312-38Q&As

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

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

https://www.certbus.com/312-38.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following RAID storage techniques divides the data into multiple blocks, which are further written across the RAID system?

A. Striping

B. None of these

C. Parity

D. Mirroring

Correct Answer: A

QUESTION 2

In MacOS, how can the user implement disk encryption?

A. By enabling BitLocker feature

B. By executing dm-crypt command

C. By turning on Device Encryption feature

D. By enabling FileVault feature

Correct Answer: D

QUESTION 3

Which encryption algorithm h used by WPA5 encryption?

A. RC4.TKIP

B. RC4

C. AES-GCMP 256

D. AES-CCMP

Correct Answer: D

QUESTION 4

Kelly is taking backups of the organization\\'s data. Currently, she is taking backups of only those files that are created or modified after the last backup. What type of backup is Kelly using?

A. Full backup

B. Incremental backup

C. Normal backup

D. Differential backup

Correct Answer: D

QUESTION 5

Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps?

A. Category 5e

B. Category 3

C. Category 5

D. Category 6

Correct Answer: B

Category 3 type of UTP cable uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps. They are commonly used in Ethernet networks that operate at the speed of 10 Mbps. A higher speed is also possible by these cables implementing the Fast Ethernet (100Base-T4) specifications. This cable is used mainly for telephone systems. Answer option C is incorrect. This category of UTP cable is the most commonly used cable in present day networks. It consists of four twisted pairs and is used in those Ethernet networks that run at the speed of 100 Mbps. Category 5 cable can also provide a higher speed of up to 1000 Mbps. Answer option A is incorrect. It is also known as Category 5 Enhanced cable. Its specification is the same as category 5, but it has some enhanced features and is used in Ethernets that run at the speed of 1000 Mbps. Answer option D is incorrect. This category of UTP cable is designed to support high-speed networks that run at the speed of 1000 Mbps. It consists of four pairs of wire and uses all of them for data transmission. Category 6 provides more than twice the speed of Category 5e, but is also more expensive.

QUESTION 6

Which of the following is a presentation layer protocol?

A. TCP

B. RPC

C. BGP

D. LWAPP

Correct Answer: D

QUESTION 7

Which of the following is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference?

A. Incident response

B. Incident handling

C. Incident management

D. Incident planning

Correct Answer: A

Incident response is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference. One of the primary goals of incident response is to "freeze the scene". There is a close relationship between incident response, incident handling, and incident management. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage. Incident management manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred. Answer option B is incorrect. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage. Answer option C is incorrect. It manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred. Answer option D is incorrect. This is an invalid option.

QUESTION 8

Kyle is an IT technician managing 25 workstations and 4 servers. The servers run applications and mostly store confidential data. Kyle must backup the server\\'s data daily to ensure nothing is lost. The power in the company\\'s office is not always reliable, Kyle needs to make sure the servers do not go down or are without power for too long. Kyle decides to purchase an Uninterruptible Power Supply (UPS) that has a pair of inverters and converters to charge the battery and provides power when needed. What type of UPS has Kyle purchased?

A. Kyle purchased a Ferro resonant Standby UPS.

B. Kyle purchased a Line-Interactive UPS

C. He has bought a Standby UPS

D. He purchased a True Online UPS.

Correct Answer: C

QUESTION 9

Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21. What does this source address signify?

A. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.

B. This source address is IPv6 and translates as 13.1.68.3

C. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank\\'s network

D. This means that the source is using IPv4

Correct Answer: D

QUESTION 10

Fill in the blank with the appropriate term. In computing, is a class of data storage devices that read their data in sequence.

Correct Answer: SAM

In computing, sequential access memory (SAM) is a class of data storage devices that read their data in sequence. This is in contrast to random access memory (RAM) where data can be accessed in any order. Sequential access devices are usually a form of magnetic memory. While sequential access memory is read in sequence, access can still be made to arbitrary locations by "seeking" to the requested location. Magnetic sequential access memory is typically used for secondary storage in general-purpose computers due to their higher density at lower cost compared to RAM, as well as resistance to wear and non-volatility. Examples of SAM devices include hard disks, CD-ROMs, and magnetic tapes.

QUESTION 11

DRAG DROP

Drag and drop the terms to match with their descriptions.

Select and Place:

	Terms	Description
Backdoor	Place Here	It is malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Place Here	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Place Here	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Place Here	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Correct Answer:

	Terms	Description
	Trojan horse	It is malicious software program that contains hidden code and masquerades itself as a normal program.
	Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
	Spamware	It is software designed by or for spammers to send out automated spam e-mail.
	Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Following are the terms with their descriptions:

Terms	Description
Trojan horse	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

A Trojan horse is a malicious software program that contains hidden code and masquerades itself as a normal program. When a Trojan horse program is run, its hidden code runs to destroy or scramble data on the hard disk. An example of a Trojan horse is a program that masquerades as a computer logon to retrieve user names and password information. The developer of a Trojan horse can use this information later to gain unauthorized access to computers. Trojan horses are normally spread by e-mail attachments. Ping sweep is a technique used to determine which of a range of IP addresses map to live hosts. It consists of ICMP ECHO requests sent to multiple hosts. If a given address is live, it will return an ICMP ECHO reply. A ping is often used to check that a network device is functioning. To disable ping sweeps on a network, administrators can block ICMP ECHO requests from outside sources. However, ICMP TIMESTAMP and ICMP INFO can be used in a similar manner. Spamware is software designed by or for spammers to send out automated spam e-mail. Spamware is used to search for e-mail addresses to build lists of e-mail addresses to be used either for spamming directly or to be sold to spammers. The spamware package also includes an e-mail harvesting tool. A backdoor is any program that allows a hacker to connect to a computer without going through the normal authentication process. The main advantage of this type of attack is that the network traffic moves from inside a network to the hacker\\'s computer. The traffic moving from inside a network to the outside world is typically the least restrictive, as companies are more concerned about what comes into a network, rather than what leaves it. It, therefore, becomes hard to detect backdoors.

QUESTION 12

Physical access controls help organizations monitor, record, and control access to the information assets and facility. Identify the category of physical security controls which includes security labels and warning signs.

A. Technical control

B. Environmental control

C. Physical control

D. Administrative control

Correct Answer: D

QUESTION 13

Which of the following is the full form of SAINT?

A. System Automated Integrated Network Tool

B. Security Admin Integrated Network Tool

C. System Admin Integrated Network Tool

D. System Administrators Integrated Network Tool

Correct Answer: D

QUESTION 14

Which of the following is a physical security device designed to entrap a person on purpose?

A. Mantrap

B. Trap

C. War Flying

D. War Chalking

Correct Answer: A

QUESTION 15

Steven\\'s company has recently grown from 5 employees to over 50. Every workstation has a public IP address and navigated to the Internet with little to no protection. Steven wants to use a firewall. He also wants IP addresses to be private addresses, to prevent public Internet devices direct access to them. What should Steven implement on the firewall to ensure this happens?

A. Steven should use Open Shortest Path First (OSPF).

B. Steven should enable Network Address Translation (NAT).

C. Steven should use a Demilitarized Zone (DMZ).

D. Steven should use IPsec.

Correct Answer: C