ज्ञान, विज्ञान आणि सुसंस्कार यांसाठी शिक्षण प्रसार" - शिक्षणमहर्षी डॉ. बापूजी साळुंखे
Shri Swami Vivekanand Shikshan Sanstha, Kolhapur.

VIVEKANAND COLLEGE, KOLHAPUR

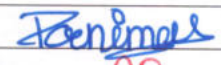
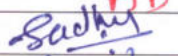
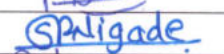
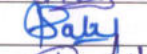
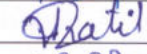
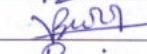
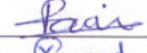
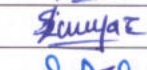
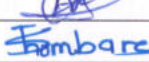
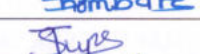
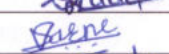
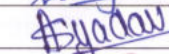
(An Empowered Autonomous Institute)
Affiliated to Shivaji University
NAAC Reaccredited "A+" CGPA 3.29 | College with Potential for excellence | ISO 9001:2015

Department of Computer Studies

Subject-Ethical Hacking
Date-09/09/2025
Surprise Test

ROLL NO.	NAME	SIGN
1	AGLAVE AARTI HARIDAS	Aglave
2	*AMANE SALONI SATISH	Amane
3	*APATE KOMAL ARVIND	Apate
4	*BAVADEKAR MANASI PRAKASH	Bavadekar
5	*BHOI SHREYA SACHIN	Bhoi
6	BHOSALE KARTIK KUMAR	AB
7	*BHOSALE DEVIKA RAMCHANDRA	Bhosale
8	CHAVAN ABHISHEK RAJESH	Chavan
9	*CHAVAN PRANALI SUHAS	Chavan
10	*CHECHAR ADITI UTTAM	Aditi
11	*SHIVANI DATTATRAY CHOPADE	Shivani
12	CHOPADE JAMES PRAVIN	Chopade
13	*CHORMARE PRERANA SANJAY	B
14	*CHOUGALE NANDINI SHASHIKANT	Bhougale
15	*JADHAV HARSHADA MOHAN	Jadhav
16	JADHAV AKASH SURYAKANT	AB
17	*JADHAV RADHIKA NITIN	AB
18	*JADHAV NISHA GUNDOPANT	AB
19	KAKADE SIDDHESH VINIT	AB
20	*KALE SHRUTI SATISH	Shruti
21	*KAMAT SWATI SHRIKANT	AB
22	KAMBALE SHREYASH RAJENDRA	AB
23	KAMBLE RUTVIK MURALIDHAR	
24	KAMBLE VINAY KAKASO	AB
25	KHADRE JAY SANJAY	
26	*KHAMBE VAISHNAVI MADHUKAR	AB
27	*KHOT SAKSHI DATTATRAY	Sakshi
28	*KOKATE SANDHYA ARUN	Kokate
29	KORADE SIDDHESH RAMAKANT	Korade

VIVEKANAND COLLEGE KOLHAPUR (Empowered Autonomous) ESTD JUNE 1964

30	*KOTAMIRE POURNIMA UJWAL	
31	KUMBHAR SOURABH RAJESH	AB
32	*KUMBHAR POOJA MARUTI	AB
33	*LOKHANDE ASHLESHA ANANDA	AB
34	LOTAKE OM RAHUL	
35	*MAGDUM JYOTI KUMAR	AB
36	MAHADIK SANGRAMSINH TATYASAHEB	AB
37	*MARALKAR PRATIKSHA VITTHAL	
38	NADAWADE PRASANNAJEET BHAGAVAN	
39	NIGADE SNEHAL RAMCHANDRA	
40	*NILKANTH NIKITA NAMDEV	
41	PATEL MUHAFIJ GOUSMAHAMAD	
42	PATHAN AAKIBMATIN FIROZKHAN	AB
43	*PATIL SHIVALI SANDIP	
44	*PATIL SHRAVANI MALGOUNDA	
45	*PATIL SHREYA SHAMRAO	
46	*PATIL VAISHNAVI VISHWAS	
47	*PATIL VAISHNAVI BALIRAM	
48	*PATIL ROHINI DATTATRAY	
49	PRASAD VIVEK KALPNATH	
50	*SANGAR SHITAL RAVINDRA	
51	*SHAIKH SUMAIYA AMAN	
52	SHELAKE PARTH PRABHAKAR	
53	*SHINDE ARATI ARUN	
54	SHIVASHARAN ADITYA RAMESH	
55	*THOMBARE SHRUTI VILAS	
56	*TUPE SHREYA MOHAN	
57	*VADD SHWETA YASHVANT	
58	*VARNE SAKSHI SUNIL	
59	*WAINGADE SAMRUDDHI SANJAY	
60	YADAV AISHWARYA SANJAY	
61	*KHADE SHARVARI EKNATH	AB

FACULTY SIGN

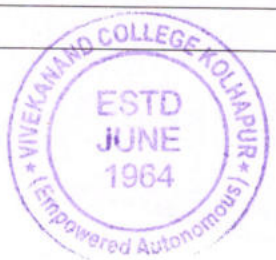
(Mr. Vaishnav. V. Shegale)

"ज्ञान, विज्ञान आणि सुसंस्कार यांसाठी शिक्षण प्रसार" – शिवमहर्षी डॉ. बापूजी साळुंखे
Shri Swami Vivekanand Shikshan Sanstha, Kolhapur.
VIVEKANAND COLLEGE, KOLHAPUR
(Empowered Autonomous)
Affiliated to Shivaji University
NAAC Reaccrediated "A" | College with Potential for excellence | ISO 9001 : 2015

MCA – II Semester – III
Surprise Test– I Result
Subject: Ethical Hacking

Marks: 20 **Date: 09/09/2025**

ROLL NO.	NAME	MARKS
1	AGLAVE AARTI HARIDAS	12
2	*AMANE SALONI SATISH	10
3	*APATE KOMAL ARVIND	09
4	*BAVADEKAR MANASI PRAKASH	11
5	*BHOI SHREYA SACHIN	12
6	BHOSALE KARTIK KUMAR	AB
7	*BHOSALE DEVIKA RAMCHANDRA	11
8	CHAVAN ABHISHEK RAJESH	09
9	*CHAVAN PRANALI SUHAS	10
10	*CHECHAR ADITI UTTAM	13
11	*SHIVANI DATTATRAY CHOPADE	11
12	CHOPADE JAMES PRAVIN	12
13	*CHORMARE PRERANA SANJAY	11
14	*CHOUGALE NANDINI SHASHIKANT	10
15	*JADHAV HARSHADA MOHAN	09
16	JADHAV AKASH SURYAKANT	AB
17	*JADHAV RADHIKA NITIN	AB
18	*JADHAV NISHA GUNDOPANT	AB
19	KAKADE SIDDHESH VINIT	AB
20	*KALE SHRUTI SATISH	12
21	*KAMAT SWATI SHRIKANT	AB
22	KAMBALE SHREYASH RAJENDRA	AB
23	KAMBLE RUTVIK MURALIDHAR	09
24	KAMBLE VINAY KAKASO	AB
25	KHADRE JAY SANJAY	09
26	*KHAMBE VAISHNAVI MADHUKAR	AB
27	*KHOT SAKSHI DATTATRAY	10
28	*KOKATE SANDHYA ARUN	09
29	KORADE SIDDHESH RAMAKANT	09
30	*KOTAMIRE POURNIMA UJWAL	11
31	KUMBHAR SOURABH RAJESH	AB
32	*KUMBHAR POOJA MARUTI	AB



33	*LOKHANDE ASHLESHA ANANDA	AB
34	LOTAKE OM RAHUL	11
35	*MAGDUM JYOTI KUMAR	AB
36	MAHADIK SANGRAMSINH TATYASAHEB	AB
37	*MARALKAR PRATIKSHA VITTHAL	11
38	NADAWADE PRASANNAJEET BHAGAVAN	10
39	NIGADE SNEHAL RAMCHANDRA	10
40	*NILKANTH NIKITA NAMDEV	11
41	PATEL MUHAFIJ GOUSMAHAMAD	12
42	PATHAN AAKIBMATIN FIROZKHAN	AB
43	*PATIL SHIVALI SANDIP	13
44	*PATIL SHRAVANI MALGOUNDA	12
45	*PATIL SHREYA SHAMRAO	11
46	*PATIL VAISHNAVI VISHWAS	10
47	*PATIL VAISHNAVI BALIRAM	09
48	*PATIL ROHINI DATTATRAY	10
49	PRASAD VIVEK KALPNATH	09
50	*SANGAR SHITAL RAVINDRA	11
51	*SHAIKH SUMAIYA AMAN	14
52	SHELAKE PARTH PRABHAKAR	10
53	*SHINDE ARATI ARUN	10
54	SHIVASHARAN ADITYA RAMESH	09
55	*THOMBARE SHRUTI VILAS	11
56	*TUPE SHREYA MOHAN	12
57	*VADD SHWETA YASHVANT	11
58	*VARNE SAKSHI SUNIL	11
59	*WAINGADE SAMRUDDHI SANJAY	10
60	YADAV AISHWARYA SANJAY	14
61	*KHADE SHARVARI EKNATH	AB

HEAD
DEPARTMENT OF M. C. A.
VIVEKANAND COLLEGE, KOLHAPUR
(EMPOWERED AUTONOMOUS)

Mr. Vaishnav V. Shegale

VIVEKANAND COLLEGE KOLHAPUR (Empowered Autonomous)
ESTD JUNE 1964

10/20

Surprise Test

Name:- Nandini S. Chougale
Roll No. 14
Sub. : Ethical Hacking
Date : 9/9/25

1.

1. What is ethical Hacking & Briefly explain any two types of Hackers.

→ Ethical Hacking is the practice of protecting computer system, network and application from attackers.

Black Hat → Harmful, malicious
White Hat → Ethical, Helpful
Grey Hat → Between good and Bad.

Example : A company hire a ethical hacker to test their application and website. Hacker check the system, website if some issue find they report it to the company and issue is fixed.

Explain two types of Hackers :-

Hackers are categorized based on their intent, skill level, and legality of their actions.

1. Black Hat

They are illegal hackers who break into system to steal data, damage files, or makes money. Their actions are harmful and criminal.

2] White Hat

These Hackers are legal and authorised to test their system.
They find and fix security problems to protect the system from real attacks.
Companies hire them to improve cyber security.

03

3. Differentiate between active and passive footprinting.

	Active Footprinting	Passive Footprinting
1]	Direct interaction with the target	Intraction through Company website, post,
2]	Active footprinting is risky	Passive footpring is safe.
3]	It is highly detected	It is low detected.
4]	Scanning Nmap to find open ports.	Checking a Company websites, Linkedin post to find employee detects.
5]		

2. Attack vectors

1. Phishing - This involves tricking people into giving up sensitive information. like password, credit card details, by disguising as a trustworthy entity. For example, a fake email that looks like its from your bank.

2. Malware -
Malicious software designed to harm a computer system. It can be spread through email attachments or by visiting compramised websites. for example, downloading a file that secretaly install a virus.

04.

3. Man - in the Middle (Mitm)
Intercept the communication between two parties.

4. SQL injection
An attack that attacker send a malicious SQL query in the database, and gain database data.

Surprise Test

14/20

Page No.
Date

Name :- Sumaiya Aman Shaikh
Subject :- Ethical Hacking
Roll No :- 51

Q.1) What is ethical hacking and briefly explain two types of hackers.

→ X Ethical Hacking -

Ethical hacking is the practice of intentionally probing computer systems, networks or applications for security vulnerabilities, with the permission of the owner. The goal is to identify and fix weaknesses before malicious hackers can exploit them. Ethical hackers, also known as white hat hackers.

Two types of Hackers :

1- White Hat Hackers (Ethical Hackers)

- These are professionals who hack systems legally and with permission.
- They work for companies or security firms to test and strengthen security.
- Their goal is to protect data and networks by finding and fixing vulnerabilities.
- Example : A CyberSecurity expert hired to perform penetration testing on a company's network.

2- Black Hat Hackers (Malicious Hackers)

- These hackers break into systems illegally without permission.

- Their intentions are harmful - such as stealing data, spreading malware, or causing system damage.
- They often hack for personal, financial or political gain.
- Example : A hacker who steal credit card information through phishing or malware attack.

Q.2) Mention any four attack vectors with a short explanation.

→ Here are four common attack vector with short explanations :

1- Phishing -
A method where attackers trick users into revealing sensitive information (like passwords or credit card numbers) through fake emails or websites.

2 - Malware -
Malicious software (such as viruses, worms or ransomware) that infects systems to steal data, damage files, or take control of devices.

3- Social Engineering -
Manipulating people into giving up confidential information by pretending to be a trustworthy person or authority.

4- Brute Force Attack -
An attack where the hacker tries many combinations of passwords or encryption keys until the correct one is found.

Q.3) Differentiate between active and passive footprinting with example.

→ Difference Between Active and passive Footprinting :

Aspect	Active Footprinting	Passive Footprinting
Definition	Directly interacting with the target system to gather info.	collecting information without directly interacting with the target
Risk of Detection	High - target may detect the activity	Low - no direct contact, so harder to detect.
Tools Used	Ping, Traceroute, Nmap, etc.	WHOIS lookup, Google Search, Social media, etc.
Example	Scanning a website using Nmap to Find Open ports.	Finding company details on LinkedIn or through a Google search.

Q.4) What is network Scanning and mention any two scanning techniques.

→ * Network Scanning -
Network Scanning is the process of identifying active devices, open ports, and services running on a network to access security and detect vulnerabilities.

It can be used for :
- Identifying live hosts (devices connected to the network)
- Detecting open ports and services.
- Finding vulnerabilities or misconfigurations.
- Mapping the network.

Two common Network Scanning techniques :

1. Port Scanning -
- Purpose : To Find open or closed ports on a target devices.
- How it works : The scanner sends requests to a range of ports on a host to determine which ones are open and what service are running.
- Tools Used : Nmap, NetCat
- Example : Scanning a Server to see if ports like 22 (SSH), 80 (HTTP), or 443 (HTTPS) are open.

2 - Ping Sweep (ICMP Scan)

- purpose : To identify which hosts are active (alive) on a network.
- How it works : It sends ICMP Echo Request packets (like a ping) to multiple IP addresses. If a host replies, it is considered live.
- Tools Used : Nmap , Angry IP Scanner
- Example : Scanning a subnet (e.g, 192.168.1.0 /24) to find all devices currently connected and responsive.

Q.5) What is banner grabbing and name one tool used and its purpose

→ * What is Banner Grabbing -

Banner grabbing is a technique used in ethical hacking and penetration testing to collect information from network services running on open ports of a target system. When a connection is made to a network service (such as a web server, FTP server, or mail server), it often responds with a banner - a message that may include the software name, version, and sometimes the operating system.

Tool Used :

Tool Name : Netcat (nc)

- Purpose :

Netcat is used to connect to a specific port on a target system and retrieve the service

banner, helping in identifying the running Software and its version for Security Analysis.

- Netcat is a powerful network utility used for reading from and writing to network connections. It can be used for banner grabbing by manually collecting to a Service port and reading the banner information sent back by the Service.

- Example Usage:

Bash

```
nc target_ip 80
```

This command connects to a web server on port 80. If the Server is configured to send a banner, it might return something like:

```
HTTP/1.1 200 OK
Server: Apache/2.4.41 (Ubuntu)
```