



# 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

Prepared by: Primrose Mncube .....	1
Date: .....	1
Introduction.....	2
Recommendations to Harden the Network .....	2
OWASP REPORT .....	3
Q2: Attacking a vulnerable Machine .....	4
Q3b. Demonstrate a Brute Force attack using Kali Linux against a vulnerable VM Metasploit-able Linux.....	6
Q4. Installation and use of Tenable's Nessus Vulnerability scanner. ....	7
Q5. Mitre ATT&CK Framework research .....	9
Q6. Perform a Man in the Middle (MiTM) Attack on the Windows VM (required: Kali Linux and Windows or Linux VM). ....	10
REFERENCES .....	15

## 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 HTTP 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*

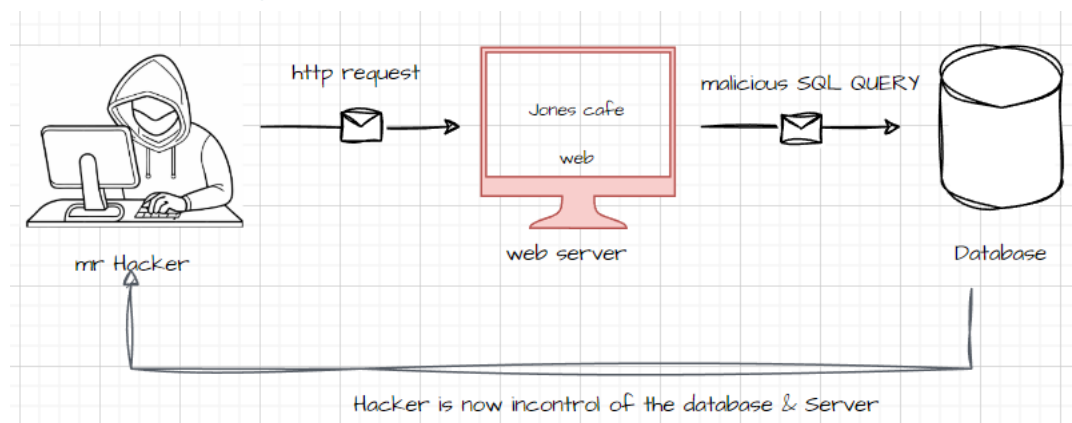
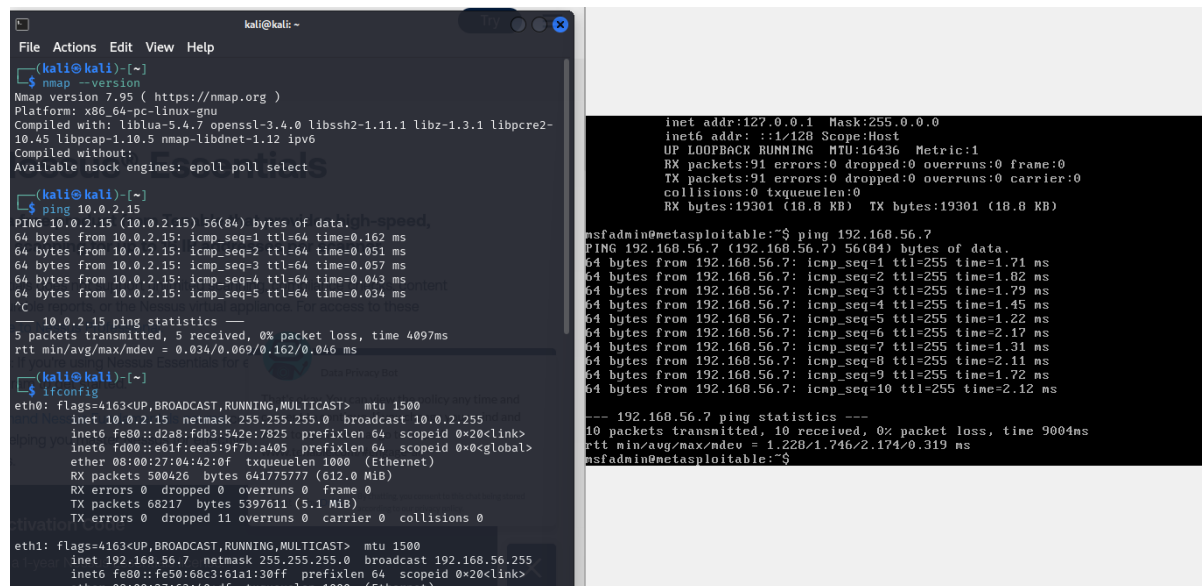


Fig 1: a Flow showing a user submitting a logging, and because the server hasn't been properly cleaned the attacker has gained access

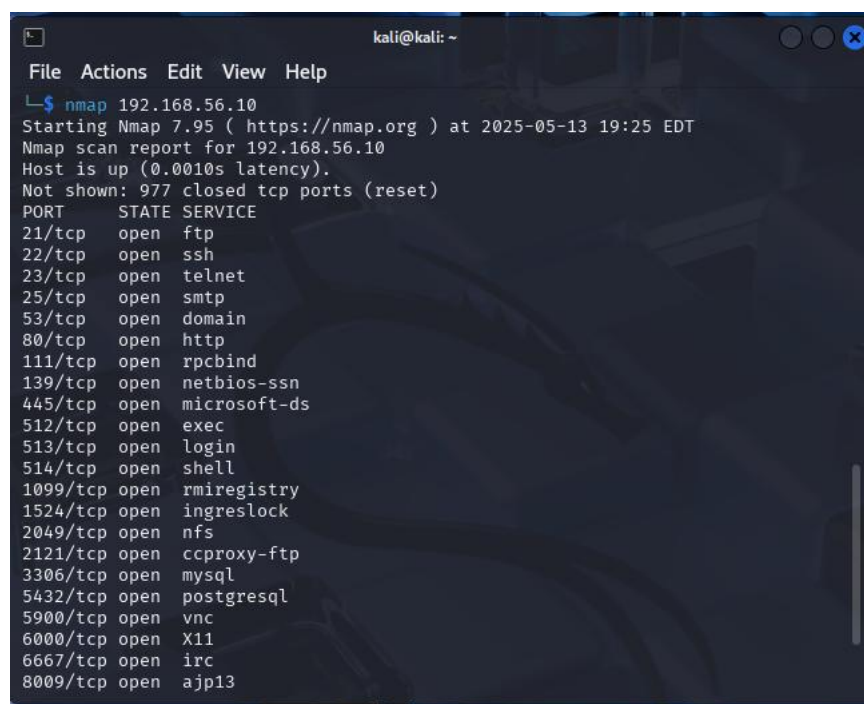
## Q2: Attacking a vulnerable Machine

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



```
kali@kali: ~  
File Actions Edit View Help  
$ nmap -version  
Nmap version 7.95 ( https://nmap.org )  
Platform: x86_64-pc-linux-gnu  
Compiled with: liblua-5.4.7 openssl-3.4.0 libssh2-1.11.1 libz-1.3.1 libpcap-1.10.5 libbpf-1.0.5 nmap-libndnet-1.12 ipv6  
Compiled without:  
Available nsock engines: epoll poll select  
$ ping 10.0.2.15  
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.  
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.162 ms  
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.051 ms  
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.057 ms  
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.043 ms  
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.034 ms  
--- 10.0.2.15 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4097ms  
rtt min/avg/max/mdev = 0.034/0.069/0.162/0.046 ms  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
inet6 fe80::d2a8:fdb3:542e:7825 prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)  
RX packets 500426 bytes 641775777 (612.0 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 68217 bytes 5397611 (5.1 MiB)  
TX errors 0 dropped 11 overruns 0 carrier 0 collisions 0  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.56.7 netmask 255.255.255.0 broadcast 192.168.56.255  
inet6 fe80::fe50:68c3:61a1:30ff prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:62:40:df txqueuelen 1000 (Ethernet)  
msfadmin@metasploitable:~$ ping 192.168.56.7  
PING 192.168.56.7 (192.168.56.7) 56(84) bytes of data.  
64 bytes from 192.168.56.7: icmp_seq=1 ttl=255 time=1.71 ms  
64 bytes from 192.168.56.7: icmp_seq=2 ttl=255 time=1.82 ms  
64 bytes from 192.168.56.7: icmp_seq=3 ttl=255 time=1.79 ms  
64 bytes from 192.168.56.7: icmp_seq=4 ttl=255 time=1.45 ms  
64 bytes from 192.168.56.7: icmp_seq=5 ttl=255 time=1.22 ms  
64 bytes from 192.168.56.7: icmp_seq=6 ttl=255 time=2.17 ms  
64 bytes from 192.168.56.7: icmp_seq=7 ttl=255 time=1.31 ms  
64 bytes from 192.168.56.7: icmp_seq=8 ttl=255 time=2.11 ms  
64 bytes from 192.168.56.7: icmp_seq=9 ttl=255 time=1.72 ms  
64 bytes from 192.168.56.7: icmp_seq=10 ttl=255 time=2.12 ms  
--- 192.168.56.7 ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 9004ms  
rtt min/avg/max/mdev = 1.228/1.746/2.174/0.319 ms  
msfadmin@metasploitable:~$
```

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



```
kali@kali: ~  
File Actions Edit View Help  
$ nmap 192.168.56.10  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-13 19:25 EDT  
Nmap scan report for 192.168.56.10  
Host is up (0.0010s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13
```

Fig 2: Scanning to see how many ports are open

```
kali@kali: ~  
File Actions Edit View Help  
5432/tcp open  postgresql  
5900/tcp open  vnc  
6000/tcp open  X11  
6667/tcp open  irc  
8009/tcp open  ajp13  
8180/tcp open  unknown  
MAC Address: 08:00:27:38:34:E3 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds  
  
(kali@kali)-[~]  
$ sudo nmap -sT -p 80,53 192.168.56.10  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-13 19:29 EDT  
Nmap scan report for 192.168.56.10  
Host is up (0.0023s latency).  
  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
MAC Address: 08:00:27:38:34:E3 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds  
  
(kali@kali)-[~]  
$
```

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

```
kali@kali: ~  
File Actions Edit View Help  
$ sudo nmap -sV 192.168.56.10  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-13 19:39 EDT  
Nmap scan report for 192.168.56.10  
Host is up (0.022s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
```

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



```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -A 192.168.56.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-13 19:34 EDT
Nmap scan report for 192.168.56.10
Host is up (0.0071s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.56.7
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd

```

Fig 5: Aggression Scan

```

kali@kali: ~
File Actions Edit View Help

6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:38:34:E3 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.13 seconds

(kali@kali)-[~]
$ sudo nmap --script=ftp-anon -p 22 192.168.56.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-13 19:42 EDT
Nmap scan report for 192.168.56.10
Host is up (0.0095s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:38:34:E3 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds

(kali@kali)-[~]
$

```

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

```
kali@kali: ~  
File Actions Edit View Help  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume ses  
sion.  
(kali@kali)-[~]  
$ echo "msfadmin" > testlist.txt  
(kali@kali)-[~]  
$ hydra -l msfadmin -P testlist.txt ftp://192.168.56.10  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in  
military or secret service organizations, or for illegal purposes (this is n  
on-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-14 07:  
38:54  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip  
waiting)) from a previous session found, to prevent overwriting, ./hydra.res  
tore  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try  
per task  
[DATA] attacking ftp://192.168.56.10:21/  
[21][ftp] host: 192.168.56.10 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-14 07:  
39:05  
(kali@kali)-[~]  
$
```

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.

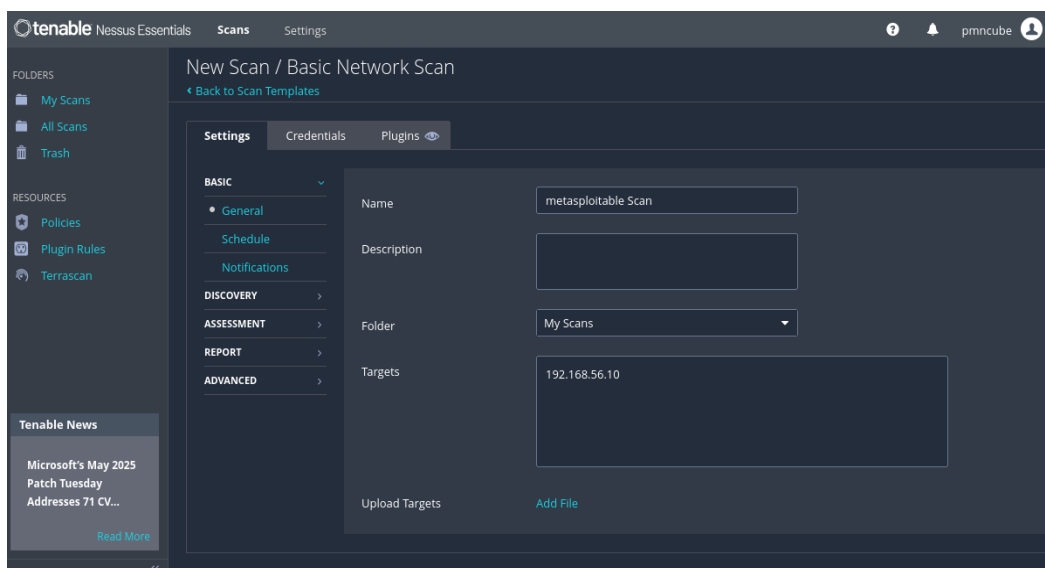


Fig 1: new Scan with the Metasploit-able IP address

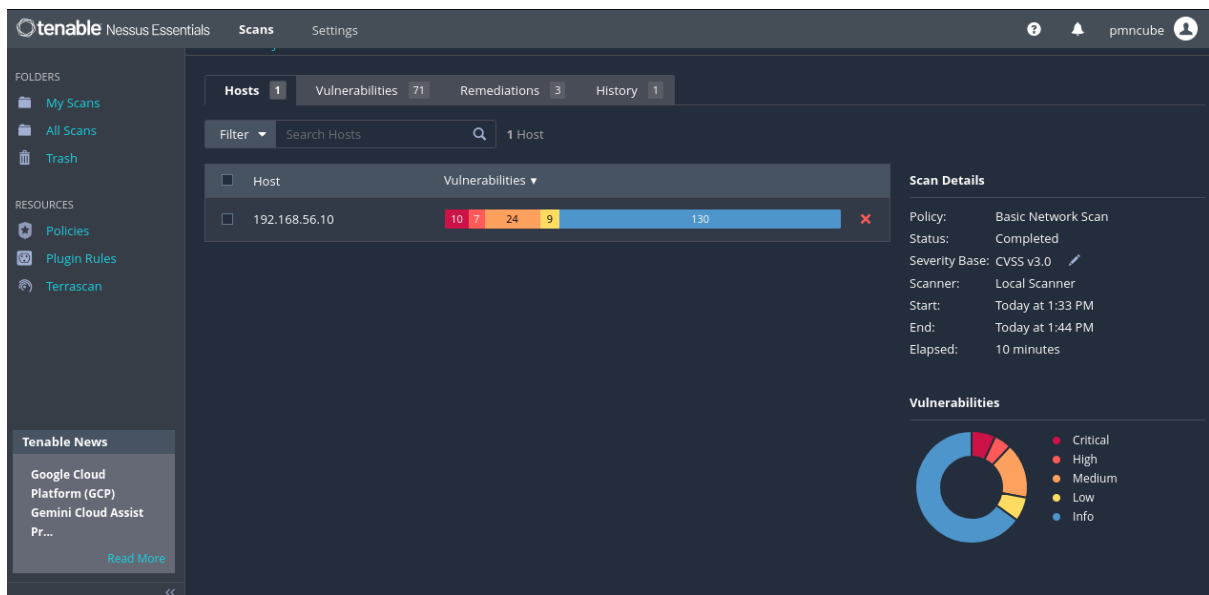


Fig2: view of all the vulnerabilities

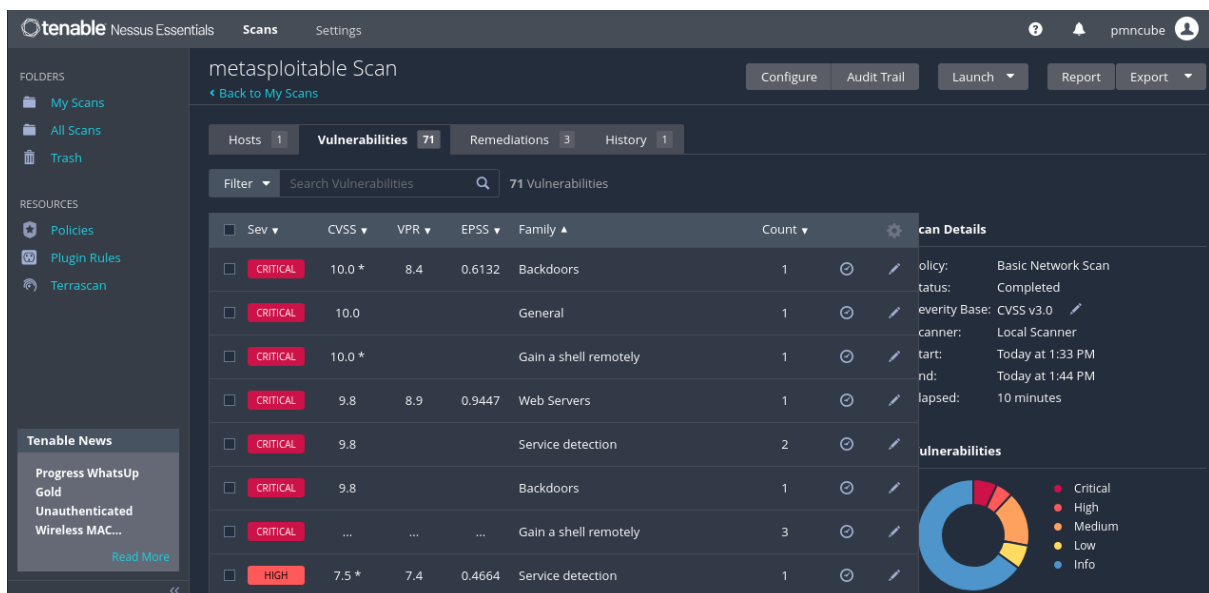


Fig 3: clicked on vulnerabilities



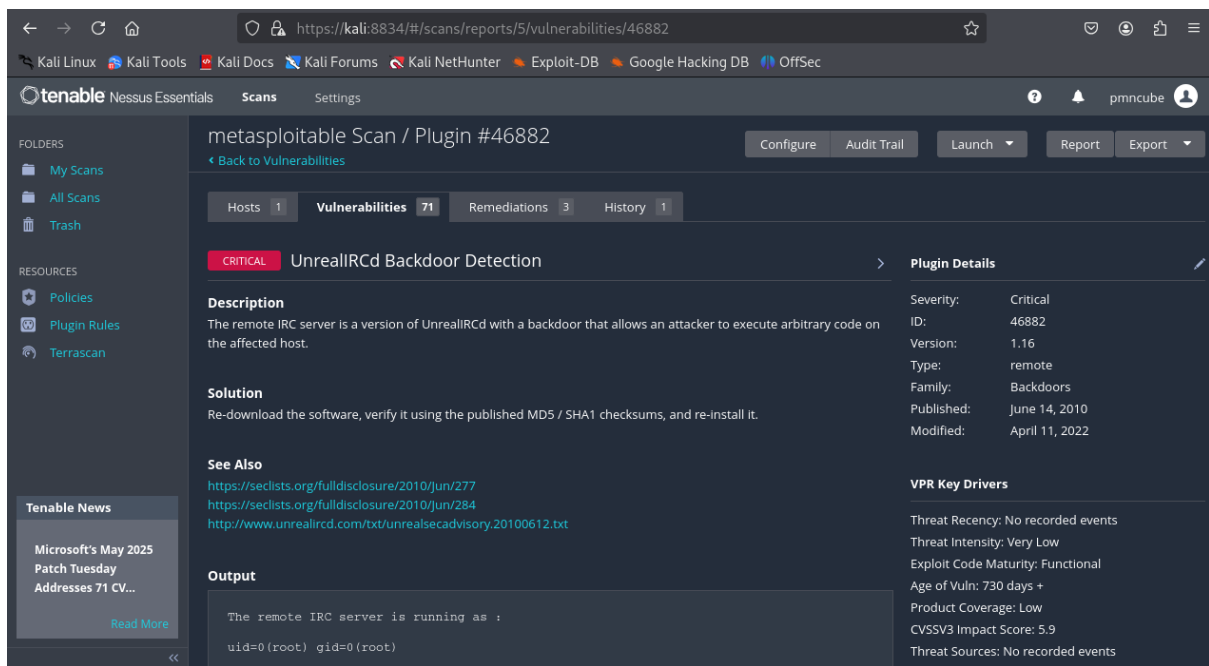


Fig 4: clicked on one critical vulnerability to read more on it

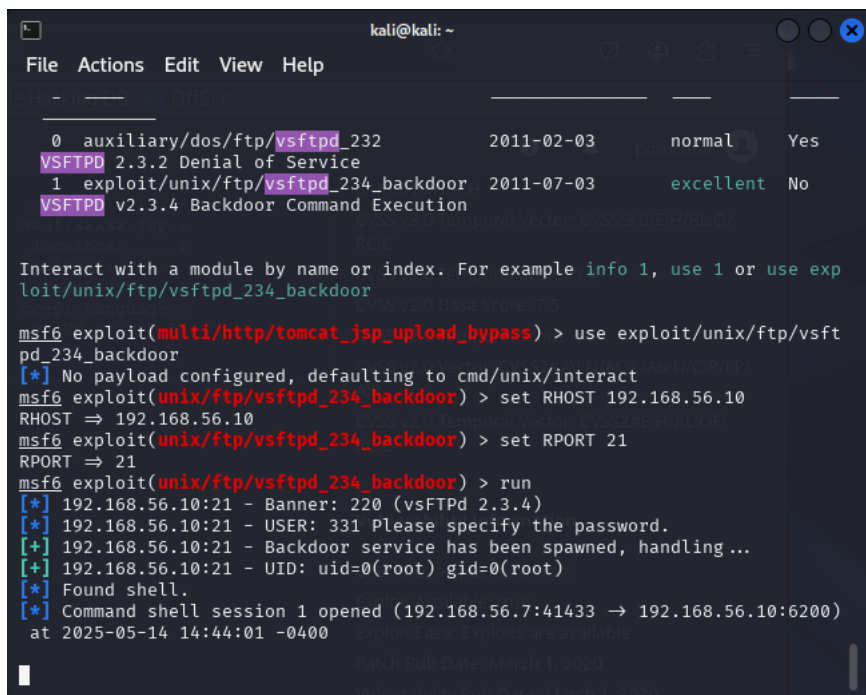


Fig 5: Using Metasploit, I explored vsftpd 234 backdoor vulnerability which was identified by Nessus as a vulnerability.

## 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

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo ettercap -G  
[sudo] password for kali:   
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team  
View Help  
(ettercap:98476): Glib-WARNING **: 15:27:29.631: In call to g_spawn_sync(), wait status of a child process was requested but ECHILD was received by waitpid(). See the documentation of g_child_watch_source_new() for possible causes.  
(ettercap:98476): Glib-WARNING **: 15:31:25.910: In call to g_spawn_sync(), wait status of a child process was requested but ECHILD was received by waitpid(). See the documentation of g_child_watch_source_new() for possible causes.  
[1] 160402  
18:19:13.623246 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette  
18:19:13.624912 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette  
18:19:13.625216 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette  
18:19:13.625230 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette  
18:19:13.625242 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette
```

Fig1: This opens the Ettercap GUI

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ cat /proc/sys/net/ipv4/ip_forward  
0  
(kali@kali)-[~]  
$ echo 1 > /proc/sys/net/ipv4/ip_forward  
zsh: permission denied: /proc/sys/net/ipv4/ip_forward  
(kali@kali)-[~]  
$ wireshark &  
[1] 160402  
(kali@kali)-[~]  
$ ** (wireshark:160402) 18:19:13.623246 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette  
** (wireshark:160402) 18:19:13.624912 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette  
** (wireshark:160402) 18:19:13.625216 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette  
** (wireshark:160402) 18:19:13.625230 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette  
** (wireshark:160402) 18:19:13.625242 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette
```

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.

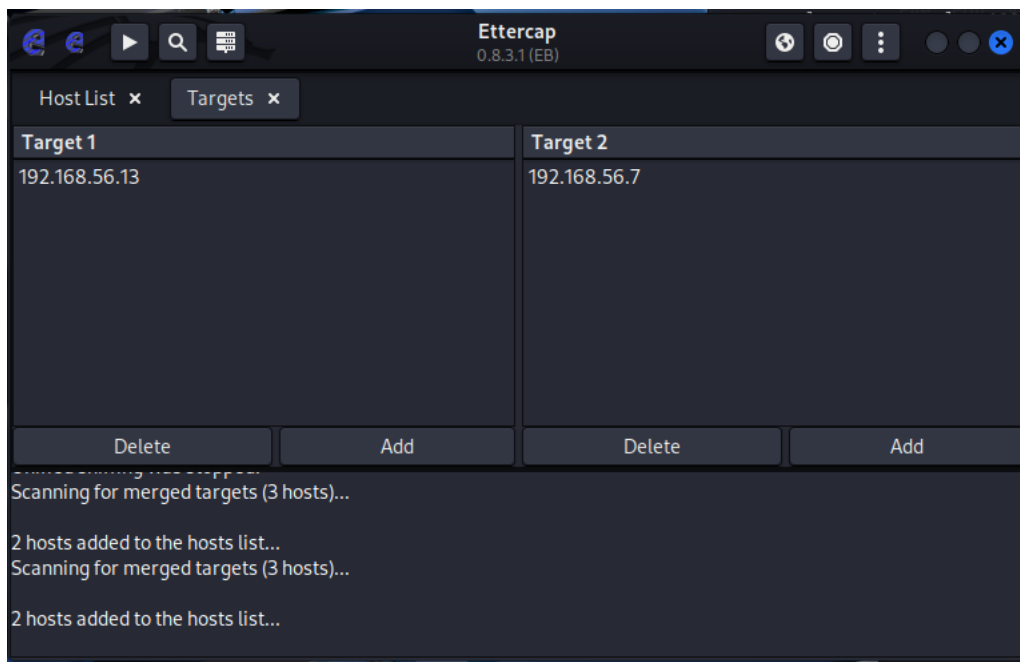


Fig3 : I have set 2 targeted IP address, the one IP address belongs to the windows machine

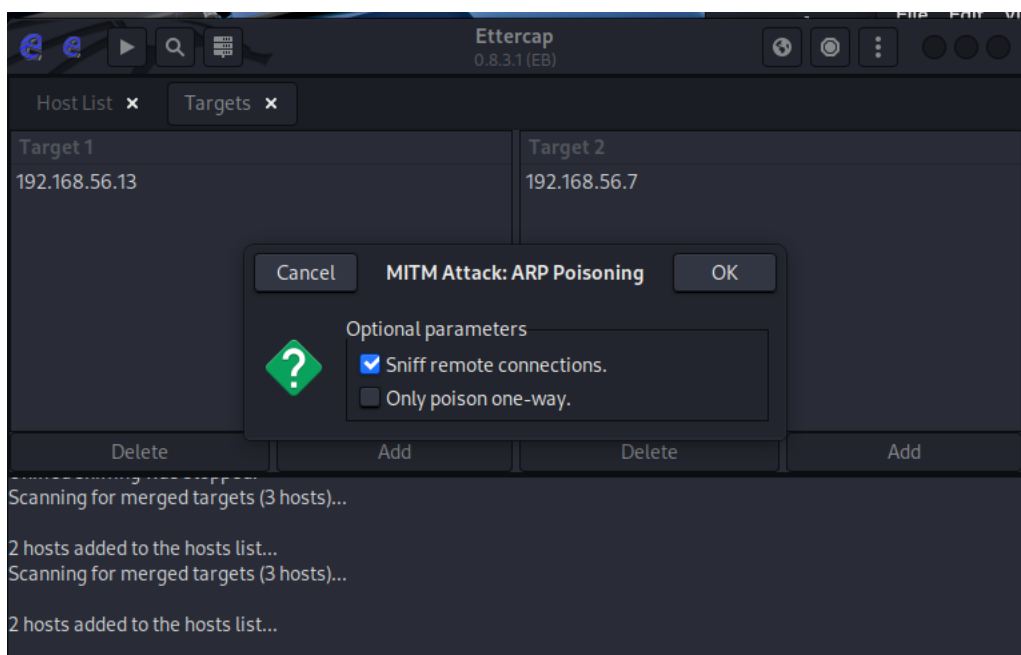


Fig 4: starting the ARP poisoning

## Part 2: showing evidence and the traffic capture

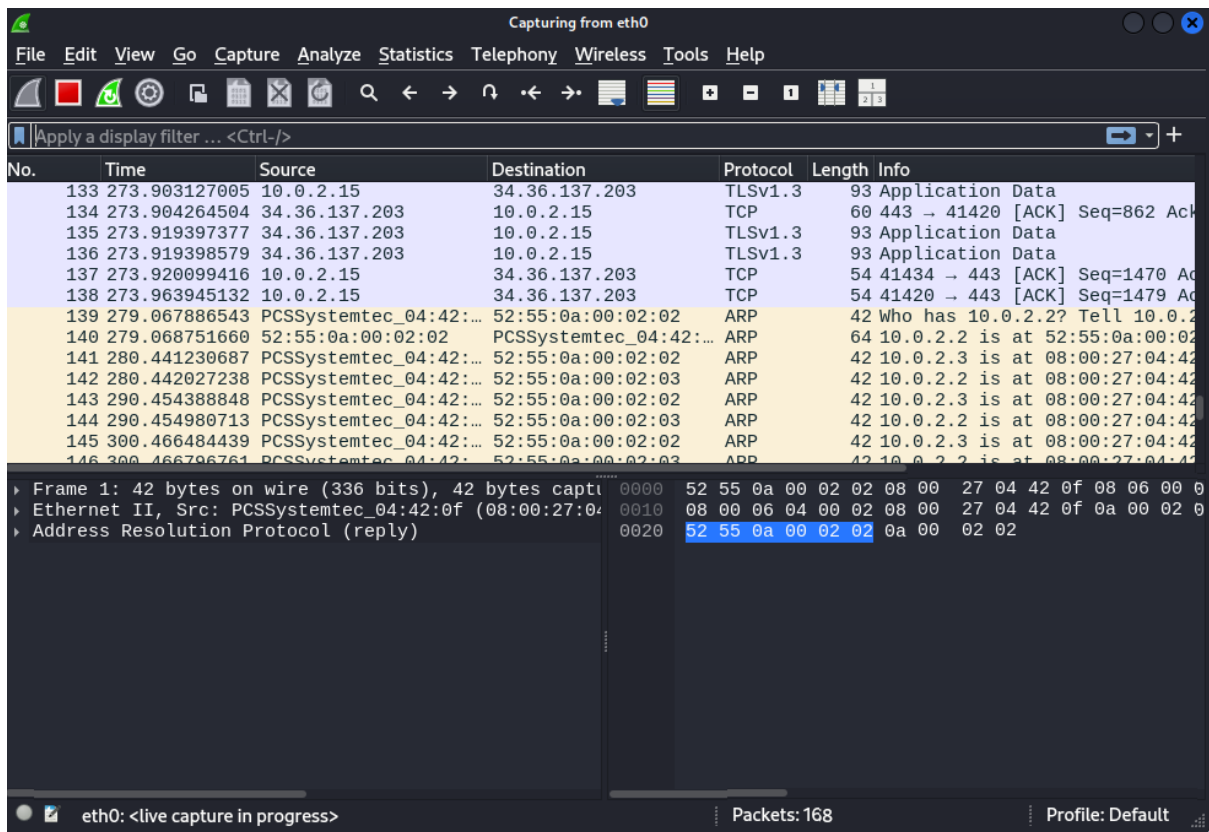


Fig5: Started capturing the traffic on Wireshark as you can see there ARP information is being sent out in the environment to confuse the different IP addresses. The ARP cache of these machines is being messed with

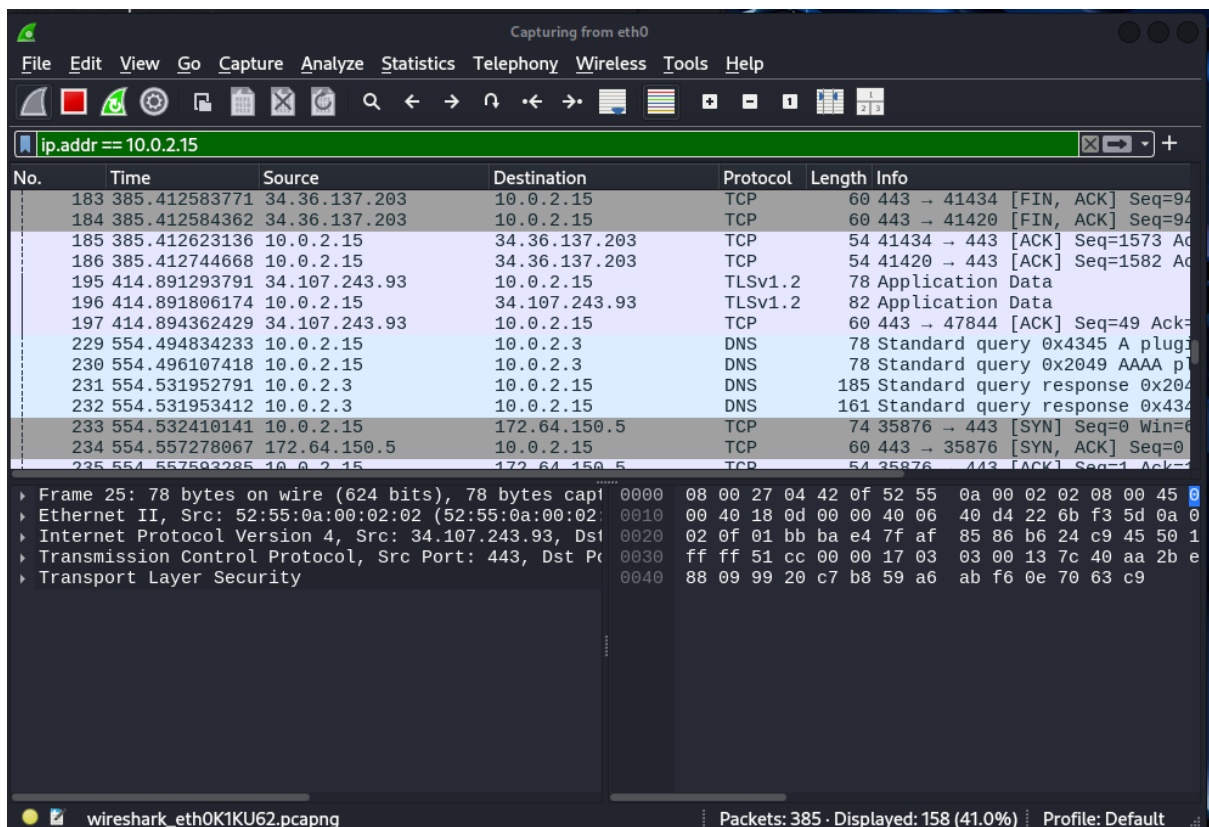


Fig 6: I have now filtered to show all packets to and from the victim, this confirms if the MiTM attack is working.

### Part 3 -ARP command to confirm

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> arp -a

Interface: 10.0.2.15 --- 0x2
Internet Address      Physical Address      Type
-----
10.0.2.2              52-55-0a-00-02-02     dynamic
10.0.2.3              52-55-0a-00-02-03     dynamic
10.0.2.255            ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.13 --- 0x5
Internet Address      Physical Address      Type
-----
192.168.56.2          08-00-27-18-82-97     dynamic
192.168.56.7          08-00-27-63-40-df     dynamic
192.168.56.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

PS C:\Users\Administrator>
```

Fig 7: as you can see on the image 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](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/](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/>.