[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 3 Exam Answers

1. Why would a network administrator choose Linux as an operating system in the Security Operations Center (SOC)?

- It is easier to use than other operating systems.
- It is more secure than other server operating systems.
- **The administrator has more control over the operating system.**
- More network applications are created for this environment

3. Which Linux command can be used to display the name of the current working directory?

- chmod
- **pwd**
- ps
- sudo

5. Consider the result of the ls -l command in the Linux output below. What are the file permissions assigned to the sales user for the analyst.txt file?

ls –l analyst.txt

-rwxrw-r– sales staff 1028 May 28 15:50 analyst.txt

- write only
- **read, write, execute**
- read, write
- read only

6. A Linux system boots into the GUI by default, so which application can a network administrator use in order to access the CLI environment?

- file viewer
- package management tool
- **terminal emulator**
- system viewer

7. The image displays a laptop that is acting as the SSH client that is communicating with an SSH server. Refer to the exhibit. Which well-known port number is used by the server?

- 23
- **22**
- 21
- 25

8. How is a server different from a workstation computer?

- The server works as a standalone computer.
- **The server is designed to provide services to clients.**
- The workstation has fewer applications installed.
- The workstation has more users who attach to it.

10. Which two methods can be used to harden a computing device? (Choose two.)

- Allow default services to remain enabled.

- Update patches on a strict annual basis irrespective of release date.
- **Enforce the password history mechanism.**
- **Ensure physical security.**
- Allow USB auto-detection.

11. What is the main purpose of the X Window System?

- to provide a customizable CLI environment
- **to provide a basic framework for a GUI**
- to provide remote access to a Linux-based system
- to provide a basic set of penetration testing tools

12. Which Linux command is used to manage processes?

- **kill**
- grep
- chrootkit
- ls

13. Why is Linux considered to be better protected against malware than other operating systems?

- fewer deployments
- integrated firewall
- customizable penetration and protection tools
- **file system structure, file permissions, and user account restrictions**

14. Which two Linux commands might be used before using the kill command? (Choose two.)

- **top**
- ls
- grep
- **ps**
- chroot

15. What term is used for operating system updates?

- **patches**
- new releases
- penetration testing
- packages

16. What term describes a set of software tools designed to increase the privileges of a user or to grant access to the user to portions of the operating system that should not normally be allowed?

- penetration testing
- package manager
- **rootkit**
- compiler

17. What is the well-known port address number used by DNS to serve requests?

- 60
- 110
- 25
- **53**

18. Which file system is the primary file system used by Apple in current Macintosh computers?

- CDFS

- **APFS**
- ext3
- ext2
- HFS+

19. Which type of tool allows administrators to observe and understand every detail of a network transaction?

- malware analysis tool
- **packet capture software**
- ticketing system
- log manager

20. Which command can be utilized to view log entries of NGINX system events in real time?

- **sudo journalctl –u nginx.service -f**
- sudo journalctl –f
- sudo journalctl –until “1 hour ago”
- sudo journalctl –u nginx.services

21. What is the purpose of a Linux package manager?

- It provides access to settings and the shutdown function.
- It is used to compile code that creates an application.
- **It is used to install an application.**
- It provides a short list of tasks a particular application can perform.

22. Which user can override file permissions on a Linux computer?

- only the creator of the file
- any user that has ‘group’ permission to the file
- any user that has ‘other’ permission to the file
- **root user**

23. Which Linux file system introduced the journaled file system, which can be used to minimize the risk of file system corruption in the event of a sudden power loss?

- ext2
- **ext3**
- NFS
- CDFS

24. What is the method employed by a Linux kernel to create new processes for multitasking of a process?

- creating interdependent processes
- dynamic processes
- pipelining
- **forking**

25. What is a purpose of apt-get commands?

- to configure an appointment for a specific date and time
- to configure and manage task (to-do) lists
- **to update the operating system**
- to apportion and configure a part of the hard disk for file storage