Dr. D. Y. Patil Institute of Management & Entrepreneur Development
LIBRARY

April - May - 2026

Total No. of Questions : 5]

SEAT No. :

PF-5662

[Total No. of Pages : 3

[6651] - 39
M.C.A. (Management)
EH617MJ : Ethical Hacking
(2024 Pattern) (Semester - III)

Time : 2½ Hours] *[Max. Marks : 50*

Instructions to the candidates :

1) *All questions are compulsory*
2) *Figures to the right indicate full marks.*

Q1) Solve any Two :

a) Describe ethical hacking and its importance in modern cyber security? **[5]**

b) Distinguish between red team and blue team of ethical Hacking. **[5]**

c) Explain how does ethical hacking improve the security posture of a company. **[5]**

Q2) Solve any One :

a) You are a network administrator and your company received suspicious emails from a domain example.com. You need to investigate the domain registration details to identify the source as well as need to troubleshoot issues with the domain resolving incorrectly in your network. Your organization's security team wants to check for open ports on example.com to ensure there are no exposed services. You are requested to make use of appropriate tools like who is, lookup and Nmap and provide the appropriate commands. **[10]**

P.T.O.

SPPUQuestionPapers.com

b) As an ethical hacker you are advised to identify the following stub to exploit the vulnerabilities for footprinting the websites. **[10]**

i) Find login or admin portals of a website to understand potential entry points (authorized testing only)

ii) Identify documents (PDFs, word files, spreadsheets) that may contain sensitive data such as employee manuals, reports or emails.

iii) Check for misconfigured servers exposing backups, configuration files, or source code.

iv) Identify additional subdomain of the target domain to get a broader picture of infrastructure.

v) Determine the technologies, servers, or CMS used by a target site.

Q3) Solve any One :

a) You are provided with a lab virtual machine hosting an FTP server running VSftpd 2.3.4, which contains a known backdoor vulnerability, Your task is to exploit this service, using metasploit to gain access to the target system. **[10]**

Instructions :

i) Identify the vulnerable service and confirm it is running Vsftpd 2.3.4

ii) Use metasploit to select the appropriate exploit module.

iii) Configure the necessary options, including target IP and payload.

iv) Execute the exploit and obtain a meterpreter session.

v) Document the steps taken and the commands used.

b) You have successfully exploited a windows machine via a metasploit exploit for an unpatched vulnerability. Your goal is to maintain access without raising suspicious and be able to pivot into the internal network. Main objectives are to maintain a persistent backdoor, cover tracks to avoid detection and pivot to other machines in the same network. make your own asssumptions wherever required. **[10]**