Deccan Education Society's

Navinchandra Mehta Institute of Technology and Development

CERTIFICATE

This is to certify that Ms **. Anushree Yevle** of M.C.A. Semester III with Roll No. **C22138** has completed **All** practical's of MCALE334 **Ethical Hacking** under my supervision in this college during the year 2022-2024.

CO	R1 (Attendance)	R2 (Performance during lab session)	R3 (Innovation in problem solving technique)	R4 (Mock Viva)	R5 (Variation in implementation of learnt topics on projects)
CO1					
CO2					
CO3					
CO4					

Practical-in-charge

(NMITD)

Head of Department

MCA

Practical.No	Practical Topics	Date	Signature
1	**Footprinting and Reconnaissance**: Using the software tools/commands to perform the following , generate an analysis report : A. To perform footprinting using Google Hacking . B. To find out the information about the a website C. To find the information about an archived website. D. To trace any received email and generate a report. E. To fetch DNS information.		
2	**Scanning networks, Enumeration and sniffing**: Using the software tools/commands to perform the following , generate an analysis report : A. Port scanning . B. Network scanning tools C. IDS tool D. Sniffing tool		
3	**Malware Threats : Worms, viruses, Trojans:** Using the software tools/commands to perform the following , generate an analysis report : A. Password cracking. B. Dictionary attack. C. Encrypt and decrypt passwords. D. DoS attack. E. ARP poisoning in windows. F. Ifconfig,ping,netstat, traceroute. G. Steganography tools.		
4	**Developing and implementing malwares** : A. Creating a simple keylogger in python. B. Creating a virus. C. Creating a trojan.		
5	**Hacking web servers, web applications**: A. Hack a website by Remote File Inclusion B. Disguise as Google Bot to view Hidden Content of a Website C. How to use Kaspersky for Lifetime without Patch.		
6	**SQL injection and Session hijacking** : A. SQL injection for website hacking, B. Session hijacking.		
7	**Wireless network hacking, cloud computing security, cryptography** 1 .Using Cryptool to encrypt and decrypt password, 2. Implement encryption and decryption using Ceaser Cipher.		
8	**Pen testing :** Penetration Testing using Metasploit and metasploitable, **Cyberlaw** : Cyberlaw section under IT act 2000 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74 , Penalty and preventive measures to be taken for the crime associated with each case if any and real life cybercrime cases under each section.		

Practical.No 1 : Footprinting and Reconnaissance:

Aim : Using the software tools/commands to perform the following , generate an analysis report :
A) To perform footprinting using Google Hacking .

Description :

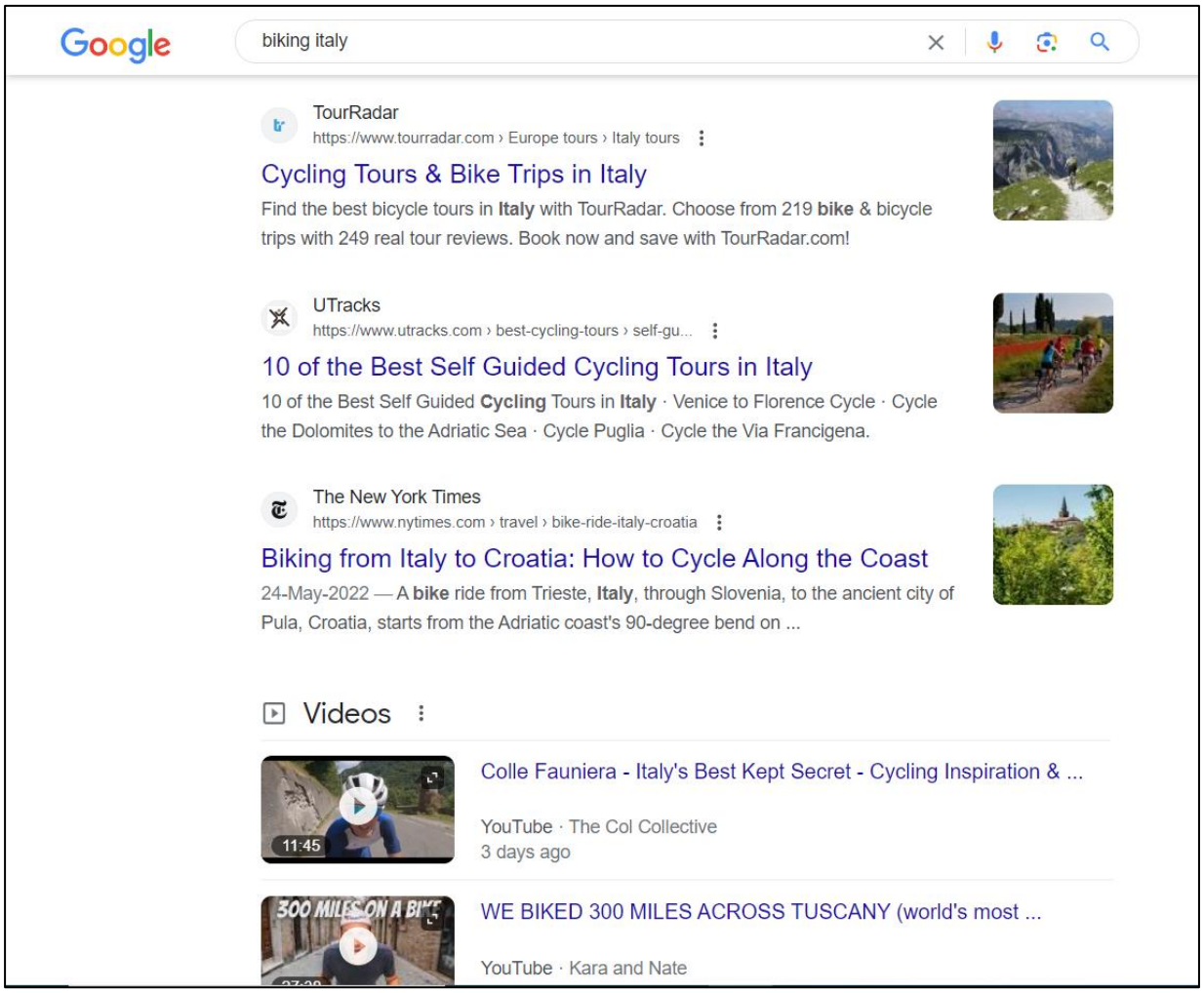
Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.
The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.
There are two types of footprinting in ethical hacking:
1. active footprinting
2. passive footprinting

Output:

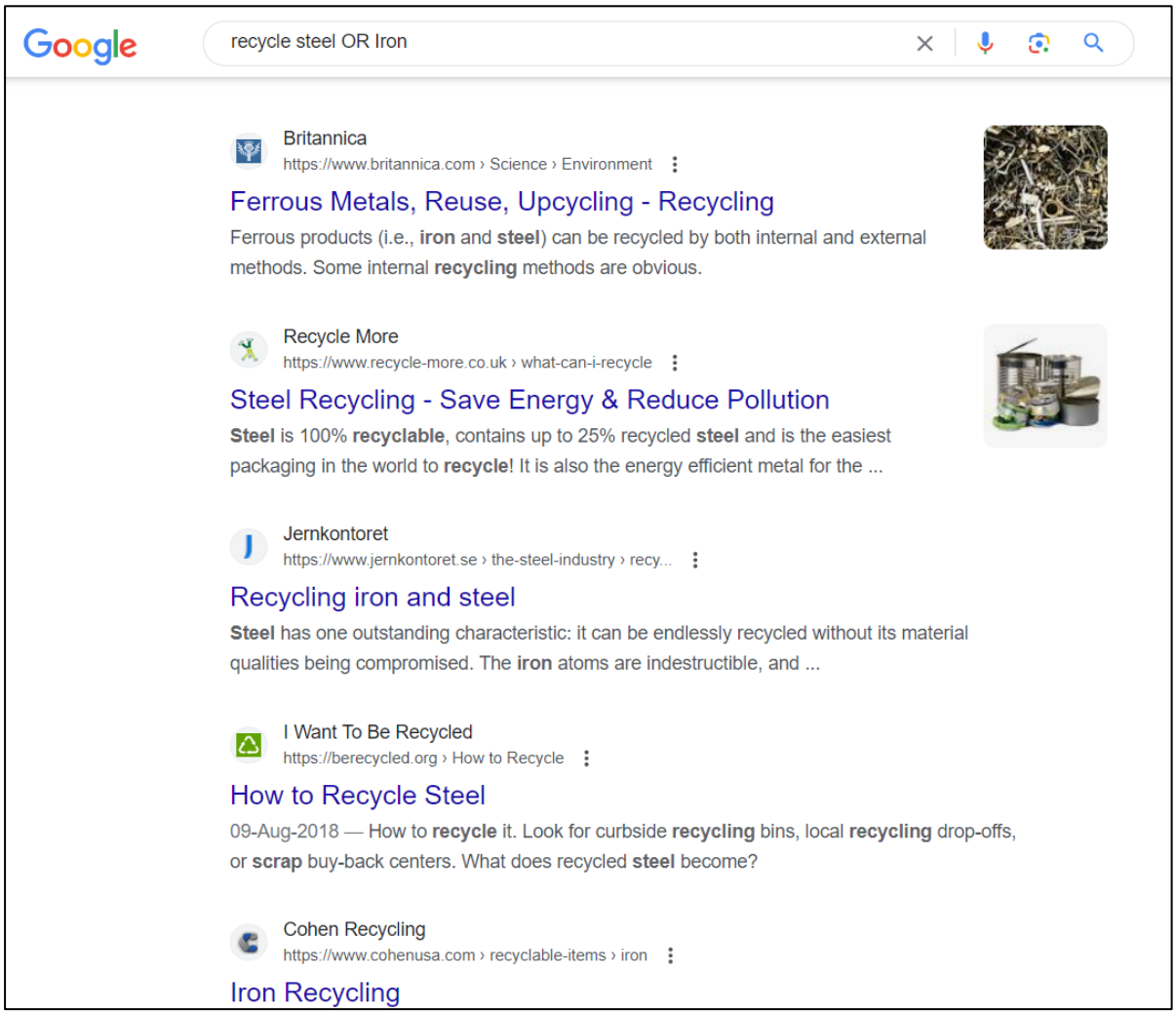
1. To perform footprinting using Google Hacking .

No.	Basic Examples	Finds Pages Containing
1	biking Italy	The words biking and Italy
2	recycle steel OR Iron	Information on recycling steel or recycling iron
3	“I have a dream”	The extract phase I have a dream
4	Salsa -dance	The word salsa but not the word dance
5	Louis “I” France	Information about the Louis the First(I), weeding out the kings of France
6	castle ~glossary	Glosarries about caatles, as well as dictionary,list of terms,terminology etc
7	Fortune-telling	All forms of terms wether spelled as a single word, a phrase or hyphenated
8	Define: imbrogllo	Definations of the word Imbrogllo from the web

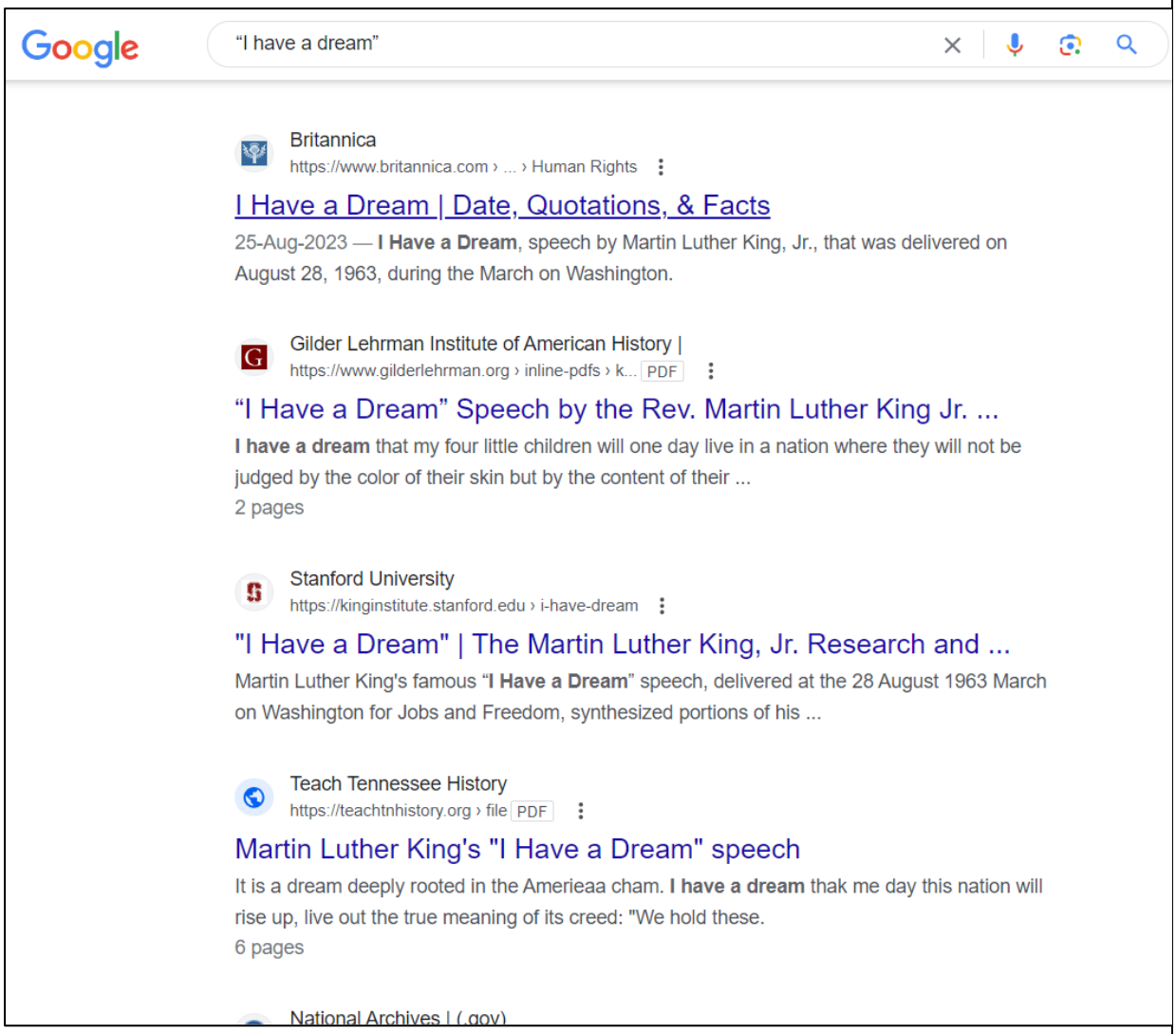
1. biking Italy



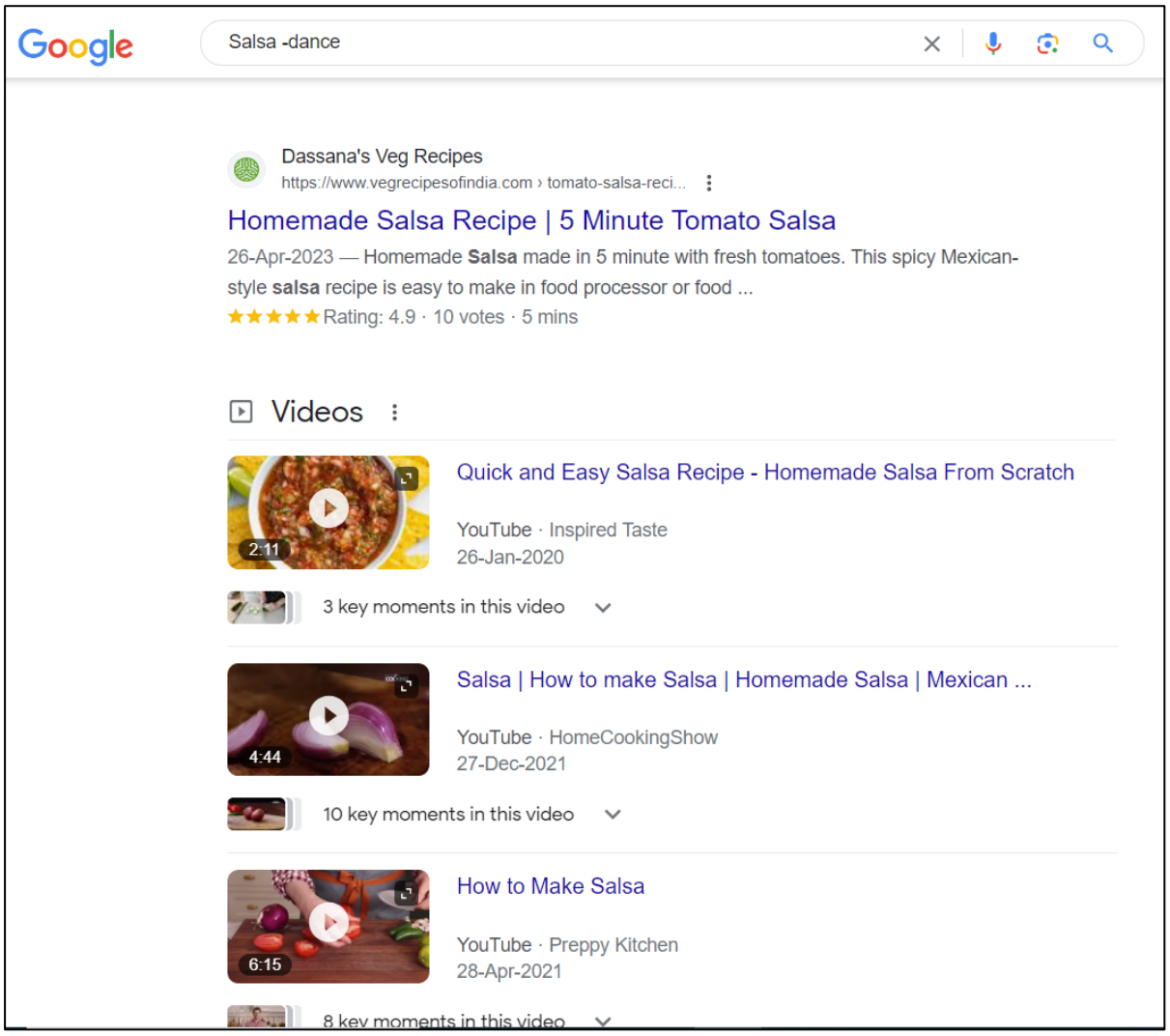
2. recycle steel OR Iron



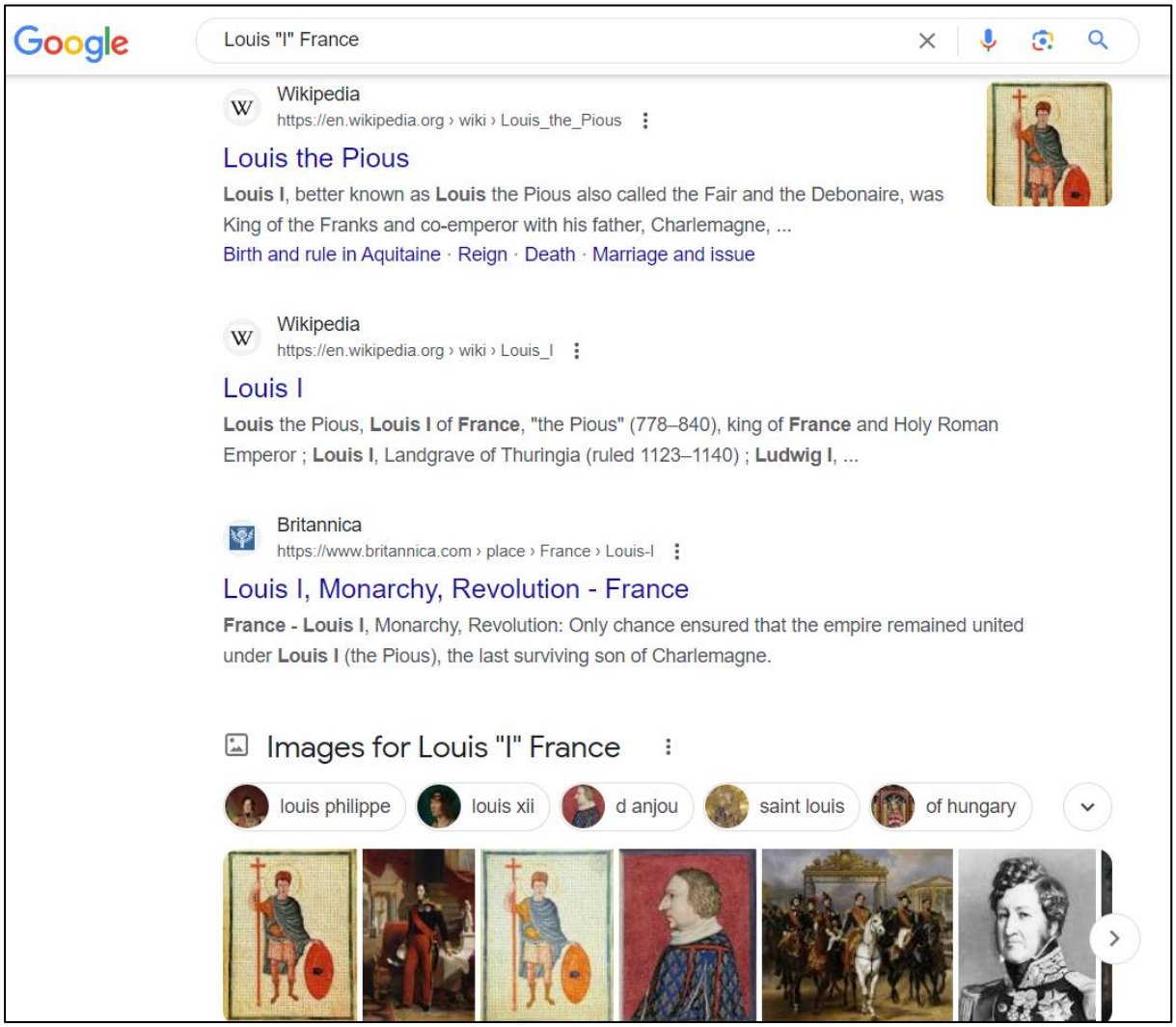
3. “I have a dream”



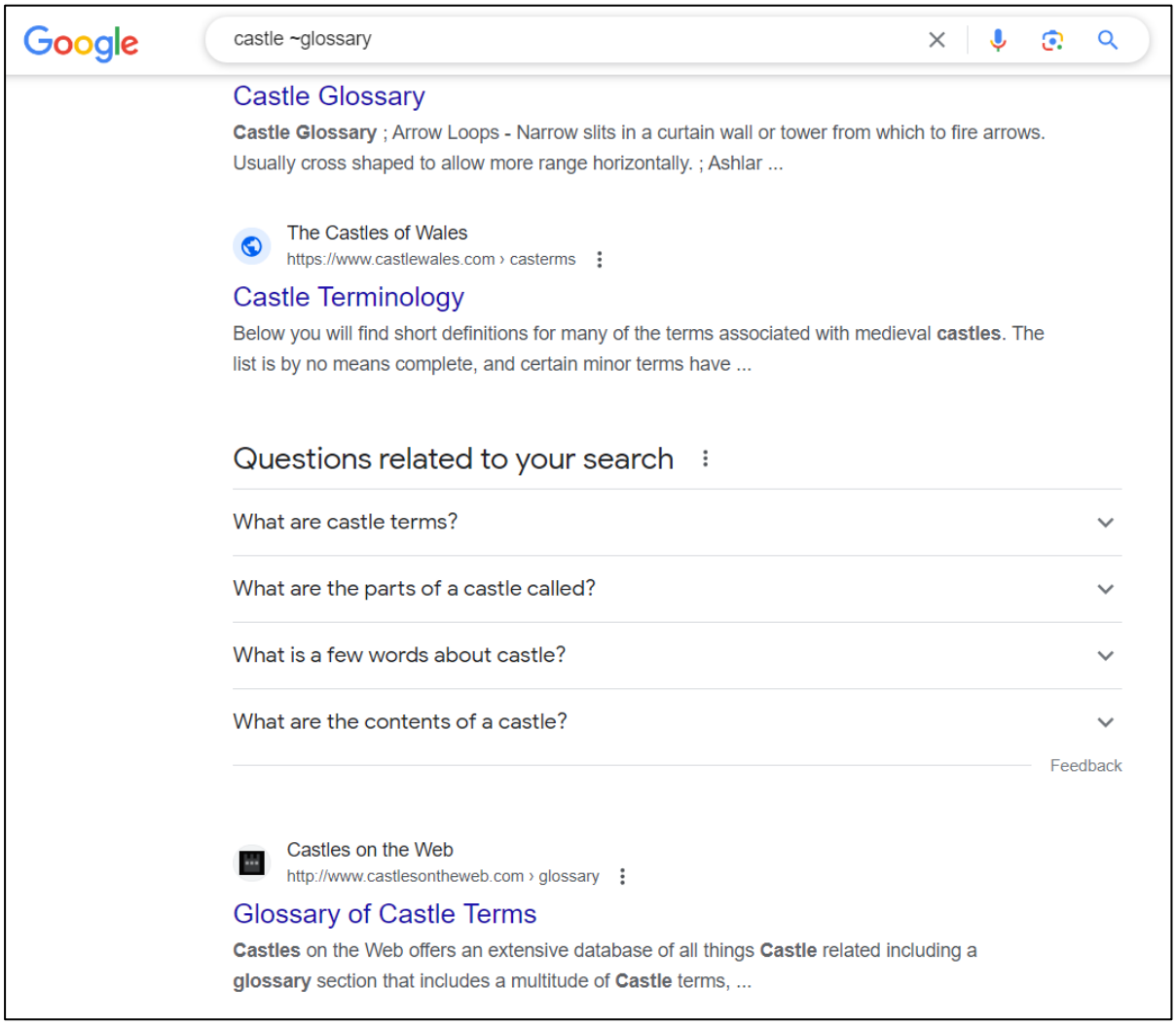
4. Salsa -dance



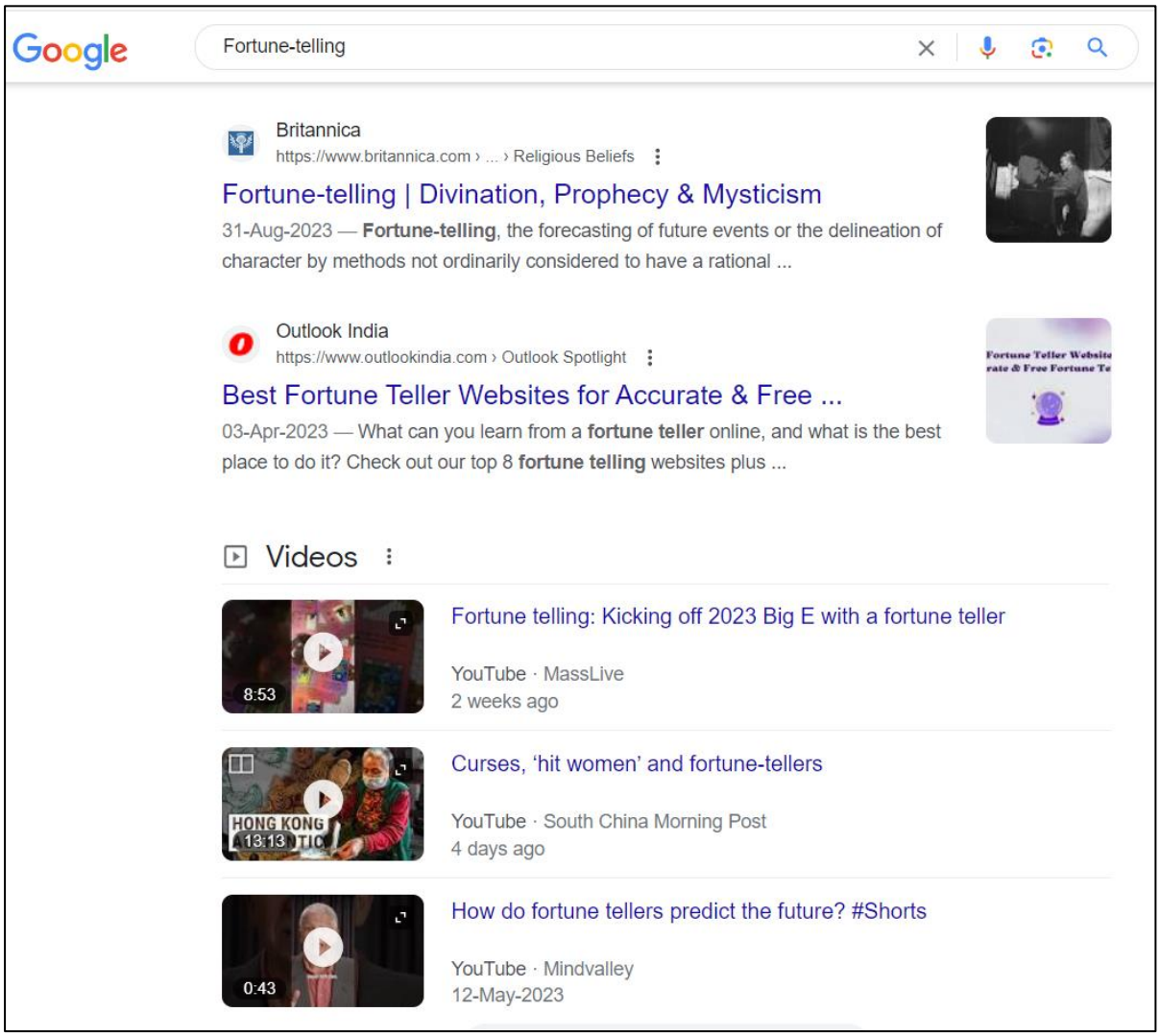
5. Louis “I” France



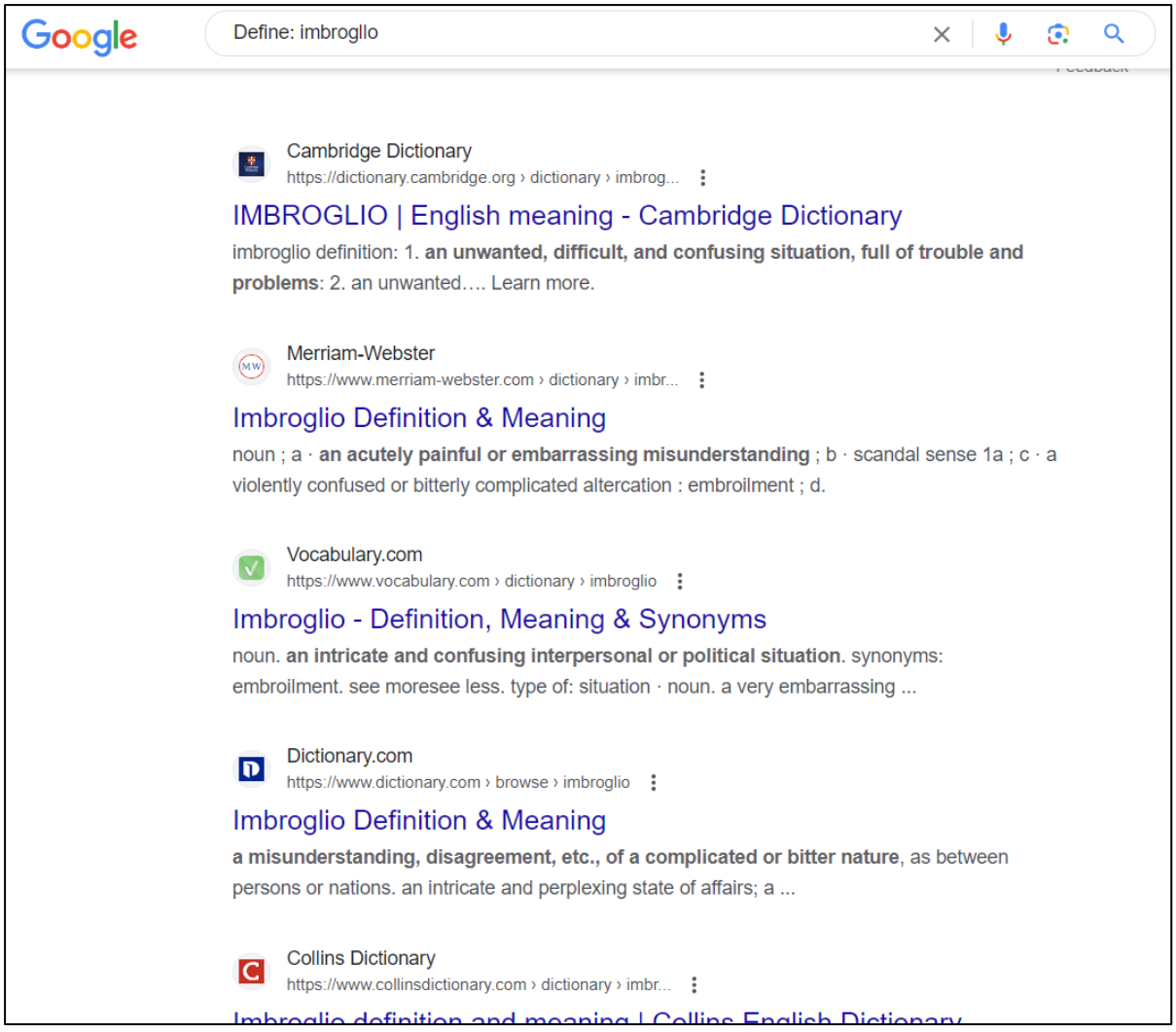
6. castle ~glossary



7. Fortune-telling

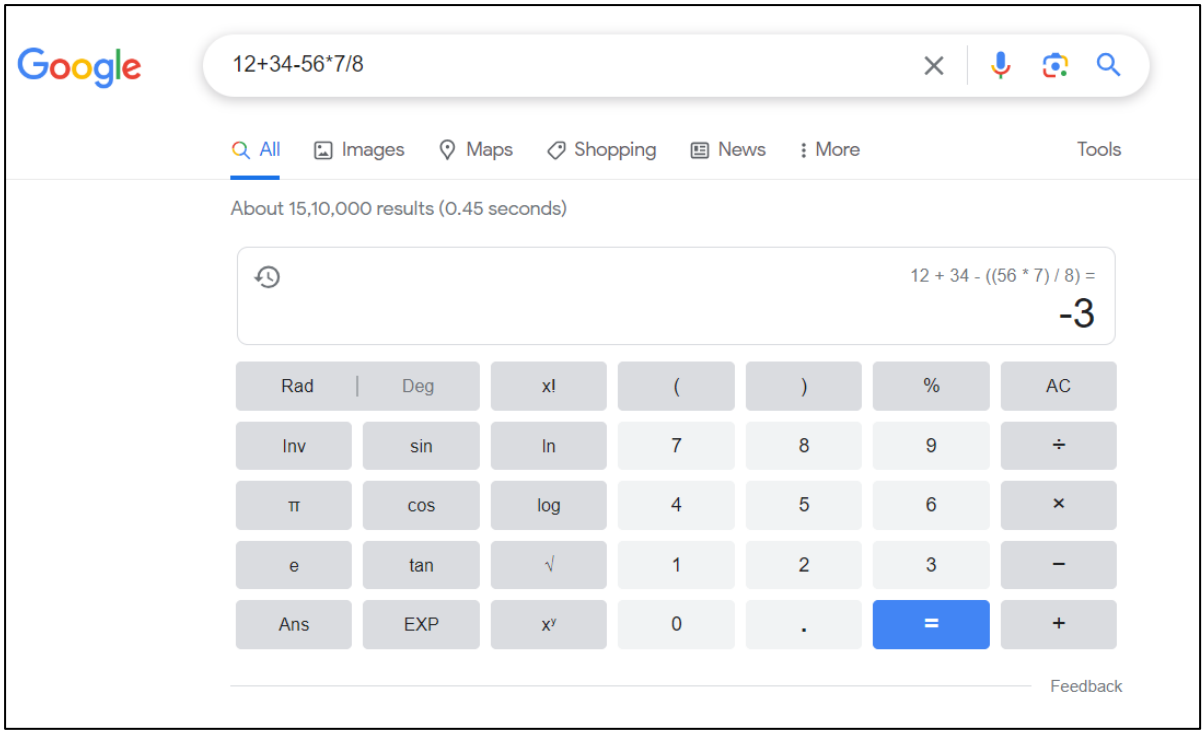


8. Define: imbrogllo

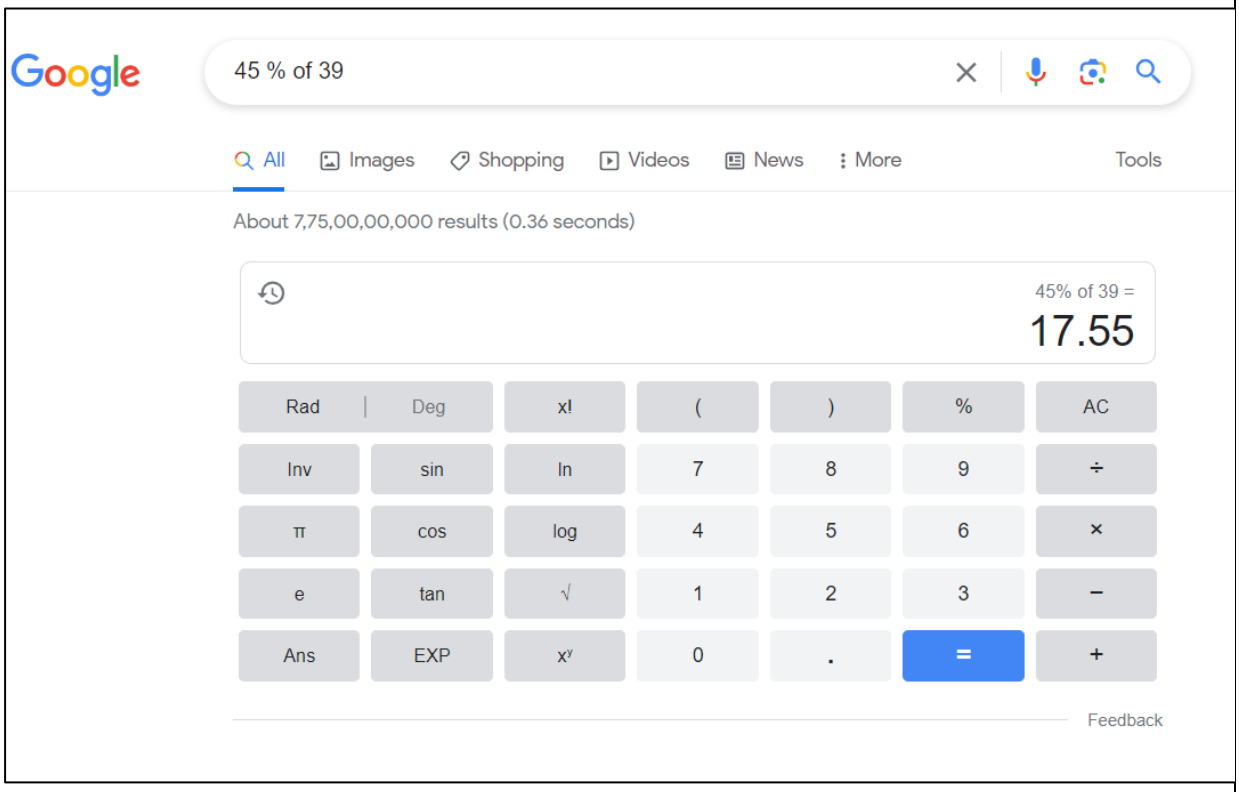


No.	Calculator Operators	Meaning	Search Query
1	+ - * /	Basic arithmetic	12+34-56*7/8
2	% of	Percentage of	45 % of 39
3	^ or **	Raise to a power	2^5 or 2**5
4	Old units in new units	Convert units	300 Euros in USD, 130 lbs in kg, 31 in hex

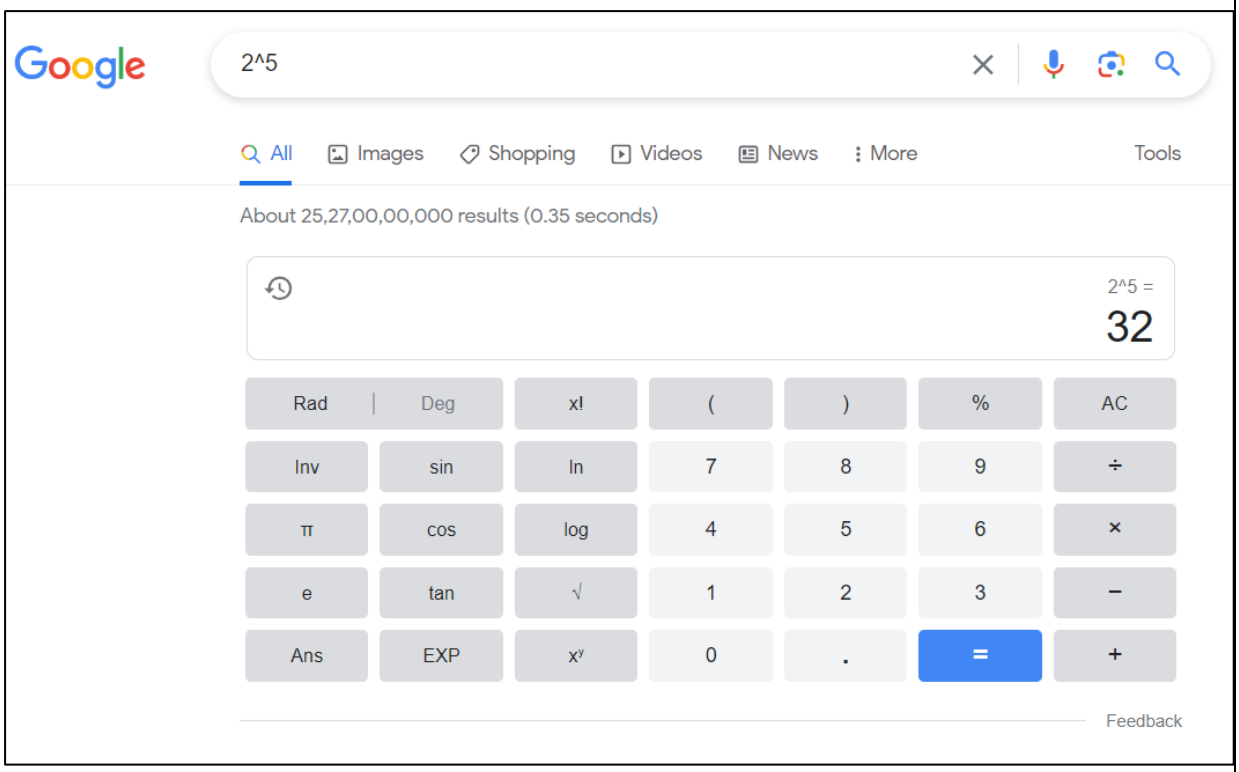
1. + - * /



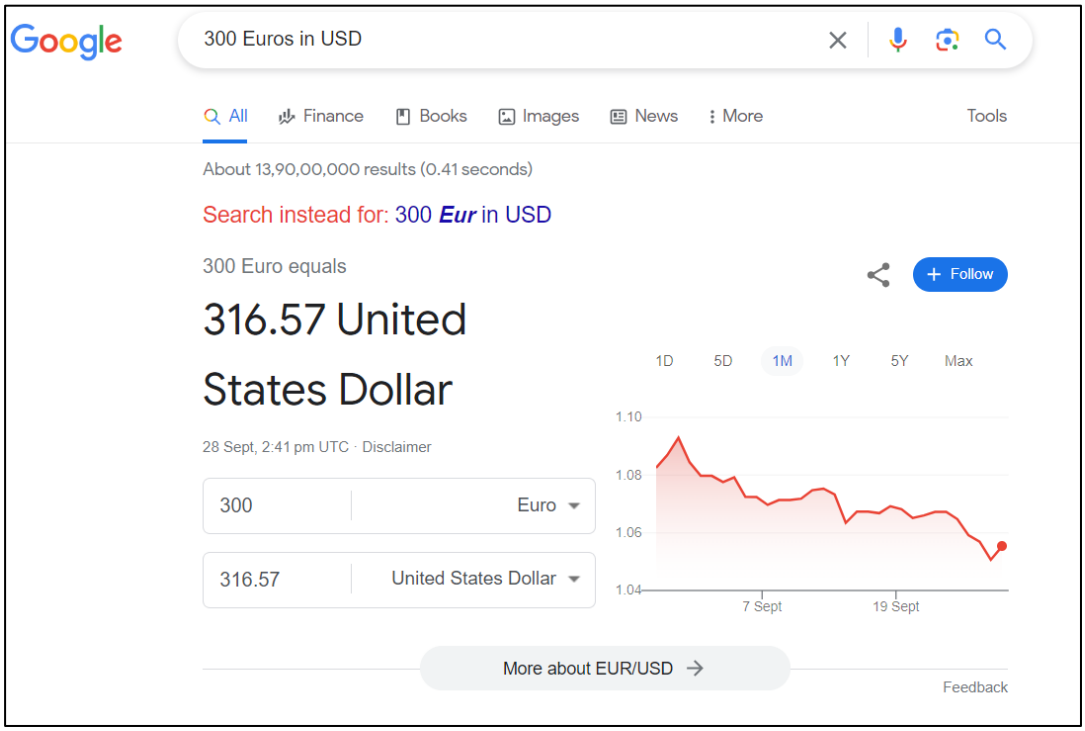
2. % of

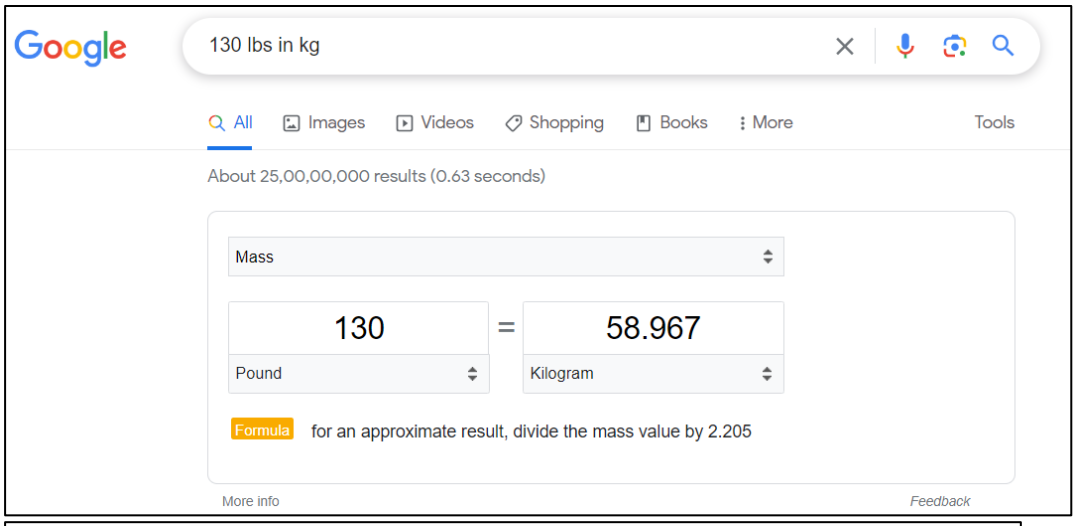

Google
45 % of 39
All
Images
Shopping
Videos
News
More
Tools
About 7,75,00,00,000 results (0.36 seconds)
45% of 39 =
17.55
Rad
Deg
x!
(
)
%
AC
Inv
sin
ln
7
8
9
÷
π
cos
log
4
5
6
×
e
tan
√
1
2
3
−
Ans
EXP
xʸ
0
.
=
+
Feedback

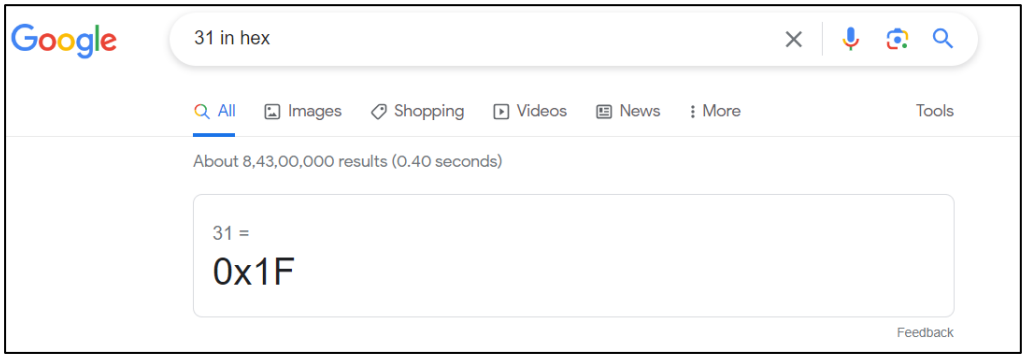
3. ^ or **


Google
2^5
All
Images
Shopping
Videos
News
More
Tools
About 25,27,00,00,000 results (0.35 seconds)
2^5 =
32
Rad
Deg
x!
(
)
%
AC
Inv
sin
ln
7
8
9
÷
π
cos
log
4
5
6
×
e
tan
√
1
2
3
−
Ans
EXP
xʸ
0
.
=
+
Feedback

4. Old units in new units



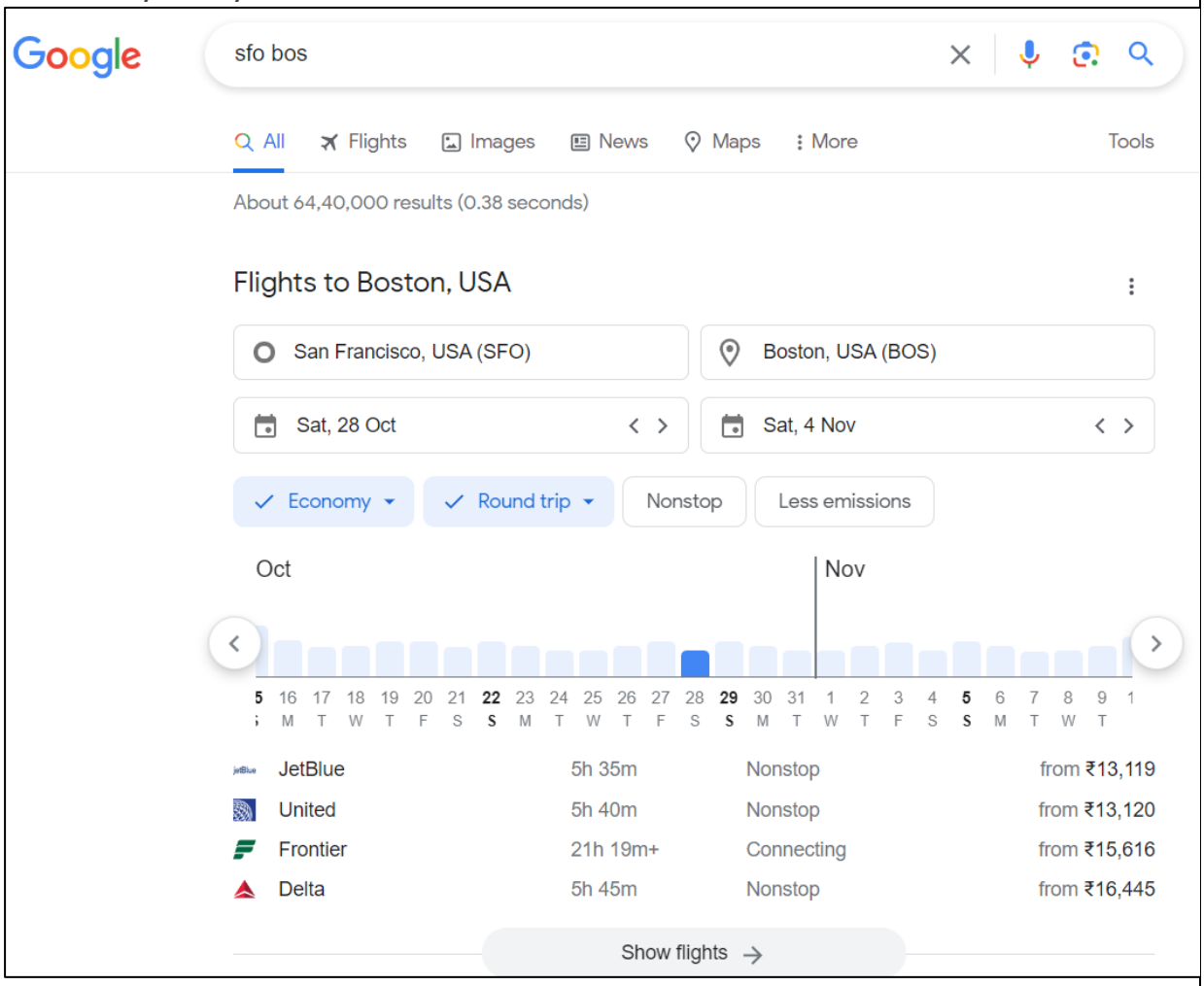




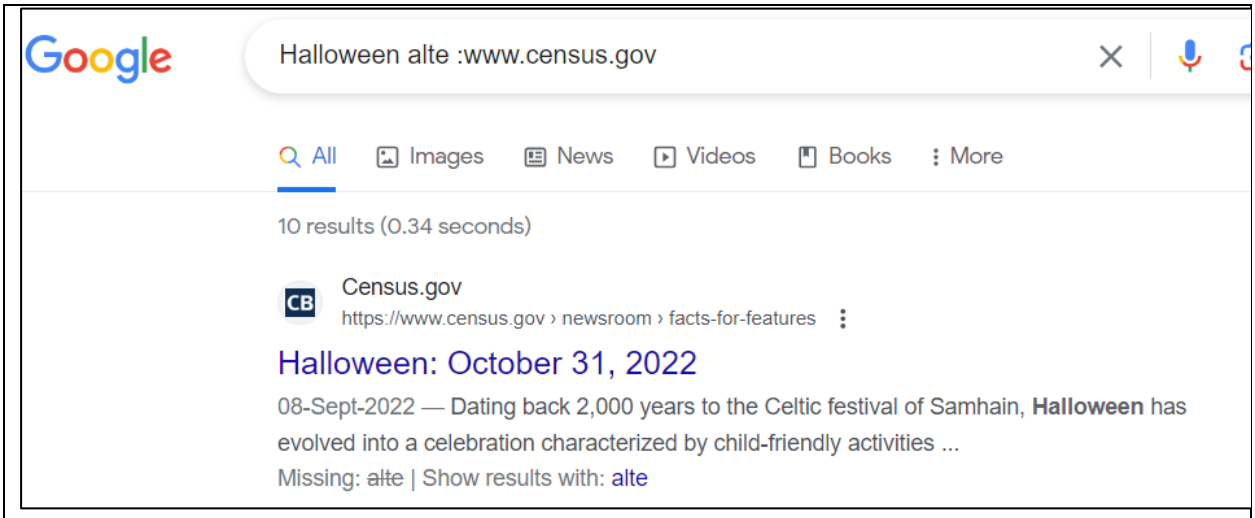
No.	Restrict Search	Meaning	Search Query
1	City 1 City 2	Book flights	sfo bos

2	Site:	Search only one website or domain	Halloween alte :www.census.gov
3	[#] [#]	Search within a range of numbers	Dave Barry pirate 2002 2006
4	filetype:	Find documents of the specified type	form 1098 -T IRS filetype:pdf
5	Llnk	Find linked pages , show pages that point to url	llnk:warriorlibrarian.com

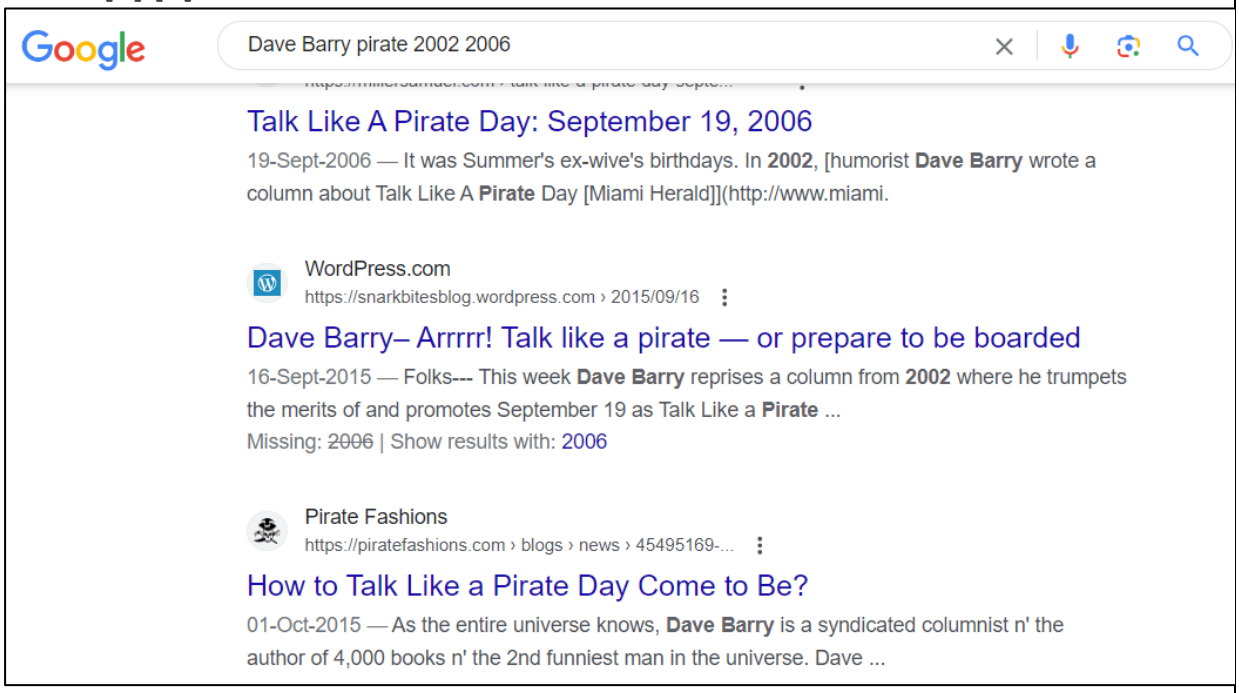
1. City 1 City 2



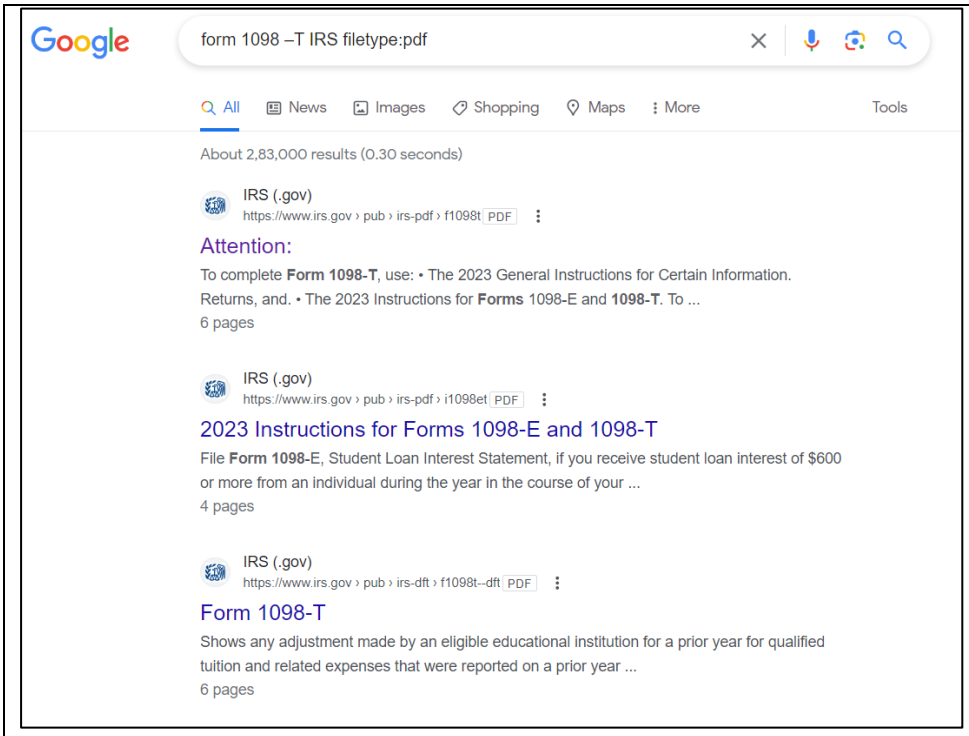
2. Site:


Google
Halloween alte :www.census.gov
All
Images
News
Videos
Books
More
10 results (0.34 seconds)
Census.gov
https://www.census.gov › newsroom › facts-for-features
Halloween: October 31, 2022
08-Sept-2022 — Dating back 2,000 years to the Celtic festival of Samhain, Halloween has evolved into a celebration characterized by child-friendly activities ...
Missing: alte | Show results with: alte

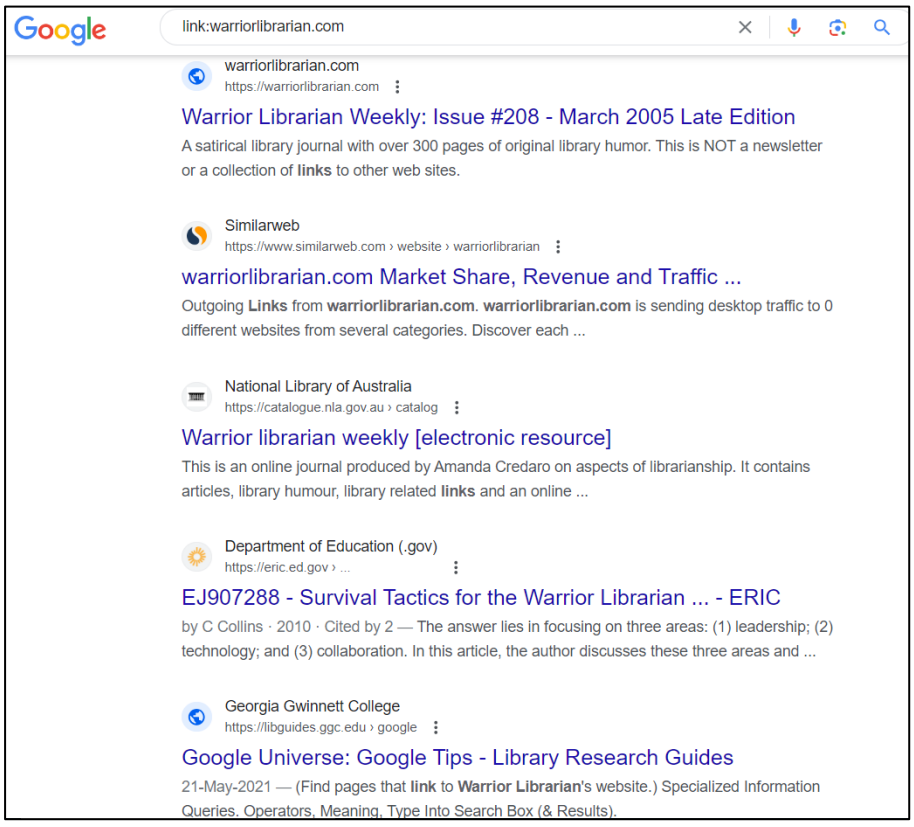
3. [#] [#]


Google
Dave Barry pirate 2002 2006
Talk Like A Pirate Day: September 19, 2006
19-Sept-2006 — It was Summer's ex-wive's birthdays. In 2002, [humorist Dave Barry wrote a column about Talk Like A Pirate Day [Miami Herald]](http://www.miami.
WordPress.com
https://snarkbitesblog.wordpress.com › 2015/09/16
Dave Barry– Arrrrr! Talk like a pirate — or prepare to be boarded
16-Sept-2015 — Folks--- This week Dave Barry reprises a column from 2002 where he trumpets the merits of and promotes September 19 as Talk Like a Pirate ...
Missing: 2006 | Show results with: 2006
Pirate Fashions
https://piratefashions.com › blogs › news › 45495169-...
How to Talk Like a Pirate Day Come to Be?
01-Oct-2015 — As the entire universe knows, Dave Barry is a syndicated columnist n' the author of 4,000 books n' the 2nd funniest man in the universe. Dave ...

4. filetype:



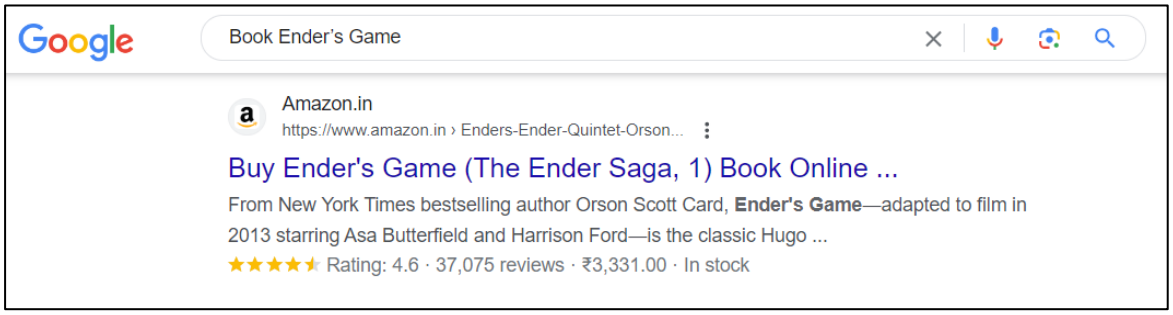
5. LInk



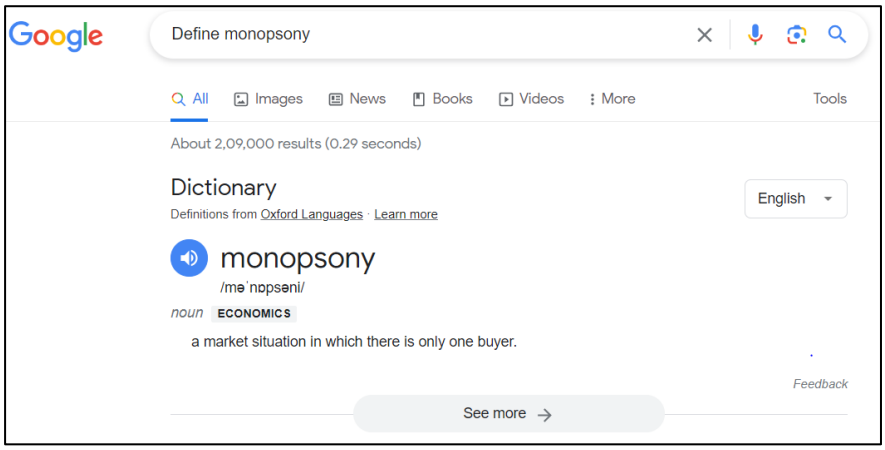
No.	Specialized Information Queries	Meaning	Search Query

1	Book or books	Search full text of books	Book Ender's Game
2	Define, what is, what are	Show a definition for a word or phrase	Define monopsony , what is podcast,
3	define:	Provide definations for a word , phrases and acronomy from the web	define: kerning
4	movie:	Find reviews and showtimes	movie: traffic
5	stocks:	Given ticker symbol,show stock information.	stocks: goog
6	weather	Given a location , show the weather	Weather Mumbai 400034

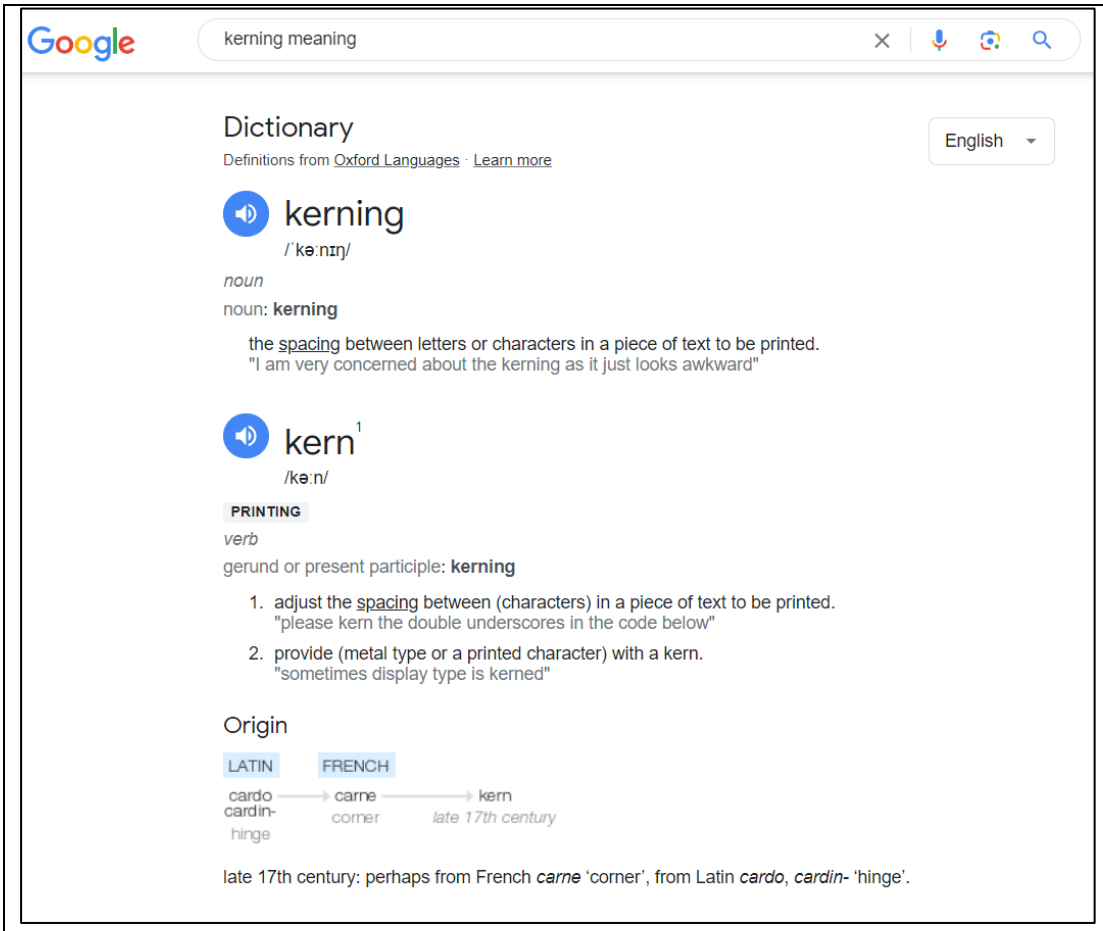
1. Book or books



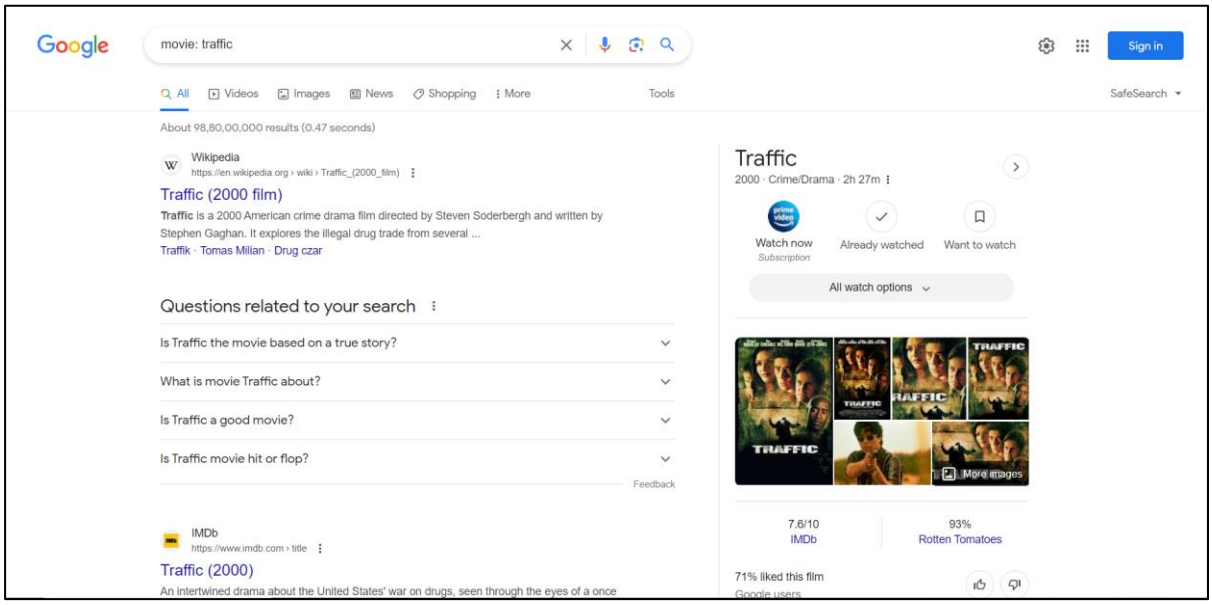
2. Define, what is, what are



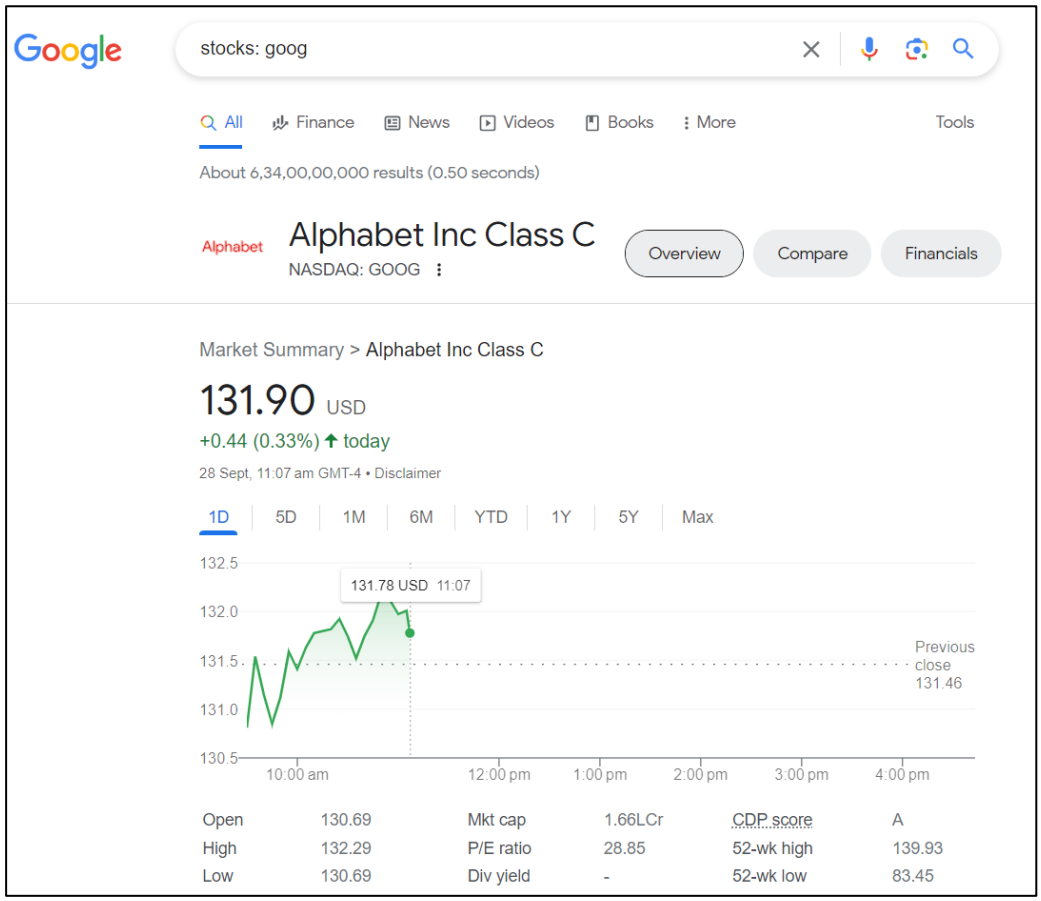
3. define:


Google
kerning meaning
Dictionary
Definitions from Oxford Languages · Learn more
English
kerning
/ˈkəːnɪŋ/
noun
noun: kerning
the spacing between letters or characters in a piece of text to be printed.
"I am very concerned about the kerning as it just looks awkward"
kern[1]
/kəːn/
PRINTING
verb
gerund or present participle: kerning
1. adjust the spacing between (characters) in a piece of text to be printed.
"please kern the double underscores in the code below"
2. provide (metal type or a printed character) with a kern.
"sometimes display type is kerned"
Origin
LATIN
FRENCH
cardo
cardin-
hinge
carne
corner
kern
late 17th century
late 17th century: perhaps from French carne 'corner', from Latin cardo, cardin- 'hinge'.

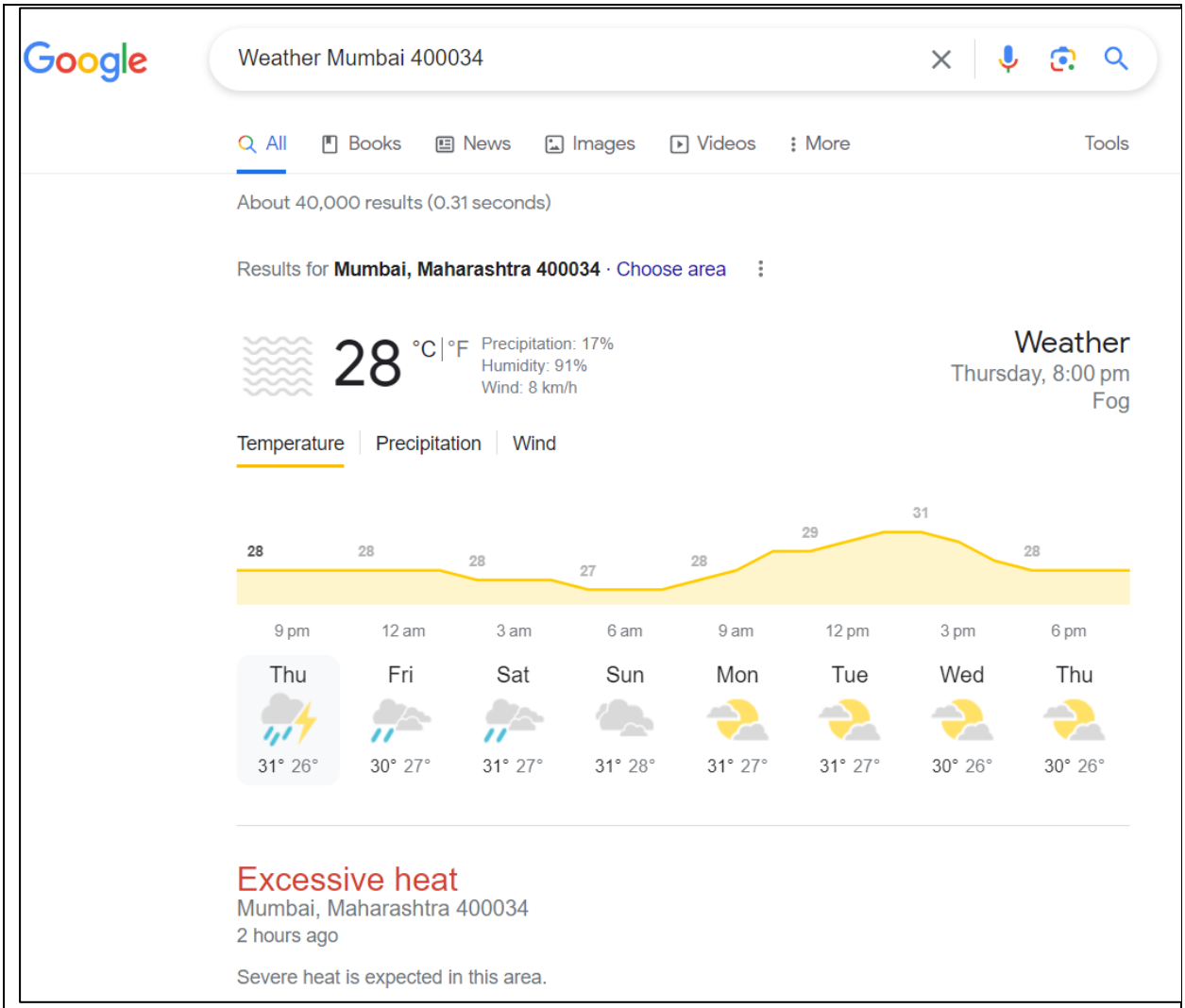
4. movie:


Google
movie: traffic
Sign in
All
Videos
Images
News
Shopping
More
Tools
SafeSearch
About 98,80,00,000 results (0.47 seconds)
Wikipedia
https://en.wikipedia.org › wiki › Traffic_(2000_film)
Traffic (2000 film)
Traffic is a 2000 American crime drama film directed by Steven Soderbergh and written by Stephen Gaghan. It explores the illegal drug trade from several ...
Traffik · Tomas Milian · Drug czar
Questions related to your search
Is Traffic the movie based on a true story?
What is movie Traffic about?
Is Traffic a good movie?
Is Traffic movie hit or flop?
Feedback
IMDb
https://www.imdb.com › title
Traffic (2000)
An intertwined drama about the United States' war on drugs, seen through the eyes of a once
Traffic
2000 · Crime/Drama · 2h 27m
Watch now
Subscription
Already watched
Want to watch
All watch options
More images
7.6/10
IMDb
93%
Rotten Tomatoes
71% liked this film
Google users

5. stocks:



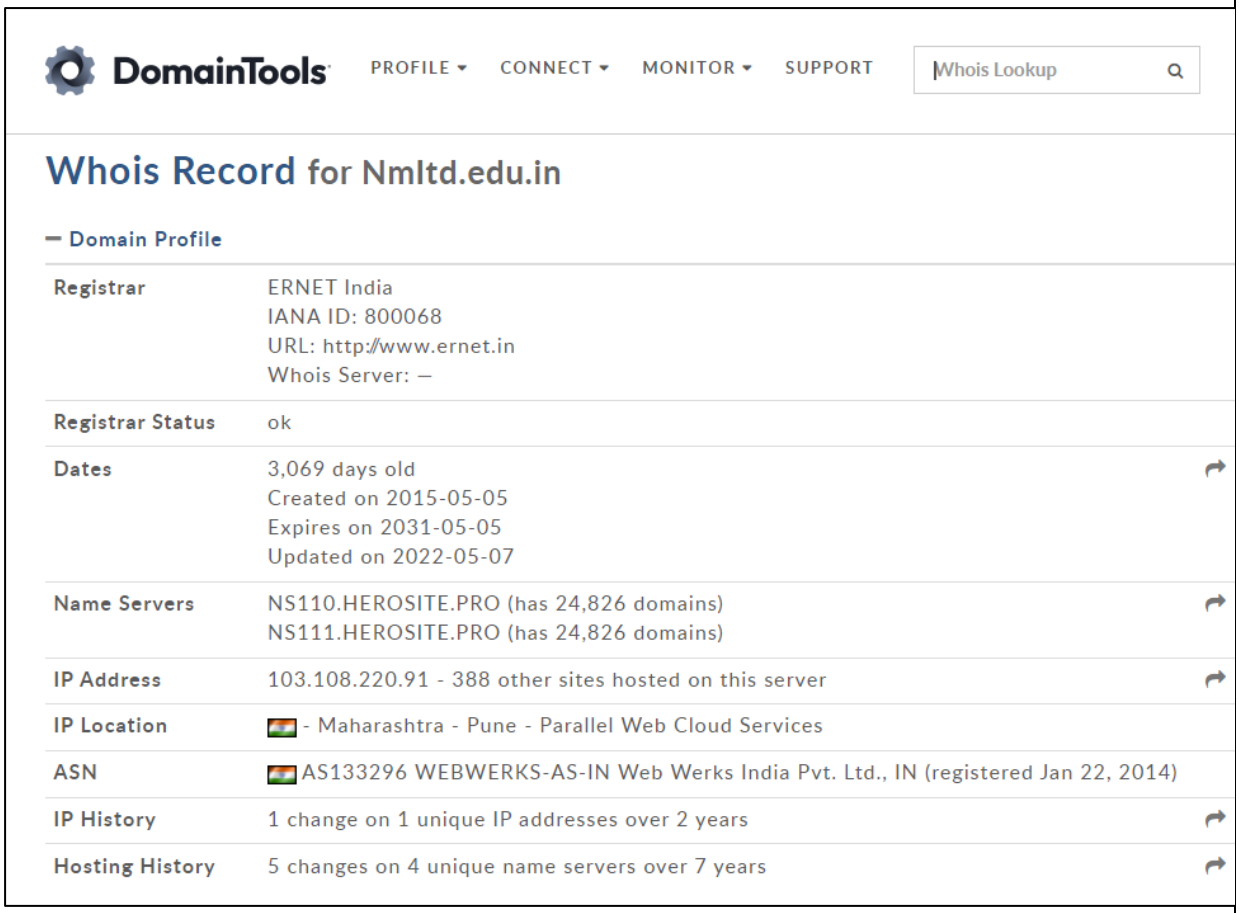
6. weather



Aim : Using the software tools/commands to perform the following , generate an analysis report :
B) To find out the information about a website

Description :
Input your college website in the input box and display the information obtained.

Output:


DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
Whois Record for Nmltd.edu.in
Domain Profile
Registrar
ERNET India
IANA ID: 800068
URL: http://www.ernet.in
Whois Server: —
Registrar Status
ok
Dates
3,069 days old
Created on 2015-05-05
Expires on 2031-05-05
Updated on 2022-05-07
Name Servers
NS110.HEROSITE.PRO (has 24,826 domains)
NS111.HEROSITE.PRO (has 24,826 domains)
IP Address
103.108.220.91 - 388 other sites hosted on this server
IP Location
- Maharashtra - Pune - Parallel Web Cloud Services
ASN
AS133296 WEBWERKS-AS-IN Web Werks India Pvt. Ltd., IN (registered Jan 22, 2014)
IP History
1 change on 1 unique IP addresses over 2 years
Hosting History
5 changes on 4 unique name servers over 7 years

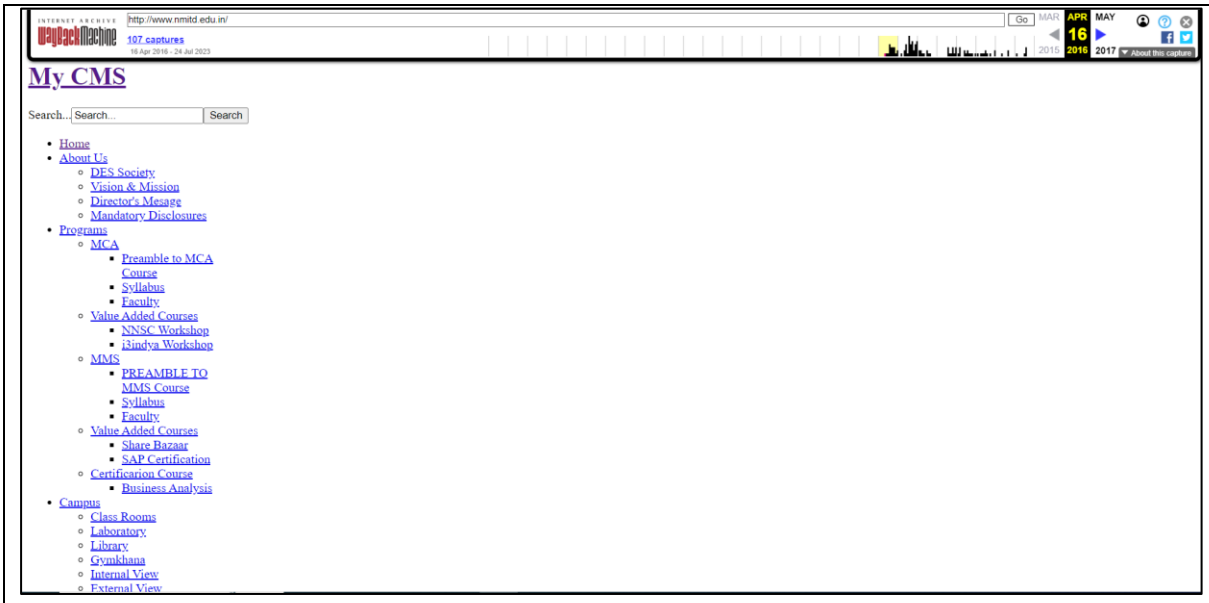
Whois Record (last updated on 2023-09-29)

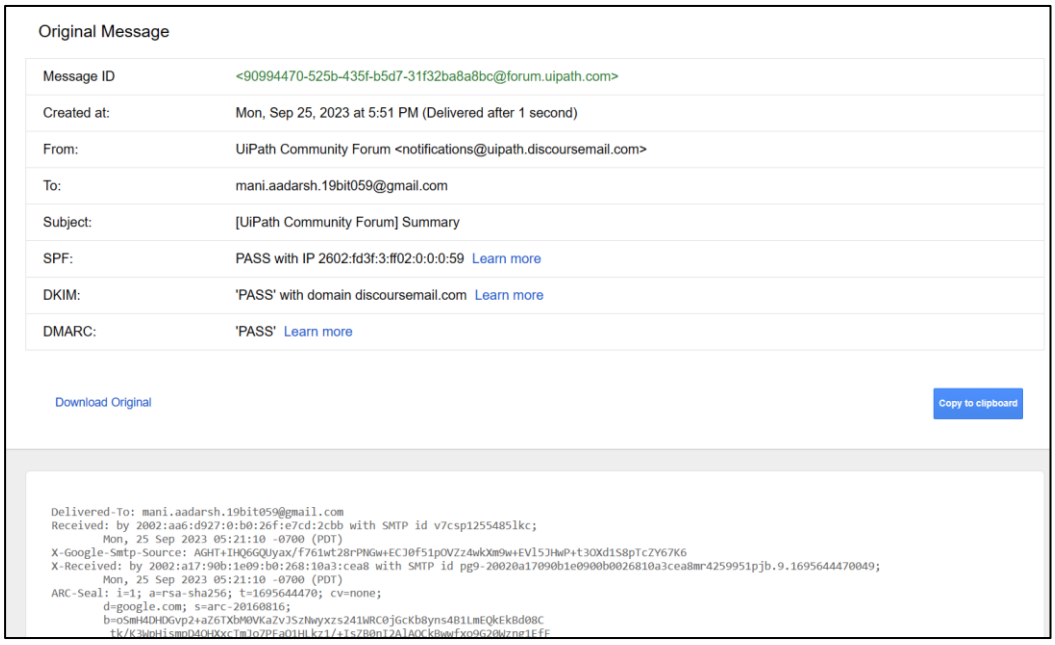
```
Domain Name: nmitd.edu.in
Registry Domain ID: D9437720-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2022-05-07T06:08:38Z
Creation Date: 2015-05-05T08:32:01Z
Registry Expiry Date: 2031-05-05T08:32:01Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: NAVINCHANDRA MEHTA INSTITUTE OF TECHNOLOGY AND DEVELOPMENT
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
```

Aim : Using the software tools/commands to perform the following , generate an analysis report :
C) To find the information about an archived website

Description : Display the snapshot of how the your college website looked like(Eg nmitd.edu.in) in the year 2016 on 16th April.

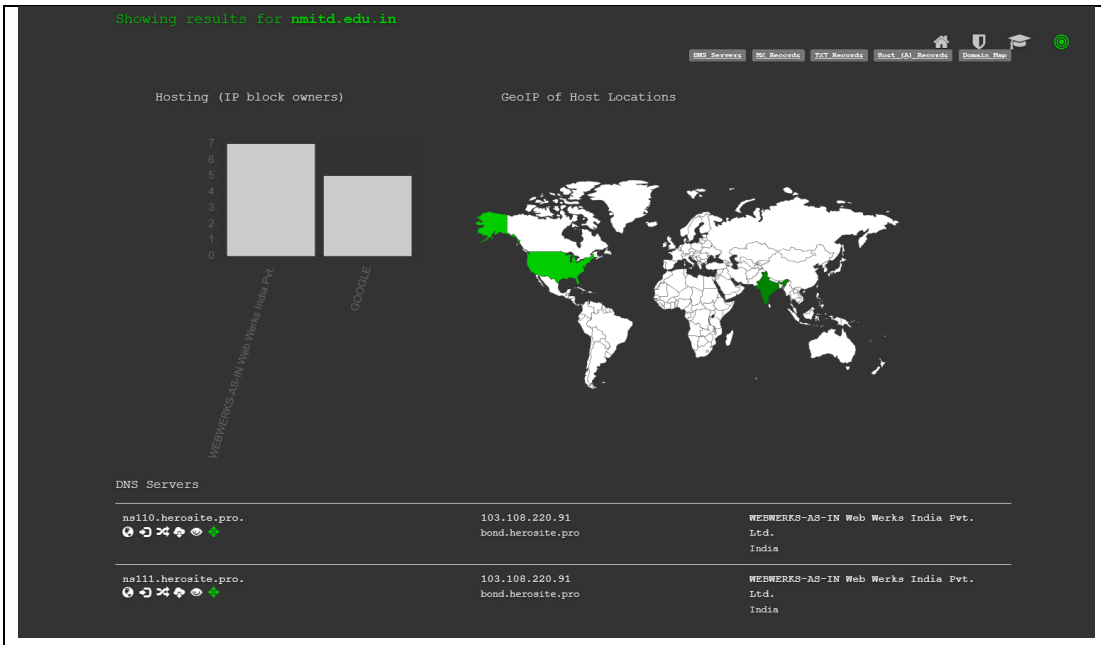
Output:

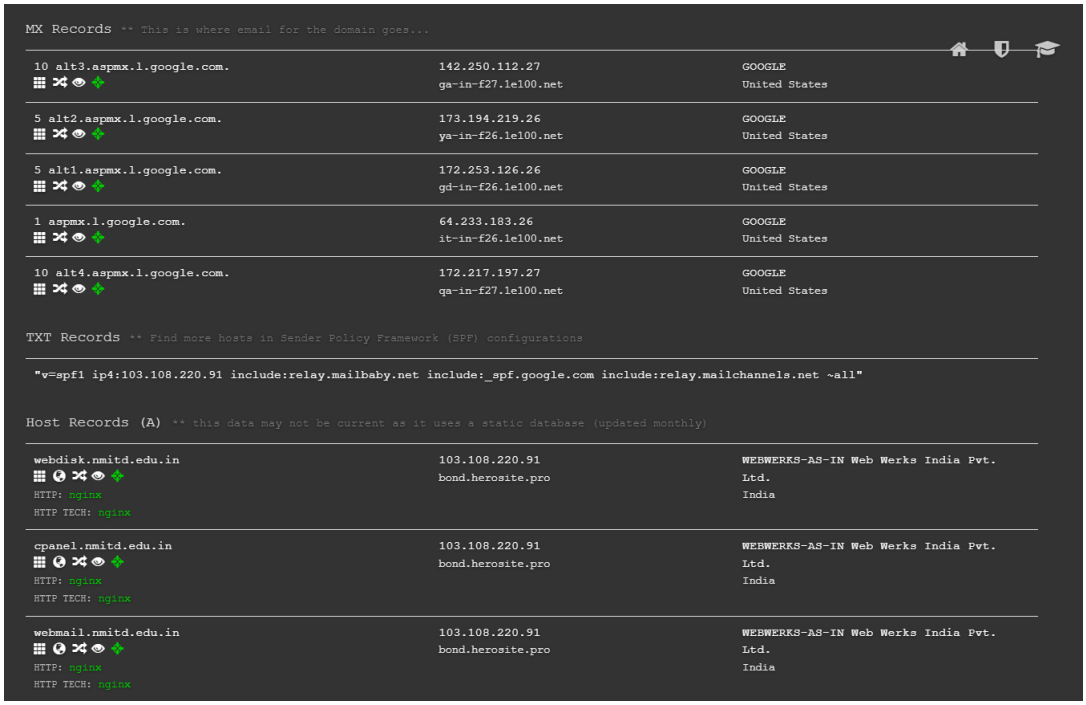




Aim : Using the software tools/commands to perform the following , generate an analysis report :
D) To fetch DNS information.

Output:





Practical.No 2 : Scanning networks, Enumeration and sniffing:

Aim : Using the software tools/commands to perform the following , generate an analysis report :

A. Port scanning .

Description :

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can't take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

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.

Output:

1. Display the following for ip address 127.0.0.1 or any other ip address
   a. Scan open ports (syntax: nmap –open ip_address / url)
   b. Scan ports (syntax: nmap ip_address / url)
   c. Scan single port (syntax: nmap -p 80 ip_address)
   d. Scan specified range of ports (syntax: nmap -p 1-200 ip_address)
   e. Scan entire port range (syntax: nmap -p 1-65535 ip_address)
   f. Scan top 100 ports (fast scan) (syntax: nmap -F ip_address)

Aim : Using the software tools/commands to perform the following , generate an analysis report :
B. Network scanning tools

Description : Network scanning consists of network port scanning as well as vulnerability scanning.
Network port scanning refers to the method of sending data packets via the network to a computing system's specified service port numbers (for example, port 23 for Telnet, port 80 for HTTP and so on). This is to identify the available network services on that particular system. This procedure is effective for troubleshooting system issues or for tightening the system's security.
Vulnerability scanning is a method used to discover known vulnerabilities of computing systems available on a network. It helps to detect specific weak spots in an application software or the operating system (OS), which could be used to crash the system or compromise it for undesired purposes.
Network port scanning as well as vulnerability scanning is an information-gathering technique, but when carried out by anonymous individuals, these are viewed as a prelude to an attack.
Network scanning processes, like port scans and ping sweeps, return details about which IP addresses map to active live hosts and the type of services they provide. Another network scanning method known as inverse mapping gathers details about IP addresses that do not map to live hosts, which helps an attacker to focus on feasible addresses.
Network scanning is one of three important methods used by an attacker to gather information. During the footprint stage, the attacker makes a profile of the targeted organization. This includes data such as the organization's domain name system (DNS) and e-mail servers, in addition to its IP address range. During the scanning stage, the attacker discovers details about the specified IP addresses that could be accessed online, their system architecture, their OSs and the services running on every computer. During the enumeration stage, the attacker collects data, including routing tables, network user and group names, Simple Network Management Protocol (SNMP) data and so on.

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

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

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

OS Scan – This command returns information on the OS (and version) of a host.

Output: Demonstrate how to scan networks. Explain the steps and attach output

```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::908f:24ce:e0:6797%6
   IPv4 Address. . . . . . . . . . . : 192.168.53.45
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.52.1
```

Nmap –sP <ip address>

```
C:\Users\admin>Nmap -sP 192.168.53.45
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 15:45 India Standard Time
Nmap scan report for 192.168.53.45
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Nmap –sN <ip address>

```
C:\Users\admin>nmap -sn 192.168.52.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 15:47 India Standard Time
Nmap scan report for 192.168.52.1
Host is up (0.0010s latency).
MAC Address: C8:4F:86:02:4B:00 (Sophos)
Nmap scan report for 192.168.52.5
Host is up (0.0010s latency).
MAC Address: C0:74:AD:25:7F:82 (Grandstream Networks)
Nmap scan report for 192.168.52.6
Host is up (0.0010s latency).
MAC Address: F4:B5:49:F3:15:A5 (Xiamen Yeastar Information Technology)
Nmap scan report for 192.168.52.7
Host is up (0.0010s latency).
MAC Address: EC:A8:6B:FD:46:F8 (Elitegroup Computer Systems)
Nmap scan report for 192.168.52.10
Host is up (0.00s latency).
MAC Address: 00:17:61:11:F2:89 (Private)
Nmap scan report for 192.168.52.21
Host is up (0.0020s latency).
MAC Address: C0:74:AD:55:AA:C8 (Grandstream Networks)
Nmap scan report for 192.168.52.22
Host is up (0.0020s latency).
```

Nmap –sL <ip address>

```
C:\Users\admin>nmap -sL 192.168.53.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 15:57 India Standard Time
Nmap scan report for 192.168.53.0
Nmap scan report for 192.168.53.1
Nmap scan report for 192.168.53.2
Nmap scan report for 192.168.53.3
Nmap scan report for 192.168.53.4
Nmap scan report for 192.168.53.5
Nmap scan report for 192.168.53.6
Nmap scan report for 192.168.53.7
Nmap scan report for 192.168.53.8
Nmap scan report for 192.168.53.9
Nmap scan report for 192.168.53.10
Nmap scan report for 192.168.53.11
Nmap scan report for 192.168.53.12
Nmap scan report for 192.168.53.13
Nmap scan report for 192.168.53.14
Nmap scan report for 192.168.53.15
Nmap scan report for 192.168.53.16
Nmap scan report for 192.168.53.17
Nmap scan report for 192.168.53.18
Nmap scan report for 192.168.53.19
Nmap scan report for 192.168.53.20
Nmap scan report for 192.168.53.21
Nmap scan report for 192.168.53.22
Nmap scan report for 192.168.53.23
```

Finding the Os of the neighbouring

nmap -O <target IP>

```
C:\Users\admin>nmap -O 192.168.53.45
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 16:03 India Standard Time
Nmap scan report for 192.168.53.45
Host is up (0.00043s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 2004
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

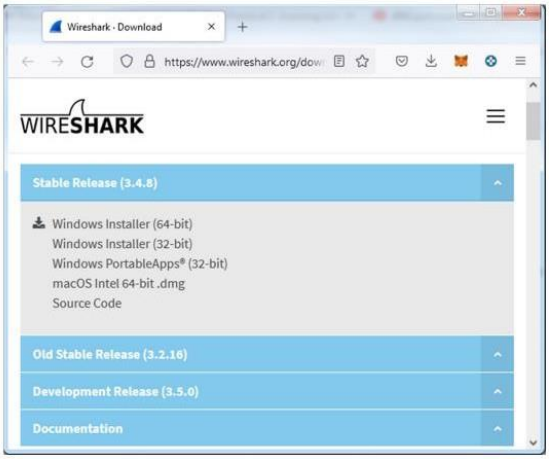
```
C:\Users\admin>nmap -O 142.250.199.164
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 16:01 India Standard Time
Nmap scan report for bom07s37-in-f4.1e100.net (142.250.199.164)
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|broadband router|proxy server
Running (JUST GUESSING): Google Android 7.X (91%), Linux 3.X (91%), OneAccess embedded (89%), Blue Coat embedded (85%)
OS CPE: cpe:/o:google:android:7.1.2 cpe:/o:linux:linux_kernel:3.10 cpe:/h:oneaccess:1641 cpe:/h:bluecoat:packetshaper
Aggressive OS guesses: Android 7.1.2 (Linux 3.10) (91%), OneAccess 1641 router (89%), Blue Coat PacketShaper appliance
85%)
No exact OS matches for host (test conditions non-ideal).
```

Aim : Using the software tools/commands to perform the following , generate an analysis report :
D. Sniffing tool

Description :

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

Output:



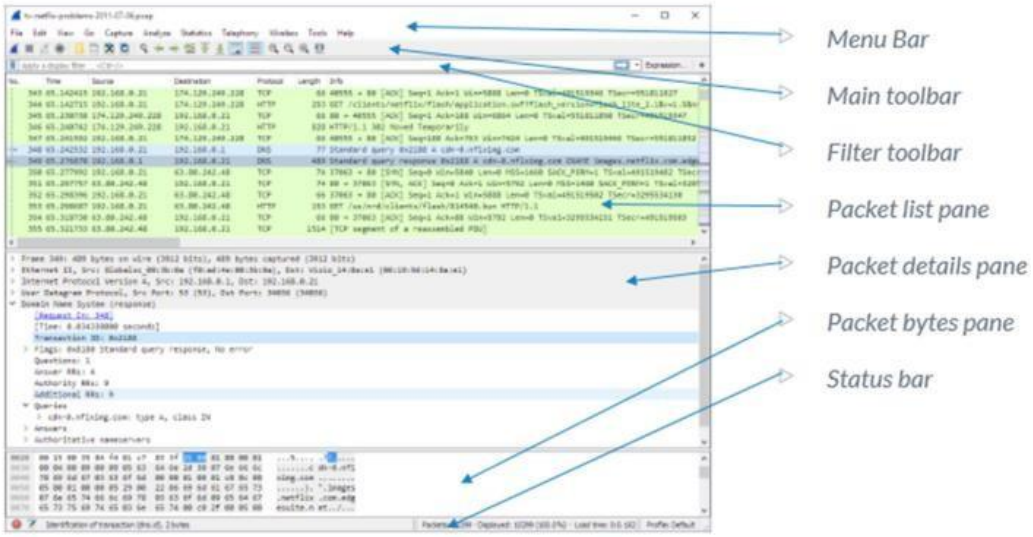
Questions:

a. How Wireshark works? Explain with steps to

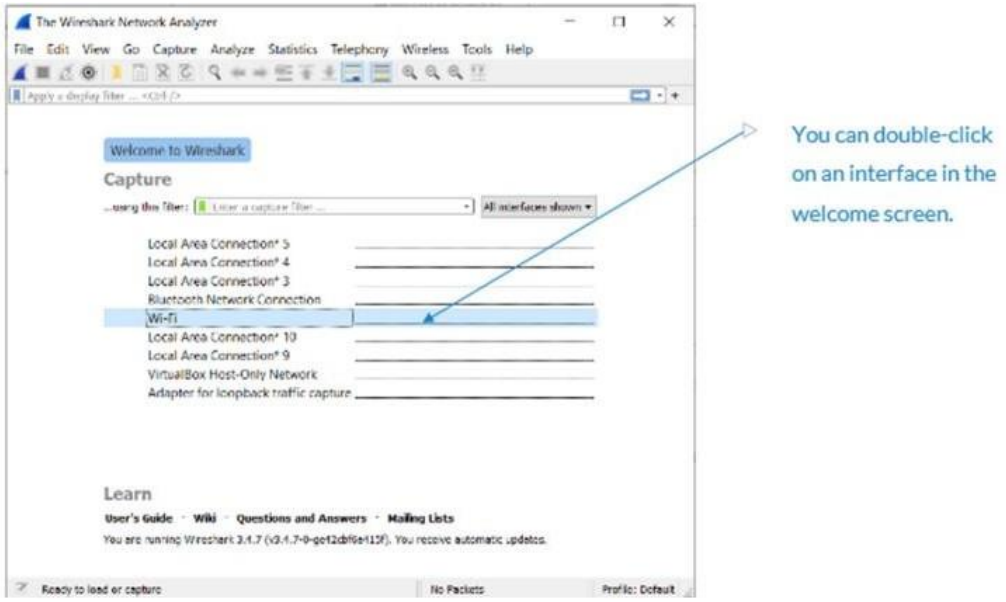
1. capture and analyse packets,

2. Apply filters and analyse packets

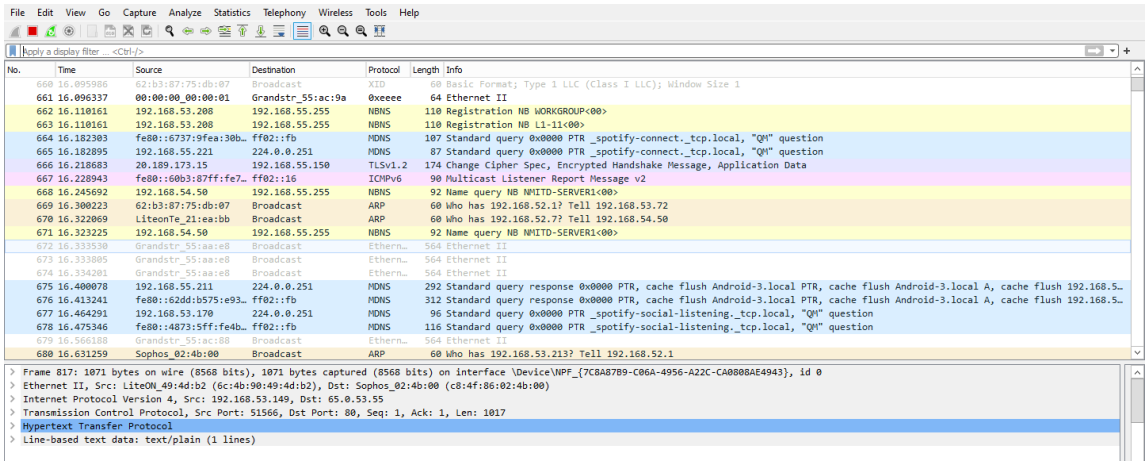
4.1 Wireshark User Interface



4.2 Capturing Live Network Data

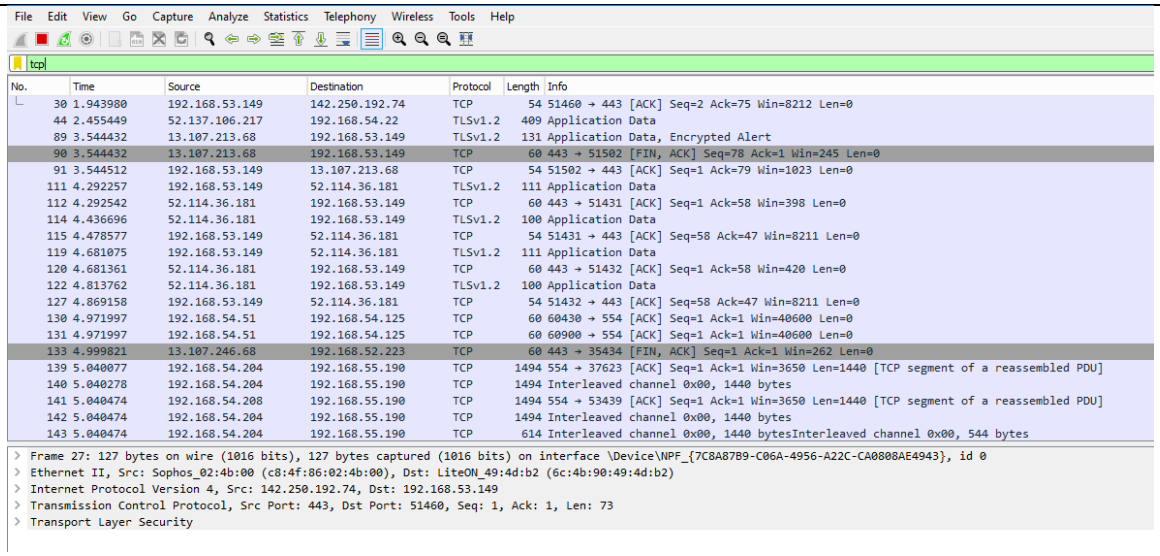


4.3 Viewing Captured Packets

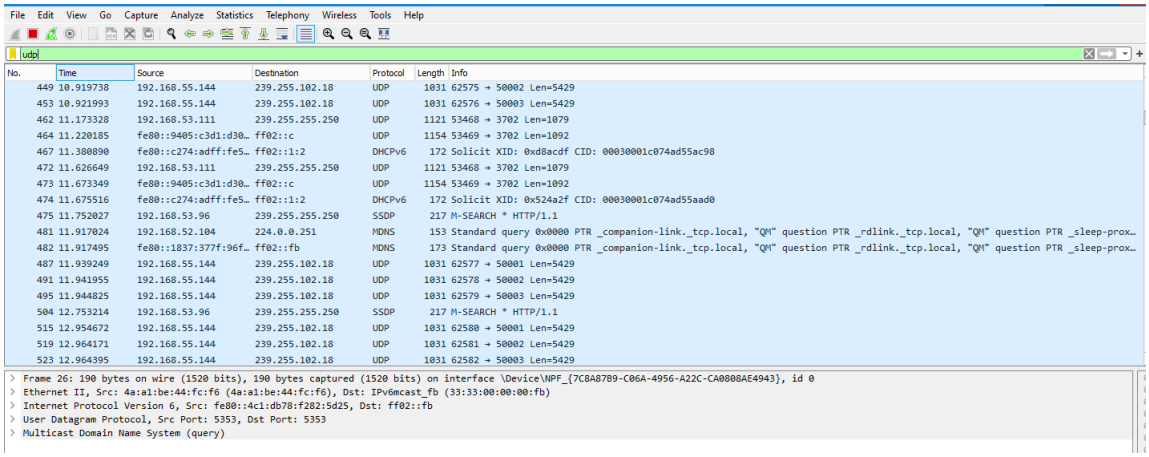


4.4 Filtering Packets While Viewing

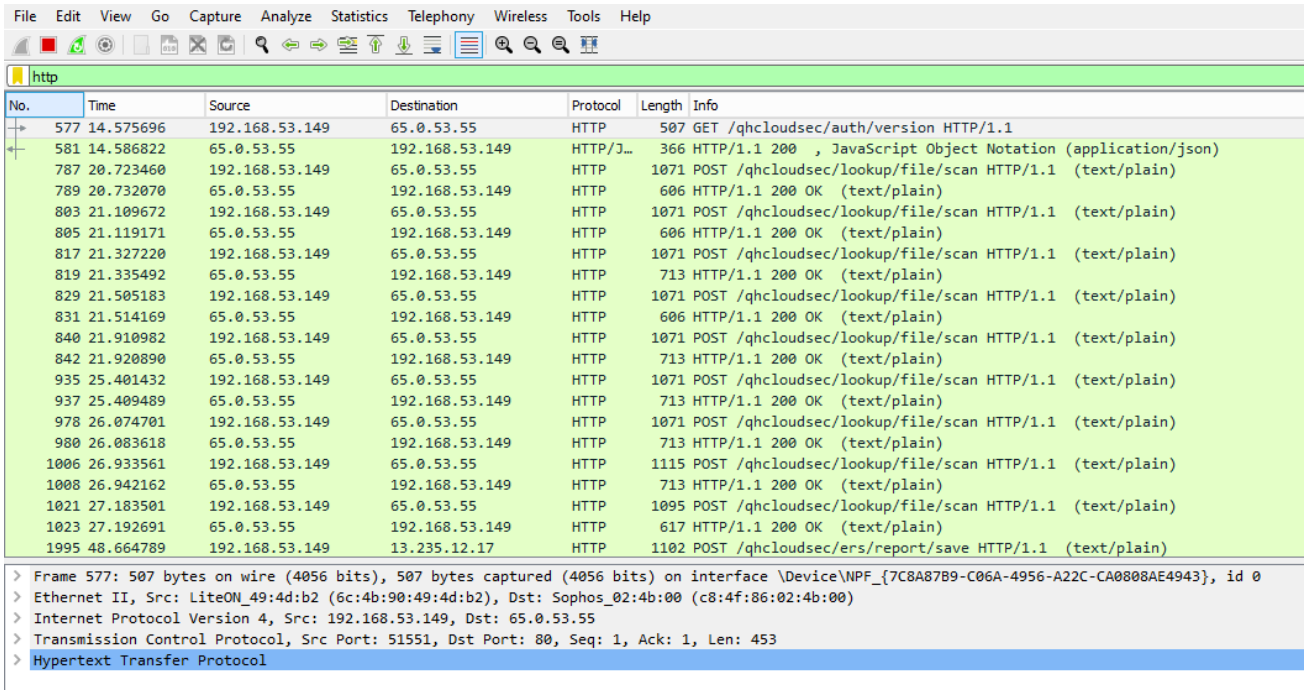
TCP



UDP



HTTP



b) How to sniff the network using Wireshark?

we are going to use Wireshark to sniff data packets as they are transmitted over HTTP protocol.For example

Step 1 start Wireshark and start capturing network

Step 2 Login to a web application that does not use secure communication.

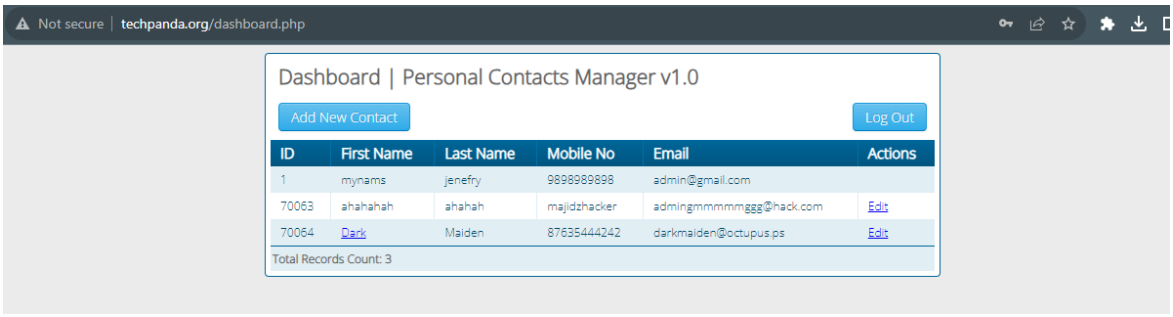
We will login to a web application on

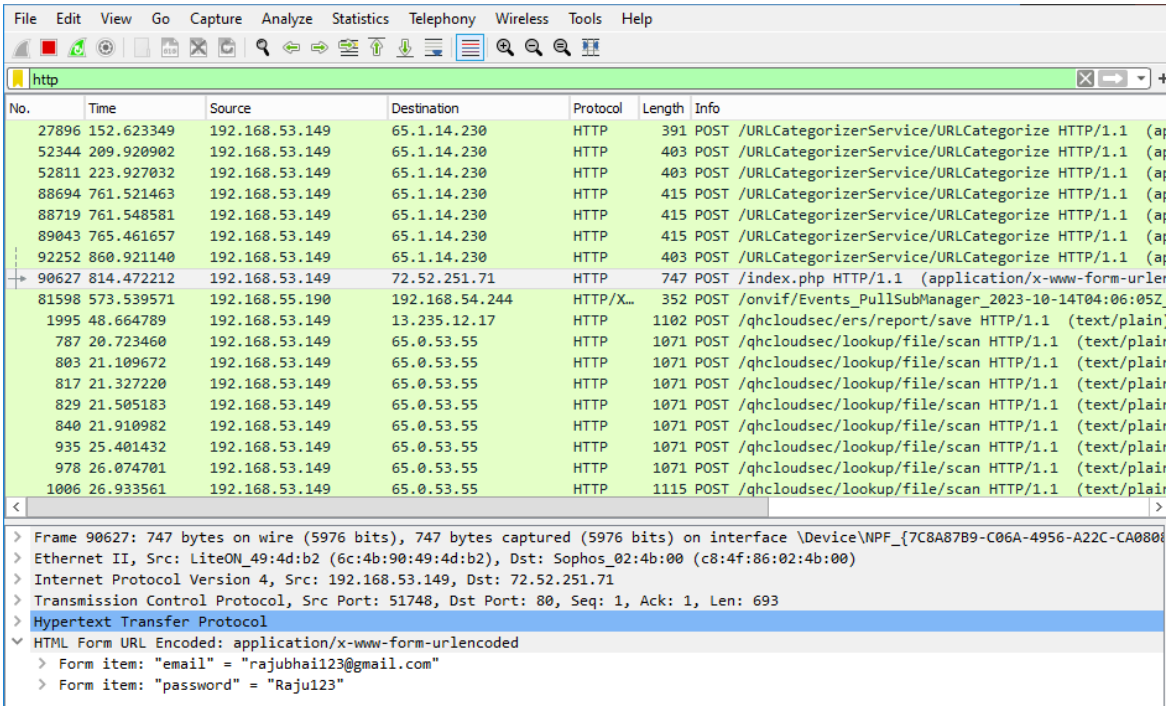
http://www.techpanda.org/

address with the **login** name is admin@google.com,

and the **password** is Password2010.

Note: we will login to the web app for demonstration purposes only.





Practical.No 3 : Malware Threats : Worms, viruses, Trojans:

Aim : Using the software tools/commands to perform the following , generate an analysis report :
A. Password cracking.

Description :
Password cracking is the process that involves computational methods to guess or retrieve a password from stored or transmitted data, typically employing algorithms executed by a computer. It is often used by hackers or malicious actors to gain unauthorized access to a target computer system or online account by guessing or cracking the password. It can be accomplished for several reasons, such as gaining access to sensitive information, stealing data or resources, conducting espionage, or carrying out malicious activities. Security professionals also use this method to test the strength of passwords and identify vulnerabilities in a system's security. However, in most cases, password cracking is done with malicious intent and is considered illegal and unethical.

Output: Generate Hash for below passwords

a. Password@123
b. PlainText
c. HelloWorld
d. 5Crocod!l3s!nL@k3

a. Password@123

Your String	Password@123
MD5 Hash	d00f5d5217896fb7fd601412cb890830 Copy

b. PlainText

Your String	PlainText
MD5 Hash	b7ebbf7f254ef646928dd58f62383a85 Copy

c. HelloWorld

Your String	HelloWorld
MD5 Hash	68e109f0f40ca72a15e05cc22786f8e6 Copy

d. 5Crocod!l3s!nL@k3

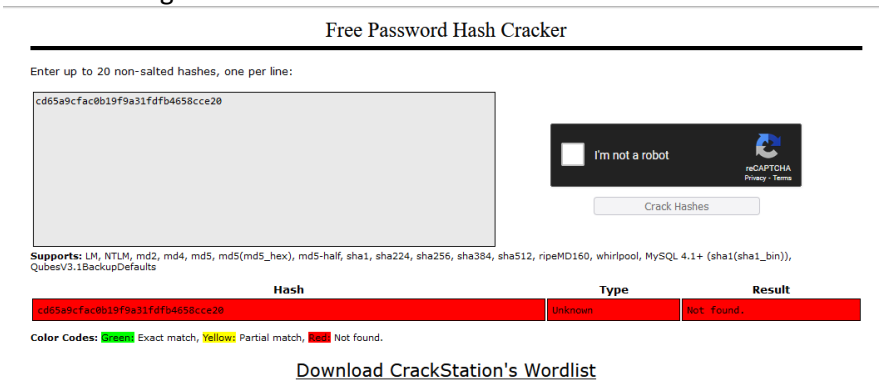
Your String	5Crocod!l3s!nL@k3
MD5 Hash	cd65a9cfac0b19f9a31fdfb4658cce20 Copy

How to decrypt MD5

It is practically impossible to reverse engineer MD5 hash as they are one-way functions.
The only way is to lookup on the web for MD5 is the Hash Databases and sites may or may not provide a correctoutput.

https://crackstation.net/

You may paste the MD5 hash and the site will lookup the hash in its database and share the result if the matchinghash is returned.



Aim : Using the software tools/commands to perform the following , generate an analysis report :
B. Dictionary attack.

Description :

Dictionary search attack: In this method, the attacker uses a list of commonly used words or phrases, also known as a dictionary, to guess the password. The attacker uses a software program that automatically tests each word in the dictionary list against the password field of the target account.
Benefits:
Faster than brute force attacks
Can crack simple passwords
Uses a pre-existing list of common passwords
Drawbacks:
Limited to common passwords
Ineffective against strong passwords
Cannot crack passwords that are not in the dictionary

Output:

Using the MD5 generator get few fingerprints of the password strings which are present in thepasswordlist.txt file.

For Eg

Password String	MD5 Finger Print
password	5f4dcc3b5aa765d61d8327deb882cf99
123456	e10adc3949ba59abbe56e057f20f883e
abc123	e99a18c428cb38d5f260853678922e03

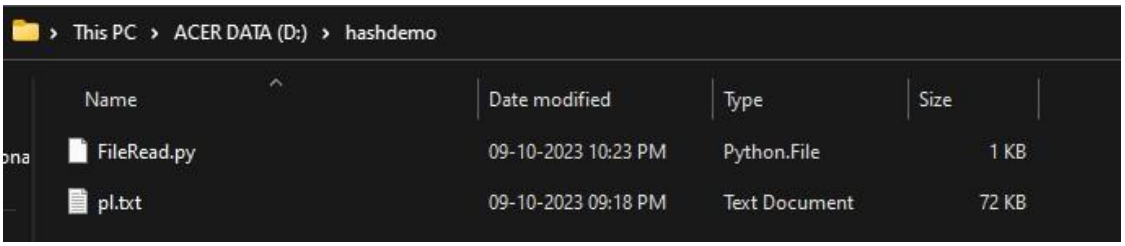
You can execute the below python program on your machine.

Be mindful of the code indentations else the program will throw an error message.

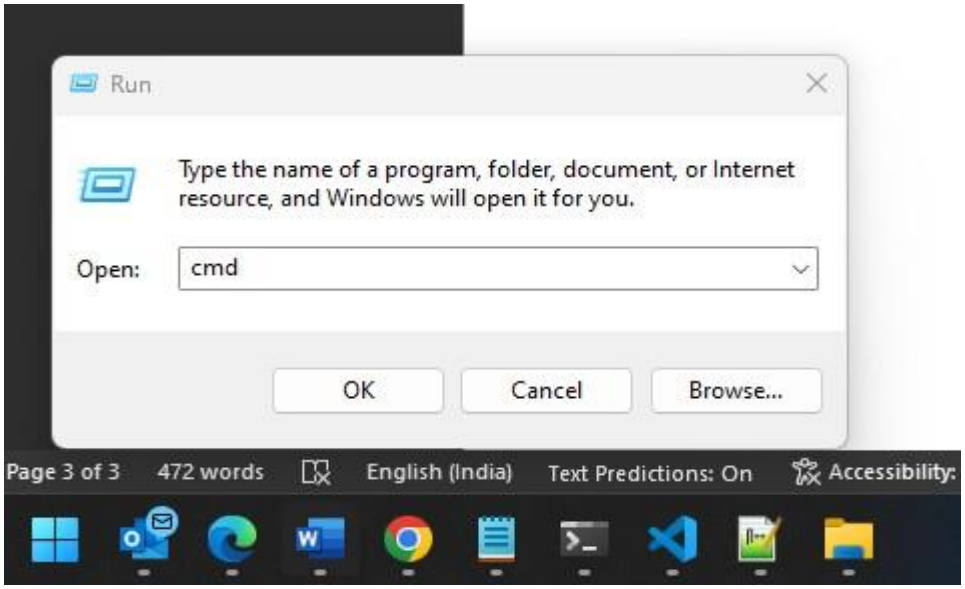
```
import hashlib
fileInput=input("Enter path of Possible Password Database File List :")
mdhash=input("Enter the MD5 Hash to lookup for possible match of Password : ")
 try:
wordList = open(fileInput, "r")
except:
print("No file found")
 quit()
flag=0
for word in wordList: #print(word)
word_encode = word.encode('utf-8') digest=hashlib.md5(word_encode.strip()).hexdigest() #print("MD5 Digest is "+digest)
if mdhash == digest: print("Match Found")
print("Password Is "+word+" For the Given MD5"+mdhash) flag=1
wordList.close() if flag==0:
print("No Password Found for the given hash")
exit()
```

How to Execute the Program: Save the files in a folder.

Open Command Prompt

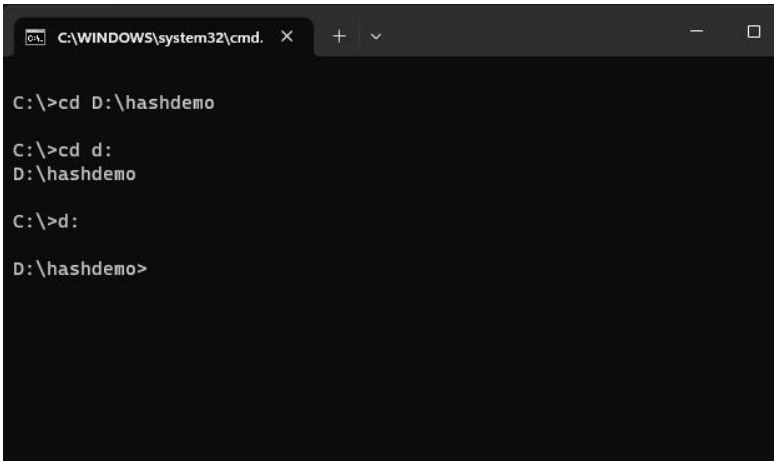


Start > Run > type cmd

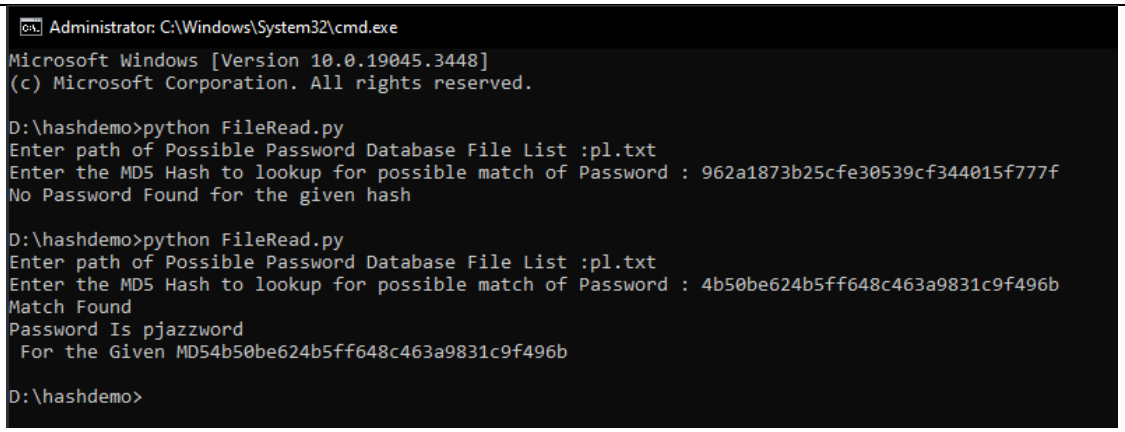


Change the directory to where the files are saved.

You may use the below sequence of command & execute the same



Below is the example on how the program will produce the Output when the Hash is matched and whenthe hash is not matched.



Aim : Using the software tools/commands to perform the following , generate an analysis report :
C. DoS attack.

Description : Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to deny services to intended users. Their purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. For example, if a bank website can handle 10 people a second by clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can log in. DoS attacks exploit various weaknesses in computer network technologies. They may target servers, network routers, or network communication links. They can cause computers and routers to crash and links to bog down. The most famous DoS technique is the Ping of Death. The Ping of Death attack works by generating and sending special network messages (specifically, ICMP packets of non-standard sizes) that cause problems for systems that receive them. In the early days of the Web, this attack could cause unprotected Internet servers to crash quickly. **It is strongly recommended to try all described activities on virtual machines rather than in your working environment.**

Aim : Using the software tools/commands to perform the following , generate an analysis report :
D. ARP poisoning in windows.

Description : ARP or Address Resolution Protocol is one of the most essential protocol layers in the OSI model. whenever a device wants to communicate with any other device in a local area network, our protocol comes into play. ARP protocol lets devices communicate with each other by translating the MAC address of the device with its IP address and vice versa. There are two identifiers to identify devices on a network.
IP addresses (logical addresses) are used to identify devices on a wide-area network (Internet).
MAC addresses (Physical addresses) are used to identify devices on a local area network.

ARP Cache: It is an ARP table or a collection of ARP entries that every network-connected device maintains. ARP Cache is created whenever a device's MAC address is mapped with its local IP address. Devices use the ARP cache to avoid redundant address resolution requests. but this Cache can be poisoned (Using ARP Spoofing) here the term "poisoned" basically means a fake MAC address

associated with an IP address. this leads to the man-in-the-middle attack where data can be intercepted, modified, dropped, or stopped.

ARP Spoofing: ARP Spoofing, also referred to as ARP Cache Poisoning as we discussed earlier. it is a type of malicious attack in which the attacker sends a fake ARP message over a local network in order to link the attacker's MAC address with the IP address of another device on a local area network to achieve a malicious attack. If an attacker can manage the linking of the MAC address of his/her device with the IP address of any other device on a local area network, this linking leads to ARP Poisoning and allows an attacker to carry out several malicious tasks such as intercepting network traffic, modify, and even stop or dropped the data in-transit by putting an attacker in the middle of the communication of the devices (Man In The Middle Attack).

Man-in-the-Middle (MIM) Attack: ARP Spoofing also known as ARP Poisoning is the Man-in-the-Middle (MIM) Attack. In this type of attack, the attacker secretly intercepts and, in some cases, alters the communication between two parties without their knowledge. ARP Spoofing serves as the means to achieve this interception.

- ARP Poisoning: ARP Poisoning is a wider term that contains both ARP Spoofing and ARP Cache Poisoning. It describes any form of malicious manipulation of ARP messages to compromise network security. This manipulation can involve either redirecting network traffic or spying on network communications.
- Packet Sniffing: Packet Sniffing is a passive network monitoring technique where an attacker captures data packets as they travel through the network. ARP Spoofing is often used to facilitate packet sniffing, allowing the attacker to grab sensitive information.

ARP Spoofing can have severe consequences, including:

1. Data Interception: Attackers can intercept sensitive data, such as login credentials or financial information.
2. Data Modification: It can allow attackers to modify data packets in transit, leading to potential data corruption.
3. Denial of Service (DoS): In some cases, ARP Spoofing can disrupt network connectivity for legal users.

Basic terms	ARP Spoofing	ARP Poisoning
Focus	The main focus of ARP Spoofing is to intercept or modify network traffic within a LAN(Local area network)	ARP Poisoning is a wider term that contains both ARP Spoofing and ARP Cache Poisoning.
Outcome	In ARP Spoofing, the attacker sends false ARP messages to mislead devices on the network into associating their MAC address with a legal IP address. This manipulation allows the attacker to intercept or modify data packets intended for the target IP address.	While ARP Poisoning includes ARP Spoofing, it also covers other ARP-related attacks, such as ARP Cache Poisoning. ARP Poisoning can involve either redirecting network traffic or spying on network communications.
purpose	ARP Spoofing is often a component of Man-in-the-Middle (MIM) attacks, where the attacker secretly intercepts and potentially alters the communication between two parties without their knowledge.	ARP Poisoning is used as a general term to describe any form of malicious ARP message manipulation aimed at compromising network security.

Aim : Using the software tools/commands to perform the following , generate an analysis report :
E. Ifconfig,ping,netstat, traceroute.

Output:

Ipconfig command

Lists all the details of the IP configuration of the machine on which the command is execute.
The “ipconfig” displays the current information about your network such as your your IP and MAC address, and the IPaddress of your router. It can also display information about your DHCP and DNS servers

Ipconfig /all gives the details of all the network adapters which are not connected to the network and also of thosewhich are connected to the network.

```
D:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.54.210
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.52.1

D:\>
```

ping:

Allows you to send a signal to another device, and if that device is active, it will send a response back to the sender. The “ping” command is a subset of the ICMP (Internet Control Message Protocol), and it uses what is called an “echorequest”.
So, when you ping a device you send out an echo request, and if the device you pinged is active or online, you get anecho response.

In the below example you can ping either to a website or to an IP which is connected on your

```
D:\>ping google.com

Pinging google.com [142.250.67.174] with 32 bytes of data:
Reply from 142.250.67.174: bytes=32 time=2ms TTL=116
Reply from 142.250.67.174: bytes=32 time=2ms TTL=116
Reply from 142.250.67.174: bytes=32 time=2ms TTL=116
Reply from 142.250.67.174: bytes=32 time=2ms TTL=116

Ping statistics for 142.250.67.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Netstat

Displays all sorts of network statistics when used with its various options.
One of the most interesting variants of netstat is netstat -an , which will display a list of all open

network connectionson their computer, along with the port they're using and the foreign IP address they're connected to

```
D:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1521         L1-08:49696            ESTABLISHED
  TCP    127.0.0.1:1521         L1-08:49965            ESTABLISHED
  TCP    127.0.0.1:49696        L1-08:1521             ESTABLISHED
  TCP    127.0.0.1:49965        L1-08:1521             ESTABLISHED
  TCP    127.0.0.1:53429        L1-08:53430            ESTABLISHED
  TCP    127.0.0.1:53430        L1-08:53429            ESTABLISHED
  TCP    127.0.0.1:53431        L1-08:53432            ESTABLISHED
  TCP    127.0.0.1:53432        L1-08:53431            ESTABLISHED
  TCP    127.0.0.1:53643        L1-08:53644            ESTABLISHED
  TCP    127.0.0.1:53644        L1-08:53643            ESTABLISHED
  TCP    127.0.0.1:53645        L1-08:53646            ESTABLISHED
  TCP    127.0.0.1:53646        L1-08:53645            ESTABLISHED
  TCP    127.0.0.1:55360        L1-08:55361            ESTABLISHED
  TCP    127.0.0.1:55361        L1-08:55360            ESTABLISHED
  TCP    192.168.54.210:52976   52.114.16.78:https     ESTABLISHED
  TCP    192.168.54.210:54084   52.114.16.78:https     ESTABLISHED
  TCP    192.168.54.210:54159   55:https               ESTABLISHED
  TCP    192.168.54.210:54777   192.168.55.75:8009     ESTABLISHED
  TCP    192.168.54.210:54985   20.140.64.69:https     CLOSE_WAIT
  TCP    192.168.54.210:54986   a23-54-82-226:https    CLOSE_WAIT
  TCP    192.168.54.210:54993   13.107.51.254:https    CLOSE_WAIT
  TCP    192.168.54.210:54994   204.79.197.222:https   CLOSE_WAIT
  TCP    192.168.54.210:54996   13.107.6.254:https     CLOSE_WAIT
  TCP    192.168.54.210:54997   13.107.246.68:https    CLOSE_WAIT
  TCP    192.168.54.210:54998   152.195.38.76:http     CLOSE_WAIT
  TCP    192.168.54.210:54999   52.123.129.254:https   CLOSE_WAIT
  TCP    192.168.54.210:55246   52.123.178.16:https    ESTABLISHED
  TCP    192.168.54.210:55270   20.198.118.190:https   ESTABLISHED
  TCP    192.168.54.210:55346   216.24.57.253:https    ESTABLISHED
  TCP    192.168.54.210:55347   216.24.57.253:https    ESTABLISHED
  TCP    192.168.54.210:55353   NMITD-SERVER1:5057     ESTABLISHED
  TCP    192.168.54.210:55354   NMITD-SERVER1:5057     ESTABLISHED
  TCP    192.168.54.210:55355   NMITD-SERVER1:5057     ESTABLISHED
  TCP    192.168.54.210:55356   NMITD-SERVER1:5057     ESTABLISHED
  TCP    192.168.54.210:55357   NMITD-SERVER1:5057     ESTABLISHED
  TCP    192.168.54.210:55358   NMITD-SERVER1:5057     ESTABLISHED
  TCP    192.168.54.210:55359   13.89.179.10:https     ESTABLISHED
  TCP    192.168.54.210:55364   ec2-3-7-50-164:http    ESTABLISHED

D:\>
```

Aim : Using the software tools/commands to perform the following , generate an analysis report :
F. Steganography tools.

Description :

A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. It comes from the Greek words steganos, which means "covered" or "hidden," and graph, which means "to write." Hence, "hidden writing."

You can use steganography to hide text, video, images, or even audio data. It's a helpful bit of knowledge, limited only by the type of medium and the author's imagination.

Different Types of Steganography

1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image − A stego image is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

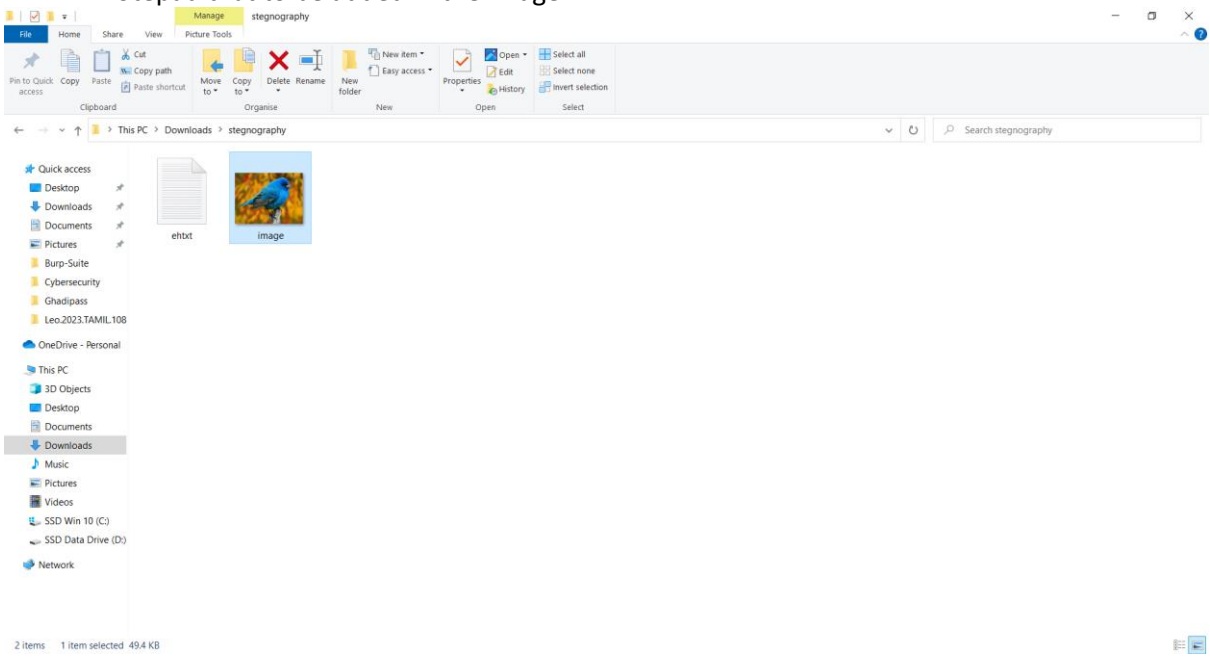
4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography − It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

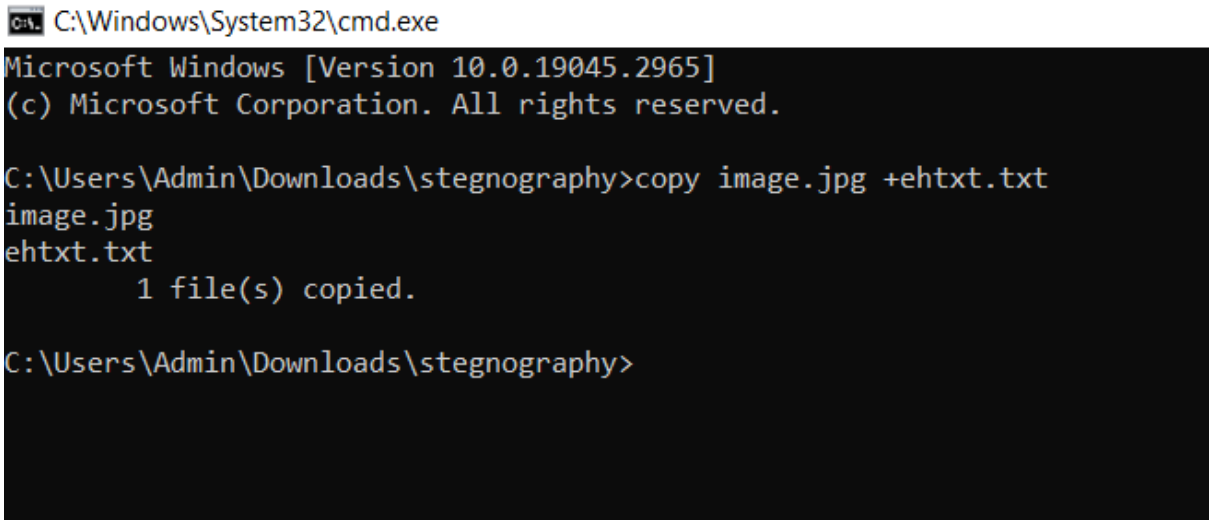
Output:

Steps:

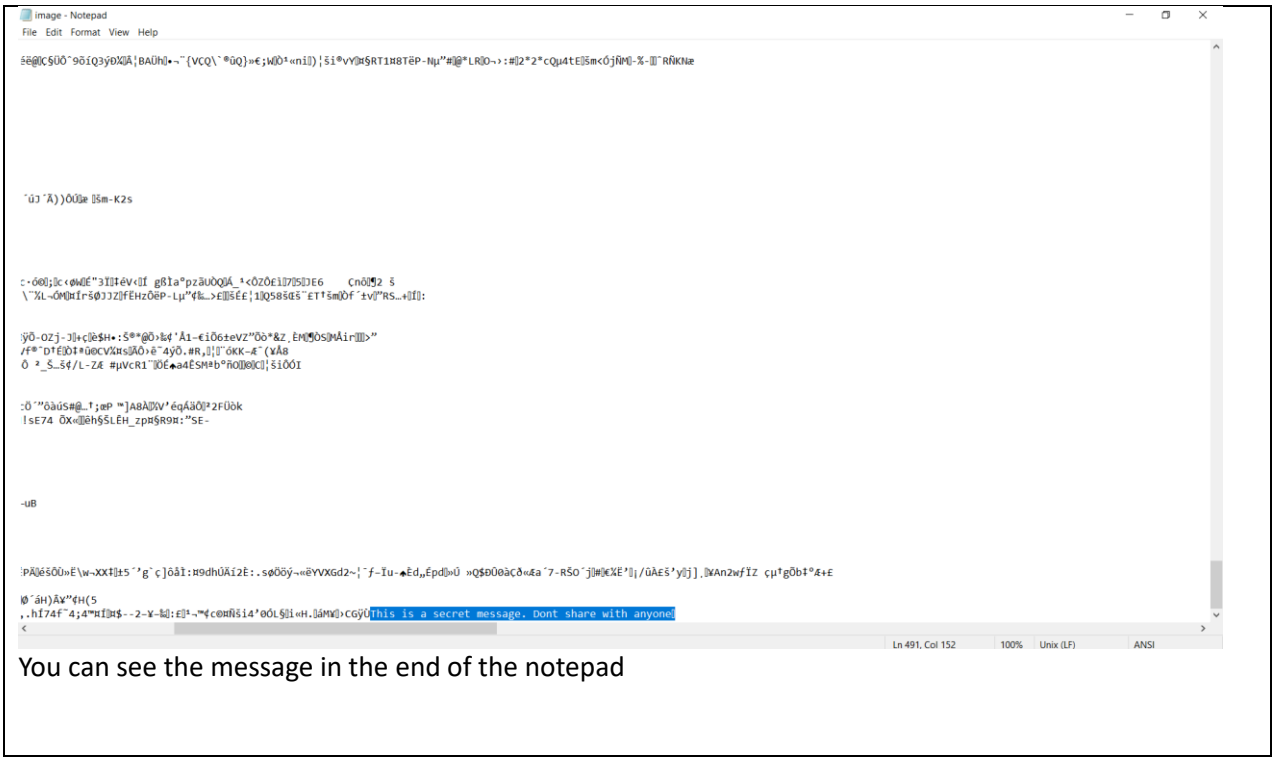
1. Download an image and then create a text file in the same folder. Enter the message in the notepad that to be added in the Image.



2. Open the cmd in the same folder and then enter the command given below



3. Once successfully copied open the image file in notepad



You can see the message in the end of the notepad

Practical 4. Developing and implementing malwares ::

Aim : Developing and implementing malwares

A. Creating a simple keylogger in python.

Description : Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware. Working: Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983. 1. Software key-loggers : Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1. JavaScript based key logger – It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.

2. Form Based Key loggers – These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers : These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

1. USB keylogger – There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.

2. Smartphone sensors – Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

Output:

Aim : Developing and implementing malwares

B. Creating a virus.

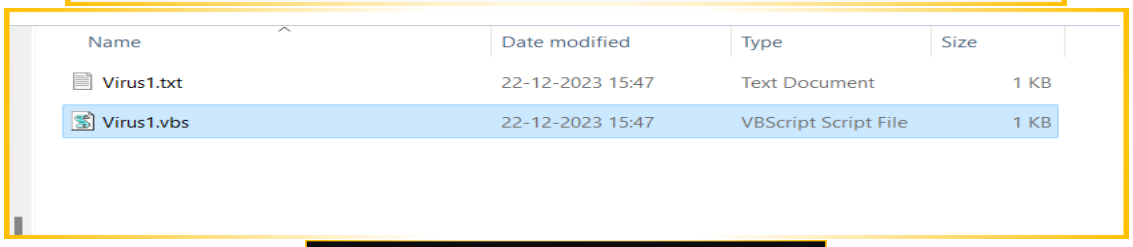
Description :

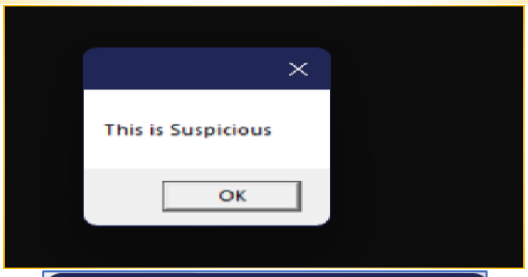
A virus is a program that can infect other programs by modifying them. The modification includes a copy of the virus program which then goes on to infect other programs. Virus are self-replicating and can wreak havoc in a system by modifying or destroying files and causing system crashing and program malfunction.

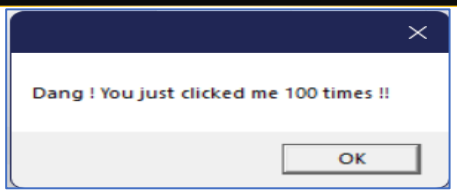
Output:

File Edit View

```
set x = wscript.CreateObject("wscript.shell")
   dim a : a = 100
   For i = 0 to a step 1
   wscript.sleep 50
   MsgBox("This is Suspicious")
next
MsgBox("Dang ! You just clicked me 100 times !!")
wscript.Quit
```



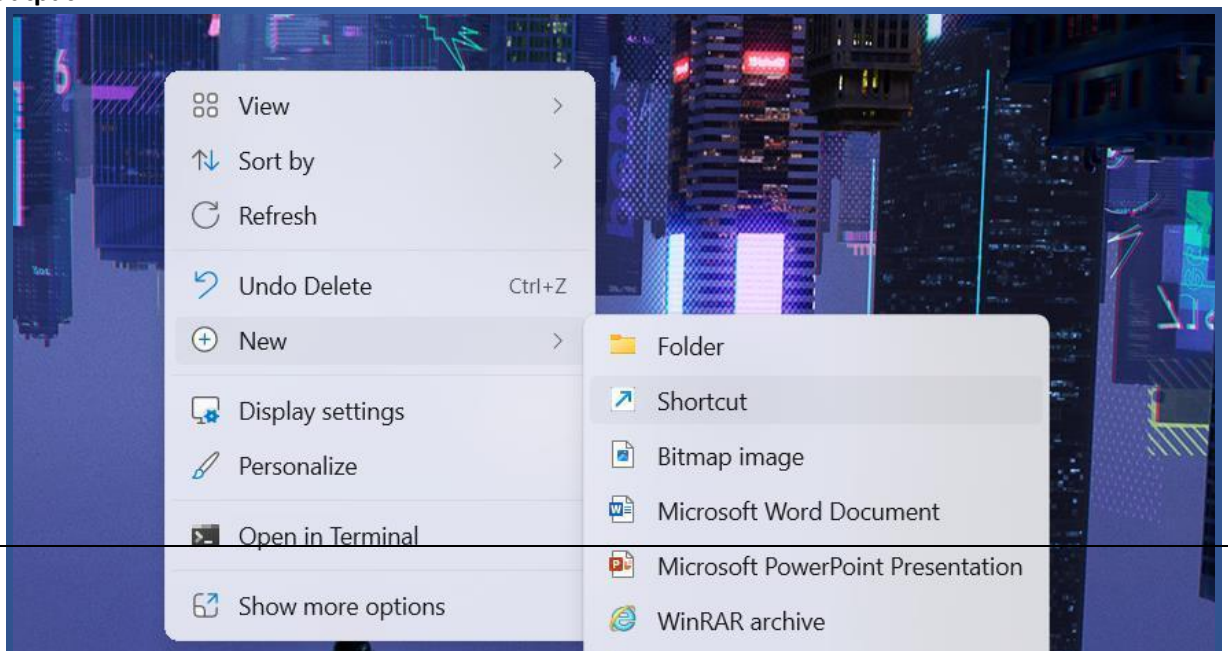


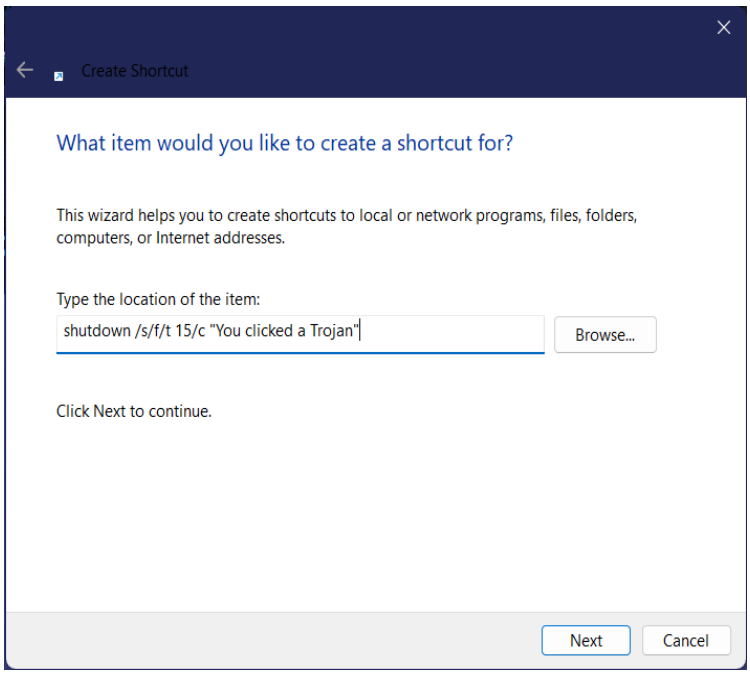


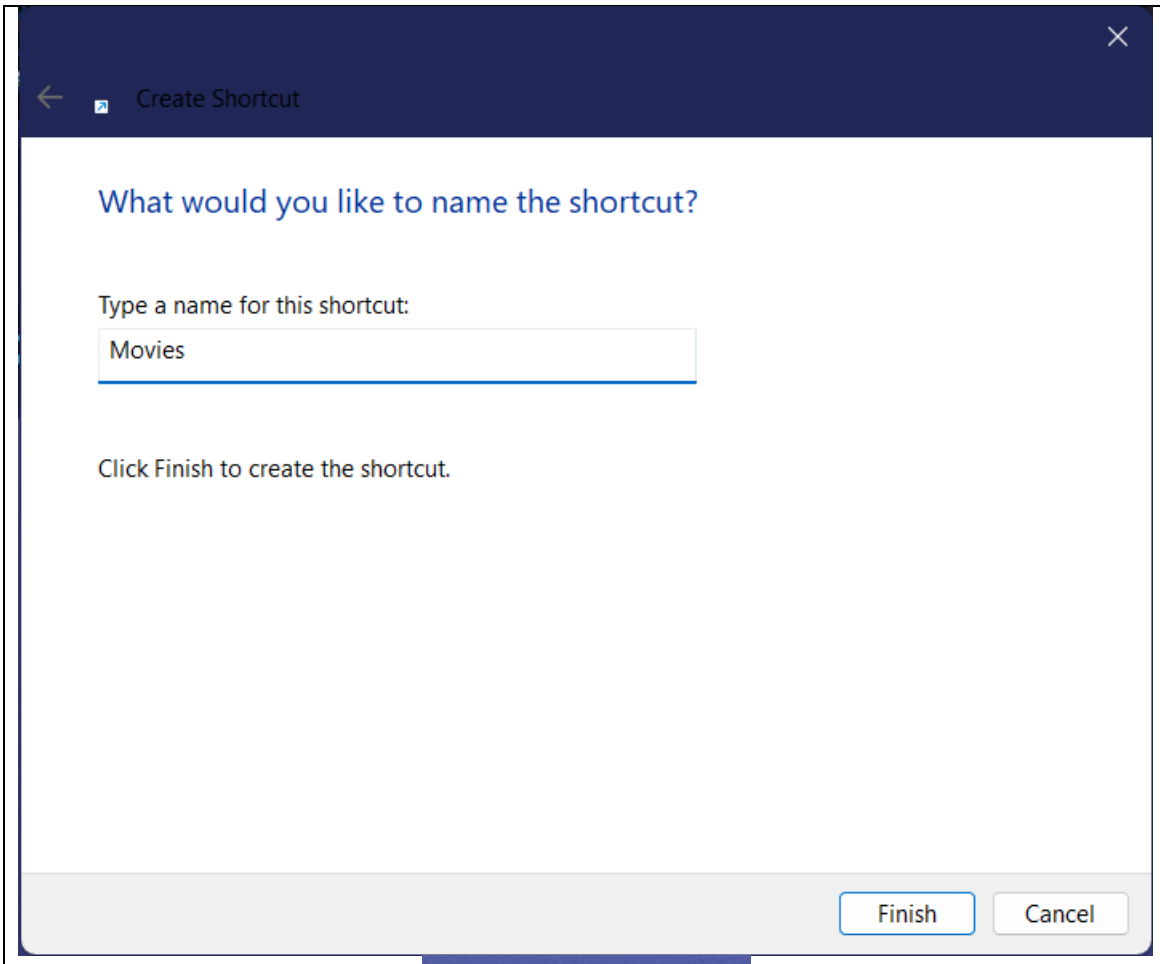
Aim : Developing and implementing malwares
C. Creating a trojan.

Description : The name of the **Trojan Horse** is taken from a classical story of the Trojan War. It is a code that is malicious in nature and has the capacity to take control of the computer. It is designed to steal, damage, or do some harmful actions on the computer. It tries to deceive the user to load and execute the files on the device. After it executes, this allows cybercriminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more.

Output:




Create Shortcut
What item would you like to create a shortcut for?
This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.
Type the location of the item:
shutdown /s/f/t 15/c "You clicked a Trojan"
Browse...
Click Next to continue.
Next
Cancel


Create Shortcut
What would you like to name the shortcut?
Type a name for this shortcut:
Movies
Click Finish to create the shortcut.
Finish
Cancel


Movies

Practical 5. Hacking web servers, web applications:

Aim : Hacking web servers, web applications:

A. Hack a website by Remote File Inclusion

Description : Remote File Inclusion (RFI) is a type of vulnerability most often found on the suited PHP running web portals be on the web and the Local File Inclusion (LFI) is similar to RFI, the only difference is that in LFI, the attacker has been uploading the malicious scripts types.

Remote File Inclusion (RFI) is a type of vulnerability found in PHP running websites or web servers. The RFI is enabling an attacker to include the remotely hosting file however through scripting on the website servers and vulnerability occurring due to usage of its user-supplied user input without final validations through it.

The remote file inclusion (RFI) is the attacker's targeted code for the malware attack in website server applications that reference outer external scripts. The perpetrator's aim is to exploit the reference function in an application to upload malware(i.e. as backdoor shells) from a remote URL located within a different domain as RFI vulnerability exists in a website or web application, an attacker can include malicious external files that run by website or website applications

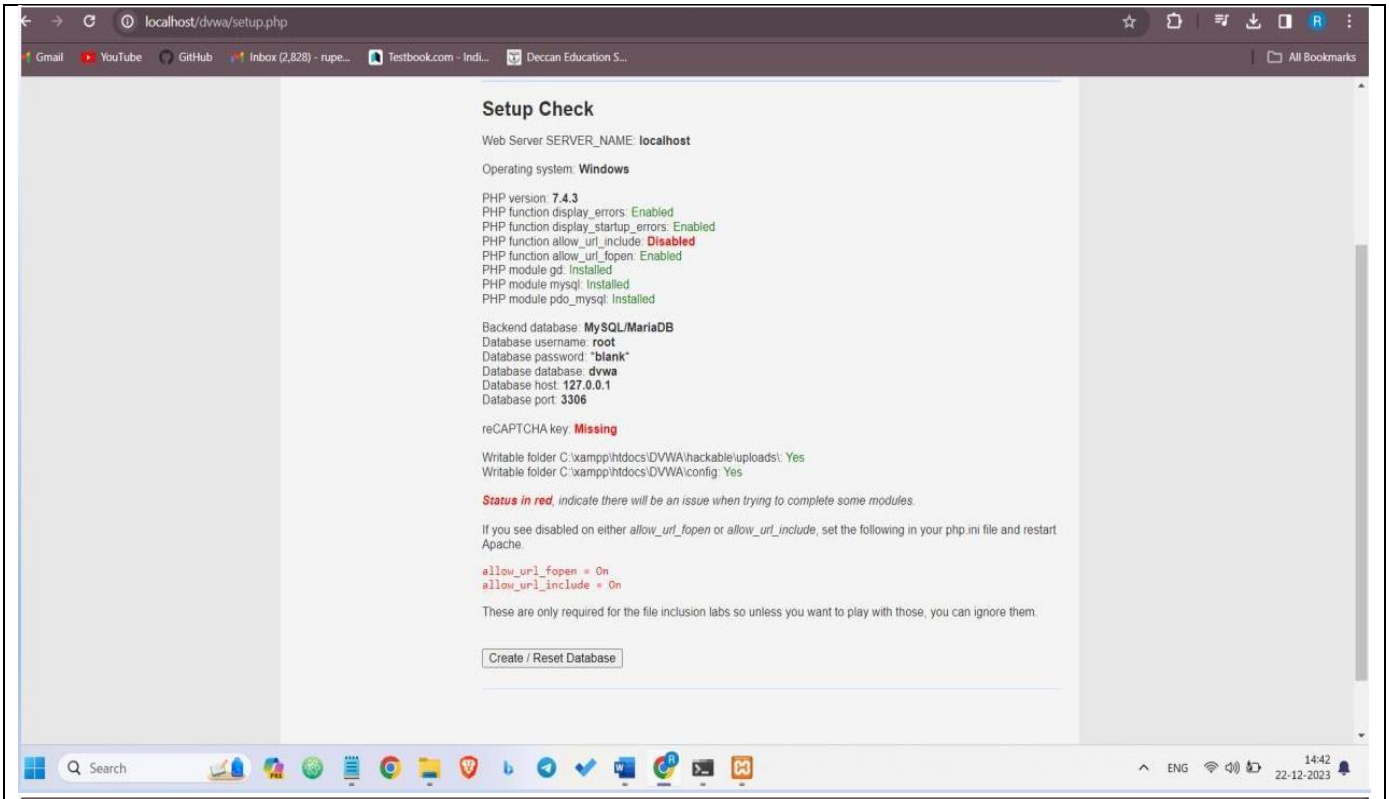
In RFI attacks, third party hackers employ scripting to include likewise remotely hosting files on the web portals. In an LFI attack, a hacker used to target local files to execute the malicious harmful scripts

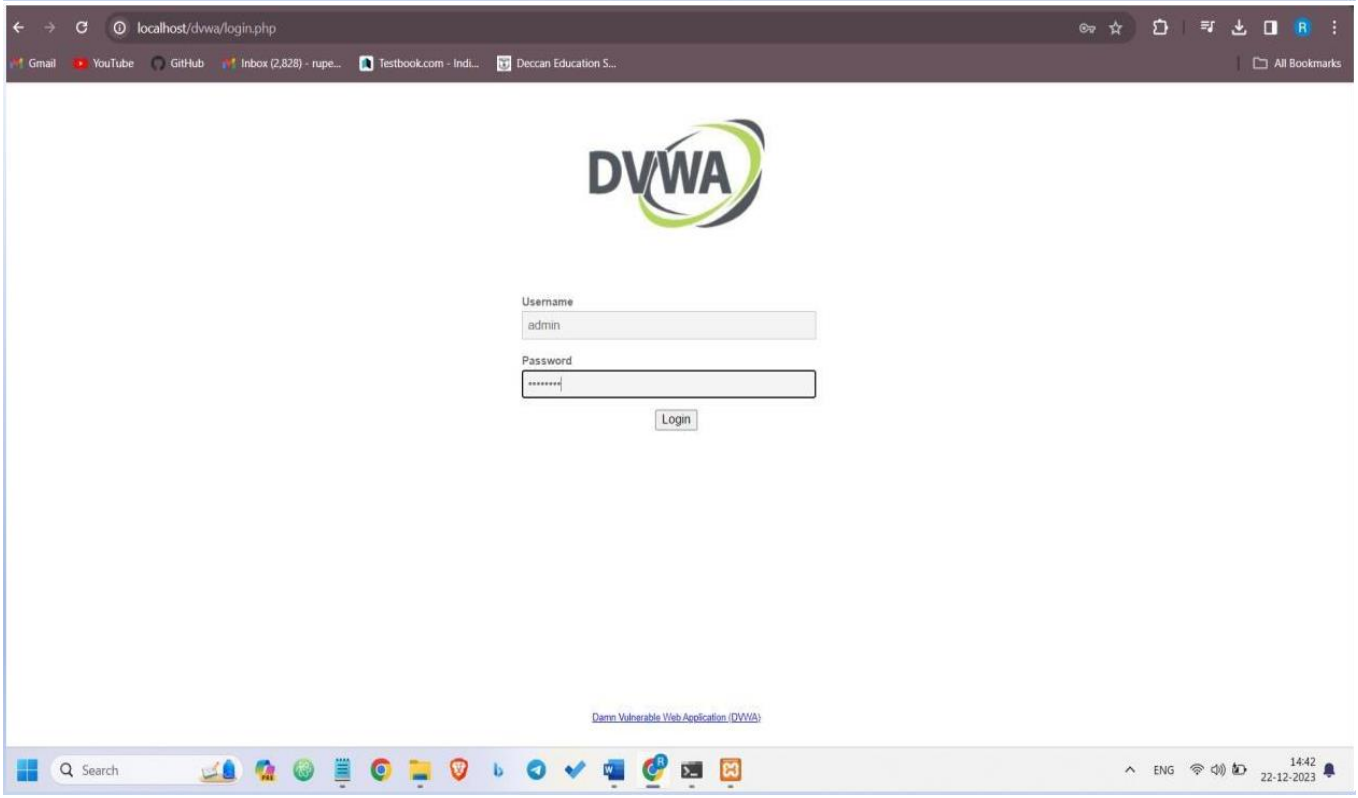
In Remote File Inclusion RFI attacks, hackers take the merits of the "dynamic file including" commands that are in such website/ web portal applications to send malicious external files or scripts to it. When website applications allow user input, such as URL, parameters passing value, etc. and passing to the "file including" steps without having proper validation on it, thus harmful perpetrators can be excluding the website's browsing application to include remote files with harmful scripts, LFI detects the harmful threats like actors using a local file that is stored on the target server, RFI attack, they using the file from external server resources.

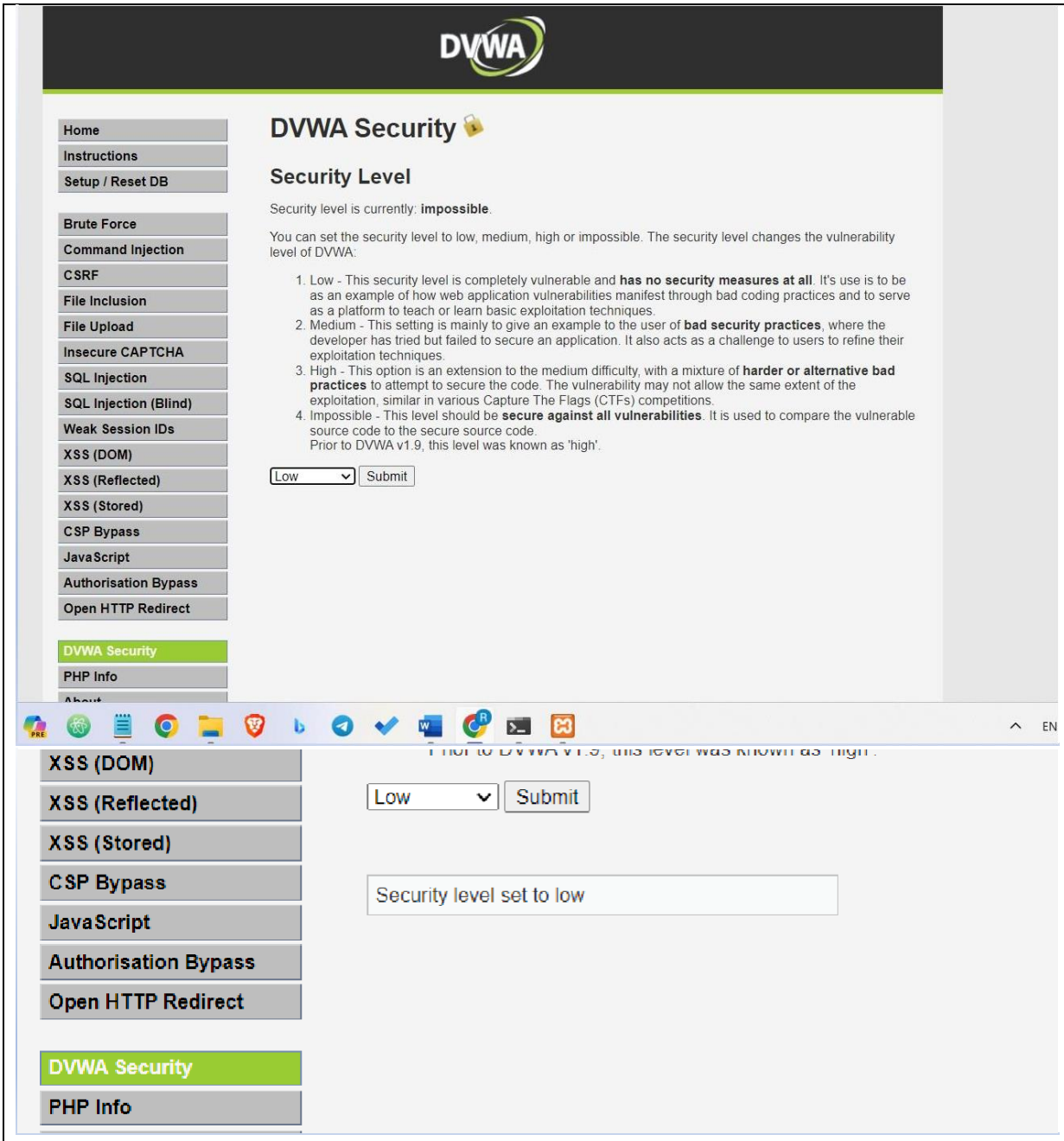
This malicious malware file execution of attacks can be done with Blacklisting as well as Code fixing within it.

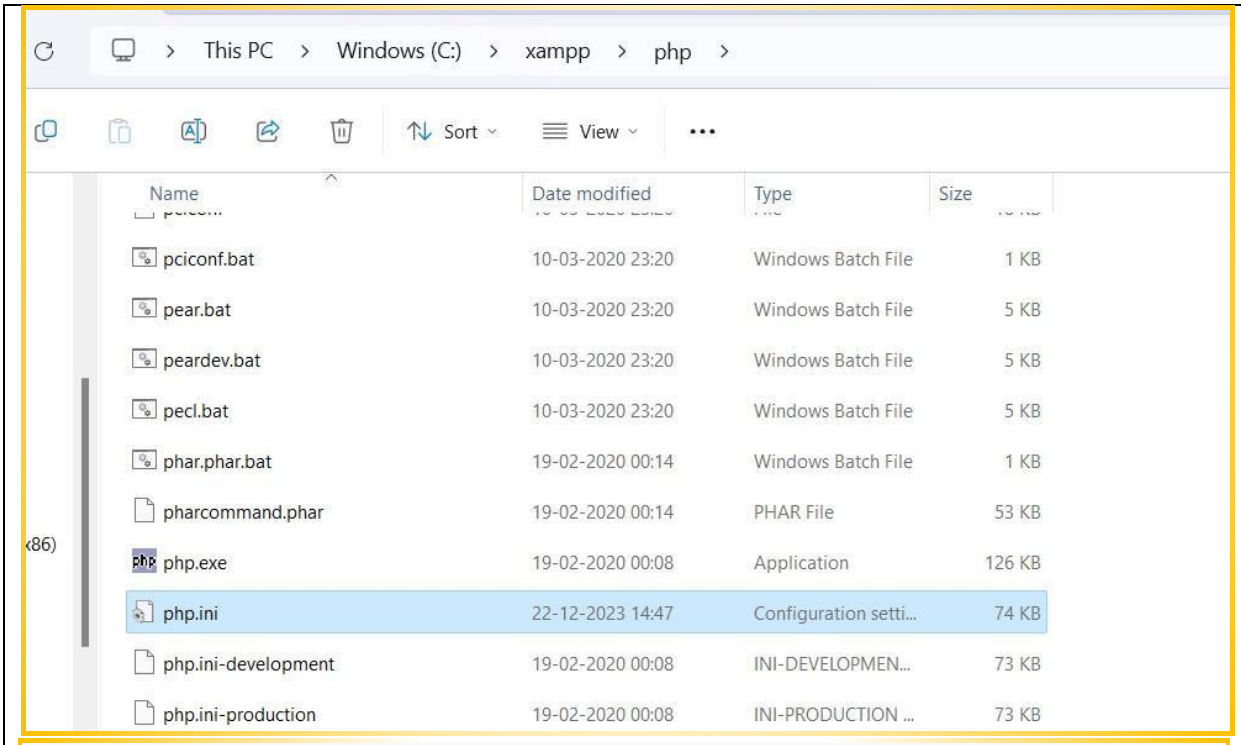
1. The perpetrator can be executing malicious code from an external source instead of accessing a file on the local web servers, as is the case with an LFI attack
2. The goal is to exploit the insecurity of local files uploaded on functions that fail to validate user-supplied/controlled inputs

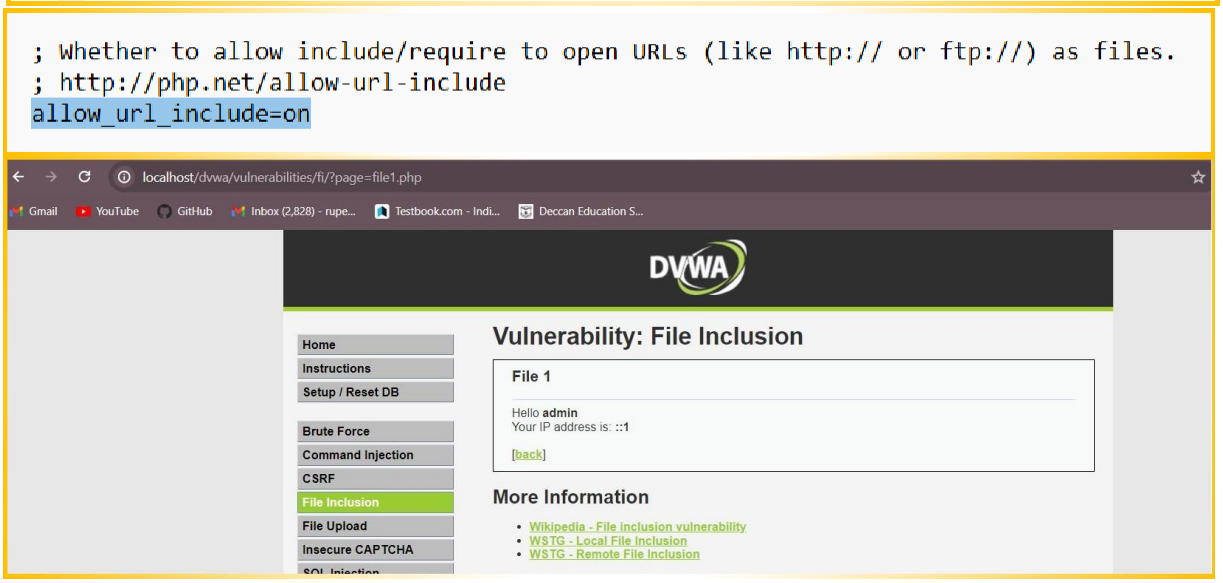
Output:


localhost/dvwa/setup.php
Gmail
YouTube
GitHub
Inbox (2,828) - rupe...
Testbook.com - Indi...
Deccan Education S...
All Bookmarks
Setup Check
Web Server SERVER_NAME: localhost
Operating system: Windows
PHP version: 7.4.3
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Backend database: MySQL/MariaDB
Database username: root
Database password: "blank"
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
Writable folder C:\xampp\htdocs\DVWA\hackable\uploads\: Yes
Writable folder C:\xampp\htdocs\DVWA\config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
Create / Reset Database
Search
ENG
14:42
22-12-2023


localhost/dvwa/login.php
Gmail
YouTube
GitHub
Inbox (2,828) - rupe...
Testbook.com - Indi...
Deccan Education S...
All Bookmarks
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)
Search
ENG
14:42
22-12-2023


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
DVWA Security
Security Level
Security level is currently: impossible.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve 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'.
Low
Submit
EN
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
Low
Submit
Security level set to low





Aim : B. Disguise as Google Bot to view Hidden Content of a Website

Description : A Bot or internet bot or web robot in technology is a software application that does certain automated tasks. They run on their scripts and don't require a human user to start them. Generally, bots perform that tasks are simple and repetitive but can be also used for complex tasks. The bot is automated that's why they have much faster execution than that of a person.

Type of Bots :

Bots can be chatbots, web crawlers, social bots, malicious bots, etc.

Chatbots –

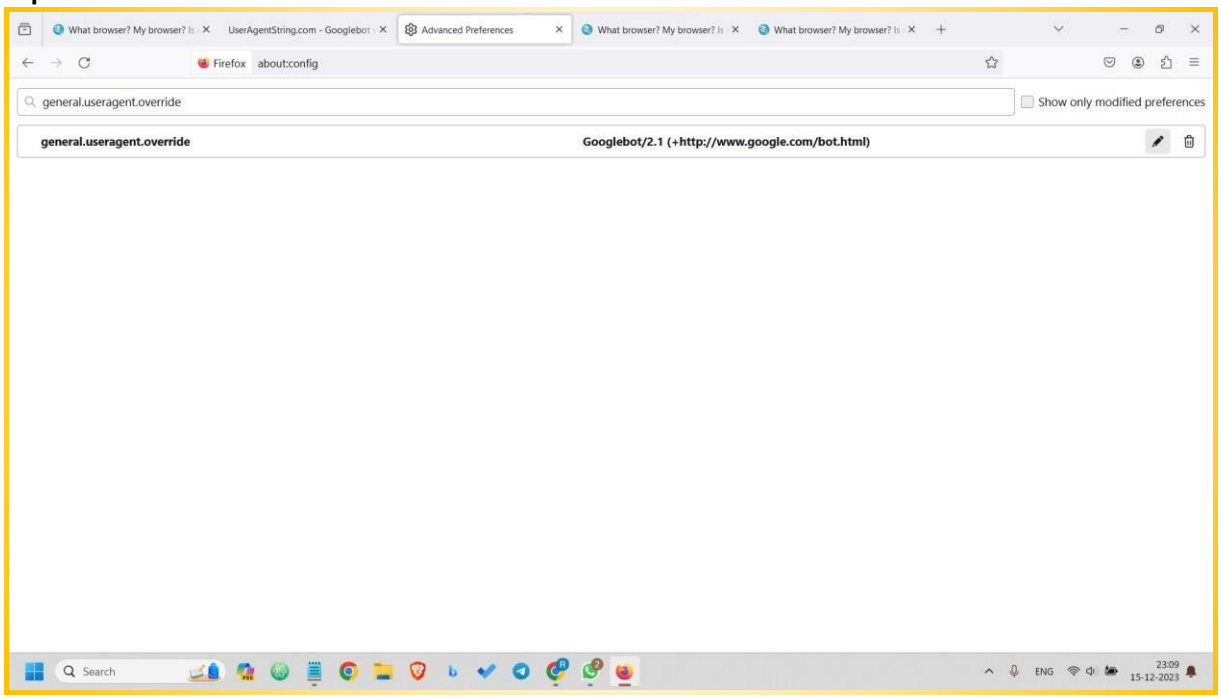
A chatbot is a bot used in the chat conversation. These bots replace humans and show human behavior. The earliest chatbot Eliza was programmed in 1964 and answered some very simple decision tree questions. Today there are a number of Chatbots present. For e.g. – Siri, Google Assistant, Alexa, Cortana, etc. These chatbots are highly AI (Artificial Intelligence) programmed chatbots that can do much more complex tasks than simple ones. They are there for making our life a little easier. They take care of you by reminding you to take an umbrella if it's going to rain or to remind someone's birthday. From showing booked tickets to pending bills or maybe chatting with customer care also.

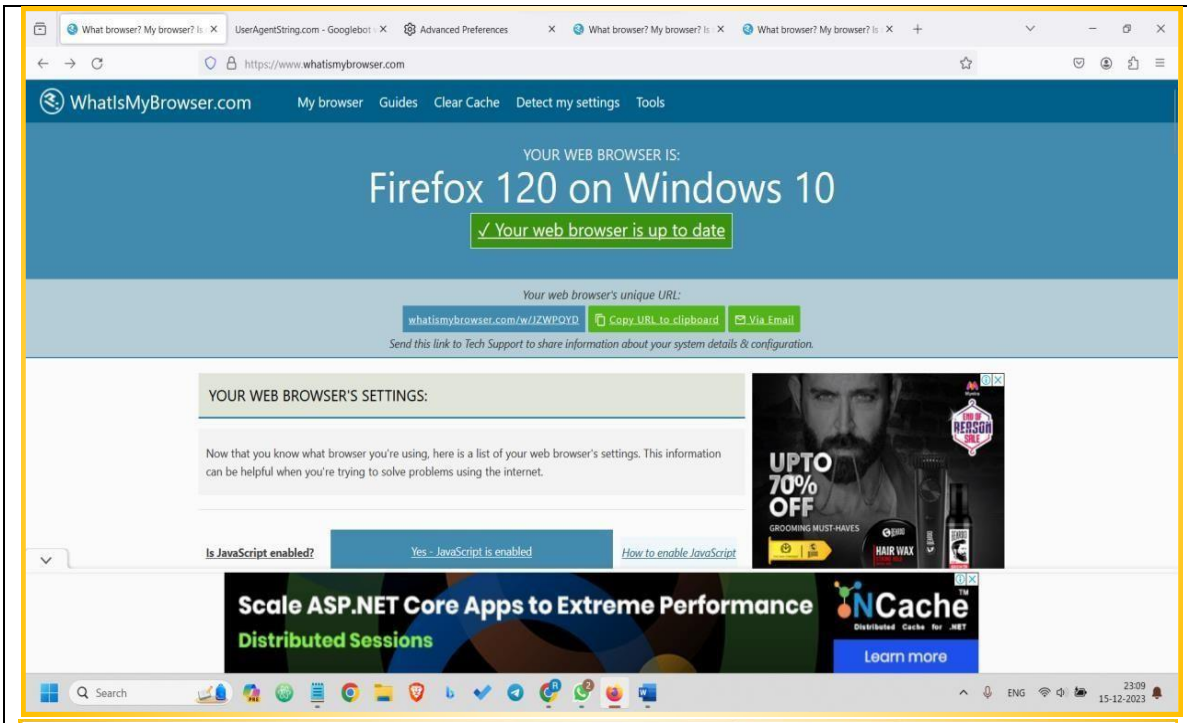
Web crawlers –
Web crawlers or also called web spiders. These are the bots that scan the webpages all over the internet and browse the web for indexing webpages and the content in that webpages. They are also used in data mining. Google is most known for its web crawler Googlebot. There are many web crawlers present such as- Baidu Spider, GoogleBot, Scraper, WebHarvy, Alexa Crawler, Yandex Bot, etc. Bots are mostly used in web crawling. Roughly more than half of web traffic is due to bots. All bots work on some input from the user and respond accordingly. They typically search for keywords or any data for responding with an accurate and precise output.

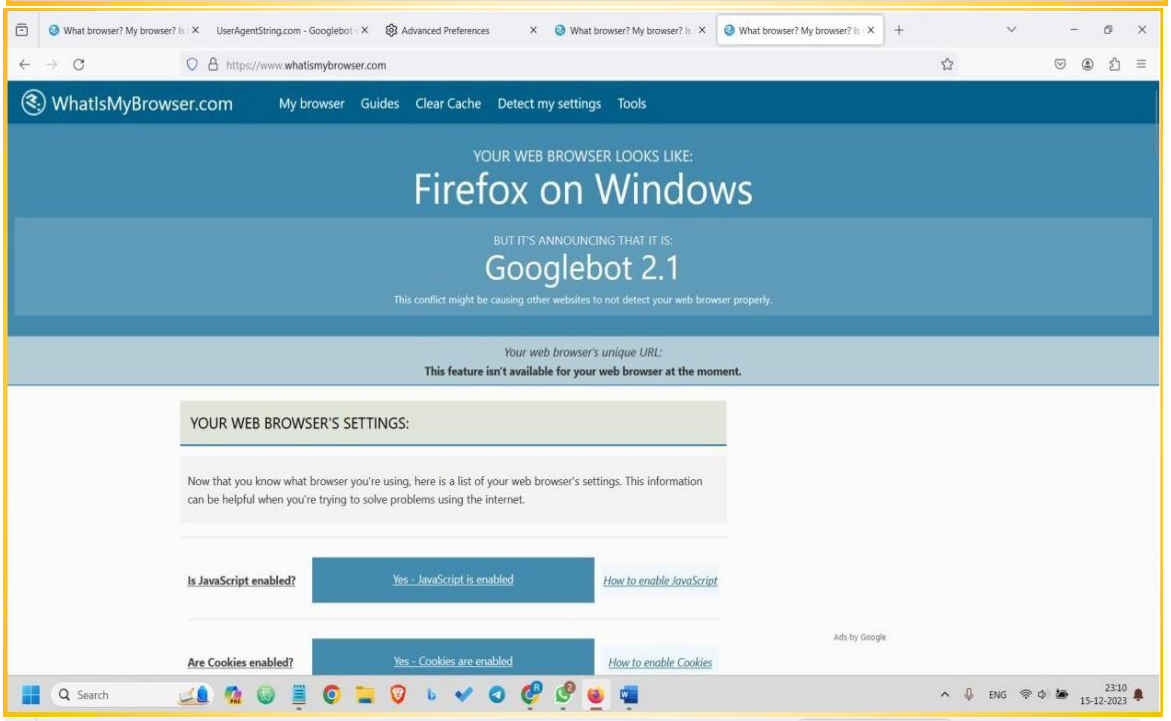
Social bots –
These are the bots that are present in social media sites but unlike chatbots, their tasks are simple, following someone or some page on social media or taking polls or influencing, etc. They can be used to work on a large scale without requiring much effort.

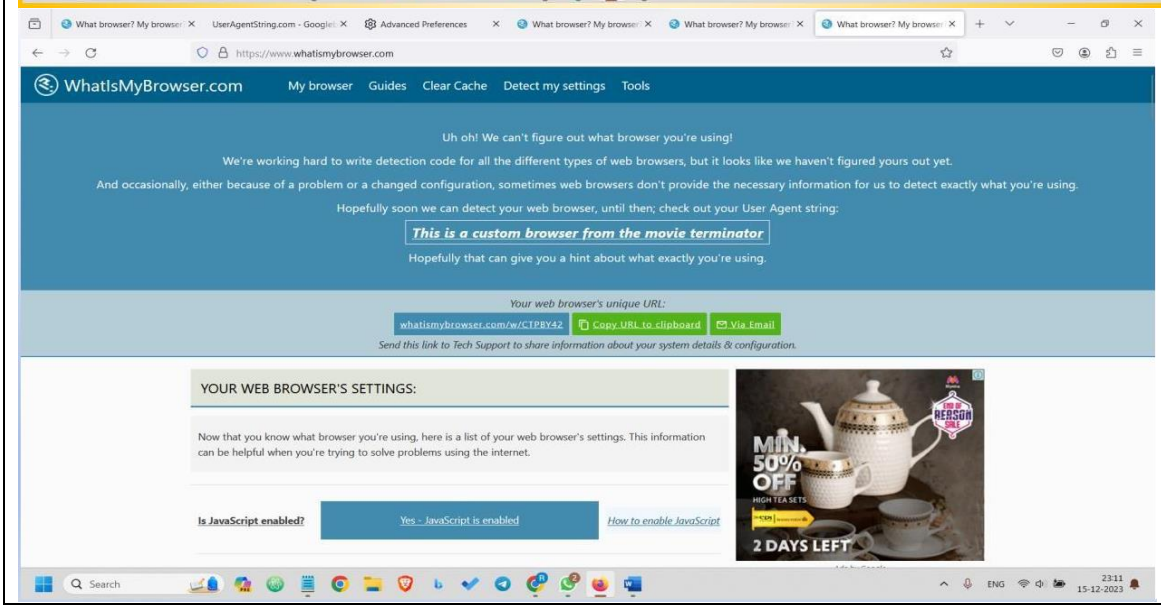
Malicious bots –
There are a number of bots present which are present in many forms and can steal user data or hack social media accounts, spread fake news, can make someone popular or damage someone's reputation, or can infect the user system by unknowingly downloading files in the user system or by any means.

Output:




WhatIsMyBrowser.com
My browser Guides Clear Cache Detect my settings Tools
YOUR WEB BROWSER IS:
Firefox 120 on Windows 10
✓ Your web browser is up to date
Your web browser's unique URL:
whatismybrowser.com/w/IZWPOYD
Copy URL to clipboard
Via Email
Send this link to Tech Support to share information about your system details & configuration.
YOUR WEB BROWSER'S SETTINGS:
Now that you know what browser you're using, here is a list of your web browser's settings. This information can be helpful when you're trying to solve problems using the internet.
Is JavaScript enabled?
Yes - JavaScript is enabled
How to enable JavaScript
UPTO 70% OFF
GROOMING MUST-HAVES
HAIR WAX
Scale ASP.NET Core Apps to Extreme Performance
Distributed Sessions
NCache
Learn more


WhatIsMyBrowser.com
My browser Guides Clear Cache Detect my settings Tools
YOUR WEB BROWSER LOOKS LIKE:
Firefox on Windows
BUT IT'S ANNOUNCING THAT IT IS:
Googlebot 2.1
This conflict might be causing other websites to not detect your web browser properly.
Your web browser's unique URL:
This feature isn't available for your web browser at the moment.
YOUR WEB BROWSER'S SETTINGS:
Now that you know what browser you're using, here is a list of your web browser's settings. This information can be helpful when you're trying to solve problems using the internet.
Is JavaScript enabled?
Yes - JavaScript is enabled
How to enable JavaScript
Are Cookies enabled?
Yes - Cookies are enabled
How to enable Cookies
Ads by Google


WhatIsMyBrowser.com
My browser Guides Clear Cache Detect my settings Tools
Uh oh! We can't figure out what browser you're using!
We're working hard to write detection code for all the different types of web browsers, but it looks like we haven't figured yours out yet.
And occasionally, either because of a problem or a changed configuration, sometimes web browsers don't provide the necessary information for us to detect exactly what you're using.
Hopefully soon we can detect your web browser, until then; check out your User Agent string:
This is a custom browser from the movie terminator
Hopefully that can give you a hint about what exactly you're using.
Your web browser's unique URL:
whatismybrowser.com/w/CTPBY42
Copy URL to clipboard
Via Email
Send this link to Tech Support to share information about your system details & configuration.
YOUR WEB BROWSER'S SETTINGS:
Now that you know what browser you're using, here is a list of your web browser's settings. This information can be helpful when you're trying to solve problems using the internet.
Is JavaScript enabled?
Yes - JavaScript is enabled
How to enable JavaScript
MIN. 50% OFF
HIGH TEA SETS
2 DAYS LEFT

Aim : C. How to use Kaspersky for Lifetime without Patch.

Description :

Quick Start Guide

Read this Quick Start Guide to get started with Kaspersky Endpoint Security Cloud. The Guide contains tips for managing the accounts of your users and installing security applications on their devices.

Quick start scenario

After you complete the scenario, the devices in your organization will be protected. The scenario proceeds in stages:

1. **Create an account.**

   To start using Kaspersky Endpoint Security Cloud, you need an account on Kaspersky Business Hub.

   To create an account:

   1. Open your browser and enter the following URL: https://cloud.kaspersky.com.
   2. Click the **Create an account** button.
   3. Follow the onscreen instructions.

2. **Create a workspace.**

   After you create the account, you can create your first workspace. We recommend that you first create one test workspace, connect your own devices to it, and then test any modifications to the settings, noting the results.

   We recommend that you create a separate workspace for each company that you manage, even if a company has only a few users. By doing this, you will be able to do the following:

   1. Change settings for each company individually.
   2. Keep track of the license count, and the increase or decrease of the number of users in the company.
   3. Assign administrator rights to a user within the company, who can access only that company's workspace.

   To create a company workspace:

   4. Open your browser and enter the following URL: https://cloud.kaspersky.com.

5. Click the **Sign in** button.

6. Follow the onscreen instructions.

3. **Perform initial setup of Kaspersky Endpoint Security Cloud.**

   After you create a company workspace, you must perform initial setup of Kaspersky Endpoint Security Cloud. The initial setup begins automatically when you start Kaspersky Endpoint Security Cloud Management Console for the first time.
   The **Welcome to Kaspersky Endpoint Security Cloud** window is displayed. Follow the onscreen instructions.

   When initial setup is complete, Kaspersky Endpoint Security Cloud Management Console is ready to use.

4. **Deploy security applications on your users' devices.**

   When your first workspace is prepared, follow the main setup steps provided in the **Information panel** → **Getting started** section. These steps include adding user accounts, connecting devices to Kaspersky Endpoint Security Cloud, and creating a certificate for iOS devices.

   These steps are divided into three groups:

   1. **Preconfigured**

      You already took these steps when you created the workspace.

   2. **Required**

      You must take this step to start protection of the devices.

      Add users by providing their email addresses. An invitation is sent to the email address and it contains the download link to the security application. When the user clicks the link, Kaspersky Endpoint Security Cloud recognizes the device operating system, thus ensuring that the proper software is downloaded.

      As an alternative, you can simultaneously protect multiple devices that are running Windows. To do this, you can deploy security applications by using a Group Policy script.

   3. **Recommended**

      We recommend that you take these steps to enhance the protection of devices.

      1. Once the software has been downloaded and installed on the device of the user, assign the user as the device owner.

      2. Create an Apple Push Notification service (APNs) certificate. The APNs certificate is created in one run. You must follow the steps for its creation without interruption, because the signing process has a time stamp that will expire if the creation process takes too long.

5. **Manage protection.**

After the security application is installed on a device, the device is assigned the **Default** security profile. This is the security profile with the default settings that are recommended by Kaspersky experts.

In the **Security management** → **Security profiles** section, you can create different security profiles. Every new security profile holds the default settings until you modify them. You can also copy existing security profiles.

Each security profile holds four tabs for the respective platforms: Windows, macOS, Android, and iOS.

When you assign a security profile to a user, the security profile is applied to all devices owned by the user. Only the **Default** security profile can be applied to devices without owners.

When creating a security profile, take into consideration the organizational structure of the company that you manage. For example, the security profile for a developer may differ from the one used for a sales representative or a human resources assistant. Name each security profile accordingly.

We recommend that you prevent users from modifying or deleting the security applications installed on their devices. Therefore, define the following settings:

1. For Windows devices, do the following:
    1. On the **Windows** → **Advanced** → **Interaction with end users** tab, make sure that **Password protection** is enabled.
    2. Select the operations that a user will be allowed to perform only with the password.
2. For Mac devices, do the following:
    1. On the **Mac** → **Advanced** → **Interaction with end users** tab, choose whether you want the Kaspersky Endpoint Security for Mac application icon visible on the menu bar or not.
    2. On each device in system preferences, use the macOS account type settings (admin or standard user) and the "lock" icon () to prevent the user from removing the software.
3. For Android devices, do the following:
    1. On the **Android** → **Security settings** tab, make sure that **Screen lock** is enabled to protect the device from unauthorized access.
    2. On the **Advanced** tab, make sure that Kaspersky Endpoint Security for Android cannot be removed.

4. For iOS devices: on the **iOS** → **Security settings** tab, make sure that **Screen lock** is enabled to protect the device from unauthorized access.

After defining the required settings of security profiles, you can assign security profiles to the intended users.

6. **Specify licenses.**

After you have created a workspace, you are granted a 30-day trial license that is embedded in your workspace. To continue using Kaspersky Endpoint Security Cloud after the trial license expires, you must purchase a commercial license or a subscription. Click **Information panel** → **License**, and then enter the activation code.

The activation code will be distributed automatically to the security applications, which may take 15 minutes, as the applications attempt to sync with the workspace every 15 minutes.

7. **Define other settings (optional).**

You can define other optional settings.

1. By default,

   background scan

   is enabled for devices running Windows. Autorun objects, system memory, and the system partition are scanned when the device is idling for five or more minutes. If you want, you can click the **Settings** tab and set the schedule for the malware scan. From the **Devices** tab, you can start the malware scan task.

2. The security applications mostly use the Kaspersky Security Network cloud service in their operation and to a lesser extent the application's anti-malware databases. If you want, you can click the **Settings** tab and set the schedule for the anti-malware database update. On the **Devices** tab, you can start the anti-malware database update task.

3. On the **Settings** tab, you can configure which event notifications you want to view in your events overview.

   The information about events is not aggregated. Each event is sent in a separate email message. If you want to configure the delivery of event notifications, be ready to receive a large number of email messages.

4. On the **Distribution packages** tab, you can download the software directly and prepare new software when it is available. The newly prepared software will then be distributed to newly invited users.

Practical 6. SQL injection and Session hijacking :

Aim : SQL injection and Session hijacking :
A. SQL injection for website hacking,

Description : SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

Look at the following example which creates a `SELECT` statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

SQL Injection Based on 1=1 is Always True

Output:

Aim : B. Session hijacking.

Description : TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Different ways of session hijacking :

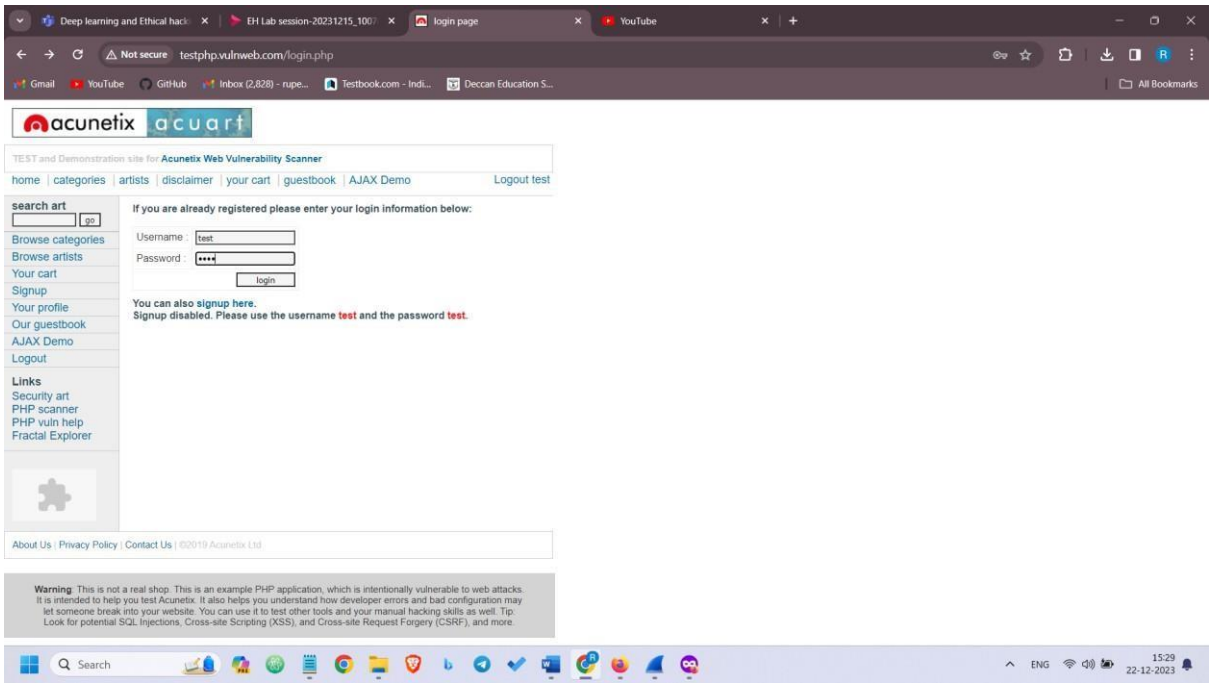
There are many ways to do Session Hijacking. Some of them are given below –

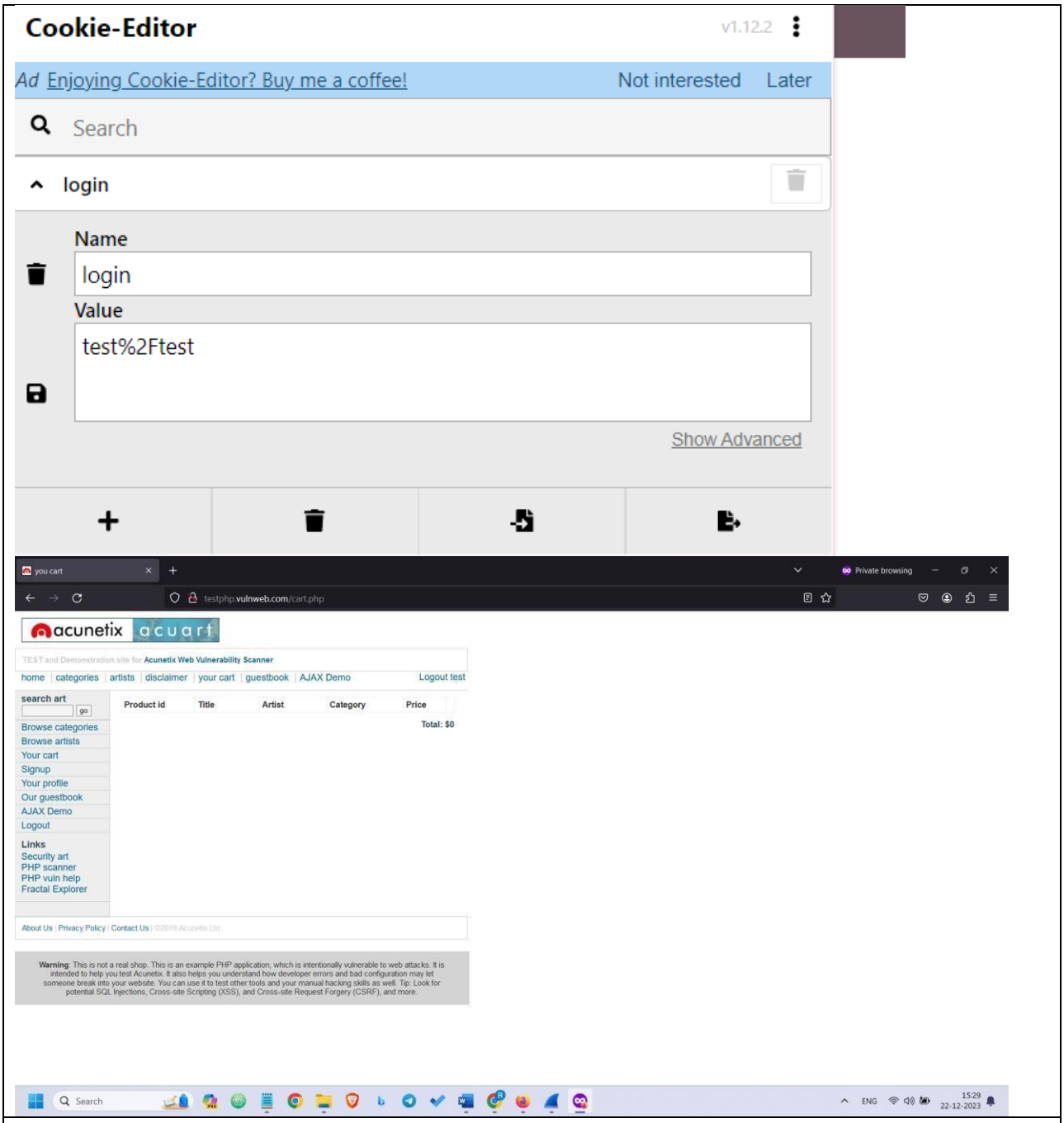
Cross Site Scripting(XSS Attack)

Attacker can also capture victim's Session ID using XSS attack by using javascript. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

- **IP Spoofing**
  Spoofing is pretending to be someone else. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host. In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.
- **Blind Attack**
  If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Output:




Cookie-Editor
v1.12.2
Ad Enjoying Cookie-Editor? Buy me a coffee!
Not interested
Later
Search
login
Name
login
Value
test%2Ftest
Show Advanced
you cart
Private browsing
testphp.vulnweb.com/cart.php
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Product id
Title
Artist
Category
Price
Total: $0
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.
Search
ENG
15:29
22-12-2023

Practical 7. Wireless network hacking, cloud computing security, cryptography :

Aim : Wireless network hacking, cloud computing security, cryptography :
1 .Using Cryptool to encrypt and decrypt password,

Description : Cryptool is an open-source and freeware program that can be used in various aspects of cryptographic and cryptanalytic concepts. There are no other programs like it available over the internet where you can analyze the encryption and decryption of various algorithms. This tools provides graphical interface, better documentation to achieve the encryption and decryption, bundles of analytic tools, and several algorithms.

What is Cryptool?

- A freeware program with graphical user interface (GUI).
- A tool for applying and analyzing cryptographic algorithms.
- With extensive online help, it's understandable without deep crypto knowledge.
- Contains nearly all state-of-the-art crypto algorithms.
- “Playful” introduction to modern and classical cryptography.
- Not a “hacker" tool.

Aim : 2. Implement encryption and decryption using Ceaser Cipher.

- **Description :** The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”.
- The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
- Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
  The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

- For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.
- Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:

1. Write down the plaintext message: HELLO
2. Choose a shift value. In this case, we will use a shift of 3.
3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

H becomes K (shift 3 from H)

E becomes H (shift 3 from E)

L becomes O (shift 3 from L)

L becomes O (shift 3 from L)

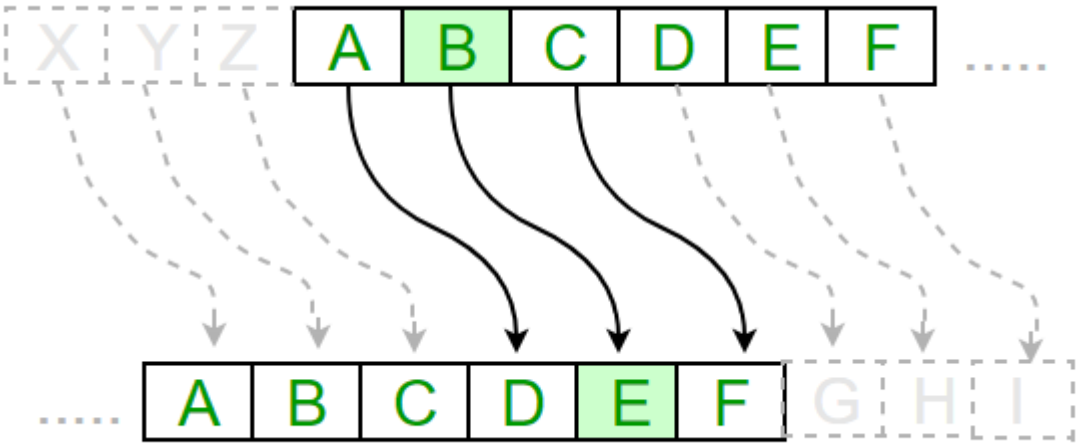
O becomes R (shift 3 from O)

4.The encrypted message is now “KHOOR”.

- To decrypt the message, you simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “KHOOR” back by 3 positions to get the original message, “HELLO”.

(Encryption Phase with shift n)

(Decryption Phase with shift n)



Examples :

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI

Output: **Encryption and Decryption of Caesar Cipher**

Here, we will implement an encryption and decryption of Caesar Cipher, which is actually a substitution method of cryptography. The Caesar Cipher involves replacing each letter of the alphabet with a letter – placed down or up according to the key given.

To start with the process you have to move to the Encrypt/Decrypt tab of the program. There, you will find Symmetric (Classic) tab - Choose Caesar Cipher. For further information, you can get guided by the image below.

Figure1: Encrypt/Decrypt of Cryptool

In encryption, we are replacing the plaintext letter with the 3rd letter of the alphabet that is if “A” is our plaintext character, then the Ciphertext will be “D”.

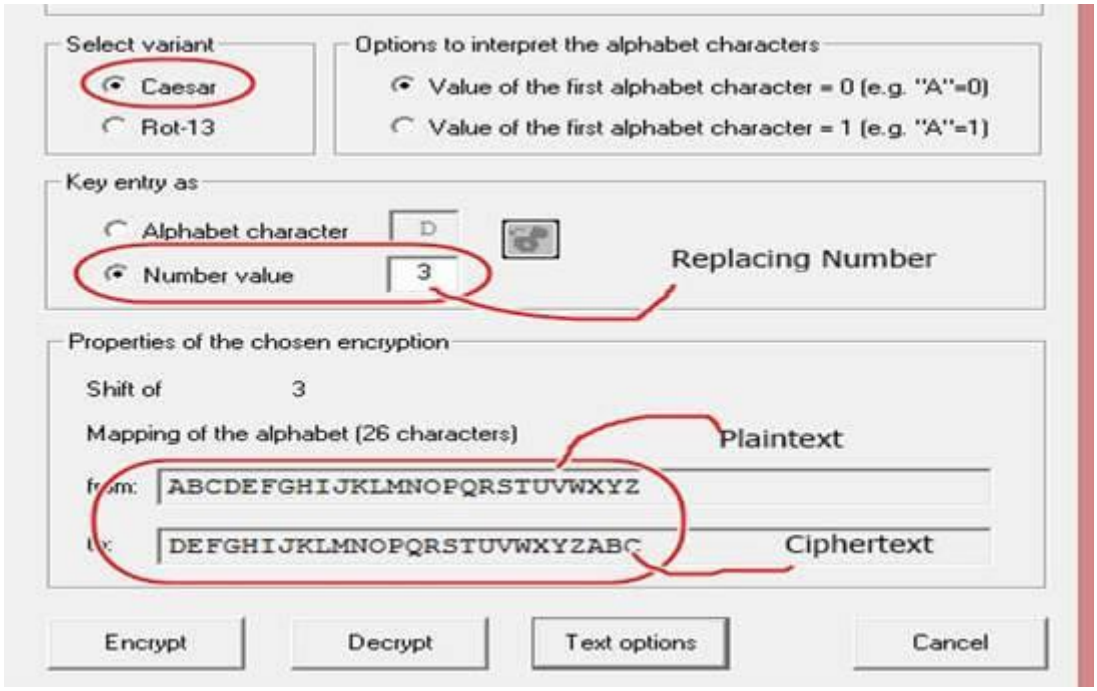


Figure2: Caesar Cipher

So, if I give “Monarchy” as plaintext in Caesar Cipher, it will show me the encryption, as shown in the below image.

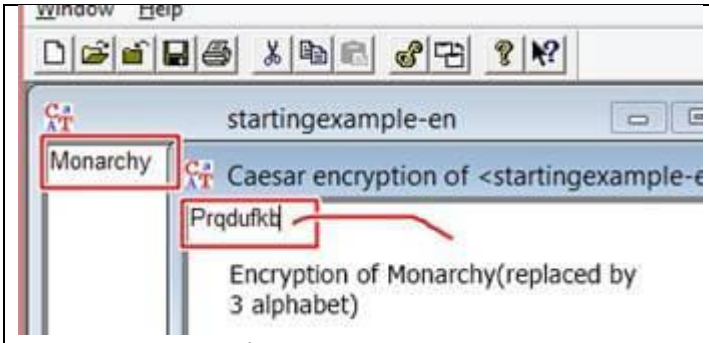


Figure3: Caesar Cipher Encryption

Encryption and Decryption of Playfair

Again, we have to move to Encrypt/Decrypt - Symmetric - Playfair Cipher and perform the encryption part. We are putting the same plaintext – MONARCHY.

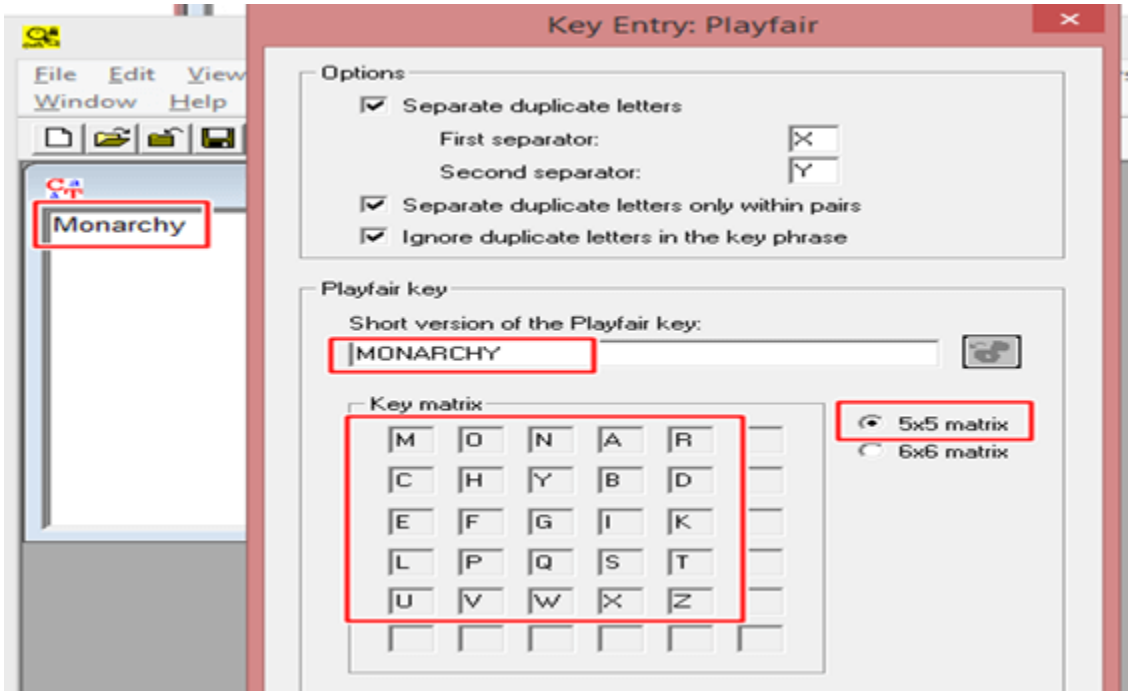


Figure4: Playfair Cipher

So, when we press the encrypt button, we will get the Ciphertext – "ONARMDYB".

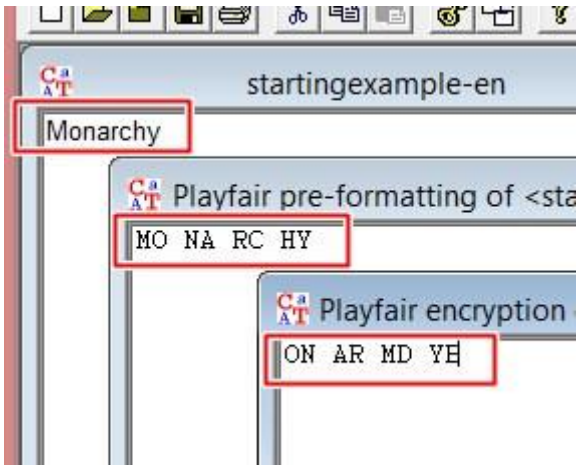


Figure5: Playfair Encryption

Encryption and Decryption of Hill Cipher

Again, we have to move to Encrypt/Decrypt - Symmetric - Hill Cipher and perform the encryption part. We are putting the plaintext as – DRGREERROCKS and assuming that the program gives us the Ciphertext as – FZIFTOTBXGPO.

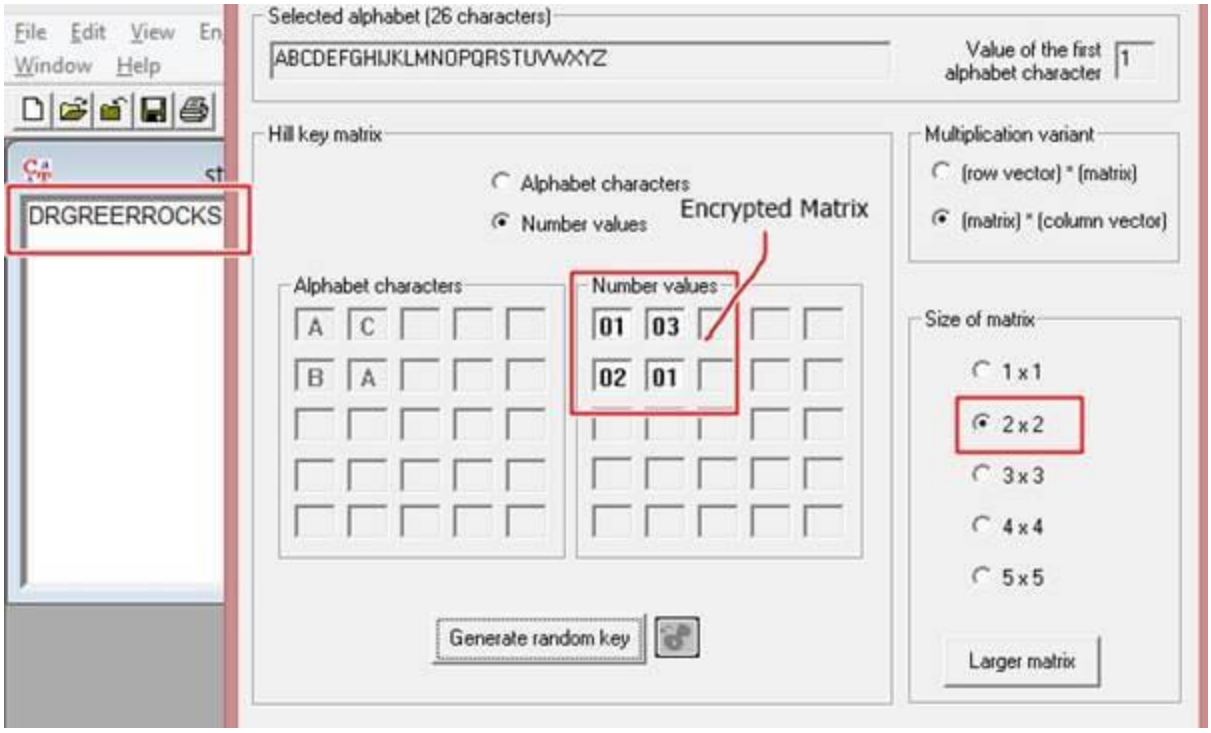


Figure6: Hill Cipher

So, when we press the encrypt button, we will get the Ciphertext – "FZIFTOTBXGPO".

Figure7: Hill Cipher Encryption

Encryption and Decryption of Vigener Cipher

Again, we have to move to Encrypt/Decrypt - Symmetric - Vigener Cipher and perform the encryption part. We are putting the plaintext as – MICHIGANTECHNOLOGICALUNIVERSITY and assuming that the program gives us the Ciphertext as – TWWNPZOAAS…..,with the help of key as – HOUGHTON.

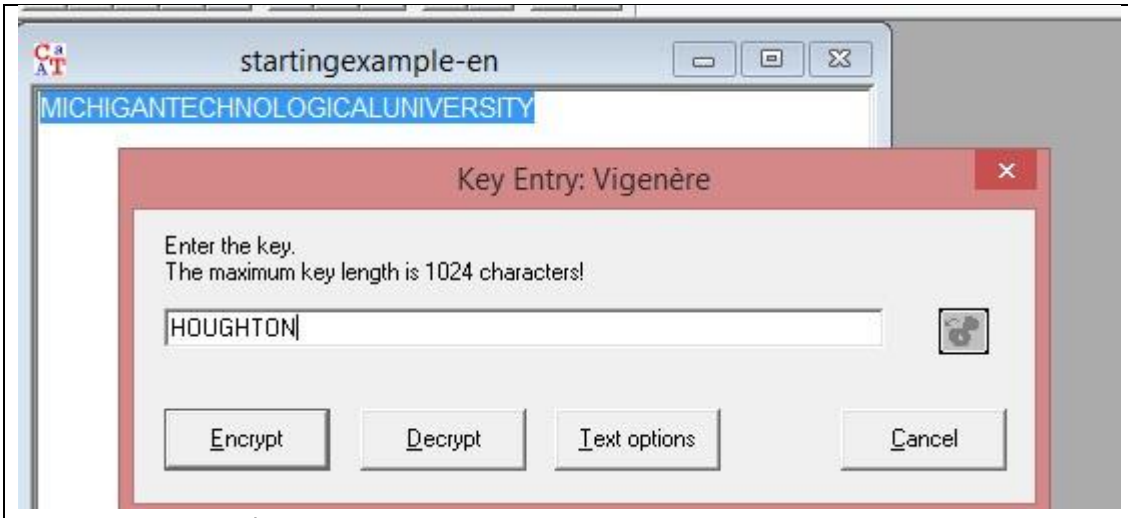


Figure8: Vigener Cipher

So, when we press the encrypt button, we will get the Ciphertext somewhat like – "TWWNPZOAASWNUHZBNWWGSNBVCSLYPMM".

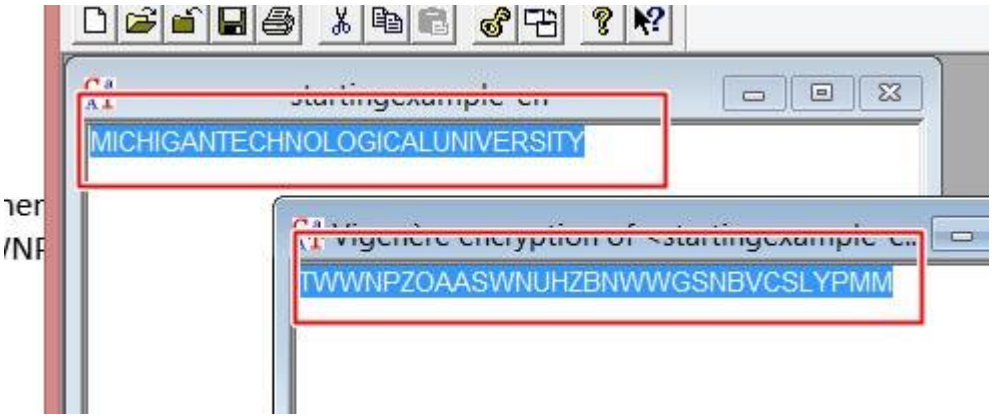


Figure9: Vigener Cipher Encryption

Encryption and Decryption of Railfence Cipher

Again, we have to move to Encrypt/Decrypt - Symmetric - Railfence Cipher and perform the encryption part. We are putting the plaintext as – UNBREAKABLE and assuming that the program gives us the Ciphertext as – UEBNRAALBKE.....,with the help of key as – 3.

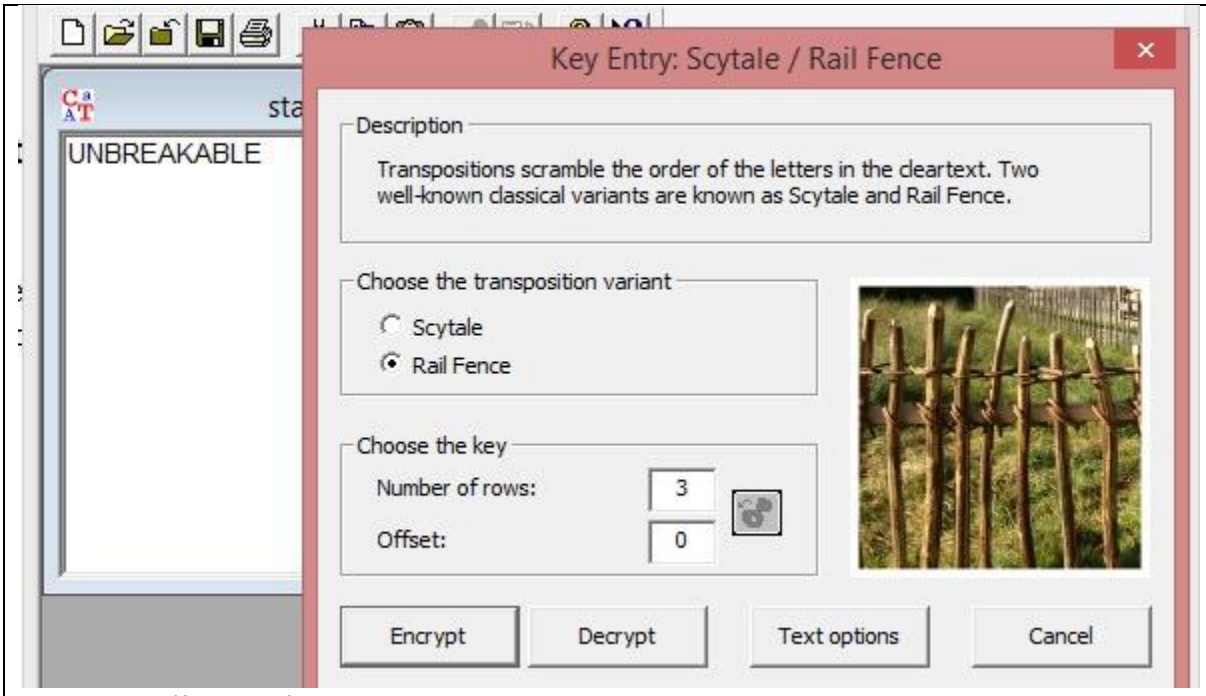


Figure10: Railfence Cipher

So, when we press the encrypt button, we will get the Ciphertext like – "UEBNRAALBKE".

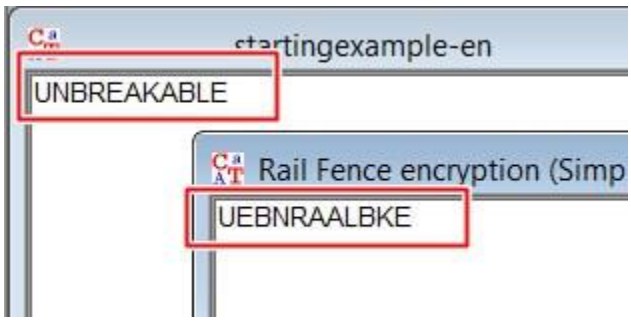


Figure11: Railfence Cipher Encryption

Practical 8. Pen testing

im : Penetration Testing using Metasploit and metasploitable

escription : Metasploit Framework is a powerful open-source penetration testing amework. You get to know all the information about penetration testing, IDS signature, nd software vulnerabilities. It allows the execution and development of the exploit code gainst a remote target tool. Metasploit is not illegal itself, but it depends on what you use for.

Major keywords in the Metasploit framework

The **module** is a software application in the Metasploit framework that carries out tasks like exploiting and scanning and the targets.

They are the key components of the framework and are broken down into 7 types below:

1. Exploits
2. Payloads
3. Auxiliaries
4. Encoders
5. Evasions
6. Nops
7. Post

Payloads are the simple scripts that are often used in module **exploits** by taking advantage of the system's vulnerabilities. **Auxiliary** modules are the only modules that are not exploited. Several interesting features allow them to do more than just exploiting.

Output: Updating the Metasploit is always a good idea. It is recommended to check this weekly.

```
└─# sudo apt update -y; sudo apt install metasploit-framework -y
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Packages [199 kB]
Fetched 18.0 MB in 1min 33s (194 kB/s)
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
```

Fig.1

Launch the Metasploit console like this.

Fig.2

ou can always seek help in the console.

Fig.3

ou can search for modules based on your target.

nsf6 > **search cisco**

nformation gathering is also an important task of ethical hacking and penetration esting. Several tools seamlessly integrate with Metasploit like Nmap. Let's test using map.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -A localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-30 01:31 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
|   3072 90:92:b8:7a:93:ac:d7:e1:e8:87:19:77:8b:dd:3a:75 (RSA)
|   256 b7:70:4c:38:e0:cf:98:d6:ba:2d:c9:a9:cb:5e:43:92 (ECDSA)
|_  256 14:ea:cf:c1:60:20:e3:32:e9:4e:e8:f3:a7:ac:45:bd (ED25519)
80/tcp open  http    Apache httpd 2.4.46 ((Debian))
|_http-server-header: Apache/2.4.46 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.00 seconds
```

Fig.4

map allows you to scan a host to identify it and to find out the services it is providing. You ave now an option to choose from the Exploit Database or search for modules n Metasploit with this information. Scan your local Kali instance, check that it enabled the SH server.

```
msf6 > search linux

Matching Modules

#    Name                                                  Disclosure Date  Rank       Check  Description
-    ----                                                  ---------------  ----       -----  -----------
0    exploit/linux/local/abrt_raceabrt_priv_esc            2015-04-14       excellent  Yes    ABRT raceabrt Privilege Escalation
1    exploit/linux/local/abrt_sosreport_priv_esc           2015-11-23       excellent  Yes    ABRT sosreport Privilege Escalation
2    exploit/linux/local/af_packet_chocobo_root_priv_esc   2016-08-12       good       Yes    AF_PACKET chocobo_root Privilege Escalation
3    exploit/linux/local/af_packet_packet_set_ring_priv_esc 2017-03-29      good       Yes    AF_PACKET packet_set_ring Privilege Escalation
4    exploit/linux/local/apt_package_manager_persistence   1999-03-09       excellent  No     APT Package Manager Persistence
5    exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent  No     ASUS infosvr Auth Bypass Command Execution
6    exploit/linux/http/atutor_filemanager_traversal       2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal / Remote Code Execution
7    exploit/multi/http/atutor_upload_traversal            2019-05-17       excellent  Yes    ATutor 2.2.4 - Directory Traversal / Remote Code Execution,
8    exploit/linux/misc/accellion_fta_mpipe2               2011-02-07       excellent  No     Accellion FTA MPIPE2 Command Execution
9    exploit/linux/http/accellion_fta_getstatus_oauth      2015-07-10       excellent  Yes    Accellion FTA getStatus verify_oauth_token Command Execution
10   exploit/multi/http/apache_activemq_upload_jsp         2016-06-01       excellent  No     ActiveMQ web shell upload
11   exploit/linux/local/asan_suid_executable_priv_esc     2016-02-17       excellent  Yes    AddressSanitizer (ASan) SUID Executable Privilege Escalation
12   exploit/multi/http/coldfusion_rds_auth_bypass         2013-08-08       great      Yes    Adobe ColdFusion RDS Authentication Bypass
13   exploit/linux/browser/adobe_flashplayer_aslaunch      2008-12-17       good       No     Adobe Flash Player ActionScript Launch Command Execution Vulne
```

```
msf6 > search ssh

Matching Modules

#    Name                                                  Disclosure Date  Rank    Check  Description
-    ----                                                  ---------------  ----    -----  -----------
0    auxiliary/admin/http/cisco_7937g_ssh_privesc          2020-06-02       normal  No     Cisco 7937G SSH Privilege Escalation
1    auxiliary/dos/cisco/cisco_7937g_dos                   2020-06-02       normal  No     Cisco 7937G Denial-of-Service Attack
2    auxiliary/dos/windows/ssh/sysax_sshd_kexchange        2013-03-17       normal  No     Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
3    auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                              normal  No     SSH Key Exchange Init Corruption
4    auxiliary/fuzzers/ssh/ssh_version_15                                   normal  No     SSH 1.5 Version Fuzzer
5    auxiliary/fuzzers/ssh/ssh_version_2                                    normal  No     SSH 2.0 Version Fuzzer
6    auxiliary/fuzzers/ssh/ssh_version_corrupt                              normal  No     SSH Version Corruption
7    auxiliary/gather/qnap_lfi                             2019-11-25       normal  Yes    QNAP QTS and Photo Station Local File Inclusion
8    auxiliary/scanner/http/cisco_firepower_login                           normal  No     Cisco Firepower Management Console 6.0 Login
9    auxiliary/scanner/http/gitlab_user_enum               2014-11-21       normal  No     GitLab User Enumeration
10   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
11   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
12   auxiliary/scanner/ssh/detect_kippo                                     normal  No     Kippo SSH Honeypot Detector
13   auxiliary/scanner/ssh/eaton_xpert_backdoor            2018-07-18       normal  No     Eaton Xpert Meter SSH Private Key Exposure Scanner
14   auxiliary/scanner/ssh/fortinet_backdoor               2016-01-09       normal  No     Fortinet SSH Backdoor Scanner
15   auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal  No     Juniper SSH Backdoor Scanner
16   auxiliary/scanner/ssh/karaf_login                                      normal  No     Apache Karaf Login Utility
17   auxiliary/scanner/ssh/libssh_auth_bypass              2018-10-16       normal  No     libssh Authentication Bypass Scanner
18   auxiliary/scanner/ssh/ssh_enum_git_keys                                normal  No     Test SSH Github Access
19   auxiliary/scanner/ssh/ssh_enumusers                                    normal  No     SSH Username Enumeration
20   auxiliary/scanner/ssh/ssh_identify_pubkeys                             normal  No     SSH Public Key Acceptance Scanner
21   auxiliary/scanner/ssh/ssh_login                                        normal  No     SSH Login Check Scanner
22   auxiliary/scanner/ssh/ssh_login_pubkey                                 normal  No     SSH Public Key Login Scanner
23   auxiliary/scanner/ssh/ssh_version                                      normal  No     SSH Version Scanner
```

Fig.5

his procedure is for “ssh” alone. Now you will get results in Metasploit.

o, if you go for the “help <command>” option, for example, you type, “help search” you will et many details regarding the use of the command. For example, you may not know that ou can filter your searches as well which is explained in the help.

```
Examples:
  search cve:2009 type:exploit
  search cve:2009 type:exploit platform:-linux
```

Fig.6

et’s try this…

nsf6 > search cve:2020 type:exploit platform:-linux ssh

```
sf6 > search cve:2020 type:exploit platform:-linux ssh

atching Modules

  #  Name                                  Disclosure Date  Rank       Check  Description
  -  ----                                  ---------------  ----       -----  -----------
  0  exploit/linux/ssh/ibm_drm_a3user      2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
```

Fig.7

et’s look at how SSH exploits on the Linux 2020 platform work.

o, what does this actually do?

nsf6 > **info exploit/linux/ssh/ibm_drm_a3user**

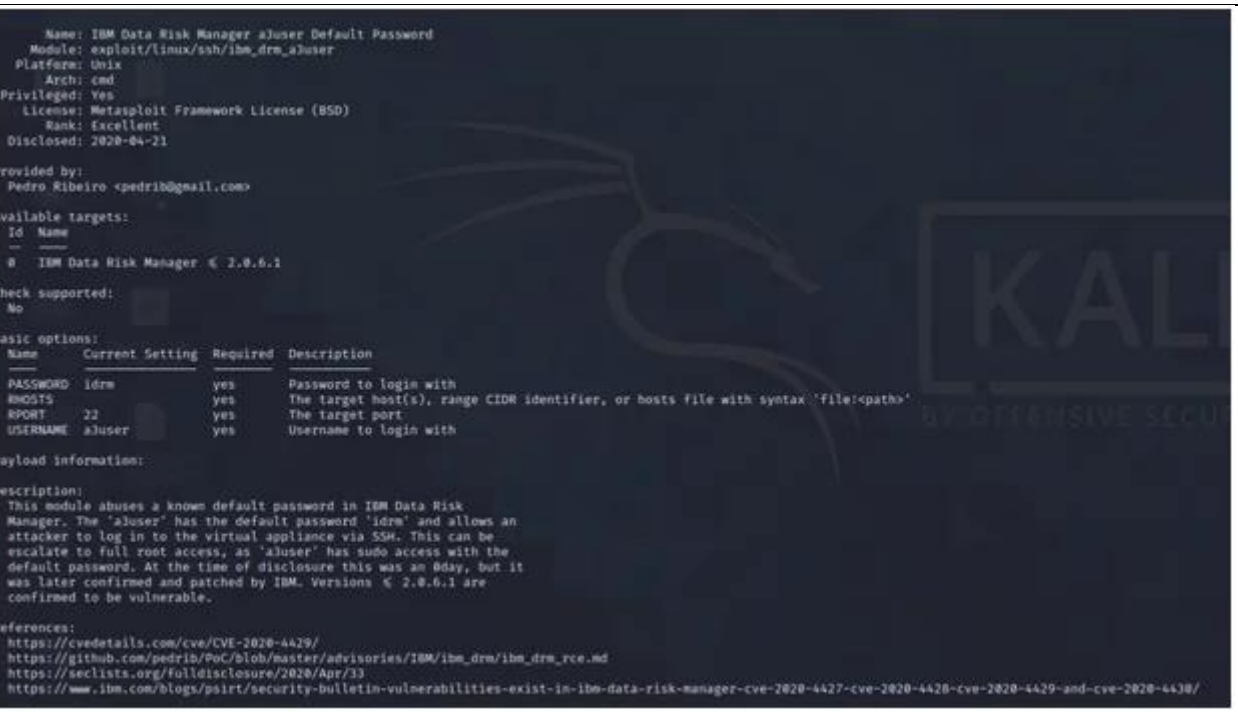


Fig.8

ime to exploit!

sing the Kali Linux SSH server for this example. The next step is to tell Metasploit that the ali Linux SSH server is used for this exploit.

msf6 > use exploit/linux/ssh/ibm_drm_a3user[*] No payload configured, defaulting to md/unix/interactmsf6 exploit(linux/ssh/ibm_drm_a3user) >

ow, configuring the options...

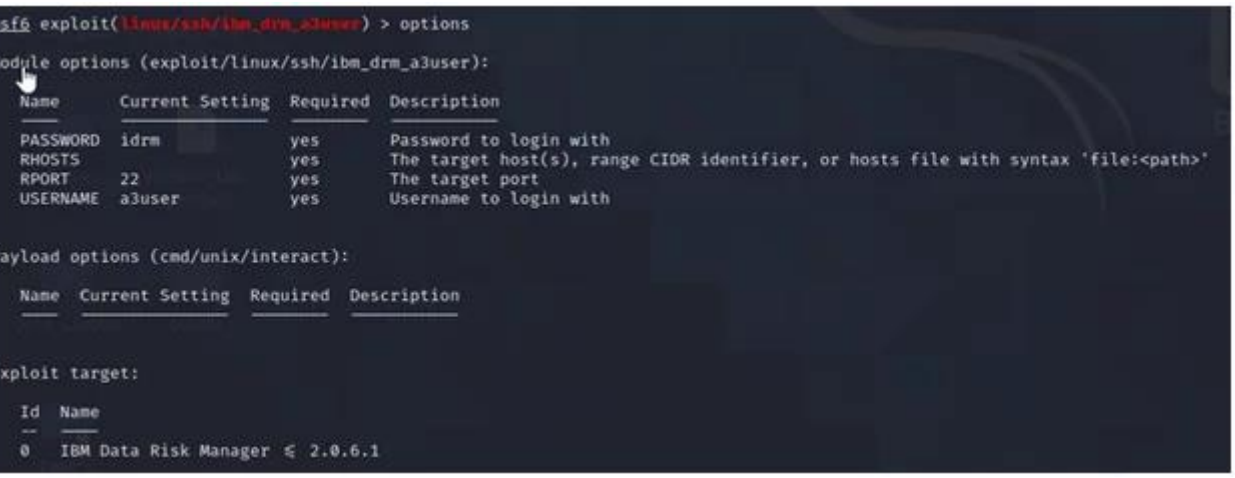


Fig.9

ow, we set the various options using the "**set**" command.

nsf6 exploit(linux/ssh/ibm_drm_a3user) > **set RHOSTS localhost**RHOSTS => localhost

nce the desired options are set, run "**exploit**" command.

nsf6 exploit(linux/ssh/ibm_drm_a3user) > **exploit**[*] Exploiting target {:address=>"0.0.0.1", ostname=>"localhost"} [*] 0.0.0.1:22 – Making an attempt to log in to the IBM Data Risk Manager appliance...

Metasploit, "search" functionality is considered to be a powerful option, but you can also nd other possible ways.

im : Cyberlaw :
yberlaw section under IT act 2000 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74 , Penalty and preventive easures to be taken for the crime associated with each case if
ny and real life cybercrime cases under each section.

Description :

Section 43: Penalty and Compensation for damage to computer, computer system, etc
If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network –
(a) accesses or secures access to such computer, computer system or computer network or computer resource;
(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injurously by any means;
(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,
he shall be liable to pay damages by way of compensation to the person so affected.

Section 65, whoever tampers with computer source documents knowingly or intentionally conceals, destroys or alters or causes another to conceal, destroy or alter any computer source code shall be punishable with imprisonment up to three years or with fine which may extend up to rupees two lakhs or with both.

Section 66A. Punishment for sending offensive messages through communication service, etc.—
Any person who sends, by means of a computer resource or a communication device,

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.--For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.]

Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device.
Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C. Punishment for identity theft.

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D. Punishment for cheating by personation by using computer resource.

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E. Punishment for violation of privacy.

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation. --For the purposes of this section--

(a) transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) capture, with respect to an image, means to videotape, photograph, film or record by any means;
(c) private area means the naked or undergarment clad genitals, *[pubic area], buttocks or female breast:
(d) publishes means reproduction in the printed or electronic form and making it available for public;

(e) under circumstances violating privacy means circumstances in which a person can have a reasonable expectation that--
(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 66F. Punishment for cyber terrorism.

(1) Whoever,--
(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--
(i) denying or cause the denial of access to any person authorised to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
(iii) introducing or causing to introduce any computer contaminant,
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or
(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,
commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life

Section 67. Punishment for publishing or transmitting obscene material in electronic form.

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

Whoever,--

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form--

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes.

Explanation--For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Section 71. Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or 1 [electronic signature Certificate], as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72. Penalty for Breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 73. Penalty for publishing electronic signature Certificate false in certain particulars.
73.

Penalty for publishing 1[electronic signature] Certificate false in certain particulars.--(1) No person shall publish a 1[electronic signature] Certificate or otherwise make it available to any other person with the knowledge that--

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a 1[electronic signature] created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 74. Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a 1 [electronic signature] Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.