Reg. No.																

Question Paper Code	**13216**

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2024

Seventh Semester

Computer Science and Engineering

20CSEL705 - ETHICAL HACKING

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (MCQ) (20 × 1 = 20 Marks)

Answer ALL Questions

		Marks	*K – Level*	*CO*
1.	Which term refers to the weaknesses in a system that can be exploited by threats? (a) Threat (b) Vulnerability (c) Attack (d) Exploit	*1*	*K1*	*CO1*
2.	Which type of attack involves sending unsolicited messages to many recipients at once? (a) Phishing (b) Spam (c) Spoofing (d) Sniffing	*1*	*K1*	*CO1*
3.	Which tool is commonly used for network scanning and enumeration? (a) Wireshark (b) Nmap (c) Meta sploit (d) John the Ripper	*1*	*K1*	*CO1*
4.	Spoofing attacks often exploit vulnerabilities in _____ protocols to impersonate legitimate entities. (a) Application Layer (b) Network Layer (c) Transport Layer (d) Presentation Layer	*1*	*K1*	*CO2*
5.	Which protocol from the options listed below is not vulnerable to sniffing? (a) HTTP (b) SMTP (c) POP (d) TCP	*1*	*K1*	*CO2*
6.	How can buffer overflow vulnerabilities affect a program? (a) They can cause the program to crash (b) They can allow unauthorized code execution (c) They can lead to data corruption (d) All of the above	*1*	*K1*	*CO2*
7.	Which vulnerability scanner is specifically known for detecting and reporting vulnerabilities like SQL injection and XSS? (a) ZAP (b) Nikto (c) Nessus (d) Acunetix	*1*	*K1*	*CO3*
8.	What is the main function of Hashcat? (a) Browser Exploitation (b) Password Recovery (c) Proxy Testing (d) Server Scanning	*1*	*K1*	*CO3*
9.	How many main types of Cross-Site Scripting (XSS) vulnerabilities exist? (a) 1 (b) 2 (c) 3 (d) 4	*1*	*K1*	*CO3*
10.	Which of the following exploits does an attacker insert malicious code into a link that appears to be from a trustworthy source? (a) XSS (b) Command injection (c) Path traversal attack (d) Buffer overflow	*1*	*K1*	*CO4*
11.	Which Web application firewalls (WAFs) help prevent which application layer attacks? (a) SQL injection (b) DDoS (c) XSS (d) All of the above	*1*	*K1*	*CO4*
12.	Web application security is not required for finance applications. (a) True (b) False	*1*	*K1*	*CO4*
13.	A _______ attack captures valid authentication data and reuses it to impersonate a legitimate user. (a) Brute Force (b) Replay (c) Phishing (d) Credential Stuffing	*1*	*K1*	*CO5*
14.	You’re shopping online, but just as you're about to pay, the website freezes. Minutes later, you notice strange purchases made using your session. What attack could have intercepted your data as you browsed? (a) SQL Injection (b) Man-in-the-Middle Attack (c) IP Spoofing (d) Replay Attack	*1*	*K1*	*CO5*
15.	Which of the following measures can mitigate the risk of brute-force attacks by limiting login attempts? (a) Enforcing strong password policies (b) Using unpredictable session identifiers (c) Implementing account lockout mechanisms (d) Allowing users to create complex passwords with special characters	*1*	*K1*	*CO5*

16. Illustrate how the web pages can help attackers gather _____ that is useful for identification attacks. *1 K2 CO5*

(a) Personal emails (b) Medical records (c) Employment history (d) Encrypted data

17. What action can attackers perform using keystroke logging scripts in xss attacks? *1 K1 CO6*

(a) Modify server-side code (b) Change the website's theme
(c) Capture user input like passwords (d) Enable two-factor authentication

18. Which of the following is the least secure method of authentication? *1 K1 CO6*

(a) Key card (b) Fingerprint (c) Retina pattern (d) Password

19. What are the common security threats? *1 K1 CO6*

(a) File Shredding (b) File sharing and permission
(c) File corrupting (d) File integrity

20. Stored XSS vulnerabilities are also known as _____ XSS vulnerabilities. *1 K1 CO6*

(a) Persistent (b) Non-persistent (c) Backup (d) Log

PART - B (10 × 2 = 20 Marks)

Answer ALL Questions

21. Define the term "Threat" in the context of cyber security. *2 K1 CO1*
22. What is meant by "Attack" in network security? *2 K1 CO1*
23. Differentiate between sniffing and spoofing. *2 K2 CO2*
24. List out the different types of spoofing attacks. *2 K1 CO2*
25. What is SQL Injection? *2 K1 CO3*
26. Compare SQL injection attack and Cross Site Scripting attack. *2 K2 CO3*
27. Define HTTP Protocol. *2 K1 CO4*
28. Define Request and Response. *2 K1 CO4*
29. What are flaws? *2 K1 CO5*
30. Define Content Security Policy (CSP). *2 K1 CO6*

PART - C (6 × 10 = 60 Marks)

Answer ALL Questions

31. a) Describe the phases involved in ethical hacking. Provide a detailed explanation of each phase, including foot printing, scanning, system hacking and session hijacking. *10 K2 CO1*

OR

b) Discuss the effectiveness of various session hijacking prevention techniques. Which techniques are most effective, and why? *10 K2 CO1*

32. a) Explain about ARP Poisoning and describe various types of ARP Poisoning Attack. *10 K2 CO2*

OR

b) Explain in detail about various types of Man-in-the-Middle attack and also discuss how to detect and prevent from Man-in-the-Middle attack. *10 K2 CO2*

33. a) Describe in detail about Web application threats. *10 K2 CO3*

OR

b) Summarize about SQL Injection attack and its types. *10 K2 CO3*

34. a) Explain briefly about the types of Session Management. *10 K2 CO4*

OR

b) Demonstrate in detail about Server Side functionality technologies (Java, ASP, PHP). *10 K2 CO4*

35. a) List the types of password attacks and explain how to prevent password attacks. *10 K2 CO5*

OR

b) Explain in detail about Authentication Technologies. *10 K2 CO5*

36. a) Discuss in detail about DOM-based Cross-Site Scripting. *10 K2 CO6*

OR

b) Explain about HTTP header injection. *10 K2 CO6*