**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | What does LKM stand for?   1. Linux Kernel Module 2. Linux Kernel Mode 3. Linked Kernel Module 4. Last Kernel Mode | [LKM stands for Linux Kernel Module.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | What GCC command is used to compile a C++ file called source into an executable file called game?   1. g++ source.c –o game 2. gcc source.c –o game 3. gcc make source.cpp –o game 4. g++ source.cpp –o game | [g++ source.cpp  o game is the GCC command to create an executable called game from the source file source .](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | What is the command to deny all users access from the network?   1. Cat “All:All”>> /etc/hosts.deny 2. Set “All:All”>> /etc/hosts.deny 3. IP deny “All:All” 4. Cat All:All deny | [Use the Cat  All:All -- /etc/hosts.deny command to deny all users access from the network on a Linux system.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N91) |
| **4.** | Of the following, which are common commercial Linux distributions?   1. SUSE, Knark, and Red Hat 2. SUSE, Adore, Debian, and Mandrake 3. SUSE, Debian, and Red Hat 4. SUSE, Adore, and Red Hat | [SUSE, Debian, and Red Hat are all commercial versions of Linux.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N128) |
| **5.** | What is a Linux live CD?   1. A Linux operating system that runs from a CD 2. A Linux operating system installed from a CD onto a hard drive 3. A Linux tool that runs applications from a CD 4. A Linux application that makes CDs | [A Linux live CD is a fully functioning operating system that runs from a CD.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N153) |
| **6.** | What type of attack can be disguised as an LKM?   1. DoS 2. Trojan 3. Spam virus 4. Rootkit | [A rootkit can be disguised as an LKM.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N178) |
| **7.** | Which of the following is a reason to use Linux?   1. Linux has no security holes. 2. Linux is always up-to-date on security patches. 3. No rootkits can infect a Linux system. 4. Linux is flexible and can be modified. | [Linux is flexible and can be modified because the source code is openly available.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N203) |
| **8.** | Which of the following is *not* a way to harden Linux?   1. Physically secure the system. 2. Maintain a current patch level. 3. Change the default passwords. 4. Install all available services. | [Linux should not have unused services running, because each additional service may have potential vulnerabilities.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N228) |
| **9.** | What type of file is used to create a Linux live CD?   1. ISO 2. CD 3. LIN 4. CDFS | [An ISO file is used to create a Linux live CD.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N256) |
| **10.** | Why is it important to use a known good distribution of Linux?   1. Source files can become corrupted if not downloaded properly. 2. Only certain distributions can be patched. 3. Source files can be modified, and a Trojan or backdoor may be included in the source binaries of some less-known or free distributions of Linux. 4. Only some versions of Linux are available to the public. | [Known good distributions have been reviewed by the Linux community to verify that a Trojan or backdoor does not exist in the source code.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N281) |
| **11.** | What command will give you the most information Linux files?   1. ls -a 2. ls -m 3. ls -t 4. ls -l | [The command ls -l lists all the information about files such as permissions, owners, size, and last modified date.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N306) |
| **12.** | What is the purpose of the man command?   1. Lists help and documentation 2. Manually configures a program 3. Performs system maintenance 4. Installs a program | [The man command will list help and documentation in Linux.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N343) |
| **13.** | In which directory are Linux system source files located?   1. source 2. src 3. sys 4. system | [The src directory contains the Linux source files.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N376) |
| **14.** | What is the Linux command that lists all current running processes?   1. ps 2. list ps 3. show ps 4. process | [The ps command lists all running processes.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N413) |
| **15.** | What is the Linux command for viewing the IP address of a network interface?   1. ifconfig 2. ipconfig 3. ipconfig /all 4. interface /ip | [Use the ifconfig command to view the IP address of a network interface. ipconfig and ipconfig/all are Windows commands to view IP address information.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N450) |
| **16.** | Which Linux command would produce the following output?  [Image from book](javascript:PopImage('IMG_66','http://images.books24x7.com/bookimages/id_31967/ng1204_0.jpg','480','94'))   1. routing 2. route print 3. route 4. show routes | [route displays the routing table. route print is a Windows command to display the routing table. show routes is a command commonly used to view a routing table.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N495) |
| **17.** | What is a recommended way to secure the Linux root account? (Choose all that apply.)   1. Prevent direct root logins except from the system console. 2. Restrict the use of su to a single group. 3. Install su protect to prevent misuse of the su command. 4. Grant the admin privilege to any user needing to install programs. | [The recommended way to secure the Linux root account is to prevent direct root logins and to restrict the use of su to one group.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N555) |
| **18.** | When you are securing local Linux file systems, which two types of directories should you be check for appropriate permissions? (Choose two.)   1. Root directory 2. Services directory 3. Writable system executable directories 4. Writable user home directories | [Writable system executable directories and writable user home directories should both be checked as they could be used to execute malicious code.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N580) |
| **19.** | What is the Cat command you would use to harden the file system of a Linux system?   1. Cat “source=All:destination=All”>> /etc/hosts.deny 2. Cat “All:All”>> /etc/hosts.deny 3. Cat “Any:Any”>> /etc/hosts.deny 4. Cat “All:All”/etc/hosts.deny | [Use the command Cat  All:All -- /etc/hosts.deny to harden a Linux system and ensure all users are denied access to certain files from the network.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N605) |
| **20.** | In which file should you check to ensure users do not have a null password in a Linux system?   1. Password file 2. Passwd file 3. Shadow file 4. Shdw file | [User passwords in a Linux system are stored in the shadow file. To harden a system, check the shadow file for null passwords.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=926507574&rowid=387&noteMenuToggle=0&leftMenuState=1#answer.N646) |

**Answers**

|  |  |
| --- | --- |
| **1.** | LKM stands for Linux Kernel Module. |
| **2.** | g++ source.cpp –o game is the GCC command to create an executable called game from the source file source. |
| **3.** | Use the Cat “All:All”>> /etc/hosts.deny command to deny all users access from the network on a Linux system. |
| **4.** | SUSE, Debian, and Red Hat are all commercial versions of Linux. |
| **5.** | A Linux live CD is a fully functioning operating system that runs from a CD. |
| **6.** | A rootkit can be disguised as an LKM. |
| **7.** | Linux is flexible and can be modified because the source code is openly available. |
| **8.** | Linux should not have unused services running, because each additional service may have potential vulnerabilities. |
| **9.** | An ISO file is used to create a Linux live CD. |
| **10.** | Known good distributions have been reviewed by the Linux community to verify that a Trojan or backdoor does not exist in the source code. |
| **11.** | The command ls -l lists all the information about files such as permissions, owners, size, and last modified date. |
| **12.** | The man command will list help and documentation in Linux. |
| **13.** | The src directory contains the Linux source files. |
| **14.** | The ps command lists all running processes. |
| **15.** | Use the ifconfig command to view the IP address of a network interface. ipconfig and ipconfig/all are Windows commands to view IP address information. |
| **16.** | route displays the routing table. route print is a Windows command to display the routing table. show routes is a command commonly used to view a routing table. |
| **17.** | The recommended way to secure the Linux root account is to prevent direct root logins and to restrict the use of su to one group. |
| **18.** | Writable system executable directories and writable user home directories should both be checked as they could be used to execute malicious code. |
| **19.** | Use the commandCat “All:All”>> /etc/hosts.deny to harden a Linux system and ensure all users are denied access to certain files from the network. |
| **20.** | User passwords in a Linux system are stored in the shadow file. To harden a system, check the shadow file for null passwords. |