2/66 **2504E179** Candidate's Seat No :________

Integrated M.Sc. Cybersecurity & Forensics Semester- 6 (External)

ICSF – 307

VAPT - Vulnerability Assessment and Penetration Testing

Duration: 2hr 30min **April-2024** **Total Max. 70**

Instructions: Illustrate your answers with neat diagrams wherever necessary.

Que 1 Write the following

(i) Discuss the importance of vulnerability assessment in risk prevention and compliance requirements. (7 Marks)

(ii) **Scenario Based Question:** (7 Marks)
You are the lead cybersecurity analyst for a large financial institution responsible for overseeing the vulnerability management process. Recently, your team conducted a comprehensive vulnerability assessment across the organization's network infrastructure. During the assessment, several critical vulnerabilities were identified across various hosts, including servers, workstations, and network devices. As part of your role, you need to guide your team through the stages of vulnerability management to effectively address these vulnerabilities.

Question:

(i) Outline the stages of vulnerability management that your team should follow to address the critical vulnerabilities identified during the assessment.

(ii) Provide a detailed explanation of each stage and discuss the importance of prioritization and remediation in mitigating security risks within a financial institution's environment.

OR

(i) Analyze the importance of having direct connectivity without a firewall during a vulnerability scan. (7 Marks)

(ii) Describe the difference between a vulnerability scan and a penetration test. (7 Marks)

Que 2 Write the following

(i) Explain the process and significance of false positive analysis in vulnerability management. (7 Marks)

(ii) Given a scenario where a web application allows unfiltered user input, discuss how an attacker might exploit this to perform a SQL injection attack. (7 Marks)

OR

(i) Discuss the implications of false positives in vulnerability scanning and how they affect security assessment. (7 Marks)

(ii) Critically analyze a scenario where buffer overflow vulnerabilities could lead to significant security breaches. (7 Marks)

Que 3 Write the following

(i) Explain the differences and benefits of Black Box, White Box, and Fuzz testing methodologies. (7 Marks)

(ii) Explain the importance of configuration and setup in using VirtualBox for penetration testing simulations. (7 Marks)

P.T.O

E 179.2

OR

(i) Explain the importance of configuration and setup in using VirtualBox for penetration testing simulations. (7 Marks)

(ii) Describe how end-user behaviour can impact the security of a system and how penetration testing can address this issue. (7 Marks)

Que 4 Write the following

(i) Provide an analysis of a Web Application Test within the context of penetration testing types. (7 Marks)

(ii) Provide an analysis of the implications of social engineering attacks on corporate security. (7 Marks)

OR

(i) Discuss the role and effectiveness of tools such as Wireshark and OpenSSL in network services testing. (7 Marks)

(ii) Evaluate the effectiveness of Acunetix in a web application security testing case study. (7 Marks)

Que 5 Attempt any seven out of twelve (14 Marks)

(i) Which tool is primarily used for analyzing web application security?

(ii) Which stage of the Vulnerability Assessment and Penetration Testing life cycle involves identifying false positives?

(iii) The phase 'Assess' in vulnerability management mainly involves: __________

(iv) A sample PenTest report is useful for: _______

(v) Social Engineering Tests are primarily concerned with: ________

(vi) What is the purpose of 'Risk severity applicability analysis' in the context of vulnerability management?

(vii) ______tool is used for vulnerability exploitation.

(viii) Which tool is best suited for static code analysis? Explain Why?
A) Nmap B) Nessus C) Acunetix D) Burpsuite

(ix) What does Acunetix's AcuSensor Technology do?

(x) Which of the following is a unique scanning capability of Acunetix?

(xi) How does the Metasploit module `auxiliary/scanner/ssh/ssh_version` help in a penetration test?

(xii) Which phase of penetration testing focuses on gathering information without engaging the target system?