Security Strategies in Linux Platforms and Applications 3rd edition Messier Test Bank

SKU: 9781284255850-TEST-BANK

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: Ahead
Information Field: Subject
Information Field: Title
Information Field: Feedback
Information Field: Taxonomy
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 9781284255904, add to Ahead, Title tags

Chapter: Chapter 01 - Quiz

Multiple Choice

1. In Linux, the operating system is referred to as the _____. This is what interfaces with the hardware to manage memory and filesystems and make sure programs run.
A) distribution
B) command-line shell
C) kernel
D) secure shell
Ans: C
Complexity: Easy
Ahead: The Origins of Linux
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy: Understand

2. You are selecting a package-management system to install programs on your Linux Ubuntu distribution. Which one do you choose?
A) Advanced Package Tool (APT)
B) Red Hat Package Manager (RPM)
C) sudo
D) Yellowdog Updater, Modified (Yum)
Ans: A
Complexity: Easy
Ahead: The Origins of Linux
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Debian-based systems like Mint and Ubuntu use APT and the related utilities to install software.
Taxonomy: Apply

3. Which of the following is true regarding open-source software versus commercial software?

A) Because open-source source code is open, processes are always in place to ensure code is written to reduce or remove vulnerabilities in the software.
B) Open-source software is always rigorously tested.
C) Open-source software often suffers from a process-heavy path to get a vulnerability fixed.
D) Open-source projects put their source code out on the open Internet at public repositories.
Ans: D
Complexity: Medium
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Because the source code is open does not mean the project has processes in place to ensure code is written to reduce or remove vulnerabilities in the software. It also does not mean there has been rigorous testing. Unlike commercial software, an open-source project may not suffer from a process-heavy path to get a vulnerability fixed.
Taxonomy: Understand

4. The Linux open-source license, referred to as GNU General Public License (GPL), requires that:
A) the source code be considered closed source after modification by an organization.
B) any software based on GPLed software retain the same rights as the original software.
C) all GPLed software be attributed to GNU Project founder Richard Stallman.
D) any software based on GPLed software may not retain the same rights as the original software.
Ans: B
Complexity: Hard
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Any software that is based on GPLed software is required to retain the same rights as the original software. In other words, if a software project licensed using GPL is taken and modified by another party, that party would have to release it under GPL as well.
Taxonomy: Understand

5. You are downloading open-source code for a web server. A cryptographic hash is generated for the downloadable source code file. What does this protect you from?
A) A backdoor being installed in the software
B) An attacker generating a new MD5
C) The download being corrupted
D) The tarball being packed
Ans: C
Complexity: Medium
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Along with the source code, there is generally a cryptographic hash generated to demonstrate that what you downloaded is what you are actually looking for. Where you are protected with this is if the download gets corrupted. It does not protect you if the tarball has been altered and a new MD5 has been generated.
Taxonomy: Understand

6. Fedora Core and Ubuntu are examples of:
A) source code.

B) distributions.
C) applications.
D) virtual platforms.
Ans: B
Complexity: Easy
Ahead: Linux Distributions
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy: Understand

7. Which of the following is a distribution based on Debian?
A) CentOS
B) Mint
C) RHEL
D) Rocky
Ans: B
Complexity: Easy
Ahead: Linux Distributions
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy: Remember

8. You are developing a security protocol using cryptography. You want to prevent a party to a computer transaction from denying that the transaction took place. What security issue are you addressing?
A) Confidentiality
B) Integrity
C) Availability
D) Nonrepudiation
Ans: D
Complexity: Medium
Ahead: The C-I-A Triad
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy: Apply

9. Keeping secrets is the essence of which tenet of the C-I-A triad?
A) Confidentiality
B) Integrity
C) Availability
D) Nonrepudiation
Ans: A
Complexity: Easy
Ahead: The C-I-A Triad
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy: Understand

10. A denial of service (DoS) attack jeopardizes which tenet of the C-I-A triad?
A) Confidentiality
B) Integrity
C) Availability
D) Nonrepudiation
Ans: C
Complexity: Medium
Ahead: The C-I-A Triad
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy: Understand

11. What does the Parkerian hexad include that the C-I-A triad does not?
A) Confidentiality
B) Authenticity
C) Integrity
D) Availability
Ans: B
Complexity: Medium
Ahead: The C-I-A Triad
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: The Parkerian hexad includes confidentiality, possession or control, integrity, authenticity, availability, and utility. The C-I-A triad includes confidentiality, integrity, and availability.
Taxonomy: Understand

12. You are working with virtualization software on a Linux hardware host. You want to put several virtual applications in a container package that is native to Linux. What do you use?
A) Docker
B) LXC
C) A GNU General Public License (GPL)
D) Transport Layer Security (TLS)
Ans: B
Complexity: Medium
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Containers are a way of virtualizing applications by tagging the memory assigned to an application so it's not possible for the application to refer to memory that has not been tagged in the same way. LXC is a set of programs required to manage native Linux containers.
Taxonomy: Apply

13. What is Snort?
A) A firewall
B) A gateway
C) A bastion host

D) An intrusion-detection service
Ans: D
Complexity: Easy
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Snort is an intrusion-detection service that watches network traffic as it goes by, looking for areas of concern. Any packet or frame that passes by the Snort sensor that looks suspicious generates an alert.
Taxonomy: Understand

14. Which of the following is the best definition of a bastion host?
A) A type of open-source license
B) A system that is presented to the outside world that can be used to protect other systems that are more sensitive
C) A system logger
D) Hardware or software capable of blocking networking communications based on established criteria or "rules"
Ans: B
Complexity: Easy
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy: Understand

15. You are configuring a Linux-based device as a firewall in a current version of Linux. What package do you use to create firewall rules that live within the kernel?
A) ipfreewall
B) ipchains
C) ipsecurity
D) iptables
Ans: D
Complexity: Medium
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Where Linux previously used a package called ipchains, the current firewall software available for Linux is called iptables. Iptables is a program that you use to create firewall rules that live within the kernel.
Taxonomy: Apply

16. What is one of the first host-based intrusion-detection systems deployed under Linux? It is now a commercial product that monitors operating system files.
A) Bastion host
B) Snort
C) Syslog
D) Tripwire
Ans: D
Complexity: Easy

Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Tripwire, now a commercial product, was developed to monitor critical operating system files. It was one of the first host-based intrusion-detection systems developed for Unix-like operating systems.
Taxonomy: Remember

17. Which of the following is *not* true of system hardening?
A) A hardened system is more resistant to attack.
B) System hardening involves removing all but the most critical users from the system.
C) A hardened system usually has more packages to update than an unhardened system.
D) System hardening involves ensuring permissions are restricted on files and directories.
Ans: C
Complexity: Medium
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: When you harden an operating system, you make it more resistant to attack. To do this, you remove any software you are not going to be using. As a result, there are fewer ways in for an adversary. There are also fewer packages you have to monitor for updates in case vulnerabilities are found in the software. Hardening also involves removing all but the most critical users from the system, which would have a minimum number of packages installed.
Taxonomy: Understand

18. You are running a firewall but it is not on a Linux host. The operating system is Unix based but the kernel is different. What is the most likely system you are on?
A) BSD
B) Red Hat
C) Slackware
D) Ubuntu
Ans: A
Complexity: Medium
Ahead: Linux in the Enterprise
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: BSD is a Unix-based operating system but its operating system kernel is different. Red Hat, Slackware, and Ubuntu all run on the Linux kernel.
Taxonomy: Understand

19. Which of the following is commonly exposed to outside systems from within an enterprise; is the way customers get access to information, products, and services offered by businesses; and is relied upon for many business-to-business services?
A) Web server
B) Application server
C) Proxy server
D) File server
Ans: A
Complexity: Medium
Ahead: Linux in the Enterprise
Subject: Chapter 1

Title: Security Threats to Linux
Feedback:
Taxonomy: Understand

20. You are referred to as a black-hat hacker. Which of the following activities are you most likely to perform?
A) Penetration testing to reveal holes in an employer's network security
B) Installing ransomware on corporate servers on behalf of a competitor
C) Luring cybercriminals to a fake website for your company as requested by your chief information security officer in an attempt to gain information on them
D) Using social engineering to test the security training of a company and then reporting the results to the company's chief information officer
Ans: B
Complexity: Hard
Ahead: Recent Security Issues
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: A black-hat hacker is someone who performs attacks against victims for malicious purposes. This can include working for a criminal organization that is hired to install ransomware on a competitor's computers or other illegal actions. Performing penetration testing, using social engineering at the request of an employer or client, or getting information on cybercriminals are more typical of gray-hat or white-hat hackers.
Taxonomy: Apply

True/False

1. True or False? The package-management system in Linux is used to restrict permissions on files and folders.
Ans: False
Complexity: Easy
Ahead: The Origins of Linux
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: The Linux package-management system is used to install software.
Taxonomy:

2. True or False? Linux "open-source" means the source code cannot be viewed or modified by anyone other than the individual or company that developed the code.
Ans: False
Complexity: Easy
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: "Open source" means the source code is open for anyone to see. Software developed by companies that ask you to pay for the program is commonly called "closed source" in addition to being commercial software.
Taxonomy:

3. True or False? Branches in Linux source code repositories help keep malicious software or software with vulnerabilities out of production.
Ans: True
Complexity: Medium
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

4. True or False? The term "copyleft" is associated with the GNU General Public License (GPL).
Ans: True
Complexity: Easy
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

5. True or False? GNU's Not Unix (GNU) refers only to commercial versions of Linux software.
Ans: False
Complexity: Easy
Ahead: The Origins of Linux
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: GNU is an open-source project that originally attempted to create a Unix-like operating system and today contributes tools that are used in the overall environment on top of the operating system.
Taxonomy:

6. True or False? The concept that Linux source code should be freely available means that it should be without cost.
Ans: False
Complexity: Medium
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: The concept that source code should be available should not be read as a belief that everything should be without cost.
Taxonomy:

7. True or False? One benefit of open-source code is the ability to learn what the code does and how the program operates.
Ans: True
Complexity: Medium
Ahead: Security in an Open-Source World
Subject: Chapter 1

Title: Security Threats to Linux
Feedback:
Taxonomy:

8. True or False? Because Linux open-source code is available to anyone to fix a bug, there is no guarantee that the fix will be high quality.
Ans: True
Complexity: Medium
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

9. True or False? The process of fixing commercial software is typically less constrained by human resource issues than open-source software projects.
Ans: False
Complexity: Medium
Ahead: Security in an Open-Source World
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Open-source projects like Linux (and all of the packages that go into a regular Linux distribution) are less constrained by human resource issues than commercial software projects. Anyone can pick up the open-source code and also pick up a bug and go fix it.
Taxonomy:

10. True or False? Most Linux distributions have pre-compiled packages, which determine all the dependencies.
Ans: True
Complexity: Easy
Ahead: Linux Distributions
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

11. True or False? Installation of a source-based distribution, such as Linux From Scratch or Gentoo Linux, typically takes less time than installing a pre-packaged Linux distribution.
Ans: False
Complexity: Medium
Ahead: Linux Distributions
Subject: Chapter 1
Title: Security Threats to Linux
Feedback: Unlike a pre-packaged Linux distribution, installing a source-based distribution can be a very time-consuming process taking several hours.
Taxonomy:

12. True or False? All packages in a source-based distribution of Linux must be compiled from source.
Ans: True
Complexity: Easy
Ahead: Linux Distributions
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

13. True or False? The C-I-A triad and Parkerian hexad define concepts with respect to information security.
Ans: True
Complexity: Easy
Ahead: The C-I-A Triad
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

14. True or False? A Linux system may be deployed as a system logger (syslog) facility, which is a place to collect log files from across a network.
Ans: True
Complexity: Medium
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

15. True or False? A firewall is hardware or software capable of blocking networking communications based on established criteria or "rules."
Ans: True
Complexity: Medium
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

16. True or False? In a Linux system, a smaller number of packages means a smaller surface area for attack.
Ans: True
Complexity: Medium
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:

Taxonomy:

17. True or False? A hardened Linux system typically contains fewer packages to be monitored for updates in case vulnerabilities are found in the software.
Ans: True
Complexity: Medium
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

18. True or False? A virtual machine is an operating system that typically does not run directly on the user's hardware.
Ans: True
Complexity: Easy
Ahead: Linux as a Security Device
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

19. True or False? Linux may be used as a proxy server or a gateway on a network.
Ans: True
Complexity: Easy
Ahead: Linux in the Enterprise
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

20. True or False? An application server is software that provides a framework inside which applications can be written.
Ans: True
Complexity: Easy
Ahead: Linux in the Enterprise
Subject: Chapter 1
Title: Security Threats to Linux
Feedback:
Taxonomy:

