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

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

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

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

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

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

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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Nslookup displays detailed information about how a device is communicating with other network devices.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |
| 9. Vulnerability scanning should be conducted on existing systems and particularly as new technology equipment is deployed.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | 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 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

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

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

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |
| --- |
| **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 |  |  |  | | --- | --- | | *ANSWER:* | a, b, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. |  |  |  | | --- | --- | | *ANSWER:* | a, b, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b, d | |

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

|  |  |  |
| --- | --- | --- |
| 41. Discuss one type of asset that an organization might have.   |  |  | | --- | --- | | *ANSWER:* | An organization has many different types of assets. Two of the most common are people (employees, customers, business partners, contractors, and vendors) and physical assets (buildings, automobiles, and other non-computer equipment). Yet the elements of information technology (IT) are also key assets. This includes data (all information used and transmitted by the organization, such as employee databases and inventory records), hardware (desktop computers, servers, networking equipment, and telecommunications connections), and software (application programs, operating systems, and security software). | |

|  |  |  |
| --- | --- | --- |
| 42. List and describe the three categories that TCP/IP divides port numbers into.   |  |  | | --- | --- | | *ANSWER:* | Well-known port numbers (0-1023). Reserved for the most universal applications Registered port numbers (1024-49151). Other applications that are not as widely used Dynamic and private port numbers (49152 - 65535). Available for use by any application. | |

|  |  |  |
| --- | --- | --- |
| 43. List and describe two common uses for a protocol analyzer.   |  |  | | --- | --- | | *ANSWER:* | Protocol analyzers are widely used by network administrators for network monitoring. They can assist in network troubleshooting by detecting and diagnosing network problems such as addressing errors and protocol configuration mistakes. They also are used for network traffic characterization. Protocol analyzers can be used to paint a picture of the types and makeup of network traffic. This representation can be used to fine-tune the network and manage bandwidth to provide the highest level of service to users. | |

|  |  |  |
| --- | --- | --- |
| 44. List at least four things that a vulnerability scanner can do.   |  |  | | --- | --- | | *ANSWER:* | A vulnerability scanner can do the following: Alert when new systems are added to the network. Detect when an application is compromised or subverted. Detect when an internal system begins to port scan other systems. Detect which ports are served and which ports are browsed for each individual system. Identify which applications and servers host or transmit sensitive data. Maintain a log of all interactive network sessions. Passively determine the type of operating system of each active system. Track all client and server application vulnerabilities. Track which systems communicate with other internal systems. | |

|  |  |  |
| --- | --- | --- |
| 45. Describe the purpose of a honeypot.   |  |  | | --- | --- | | *ANSWER:* | A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. | |

|  |  |  |
| --- | --- | --- |
| 46. Describe a penetration testing report.   |  |  | | --- | --- | | *ANSWER:* | The end product of a penetration test is the penetration test report. The report focuses on what data was compromised, how and why it was compromised and includes details of the actual attack method and the value of the data exploited. If requested, potential solutions can be provided, but often it is the role of the organization to determine how best to solve the problems. | |

|  |  |  |
| --- | --- | --- |
| 47. List and describe the elements that make up a security posture.   |  |  | | --- | --- | | *ANSWER:* | Initial baseline configuration: A baseline is the standard security checklist against which systems are evaluated for a security posture. A baseline outlines the major security considerations for a system and becomes the starting point for solid security. It is critical that a strong baseline be created when developing a security posture. Continuous security monitoring: Continual observation of systems and networks through vulnerability scanning and penetration testing can provide valuable information regarding the current state of preparedness. Remediation: As vulnerabilities are exposed through monitoring, there must be a plan in place to address the vulnerabilities before they are exploited by attackers. | |

|  |  |  |
| --- | --- | --- |
| 48. When a security hardware device fails or a program aborts, which state should it go into?   |  |  | | --- | --- | | *ANSWER:* | A firewall device that went into a fail-safe control state could prevent all traffic from entering or exiting, resulting in no traffic coming into the network. It also means that internal devices cannot send traffic out, thereby restricting their access to the Internet. If the firewall went into a fail-open state, then all traffic would be allowed, opening the door for unfiltered attacks to enter the system. If a software program abnormally terminates, then a fail-open state could allow an attacker to launch an insecure activity, whereas the fail-safe state would close the program or even stop the entire operating system in order to prevent any malicious activity. | |

|  |  |  |
| --- | --- | --- |
| 49. List two types of hardening techniques.   |  |  | | --- | --- | | *ANSWER:* | Protecting accounts with passwords, disabling any unnecessary accounts, disabling all unnecessary services, and protecting management interfaces and applications. | |

|  |  |  |
| --- | --- | --- |
| 50. Explain the concepts of personal data theft and identity theft.   |  |  | | --- | --- | | *ANSWER:* | Personal data theft involves user personal data such as credit card numbers that can then be used to purchase thousands of dollars of merchandise online before the victim is even aware the number has been stolen. Personal data theft can also lead to identity theft, or stealing another person's personal information, such as a Social Security number, and then use the information to impersonate the victim, generally for financial gain. | |