Code No: **R204105K**   **R20**   Set No. 1

IV B.Tech I Semester Regular Examinations, January– 2024
ETHICAL HACKING
(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours   **Max. Marks: 70**

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks
*****

UNIT - I

1 a) What is hacking? What are types of hacking? Explain briefly.   [7]
   b) Explain phases of hacking with the help of a diagram.   [7]
                                   (OR)
2 a) What are different categories of penetration testing?   [7]
   b) Discuss the complete structure of penetrating testing report.   [7]

UNIT - II

3 a) Define foot printing. Discuss any two foot printing tools.   [7]
   b) Describe various foot printing techniques used in Ethical Hacking.   [7]
                                   (OR)
4 a) Discuss various techniques of scanning.   [7]
   b) What is scanning? Discuss the three types of scanning.   [7]

UNIT - III

5 a) Differentiate between manual password cracking and automated passwords
      cracking.   [7]
   b) Explain the process of system cracking with a neat sketch.   [7]
                                   (OR)
6 a) What is Trojan? Explain the working of Trojan.   [7]
   b) Elaborate on Trojan infection techniques.   [7]

UNIT - IV

7 a) Elaborate on various types of session hijacking? Give their merits and   [7]
      demerits.
   b) How does identity theft differ from financial fraud? Give a case study.   [7]
                                   (OR)
8 a) Explain the process of social engineering with a neat diagram.   [7]
   b) Discuss the social Engineering tool kit (SET) merits and demerits.   [7]

UNIT - V

9 a) Explain vulnerability assessment in detail.   [7]
   b) How does watermarking safeguard data? Describe.   [7]
                                   (OR)
10 a) Describe the use of hash functions in cryptography and ethical hacking   [7]
   b) Elaborate on the steganography methods and attacks.   [7]

|''|''|||''|''|||'|

IV B.Tech I Semester Regular Examinations, January– 2024
ETHICAL HACKING
(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours   Max. Marks: 70

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks
*****

UNIT - I

1	a)	What are ports? List some useful ports.	[7]
	b)	What are Protocols? Explain any three widely used protocols.	[7]

(OR)

2	a)	Explain various steps in the installation of Kali LINUX.	[7]
	b)	Give the significance of virtual machine and explain some virtualization softwares.	[7]

UNIT - II

3	a)	What are the objectives of foot printing? Explain External foot printing.	[7]
	b)	Why does attacker need foot printing? Discuss the use of "Whois" in detail.	[7]

(OR)

4	a)	Explain flagscan using hPing3 with suitable examples.	[7]
	b)	Describe Xmas scan and ICMP echo scan.	[7]

UNIT - III

5	a)	What is virus? Explain the working of virus.	[7]
	b)	Give the characteristics of virus attacks. Mention the threats from a virus attack.	[7]

(OR)

6	a)	Discuss manual and automated password cracking.	[7]
	b)	Differentiate amongst Trojan, virus, worm and attack.	[7]

UNIT - IV

7	a)	What are various types of sniffing? Explain some active sniffing techniques.	[7]
	b)	What is phishing? Mention some types of phishing attacks.	[7]

(OR)

8	a)	Explain identity theft in detail. Give its implications.	[7]
	b)	Describe the step by step procedure to be followed in session hijacking.	[7]

UNIT - V

9	a)	Discuss the role of digital signatures in cryptography.	[7]
	b)	Give the features of The Open Web Application Security Project (OWASP).	[7]

(OR)

10	a)	Describe the process of steganography with a neat sketch.	[7]
	b)	How Damn Vulnerable Web Application (DVWA) is installed and tested?	[7]

Code No: **R204105K**

R20

Set No. 3

IV B.Tech I Semester Regular Examinations, January– 2024
ETHICAL HACKING
(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours   **Max. Marks: 70**

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks
*****

UNIT - I

1 a) Describe the steps to be followed in web application penetration testing.   [7]
   b) Explain the network penetration testing. How is it differing from other types? [7]
                                    (OR)
2 a) What is Kali LINUX? Explain its included tools and supported platforms.   [7]
   b) What is Virtualization? Briefly explain some virtualization software.   [7]

UNIT - II

3 a) Compare and contrast active and passive foot printing.   [7]
   b) Explain the use of nsLookup in windows command line with suitable   [7]
      examples.
                                    (OR)
4 a) What is the objective of scanning? Elaborate on vulnerability scanning.   [7]
   b) Explain port scanning using Nmap.   [7]

UNIT - III

5 a) Draw the lifecycle of virus? give the classification of virus.   [7]
   b) What is Trojan? Explain the working of Trojan.   [7]
                                    (OR)
6 a) Explain password cracking in detail. What countermeasures need to be taken   [7]
      to withstand with password cracking?
   b) Write a short note on virus construction kit.   [7]

UNIT - IV

7 a) What are various tools available for session hijacking? Give their features. [7]
   b) What is the difference between data theft and identity theft? Explain with an [7]
      example.
                                    (OR)
8 a) Discuss human based and computer based social engineering techniques.   [7]
   b) What is sniffing? Compare active with passive sniffing techniques.   [7]

UNIT - V

9 a) What are the requirements of watermark? Give its limitations.   [7]
   b) List and explain the major challenges of Steganography.   [7]
                                    (OR)
10   What are the five types of vulnerability assessments? What questions need to
      be asked during vulnerability assessment?   [14]

|''|''|||''|''|||'|

Code No: **R204105K**   **R20**   Set No. 4

IV B.Tech I Semester Regular Examinations, January– 2024
ETHICAL HACKING
(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours   **Max. Marks: 70**

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks
*****

UNIT - I
1 a) Differentiate between web application penetration testing and mobile application penetration testing. [7]
  b) Describe the procedure for report writing of penetration testing. [7]

(OR)

2 a) Outline the included tools and supported platforms of Kali LINUX. [7]
  b) Explain various network types? Mention and explain widely used protocols. [7]

UNIT - II
3 a) Compare Internal foot printing with external foot printing [7]
  b) Explain the use of ping tool for foot printing. [7]

(OR)

4 a) Compare and contrast remote scanning with port scanning. [7]
  b) How do hackers scan for vulnerability? Explain. [7]

UNIT - III
5 a) Write short notes on Keyloggers and describe how do they affect the system? [7]
  b) Explain the working of Trojans and Backdoors. [7]

6 a) What are the various ways in which a system can be hacked? Explain them. [7]
  b) Explain the infection techniques of Trojan. [7]

UNIT - IV
7 a) Differentiate between human based social engineering and computer based social engineering. [7]
  b) How packet analysis does causes a threat to user community? Explain. [7]

(OR)

8 What types of social engineering attacks can be simulated via social engineering tools? Explain with examples. [14]

UNIT - V
9 a) What techniques are used in steganography? Explain them. [7]
  b) What are the merits and demerits of DVWA? [7]

(OR)

10 What services are provided through OWASP? What tool does OWASP provide that can be used to find vulnerabilities? [14]

|"|"|||"|"|||'|