|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. A DNS amplification attack floods an unsuspecting victim by redirecting valid responses to it.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. A SYN flood attack broadcasts a network request to multiple computers but changes the address from which the request came to the victim's computer.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. Traditional network security devices can block traditional network attacks, but they cannot always block web application attacks.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. The return address is the only element that can be altered in a buffer overflow attack.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. JavaScript cannot create separate stand-alone applications.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. XSS is like a phishing attack but without needing to trick the user into visiting a malicious website.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. Securing web applications is easier than protecting other systems.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. The malicious content of an XSS URL is confined to material posted on a website   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. A buffer overflow attack occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. In an integer overflow attack, an attacker changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What type of attack intercepts communication between parties to steal or manipulate the data?   |  |  |  | | --- | --- | --- | |  | a. | replay | |  | b. | MAC spoofing | |  | c. | man-in-the-browser | |  | d. | ARP poisoning |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. What protocol can be used by a host on a network to find the MAC address of another device based on an IP address?   |  |  |  | | --- | --- | --- | |  | a. | DNS | |  | b. | ARP | |  | c. | TCP | |  | d. | UDP |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What two locations can be a target for DNS poisoning? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | local host table | |  | b. | external DNS server | |  | c. | local database table | |  | d. | directory server |  |  |  | | --- | --- | | *ANSWER:* | a, b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What type of additional attack does ARP spoofing rely on?   |  |  |  | | --- | --- | --- | |  | a. | DNS Poisoning | |  | b. | replay | |  | c. | MITB | |  | d. | MAC spoofing |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. What type of privileges to access hardware and software resources are granted to users or devices?   |  |  |  | | --- | --- | --- | |  | a. | access privileges | |  | b. | user rights | |  | c. | access rights | |  | d. | permissions |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. When an attack is designed to prevent authorized users from accessing a system, it is called what kind of attack?   |  |  |  | | --- | --- | --- | |  | a. | MITM | |  | b. | spoofing | |  | c. | denial of service | |  | d. | blocking |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. Which type of attack broadcasts a network request to multiple computers but changes the address from which the request came to the victim's computer?   |  |  |  | | --- | --- | --- | |  | a. | IP spoofing | |  | b. | denial of service | |  | c. | DNS Poisoning | |  | d. | smurf attack |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. An attack that takes advantage of the procedures for initiating a session is known as what type of attack?   |  |  |  | | --- | --- | --- | |  | a. | DNS amplification attack | |  | b. | IP spoofing | |  | c. | smurf attack | |  | d. | SYN flood attack |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. What are the two types of cross-site attacks? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | cross-site input attacks | |  | b. | cross-site scripting attacks | |  | c. | cross-site request forgery attacks | |  | d. | cross-site flood attacks |  |  |  | | --- | --- | | *ANSWER:* | b, c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. What language below is used to view and manipulate data that is stored in a relational database?   |  |  |  | | --- | --- | --- | |  | a. | C | |  | b. | DQL | |  | c. | SQL | |  | d. | ISL |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. Which SQL statement represents a SQL injection attempt to determine the names of different fields in a database?   |  |  |  | | --- | --- | --- | |  | a. | whatever AND email IS NULL; -- | |  | b. | whatever; AND email IS NULL; -- | |  | c. | whatever" AND email IS NULL; -- | |  | d. | whatever' AND email IS NULL; -- |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. Choose the SQL injection statement example below that could be used to find specific users:   |  |  |  | | --- | --- | --- | |  | a. | whatever' OR full\_name = '%Mia%' | |  | b. | whatever' OR full\_name IS '%Mia%' | |  | c. | whatever' OR full\_name LIKE '%Mia%' | |  | d. | whatever' OR full\_name equals '%Mia%' |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. Which SQL injection statement example below could be used to discover the name of the table?   |  |  |  | | --- | --- | --- | |  | a. | whatever%20 AND 1=(SELECT COUNT(\*) FROM tabname); -- | |  | b. | whatever' AND 1=(SELECT COUNT(\*) FROM tabname); -- | |  | c. | whatever; AND 1=(SELECT COUNT(\*) FROM tabname); -- | |  | d. | whatever%; AND 1=(SELECT COUNT(\*) FROM tabname); -- |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. An attack in which the attacker attempts to impersonate the user by using his or her session token is known as:   |  |  |  | | --- | --- | --- | |  | a. | Session replay | |  | b. | Session spoofing | |  | c. | Session hijacking | |  | d. | Session blocking |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Which type of attack below is similar to a passive man-in-the-middle attack?   |  |  |  | | --- | --- | --- | |  | a. | replay | |  | b. | hijacking | |  | c. | denial | |  | d. | buffer overflow |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. When TCP/IP was developed, the host table concept was expanded into a hierarchical name system for matching computer names and numbers using this service:   |  |  |  | | --- | --- | --- | |  | a. | HTTP | |  | b. | NSDB | |  | c. | URNS | |  | d. | DNS |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. How can an attacker substitute a DNS address so that a computer is automatically redirected to another device?   |  |  |  | | --- | --- | --- | |  | a. | DNS poisoning | |  | b. | Phishing | |  | c. | DNS marking | |  | d. | DNS overloading |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. The exchange of information among DNS servers regarding configured zones is known as:   |  |  |  | | --- | --- | --- | |  | a. | resource request | |  | b. | zone sharing | |  | c. | zone transfer | |  | d. | zone removal |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. On a compromised computer, you have found that a user without administrative privileges was able to perform a task limited to only administrative accounts. What type of exploit has occurred?   |  |  |  | | --- | --- | --- | |  | a. | Privilege escalation | |  | b. | DNS cache poisoning | |  | c. | ARP poisoning | |  | d. | Man-in-the-middle |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What type of web server application attacks introduce new input to exploit a vulnerability?   |  |  |  | | --- | --- | --- | |  | a. | language attacks | |  | b. | cross-site request attacks | |  | c. | hijacking attacks | |  | d. | injection attacks |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What specific ways can a session token be transmitted? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | In the URL. | |  | b. | In the trailer of a frame. | |  | c. | In the header of a packet. | |  | d. | In the header of the HTTP requisition. |  |  |  | | --- | --- | | *ANSWER:* | a, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. If an attacker purchases and uses a URL that is similar in spelling and looks like a well-known web site in order for the attacker to gain Web traffic to generate income, what type of attack are they using?   |  |  |  | | --- | --- | --- | |  | a. | spoofing | |  | b. | URL hijacking | |  | c. | Web squatting | |  | d. | typo hijacking |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What attack occurs when a domain pointer that links a domain name to a specific web server is changed by a threat actor?   |  |  |  | | --- | --- | --- | |  | a. | pointer hack | |  | b. | DNS spoofing | |  | c. | clickjacking | |  | d. | domain hijacking |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. When an attacker promotes themselves as reputable third-party advertisers to distribute their malware through the Web ads, what type attack is being performed?   |  |  |  | | --- | --- | --- | |  | a. | ad squatting | |  | b. | clickjacking | |  | c. | malvertising | |  | d. | ad spoofing |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What technology expands the normal capabilities of a web browser for a specific webpage?   |  |  |  | | --- | --- | --- | |  | a. | extensions | |  | b. | add-ons | |  | c. | plug-ins | |  | d. | Java applets |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which of the following are considered to be interception attacks? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | denial of service | |  | b. | amplification attack | |  | c. | man-in-the-middle | |  | d. | replay attacks |  |  |  | | --- | --- | | *ANSWER:* | c, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Where are MAC addresses stored for future reference?   |  |  |  | | --- | --- | --- | |  | a. | MAC cache | |  | b. | Ethernet cache | |  | c. | ARP cache | |  | d. | NIC |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. What type of an attack is being executed if an attacker substituted an invalid MAC address for the network gateway so no users can access external networks?   |  |  |  | | --- | --- | --- | |  | a. | ARP poisoning | |  | b. | man-in-the-middle | |  | c. | denial of service | |  | d. | DNS poisoning |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. What type of attack is being performed when multiple computers overwhelm a system with fake requests?   |  |  |  | | --- | --- | --- | |  | a. | DDoS | |  | b. | DoS | |  | c. | SYN flood | |  | d. | replay attacks |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. What criteria must be met for an XXS attack to occur on a specific website?   |  |  |  | | --- | --- | --- | |  | a. | The website must accept user input while validating it and use that input in a response. | |  | b. | The website must accept user input without validating it and use that input in a response. | |  | c. | The website must not accept user input without validating it and use that input in a response. | |  | d. | The website must accept user input while validating it and omit that input in a response. |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |
| --- | --- | --- |
| 41. How is a network-based MITM attack executed?   |  |  | | --- | --- | | *ANSWER:* | A network-based MITM attack involves a threat actor who inserts himself into a conversation between two parties. The actor impersonates both parties to gain access to information they are sending to each other. Neither of the legitimate parties is aware of the presence of the threat actor and thus communicate freely, thinking they are talking only to the authentic party. | |

|  |  |  |
| --- | --- | --- |
| 42. If a MAC address is permanently "burned" into a network interface card, how can an attacker change the MAC address to perform an ARP poisoning attack?   |  |  | | --- | --- | | *ANSWER:* | A MAC address is permanently "burned" into a network interface card (NIC) so that there is not a means of altering the MAC address on a NIC. However, because the MAC address is stored in a software ARP cache, it can be changed there, which would then result in the corresponding IP address pointing to a different computer. This process allows an ARP poisoning attack to occur. | |

|  |  |  |
| --- | --- | --- |
| 43. What is the basis for domain name resolution of names-to-IP addresses?   |  |  | | --- | --- | | *ANSWER:* | When TCP/IP was developed, the host table concept was expanded to a hierarchical name system for matching computer names and numbers known as the Domain Name System (DNS), which is the basis for domain name resolution of names-to-IP addresses used today. | |

|  |  |  |
| --- | --- | --- |
| 44. What are zero-day attacks?   |  |  | | --- | --- | | *ANSWER:* | Zero day attacks are previously unknown vulnerabilities that are exploited. | |

|  |  |  |
| --- | --- | --- |
| 45. How does a cross-site scripting (XSS) attack work?   |  |  | | --- | --- | | *ANSWER:* | In a cross-site scripting (XSS) attack, the threat actor takes advantage of web applications that accept user input without validating it before presenting it back to the user. An attacker can take advantage of this in an XSS attack by tricking a valid website into feeding a malicious script to another user's web browser, which will then execute it. | |

|  |  |  |
| --- | --- | --- |
| 46. How does a cross-site request forgery (XSRF) attack work?   |  |  | | --- | --- | | *ANSWER:* | In a cross-site request forgery (XSRF) attack the user's web browser settings are used to impersonate that user. If a user is currently authenticated on a website and is then tricked into loading another webpage, the new page inherits the identity and privileges of the victim to perform an undesired function on the attacker's behalf. | |

|  |  |  |
| --- | --- | --- |
| 47. How does a buffer overflow attack occur?   |  |  | | --- | --- | | *ANSWER:* | A buffer overflow attack occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer. This extra data overflows into the adjacent memory locations. Because the storage buffer typically contains the "return address" memory location of the software program that was being executed when another function interrupted the process, an attacker can overflow the buffer with a new address pointing to the attacker's malware code. | |

|  |  |  |
| --- | --- | --- |
| 48. What directory are the host tables found in the /etc/ directory in UNIX, Linux, and macOS on a Windows system?   |  |  | | --- | --- | | *ANSWER:* | They are found in the Windows\System32\drivers\etc directory in Windows. | |

|  |  |  |
| --- | --- | --- |
| 49. Explain how an attacker can use privilege escalation to gain access to a resources that are restricted?   |  |  | | --- | --- | | *ANSWER:* | One type of privilege escalation is when a user with a lower privilege uses privilege escalation to grant herself access to functions reserved for higher-privilege users. Another type of privilege escalation is when a user with restricted privileges accesses the different restricted functions of a similar user. | |

|  |  |  |
| --- | --- | --- |
| 50. What are some of the typical server attacks used by attackers?   |  |  | | --- | --- | | *ANSWER:* | Typical server attacks include denial of service, web server application attacks, hijacking, overflow attacks, advertising attacks, and exploiting browser vulnerabilities. | |