



212-82^{Q&As}

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.passapply.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

Lorenzo, a security professional in an MNC, was instructed to establish centralized authentication, authorization, and accounting for remote-access servers. For this purpose, he implemented a protocol that is based on the client-server model and works at the transport layer of the OSI model.

Identify the remote authentication protocol employed by Lorenzo in the above scenario.

- A. SNMPv3
- B. RADIUS
- C. POP3S
- D. IMAPS

Correct Answer: B

Explanation: The correct answer is B, as it identifies the remote authentication protocol employed by Lorenzo in the above scenario. RADIUS (Remote Authentication Dial-In User Service) is a protocol that provides centralized authentication, authorization, and accounting (AAA) for remote-access servers such as VPNs (Virtual Private Networks), wireless networks, or dial-up connections. RADIUS is based on the client-server model and works at the transport layer of the OSI model. RADIUS uses UDP (User Datagram Protocol) as its transport protocol and encrypts only user passwords in its messages. In the above scenario, Lorenzo implemented RADIUS to provide centralized AAA for remote-access servers. Option A is incorrect, as it does not identify the remote authentication protocol employed by Lorenzo in the above scenario. SNMPv3 (Simple Network Management Protocol version 3) is a protocol that provides network management and monitoring for network devices such as routers, switches, servers, or printers. SNMPv3 is based on the manager-agent model and works at the application layer of the OSI model. SNMPv3 uses UDP as its transport protocol and encrypts all its messages with AES (Advanced Encryption Standard) or DES (Data Encryption Standard). In the above scenario, Lorenzo did not implement SNMPv3 to provide network management and monitoring for network devices. Option C is incorrect, as it does not identify the remote authentication protocol employed by Lorenzo in the above scenario. POP3S (Post Office Protocol version 3 Secure) is a protocol that provides secure email access and retrieval for email clients from email servers. POP3S is based on the client-server model and works at the application layer of the OSI model. POP3S uses TCP (Transmission Control Protocol) as its transport protocol and encrypts all its messages with SSL (Secure Sockets Layer) or TLS (Transport Layer Security). In the above scenario, Lorenzo did not implement POP3S to provide secure email access and retrieval for email clients from email servers. Option D is incorrect, as it does not identify the remote authentication protocol employed by Lorenzo in the above scenario. IMAPS (Internet Message Access Protocol Secure) is a protocol that provides secure email access and management for email clients from email servers. IMAPS is based on the client-server model and works at the application layer of the OSI model. IMAPS uses TCP as its transport protocol and encrypts all its messages with SSL or TLS. In the above scenario, Lorenzo did not implement IMAPS to provide secure email access and management for email clients from email servers. References: , Section 8.2

QUESTION 2

Leilani, a network specialist at an organization, employed Wireshark for observing network traffic. Leilani navigated to the Wireshark menu icon that contains items to manipulate, display and apply filters, enable, or disable the dissection of protocols, and configure user-specified decodes.

Identify the Wireshark menu Leilani has navigated in the above scenario.

- A. Statistics



- B. Capture
- C. Main toolbar
- D. Analyze

Correct Answer: B

Explanation: Capture is the Wireshark menu that Leilani has navigated in the above scenario. Wireshark is a network analysis tool that captures and displays network traffic in real-time or from saved files. Wireshark has various menus that contain different items and options for manipulating, displaying, and analyzing network data. Capture is the Wireshark menu that contains items to start, stop, restart, or save a live capture of network traffic. Capture also contains items to configure capture filters, interfaces, options, and preferences. Statistics is the Wireshark menu that contains items to display various statistics and graphs of network traffic, such as packet lengths, protocols, endpoints, conversations, etc. Main toolbar is the Wireshark toolbar that contains icons for quick access to common functions, such as opening or saving files, starting or stopping a capture, applying display filters, etc. Analyze is the Wireshark menu that contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, and configure user-specified decodes.

QUESTION 3

George, a security professional at an MNC, implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. Identify the type of Internet access policy implemented by George in this scenario.

- A. Permissive policy
- B. Paranoid policy
- C. Prudent policy
- D. Promiscuous policy

Correct Answer: A

Explanation: Permissive policy is the type of Internet access policy implemented by George in this scenario. An Internet access policy is a policy that defines the rules and guidelines for accessing the Internet from a system or network. An Internet access policy can be based on various factors, such as security, productivity, bandwidth, etc. An Internet access policy can have different types based on its level of restriction or control. A permissive policy is a type of Internet access policy that allows users to access any site, download any application, and access any computer or network without any restrictions. A permissive policy can be used to provide maximum flexibility and freedom to users, but it can also pose significant security risks and challenges. In the scenario, George implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. This means that he implemented a permissive policy for those employees. A paranoid policy is a type of Internet access policy that blocks or denies all Internet access by default and only allows specific sites, applications, or computers that are explicitly authorized. A prudent policy is a type of Internet access policy that allows most Internet access but blocks or restricts some sites, applications, or computers that are deemed inappropriate, malicious, or unnecessary. A promiscuous policy is not a type of Internet access policy, but a term that describes a network mode that allows a network interface card (NIC) to capture all packets on a network segment, regardless of their destination address.

QUESTION 4



An organization's risk management team identified the risk of natural disasters in the organization's current location. Because natural disasters cannot be prevented using security controls, the team suggested to build a new office in another location to eliminate the identified risk. Identify the risk treatment option suggested by the risk management team in this scenario.

- A. Risk modification
- B. Risk avoidance
- C. Risk sharing
- D. Risk retention

Correct Answer: B

Explanation: Risk avoidance is the risk treatment option suggested by the risk management team in this scenario. Risk avoidance is a risk treatment option that involves eliminating the identified risk by changing the scope, requirements, or objectives of the project or activity. Risk avoidance can be used when the risk cannot be prevented using security controls or when the risk outweighs the benefits. References: Risk Avoidance

QUESTION 5

Giovanni, a system administrator, was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. Identify the type of account created by Giovanni in this scenario.

- A. Third-party account
- B. Group-based account
- C. Shared account
- D. Application account

Correct Answer: B

Explanation: Group-based account is the type of account created by Giovanni in this scenario. An account is a set of credentials, such as a username and a password, that allows a user to access a system or network. An account can have different types based on its purpose or usage. A group-based account is a type of account that allows multiple users to access a system or network with the same credentials and permissions. A group-based account can be used to simplify the management of users and resources by assigning them to groups based on their roles or functions. In the scenario, Giovanni was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. This means that he created a group-based account for those employees. A third-party account is a type of account that allows an external entity or service to access a system or network with limited permissions or scope. A shared account is a type of account that allows multiple users to access a system or network with the same credentials but different permissions. An application account is a type of account that allows an application or software to access a system or network with specific permissions or functions.