Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree Regular and Supplementary Examination December 2023 (2019 Scheme)

Course Code: CCT401

Course Name: ETHICAL HACKING

Max. Marks: 100 **Duration: 3 Hours**

PART A

Answer all questions, each carries 3 marks. Marks

1		List the elements of information security.	(3)
2		Define the role of a penetration tester.	(3)
3		What are two goals of social engineering?	(3)
4		Give the preventive measures for dumpster diving.	(3)
5		Illustrate the types of exploits with example	(3)
6		How to detect **Man in the Middle** Attacks.	(3)
7		Define the security challenges with routers.	(3)
8		List the generations of firewall.	(3)
9		How can we hide evidence by altering logs?	(3)
10		Define horizontal escalation technique.	(3)

PART B

Answer any one full question from each module, each carries 14 marks.

Module I

11	a)	Explain the four modules in OSSTMM.	(6)
	b)	Describe the security risk reported using OWASP.	(8)

OR

12	a)	Illustrate the six security challenges in information security.	(6)
	b)	Explain vulnerability assessment and its types.	(8)

Module II

13	a)	Compare virus and worms.	(8)
	b)	Explain **Denial-of-Service** attacks and its types.	(6)

OR

14	a)	Differentiate proxy and packet firewalling.	(6)
	b)	Explain scanning method in footprinting and its types.	(8)

Module III

15	a)	Illustrate the classifications of remote attacks.	(6)
	b)	Explain the method of brute force attack and its types.	(8)

OR

16	a)	Describe the types of network sniffers.	(6)
	b)	With an example, How an attacker breaks the confidentiality using SMTP.	(8)

Module IV

17	a)	Compare the advantages and disadvantages of Routers and Honeypots	(8)
	b)	Describe the working of a Web Server.	(6)

OR

18	a)	Explain the working of Cross-Site scripting technique.	(6)
	b)	What happens when a mobile phone is hacked? How can we prevent it?	(8)

Module V

19	a)	Describe the five primary methods used in hiding files.	(6)
	b)	Explain the process of privilege escalation with figure.	(8)

OR

20	a)	Explain about system hacking.	(8)
	b)	Describe the methods used in hiding evidence on network.	(6)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree (R, S) Examination November 2024 (2019 Scheme)

Course Code: CCT401

Course Name: ETHICAL HACKING

Max. Marks: 100 **Duration: 3 Hours**

PART A

Answer all questions, each carries 3 marks. Marks

1		Give definitions for the information security components.	(3)
2		What is vulnerability assessment in penetration testing?	(3)
3		Define social engineering and give an example.	(3)
4		What is shoulder surfing in the context of social engineering attacks?	(3)
5		What is ARP spoofing, and how does it work?	(3)
6		Define Man-in-the-Middle (MITM) attacks.	(3)
7		What is SQL injection, and how does it affect web applications?	(3)
8		What is session hijacking, and how does it threaten web applications?	(3)
9		What is event logging in the context of cybersecurity?	(3)
10		Explain the concept of password cracking.	(3)

PART B

Answer any one full question from each module, each carries 14 marks.

Module I

11	a)	What are the main types of hackers, and how do they differ from ethical hackers?	(6)
	b)	Explain in detail the categories of penetration tests with relevant examples.	(8)

OR

12	a)	Compare the OSSTMM and NIST penetration testing methodologies.	(6)
	b)	Discuss the effects of hacking on individuals, organizations, and society.	(8)

Module II

13	a)	What are the key tools used for footprinting during reconnaissance?	(6)
	b)	Explain how social engineering attacks like piggybacking can compromise organizational security.	(8)

OR

14	a)	Explain the concept of denial-of-service (DoS) attacks.	(6)
	b)	What are the differences between Trojans and backdoors, and how do they affect network security?	(8)

Module III

15	a)	Describe how remote exploitation works in the context of network attacks.	(6)
	b)	Explain the steps involved in conducting an MITM attack, including session hijacking.	(8)

OR

16	a)	What are brute force attacks, and how do they compromise system security?	(6)
	b)	How does ARP spoofing lead to denial-of-service attacks, and what are its countermeasures?	(8)

Module IV

17	a)	Discuss the role of routers and firewalls in protecting a network.	(6)
	b)	Explain the process of reverse engineering and how it is used in identifying vulnerabilities.	(8)

OR

18	a)	What is buffer overflow, and what are its implications in web security?	(6)
	b)	Describe the steps involved in writing an exploit and its potential risks.	(8)

Module V

19	a)	Discuss the methods used to hide files and cover tracks in system hacking.	(6)
	b)	Explain the importance of password cracking techniques in system hacking and ways to mitigate such attacks.	(8)

OR

20	a)	How can network evidence be hidden by attackers?	(6)
	b)	Describe the techniques used by attackers to cover their tracks after gaining access to a system.	(8)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree 7th semester (S,FE) Exam April 2025 (2019 Scheme)

Course Code: CCT401

Course Name: ETHICAL HACKING

Max. Marks: 100 **Duration: 3 Hours**

PART A

Answer all questions, each carries 3 marks.

		Marks
1	What is the difference between a hacker and an ethical hacker?	(3)
2	Briefly explain the concept of non-repudiation in information security.	(3)
3	What is Google hacking, and how is it used in ethical hacking?	(3)
4	What is dumpster diving in social engineering attacks?	(3)
5	What are exploit databases, and why are they important for attackers and defenders?	(3)
6	What is network sniffing, and what are its types?	(3)
7	What is cross-site scripting (XSS)?	(3)
8	What is the difference between IDS and IPS in network security?	(3)
9	Define the process of hiding evidence by altering event logs.	(3)
10	What is privilege escalation?	(3)

PART B

Answer any one full question from each module, each carries 14 marks.

Module I

11	a)	Explain the role of security and penetration testers.	(6)
	b)	Describe the OWASP methodology for penetration testing and its significance in web application security.	(8)

OR

12	a)	Discuss the security challenges faced by organizations today.	(6)
	b)	How does non-repudiation enhance security in online communication systems?	(8)

Module II

13	a)	Discuss the differences between viruses and worms.	(6)
	b)	Discuss the importance of competitive intelligence in the reconnaissance phase of penetration testing.	(8)

OR

14	a)	What is the role of proxy and packet filtering in network security?	(6)
	b)	Describe the process of scanning and enumeration in ethical hacking and their importance in gathering network information	(8)

Module III

15	a)	Explain the concept of DNS spoofing and its consequences.	(6)
	b)	Discuss the various types of sniffing techniques and their impact on network security.	(8)

OR

16	a)	Explain how weak authentication can lead to successful network attacks.	(6)
	b)	How does ARP spoofing lead to denial-of-service attacks, and what are its countermeasures?	(8)

Module IV

17	a)	What is web filtering, and how does it enhance security?	(6)
	b)	Discuss the techniques used in penetration testing for web servers and their impact on security.	(8)

OR

18	a)	What is buffer overflow, and what are its implications in web security?	(6)
	b)	How can incident handling and response procedures mitigate the effects of a security breach?	(8)

Module V

19	a)	How can attackers manipulate event logs to avoid detection?	(6)
	b)	Discuss the various methods used to escalate privileges in a compromised system.	(8)

OR

20	a)	What are the defenses used to protect log and accounting files from tampering?	(6)
	b)	How can incident responders detect and respond to log and event file manipulation during an investigation?	(8)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree (S, FE) Examination May 2024 (2019 Scheme)

Course Code: CCT401

Course Name: ETHICAL HACKING

Max. Marks: 100 **Duration: 3 Hours**

PART A

Answer all questions, each carries 3 marks. Marks

1		List the steps involved in penetration testing.	(3)
2		Give the three dimensions in vulnerability assessment.	(3)
3		Define the steps for the social engineering attack cycle.	(3)
4		What are the protective measures taken to avoid shoulder surfing?	(3)
5		Illustrate the types of network sniffing.	(3)
6		Illustrate the types of exploits.	(3)
7		Explain the architecture of a router.	(3)
8		What are the two main types of honeypots?	(3)
9		How can we examine encrypted files?	(3)
10		Define vertical escalation technique.	(3)

PART B

Answer any one full question from each module, each carries 14 marks.

Module I

11	a)	Explain the categories of hackers with examples.	(8)
	b)	Explain the types of penetration testing.	(6)

OR

12	a)	Describe the functions and their categories of NIST.	(8)
	b)	How will be the effect of hacking affects our society.	(6)

Module II

13	a)	Explain footprinting and its types.	(8)
	b)	Describe piggybacking.	(6)

OR

14	a)	Explain enumeration and its categories.	(8)
	b)	Compare trojan and backdoors.	(6)

Module III

15	a)	How can we manipulate DNS Records using DHCP spoofing technique?	(6)
	b)	Explain the different types of **Man in the Middle** attacks.	(8)

OR

16	a)	Describe the working of session hijacking.	(6)
	b)	Explain the top sources of vulnerability databases.	(8)

Module IV

17	a)	Explain Bluetooth hacking and its types.	(6)
	b)	Describe the process of incident response with its steps.	(8)

OR

18	a)	Explain the different techniques used in e-mail hacking?	(6)
	b)	Describe the process of reverse engineering with its stages and tools.	(8)

Module V

19	a)	Explain the six default categories to classify event logs.	(6)
	b)	Illustrate how can cover tracks and hide it?	(8)

OR

20	a)	What are defenses against logs and accounting file attacks?	(6)
	b)	With diagram explain password sniffing method.	(8)

****