Program: BE Computer Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester VII

Course Code: CSDLO7031 and Course Name: Advanced System Security and Digital Forensics

Time: 1 hour Max. Marks: 50

Note to the students:- All the Questions are compulsory and carry equal marks .

|  |  |
| --- | --- |
| Q1. | When a cyber attacker knows the type of person he is attacking and tries to break the passwords using the victim's date of birth, pets name, etc. What kind of attack is this? |
| Option A: | Dictionary Attacks |
| Option B: | Inferring Passwords Likely for a User |
| Option C: | Brute Force Attacks |
| Option D: | Exhaustive Attacks |
|  |  |
| Q2. | The given diagram showcases what type of security model/management?  Security models Lecture Note 11 Contents |
| Option A: | Biba |
| Option B: | Federated Identity |
| Option C: | Single Sign-on |
| Option D: | Bell Lapadula |
|  |  |
| Q3. | The given diagram showcases what type of security model/management?  RSA Federated Identity Manager | TokenGuard.com |
| Option A: | Biba |
| Option B: | Federated Identity |
| Option C: | Single Sign-on |
| Option D: | Bell Lapadula |
|  |  |
| Q4. | By mitigating it is meant that, |
| Option A: | The harm should be made less severe |
| Option B: | Causing of the harm should be made difficult |
| Option C: | The harm should be stopped from happening |
| Option D: | Virus Attack |
|  |  |
| Q5. | A method to confine users to one side of a boundary is called: |
| Option A: | Compound |
| Option B: | Firewall |
| Option C: | Fence |
| Option D: | Back Door |
|  |  |
| Q6. | When one or more extra bits are given to identify the access rights to that word, it is called as |
| Option A: | Based and Bound Registers |
| Option B: | Tagged Architecture |
| Option C: | Fence |
| Option D: | Back Door |
|  |  |
| Q7. | Worms are: |
| Option A: | Non-Malicious Codes |
| Option B: | Malicious Codes |
| Option C: | Targeted Malicious Code |
| Option D: | Selectively malicious |
|  |  |
| Q8. | Covert Channels are: |
| Option A: | Non-Malicious Codes |
| Option B: | Malicious Codes |
| Option C: | Targeted Malicious Code |
| Option D: | Selectively malicious |
|  |  |
| Q9. | This attack can be deployed by infusing a malicious code in a website’s comment section. What is “this” attack referred to here? |
| Option A: | SQL injection |
| Option B: | HTML Injection |
| Option C: | Cross Site Scripting (XSS) |
| Option D: | Cross Site Request Forgery (XSRF) |
|  |  |
| Q10. | \_\_\_\_\_\_\_ Protocol under SSL indicated that the upcoming data is protected. |
| Option A: | Record Protocol |
| Option B: | Change Cipher Spec |
| Option C: | Alert |
| Option D: | Handshake |
|  |  |
| Q11. | Privileges of trusted user is used in which attack? |
| Option A: | Cross Site Scripting |
| Option B: | Account Harvesting |
| Option C: | Cross Site Request Forgery |
| Option D: | Phishing |
|  |  |
| Q12. | The session token could be compromised in different ways; the most common are:  Predictable session token  Session Sniffing  Man-in-the-middle attack |
| Option A: | i and ii |
| Option B: | ii and iii |
| Option C: | i and iii |
| Option D: | i, ii and iii |
|  |  |
| Q13. | IEEE 802.11i is called as |
| Option A: | Wired Equivalent Security |
| Option B: | Robust Security Protocol |
| Option C: | Robust Security Network |
| Option D: | Wired Equivalent Protocol |
|  |  |
| Q14. | Error detection is performed at which level of IEEE 802 |
| Option A: | Physical |
| Option B: | Medium Access Control |
| Option C: | Logical Link Control |
| Option D: | Transport |
|  |  |
| Q15. | IEEE 802 committee was formed for developing which standards |
| Option A: | LAN |
| Option B: | WLAN |
| Option C: | WEP |
| Option D: | WPA |
|  |  |
| Q16. | IEEE 802.11i has come out with what protocol |
| Option A: | HTTP |
| Option B: | WEP |
| Option C: | WPA |
| Option D: | WPA2 |
|  |  |
| Q17. | Which is generally considered as crime against Society |
| Option A: | Cyberterrorism |
| Option B: | Cyberdefamation |
| Option C: | Logic Bomb |
| Option D: | Pornographic offenses |
|  |  |
| Q18. | Which is generally considered as crime against organisation |
| Option A: | Phishing |
| Option B: | Cyberdefamation |
| Option C: | Logic Bomb |
| Option D: | Pornographic offenses |
|  |  |
| Q19. | The Intellectual property rights of Kolhapuri Chappal can be protected under\_\_\_\_\_\_\_\_\_\_. |
| Option A: | Patents |
| Option B: | Designs |
| Option C: | Copyrights |
| Option D: | Geographical Indications |
|  |  |
| Q20. | \_\_\_\_\_\_\_\_\_\_\_\_ generally evolves through court decisions |
| Option A: | Criminal and Civil Law |
| Option B: | Contract Law |
| Option C: | Tort Law |
| Option D: | Personal Law |
|  |  |
| Q21. | The three A’s in digital Forensics are  Acquire  Authenticate  Apply  Analyse  Appraise |
| Option A: | i, ii, and iii |
| Option B: | i, ii, and iv |
| Option C: | i, iii and v |
| Option D: | ii, iii and iv |
|  |  |
| Q22. | Forensic duplicate is stored is stored in what format? |
| Option A: | Original |
| Option B: | Raw |
| Option C: | JPEG |
| Option D: | HTML |
|  |  |
| Q23. | \_\_\_\_\_\_\_ adds significant amount of functionality in duplication like block based hashes and a progress indicator. |
| Option A: | dc |
| Option B: | dd |
| Option C: | dcfldd |
| Option D: | dfl |
|  |  |
| Q24. | A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a file that contains every bit of information from the source, but may be stored in an altered or changed form. |
| Option A: | Forensic Duplicate |
| Option B: | Qualified Forensic Duplicate |
| Option C: | Restored Image |
| Option D: | Mirror Image |
|  |  |
| Q25. | A system tool that enumerates all listening ports and all current connections to those ports |
| Option A: | Fport |
| Option B: | Pslist |
| Option C: | Netstat |
| Option D: | ipconfig |