|  |  |  |
| --- | --- | --- |
| **1.** | What is the process of hiding text within an image called?   1. Steganography 2. Encryption 3. Spyware 4. Keystroke logging | [Steganography is the process of hiding text within an image.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | What is a rootkit?   1. A simple tool to gain access to the root of the Windows system 2. A Trojan that sends information to an SMB relay 3. An invasive program that affects the system files, including the kernel and libraries 4. A tool to perform a buffer overflow | [A rootkit is a program that modifies the core of the operating system: the kernel and libraries.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | Why would hackers want to cover their tracks?   1. To prevent another person from using the programs they have installed on a target system 2. To prevent detection or discovery 3. To prevent hacking attempts 4. To keep other hackers from using their tools | [Hackers cover their tracks to keep from having their identity or location discovered.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N64) |
| **4.** | What is privilege escalation?   1. Creating a user account with higher privileges 2. Creating a user account with administrator privileges 3. Creating two user accounts: one with high privileges and one with lower privileges 4. Increasing privileges on a user account | [Privilege escalation is a hacking method to increase privileges on a user account.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N89) |
| **5.** | What are two methods used to hide files? (Choose all that apply.)   1. NTFS file streaming 2. attrib command 3. Steganography 4. Encrypted File System | [NTFS file streaming and the attrib command are two hacking techniques used to hide files.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N114) |
| **6.** | What is the recommended password-change interval?   1. 30 days 2. 20 days 3. 1 day 4. 7 days | [Passwords should be changed every 30 days for the best balance of security and usability.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N146) |
| **7.** | What type of password attack would be most successful against the password T63k#s23A?   1. Dictionary 2. Hybrid 3. Password guessing 4. Brute force | [A brute-force attack tries every combination of letters, numbers, and symbols.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N171) |
| **8.** | Which of the following is a passive online attack?   1. Password guessing 2. Network sniffing 3. Brute-force attack 4. Dictionary attack | [Network sniffing is a passive online attack because it can't be detected.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N200) |
| **9.** | Why is it necessary to clear the event log after using theauditpol command to turn off logging?   1. The auditpol command places an entry in the event log. 2. The auditpol command doesn't stop logging until the event log has been cleared. 3. auditpol relies on the event log to determine whether logging is taking place. 4. The event log doesn't need to be cleared after running the auditpol command. | [The event log must be cleared because the auditpol command places an entry in the event log indicating that logging has been disabled.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N225) |
| **10.** | What is necessary in order to install a hardware keylogger on a target system?   1. The IP address of the system 2. The administrator username and password 3. Physical access to the system 4. Telnet access to the system | [A hardware keylogger is an adapter that connects the keyboard to the PC. A hacker needs physical access to the PC in order to plug in the hardware keylogger.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N273) |
| **11.** | What is the easiest method to get a password?   1. Brute-force cracking 2. Guessing 3. Dictionary attack 4. Hybrid attack | [The easiest way to get a password is to guess the password. For this reason it is important to create strong passwords and to not reuse passwords.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N298) |
| **12.** | Which command is used to cover tracks on a target system?   1. elsave 2. coverit 3. legion 4. nmap | [elsave is a command used to clear the event log and cover a hacker's tracks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N323) |
| **13.** | What type of hacking application is Snow?   1. Password cracker 2. Privilege escalation 3. Spyware 4. Steganography | [Snow is a steganography program used to hide data within the whitespace of text files.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N359) |
| **14.** | What is the first thing a hacker should do after gaining administrative access to a system?   1. Create a new user account 2. Change the administrator password 3. Copy important data files 4. Disable auditing | [The first thing a hacker should do after gaining administrative level access to a system is disable system auditing to prevent detection and attempt to cover tracks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N384) |
| **15.** | Which of the following programs is a steganography detection tool?   1. Stegdetect 2. Stegoalert 3. Stegstopper 4. Stegorama | [Stegdetect is a steganography detection tool.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N409) |
| **16.** | Which countermeasure tool will detect NTFS streams?   1. Windows Security Manager 2. LNS 3. Auditpol 4. RPS | [LNS is an NTFS countermeasure tool used to detect NTFS streams.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N434) |
| **17.** | Which program is used to create NTFS streams?   1. StreamIT 2. makestrm.exe 3. NLS 4. Windows Explorer | [makestrm.exe is a program used to make NTFS streams.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N459) |
| **18.** | Why is it important to clear the event log after disabling auditing?   1. An entry is created that the administrator has logged on. 2. An entry is created that a hacking attempt is underway. 3. An entry is created that indicates auditing has been disabled. 4. The system will shut down otherwise. | [It is important to clear the event log after disabling auditing because an entry is created indicating that auditing is disabled.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N489) |
| **19.** | What is the most dangerous type of rootkit?   1. Kernel level 2. Library level 3. System level 4. Application level | [A kernel-level rootkit is the most dangerous because it infects the core of the system.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N514) |
| **20.** | What is the command to hide a file using the attrib command?   1. att +h [file/directory] 2. attrib +h [file/directory] 3. attrib hide [file/directory] 4. hide [file/directory] | [attrib +h [file/directory] is the command used to hide a file using the hide attribute.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=565019199&rowid=209&noteMenuToggle=0&leftMenuState=1#answer.N539) |

**Answers**

|  |  |
| --- | --- |
| **1.** | Steganography is the process of hiding text within an image. |
| **2.** | A rootkit is a program that modifies the core of the operating system: the kernel and libraries. |
| **3.** | Hackers cover their tracks to keep from having their identity or location discovered. |
| **4.** | Privilege escalation is a hacking method to increase privileges on a user account. |
| **5.** | NTFS file streaming and the attrib command are two hacking techniques used to hide files. |
| **6.** | Passwords should be changed every 30 days for the best balance of security and usability. |
| **7.** | A brute-force attack tries every combination of letters, numbers, and symbols. |
| **8.** | Network sniffing is a passive online attack because it can't be detected. |
| **9.** | The event log must be cleared because the auditpol command places an entry in the event log indicating that logging has been disabled. |
| **10.** | A hardware keylogger is an adapter that connects the keyboard to the PC. A hacker needs physical access to the PC in order to plug in the hardware keylogger. |
| **11.** | The easiest way to get a password is to guess the password. For this reason it is important to create strong passwords and to not reuse passwords. |
| **12.** | elsave is a command used to clear the event log and cover a hacker's tracks. |
| **13.** | Snow is a steganography program used to hide data within the whitespace of text files. |
| **14.** | The first thing a hacker should do after gaining administrative level access to a system is disable system auditing to prevent detection and attempt to cover tracks. |
| **15.** | Stegdetect is a steganography detection tool. |
| **16.** | LNS is an NTFS countermeasure tool used to detect NTFS streams. |
| **17.** | makestrm.exe is a program used to make NTFS streams. |
| **18.** | It is important to clear the event log after disabling auditing because an entry is created indicating that auditing is disabled. |
| **19.** | A kernel-level rootkit is the most dangerous because it infects the core of the system. |
| **20.** | attrib +h [file/directory] is the command used to hide a file using the hide attribute. |