**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | What is a wrapper?   1. A Trojaned system 2. A program used to combine a Trojan and legitimate software into a single executable 3. A program used to combine a Trojan and a backdoor into a single executable 4. A way of accessing a Trojaned system | [A wrapper is software used to combine a Trojan and legitimate software into a single executable so that the Trojan is installed during the installation of the other software. After a Trojan has been installed, a system is considered Trojaned. A backdoor is a way of accessing a Trojaned system and can be part of the behavior of a Trojan.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | What is the difference between a backdoor and a Trojan?   1. A Trojan usually provides a backdoor for a hacker. 2. A backdoor must be installed first. 3. A Trojan is not a way to access a system. 4. A backdoor is provided only through a virus, not through a Trojan. | [A Trojan infects a system first and usually includes a backdoor for later access. The backdoor is not installed independently, but is part of a Trojan. A Trojan is one way a hacker can access a system.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N42) |
| **3.** | What port does Tini use by default?   1. 12345 2. 71 3. 7777 4. 666 | [Tini uses port 7777 by default. Doom uses port 666.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N67) |
| **4.** | Which is the best Trojan and backdoor countermeasure?   1. Scan the hard drive on network connection, and educate users not to install unknown software. 2. Implement a network firewall. 3. Implement personal firewall software. 4. Educate systems administrators about the risks of using systems without firewalls. 5. Scan the hard drive on startup. | [The best prevention is to scan the hard drive for known Trojans on network connections and backdoors and to educate users not to install any unknown software. Scanning the hard drive at startup is a good method for detecting a Trojan, but will not prevent its installation. User education is an important component of security but will not always and consistently prevent a Trojan attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N92) |
| **5.** | How do you remove a Trojan from a system?   1. Search the Internet for freeware removal tools. 2. Purchase commercially available tools to remove the Trojan. 3. Reboot the system. 4. Uninstall and reinstall all applications. | [To remove a Trojan, you should use commercial tools. Many freeware tools contain Trojans or other malware. Rebooting the system alone will not remove a Trojan from the system. Uninstalling and reinstalling applications will not remove a Trojan as it infects the OS.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N120) |
| **6.** | What is ICMP tunneling?   1. Tunneling ICMP messages through HTTP 2. Tunneling another protocol through ICMP 3. An overt channel 4. Sending ICMP commands using a different protocol | [ICMP tunneling involves sending what appear to be ICMP commands but really are Trojan communications. An overt channel sends data via a normal communication path such as via email. Sending or tunneling ICMP within another protocol such as HTTP is not considered ICMP tunneling.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N145) |
| **7.** | What is reverse WWW shell?   1. Connecting to a website using a tunnel 2. A Trojan that connects from the server to the client using HTTP 3. A Trojan that issues commands to the client using HTTP 4. Connecting through a firewall | [Reverse WWW shell is a connection from a Trojan server component on the compromised system to the Trojan client on the hacker's system. Connecting to a website using tunneling or through a firewall is not considered a reverse WWW shell.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N170) |
| **8.** | What is a covert channel?   1. Using a communications channel in a way that was not intended 2. Tunneling software 3. A Trojan removal tool 4. Using a communications channel in the original, intended way | [A covert channel is the use of a protocol or communications channel in a nontraditional way. Tunneling software is one way of using a covert channel but does not necessarily define all covert channels. Using a communications channel in the original intended way is considered an overt channel.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N195) |
| **9.** | What is the purpose of system file verification?   1. To find system files 2. To determine whether system files have been changed or modified 3. To find out if a backdoor has been installed 4. To remove a Trojan | [System file verification tracks changes made to system files and ensures that a Trojan has not overwritten a critical system file. System files and backdoors are not located using system file verification. To remove a Trojan, you should use commercial removal tools.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N220) |
| **10.** | Which of the following is an example of a covert channel?   1. Reverse WWW shell 2. Firewalking 3. SNMP enumeration 4. Steganography | [Reverse WWW shell is an example of a covert channel. Firewalking is enumerating a firewall for firewall rules, allowed traffic, and open ports. Steganography is hiding information in text or graphics. SNMP enumeration is used to identify SNMP MIB settings on networking devices.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N245) |
| **11.** | What is the difference between a virus and a worm?   1. A virus can infect the boot sector but a worm cannot. 2. A worm spreads by itself but a virus must attach to an email. 3. A worm spreads by itself but a virus must attach to another program. 4. A virus is written in C++ but a worm is written in shell code. | [A worm can replicate itself automatically, but a virus must attach to another program. Viruses are not always spread via email but can also be attached to other programs or installed directly by tricking the user. Both viruses and worms can infect the boot sector. The programming language is not used to categorize malware as either viruses or worms.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N270) |
| **12.** | What type of virus modifies itself to avoid detection?   1. Stealth virus 2. Polymorphic virus 3. Multipartite virus 4. Armored virus | [A polymorphic virus modifies itself to evade detection. Stealth viruses hide the normal virus characteristics to prevent detection. Multipartite viruses are viruses that create multiple infections or infect multiple files or programs. Armored viruses use encryption to evade detection.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N295) |
| **13.** | Which virus spreads through Word macros?   1. Melissa 2. Slammer 3. Sobig 4. Blaster | [Melissa is a virus that spreads via Word macros. Slammer and Blaster are actually worm infections, not viruses. Sobig is another type of virus.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N320) |
| **14.** | Which worm affects SQL servers?   1. Sobig 2. SQL Blaster 3. SQL Slammer 4. Melissa | [SQL Slammer is a worm that attacks SQL servers. Melissa affects Word files through the use of macros. There is no such worm as SQL Blaster.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N345) |
| **15.** | Which of the following describes armored viruses?   1. Hidden 2. Tunneled 3. Encrypted 4. Stealth | [Armored viruses are encrypted. They are not by nature tunneled and do not change characteristics, as do stealth viruses. Also, armored viruses are not hidden in any other way.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N370) |
| **16.** | What are the three methods used to detect a virus?   1. Scanning 2. Integrity checking 3. Virus signature comparison 4. Firewall rules 5. IDS anomaly detection 6. Sniffing | [Scanning, integrity checking, and virus signature comparison are three ways to detect a virus infection. Firewalls, IDS anomaly detection, and sniffing all work at lower layers of the OSI model and are not able to detect viruses.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N395) |
| **17.** | What components of a system do viruses infect? (Choose all that apply.)   1. Files 2. System sectors 3. Memory 4. CPU 5. DLL files | [A virus can affect files, system sectors, and DLL files. Memory and CPU cannot be infected by viruses.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N426) |
| **18.** | Which of the following are the best indications of a virus attack? (Choose all that apply.)   1. Any anomalous behavior 2. Unusual program opening or closing 3. Strange pop-up messages 4. Normal system operations as most viruses run in the background | [Trojans, backdoors, spyware, and other malicious software can cause a system to not act normally. Any indications of programs opening or closing without user intervention, unresponsive programs, unusual error messages, or pop-ups could indicate any type of malware has infected the system. But not all anomalous behavior can be attributed to a virus.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N454) |
| **19.** | A virus that can cause multiple infections is known as what type of virus?   1. Multipartite 2. Stealth 3. Camouflage 4. Multi-infection | [A multipartite virus can cause multiple infections. Stealth viruses hide the normal virus characteristics to prevent detection. Camouflage and multi-infection are not categories of viruses.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N482) |
| **20.** | Which of the following is a way to evade an antivirus program?   1. Write a custom virus script. 2. Write a custom virus signature. 3. Write a custom virus evasion program. 4. Write a custom virus detection program. | [A custom virus script can be used to evade detection because the script will not match a virus signature.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=411506315&rowid=238&noteMenuToggle=0&leftMenuState=1#answer.N507) |

**Answers**

|  |  |
| --- | --- |
| **1.** | A wrapper is software used to combine a Trojan and legitimate software into a single executable so that the Trojan is installed during the installation of the other software. After a Trojan has been installed, a system is considered "Trojaned." A backdoor is a way of accessing a Trojaned system and can be part of the behavior of a Trojan. |
| **2.** | A Trojan infects a system first and usually includes a backdoor for later access. The backdoor is not installed independently, but is part of a Trojan. A Trojan is one way a hacker can access a system. |
| **3.** | Tini uses port 7777 by default. Doom uses port 666. |
| **4.** | The best prevention is to scan the hard drive for known Trojans on network connections and backdoors and to educate users not to install any unknown software. Scanning the hard drive at startup is a good method for detecting a Trojan, but will not prevent its installation. User education is an important component of security but will not always and consistently prevent a Trojan attack. |
| **5.** | To remove a Trojan, you should use commercial tools. Many freeware tools contain Trojans or other malware. Rebooting the system alone will not remove a Trojan from the system. Uninstalling and reinstalling applications will not remove a Trojan as it infects the OS. |
| **6.** | ICMP tunneling involves sending what appear to be ICMP commands but really are Trojan communications. An overt channel sends data via a normal communication path such as via email. Sending or tunneling ICMP within another protocol such as HTTP is not considered ICMP tunneling. |
| **7.** | Reverse WWW shell is a connection from a Trojan server component on the compromised system to the Trojan client on the hacker's system. Connecting to a website using tunneling or through a firewall is not considered a reverse WWW shell. |
| **8.** | A covert channel is the use of a protocol or communications channel in a nontraditional way. Tunneling software is one way of using a covert channel but does not necessarily define all covert channels. Using a communications channel in the original intended way is considered an overt channel. |
| **9.** | System file verification tracks changes made to system files and ensures that a Trojan has not overwritten a critical system file. System files and backdoors are not located using system file verification. To remove a Trojan, you should use commercial removal tools. |
| **10.** | Reverse WWW shell is an example of a covert channel. Firewalking is enumerating a firewall for firewall rules, allowed traffic, and open ports. Steganography is hiding information in text or graphics. SNMP enumeration is used to identify SNMP MIB settings on networking devices. |
| **11.** | A worm can replicate itself automatically, but a virus must attach to another program. Viruses are not always spread via email but can also be attached to other programs or installed directly by tricking the user. Both viruses and worms can infect the boot sector. The programming language is not used to categorize malware as either viruses or worms. |
| **12.** | A polymorphic virus modifies itself to evade detection. Stealth viruses hide the normal virus characteristics to prevent detection. Multipartite viruses are viruses that create multiple infections or infect multiple files or programs. Armored viruses use encryption to evade detection. |
| **13.** | Melissa is a virus that spreads via Word macros. Slammer and Blaster are actually worm infections, not viruses. Sobig is another type of virus. |
| **14.** | SQL Slammer is a worm that attacks SQL servers. Melissa affects Word files through the use of macros. There is no such worm as SQL Blaster. |
| **15.** | Armored viruses are encrypted. They are not by nature tunneled and do not change characteristics, as do stealth viruses. Also, armored viruses are not hidden in any other way. |
| **16.** | Scanning, integrity checking, and virus signature comparison are three ways to detect a virus infection. Firewalls, IDS anomaly detection, and sniffing all work at lower layers of the OSI model and are not able to detect viruses. |
| **17.** | A virus can affect files, system sectors, and DLL files. Memory and CPU cannot be infected by viruses. |
| **18.** | Trojans, backdoors, spyware, and other malicious software can cause a system to not act normally. Any indications of programs opening or closing without user intervention, unresponsive programs, unusual error messages, or pop-ups *could* indicate any type of malware has infected the system. But not all anomalous behavior can be attributed to a virus. |
| **19.** | A multipartite virus can cause multiple infections. Stealth viruses hide the normal virus characteristics to prevent detection. Camouflage and multi-infection are not categories of viruses. |
| **20.** | A custom virus script can be used to evade detection because the script will not match a virus signature. |