?v=jD02Q3RStaM&t=145s [Accessed 14 May 2025].
- www.juniper.net. (n.d.). *Configuring Static ARP Table Entries For Mapping IP Addresses to MAC Addresses | Junos OS | Juniper Networks*. [online] Available at: https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/task/interfaces-configuring-static-arp-table-entries.html.
- Basan, M. (2024). *What is a VLAN? Ultimate Guide to How VLANs Work*. [online] eSecurityPlanet. Available at: https://www.esecurityplanet.com/networks/what-is-a-vlan/.