


<b>Name:</b> <b>Enrolment No:</b>			
<p style="text-align: center;"><b>UPES</b>  <b>End Semester Examination, May 2025</b></p> <p> <b>Course: Ethical Hacking &amp; Penetration Testing</b>  <b>Program: B. Tech CSE (H+NH)_All</b>  <b>Course Code: CSSF3023</b> </p> <p style="text-align: right;"> <b>Semester: VI</b>  <b>Time : 03 hrs.</b>  <b>Max. Marks: 100</b> </p> <p><b>Instructions: Attempt all questions, mention examples &amp; draw diagrams if required.</b></p>			
<b>SECTION A</b> <b>(5Qx4M=20Marks)</b>			
<b>S. No.</b>		<b>Marks</b>	<b>CO</b>
Q 1	Describe Threat Maps, how are they useful in understanding real-time attack trends, mention four threat map links as examples?	<b>4</b>	<b>CO1</b>
Q2	Differentiate between White Hat, Black Hat, and Grey Hat hackers with suitable examples.	<b>4</b>	<b>CO1</b>
Q3	List and explain four major types of online cybercrimes with examples.	<b>4</b>	<b>CO1</b>
Q4	What is the Information Technology Act, 2000 (India)? Mention two key provisions.	<b>4</b>	<b>CO2</b>
Q5	What is meant by Digital Certificates, explain their role in securing online communications.	<b>4</b>	<b>CO3</b>
<b>SECTION B</b> <b>(4Qx10M= 40 Marks)</b>			
Q 6	Describe the evolution of Cyberattacks from early viruses to new-age attacks with examples. Include a timeline or flowchart to support your answer.	<b>10</b>	<b>CO2</b>
Q7	Explain how you would identify threats at different layers – Operating System, Applications, Network, and Database with examples for each.	<b>10</b>	<b>CO1</b>
Q8	Discuss OWASP Top 10 vulnerabilities. Choose any 5 vulnerabilities and explain with examples and potential security solutions.	<b>10</b>	<b>CO1</b>
Q9	Compare and contrast Vulnerability Assessment and Penetration Testing. Include their stages, methods, and the use of tools (manual/automated) to present the answer.	<b>10</b>	<b>CO1</b>

**SECTION-C**  
**(2Qx20M=40 Marks)**

Q 10	<p>You are assigned to test the security of a Metasploitable2 instance hosted on a virtual machine. Describe how you would:</p> <ol style="list-style-type: none"> <li>Set up the testing environment</li> <li>Perform Vulnerability Assessment</li> <li>Perform Penetration Testing</li> <li>Document the findings.</li> </ol> <p>Assume that the Gateway IP is 192.168.119.1, DHCP/DNS server is 192.168.119.2, Attacker IP is 192.168.119.11 and Metasploitable2 IP is 192.168.119.12. Include detailed process you would follow with steps, diagrams.</p>	<b>20</b>	<b>CO3</b>
Q11	<p>Assume your organization has been targeted by a phishing campaign. As a Cybersecurity analyst, prepare a response plan including how to detect the phishing attempt, prevent user compromise and remediate the systems. Include detection techniques, use of honeypots if applicable, and user awareness strategies.</p> <p>OR</p> <p>Illustrate the working of HTTP v/s HTTPS. How are SSL/TLS protocols used in securing online communication. Include the process of certificate issuance, the handshake protocol, encryption mechanisms with a use case (your laptop connecting to HDFC bank over the Internet).</p>	<b>20</b>	<b>CO2</b>