|  |
| --- |
| **True / False** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. A risk management assessment is a systematic and methodical evaluation of the security posture of the enterprise.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2. TCP/IP uses a numeric value as an identifier to the applications and services on these systems.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3. The second step in a vulnerability assessment is to determine the assets that need to be protected.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4. Determining vulnerabilities often depends on the background and experience of the assessor.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5. Realistically, risks can never be entirely eliminated.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6. Each packet/datagram contains a source port and destination port.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7. Netstat displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and DNS settings.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8. Nslookup displays detailed information about how a device is communicating with other network devices.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9. Vulnerability scanning should be conducted on existing systems and particularly as new technology equipment is deployed.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10. In white box and gray box testing, the first task of the tester is to perform preliminary information gathering on their own from outside the organization, sometimes called open source intelligence (OSINT).   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |
| --- |
| **Multiple Choice** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. The goal of what type of threat evaluation is to better understand who the attackers are, why they attack, and what types of attacks might occur?   |  |  |  | | --- | --- | --- | |  | a. | threat mitigation | |  | b. | threat profiling | |  | c. | risk modeling | |  | d. | threat modeling | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. What is the name of the process that basically takes a snapshot of the current security of an organization?   |  |  |  | | --- | --- | --- | |  | a. | threat analysis | |  | b. | vulnerability appraisal | |  | c. | risk assessment | |  | d. | threat assessment | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. Which item below is the standard security checklist against which systems are evaluated for a security posture?   |  |  |  | | --- | --- | --- | |  | a. | profile | |  | b. | threat | |  | c. | control | |  | d. | baseline | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. During a vulnerability assessment, what type of software can be used to search a system for port vulnerabilities?   |  |  |  | | --- | --- | --- | |  | a. | threat scanner | |  | b. | vulnerability profiler | |  | c. | port scanner | |  | d. | application profiler | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. A port in what state below implies that an application or service assigned to that port is listening for any instructions?   |  |  |  | | --- | --- | --- | |  | a. | open port | |  | b. | empty port | |  | c. | closed port | |  | d. | interruptible system | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. An administrator running a port scan wants to ensure that no processes are listening on port 23. What state should the port be in?   |  |  |  | | --- | --- | --- | |  | a. | open port | |  | b. | secure port | |  | c. | hardened port | |  | d. | closed port | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. An administrator needs to view packets and decode and analyze their contents. What type of application should the administrator use?   |  |  |  | | --- | --- | --- | |  | a. | application analyzer | |  | b. | protocol analyzer | |  | c. | threat profiler | |  | d. | system analyzer | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. Which is the term for a computer typically located in an area with limited security and loaded with software and data files that appear to be authentic, yet they are imitations of real data files?   |  |  |  | | --- | --- | --- | |  | a. | port scanner | |  | b. | honeynet | |  | c. | honeypot | |  | d. | honeycomb | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. What is the term for a network set up with intentional vulnerabilities?   |  |  |  | | --- | --- | --- | |  | a. | honeynet | |  | b. | honeypot | |  | c. | honeycomb | |  | d. | honey hole | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. What is another term used for a security weakness?   |  |  |  | | --- | --- | --- | |  | a. | threat | |  | b. | vulnerability | |  | c. | risk | |  | d. | opportunity | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. Which scan examines the current security, using a passive method?   |  |  |  | | --- | --- | --- | |  | a. | application scan | |  | b. | system scan | |  | c. | threat scan | |  | d. | vulnerability scan | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What is the end result of a penetration test?   |  |  |  | | --- | --- | --- | |  | a. | penetration test profile | |  | b. | penetration test report | |  | c. | penetration test system | |  | d. | penetration test view | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. Which tester has an in-depth knowledge of the network and systems being tested, including network diagrams, IP addresses, and even the source code of custom applications?   |  |  |  | | --- | --- | --- | |  | a. | white box | |  | b. | black box | |  | c. | replay | |  | d. | system | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. What security goal do the following common controls address: hashing, digital signatures, certificates, nonrepudiation tools?   |  |  |  | | --- | --- | --- | |  | a. | confidentiality | |  | b. | integrity | |  | c. | availability | |  | d. | safety | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Which security procedure is being demonstrated if an administrator is using Wireshark to watch for specific inbound and outbound traffic?   |  |  |  | | --- | --- | --- | |  | a. | application search | |  | b. | application control | |  | c. | firewall monitoring | |  | d. | virus control | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. What type of scanner sends "probes" to network devices and examine the responses received back to evaluate whether a specific device needs remediation?   |  |  |  | | --- | --- | --- | |  | a. | active | |  | b. | non-intrusive | |  | c. | passive | |  | d. | intrusive | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. Which of the following is used to replicate attacks during a vulnerability assessment by providing a structure of exploits and monitoring tools?   |  |  |  | | --- | --- | --- | |  | a. | replication image | |  | b. | assessment image | |  | c. | penetration framework | |  | d. | exploitation framework | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. Select the vulnerability scan type that will use only the available information to hypothesize the status of the vulnerability.   |  |  |  | | --- | --- | --- | |  | a. | active | |  | b. | non-intrusive | |  | c. | passive | |  | d. | intrusive | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What type of penetration testing technique is used if the tester has no prior knowledge of the network infrastructure that is being tested?   |  |  |  | | --- | --- | --- | |  | a. | white box | |  | b. | gray box | |  | c. | black box | |  | d. | sealed box | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What type of reconnaissance is a penetration tester performing if they are using tools that do not raise any alarms?   |  |  |  | | --- | --- | --- | |  | a. | active | |  | b. | passive | |  | c. | invasive | |  | d. | evasive | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What process does a penetration tester rely on to access an ever higher level of resources?   |  |  |  | | --- | --- | --- | |  | a. | pivot | |  | b. | spinning | |  | c. | persistence | |  | d. | continuous exploitation | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. If a penetration tester has gained access to a network and then tries to move around inside the network to other resources, what procedure is the tester performing?   |  |  |  | | --- | --- | --- | |  | a. | pivot | |  | b. | spinning | |  | c. | persistence | |  | d. | secondary exploitation | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What term is defined as the state or condition of being free from public attention to the degree that you determine?   |  |  |  | | --- | --- | --- | |  | a. | freedom | |  | b. | secure | |  | c. | privacy | |  | d. | contentment | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What process addresses how long data must be kept and how it is to be secured?   |  |  |  | | --- | --- | --- | |  | a. | legal retention | |  | b. | data retention | |  | c. | legal and compliance | |  | d. | data methodology | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What security goal do the following common controls address: Redundancy, fault tolerance, and patching.?   |  |  |  | | --- | --- | --- | |  | a. | confidentiality | |  | b. | integrity | |  | c. | availability | |  | d. | safety | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which data erasing method will permanently destroy a magnetic-based hard disk by reducing or eliminating the magnetic field?   |  |  |  | | --- | --- | --- | |  | a. | wiping | |  | b. | purging | |  | c. | degaussing | |  | d. | data sanitation | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. If a user uses the operating system's "delete" command to erase data, what type of data removal procedure was used?   |  |  |  | | --- | --- | --- | |  | a. | wiping | |  | b. | purging | |  | c. | degaussing | |  | d. | data sanitation | |

|  |
| --- |
| **Multiple Response** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following is the goal of a vulnerability scan? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | identify vulnerabilities | |  | b. | identify common misconfigurations | |  | c. | identify threat actors | |  | d. | identify a lack of security controls | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following groups categorize the risks associated with the use of private data? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | Statistical inferences. | |  | b. | Associations with groups. | |  | c. | Private and consumer data | |  | d. | Individual inconveniences and identity theft. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Which of the following is a valid data sensitivity labeling and handling category? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | high-risk | |  | b. | confidential | |  | c. | personal health information | |  | d. | proprietary | |

|  |
| --- |
| **Subjective Short Answer** |

|  |
| --- |
| 41. Discuss one type of asset that an organization might have. |

|  |
| --- |
| 42. List and describe the three categories that TCP/IP divides port numbers into. |

|  |
| --- |
| 43. List and describe two common uses for a protocol analyzer. |

|  |
| --- |
| 44. List at least four things that a vulnerability scanner can do. |

|  |
| --- |
| 45. Describe the purpose of a honeypot. |

|  |
| --- |
| 46. Describe a penetration testing report. |

|  |
| --- |
| 47. List and describe the elements that make up a security posture. |

|  |
| --- |
| 48. When a security hardware device fails or a program aborts, which state should it go into? |

|  |
| --- |
| 49. List two types of hardening techniques. |

|  |
| --- |
| 50. Explain the concepts of personal data theft and identity theft. |