Signature of the Candidate

Marks Awarded

Signature of the HOD

Signature of the Faculty with D

LIST OF EXPERIMENTS

Sl. No.	Date	Name of the Experiment	Page No.	Marks
1	31/3/23	Experiment 1(A) Steps to ensure security of any one web browser	2-3	
2	31/3/23	Experiment-1(B) Gathering information using windows command line utilities	4-5	
3	5/5/23	Experiment-2(a) Password cracking on an unauthorized MS Excel document	6-7	
4	5/5/23	Experiment-2(b) Scanning system vulnerabilities using microsoft baseline security analyzer tool	8	
5	19/5/23	Experiment-3(A) Study of Cyber forensic tools	9-10	
6	19/5/23	Experiment-3(b) Comparison of two files for forensics investigation by comparit tool.	11	
7	26/5/23	Experiment-4(a) Analyze port vulnerability of system using NMAP to ensure security	12	
8	26/5/23	Experiment-4(b) Stegnography	13-14	
9	26/5/23	Experiment-5(a) Program to illustrate buffer overflow attack	15	
10	26/5/23	Experiment-5(b) Implement versatile hacking tool, hashcat for cracking the password	16	

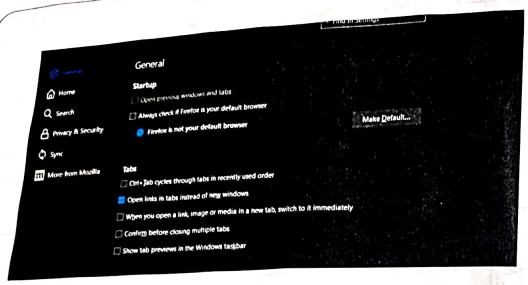
Signature of the HOD

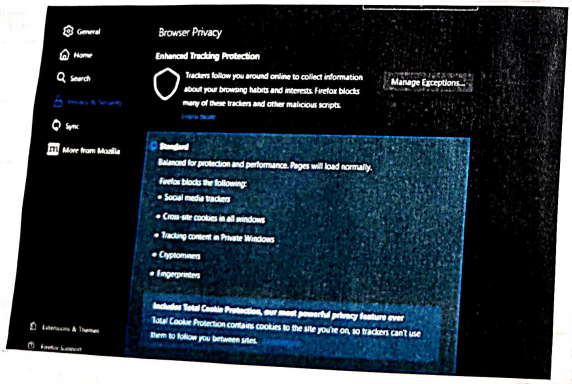
LIST OF EXPERIMENTS

Sl. No.	Date	Name of the Experiment	Page No.	Marks
11	2/6/23	Experiment No- 6(a) Downloading a website using website copier tool (HTTrack)	17-18	
12	2/6/23	Experiment No-6(b) Text steganography	19-20	
13	9/6/23	Experiment No-7(a) Analyze the Packet capture using wireshark tool	21-23	
14	9/6/23	Experiment No-7(b) Analyze the packet using wireshark (FTP)	24-25	
15	9/6/23	Experiment - 8(a) Implement of Caesar cipher using C program	26-27	
16	9/6/23	Experiment - 8(b) Step by step process for hiding & extracting text behind image	28-29.	
17				
18				
19				
20				

Signature of the HOD

Signature of the Faculty with Date





D.S.C.E.

D D M M Y Y Y Y
31 03 2023

EXPERIMENT-11(A)

Steps to ensure security of any one web browser (Mozilla firefox/Google chrome)

Aim: The main aim to study the steps to ensure security of any on web browser

Procedure:

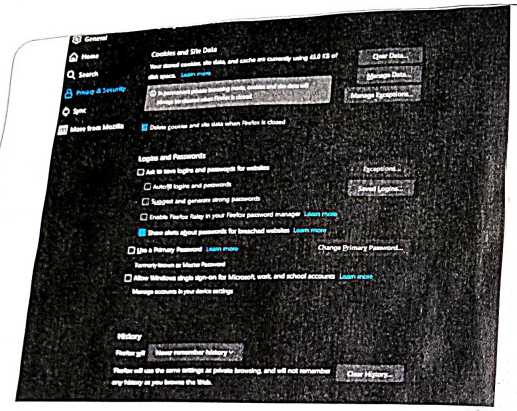
* There are 6 ways to ensure security of our web browser are:
- Configure the browser security system.
- Installing Antivirus
- Update the browser.
- Install security plugins
- Sign in google alerts
- Be careful while installing.

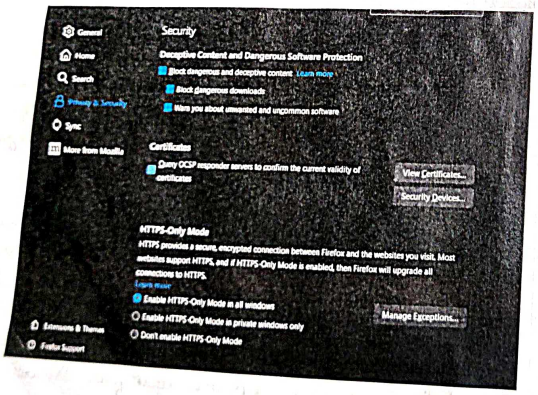
* Setting to configure in the web browser:
- In the general tab:
  - In the Tabs, check the option "open links in tabs instead of new windows".
  - In the Files and Application, Check the option "Always ask you where to save files".
- In the Privacy & Security Tab:
  - In the enhanced tracking protection, enable the standard protection mode.
  - In the logins and Passwords, disable the option "Ask to save logins and Passwords for websites".
  - In the history, select the never remember history option.
  - Set the block dangerous & deceptive content to check.
  - Check the Query OCSP responder to confirm the current validity of certificates

D.S.C.E.

Signature of the HOD

Signature of the Faculty with Date





D.S.C.E.

③

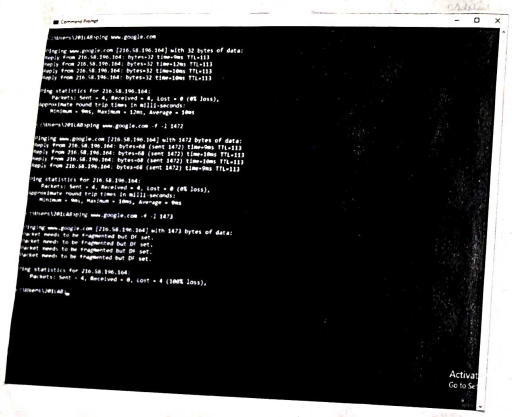
D D M M Y Y Y Y

- Enable HTTPs - only MODE in all windows.
- At the "Tracking" section press the blue text with 'Manage your Do Not Track settings" and check "Always apply do not track"
- In the "Logins" section you can set up a Master Password. Doing this is especially useful when multiple people have access to the computer, since it asks you introduce a master password before you can access logins.

Result:-

The detail studies of the steps to ensure security of any one web browser (Mozilla firefox / google chrome) is completed successfully.

D.S.C.E.



D.S.C.E.

④

D D M M Y Y Y Y
31 03 2023

EXPERIMENT - 1(B)

Gathering information using windows command line utilities.

Aim: The main aim is to gather the information using windows command line utilities

Procedure:

Consider a network where you have access to a Windows PC connected to the Internet.

Using Windows-based tools, let's gather some information about the target. You can ask any target domain or IP address

- Open the Windows Command Line (cmd) from Windows PC.
- Enter the command "ping yahoo.com" or "ping google.com" to ping
- From the output you can observe the following information
  - yahoo.com is live
  - IP address of yahoo.com
  - Round trip time.
  - TTL value
  - Packet loss statistics
- Now, enter the command "ping yahoo.com -f -l 1500" to check the value of fragmentation.

- Ping - command to determine the connectivity between your computer & a particulars address (within the local network or the Internet)
- URL or local address - web browser or the IP address of the server you're trying to check for a good connectivity.
- -f: a command to make sure that when you ping a certain address, it will not be fragment the packet sent or received.

D.S.C.E.

Signature of the Faculty with Date

Signature of the HOD

D D M M Y Y Y Y

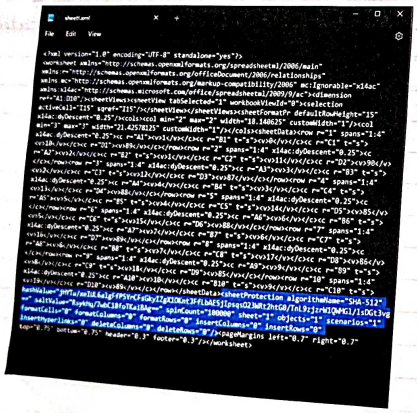
...-l : a command to help you determine the best MTU size for your network.

Here are the results that you may get after doing the ping test:

- four replies received - This means that the packet size entered is either within or the actual MTU size.
- Destination net unreachable - This means that there was no path or route to the destination.
- Request Time Out.. - This means that within the default wait period (1sec), there was no response.
- Packet needs to be fragmented but DF is set - This means that the packet size is too high.

Result:

The detail studies of the steps to given information about the target is completed successfully.



D.S.C.E.

D D M M Y Y Y Y
05 05 2023

Experiment - 2 (A)

Password cracking on an unauthorized ms excel document.

AIM: The main aim is to open an unauthorized ms excel document by password cracking

Procedure.

1. Open the MS Excel by clicking start menu icon in the task bar.
2. Create an any highly official document (ex: Student marksheet, EMP salary)

SNO	REGNO	STUDENT NAME	MARKS
1	100	Abhay	10
2	101	Bharat	20
3	102	Charan	30
4	103	Deepak	40
5	104	Eshwar	50

3. Save the MS Excel document with a file name & with the extension of .xls
4. Protect your document with a password by selecting review tab & choose protect sheet Assign a password.

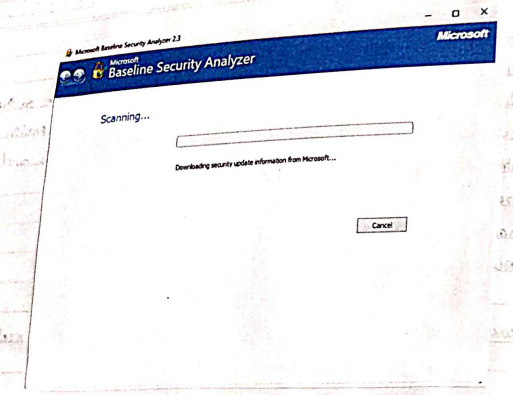
SNO	REGNO	STUDENT NAME	MARKS
1	100	Abhay	10
2	101	Bharat	20

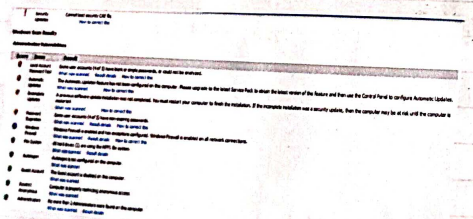
5. Enable all the alignment edition option so therefore one can edit out official document select OK.
6. And re-enter the password to confirm the password.
7. Now check if the editing is possible in our official document If we try to change any thin will display that this document is protected by password.

D.S.C.E.

8. Save the document in a new folder or in a desktop.
9. Select the file and change the extension as zip or right click on the file select the properties from the pop-menu & change the extension of the document otherwise right click on the file select open with and choose with RAR. The .xsls file is changed to .zip.
10. Open zip file & delete sheet protection tag & save file.
11. Change the extension back to .xlsx.
12. Now can change the file data.

Result: The main aim is to open an unauthorized ms excel document by password cracking is completed successfully.





DD MM YYYY
05 05 2023

Experiment-2 (B)

Scanning system vulnerabilities using microsoft Baseline security Analyzer (MBSA) tool.

Aim: The main aim is to scan the system vulnerabilities using MBSA tool.

Procedure:

1. download the MBSA
2. Start & install MBSA
3. Choose location to install
4. Click Scan computer to start.
5. Provide IP address & click start scan.
6. Scanning process started.
7. detail report is generated for the system

Result: The main aim is to scan the system vulnerabilities using MBSA is successfully completed.

DD MM YYYY 14/05/2022

Experiment -3(a)

Study of cyber forensic tools

1) NMAP (Network mapper)- It is a tool for network scanning & auditing its core advantage is that it supports all operating systems. It is open source.

2. oxygen forensics suite : It is open source, mobile forensics tools that will help to gather evidences you need from a mobile phone. It can bypass password or lock screen gesture prompt granting you to access stored data.

3. The SleuthKit - It is open source data extraction tool from Hard disk or other types of storage. It is not so user-friendly.

4. SIFT - It is ubuntu based software. It is open source. It has incident response functionality.

5. Volatility - It extracts information from the running processes on the computer. It is used for malware analysis & incident response capabilities. It also allows you to extract data from DLL's crash dump files, network sockets & network connection.

6. Hex editor Neo - It is a database forensics tool used for data extraction low level file editing & performing a deep scan to uncover hidden data.

7. MVT - It is a collection of utilities designed to facilitate the consensual forensic acquisition of ios & android devices for the purpose of identifying any signs of compromise, mainly by the Pegasus spyware.

D.S.C.E.

D D M M Y Y Y Y

8) Wireshark - It is network capture & analyzer tool to see what's happening in your network. It is handy to investigate network related incident.

9) CAINE - It is Ubuntu based app that offers complete forensic environment that provides a graphical interface. Can be integrated into existing software as module & extracts timeline from RAM.

10) Network Miner - A network forensic analyzer for windows, linux, MacOS to detect OS, hostname, session, open ports through packet sniffing or by PCAP file. It gives extracted artifacts in an intuitive user interface.

11) RAM capturer - It is a free tool to dump data from computer's volatile memory. May contain volume's password & login credentials for web mails & social network services.

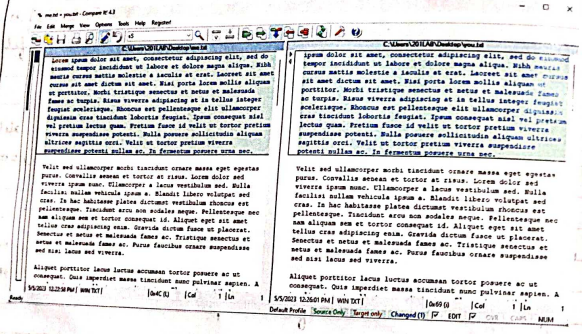
12) Encase - It helps you to recover evidence from hard drives. It allows you to conduct an in-depth analysis of files to collect proof like documents, pictures etc. & also used for mobile phones.

13) Crowdstrike - It provide threat intelligence, endpoint, security etc. It can easily detect & recover from cybersecurity incident and also use to find & block attackers in real time.

14) FIK Imager - It is forensic toolkit developed by Access data to get evidence & create evidence or copies of data without making changes to original evidence & lets you specify criteria like file size, pixel & reduce irrelevant data.

15) Xplico - It is forensic analysis app supporting HTTP, IMAP & more.

D.S.C.E.



D D M M Y Y Y Y
19 05 2023

Experiment - 3(A)

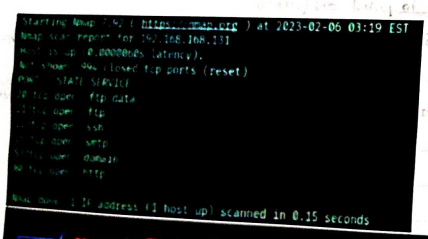
Comparison of two files for forensics investigation by compare it tool.

Aim: The main aim is to comparison of two files for forensics investigation by compare it tool.

Procedure

1. Open notepad & create file1.txt
2. Create second file file2.txt
3. Download compare it tool from http://www.grigsoft.com/wincmp3.html
4. Upload second file.
5. Upload first file.
6. Display 2 files side by side. colored differences sections to simplify analyzing.
7. It gives report to print differences.
8. Display comparison report.

Result: The main aim is to comparison of two files for forensic investigation by COMPARE IT tool is executed successfully.



D D M M Y Y Y Y
26 02 2023

Experiment-9(A)

Analyze the port vulnerability of the system using NMAP to ensure security in Apache server.

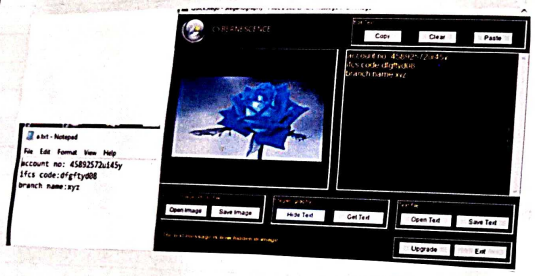
Aim:- The main aim is to scan the port using NMap in apache server.

Procedure:-

1. ~~Step~~ Start the virtual machine and launch Kali linux
2. Open the terminal
3. Stop the previously running Apache server (if any) using the code,
   sudo systemctl stop apache2
4. Now using the following code, start the Apache server
   sudo systemctl start apache2.
5. Use NMAP to scan the current working system's IP address for any open ports.
6. Analyze the output & the services that are running on that IP address.
7. Close the Apache server using the code below.

   sudo systemctl stop apache2

RESULT: The main aim is to scan the port using nmap in apache server is successfully completed



D D M M Y Y Y Y
26 05 2023

Experiment-4(B)

Steganography - Hiding and recovering the information using Quickstego tool.

AIM: The main aim is to hide & recover the information using Quickstego Tool.

Procedure

1. Download the Quickstego tool.
2. Install the Quickstego tool and launch the desktop icon.
3. Open the Quickstego application.
4. Create a text file or otherwise directly we can give the text data here we are creating a secrete text file with the extension .txt to upload in the image.
5. Upload the image file to the Quickstego application
6. Upload the text file to the Quickstego application.
7. Click hide text to hide the text document to image
8. Click save image to upload the secret data to image a new image file is created & saved.
9. Now close the stego application & open it again.

D D M M Y Y Y Y

10. Now open the newly saved image & click the Get text.

Result :- The main aim is to hide and recover the information using QUICKSTEGO TOOL is completed successfully.

OUTPUT

RUN1

Enter the password:

thegukstuff

Correct Password:

Root privelges given to the user

RUN 2

Enter the password:

hhhhhhhhhhhhhhh

Wrong password

Root privileges given to the user.

D D M M Y Y Y Y
26 03 2021

Experiment - 5(A)

Write a program to illustrate Buffer overflow attack

AIM: The main aim is to write a program to illustrate buffer overflow attack.

PROCEDURE:

```
#include <stdio.h>
#include <string.h>
int main()
{ char buff[15];
  int pass=0;
  printf("\n Enter the password \n");
  gets(buff);
  if(strcmp(buff,"thegukstuff"))
  { printf("\n Wrong password \n"); }
  else
  { printf("\n Correct Password \n");
    pass=1;
  }
  if(pass) { printf("Root privelges given to the user \n");
  }
  return 0;
}
```

Result: The main aim is to write a program to illustrate buffer overflow attack is completed successfully

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop]
└─$ cat hashfile.txt
e10adc3949ba59abbe56e057f20f883e

┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 0 --show hashfile.txt rockyou.txt
e10adc3949ba59abbe56e057f20f883e:123456

┌──(kali㉿kali)-[~/Desktop]
└─$
```


D D M M Y Y Y Y
26 05 2022

Experiment-5(B)

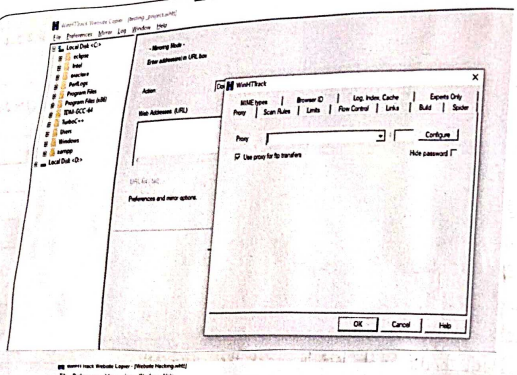
Implement a versatile hacking tool - Hashcat Tool for cracking the password.

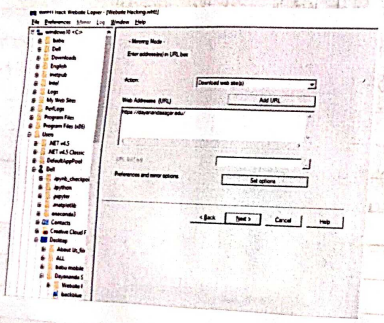
Aim: The main aim is to crack the password using Hashcat tool.

PROCEDURE:

1. Open the hash file with the cat command, which will display the hash
   cat file.txt
2. Use the hashcat tool to crack the password.
3. Write the following command for cracking the password using hash
   hashcat -m 0 hashfile.txt

Result: The main aim to crack the password using Hashcat tool is successful.





D D M M Y Y Y Y
0 2 0 2 2 0 2 3

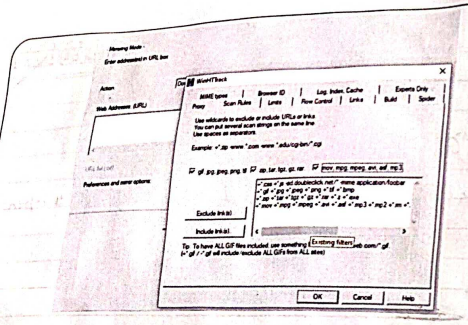
Experiment - 6(A)

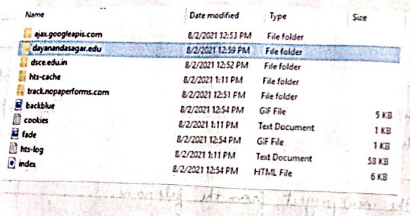
Downloading a website using Website copier tool (HTTRACK)

Aim:- The main aim is to downloading a website using website copier tool (HTTRACK)

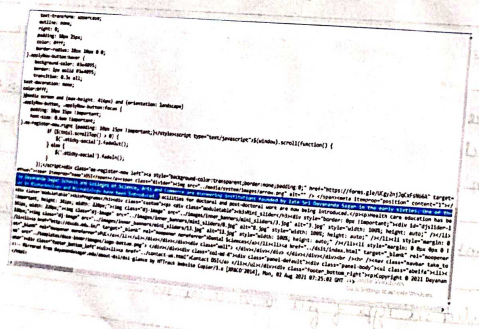
Procedure:-

1. Install WinHTTRACK.
2. Create a folder on the desktop & rename the folder name. For example: Folder name is "Dayanda Sagar Website". Open the folder "Dayananda Sagar Website". The content of the folder is empty.
3. Select the new project from the file menu.
4. Enter the project name in new project field. Example: Website hacking.
5. Give the path where you need to download the files. In order to do this click on desktop & then click the folder "Dayanda Sagar Website. Press OK.
6. WinHTTRACK option window is opened select the scan rules
7. Select all type of file to start the scan.
8. Now all the extensions is added for the scan.





Name	Date modified	Type	Size
ajax.googleapis.com	8/2/2021 12:53 PM	File folder	
dayanandasagar.edu	8/2/2021 12:59 PM	File folder	
dsce.edu.in	8/2/2021 12:52 PM	File folder	
hts-cache	8/2/2021 1:11 PM	File folder	
track.nopaperforms.com	8/2/2021 12:51 PM	File folder	
backblue	8/2/2021 12:54 PM	GIF File	5 KB
cookies	8/2/2021 1:11 PM	Text Document	1 KB
fade	8/2/2021 12:54 PM	GIF File	1 KB
hts-log	8/2/2021 1:11 PM	Text Document	58 KB
index	8/2/2021 12:54 PM	HTML File	6 KB



D.S.C.E.

(18)

(9) Now type the URL address to scan.

(10) Enable the connection adjustment if needed & click the finish button.

(11) Mirroring process is get started.

(12) The detail information about the URL will be fetched & saved in the folder "Dayananda sagar website". You can now open the folder where you can see the project name given as Website hacking as shown in step3.

(13) Click on Website hacking file, then the URL database address dayanda sagar.edu given in the step8 will be visible.

(14) Click on the file, dayanandasagar.edu. Now you can find all the files of the original page of the website will be displayed.

(15) Click on any file to alter the content: ctrl with notepad.

(16) Contents of the pages is displayed. Now you can alter the contents.

RESULT: The main aim is to downloading a website using copier tool (HTTRACK) is completed successfully.

D.S.C.E.

File Edit Format View Help

```
Hello Students.
#####################################
This is Original File!!!
#####################################

Hello World!!!

Welcome to Cyber Security Lab!!!!!!
```

```
C:\Users\CSE\Desktop\snow>snow -C -p "password123" Test.txt
My Account Number is 1234567
C:\Users\CSE\Desktop\snow>
```

Command Prompt

```
C:\Users\CSE\Desktop\snow>snow -C -m "My Account Number is 1234567" -p "password123" Sample.txt Test.txt
Compressed by 22.12%
message used approximately 166.00% of available space.

C:\Users\CSE\Desktop\snow>
```


DD MM YYYY
02/06/2022

Experiment - 6(A)

Text steganography : Hiding the information in the Text file using snow tool.

AIM: The main aim is to hide the information in the text file using SNOW TOOL Text steganography.

PROCEDURE :

1. Create a text file with some data in the same directory where SNOW tool is installed.
2. In our experiment Snow tool is installed in desktop.
3. Go to the Command Prompt, change the directory to run snow tool.
4. Type the command
   Snow -C -m "text to be hidden" -p" password" < source file> <Destination file>
5. Example :
   Snow -C -m "My account number 1234567 "-p" password 123" Sample.txt Test.txt
   The source file is a sample.txt file as shown above. Destination file will be created automatically and exact copy of source file containing hidden information.
6. Go to the directory : You will find a new file by name Test.txt. open the file

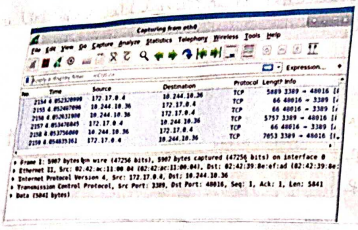
D D M M Y Y Y Y

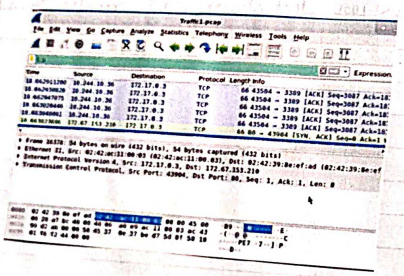
③ Now file has the same text as an original file (sample.txt) without any hidden information. This file can be sent to the target.

④ Recovering the hidden information:
On the destination, the receiver can reveal information by using the command.
snow -C -p "password" <Destination File>
snow -C -p "password" text.txt

RESULT: The main aim is to hide the information in the Text file using SNOW TOOL text steganography is completed successfully.

D.S.C.E.





D D M M Y Y Y Y
09 06 2023

Experiment - 7(A)

Analyze the Packet Capture Using Wireshark Tool

AIM: Analyze the TCP packet capture using WIRESHARK tool.

1. Capture the real time network traffic using wireshark

a. Open Wireshark Application:

To open the Wireshark Application go to the left corner, click on the icon to open the list of the tools available. Then type Wireshark in the search bar & click on the launch button

b. Select the Network interface:

Select ethO interface to start capturing the data and click on this ◫ option to capture the N packets

Once you click on the capture button, packet capturing will start. The packet capturing screen is shown below.

c. Browse a website:

To open the browser go to the Top left corner; click on the 'Application' icon to open the list of the tools available & select the web browser

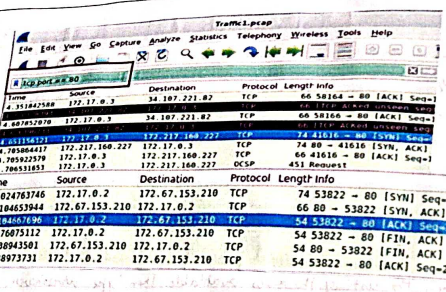
Browse any website in the web browser. For instance www.cdac.in

d. Save network Traffic

Before saving Network Traffic, stop the Wireshark packet capturing by selecting the symbol. In order to save the captured network packets, go to the top left corner & click on "File" followed by "save"

Give any name to your file. Here we have given Traffic

Now select the extension as pcap by clicking on the drop down beside the "save as". Choose the "wireshark / tcpdump-pcap "option & click on "save" button




```
Source Port: 53822
Destination Port: 80
[Stream index: 36]
[TCP Segment Len: 0]
Sequence number: 2    (relative sequence number)
[Next sequence number: 2    (relative sequence number)]
Acknowledgment number: 2    (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0xf243 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
```

D.S.C.E.

(1)

(22)

(2) Following TCP stream

a. Filter tcp traffic:

Analyze the TCP packets using the filter box. Type "tcp" in the filter box to get all the TCP packets.

b. Follow TCP stream

To view the one complete three way tcp handshake connection, right click on any green color traffic & select "Follow" choose "TCP stream" as given below.

An window will open. Click on the close button. Result after using TCP stream is given below:

(3) Analyze TCP Header

a) Analyze TCP syn Traffic

Try to observe the TCP SYN traffic captured in the Wireshark packet list pane. Type tcp.port = 80 in the filter box & press Enter.

Right click on the first SYN packet & select Follow & then click on TCP stream. Click on the close button.

Expand TCP to view the further details.

Expand flags to views flag details. Observe the flag settings. Notice that SYN is set, indicating the first segment in the TCP three way handshake.

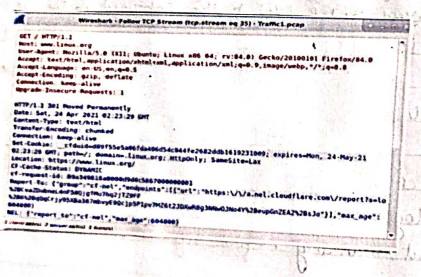
b) Analyze TCP SYN, ACK Traffic.

Click on the SYN, ACK packet & start analyzing TCP SYN, ACK Traffic.

Expand TCP to view TCP details.

D.S.C.E.

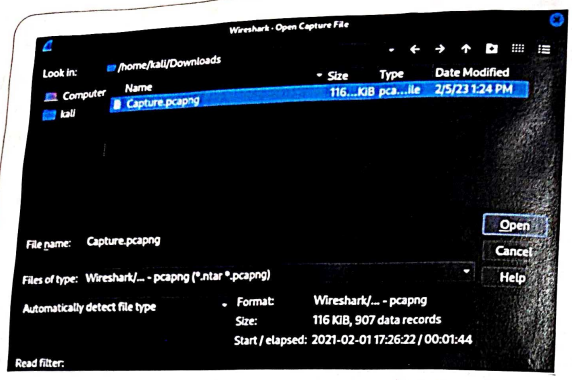
```
Source Port: 53822
Destination Port: 80
[Stream index: 36]
[TCP Segment Len: 0]
Sequence number: 1    (relative sequence number)
[Next sequence number: 1    (relative sequence number)]
Acknowledgment number: 1    (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0xf243 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Source Port: 80
Destination Port: 53822
[Stream index: 36]
[TCP Segment Len: 0]
Sequence number: 1    (relative sequence number)
[Next sequence number: 1    (relative sequence number)]
Acknowledgment number: 2    (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x011 (FIN, ACK)
Window size value: 64
[Calculated window size: 65536]
[Window size scaling factor: 1024]
Checksum: 0xbace [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
```

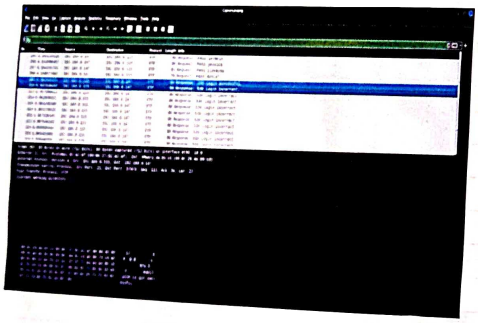


Expand flags to view flag details. Observe the flag settings. Notice that SYN & ACK are set, indicating the second segment in the TCP three-way handshake. Click on the ACK packet & start analyzing TCP ACK traffic.

c) Expand TCP to view TCP details
Perform above step for third segment

d. Analyze TCP FIN ACK Traffic
Click on the FIN, ACK packet & start analyzing TCP FIN, ACK Traffic.
Expand TCP to view TCP details
Expand flags to view flag details. Observe the flag settings. Notice that FIN & ACK are set, indicating the second segment in the TCP three way handshake. The server has indicated it is closing the TCP connection with the client.
Perform above step for third segment.





D D M M Y Y Y Y
0 9 0 6 2 0 2 3

Experiment - 7(B)

Analyze the packet capture using Wireshark tool (FTP)

AIM: The main aim is to analyze the packet capturing using wireshark tool

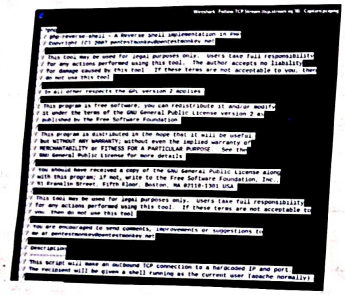
Procedure

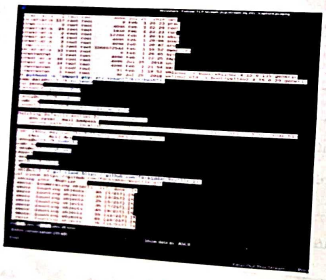
1. Start the VM & launch Kali linux.
2. Search for wireshark tool in Kali linux by clicking on the top left corner and open the Wireshark tool.
3. After the wireshark interface is open, navigate to the file menu in the upper left corner
4. Click on the captured file to open it. This file already exists in the system. (.pcapng file)
5. We are attempting to evaluate the packets transmitted over the FTP protocol. Filter the ftp packets by entering 'ftp' into the filter box & press enter.
6. You can now observe the packets being transmitted using the ftp protocol. More requests & replies may be found on you scroll below.
7. You can notice a 'login successful' packet when you scroll down to ~~the~~ examine.
8. Right-click on the packet, select follow TCP stream.

Signature of the Faculty with Date

Signature of the HOD

```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS 111111
530 Login incorrect.
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
```





D.S.C.E.

D D M M Y Y Y Y

(9) Now try to analyze the packet by changing the streams in the bottom left corner

(10) In stream 16, we can see the attacker trying to gain the "Initial Access" The attacker has installed a shell.php file in the var/www/html.

(11) In stream 18, the reverse shell.php enables the attacker to track all of the user's online behavior.

(12) In stream 20, we canse the attackers is trying to gain access to the complete console by trying to login to ssh using the same password This is called the 'Privilge Escalation'.

(13) In stream 20, We learn that the intruder set up a backdoor so he can enter the system wherever he wants. This is called 'Persistance'

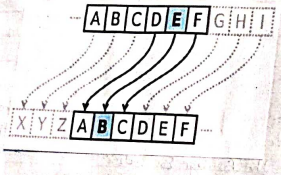
RESULT: The main aim is to analyze the packet capture using wireshark tool is completed succesfully

D.S.C.E.

Signature of the Candidate

Signature of the Faculty with Date

Signature of the HOD



D.S.C.E.

D D M M Y Y Y Y
09 02 2023

Experiment No:-8 (A)

Implementation of Caesar Cipher using C program

AIM:- To implement the simple substitution technique named Caesar cipher using C-language

Procedure:-

Algorithm

1. Read the plain text from the user
2. Read the key value from the user.
3. If the key is positive then encrypt the text by adding the key with each character in the plain text.
4. Else subtract the key from the plain text.
5. Display the cipher text obtained above.

PROGRAM (CAESAR CIPHER)

```
#include <stdio.h>
#include <string.h>
#include <conio.h>
#include <ctype.h>
int main()
{ char plain[10], cipher[10];
  int key, i, length;
  printf("Enter the plain text:\n");
  scanf("%s", plain);
  printf("Enter the key value:\n");
  scanf("%s", key);
```

D.S.C.E.

Signature of the Faculty with Date

Signature of the HOD

OUTPUT

Enter the plain text : hello

Enter the key value : 3

PLAIN TEXT : hello

ENCRYPTED TEXT : Khoor

AFTER DECRYPTION : hello

D.S.C.E.


```
printf("\n\n\t PLAIN TEXT IS : %s", plain);
printf("\n\n\t Encrypted text: ");
for(i=0; length=strlen(plain); i<len; i++)
{   cipher[i]= plain[i]+ key;
    if (isupper(plain[i]) && (cipher[i]>'Z'))
        cipher[i]= cipher[i]-26;
    if (islower(plain[i]) && (cipher[i]>'z'))
        cipher[i]= cipher[i]-26;
        printf("%c", cipher[i]);
    }
printf("\n\n\t After Decryption:");
    for(i=0 ; i< length; i++)
{   plain[i]= cipher[i]- key;
    if(isupper(cipher[i]) && (plain[i]<'A'))
        plain[i]= plain[i]+26;
    if(islower(cipher[i]) && (plain[i]<'a'))
        plain[i] = plain[i] + 26;
        printf("%c", plain[i]);
    }
    getch();
}
```

Result: The main aim is to study the detail report of cyber forensic tools is completed.

D.S.C.E.

Signature of the HOD

*a.txt - Notepad
File Edit Format View Help
Command Prompt is a command line interpreter application available in most Windows operating systems. It's used to execute entered commands. Most of those commands automate tasks via scripts and batch files, perform advanced administrative functions, and troubleshoot or solve certain kinds of Windows issues.

```
C:\Users\CSE\Desktop>a.txt

C:\Users\CSE\Desktop>b.jpg
```


D D M M Y Y Y Y
29 06 2023

Experiment-8(b)

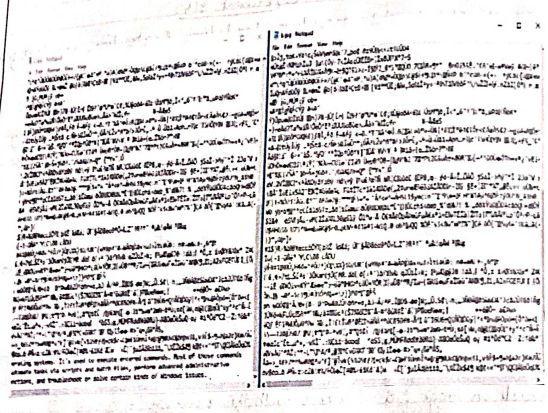
Write the steps by step procedure for hiding & extracting any text file behind an image file using Command Prompt

Aim:- The main aim is to hide & extract any text file behind an image file using Command prompt.

Procedure

1. Create a text document with the file name & .txt as an extension. example: a.txt is created
2. Type the content which you need to hide in the image & save it
3. Create an image file & save it with the extension .jpg. example: b.jpg is created.
4. Open command prompt by selecting start icon in the task bar.
5. Open the command prompt a black working place will be available press ctrl + r & type cmd & hit here.
6. Move to the folder where the two are located the cd command is used to enter into the folder.
   >> cd desktop.
7. Open the text file by its filename. Example a.txt then text file will get open

Signature of the HOD



D.S.C.E.

29

8. Open the .jpg file by its filename. Example b.jpg then the image file will get open.

4. Now type the following

Syntax : copy /b Name-of-file-containing-text-you-want-to-hide-.txt- Name-of-initial Image.jpg Resulting-image-name.jpg.

code : > copy /b B.jpg + A.txt c.jpg

10. Locate c.jpg file from where you want to retrieve text data.

11. Right click & open with notepad.

Done! Successfully opened! In the last of the notepad, you will find behind ~~or image~~ the content of the text file.

Result: The main aim is to hide & extract any text file behind an image file using command prompt is completed successfully.

D.S.C.E.