|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Malware is software that enters a computer system with the user's knowledge or consent and then performs an unwanted and harmful action.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. Once the malware reaches a system through circulation, then it must embed itself into that system.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. Two types of malware have the primary trait of circulation. These are viruses and worms.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. A polymorphic virus changes its internal code to one of a set number of predefined mutations whenever it is executed.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. A virus self-replicates on the host computer and spreads to other computers by itself.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. A remote access Trojan has the basic functionality of a Trojan but also gives the threat actor unauthorized remote access to the victim's computer by using specially configured communication protocols.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. A rootkit can hide its presence, but not the presence of other malware.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Social engineering impersonation means to masquerade as a real or fictitious character and then play out the role of that person on a victim.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. Phishing is sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. Vishing is a false warning, often contained in an email message claiming to come from the IT department.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What term below is used to describe the process of gathering information for an attack by relying on the weaknesses of individuals?   |  |  |  | | --- | --- | --- | |  | a. | phreaking | |  | b. | hacking | |  | c. | social engineering | |  | d. | reverse engineering |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. Which of the following is malicious computer code that reproduces itself on the same computer?   |  |  |  | | --- | --- | --- | |  | a. | virus | |  | b. | worm | |  | c. | adware | |  | d. | spyware |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. One of the armored virus infection techniques utilizes encryption to make virus code more difficult to detect, in addition to separating virus code into different pieces and inject these pieces throughout the infected program code. What is the name for this technique?   |  |  |  | | --- | --- | --- | |  | a. | stealth | |  | b. | appender | |  | c. | Swiss cheese | |  | d. | split |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What type of malware is heavily dependent on a user in order to spread?   |  |  |  | | --- | --- | --- | |  | a. | Trojan | |  | b. | worm | |  | c. | rootkit | |  | d. | virus |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. A virus that infects an executable program file is known as?   |  |  |  | | --- | --- | --- | |  | a. | macro virus | |  | b. | program virus | |  | c. | companion virus | |  | d. | boot sector virus |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. How many different Microsoft Windows file types can be infected with a virus?   |  |  |  | | --- | --- | --- | |  | a. | 50 | |  | b. | 60 | |  | c. | 70 | |  | d. | 80 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. A series of instructions that can be grouped together as a single command and are often used to automate a complex set of tasks or a repeated series of tasks are known as:   |  |  |  | | --- | --- | --- | |  | a. | A rootkit | |  | b. | A macro | |  | c. | A program | |  | d. | A process |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. Select below the type of malware that appears to have a legitimate use, but contains something malicious:   |  |  |  | | --- | --- | --- | |  | a. | script | |  | b. | virus | |  | c. | Trojan | |  | d. | worm |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. What type of malware consists of a set of software tools used by an attacker to hide the actions or presence of other types of malicious software, such as a virus?   |  |  |  | | --- | --- | --- | |  | a. | rootkit | |  | b. | backdoor | |  | c. | wrapper | |  | d. | shield |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. What type of computer code is typically added to a legitimate program but lies dormant until a specific logical event triggers it?   |  |  |  | | --- | --- | --- | |  | a. | script | |  | b. | logic bomb | |  | c. | macro virus | |  | d. | metamorphic virus |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. What type of undocumented yet benign hidden feature launches after a special set of commands, key combinations, or mouse clicks?   |  |  |  | | --- | --- | --- | |  | a. | Trojan horse | |  | b. | virus | |  | c. | bug | |  | d. | Easter egg |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What kind of software program delivers advertising content in a manner that is unexpected and unwanted by the user, and is typically included in malware?   |  |  |  | | --- | --- | --- | |  | a. | adware | |  | b. | keylogger | |  | c. | spam | |  | d. | Trojan |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. Which of the following is not one of the four methods for classifying the various instances of malware by using the primary trait that the malware possesses?   |  |  |  | | --- | --- | --- | |  | a. | Circulation | |  | b. | Infection | |  | c. | Concealment | |  | d. | Source |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. What type of attack is targeted against a smaller group of specific individuals, such as the major executives working for a manufacturing company?   |  |  |  | | --- | --- | --- | |  | a. | spam | |  | b. | adware | |  | c. | watering hole | |  | d. | typo Squatting |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. What type of system security malware allows for access to a computer, program, or service without authorization?   |  |  |  | | --- | --- | --- | |  | a. | botnet | |  | b. | zombie | |  | c. | backdoor | |  | d. | command and control |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. Malware that locks or prevents a device from functioning properly until a fee has been paid is known as:   |  |  |  | | --- | --- | --- | |  | a. | lock-ware | |  | b. | ransomware | |  | c. | stealware | |  | d. | hostageware |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. What type of ransomware displays a screen and prevents the user from accessing the computer's resources?   |  |  |  | | --- | --- | --- | |  | a. | crypto-malware | |  | b. | standard ransomware | |  | c. | blocker ransomware | |  | d. | locking-malware |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What type of ransomware was developed to block the user from accessing the computer and encrypts all the files on the user's device?   |  |  |  | | --- | --- | --- | |  | a. | crypto-malware | |  | b. | standard ransomware | |  | c. | blocker ransomware | |  | d. | locking-malware |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. Which of the following are considered to be the primary payload capabilities found in malware? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | launch attacks | |  | b. | modify data | |  | c. | delete data | |  | d. | collect data |  |  |  | | --- | --- | | *ANSWER:* | a, c, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. Select the term used to describe tracking software that is deployed without the consent or control of the user.   |  |  |  | | --- | --- | --- | |  | a. | botnet | |  | b. | malware | |  | c. | spyware | |  | d. | Trojan |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What type of malicious software technology is used to download and install software without the user's interaction?   |  |  |  | | --- | --- | --- | |  | a. | automatic download software | |  | b. | automated software | |  | c. | system modifying software | |  | d. | tracking software |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. What type of malicious software technology is used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information?   |  |  |  | | --- | --- | --- | |  | a. | automatic download software | |  | b. | automated software | |  | c. | system modifying software | |  | d. | tracking software |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What type of spyware silently captures and stores each keystroke that a user types on the computer's keyboard?   |  |  |  | | --- | --- | --- | |  | a. | key indexing | |  | b. | ransomware | |  | c. | passive tracking | |  | d. | keylogger |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What type of software can be installed in an individual's web browser to prevent ads from displaying?   |  |  |  | | --- | --- | --- | |  | a. | antivirus | |  | b. | ad blocking | |  | c. | cookie scanning | |  | d. | ad sensing |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What type of structure is used to provide instructions to infected bot computers?   |  |  |  | | --- | --- | --- | |  | a. | client-server | |  | b. | hive | |  | c. | bot herder | |  | d. | command & control |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. What specific science discipline do most social engineering attacks rely on when they are being used?   |  |  |  | | --- | --- | --- | |  | a. | psychiatry | |  | b. | criminology | |  | c. | psychology | |  | d. | engineering |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. What social engineering principal frightens and coerces a victim by using threats?   |  |  |  | | --- | --- | --- | |  | a. | intimidation | |  | b. | authority | |  | c. | urgency | |  | d. | scarcity |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. What social engineering principal convinces a victim an immediate action is needed?   |  |  |  | | --- | --- | --- | |  | a. | authority | |  | b. | urgency | |  | c. | intimidation | |  | d. | scarcity |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which type of phishing attack targets specific users?   |  |  |  | | --- | --- | --- | |  | a. | target phishing | |  | b. | whaling | |  | c. | vishing | |  | d. | spear phishing |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. What specific type of phishing attack uses the telephone to target a victim?   |  |  |  | | --- | --- | --- | |  | a. | target phishing | |  | b. | whaling | |  | c. | vishing | |  | d. | spear phishing |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |
| --- | --- | --- |
| 41. What is malware?   |  |  | | --- | --- | | *ANSWER:* | Malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted-and usually harmful-action. Malware is a general term that refers to a wide variety of damaging or annoying software programs. | |

|  |  |  |
| --- | --- | --- |
| 42. Explain how an appender infection works.   |  |  | | --- | --- | | *ANSWER:* | The virus first appends itself to the end of a file. It then moves the first three bytes of the original file to the virus code and replaces them with a "jump" instruction pointing to the virus code. When the program is launched, the jump instruction redirects control to the virus. | |

|  |  |  |
| --- | --- | --- |
| 43. What are some of the functions performed by viruses?   |  |  | | --- | --- | | *ANSWER:* | Viruses can corrupt or delete files, prevent programs from launching, steal data to be sent to another computer, cause a computer to crash repeatedly, and even turn off the computer's security settings. | |

|  |  |  |
| --- | --- | --- |
| 44. Describe a macro virus.   |  |  | | --- | --- | | *ANSWER:* | A macro virus is written in a script known as a macro. A macro is a series of commands and instructions that can be grouped together as a single command. Macros often are used to automate a complex set of tasks or a repeated series of tasks. Macros can be written by using a macro language, such as Visual Basic for Applications (VBA), and are stored within the user document (such as in an Excel .XLSX worksheet). Once the document is opened, the macro instructions execute, whether those instructions are benign or a macro virus. | |

|  |  |  |
| --- | --- | --- |
| 45. What is a worm?   |  |  | | --- | --- | | *ANSWER:* | A worm is a malicious program that uses a computer network to replicate, and is designed to enter a computer through the network then take advantage of vulnerability in an application or an operating system on the host computer. | |

|  |  |  |
| --- | --- | --- |
| 46. How does a rootkit work?   |  |  | | --- | --- | | *ANSWER:* | A rootkit infects a computer and hides its presence from the operating system so that the rootkit files are not visible to the operating system. | |

|  |  |  |
| --- | --- | --- |
| 47. What is a backdoor and what is it used for?   |  |  | | --- | --- | | *ANSWER:* | A backdoor gives access to a computer, program, or service that circumvents any normal security protections. Backdoors that are installed on a computer allow th attacker to return at a later time and bypass security settings. | |

|  |  |  |
| --- | --- | --- |
| 48. What are botnets?   |  |  | | --- | --- | | *ANSWER:* | Botnets are collections of thousands or even hundreds of thousands of zombie computers are gathered into a logical computer network under the control of an attacker, or bot herder. | |

|  |  |  |
| --- | --- | --- |
| 49. Describe adware.   |  |  | | --- | --- | | *ANSWER:* | Adware delivers advertising content in a manner that is unexpected and unwanted by the user. Once it becomes installed, it typically displays advertising banners, pop-up ads, or opens new web browser windows at random intervals. | |

|  |  |  |
| --- | --- | --- |
| 50. What is dumpster diving?   |  |  | | --- | --- | | *ANSWER:* | Dumpster diving involves digging through trash receptacles to find information that can be useful in an attack. | |