CCNA Cyber Ops (Version 1.1) – Chapter 3 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-3-exam-answers-full.html

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. What is the outcome when a Linux administrator enters the man man command?

- The man man command configures the network interface with a manual address.
- **The man man command provides documentation about the man command. ***
- The man man command provides a list of commands available at the current prompt.
- The man man command opens the most recent log file.

B. The man command is short for manual and is used to obtain documentation about a Linux command. The command man man would provide documentation about how to use the manual.

2. What is a benefit of Linux being an open source operating system?

- Linux distributions are maintained by a single organization.
- Linux distributions must include free support without cost.
- **Linux distribution source code can be modified and then recompiled. ***
- Linux distributions are simpler operating systems since they are not designed to be connected to a network.

C. Linux is an open source operating system and any person can access the source code, inspect it, modify it, and recompile it. Linux distributions are maintained by a community of programmers, are designed to be connected to a network, and do not have to provide free support.

3. Which types of files are used to manage services in a Linux system?

- Device files

- System files
- Directory files
- **Configuration files** *

D. In Linux, services are managed using configuration files. When the service starts, it looks for its configuration files, loads them into memory, and adjusts itself according to the settings in the files.

4. Which working environment is more user-friendly?

- A CLI
- **A GUI** *
- The command prompt
- A hybrid GUI and CLI interface

B. A graphical user interface (GUI) is considered to be more user-friendly because it presents the operating system with an interface and icons that make it easy to locate applications and complete tasks.

5. Which Linux component would be used to access a short list of tasks theapplication can perform?

- Launcher
- **Quicklist** *
- Dash Search Box
- System and Notification Menu

B. The Quicklist is accessed by right-clicking any application hosted on the Launcher. Quicklist allows access to a few tasks for the specific application.

6. Which term is used to describe a running instance of a computer program?

- Fork
- Patch
- **Process** *
- Package manager

C. A process is a running instance of a computer program. Multitasking operating systems can execute multiple processes at the same time. A processID (PID) is used to identify a process. The ps or top command can be used to see what processes are currently running on a computer.

7. Which type of tool is used by a Linux administrator to attack a computer or network to find vulnerabilities?

- Firewall
- **PenTesting** *
- Malware analysis
- Intrusion detection system

B. PenTesting is known as penetration testing and includes tools that are used to search for vulnerabilities in a network or computer by attacking it.

8. Which method can be used to harden a computing device?

- Allow USB auto-detection.
- **Force periodic password changes.** *
- Allow default services to remain enabled.
- Update patches on a strict annual basis irrespective of release date.

B. The basic best practices for device hardening are as follows:
Ensure physical security.
Minimize installed packages.
Disable unused services.
Use SSH and disable the root account login over SSH.
Keep the system updated.
Disable USB auto-detection.
Enforce strong passwords.
Force periodic password changes.
Keep users from reusing old passwords.
Review logs regularly.

9. Consider the result of the ls -l command in the Linux output below. What are the group file permissions assigned to the analyst.txt file?

```
ls -l analyst.txt
-rwxrw-r-- sales staff 1028 May 28 15:50 analyst.txt
```

- Read only
- **Read, write** *
- Full access
- Read, write, execute

B. The file permissions are always displayed in the User, Group, and Other order. In the example displayed, the file has the following permissions:
The dash (-) means that this is a file. For directories, the first dash would be replaced with a “d”.
The first set of characters is for user permission (rwx). The user, sales, who owns the file can read, write, and execute the file.

The second set of characters is for group permissions (rw-). The group, staff, who owns the file can read and write to the file.
The third set of characters is for any other user or group permissions (r–).
Any other user or group on the computer can only read the file.

10. 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

There are several reasons why Linux is a good choice for the SOC.Linux is open source.
The command line interface is a very powerful environment.
The user has more control over the operating system.
Linux allows for better network communication control.

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

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

One of the most important commands in Linux is the pwd command, which stands for print working directory. It shows users the physical path for the directory they are working in.

12. 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

The file permissions are always displayed in the User, Group and Other order. In the example displayed, the file has the following permissions:
The dash (-) means that this is a file. For directories, the first dash would replaced with a “d”.
The first set of characters is for user permission (rwx). The user, sales, who owns the file can read, write and execute the file.

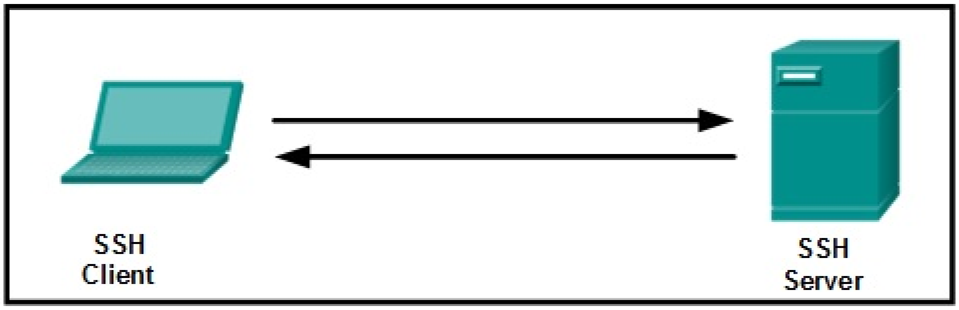
The second set of characters is for group permissions (rw-). The group, staff, who owns the file can read and write to the file.
The third set of characters is for any other user or group permissions (r–). Any other user or group on the computer can only read the file.

13. 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

A terminal emulator is an application program a user of Linux can use in order to access the CLI environment.

14. 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

SSH is a protocol that is used to securely access a remote network device. The well-known port number used by SSH is 22.

15. 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.

Servers provide services such as file management, email, web pages, log management, financial transactions, databases, and more.

16. 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.

The basic best practices for device hardening are as follows:
Ensure physical security.
Minimize installed packages.
Disable unused services.
Use SSH and disable the root account login over SSH.
Keep the system updated.
Disable USB auto-detection.
Enforce strong passwords.
Force periodic password changes.
Keep users from reusing old passwords.
Review logs regularly.

17. 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

The X Window System provides the basic framework for a GUI, but the GUI itself varies greatly between different distributions.

18. Which Linux command is used to manage processes?

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

The kill command is used to stop, restart, or pause a process. The chrootkit command is used to check the computer for rootkits, a set of software tools that can increase the privilege level of a user or grant access to portions of software normally not allowed. The grep command is used to look for a file or text within a file. The ls command is used to list files, directories, and file information.

19. 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**

The Linux operating design including how the file system is structured, standard file permissions, and user account restrictions make Linux a better protected operating system. However, Linux still has vulnerabilities and can have malware installed that affects the operating system.

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

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

The ps or top command might be used before using the kill command to discover the process ID (PID) for the specific process.

21. What term is used for operating system updates?

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

Operating system updates, also known as patches, are provided by companies that create the operating system. A user can check for operating system updates at any time. In a Linux GUI environment, the Dash Search Box can be used to search for the Software Updater icon.

22. 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

A rootkit is used by an attacker to secure a backdoor to a compromised computer, grant access to portions of the operating system normally not permitted, or increase the privileges of a user.

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

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

Port numbers are used in TCP and UDP communications to differentiate between the various services running on a device. The well-known port number used by DNS is port 53.

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

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

The primary file system used by Apple in its lates Macintosh computers is APFS.

25. 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

Network packet capture software is an important tool because it makes it possible to observe and understand the details of a network transaction.

26. 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

The journalctl command supports mixing options to achieve a desired filter set. The –u option allows filtering on the desired unit, whereas the –f option follows the specific log, thus monitoring the event in real time.

27. 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.

A package is a specific program and all of the files needed to run that application. A package manager is used to install a package and place all the associated files in the correct location within the operating system.

28. 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**

A user has as much rights to a file as the file permissions allow. The only user that can override file permission on a Linux computer is the root user. Because the root user has the power to override file permissions, the root user can write to any file.

29. 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

The ext3 file system is considered a journaled file system that was designed to improve the existing ext2 file system. A journal, the main feature added to ext3, is a technique used to minimize the risk of file system corruption in the event of sudden power loss.

30. 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**

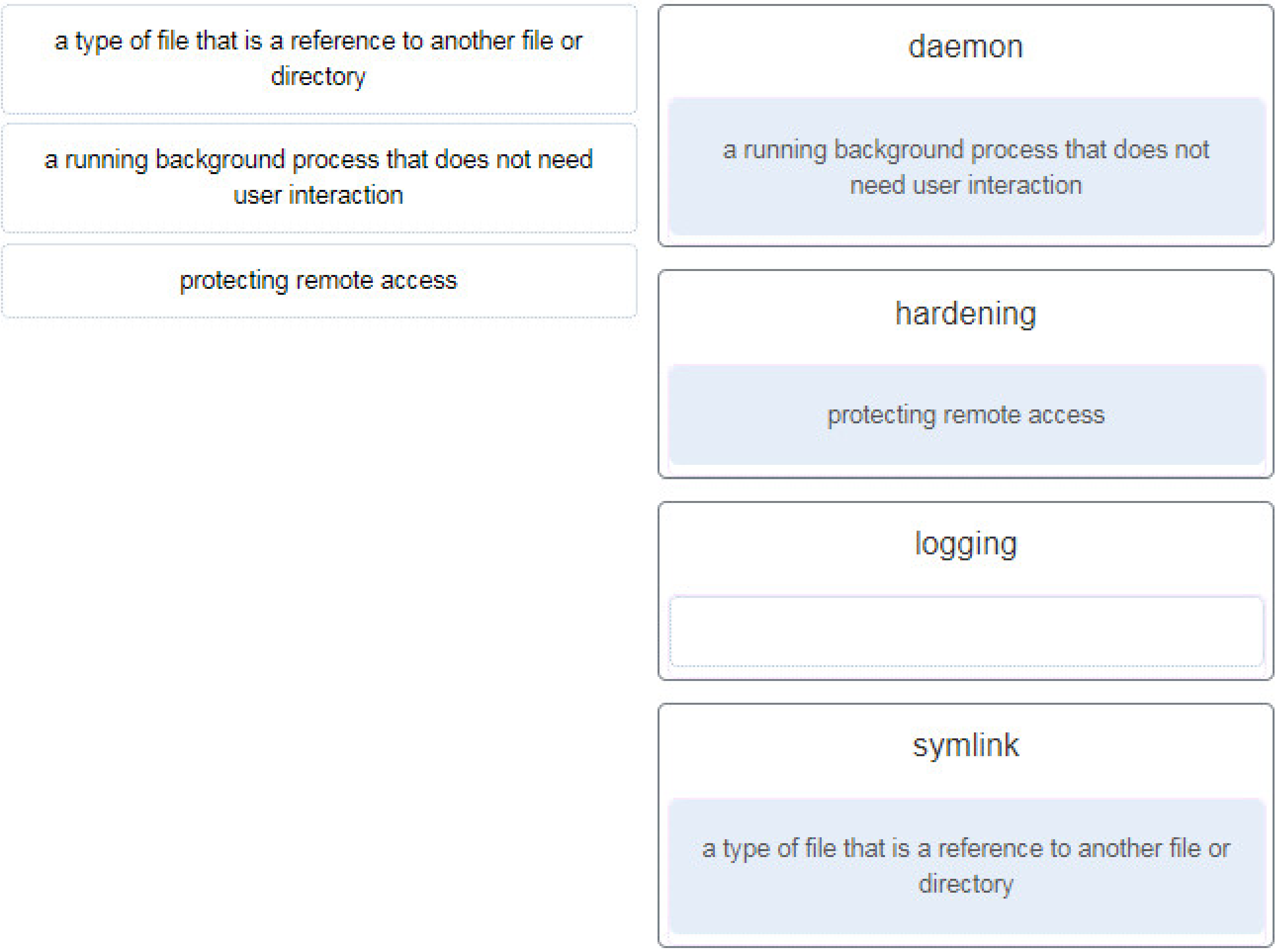
Multitasking operating systems are required to execute several processes at the same time. Forking is a method that the kernel uses to allow a process to create a copy of itself.

31. 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

The Advanced Packaging Tool (apt) package manager is used to update the operating system. The apt-get update command is used to search and obtain the package list from a repository and update the local package database.

32. Match the description to the Linux term. (Not all options are used.)



a type of file that is a reference to another file or directory

a running background process that does not need user interaction

protecting remote access

daemon

a running background process that does not need user interaction

hardening

protecting remote access

logging

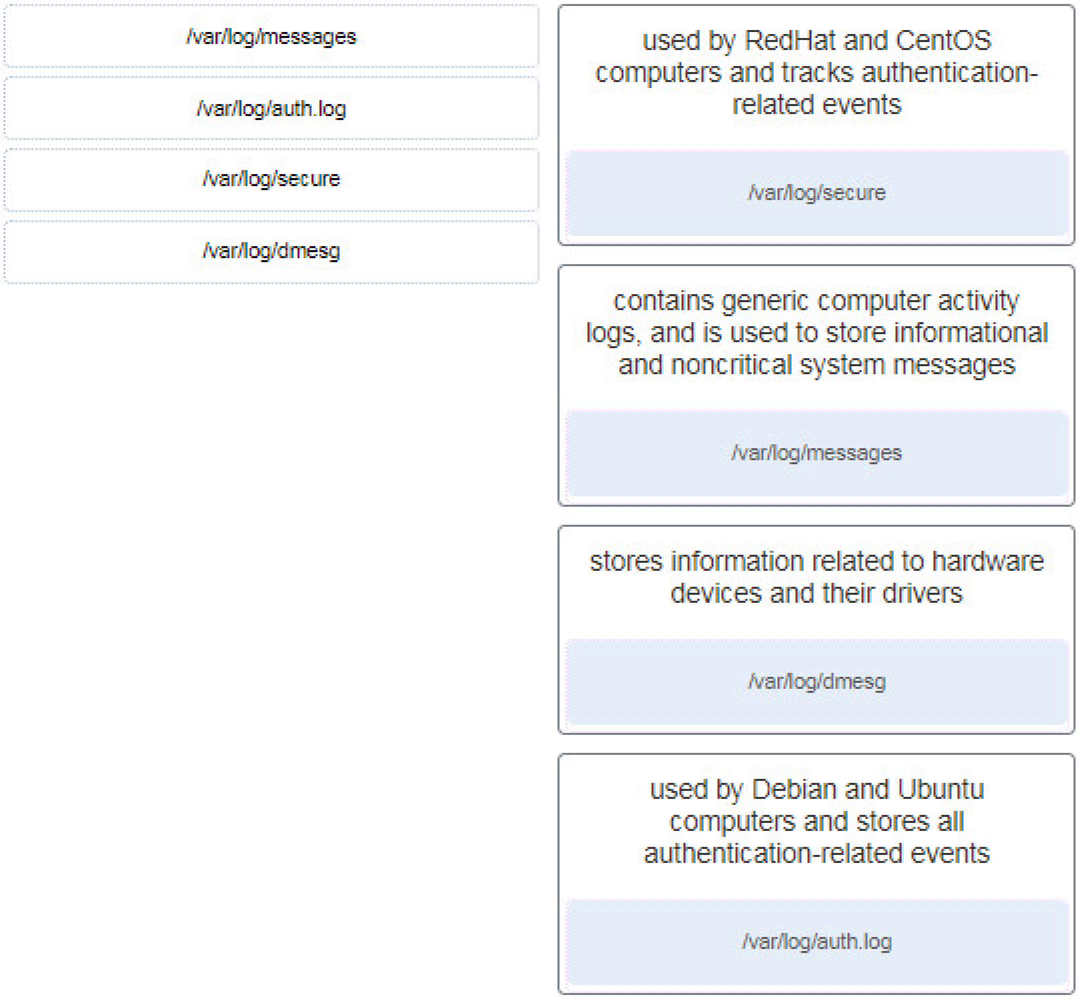
symlink

a type of file that is a reference to another file or directory

- daemon -> **a running background process that does not need user interaction**
- hardening -> **protecting remote access**

- logging -> (empty)
- symlink -> **a type of file that is a reference to another file or directory**

33. Match typical Linux log files to the function.



/var/log/messages

/var/log/auth.log

/var/log/secure

/var/log/dmesg

used by RedHat and CentOS computers and tracks authentication-related events

/var/log/secure

contains generic computer activity logs, and is used to store informational and noncritical system messages

/var/log/messages

stores information related to hardware devices and their drivers

/var/log/dmesg

used by Debian and Ubuntu computers and stores all authentication-related events

/var/log/auth.log

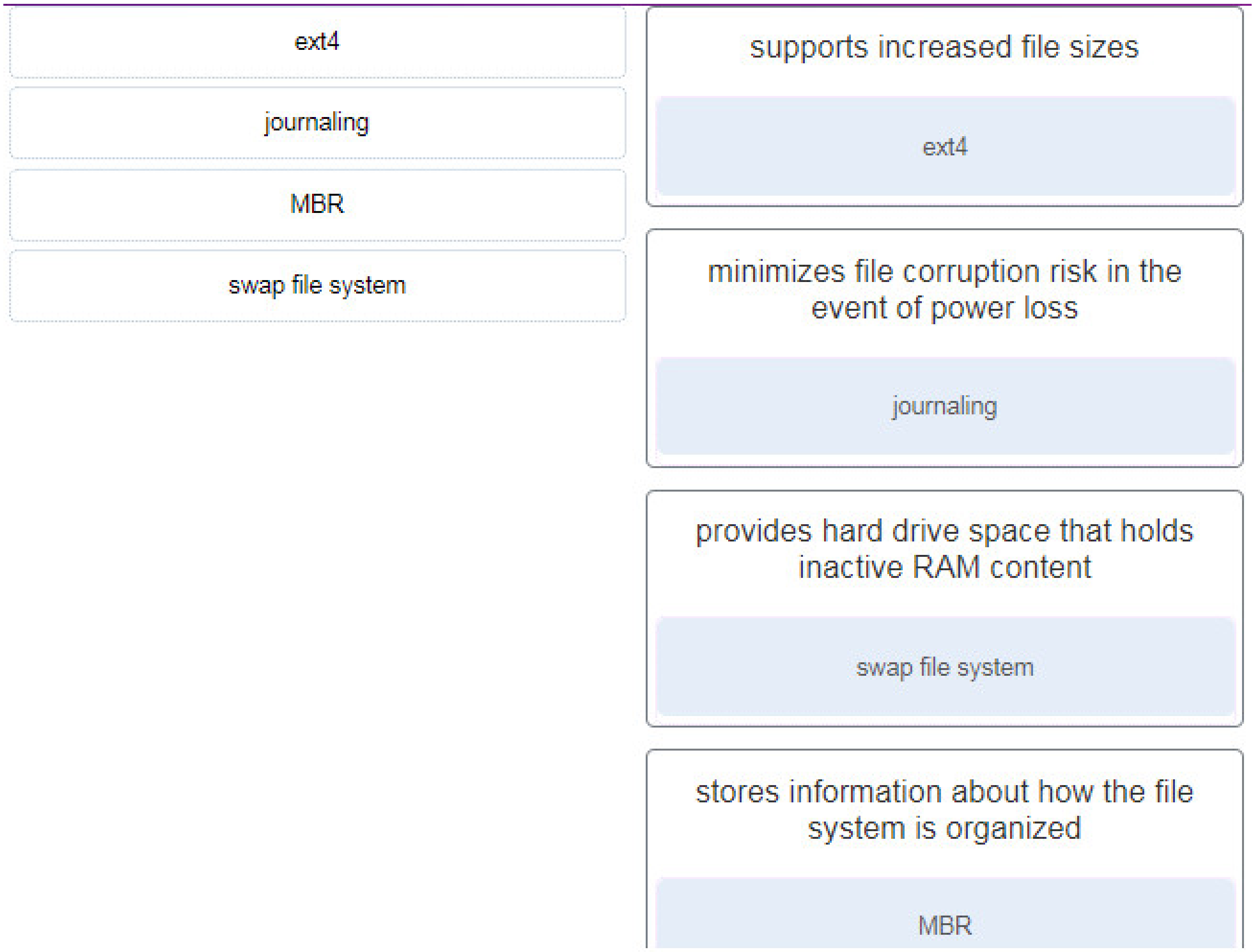
used by RedHat and Centos computers and tracks authentication related events
–> `/var/log/secure`

contains generic computer activity logs, and is used to store informational and noncritical system messages
–> `/var/log/messages`

stores information related to hardware devices and their drivers
–> `/var/log/dmesg`

used by RedHat and Centos computers and tracks authentication related events
–> `/var/log/auth.log`

34. Match the file system term used in Linux to the function.



ext4

journaling

MBR

swap file system

supports increased file sizes

ext4

minimizes file corruption risk in the event of power loss

journaling

provides hard drive space that holds inactive RAM content

swap file system

stores information about how the file system is organized

MBR

- supports increased file sizes –> **ext4**
- minimizes file corruption risk in the event of power loss –> **journaling**
- provides hard drive space that holds inactive RAM content –> **swap file system**
- stores information about how the file system is organized –> **MBR**

Download PDF File below:

[sociallocker id=”54558″]

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 3 Exam Answers.pdf 424.06 KB 1318 downloads

…

Download

[/sociallocker]