312-38 Q&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.geekcert.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

Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement

the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the data.

Which RAID level is used here?

A. RAID 3

B. RAID 1

C. RAID 5

D. RAID 0

Correct Answer: B

QUESTION 2

Fill in the blank with the appropriate term. A network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or tokenpassing scheme is used for preventing the collision of data between two computers that want to send messages at the same time.

Correct Answer: Token Ring

A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet. The IBM Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Working: Empty information frames are constantly circulated on the ring. When a computer has a message to send, it adds a token to an empty frame and adds a message and a destination identifier to the frame. The frame is then observed by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and modifies the token back to 0. When the frame gets back to the originator, it sees that the token has been modified to 0 and that the message has been copied and received. It removes the message from the particular frame. The frame continues to circulate as an empty frame, ready to be taken by a workstation when it has a message to send.

QUESTION 3

An employee of a medical service company clicked a malicious link in an email sent by an attacker. Suddenly, employees of the company are not able to access billing information or client record as it is encrypted. The attacker asked the company to pay money for gaining access to their data. Which type of malware attack is described above?

A. Logic bomb

B. Rootkits

C. Trojan

D. Ransomware

Correct Answer: D

QUESTION 4

Which of the following are the six different phases of the Incident handling process? Each correct answer represents a complete solution. Choose all that apply.

A. Containment

B. Identification

C. Post mortem review

D. Preparation

E. Lessons learned

F. Recovery

G. Eradication

Correct Answer: ABDEFG

Following are the six different phases of the Incident handling process: 1.Preparation: Preparation is the first step in the incident handling process. It includes processes like backing up copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. To apply this step a documented security policy is formulated that outlines the responses to various incidents, as a reliable set of instructions during the time of an incident. The following list contains items that the incident handler should maintain in the preparation phase i.e. before an incident occurs: Establish applicable policies Build relationships with key players Build response kit Create incident checklists Establish communication plan Perform threat modeling Build an incident response team Practice the demo incidents 2.Identification: The Identification phase of the Incident handling process is the stage at which the Incident handler evaluates the critical level of an incident for an enterprise or system. It is an important stage where the distinction between an event and an incident is determined, measured and tested. 3.Containment: The Containment phase of the Incident handling process supports and builds up the incident combating process. It helps in ensuring the stability of the system and also confirms that the incident does not get any worse. 4.Eradication: The Eradication phase of the Incident handling process involves the cleaning-up of the identified harmful incidents from the system. It includes the analyzing of the information that has been gathered for determining how the attack was committed. To prevent the incident from happening again, it is vital to recognize how it was conceded out so that a prevention technique is applied. 5.Recovery: Recovery is the fifth step of the incident handling process. In this phase, the Incident Handler places the system back into the working environment. In the recovery phase the Incident Handler also works with the questions to validate that the system recovery is successful. This involves testing the system to make sure that all the processes and functions are working normal. The Incident Handler also monitors the system to make sure that the systems are not compromised again. It looks for additional signs of attack. 6.Lessons learned: Lessons learned is the sixth and the final step of incident handling process. The Incident Handler utilizes the knowledge and experience he learned during the handling of the incident to enhance and improve the incident-handling process. This is the most ignorant step of all incident handling processes. Many times the Incident Handlers are relieved to have systems back to normal and get busy trying to catch up other unfinished work. The Incident Handler should make documents related to the incident or look for ways to improve the process. Answer option C is incorrect. The post mortem review is one of the phases of the Incident response process.

QUESTION 5

Which of the following is a computer networking protocol used by hosts to retrieve IP address assignments and other configuration information?

A. SNMP

B. ARP

C. DHCP

D. Telnet

Correct Answer: C

The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a client-server architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database. In the absence of DHCP, all hosts on a network must be manually configured individually - a time-consuming and often error-prone undertaking. DHCP is popular with ISP\\'s because it allows a host to obtain a temporary IP address. Answer option B is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets. Answer option A is incorrect. The Simple Network Management Protocol (SNMP) allows a monitored device (for example, a router or a switch) to run an SNMP agent. This protocol is used for managing many network devices remotely. When a monitored device runs an SNMP agent, an SNMP server can then query the SNMP agent running on the device to collect information such as utilization statistics or device configuration information. An SNMP-managed network typically consists of three components: managed devices, agents, and one or more network management systems. Answer option D is incorrect. Telnet (Telecommunication network) is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility. Typically, Telnet provides access to a command-line interface on a remote host via a virtual terminal connection which consists of an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). User data is interspersed in-band with TELNET control information. Typically, the Telnet protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23.