



# 212-82<sup>Q&As</sup>

Certified Cybersecurity Technician(C|CT)

## Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/212-82.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.

Which of the following virtualization approaches has Nicolas adopted in the above scenario?

- A. Hardware-assisted virtualization
- B. Full virtualization
- C. Hybrid virtualization
- D. OS-assisted virtualization

Correct Answer: A

Explanation: Hardware-assisted virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS. Hardware-assisted virtualization relies on special hardware features in the CPU and chipset to create and manage virtual machines efficiently and securely<sup>34</sup>. Full virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment, but the VMM will run in software and emulate all the hardware resources for each virtual machine<sup>5</sup>. Hybrid virtualization is a virtualization approach that combines hardware-assisted and full virtualization techniques to optimize performance and compatibility<sup>6</sup>. OS-assisted virtualization is a virtualization approach in which the guest OS will be modified to run in a virtualized environment and cooperate with the VMM to access the hardware resources

### QUESTION 2

Calvin spotted blazing flames originating from a physical file storage location in his organization because of a Short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. Which of the following firefighting systems did Calvin use in this scenario?

- A. Fire detection system
- B. Sprinkler system
- C. Smoke detectors
- D. Fire extinguisher

Correct Answer: D

Explanation: Fire extinguisher is the firefighting system that Calvin used in this scenario. A firefighting system is a system that detects and suppresses fire in a physical location or environment. A firefighting system can consist of various components, such as sensors, alarms, sprinklers, extinguishers, etc. A firefighting system can use various agents or substances to suppress fire, such as water, foam, gas, powder, etc. A fire extinguisher is a portable device that contains an agent or substance that can be sprayed or discharged onto a fire to extinguish it . A fire extinguisher can be used to curb fire in the initial stage and prevent it from spreading over a large area . In the scenario, Calvin



spotted blazing flames originating from a physical file storage location in his organization because of a short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. This means that he used a fire extinguisher for this purpose. A fire detection system is a system that detects the presence of fire by sensing its characteristics, such as smoke, heat, flame, etc., and alerts the occupants or authorities about it. A sprinkler system is a system that consists of pipes and sprinkler heads that release water onto a fire when activated by heat or smoke. A smoke detector is a device that senses smoke and emits an audible or visual signal to warn about fire.

---

### QUESTION 3

Ryleigh, a system administrator, was instructed to perform a full back up of organizational data on a regular basis. For this purpose, she used a backup technique on a fixed date when the employees are not accessing the system i.e., when a

service-level down time is allowed a full backup is taken.

Identify the backup technique utilized by Ryleigh in the above scenario.

- A. Nearline backup
- B. Cold backup
- C. Hot backup
- D. Warm backup

Correct Answer: B

Explanation: Cold backup is the backup technique utilized by Ryleigh in the above scenario. Cold backup is a backup technique that involves taking a full backup of data when the system or database is offline or shut down. Cold backup ensures that the data is consistent and not corrupted by any ongoing transactions or operations. Cold backup is usually performed on a fixed date or time when the service-level downtime is allowed or scheduled. Nearline backup is a backup technique that involves storing data on a medium that is not immediately accessible, but can be retrieved within a short time. Hot backup is a backup technique that involves taking a backup of data while the system or database is online or running. Warm backup is a backup technique that involves taking a backup of data while the system or database is partially online or running.

---

### QUESTION 4

You are Harris working for a web development company. You have been assigned to perform a task for vulnerability assessment on the given IP address 20.20.10.26. Select the vulnerability that may affect the website according to the severity factor.

Hint: Greenbone web credentials: admin/password

- A. TCP timestamps
- B. Anonymous FTP Login Reporting
- C. FTP Unencrypted Cleartext Login
- D. UDP timestamps



Correct Answer: C

Explanation: FTP Unencrypted Cleartext Login is the vulnerability that may affect the website according to the severity factor in the above scenario. A vulnerability is a weakness or flaw in a system or network that can be exploited by an

attacker to compromise its security or functionality. A vulnerability assessment is a process that involves identifying, analyzing, and evaluating vulnerabilities in a system or network using various tools and techniques. Greenbone is a tool that

can perform vulnerability assessment on various targets using various tests and scans. To perform a vulnerability assessment on the given IP address 20.20.10.26, one has to follow these steps:

Open a web browser and type 20.20.10.26:9392

Press Enter key to access the Greenbone web interface.

Enter admin as username and password as password.

Click on Login button.

Click on Scans menu and select Tasks option.

Click on Start Scan icon next to IP Address Scan task. Wait for the scan to complete and click on Report icon next to IP Address Scan task.

Observe the vulnerabilities found by the scan.

The vulnerabilities found by the scan are:

Name	Severity
TCP timestamps	Low
Anonymous FTP Login Reporting	Low
FTP Unencrypted Cleartext Login	Medium
UDP timestamps	Low

The vulnerability that may affect the website according to the severity factor is FTP Unencrypted Cleartext Login, which has a medium severity level. FTP Unencrypted Cleartext Login is a vulnerability that allows an attacker to intercept or sniff FTP login credentials that are sent in cleartext over an unencrypted connection. An attacker can use these credentials to access or modify files or data on the FTP server. TCP timestamps and UDP timestamps are vulnerabilities that allow an attacker to estimate the uptime of a system or network by analyzing the timestamp values in TCP or UDP packets. Anonymous FTP Login Reporting is a vulnerability that allows an attacker to access an FTP server anonymously without providing any username or password.

## QUESTION 5

Gideon, a forensic officer, was examining a victim's Linux system suspected to be involved in online criminal activities. Gideon navigated to a directory containing a log file that recorded information related to user login/logout. This information helped Gideon to determine the current login state of cyber criminals in the victim system, identify the Linux



log file accessed by Gideon in this scenario.

A. /var/log/mysqld.log

B. /var/log/wtmp

C. /var/log/boot.log

D. /var/log/httpd/

Correct Answer: B

Explanation: /var/log/wtmp is the Linux log file accessed by Gideon in this scenario. /var/log/wtmp is a log file that records information related to user login/logout, such as username, terminal, IP address, and login time. /var/log/wtmp can be used to determine the current login state of users in a Linux system. /var/log/wtmp can be viewed using commands such as last, lastb, or utmpdump1. References: Linux Log Files

[Latest 212-82 Dumps](#)

[212-82 Practice Test](#)

[212-82 Study Guide](#)