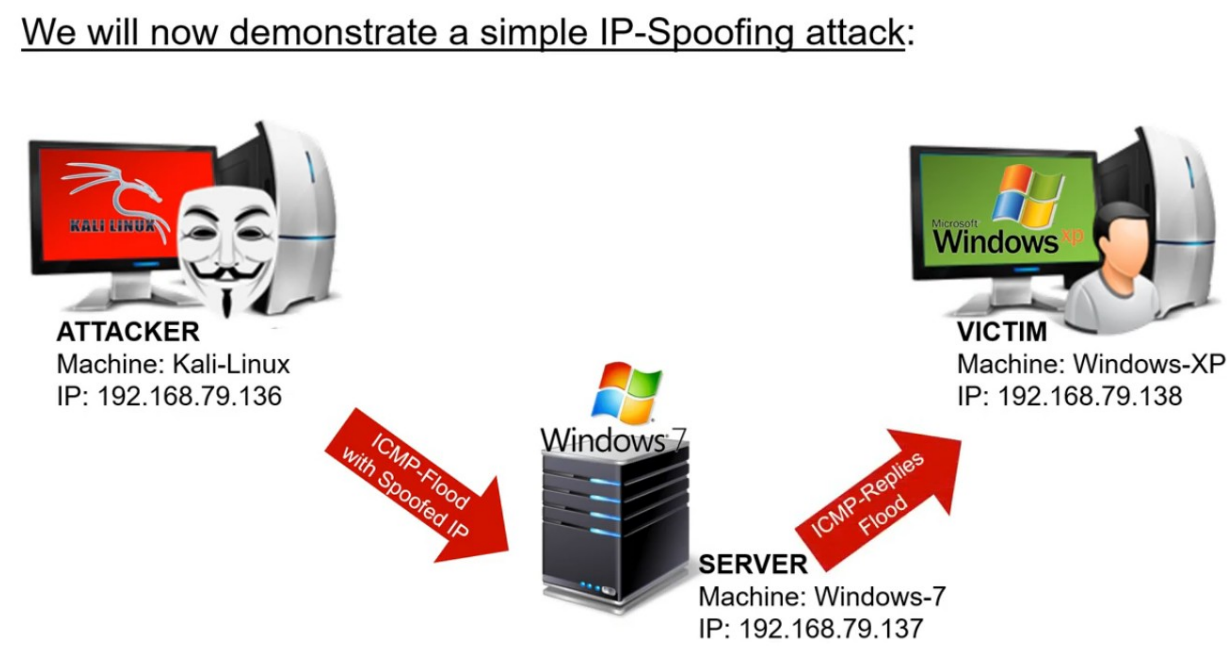
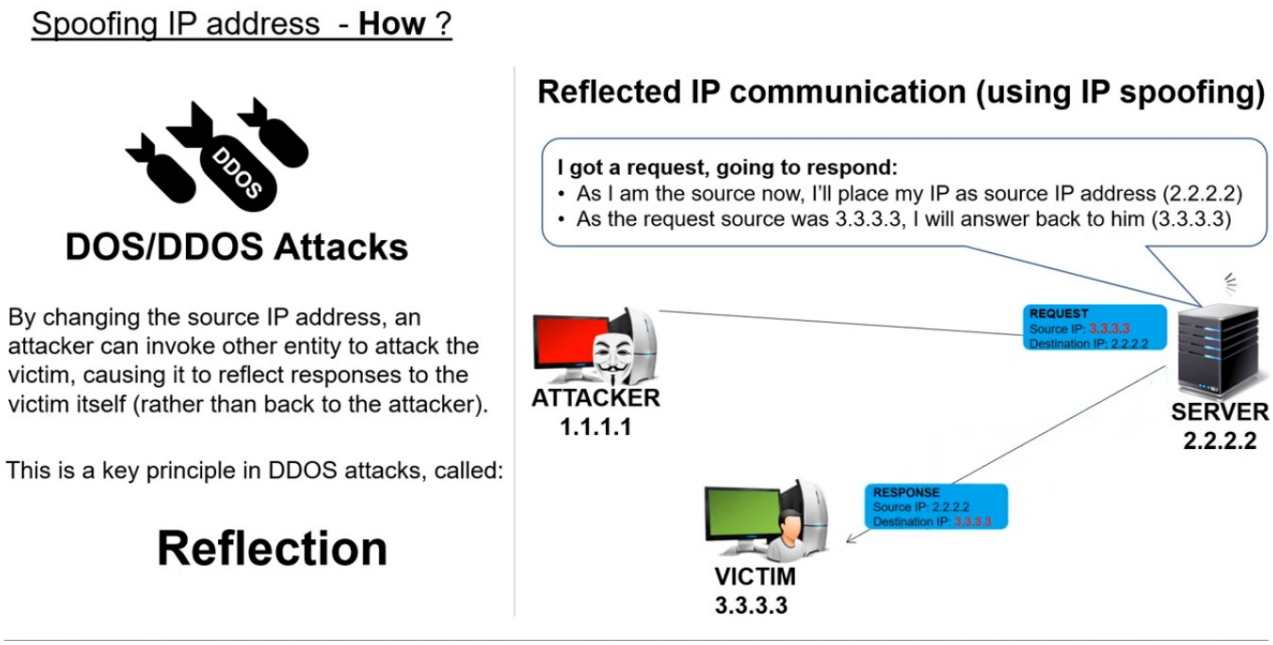
Vulnerability Analysis and Penetration Testing

1.IP Spoofing:

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.





Usage

hping is a command-line oriented TCP/IP packet assembler/analyzer.

To send flood from random ip's:

hping3 --flood -p <Destination Port> <Victim IP> -S --rand-source

To send flood from a specific spoofed ip:

hping3 --flood -p <Destination Port> <Victim IP> -S --spoof <Inactive IP>

--flood
Sent packets as fast as possible, without taking care to show incoming replies. This is ways faster than to specify the -i u0 option.

-p –dest.port
Set destination port

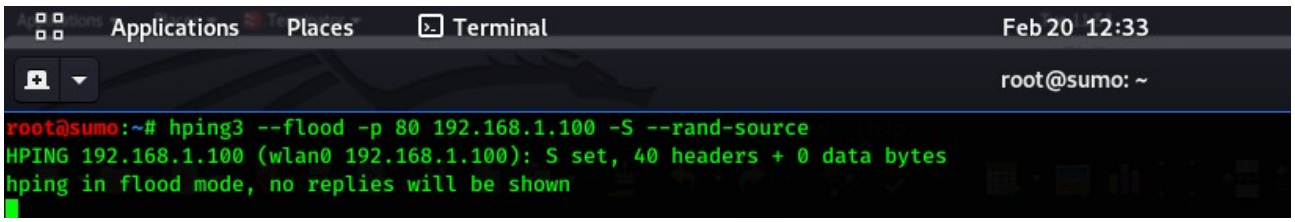
-S --syn
Set SYN tcp flag.

Step 1: Open terminal and type in “hping3 --flood -p 80 192.168.1.100 -S --rand-source”

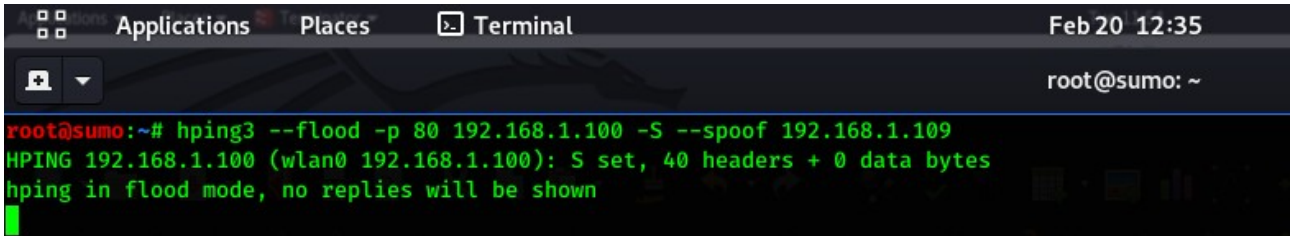
or

“ hping3 --flood -p 80 192.168.1.102 -S –spoof 192.168.1.109”
(To send flood from specified spoofed ip<192.168.1.109>)

Random:

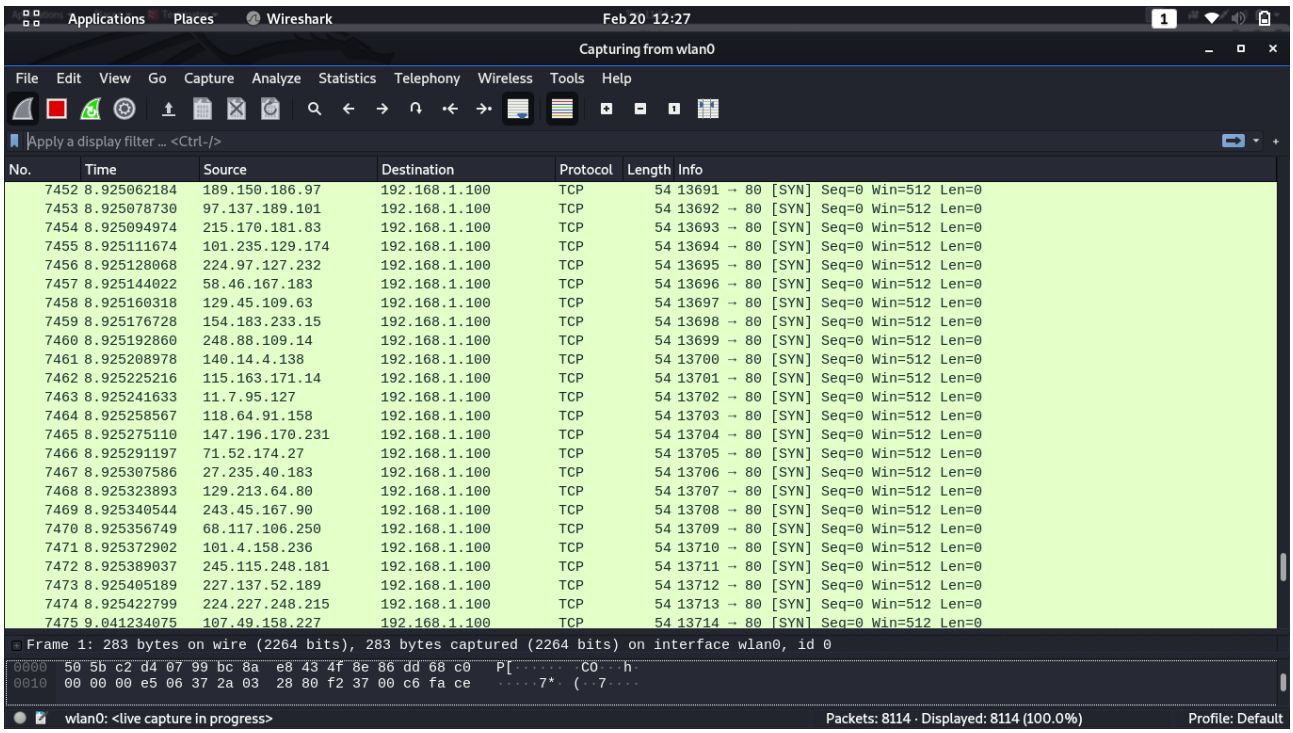


Specific:

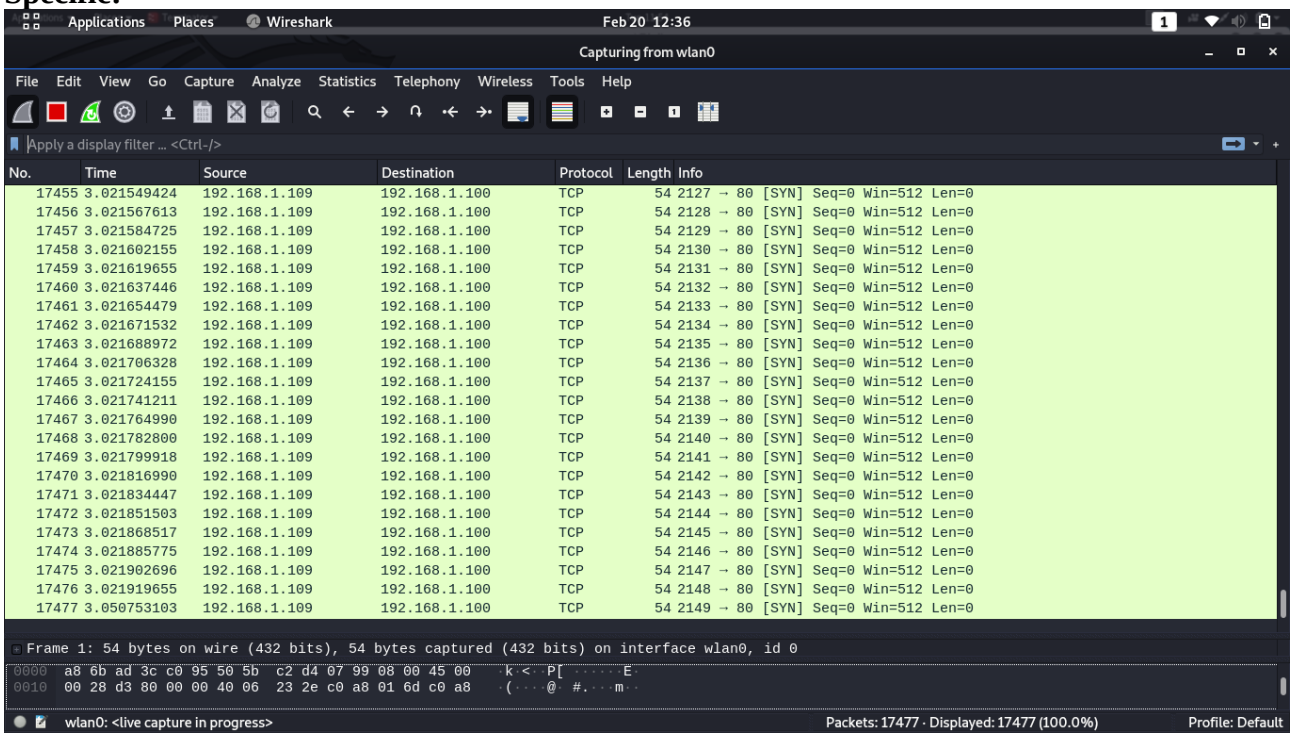


Step 2: Open Wireshark to see the traffic and observe that source keeps on changing although the desitination remains same in random where as in spoofed specific ip the source remains same as the spoofed one!

Random:

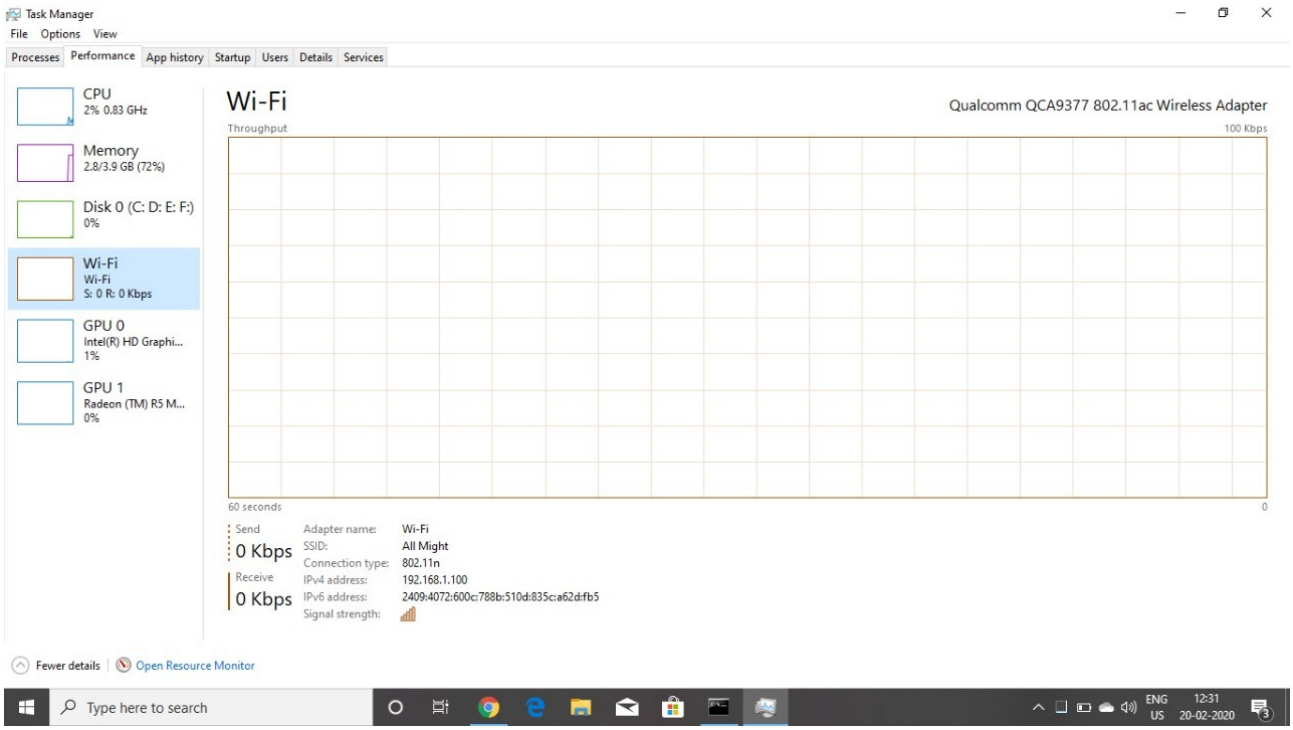


Specific:

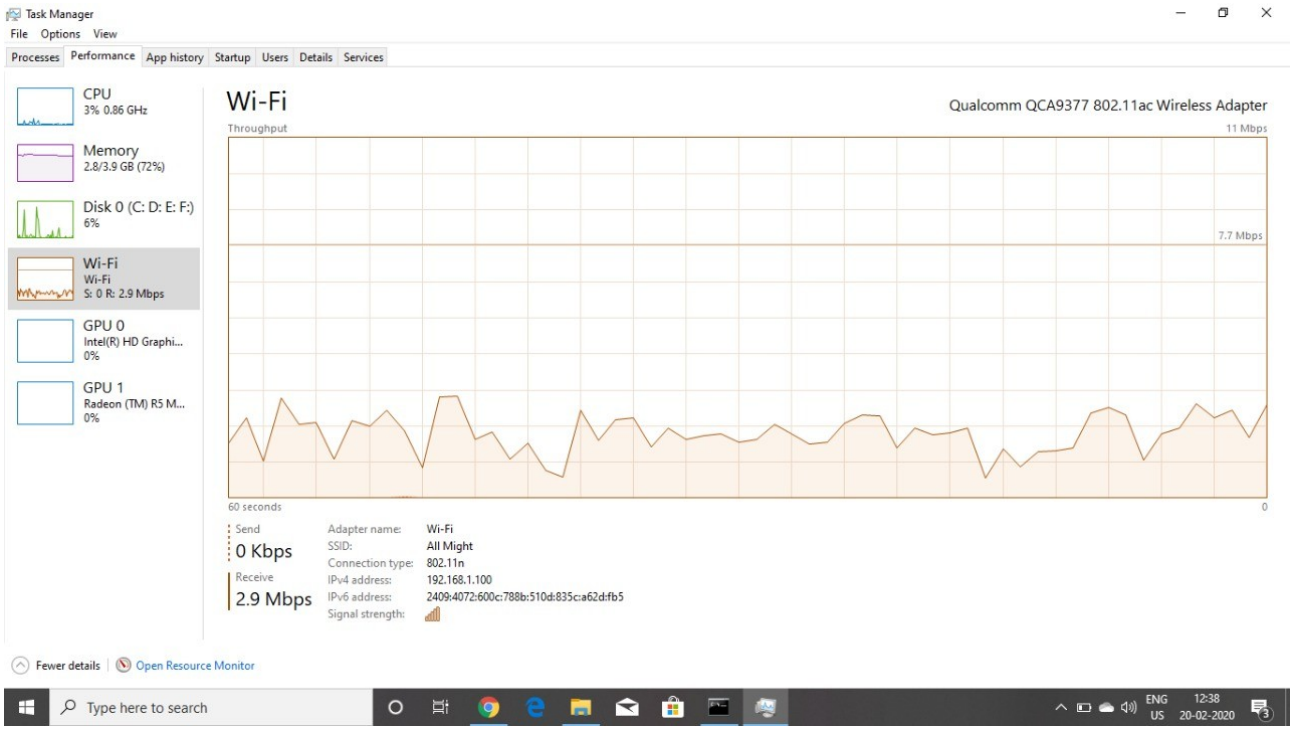


Step 3: Open Task manager in the Victim's PC there we can observe the jump in network traffic without sending any requests from the victim's machine!

Before:

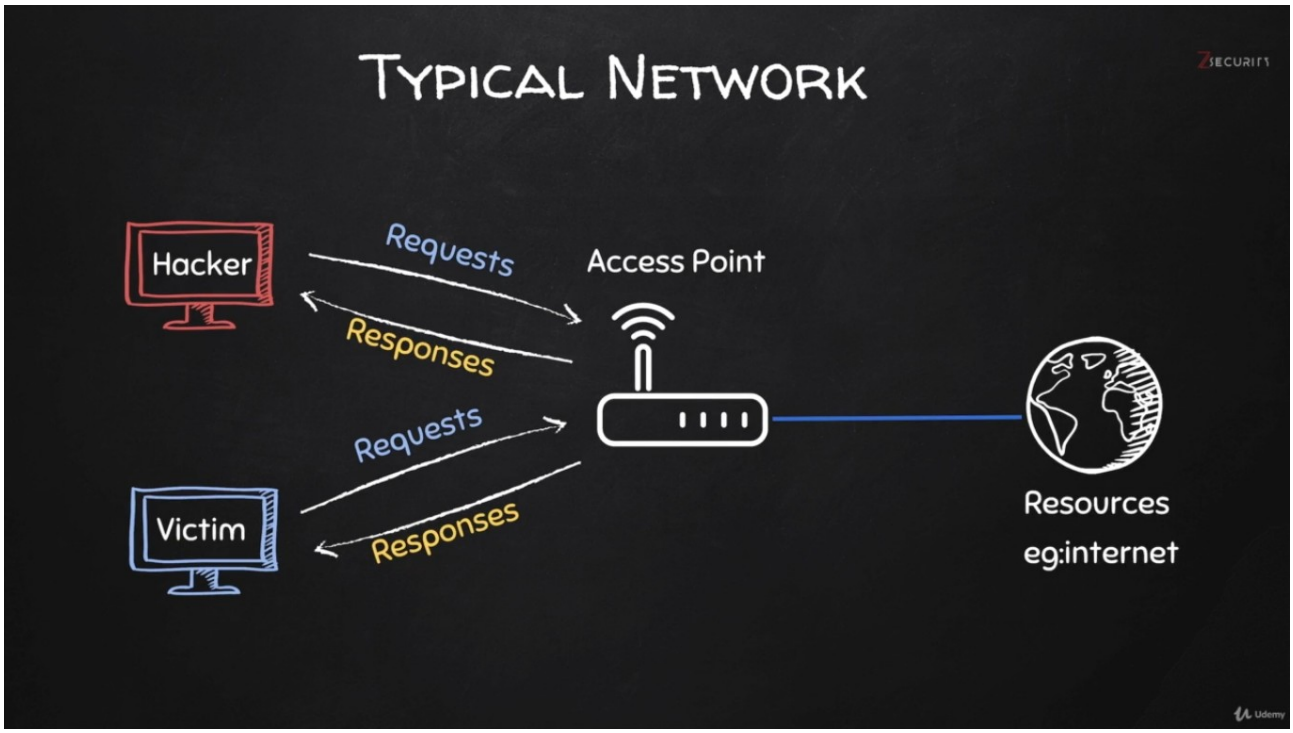


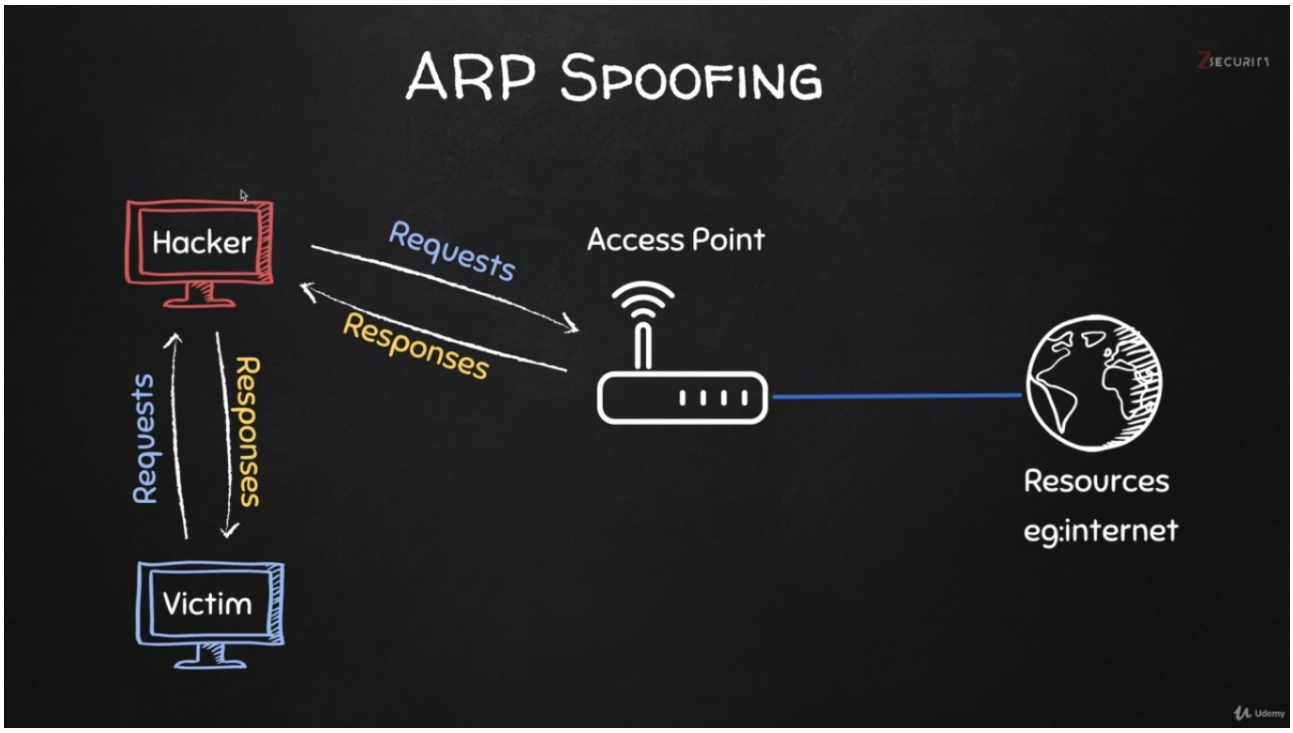
After:



2.ARP Spoofing:

ARP spoofing is a type of attack in which a malicious actor sends falsified **ARP** (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network



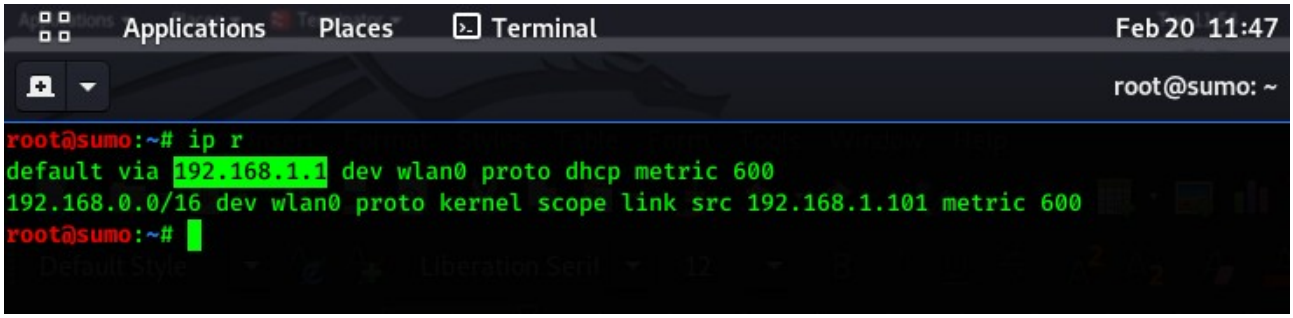


Usage:

arpspoof -i <interface> -t <target IP> <gateway ip>

Procedure:

Step 1: Type in “ip r” gives the gateway ip of the router



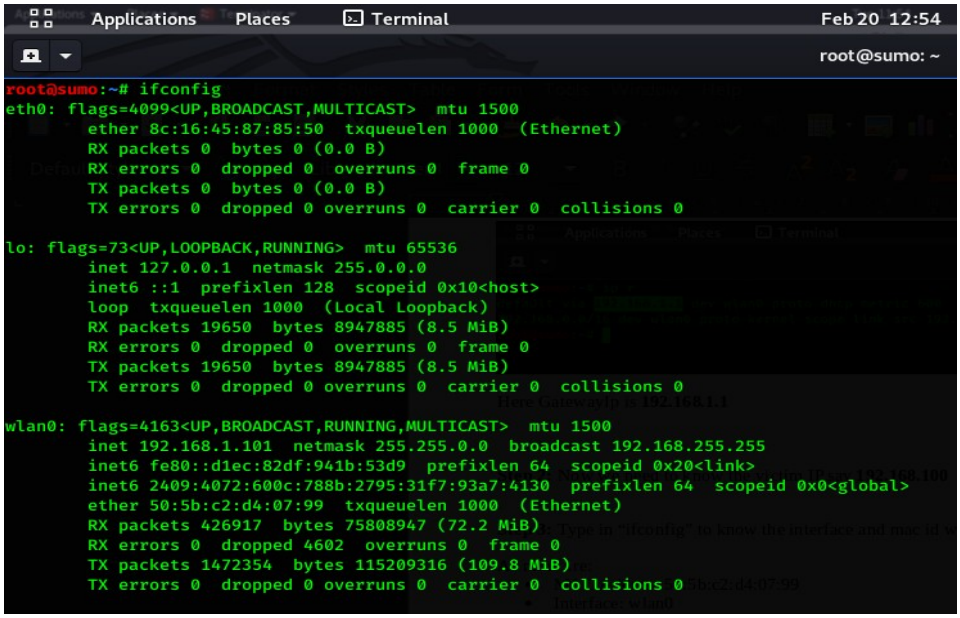
Here GatewayIp is **192.168.1.1**

Step 2: Now we need to know the victim IP say,**192.168.100**

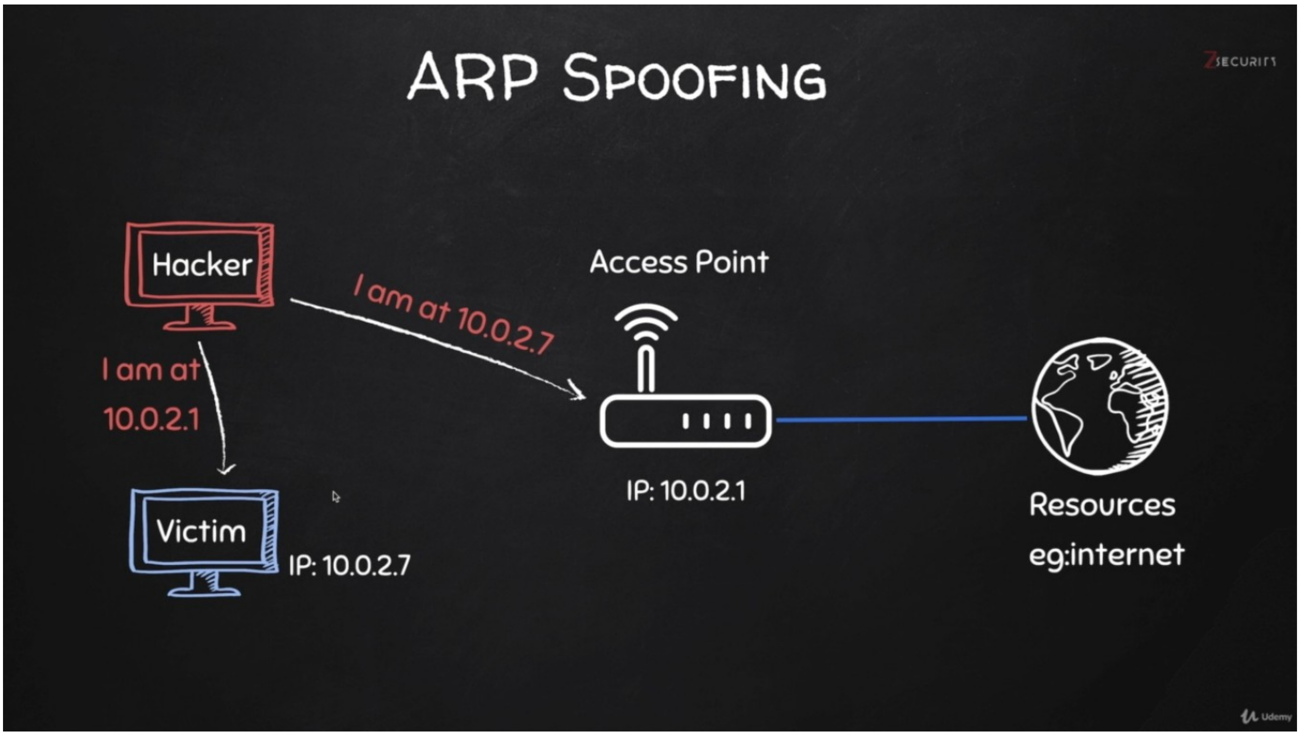
Step 3: Type in “ifconfig” to know the interface and mac id we are using

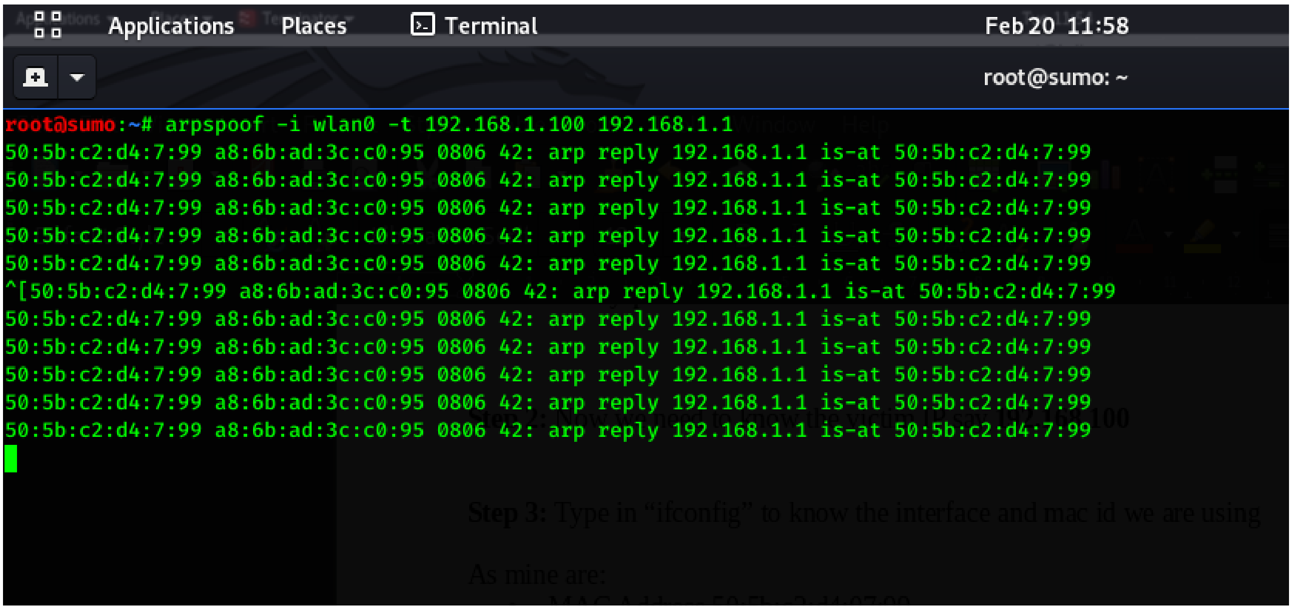
As mine are:

- MAC Address 50:5b:c2:d4:07:99
- Interface: wlan0

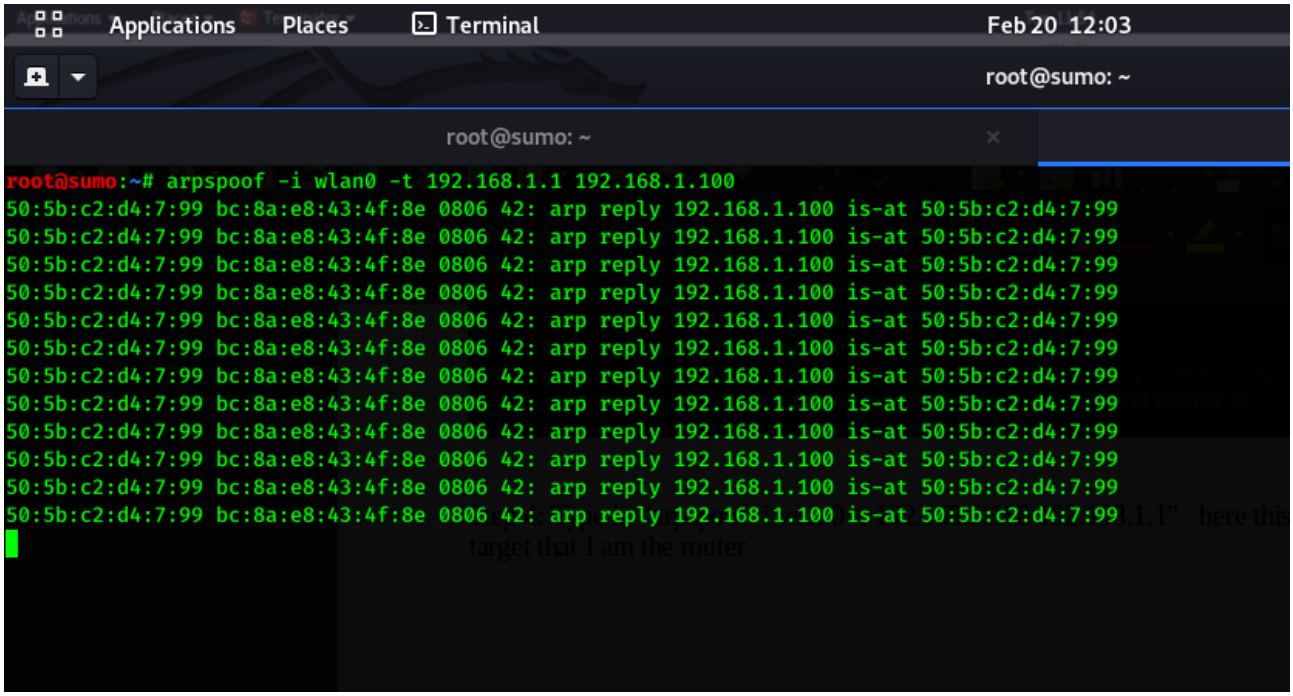


Step 4: Type in "arpspoof -i wlan0 -t 192.168.1.100 192.168.1.1"   here this command is to spoof target that I am the router



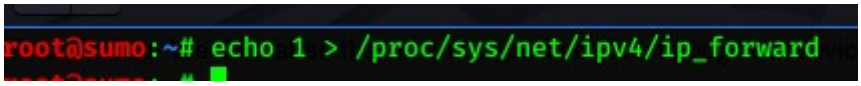


Step 5: Type in "arpspoof -i wlan0 -t 192.168.1.1 192.168.1.100"   here this command is to spoof router that I am the target



Here **a8:6b:ad:3c:c0:95(Victim's MAC id),bc:8a:e8:43:4f:8e(Router MAC id) and 50:5b:c2:d4:7:99(Attackers MAC id)**

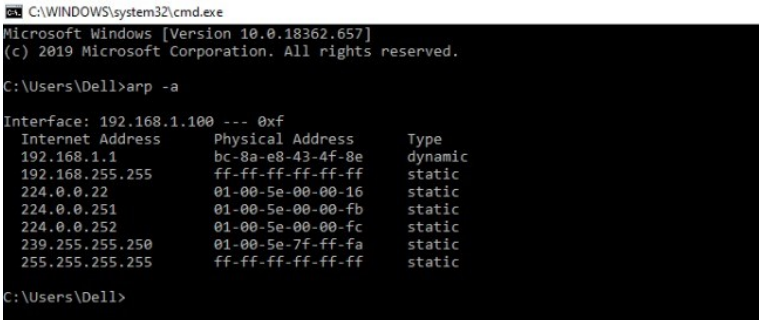
Step 6: Type in "echo 1 > /proc/sys/net/ipv4/ip_forward"



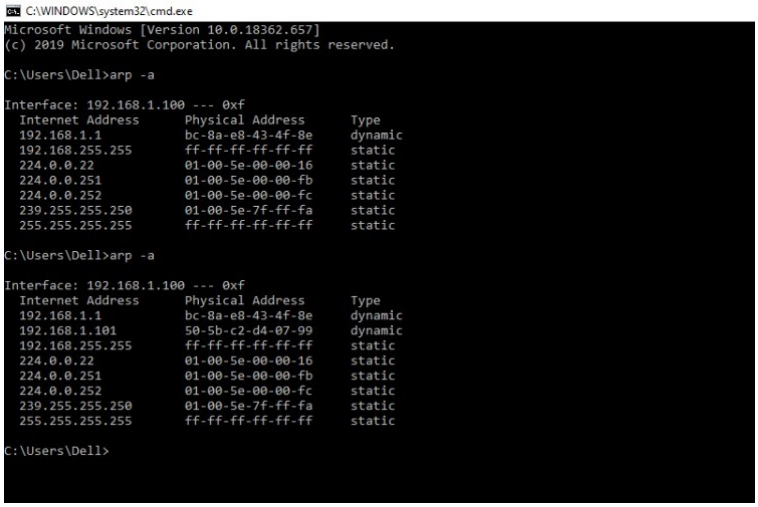
Enable the IP forwarding. so that when the packets flow through our attacker machine,they don't get dropped so that each packet that goes through our device gets actually forwarded to its destination. So, when we get a packet from the client, it goes to the router, and when a packet comes from the router, it should go to the client without being dropped in our device.

We can check the attack effectiveness in ARP tables in the victim machine

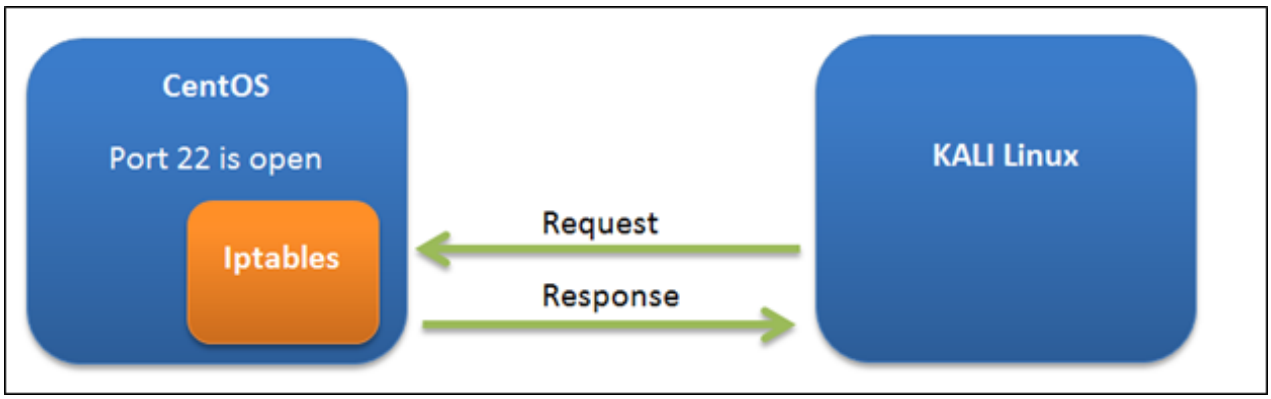
Before ArpSpoof:



After ArpSpoof:



Portspoof:




```
[root@localhost Desktop]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

As you can see, port 22 is open and any connection thorough the client machine to the server's ssh service is allowed.

```
root@root:~# nmap 192.168.150.142

Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-08 00:46 EST
Nmap scan report for 192.168.150.142
Host is up (0.00042s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:61:00:BC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
root@root:~#
```

```
root@root:~# nmap 192.168.150.142

Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-08 00:46 EST
Nmap scan report for 192.168.150.142
Host is up (0.00042s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:61:00:BC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
root@root:~#
```

Steps:

Iptables –f

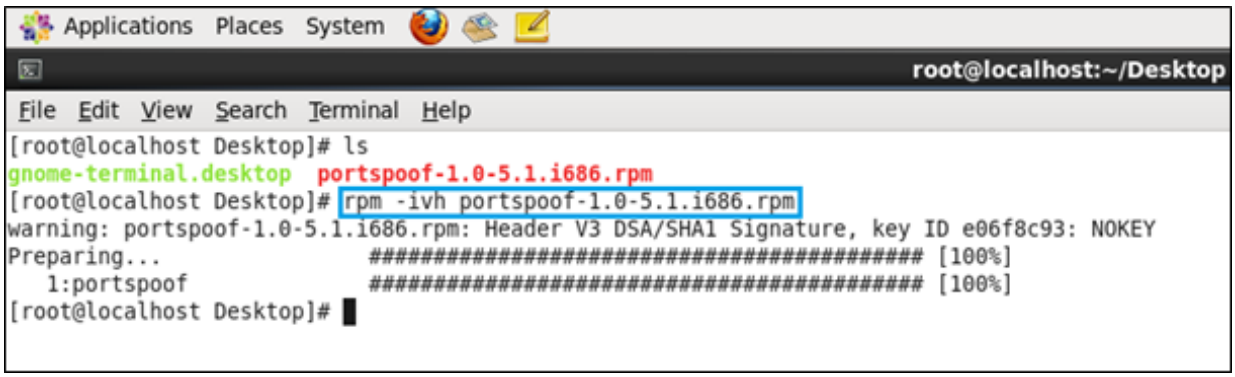
After giving this command, if you want to see the current policy, you can check it with this command:

iptables –l

```
[root@localhost Desktop]# iptables -F
[root@localhost Desktop]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost Desktop]#
```

Now it's time to configure our iptables with the portspoof. For that, let's download and install portspoof. I have downloaded the rpm package of portspoof. This command installs that package:

rpm –ivh portspoof-1.0-5.1.i686.rpm



Command/Command Option	Description
rpm	rpm package manager
-i	Install package
-v	Prints routine process verbose information
-h	Print 50 hash marks as the package archive is unpacked.

Now it is time to forward those packets to portspoof in order to reply the client machine. To do so, use the following command:

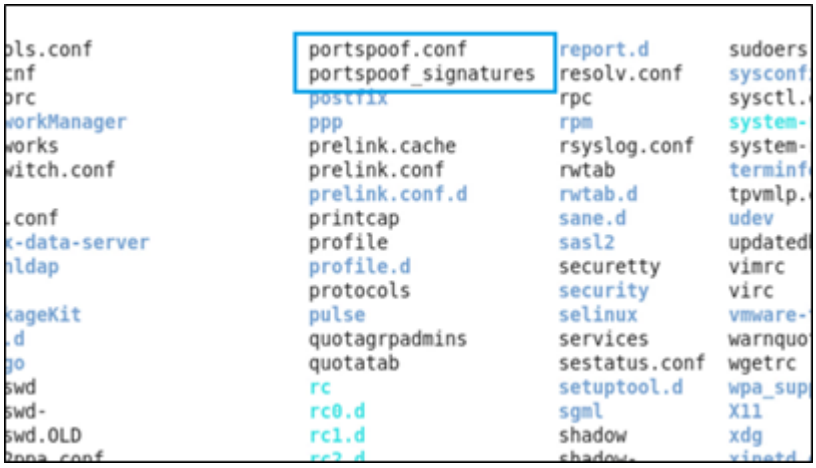
iptables –t nat –A PREROUTING –i eth0 –p tcp –m tcp –dport 1:65535 –j REDIRECT –to-ports 4444

Command/ Command Option	Description
Iptables	Linux default firewall.
-A	Appends the iptables rule to the end of the specified chain. This is the command used to add a rule when rule order in the chain does not matter.
-t	Specifies the table name which we are going to use.
-i	Selects the interface.
-m	Additional match options are also available through modules loaded by the `iptables` command. To use a match option module, load the module by name using the `-m` option, such as `-m <module-name>` (replacing *<module-name>* with the name of the module).
-p	Sets the default policy for the specified chain, so that when packets traverse an entire chain without matching a rule, they are sent on to the specified target, such as ACCEPT or DROP.
–dport	Sets a destination port
-j	Jump
–to-ports	Destination port to forward.

```
File  Edit  View  Search  Terminal  Help
[root@localhost Desktop]# iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:65535 -j REDIRECT --to-ports 4444
[root@localhost Desktop]#
```

first, it will collect all the packets accepted by iptables and then it will forward them to the 4444 port, which is by default a port of our portspoof tool.

Portspoof runs with its two main files which is lying in /etc/ folder, as shown below:



In the config file, all the rules have been written about how and what portspoof should reply to the client machine and in signatures there are lots of signature of various scanning tools.

```
root@root:~# nmap  192.168.150.142

Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-08 02:16 EST
Nmap scan report for 192.168.150.142
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.150.142 are closed
MAC Address: 00:0C:29:61:00:BC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@root:~#
```

To start portspoof, let's check the help to determine which options are provided to us.

```
[root@localhost etc]# portspoof -h
Usage: portspoof [OPTION]...
Portspoof - service emulator / frontend exploitation framework.

-i                      ip : Bind to a particular  IP address
-p                      port : Bind to a particular PORT number
-s                      file_path : Portspoof service signature regex. file
-c                      file_path : Portspoof configuration file
-l                      file_path : Log port scanning alerts to a file
-f                      file_path : FUZZER_MODE - fuzzing payload file list
-n                      file_path : FUZZER_MODE - wrapping signatures file list
-1                      FUZZER_MODE - generate fuzzing payloads internally
-2                      switch to simple reply mode (doesn't work for Nmap)!
-D                      run as daemon process
-d                      disable syslog
-v                      be verbose
-h                      display this help and exit
[root@localhost etc]#
```

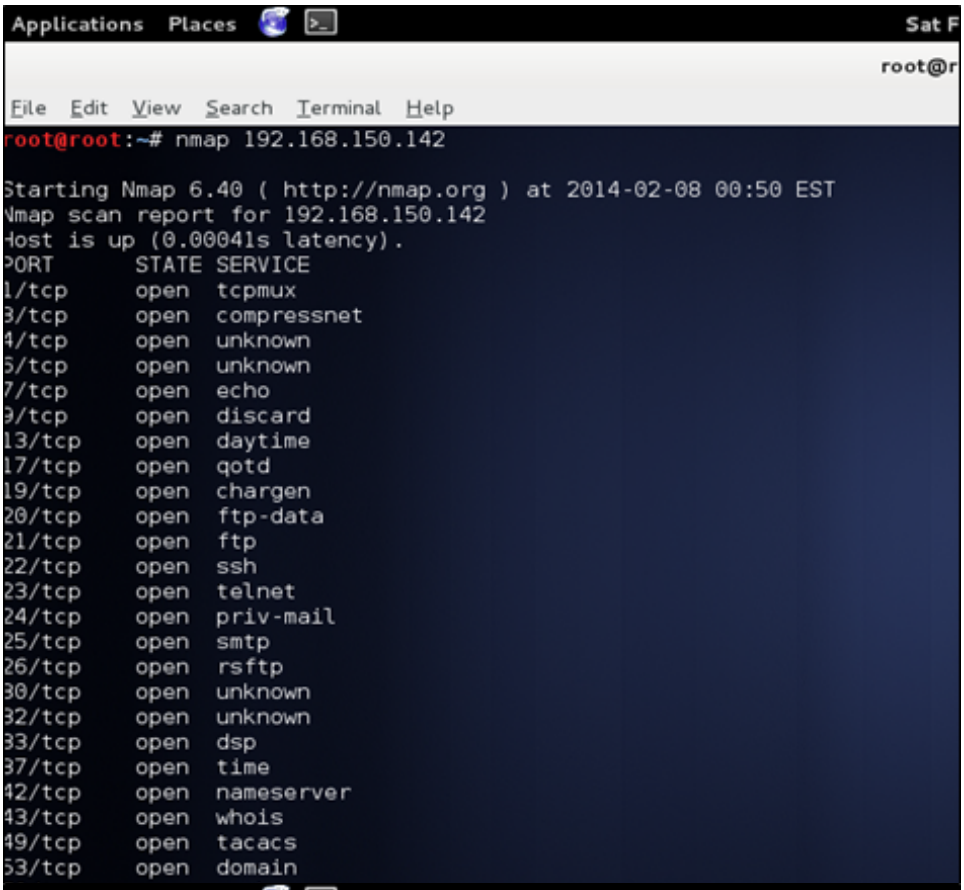
Two mandatory options are needed to run the portspoof. The command to run portspoof is:

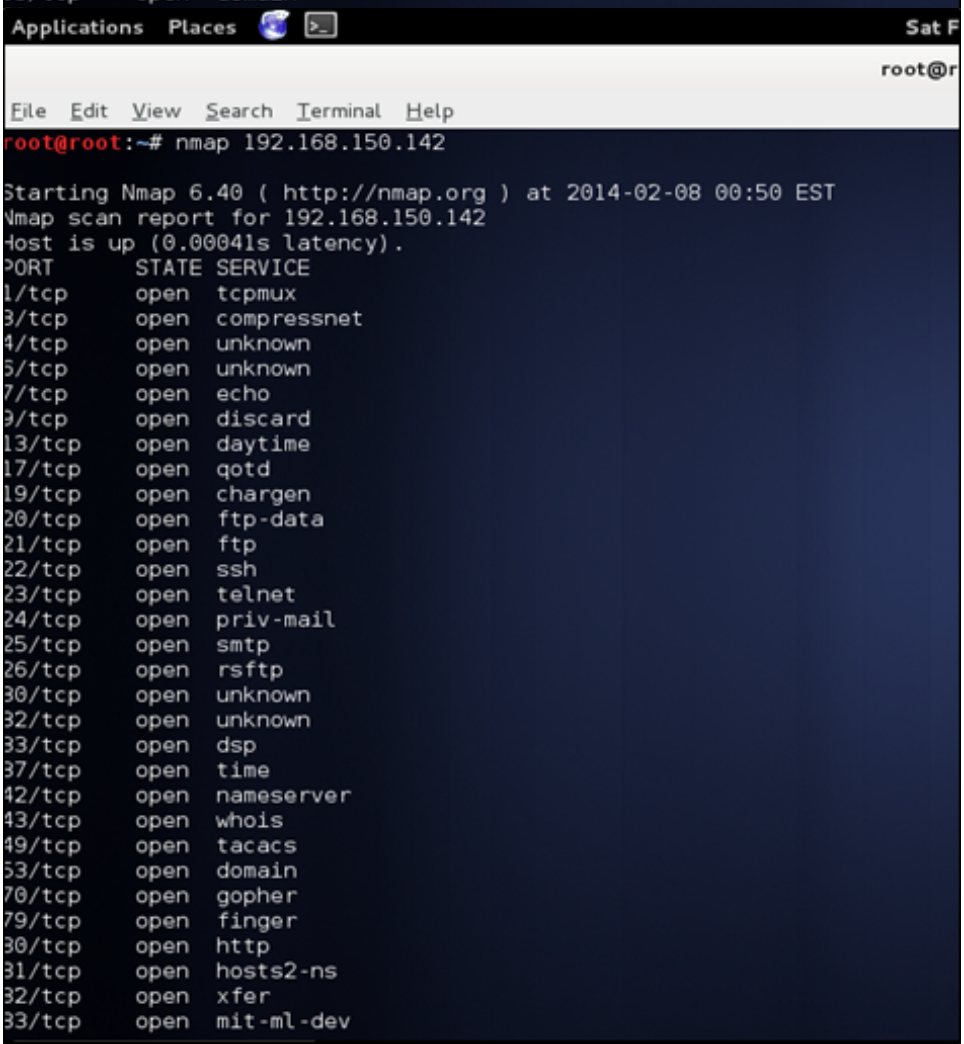
portspoof –c /etc/portspoof.conf –s /etc/portspoof_signatures

Once you give this command it will look like this:

```
File  Edit  View  Search  Terminal  Help
[root@localhost Desktop]# iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:65535 -j REDIRECT --to-ports 4444
[root@localhost Desktop]# portspoof -c /etc/portspoof.conf -s /etc/portspoof_signatures
-> Using user defined configuration file /etc/portspoof.conf
-> Using user defined signature file /etc/portspoof_signatures
```

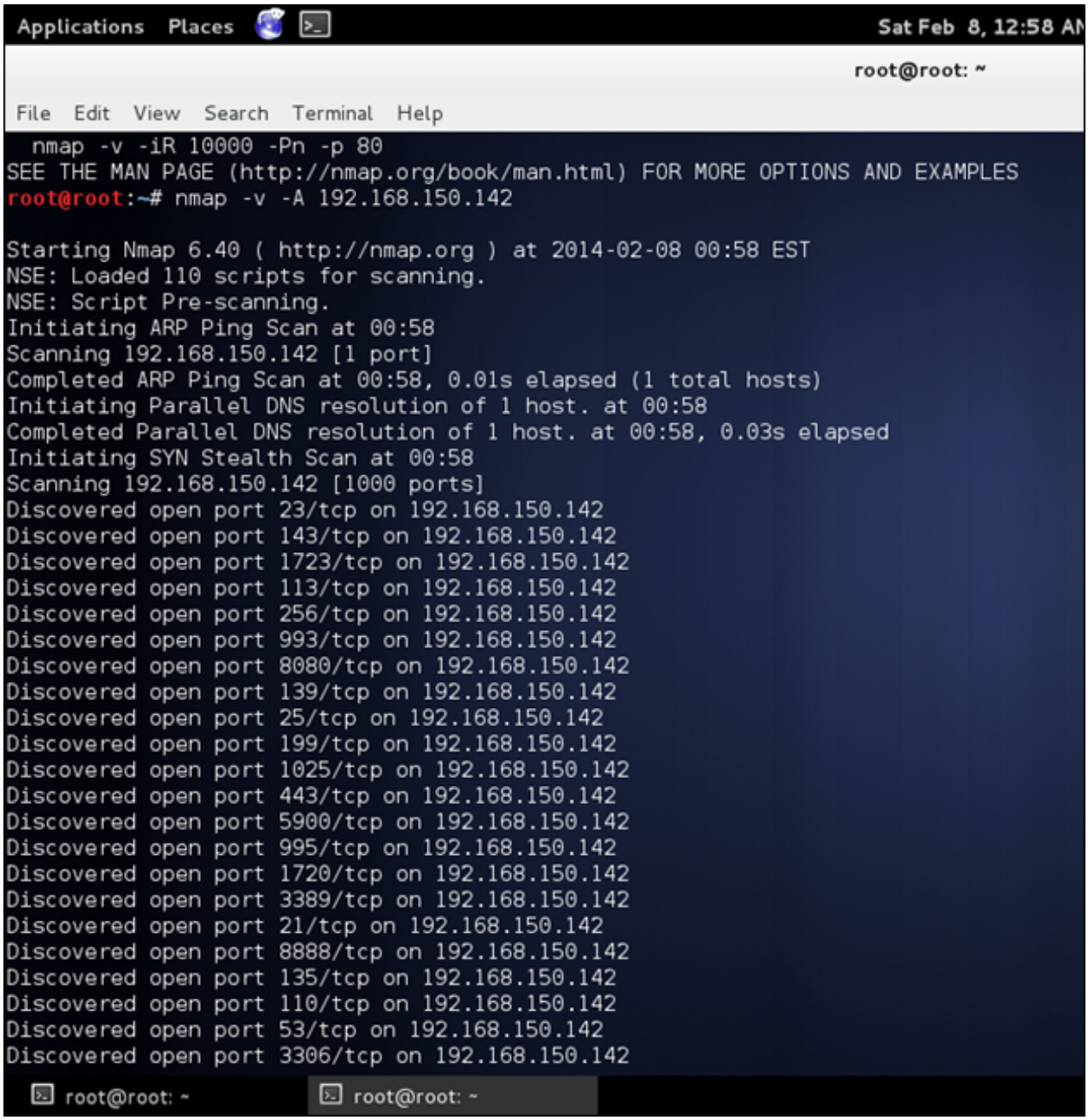
Now it is time to scan from our attacker machine (Kali Linux


Applications Places
Sat F
root@r
File Edit View Search Terminal Help
root@root:~# nmap 192.168.150.142
Starting Nmap 6.40 (http://nmap.org) at 2014-02-08 00:50 EST
Nmap scan report for 192.168.150.142
Host is up (0.00041s latency).
PORT STATE SERVICE
1/tcp open tcpmux
3/tcp open compressnet
4/tcp open unknown
5/tcp open unknown
7/tcp open echo
9/tcp open discard
13/tcp open daytime
17/tcp open qotd
19/tcp open chargen
20/tcp open ftp-data
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
24/tcp open priv-mail
25/tcp open smtp
26/tcp open rsftp
30/tcp open unknown
32/tcp open unknown
33/tcp open dsp
37/tcp open time
42/tcp open nameserver
43/tcp open whois
49/tcp open tacacs
53/tcp open domain

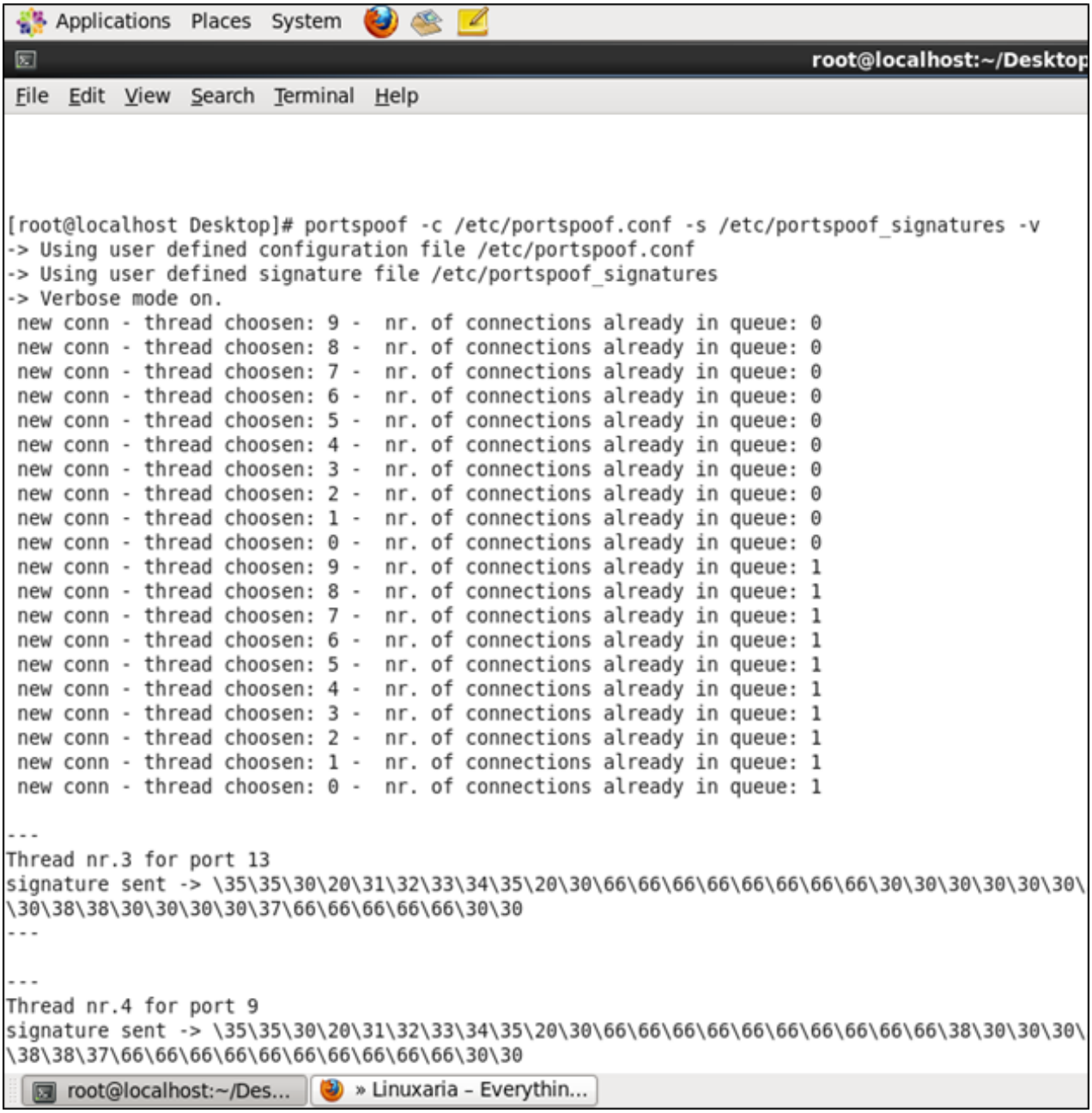

Applications Places
Sat F
root@r
File Edit View Search Terminal Help
root@root:~# nmap 192.168.150.142
Starting Nmap 6.40 (http://nmap.org) at 2014-02-08 00:50 EST
Nmap scan report for 192.168.150.142
Host is up (0.00041s latency).
PORT STATE SERVICE
1/tcp open tcpmux
3/tcp open compressnet
4/tcp open unknown
5/tcp open unknown
7/tcp open echo
9/tcp open discard
13/tcp open daytime
17/tcp open qotd
19/tcp open chargen
20/tcp open ftp-data
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
24/tcp open priv-mail
25/tcp open smtp
26/tcp open rsftp
30/tcp open unknown
32/tcp open unknown
33/tcp open dsp
37/tcp open time
42/tcp open nameserver
43/tcp open whois
49/tcp open tacacs
53/tcp open domain
70/tcp open gopher
79/tcp open finger
80/tcp open http
81/tcp open hosts2-ns
82/tcp open xfer
83/tcp open mit-ml-dev

As you can see, starting from 1, it will show all 65535 ports open. Actually these ports are not actually open and some don't eve exist, but this is how we are fooling the attacker to make him see all 65535 ports are opened.

If you want to scan that host with any signature within nmap then it will show as below. I am using nmap with the –v and –A options. Then the result, will be as shown below:



You may remember that, when we started portspoof, it was in verbose mode. So if we check the host machine now, it will show some information about which kinds of threads have been coming in and which kind of signature reply that portspoof tool has given in respond to that request. This information will be shown like this:


Applications Places System
root@localhost:~/Desktop
File Edit View Search Terminal Help
[root@localhost Desktop]# portspoof -c /etc/portspoof.conf -s /etc/portspoof_signatures -v
-> Using user defined configuration file /etc/portspoof.conf
-> Using user defined signature file /etc/portspoof_signatures
-> Verbose mode on.
new conn - thread choosen: 9 - nr. of connections already in queue: 0
new conn - thread choosen: 8 - nr. of connections already in queue: 0
new conn - thread choosen: 7 - nr. of connections already in queue: 0
new conn - thread choosen: 6 - nr. of connections already in queue: 0
new conn - thread choosen: 5 - nr. of connections already in queue: 0
new conn - thread choosen: 4 - nr. of connections already in queue: 0
new conn - thread choosen: 3 - nr. of connections already in queue: 0
new conn - thread choosen: 2 - nr. of connections already in queue: 0
new conn - thread choosen: 1 - nr. of connections already in queue: 0
new conn - thread choosen: 0 - nr. of connections already in queue: 0
new conn - thread choosen: 9 - nr. of connections already in queue: 1
new conn - thread choosen: 8 - nr. of connections already in queue: 1
new conn - thread choosen: 7 - nr. of connections already in queue: 1
new conn - thread choosen: 6 - nr. of connections already in queue: 1
new conn - thread choosen: 5 - nr. of connections already in queue: 1
new conn - thread choosen: 4 - nr. of connections already in queue: 1
new conn - thread choosen: 3 - nr. of connections already in queue: 1
new conn - thread choosen: 2 - nr. of connections already in queue: 1
new conn - thread choosen: 1 - nr. of connections already in queue: 1
new conn - thread choosen: 0 - nr. of connections already in queue: 1

Thread nr.3 for port 13
signature sent -> \35\35\30\20\31\32\33\34\35\20\30\66\66\66\66\66\66\66\66\30\30\30\30\30\30\
\30\38\38\30\30\30\30\37\66\66\66\66\66\30\30

Thread nr.4 for port 9
signature sent -> \35\35\30\20\31\32\33\34\35\20\30\66\66\66\66\66\66\66\66\66\66\38\30\30\30\
\38\38\37\66\66\66\66\66\66\66\66\66\66\30\30
root@localhost:~/Des...
» Linuxaria – Everythin...

Penetration Testing and Vulnerability Assessment Lab

Assignment 01

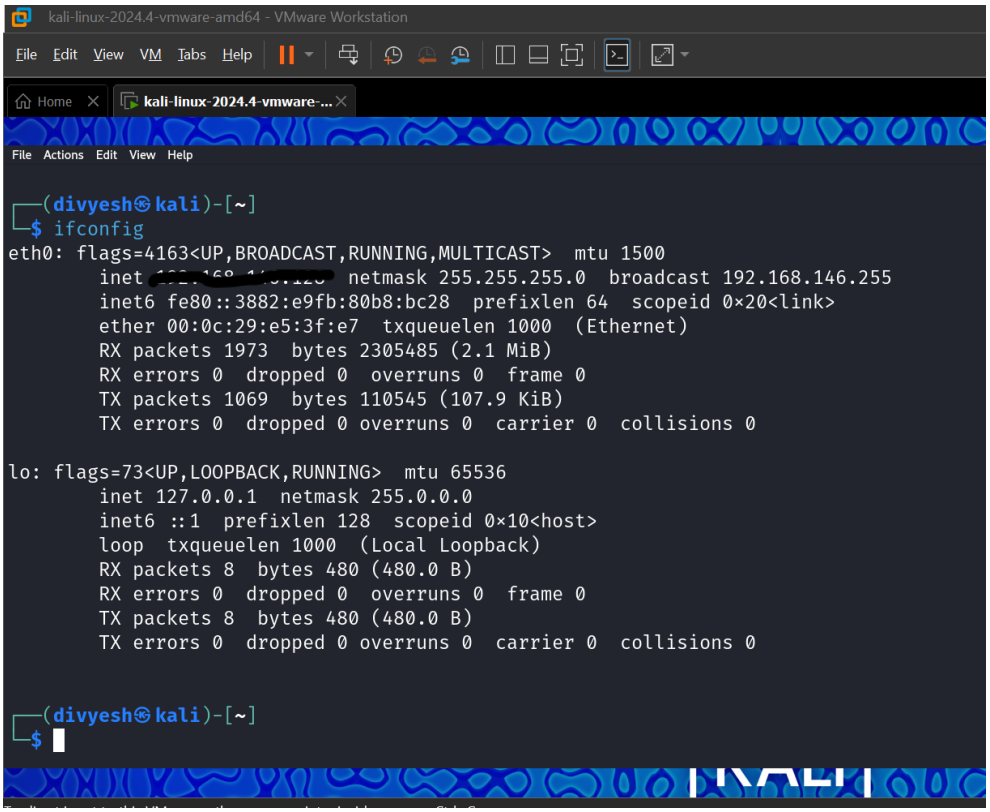
Divyesh Tharakan

24MCI0004

MTech CSE IS

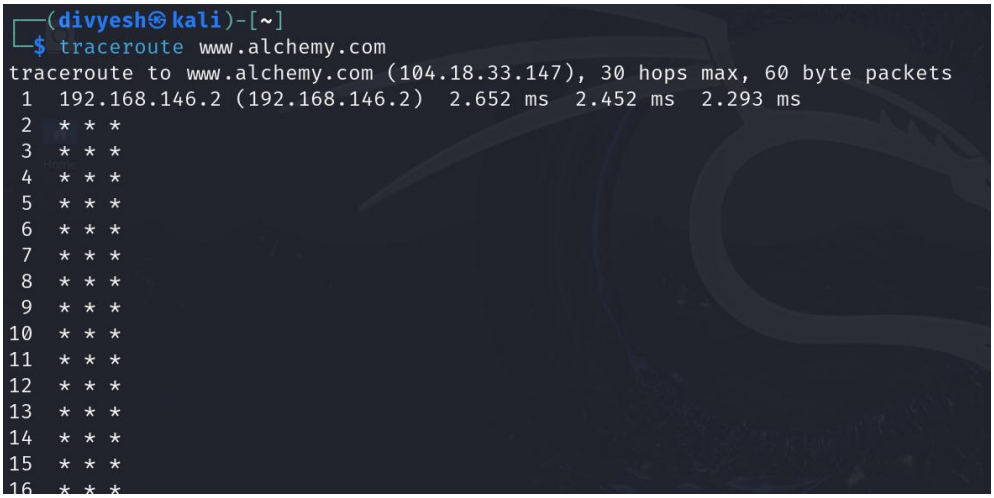
---

1. **Ifconfig command** – executed to get the IP address of the particular machine which you're currently on.



2. Traceroute

   Used to troubleshoot a network



3. Tracepath

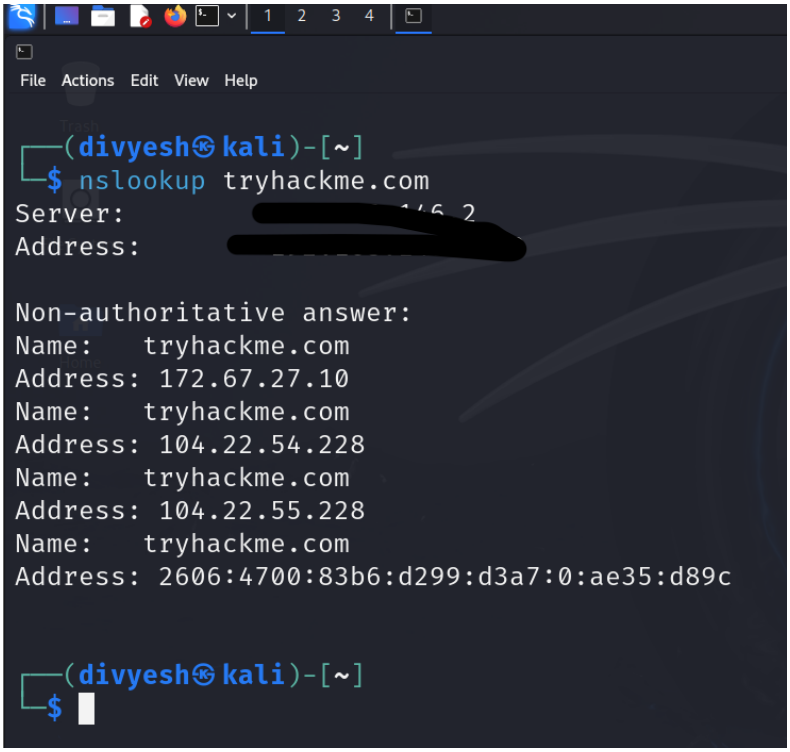
4. Ping command

```
┌──(divyesh㉿kali)-[~]
└─$ sudo ping www.tryhackme.com
PING www.tryhackme.com (104.22.54.228) 56(84) bytes of data.
64 bytes from 104.22.54.228: icmp_seq=1 ttl=128 time=9.97 ms
64 bytes from 104.22.54.228: icmp_seq=2 ttl=128 time=48.9 ms
64 bytes from 104.22.54.228: icmp_seq=3 ttl=128 time=14.4 ms
64 bytes from 104.22.54.228: icmp_seq=4 ttl=128 time=88.5 ms
64 bytes from 104.22.54.228: icmp_seq=5 ttl=128 time=85.2 ms
64 bytes from 104.22.54.228: icmp_seq=6 ttl=128 time=29.7 ms
64 bytes from 104.22.54.228: icmp_seq=7 ttl=128 time=26.1 ms
64 bytes from 104.22.54.228: icmp_seq=8 ttl=128 time=20.7 ms
64 bytes from 104.22.54.228: icmp_seq=9 ttl=128 time=27.7 ms
64 bytes from 104.22.54.228: icmp_seq=10 ttl=128 time=20.2 ms
64 bytes from 104.22.54.228: icmp_seq=11 ttl=128 time=13.3 ms
64 bytes from 104.22.54.228: icmp_seq=12 ttl=128 time=13.0 ms
64 bytes from 104.22.54.228: icmp_seq=13 ttl=128 time=14.8 ms
64 bytes from 104.22.54.228: icmp_seq=14 ttl=128 time=18.6 ms
64 bytes from 104.22.54.228: icmp_seq=15 ttl=128 time=19.9 ms
```

5. Netstat command

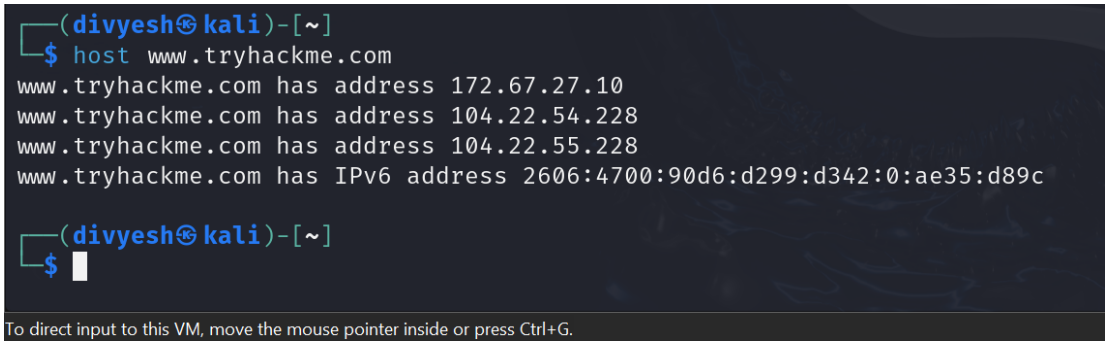
```
File  Actions  Edit  View  Help
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 [redacted]:bootpc  192.168.146.254:bootps  ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     12006
unix  3      [ ]         STREAM     CONNECTED     12301    /run/user/1000/at-spi/bus_0
unix  3      [ ]         DGRAM      CONNECTED     11281
unix  3      [ ]         STREAM     CONNECTED     8627     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12399    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     11688
unix  3      [ ]         STREAM     CONNECTED     10978    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     9500
unix  3      [ ]         STREAM     CONNECTED     12661    /run/user/1000/at-spi/bus_0
unix  2      [ ]         DGRAM                    9131
unix  3      [ ]         STREAM     CONNECTED     12336    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12078    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12357    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     10777    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12012    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     11693    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     10970
```

6. Nslookup command

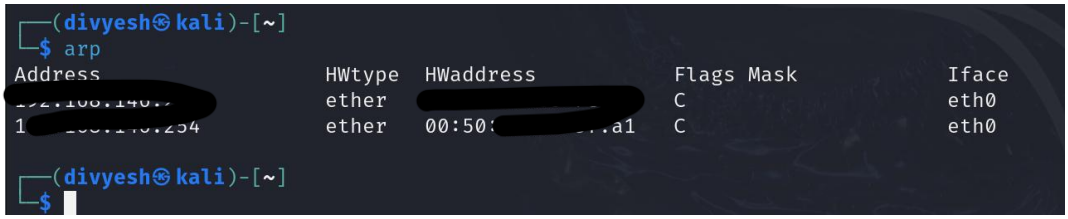


7. Route command

8. Host

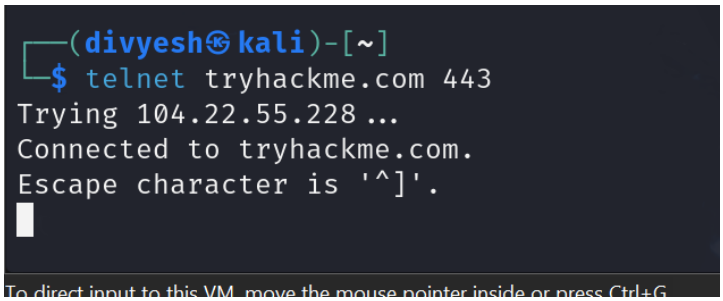


9. ARP



10. Curl command

11.telnet



12. whois command

```
┌──(divyesh㉿kali)-[~]
└─$ whois hackerrank.com
   Domain Name: HACKERRANK.COM
   Registry Domain ID: 1723775946_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.name.com
   Registrar URL: http://www.name.com
   Updated Date: 2024-05-07T21:34:39Z
   Creation Date: 2012-05-30T00:39:04Z
   Registry Expiry Date: 2027-05-30T00:39:04Z
   Registrar: Name.com, Inc.
   Registrar IANA ID: 625
   Registrar Abuse Contact Email: abuse@name.com
   Registrar Abuse Contact Phone: 7202492374
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS-1314.AWSDNS-36.ORG
   Name Server: NS-1691.AWSDNS-19.CO.UK
   Name Server: NS-431.AWSDNS-53.COM
   Name Server: NS-525.AWSDNS-01.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-02-24T11:46:59Z <<<

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

13.Nload

```
File  Actions  Edit  View  Help
Device eth0 [redacted] (1/2):
Incoming:

                                  Curr: 0.00 Bit/s
                                  Avg: 96.00 Bit/s
                                  Min: 0.00 Bit/s
                                  Max: 712.00 Bit/s
                                  Ttl: 473.36 kByte
Outgoing:

                                  Curr: 0.00 Bit/s
                                  Avg: 96.00 Bit/s
                                  Min: 0.00 Bit/s
                                  Max: 712.00 Bit/s
                                  Ttl: 329.12 kByte
```

Penetration Testing and Vulnerability Assessment Lab

Assignment 02

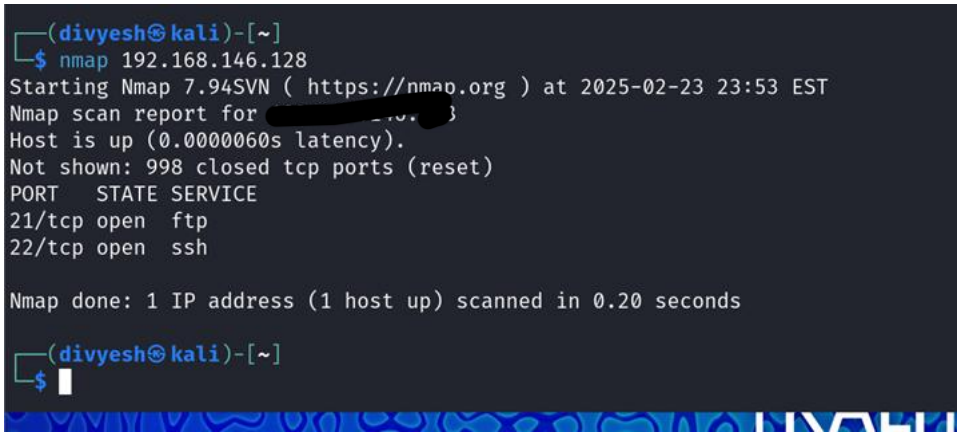
Divyesh Tharakan

24MCI0004

MTech CSE IS

---

1. **Nmap** : Basically used to scan networks to find active hosts. It can be a website URL or the IP address. It also detects open ports and services.



· Here, ssh and ftp ports have already been opened previously which is why the state is open. The command for the same is :

o For FTP :

§ sudo apt install vsftpd -y

§ sudo systemctl enable vsftpd

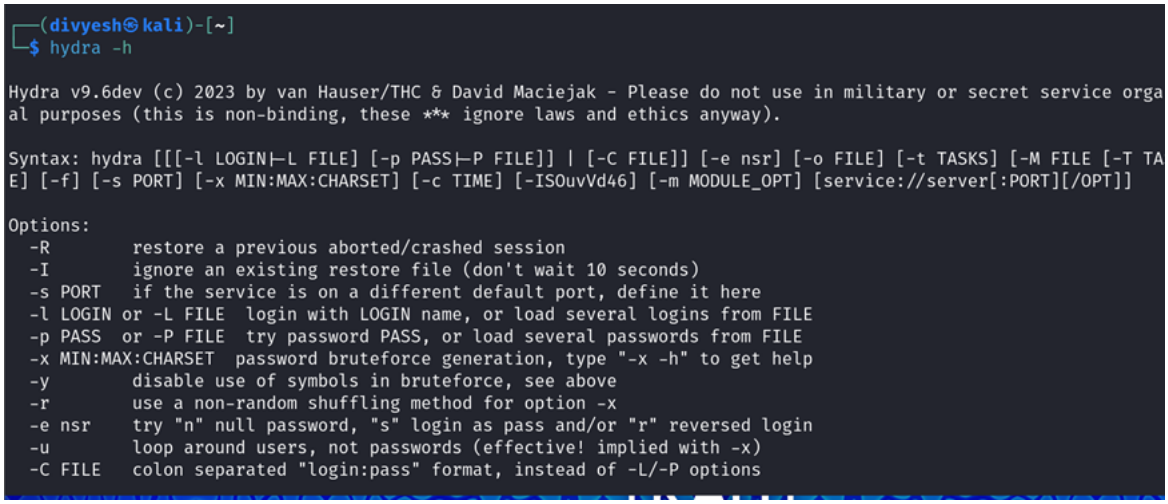
§ sudo systemctl start vsftpd

o For SSH :

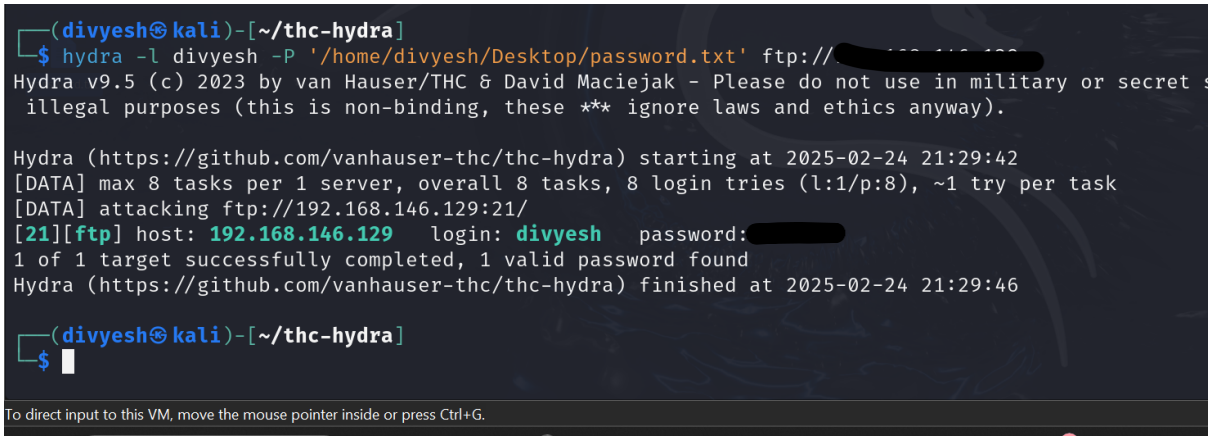
§ sudo systemctl enable ssh

§ sudo systemctl start ssh

2. **Hydra** : Hydra is a powerful tool used in penetration testing to perform brute-force attacks on various services like SSH, FTP, RDP, MySQL, and more.



Attack on a password list which contains the correct password and all incorrect passwords.



3. IP Spoofing :

- IP Spoofing to a random source

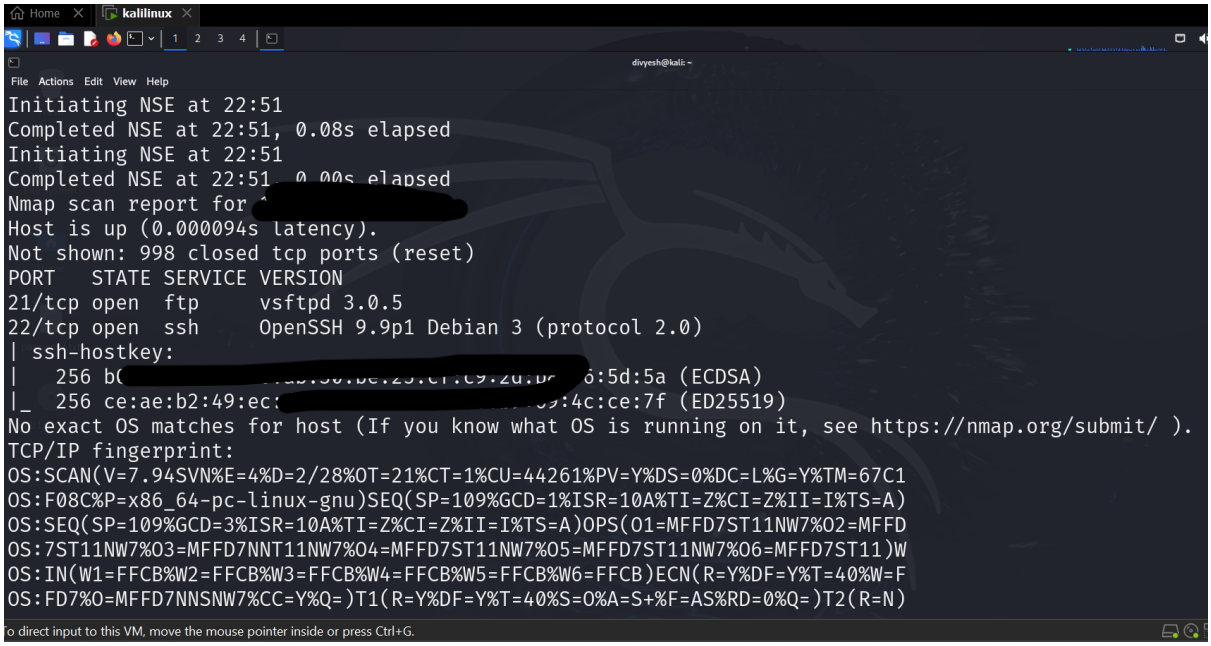
```
┌──(divyesh㉿kali)-[~/thc-hydra]
└─$ sudo hping3 --flood -p 80 [redacted] -S --rand-source
[sudo] password for divyesh:
HPING 192.168.146.129 (eth0 [redacted]): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

- To a specific address

```
┌──(divyesh㉿kali)-[~]
└─$ sudo hping3 --flood -p 80 [redacted] --spoof 152.58.224.79
[sudo] password for divyesh:
HPING 192.168.146.129 (eth0 [redacted]): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

4. Port Spoofing

```
┌──(divyesh㉿kali)-[~]
└─$ nmap -v -A [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 22:51 IST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:51
Completed NSE at 22:51, 0.00s elapsed
Initiating NSE at 22:51
Completed NSE at 22:51, 0.00s elapsed
Initiating NSE at 22:51
Completed NSE at 22:51, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:51
Completed Parallel DNS resolution of 1 host. at 22:51, 0.06s elapsed
Initiating SYN Stealth Scan at 22:51
Scanning 192.168.146.129 [1000 ports]
Discovered open port 21/tcp on [redacted]
Discovered open port 22/tcp on [redacted]
Completed SYN Stealth Scan at 22:51, 0.06s elapsed (1000 total ports)
Initiating Service scan at 22:51
Scanning 2 services on [redacted]
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```


Home
kalilinux
1 2 3 4
divyesh@kali: ~
File Actions Edit View Help
Initiating NSE at 22:51
Completed NSE at 22:51, 0.08s elapsed
Initiating NSE at 22:51
Completed NSE at 22:51, 0.00s elapsed
Nmap scan report for [redacted]
Host is up (0.000094s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.5
22/tcp open ssh OpenSSH 9.9p1 Debian 3 (protocol 2.0)
| ssh-hostkey:
| 256 b[redacted]:5d:5a (ECDSA)
|_ 256 ce:ae:b2:49:ec[redacted]:4c:ce:7f (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/28%OT=21%CT=1%CU=44261%PV=Y%DS=0%DC=L%G=Y%TM=67C1
OS:F08C%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=109%GCD=3%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O1=MFFD7ST11NW7%O2=MFFD
OS:7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFFD7ST11NW7%O6=MFFD7ST11)W
OS:IN(W1=FFCB%W2=FFCB%W3=FFCB%W4=FFCB%W5=FFCB%W6=FFCB)ECN(R=Y%DF=Y%T=40%W=F
OS:FD7%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Penetration Testing and Vulnerability Assessment Lab

Assignment 03

Divyesh Tharakan

24MCI0004

MTech CSE IS

JCryptool

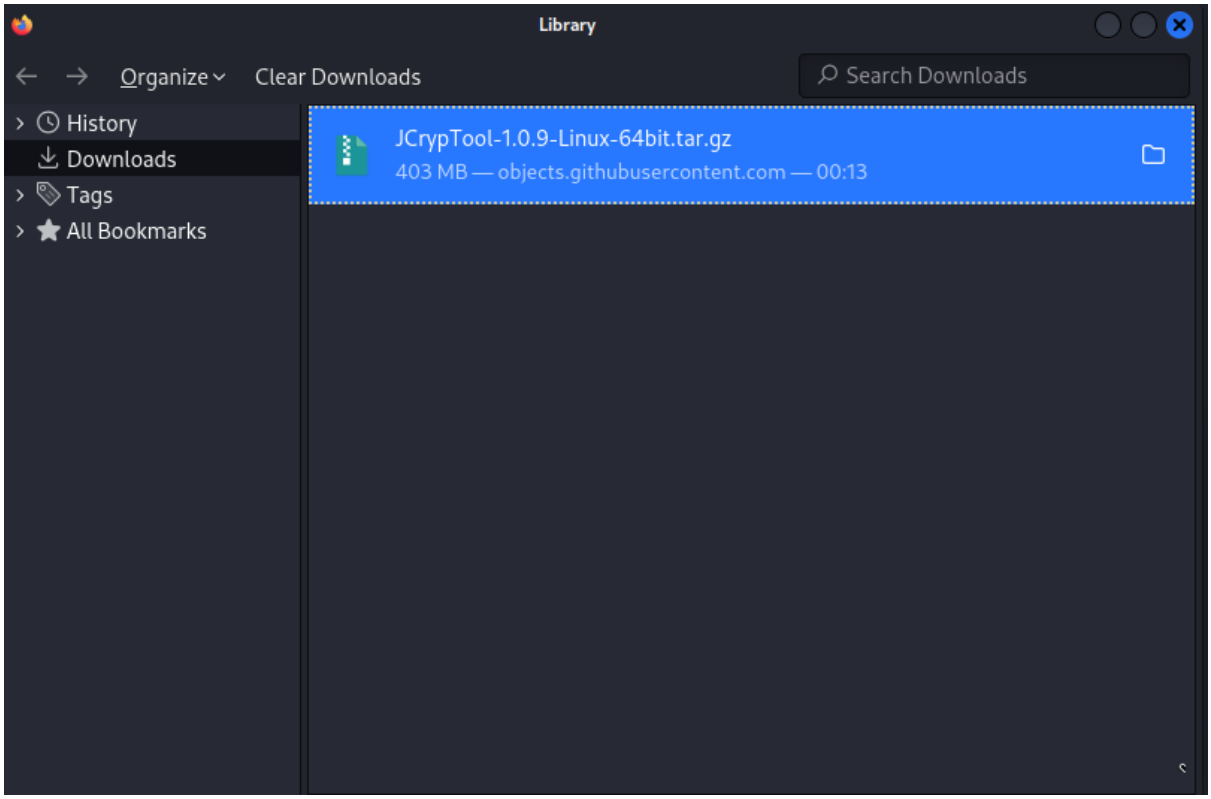
JCrypTool (JCT) is an open-source cryptography e-learning platform based on Java. It helps users experiment with and understand various cryptographic techniques such as encryption, decryption, hashing, and digital signatures.

Key Features of JCrypTool:

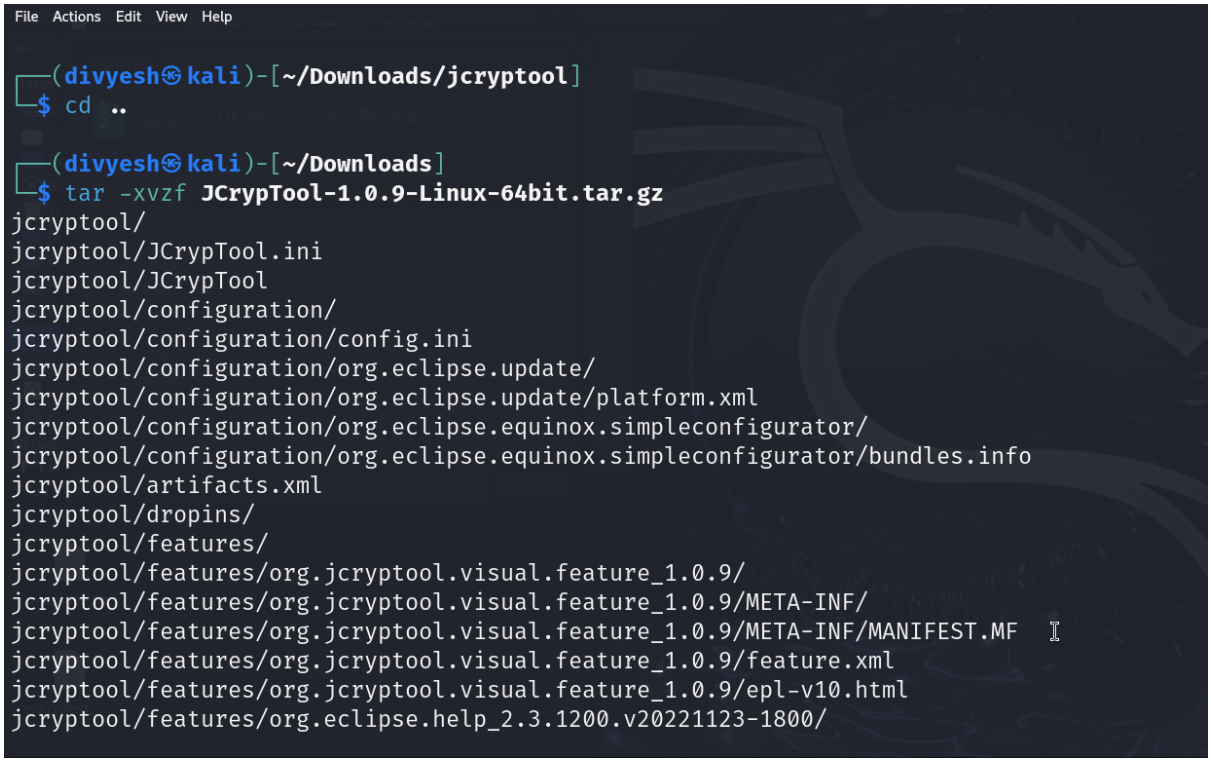
- Symmetric Encryption (AES, DES, etc.)
- Asymmetric Encryption (RSA, ECC, etc.)
- Hashing Algorithms (SHA, MD5, etc.)
- Digital Signatures
- Steganography
- Cryptanalysis Tools
- Visualizations for Learning Cryptography

Installation :

Step 1 : Download tar file of jcrypt (I am doing this in Kali Linux)

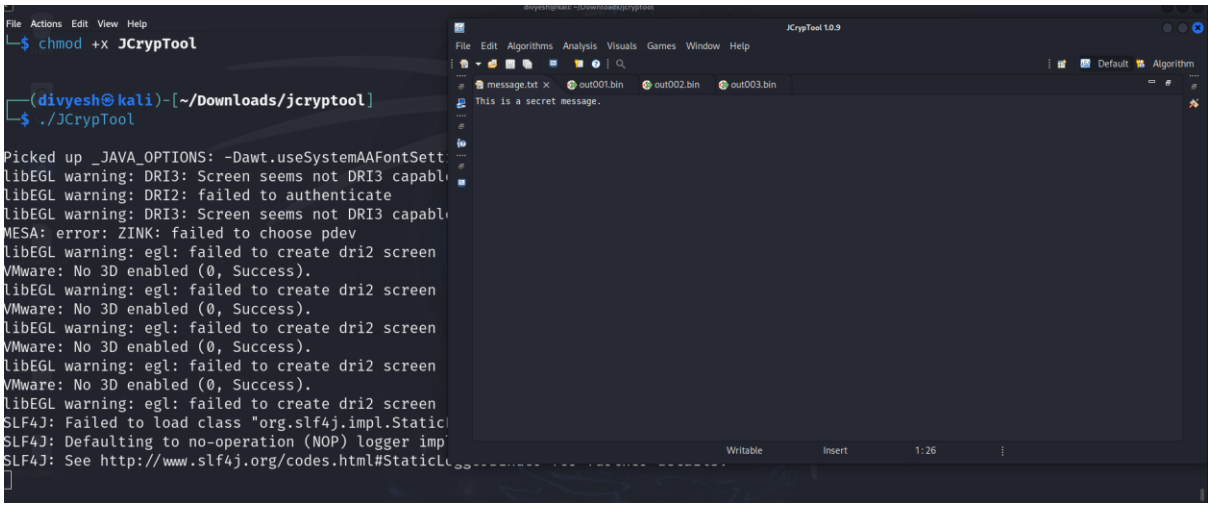


Step 2 : Extract and load jcrypt in the terminal



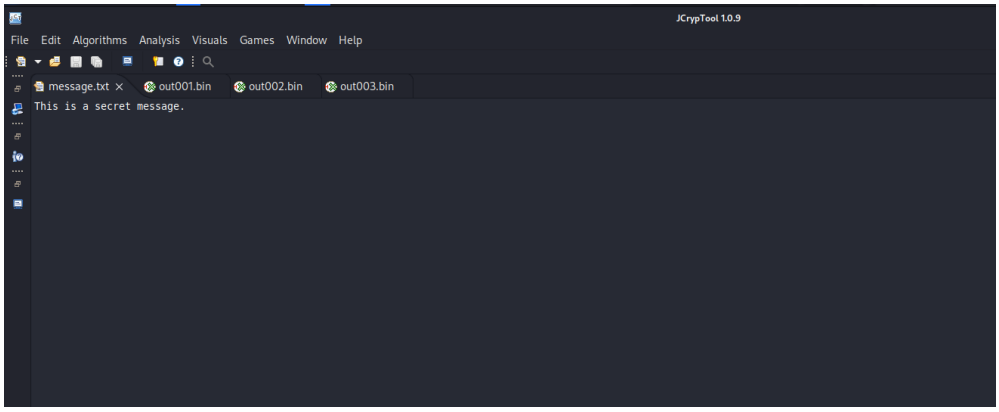
Step 3 : Navigate to jcrypt directory and make the launcher executable

Step 4 : Run JCryptool

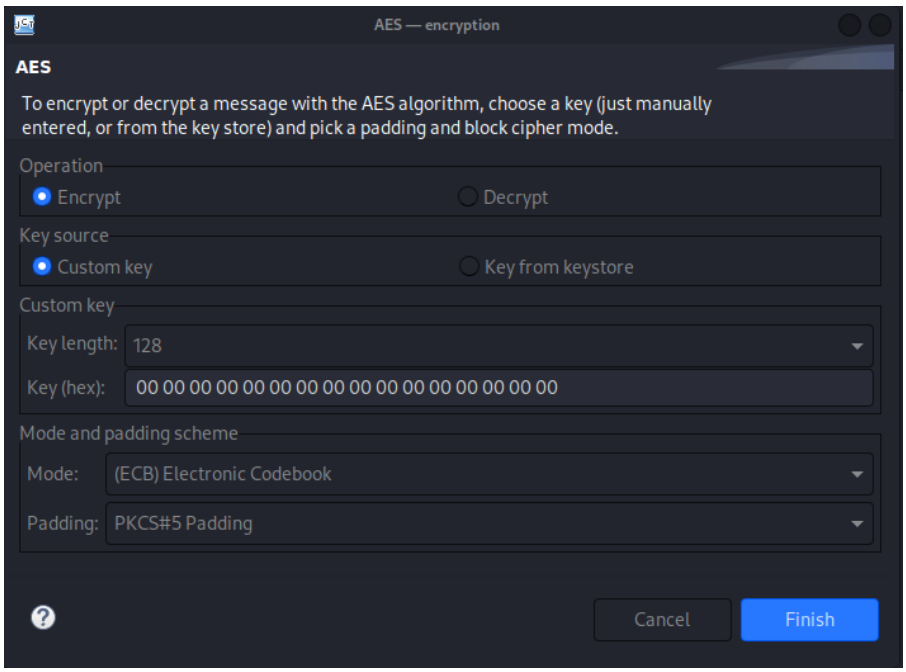


Encryption and decryption of message

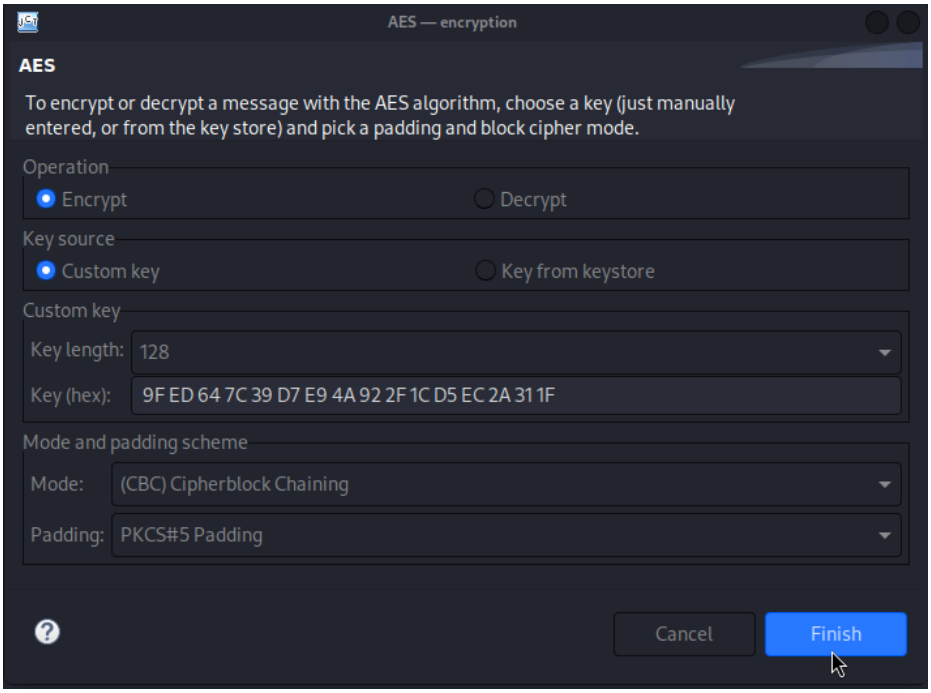
1. **Create a file, say “message.txt”, and write some content and save it.**



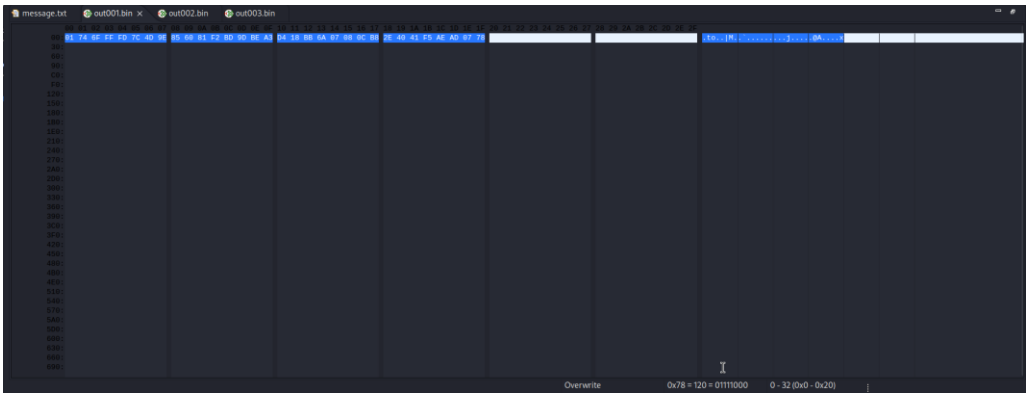
2. **Encrypt it using AES algorithm**



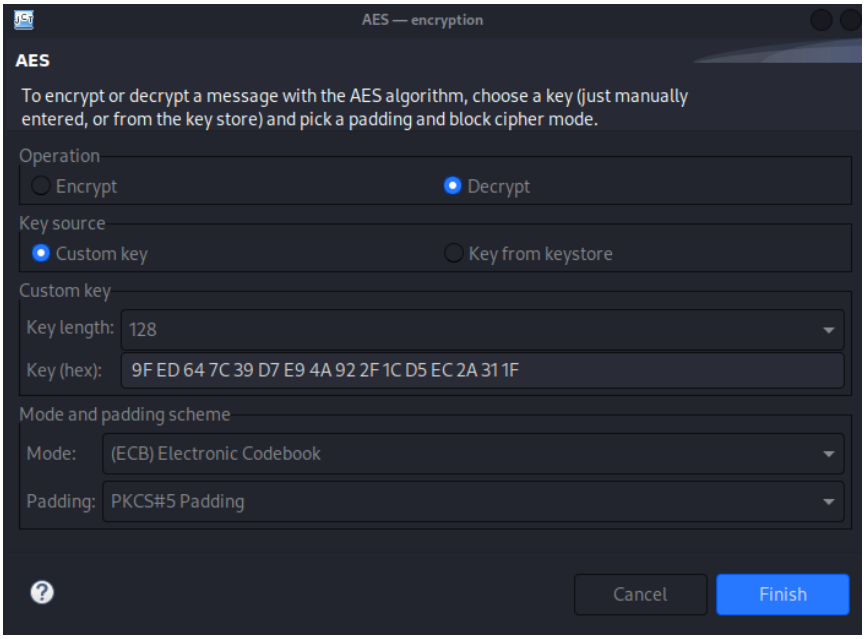
3. **Convert the message key to hexadecimal using any tool and paste it in Key(hex)**



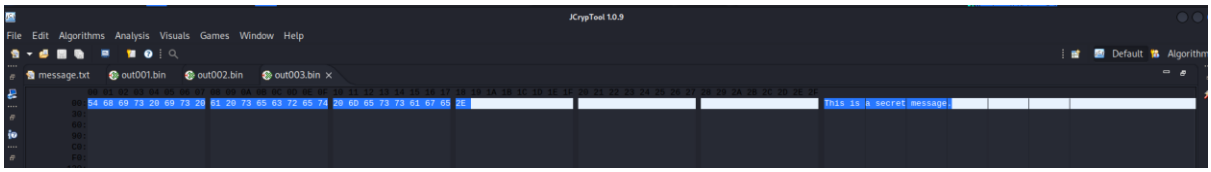
4. **The file is encrypted and saved like this (highlighted) in a .bin file**



5. **Decrypt it the same way using the same key**



6. The message is successfully decrypted.



Penetration Testing and Vulnerability Assessment Lab

Assignment 04

Divyesh Tharakan

24MCI0004

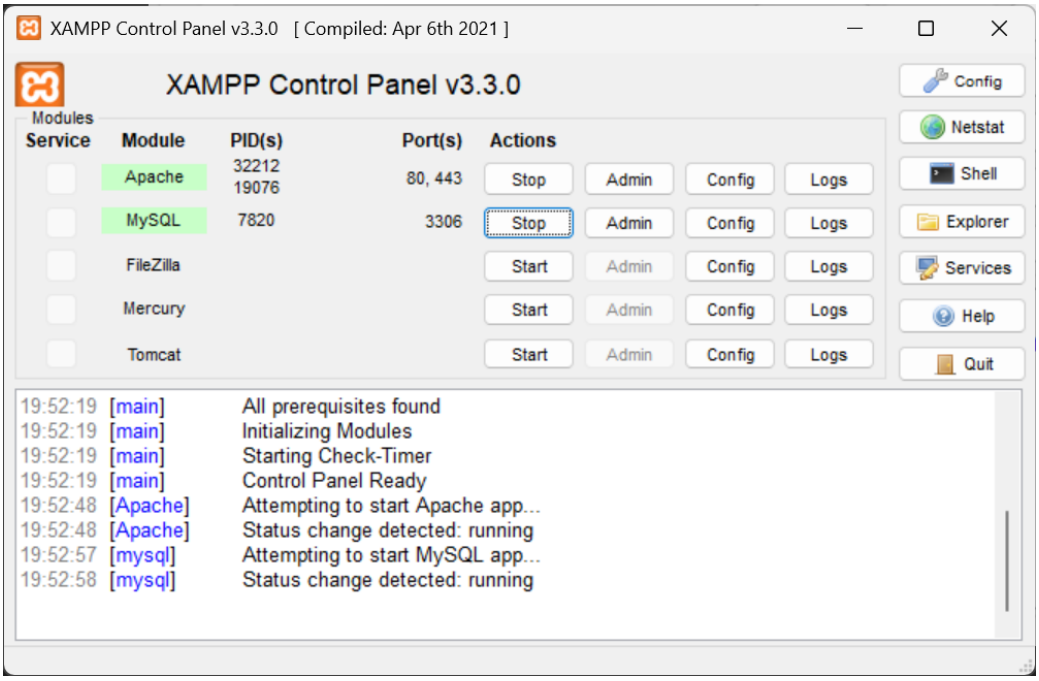
MTech CSE IS

Damn Vulnerable Web App (DVWA) is a deliberately insecure PHP/MySQL web application designed for security testing.

Its primary objectives are to assist security professionals in legally honing their skills and tools, help web developers grasp web application security concepts, and support educators and students in teaching and learning web security in a classroom setting.

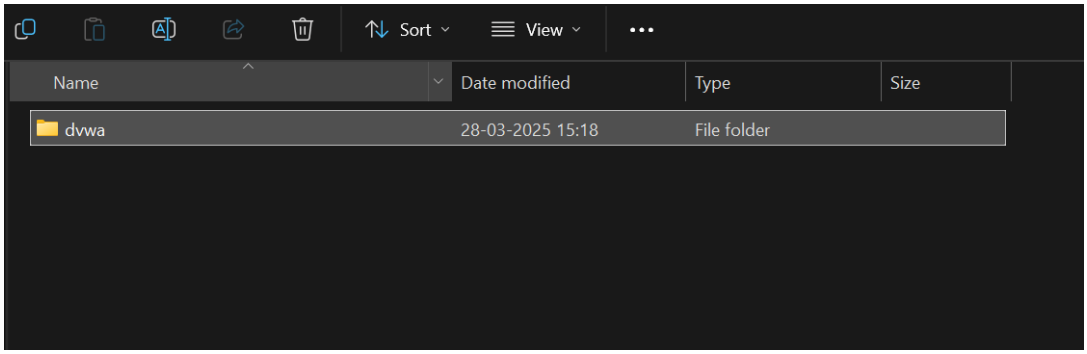
Steps to be performed :

1. Download XAMPP Server and start Apache and MySQL

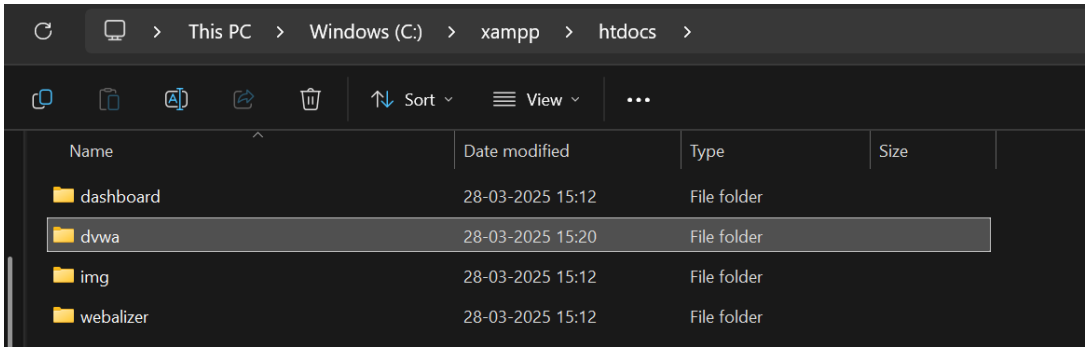


2. Download DVWA module from github, extract it and change the name to dvwa

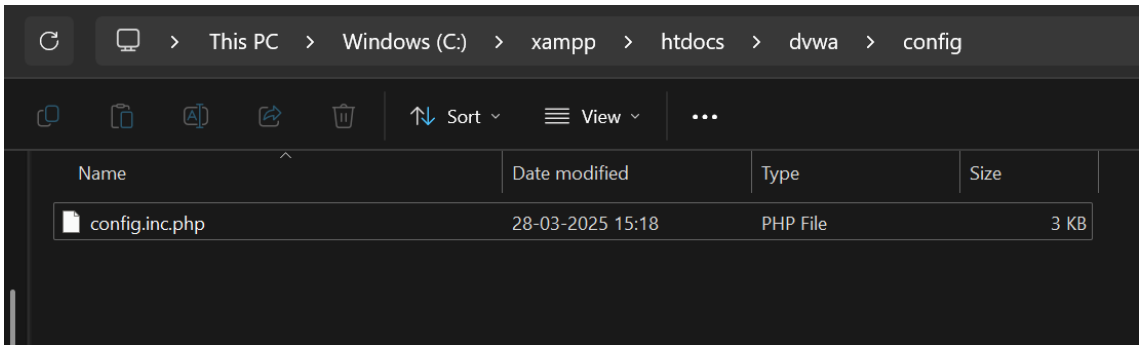
   https://github.com/digininja/DVWA



3. Copy the folder to this path : xampp/htdocs



4. Inside the DVWA folder, a file named **config** is present which will have an extra extension. Remove it and keep it in this format.



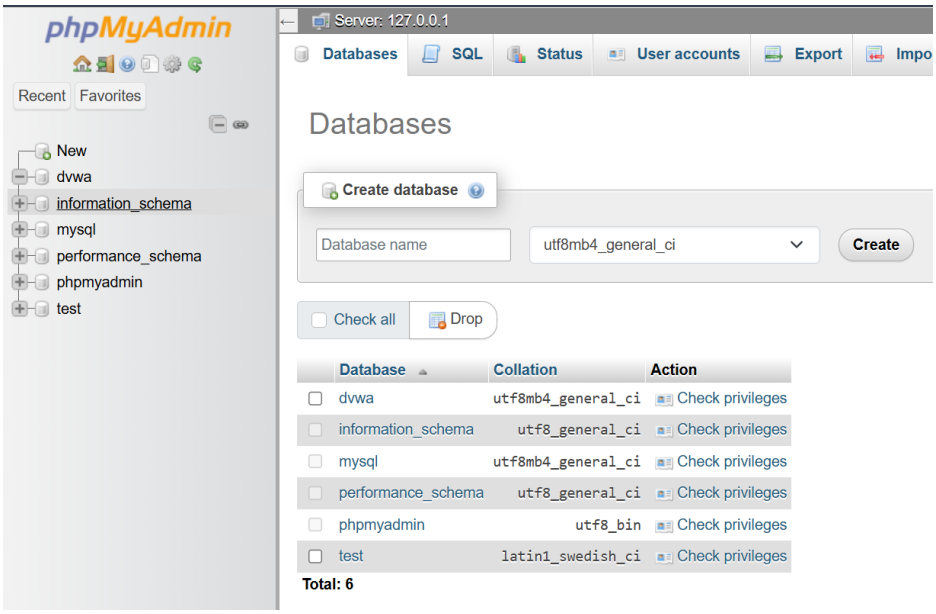
5. The same file will contain the username and password (credentials)

config.inc.php

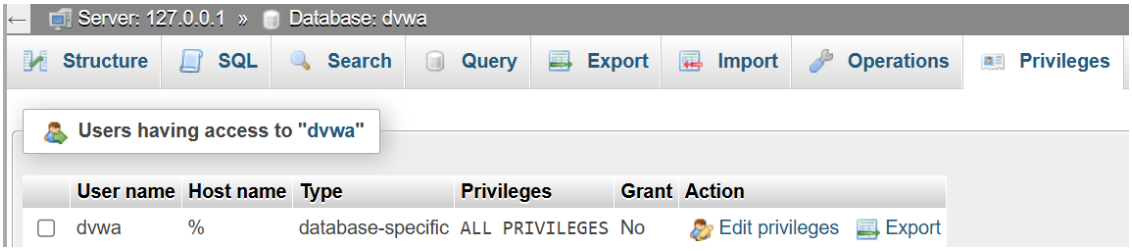
File Edit View

```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below a
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to so
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'dvwa';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'p@ssw0rd';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';
```

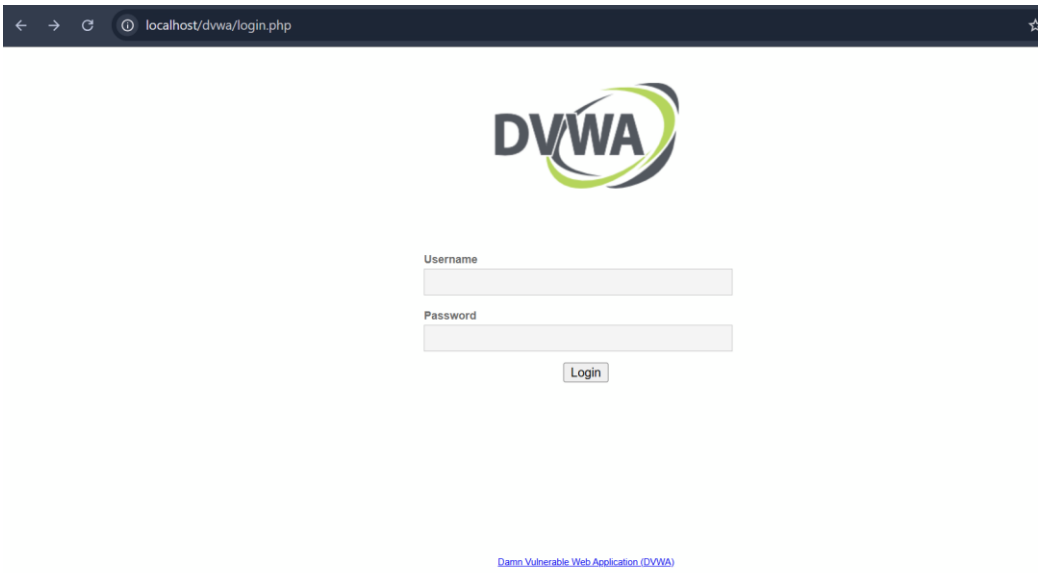
6. Go to XAMPP -> MySQL -> Admin and create a database with the name **dvwa**



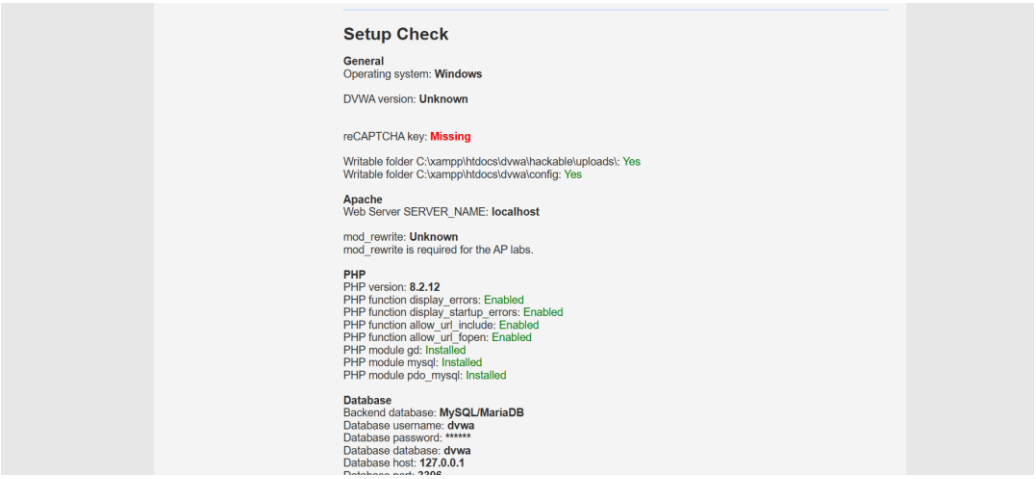
7. Inside the **dvwa** database, go to privileges and add a username, granting all privileges.



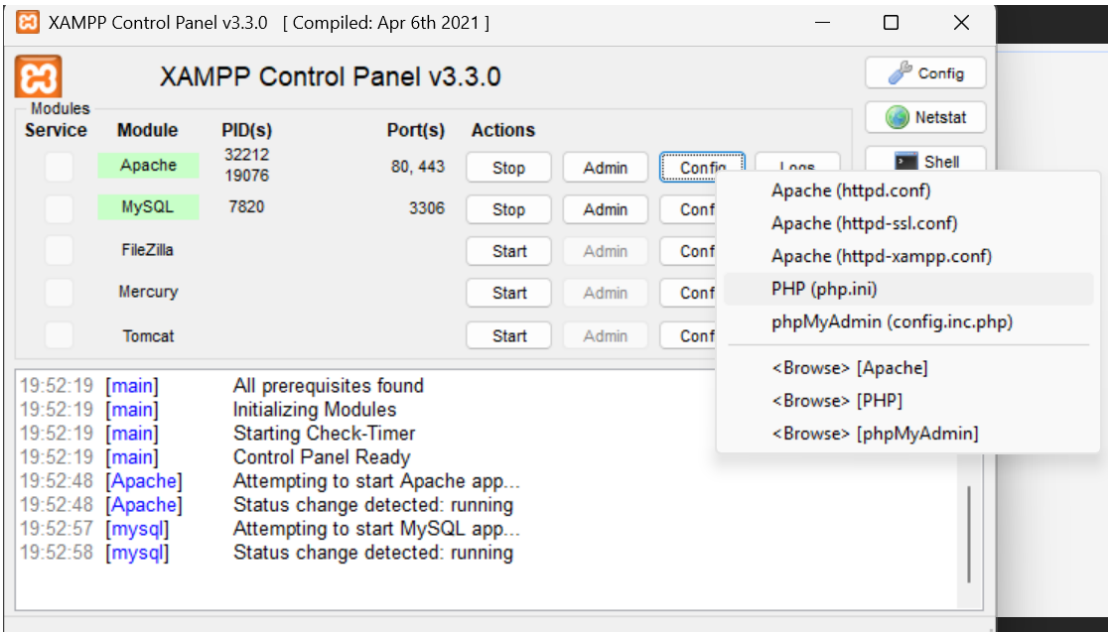
8. Go to localhost/dvwa and the login page will pop up like this. Login directly without username and password



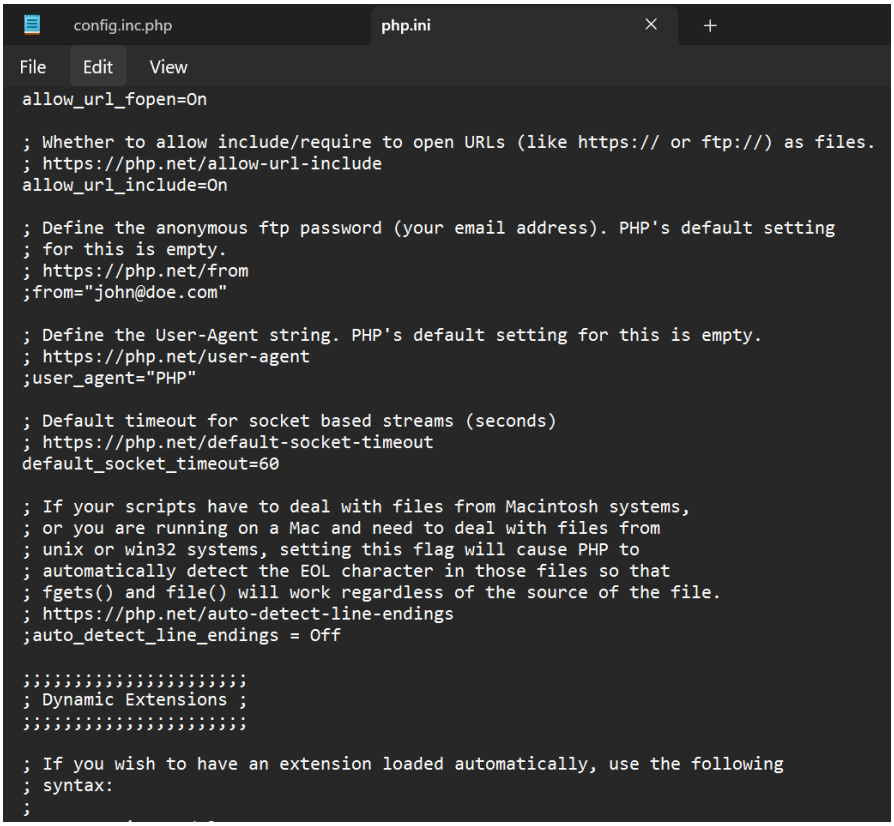
9. Check the setup here. For me, everything is enabled. By default, some modules might be missing and shown in red.



10. To enable it, go to XAMPP -> Apache -> Right click on Config and select php.ini



11. Search for the missing module here and turn it on.



Penetration Testing and Vulnerability Assessment Lab

Assignment 05

Divyesh Tharakan

24MCI0004

MTech CSE IS

JCryptool

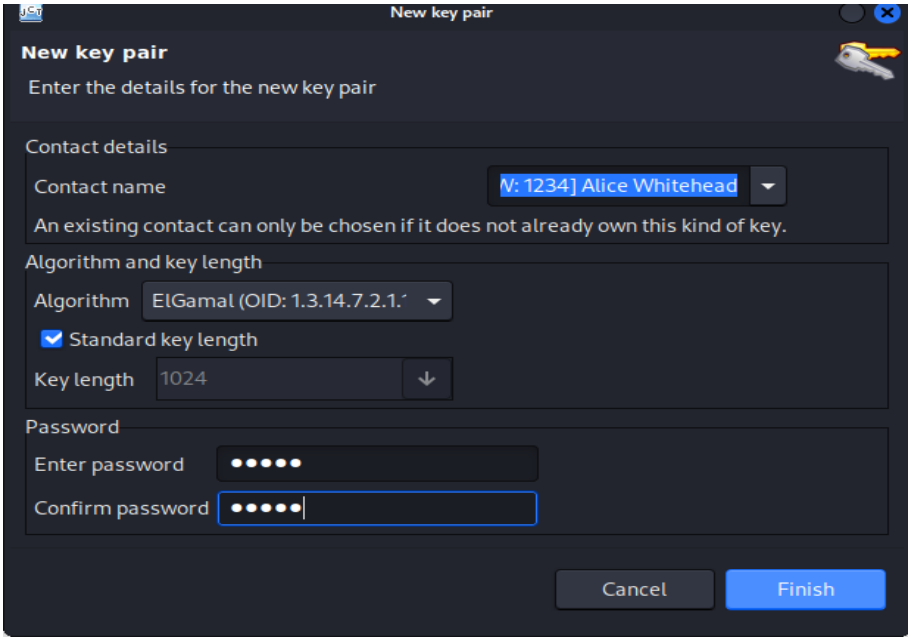
JCrypTool (JCT) is an open-source cryptography e-learning platform based on Java. It helps users experiment with and understand various cryptographic techniques such as encryption, decryption, hashing, and digital signatures.

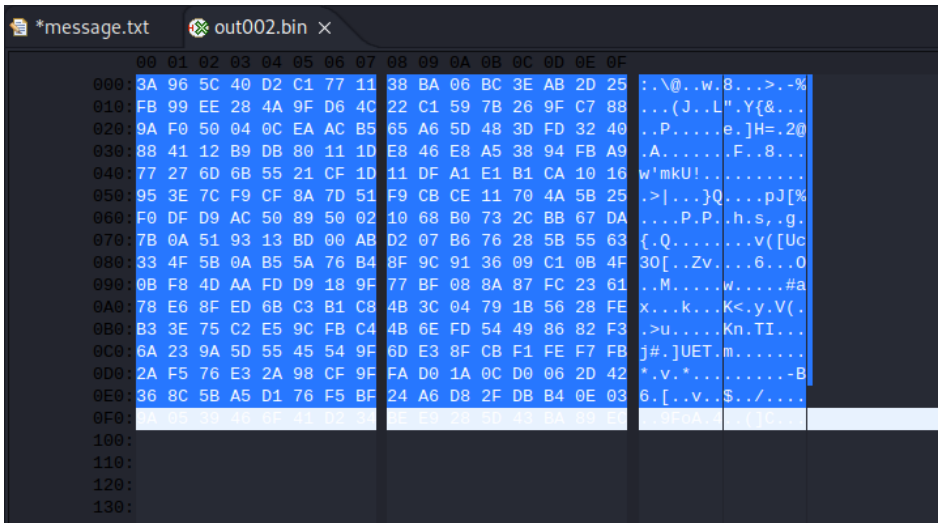
Key Features of JCrypTool:

- Symmetric Encryption (AES, DES, etc.)
- Asymmetric Encryption (RSA, ECC, etc.)
- Hashing Algorithms (SHA, MD5, etc.)
- Digital Signatures
- Steganography
- Cryptanalysis Tools
- Visualizations for Learning Cryptography

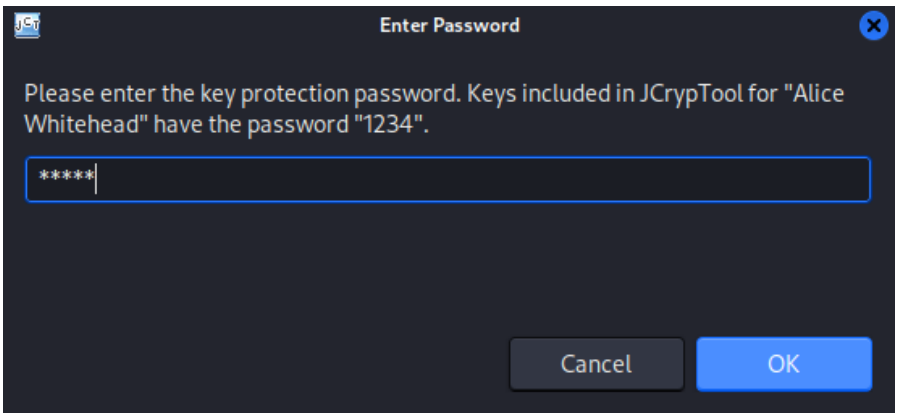
Algorithm 1 : ElGammal

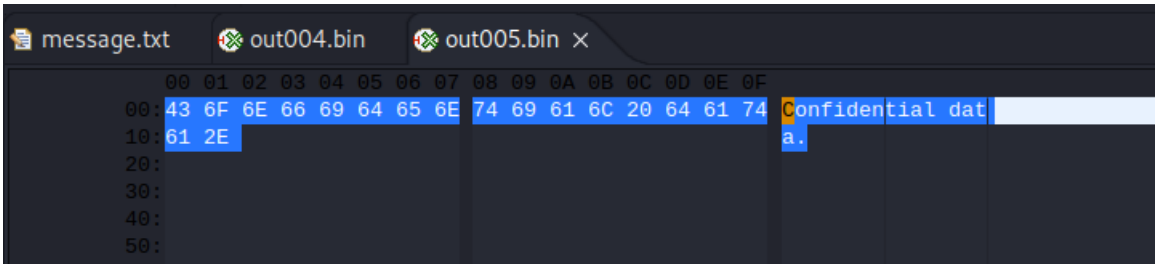
- Encryption


New key pair
New key pair
Enter the details for the new key pair
Contact details
Contact name
N: 1234] Alice Whitehead
An existing contact can only be chosen if it does not already own this kind of key.
Algorithm and key length
Algorithm
ElGamal (OID: 1.3.14.7.2.1.
Standard key length
Key length
1024
Password
Enter password
Confirm password
Cancel
Finish

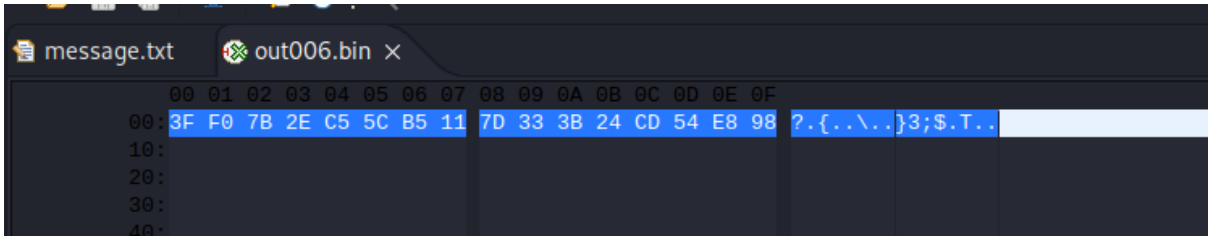

*message.txt
out002.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000: 3A 96 5C 40 D2 C1 77 11 38 BA 06 BC 3E AB 2D 25 :.\@..w.8...>.-%
010: FB 99 EE 28 4A 9F D6 4C 22 C1 59 7B 26 9F C7 88 ...(J..L".Y{&...
020: 9A F0 50 04 0C EA AC B5 65 A6 5D 48 3D FD 32 40 ..P.....e.]H=.2@
030: 88 41 12 B9 DB 80 11 1D E8 46 E8 A5 38 94 FB A9 .A.......F..8...
040: 77 27 6D 6B 55 21 CF 1D 11 DF A1 E1 B1 CA 10 16 w'mkU!..........
050: 95 3E 7C F9 CF 8A 7D 51 F9 CB CE 11 70 4A 5B 25 .>|...}Q....pJ[%
060: F0 DF D9 AC 50 89 50 02 10 68 B0 73 2C BB 67 DA ....P.P..h.s,.g.
070: 7B 0A 51 93 13 BD 00 AB D2 07 B6 76 28 5B 55 63 {.Q.......v([Uc
080: 33 4F 5B 0A B5 5A 76 B4 8F 9C 91 36 09 C1 0B 4F 3O[..Zv....6...O
090: 0B F8 4D AA FD D9 18 9F 77 BF 08 8A 87 FC 23 61 ..M.....w.....#a
0A0: 78 E6 8F ED 6B C3 B1 C8 4B 3C 04 79 1B 56 28 FE x...k...K<.y.V(.
0B0: B3 3E 75 C2 E5 9C FB C4 4B 6E FD 54 49 86 82 F3 .>u.....Kn.TI...
0C0: 6A 23 9A 5D 55 45 54 9F 6D E3 8F CB F1 FE F7 FB j#.]UET.m.......
0D0: 2A F5 76 E3 2A 98 CF 9F FA D0 1A 0C D0 06 2D 42 *.v.*.........-B
0E0: 36 8C 5B A5 D1 76 F5 BF 24 A6 D8 2F DB B4 0E 03 6.[..v..$../....
0F0: 9A 05 39 46 6F 41 D2 3F BE E9 28 5D 43 BA 89 E5 ..9FoA.?..(]C...
100:
110:
120:
130:

- Decryption


Enter Password
Please enter the key protection password. Keys included in JCrypTool for "Alice Whitehead" have the password "1234".
*****
Cancel
OK

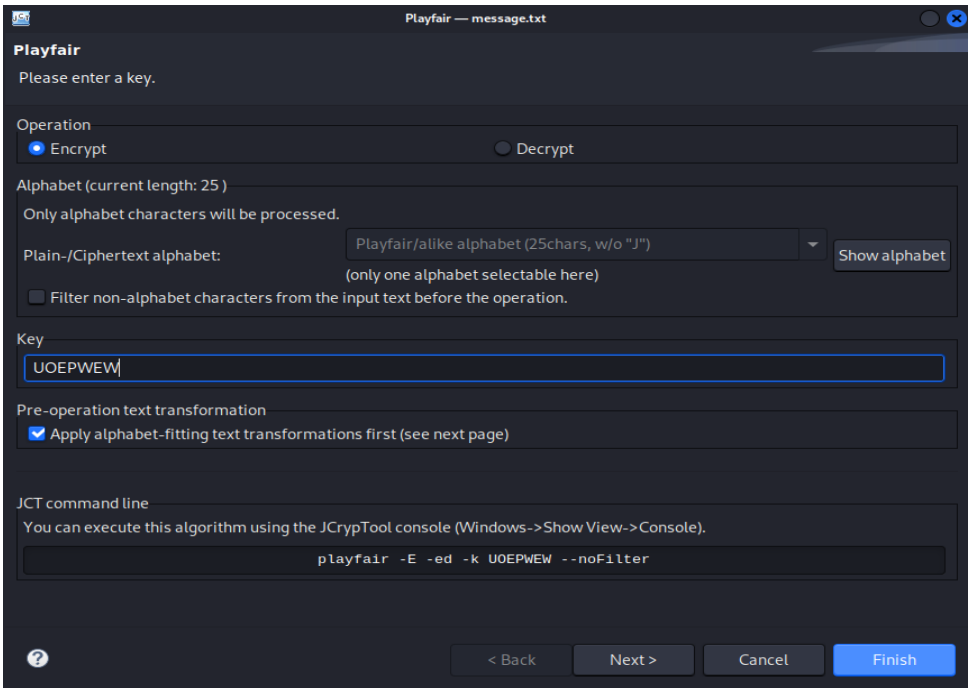


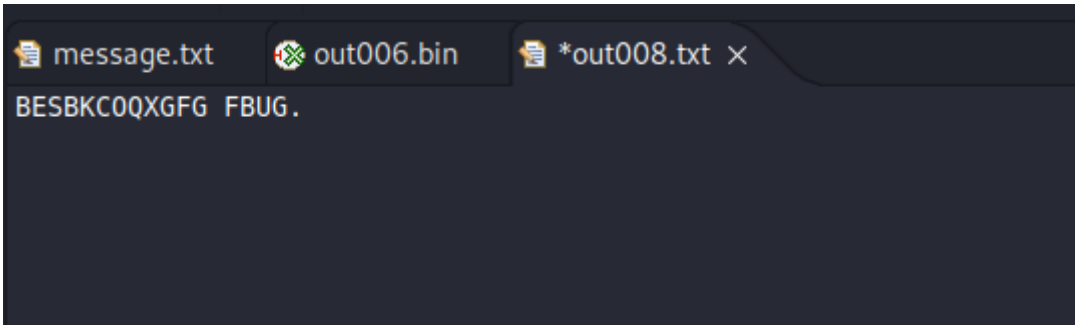
Algorithm 2 : Md5



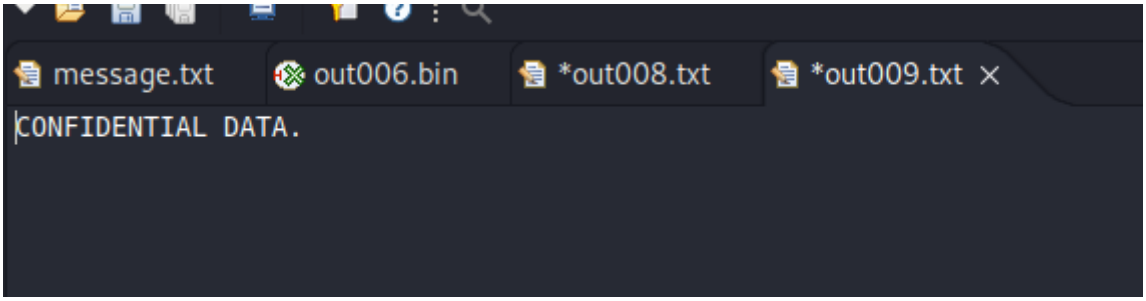
Algorithm 3 : Playfair

- Encryption

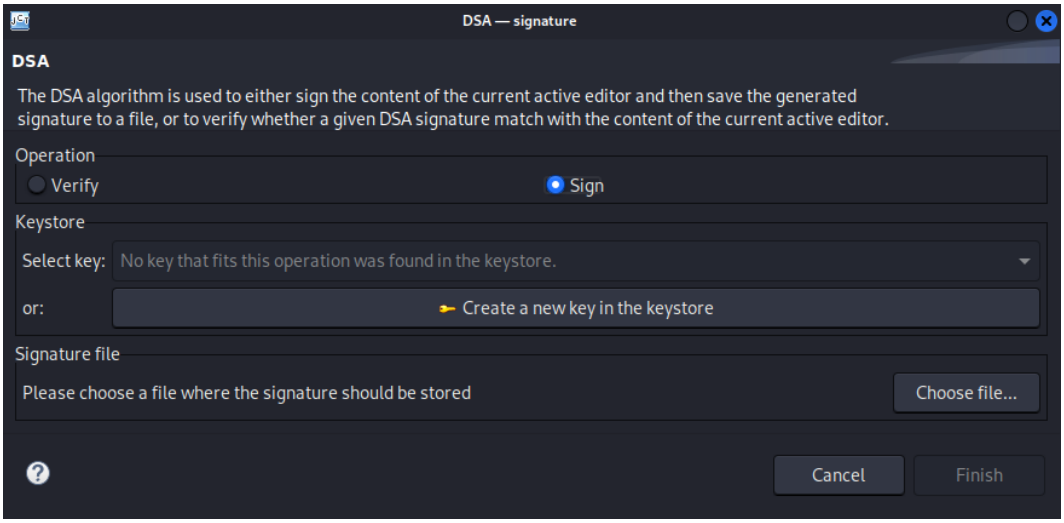


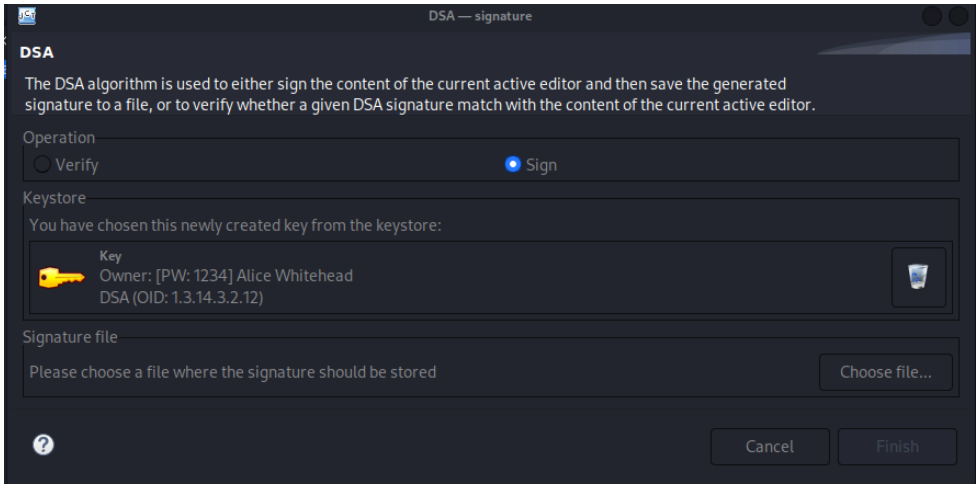


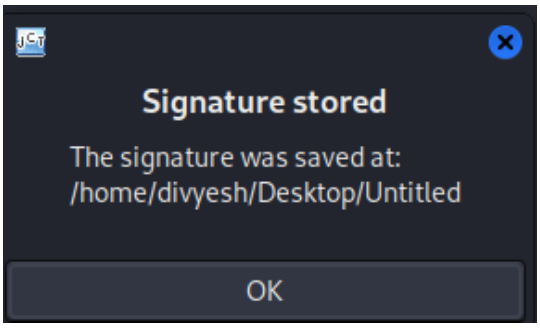
- Decryption

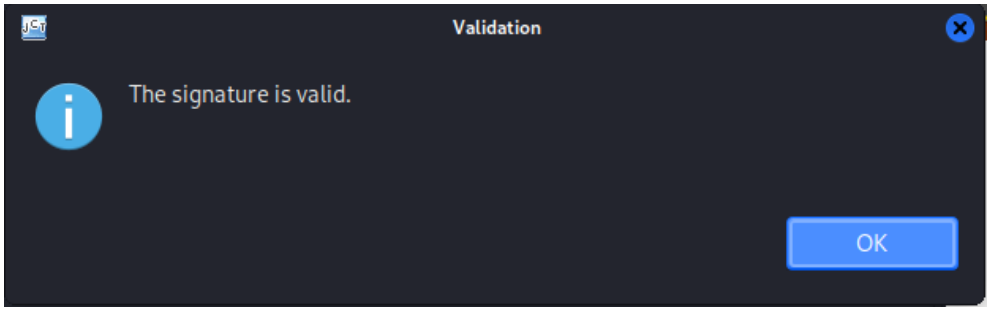


Algorithm 4 : DSA



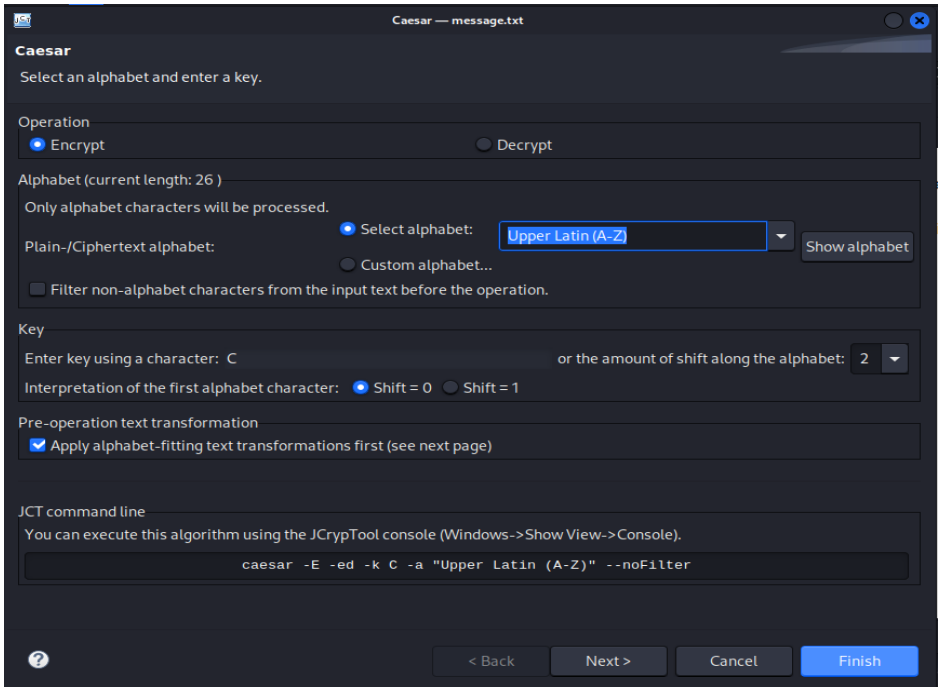


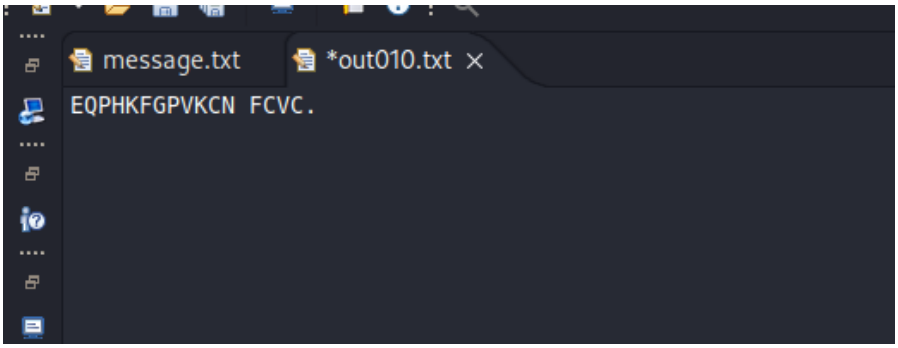




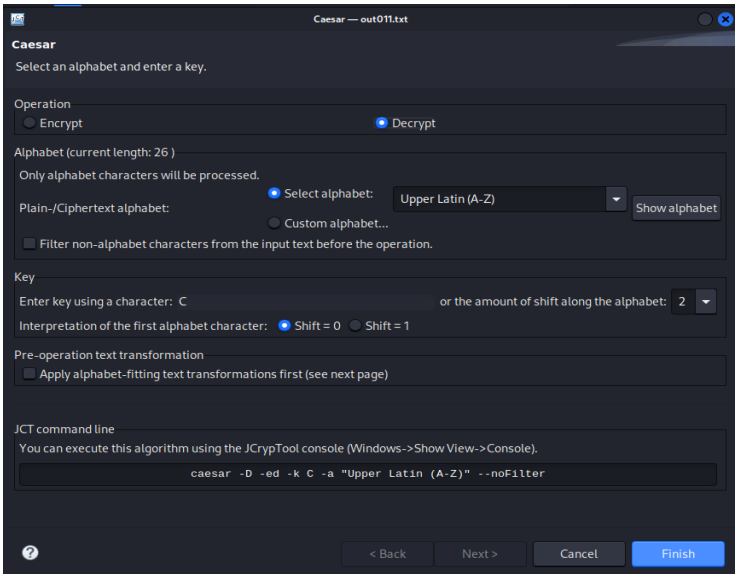
Algorithm 5 : Caesar

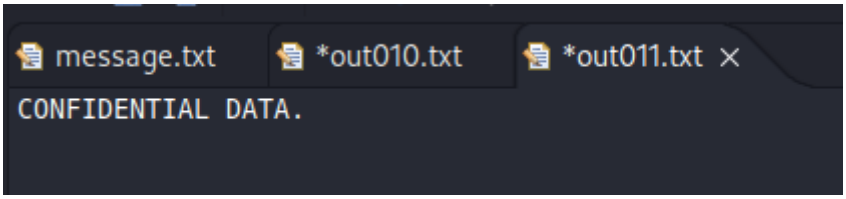
- Encryption


Caesar — message.txt
Caesar
Select an alphabet and enter a key.
Operation
Encrypt
Decrypt
Alphabet (current length: 26)
Only alphabet characters will be processed.
Plain-/Ciphertext alphabet:
Select alphabet:
Upper Latin (A-Z)
Show alphabet
Custom alphabet...
Filter non-alphabet characters from the input text before the operation.
Key
Enter key using a character: C
or the amount of shift along the alphabet: 2
Interpretation of the first alphabet character:
Shift = 0
Shift = 1
Pre-operation text transformation
Apply alphabet-fitting text transformations first (see next page)
JCT command line
You can execute this algorithm using the JCrypTool console (Windows->Show View->Console).
caesar -E -ed -k C -a "Upper Latin (A-Z)" --noFilter
< Back
Next >
Cancel
Finish


message.txt
*out010.txt
EQPHKFGPVKCN FCVC.

- Decryption


Caesar — out011.txt
Caesar
Select an alphabet and enter a key.
Operation
Encrypt
Decrypt
Alphabet (current length: 26)
Only alphabet characters will be processed.
Plain-/Ciphertext alphabet:
Select alphabet:
Upper Latin (A-Z)
Show alphabet
Custom alphabet...
Filter non-alphabet characters from the input text before the operation.
Key
Enter key using a character: C
or the amount of shift along the alphabet: 2
Interpretation of the first alphabet character:
Shift = 0
Shift = 1
Pre-operation text transformation
Apply alphabet-fitting text transformations first (see next page)
JCT command line
You can execute this algorithm using the JCrypTool console (Windows->Show View->Console).
caesar -D -ed -k C -a "Upper Latin (A-Z)" --noFilter
< Back
Next >
Cancel
Finish


message.txt
*out010.txt
*out011.txt
CONFIDENTIAL DATA.

Penetration Testing and Vulnerability Assessment Lab

Assignment 06

Divyesh Tharakan

24MCI0004

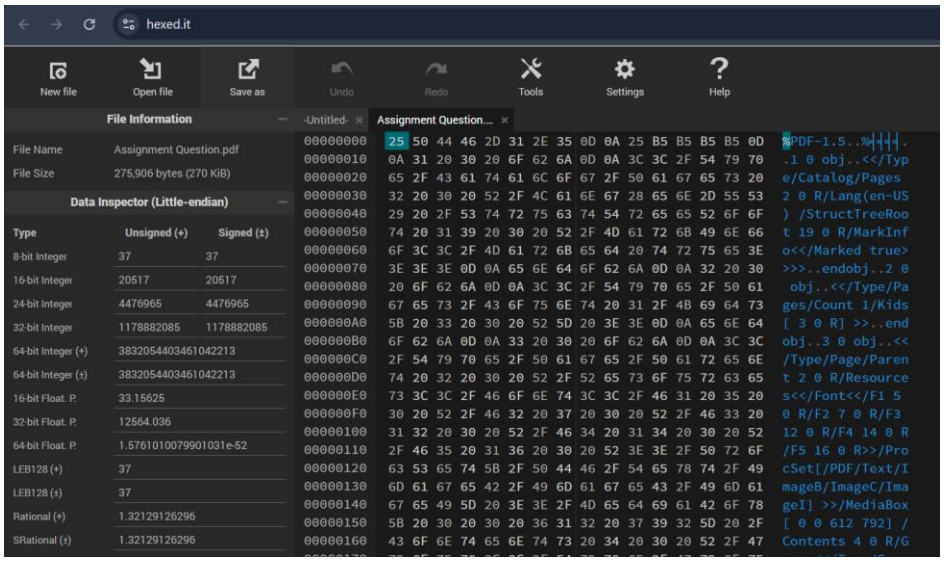
MTech CSE IS

HexEd.it is a free hex editor for Windows, MacOS, Linux and all other modern operating systems. It uses HTML5 and JavaScript (JS) technology to enable online hexediting, directly in your browser.

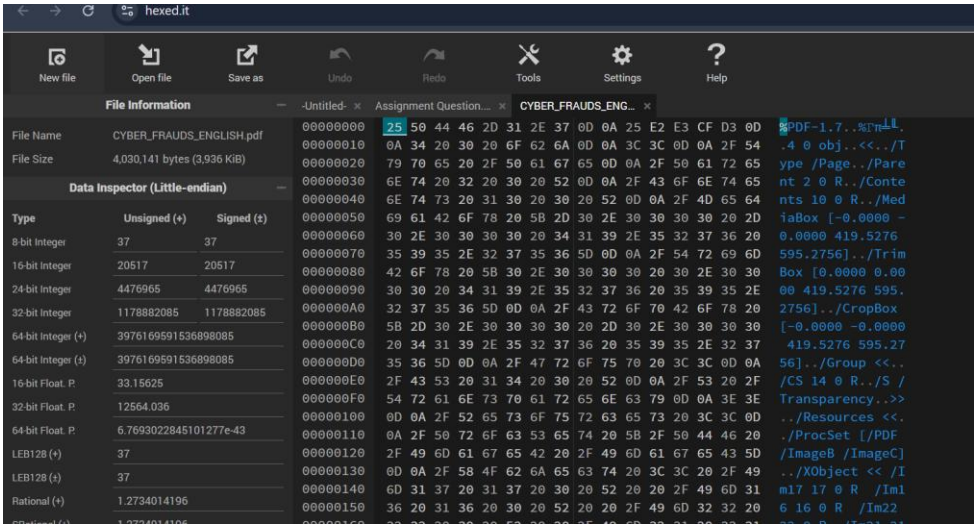
For the same extension of two different files, the starting hex signature will be same.

Also, 2 or 3 extensions might have the same hex signature at the start (4 bytes)

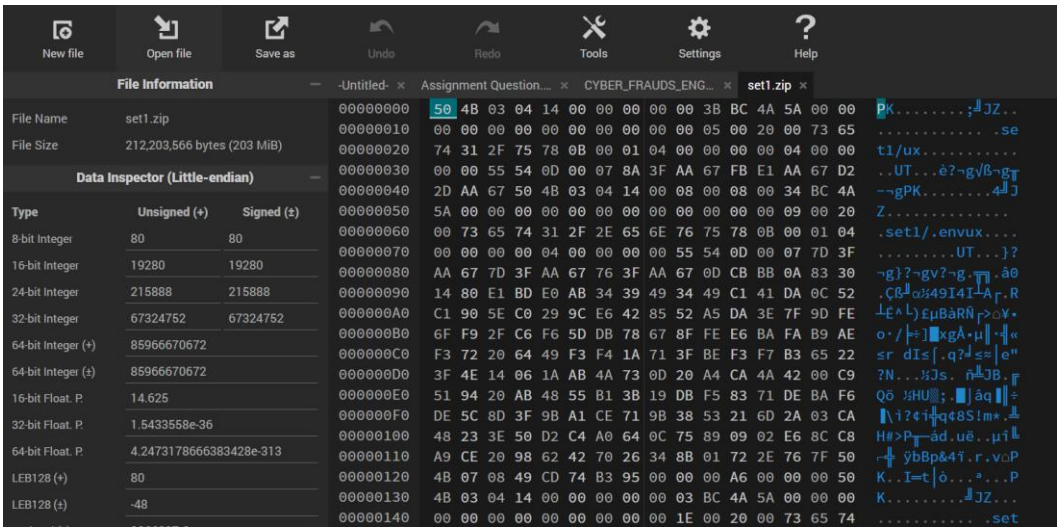
1. .pdf files



This is the hex signature generated for the above PDF and the starting four bytes : **25 50 44 46** will be same for all PDFs.

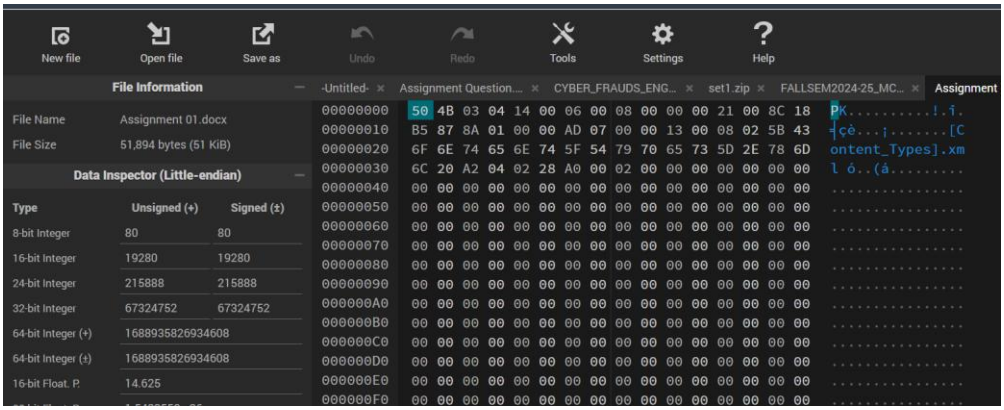


2. .zip file

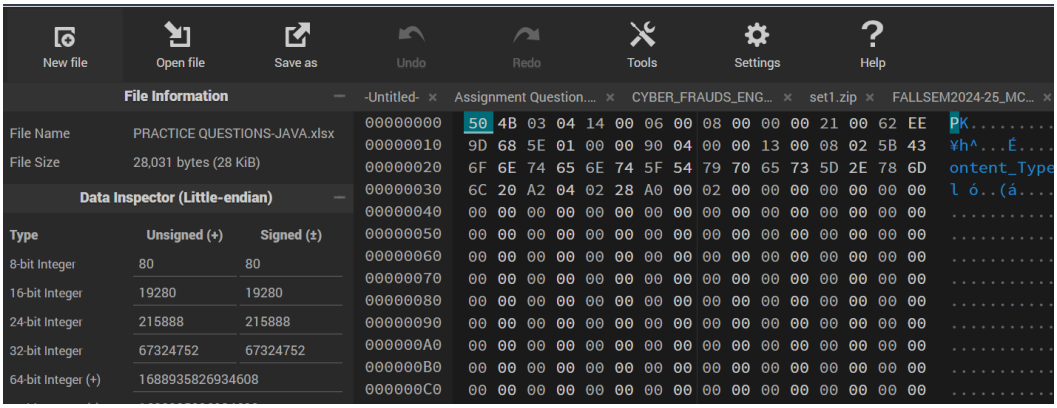


3. .docx file and .xlsx file will have the same four bytes at the start : **50 4B 03 04 14 00 06 00**

.docx file



.xlsx file



4. .jpg file