Final Assessment Test – November 202

VIT
Vellore Institute of Technology

Course: BCSE410L - Cyber Security
Class NBR(s): 1871/1877/1885/1894/1898/1903/1907/ 1909/1912/1921
Time: Three Hours

Slo
Ma

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREA MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions
(10 X 10 = 100 Marks)

1. Discuss the pivotal role of network infrastructure security, best practices to fortify the network defences and insights into common threats that could jeopardize the network.

2. Consider your team is developing a mobile application that handles sensitive user data. Illustrate how would you use attack tree analysis to evaluate potential threats specific to mobile applications? What considerations would you include for both the app's functionality and user data protection?

3. A security incident occurs when an unauthorized person gains access to your building by impersonating a maintenance worker. Elaborate on how would you address this incident and implement countermeasures to prevent similar occurrences in the future?

4. Provide a detailed overview of at least three password cracking tools, including their functionalities, use cases, and the types of attacks they can perform. Discuss the ethical implications of using these tools, particularly in penetration testing and security assessments.

5. Let assume that, a disgruntled employee installs a keylogger on their colleague's workstation to steal sensitive information.
   a) What signs might indicate that an insider threat involving a keylogger is present?
   b) What preventive measures can organizations implement to minimize the risk of insider threats related to keyloggers?
   c) How should the organization handle the incident once it is discovered?

6. Following a data breach, an organization conducts a comprehensive scan of its network to identify potential vulnerabilities exploited during the attack.

a) What specific indicators of compromise should the organization focus on during the network scan?

b) Discuss the tools that could be employed for this post-breach analysis and their effectiveness in identifying remnants of the attack.

7. A company implements a BYOD (Bring Your Own Device) policy, and the IT team is concerned about rogue devices spoofing legitimate MAC addresses to access sensitive resources. Describe the potential risks of allowing personal devices on the corporate network concerning MAC spoofing and effective countermeasures the organization can implement to prevent MAC spoofing in a BYOD environment.

8. The organization is concerned about the security of data transmitted over its wireless network and is considering implementing stronger encryption. Summarise the encryption standards should the organization adopt to enhance wireless security and why legacy protocols should be avoided?

9.a) Discuss the technical details and potential impacts of a successful null session and missing patches attack on an organization's network.

OR

9.b) A company's e-commerce website has been reported to be vulnerable to SQL injection attacks. Explain the steps would you take to identify if the website is indeed vulnerable to SQL injection? Describe the testing methods you would use.

10.a) The organization plans to engage third-party vendors that will have access to its databases for data processing. What security assessments should be conducted on third-party vendors to evaluate their database security practices?

OR

10.b) A mobile application collects user input through various forms, including chat features and comment sections. Explain the input filtering risks should developers be aware of when designing these features for mobile applications.

⇔⇔⇔ I/L/TX ⇔⇔⇔