Certiport CyberSecurity Certification Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which protocol is used to test and verify network connectivity?

A. HTTP

B. Ping/ICMP

C. FTP

D. SNMP

2. What type of protocol is UDP?

A. Connection-based protocol

B. Connection-less protocol

C. Reliable protocol

D. Secure protocol

3. What is the primary focus of the Gramm-Leach-Bliley Act (GLBA)?

A. Consumer protection relating to financial privacy

B. Health records confidentiality

C. Data protection in educational institutions

D. Privacy rights in the digital environment

4. What action can an attacker take to prevent internet access to users?

A. Encrypt the network traffic.

B. Substitute an invalid IP address for the DNS server.

C. Substitute an invalid MAC address for the network gateway.

D. Install a firewall on the network.

5. What type of attack identifies a specific individual as the target using personalized information?

A. General phishing

B. Vishing

C. Spear phishing

D. Smishing

6. Which layer of the OSI model is responsible for routing data?

A. Data Link Layer

B. Network Layer

C. Presentation Layer

D. Application Layer

7. Which Act regulates the privacy of consumer financial information?

A. GDPR

B. FERPA

C. GLBA

D. HIPAA

8. War driving is an example of what type of reconnaissance?

A. Passive reconnaissance

B. Active reconnaissance

C. Social engineering

D. Network scanning

9. Which protocol is associated with port 161?

A. HTTP

B. SNMP

C. DNS

D. FTP

10. What does confidentiality in cybersecurity focus on?

A. Access restriction for unauthorized users

B. Availability of information for authorized users

C. Data integrity verification

D. User authentication processes

Answers

1. B
2. B
3. A
4. C
5. C
6. B
7. C
8. B
9. B
10. A

Explanations

1. Which protocol is used to test and verify network connectivity?

A. HTTP

B. Ping/ICMP

C. FTP

D. SNMP

The protocol used to test and verify network connectivity is Ping, which operates using the Internet Control Message Protocol (ICMP). Ping works by sending an echo request to a specific IP address and then waiting for an echo reply. This process helps determine not only if a device is reachable over the network but also provides information about the round-trip time taken for packets to travel to the destination and back. It's a vital tool for network troubleshooting, allowing administrators to assess the status and responsiveness of devices within a network. In contrast, Hypertext Transfer Protocol (HTTP) is primarily used for transferring web pages and is not designed for connectivity testing. File Transfer Protocol (FTP) focuses on transferring files between clients and servers, while Simple Network Management Protocol (SNMP) is used for network management and monitoring, not for basic connectivity checks. Therefore, the capability and specific purpose of Ping/ICMP for connectivity verification make it the correct choice in this context.

2. What type of protocol is UDP?

A. Connection-based protocol

B. Connection-less protocol

C. Reliable protocol

D. Secure protocol

UDP, or User Datagram Protocol, is classified as a connection-less protocol. This means that it does not establish a dedicated end-to-end connection before data is transmitted. Instead, UDP sends packets, known as datagrams, to the destination without ensuring that the recipient is ready to receive them or that the packets arrive in order. This characteristic allows UDP to offer lower latency in data transmission since there is no need for the overhead associated with establishing and maintaining a connection, making it suitable for applications where speed is critical, such as video streaming, online gaming, and VoIP (Voice over Internet Protocol). In contrast to connection-oriented protocols like TCP (Transmission Control Protocol), which guarantee the delivery of packets in the correct order and handle retransmissions if packets are lost, UDP does not provide such reliability mechanisms. This lack of connection setup and error-checking can facilitate faster communication, but it also means that some packets may be lost or arrive out of order without any notification to the sender or receiver.

3. What is the primary focus of the Gramm-Leach-Bliley Act (GLBA)?

A. Consumer protection relating to financial privacy

B. Health records confidentiality

C. Data protection in educational institutions

D. Privacy rights in the digital environment

The Gramm-Leach-Bliley Act (GLBA) primarily focuses on consumer protection relating to financial privacy. This legislation was enacted to ensure that financial institutions establish privacy practices that safeguard the personal data of consumers. Specifically, the GLBA requires these institutions to provide customers with a privacy notice that outlines their data collection practices, sharing policies, and the rights of consumers regarding their information. The act also mandates that financial institutions implement safeguards to protect sensitive customer information from unauthorized access and disclosure. This ensures that individuals' financial data is handled with care and transparency, creating a framework for maintaining consumer trust in financial services. While the other options address important areas of privacy and confidentiality, they are not the focus of the GLBA. Health records confidentiality is covered under the Health Insurance Portability and Accountability Act (HIPAA), data protection in educational institutions is governed by laws like the Family Educational Rights and Privacy Act (FERPA), and privacy rights in the digital environment may relate to broader regulatory measures such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). However, none of these are the primary concerns of the GLBA.

4. What action can an attacker take to prevent internet access to users?

A. Encrypt the network traffic.

B. Substitute an invalid IP address for the DNS server.

C. Substitute an invalid MAC address for the network gateway.

D. Install a firewall on the network.

Substituting an invalid MAC address for the network gateway can effectively disrupt internet access for users on a local network. The media access control (MAC) address is a unique identifier assigned to network interfaces for communications on the physical network segment. By replacing the valid MAC address of the gateway with an invalid one, the attacker can cause devices on the network to be unable to route their traffic to the outside world. This type of action misleads the devices about where to send their requests for internet access, effectively isolating them from the network gateway that connects to the internet. Without a valid pathway to the gateway, the devices will experience a loss of connectivity, preventing users from accessing online resources. In contrast to this, encrypting network traffic protects data but does not stop users from accessing the internet. Substituting an invalid IP address for the DNS server would disrupt name resolution but not necessarily prevent internet access altogether, as users could still connect using direct IP addresses. Installing a firewall may control traffic flow and enhance security but is not inherently an action that would prevent internet access to users; rather, it can be configured to allow or deny access based on certain rules.

5. What type of attack identifies a specific individual as the target using personalized information?

A. General phishing

B. Vishing

C. Spear phishing

D. Smishing

The correct answer is spear phishing, which is a targeted attack aimed at a specific individual or organization. Unlike general phishing attacks that use broad and generic information to deceive many potential victims, spear phishing employs personalized information that makes the communication appear more legitimate and credible. This can include the use of the target's name, job title, or references to specific projects or relationships. By utilizing this tailored approach, attackers increase the likelihood of the target taking the bait, such as clicking on a malicious link or disclosing sensitive information. The effectiveness of spear phishing lies in its ability to exploit trust and the personal nature of the communication, making it a dangerous form of cyber threat. In contrast, other forms of phishing—such as vishing (voice phishing) and smishing (SMS phishing)—may use different mediums or tactics, but they do not specifically focus on the individualization that spear phishing does.

6. Which layer of the OSI model is responsible for routing data?

A. Data Link Layer

B. Network Layer

C. Presentation Layer

D. Application Layer

The Network Layer is responsible for routing data within the OSI model. It serves as a key component of the network's communication process, allowing data packets to be directed through various paths between devices and across different networks. At this layer, logical addressing is applied, meaning that each device is assigned an IP address, which is essential for routing data to its intended destination. The Network Layer interprets the IP address of both the source and the destination, making routing decisions based on this information. It also handles packet forwarding and can determine the best transmission paths through routing tables and protocols, which are critical for effective data communication, especially in large or complex networks. Understanding the responsibilities of the Network Layer is crucial for managing data transmission over networks, as it ensures that data travels efficiently and accurately between devices, adapting to network conditions and potential obstacles during transit. Other layers of the OSI model have their specific functions; for instance, the Data Link Layer focuses on the physical addressing and error detection and correction on the same local network, while the Presentation Layer is concerned with translating data formats and encryption. The Application Layer interfaces directly with end-user applications but does not concern itself with routing data.

7. Which Act regulates the privacy of consumer financial information?

A. GDPR

B. FERPA

C. GLBA

D. HIPAA

The Gramm-Leach-Bliley Act (GLBA) primarily focuses on the protection of consumer financial information by requiring financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. This act establishes the importance of privacy in the financial sector, mandating that institutions take measures to ensure the confidentiality and security of consumer data. By requiring the creation of privacy notices and allowing consumers to opt-out of certain information-sharing practices, GLBA aims to provide consumers with greater control over their personal financial information. This makes it the appropriate regulation regarding the privacy of consumer financial data, distinguishing it from acts that pertain to education or health information.

8. War driving is an example of what type of reconnaissance?

A. Passive reconnaissance

B. Active reconnaissance

C. Social engineering

D. Network scanning

War driving is classified as active reconnaissance because it involves actively searching for wireless networks while driving around in a vehicle. This method of reconnaissance typically includes the use of a device to detect and map out the locations of Wi-Fi networks, often with the intent of assessing their security measures. In active reconnaissance, the person conducting the reconnaissance engages directly with the target environment, specifically querying systems or networks to gather information. This proactive approach contrasts with passive reconnaissance, where the information is gathered without directly interacting with the target, often through observation, open-source intelligence, or other non-intrusive means. By employing active techniques, such as war driving, an attacker can gain a clearer understanding of which networks are available, their security configurations, and any potential vulnerabilities that could be exploited later.

9. Which protocol is associated with port 161?

A. HTTP

B. SNMP

C. DNS

D. FTP

Port 161 is specifically associated with the Simple Network Management Protocol (SNMP). This protocol is primarily used for network management, allowing devices such as routers, switches, and servers to communicate management information. SNMP operates by using a client-server model where management systems (the clients) can gather data from agents (the servers) on network devices. SNMP enables monitoring of network performance, as well as configuration changes and event logging. Utilizing port 161, it allows for the transmission of messages to and from managed devices effectively. This is particularly important for network administrators who need to ensure that their infrastructure operates smoothly and any issues can be identified and resolved quickly. In contrast, the other protocols listed are associated with different ports: HTTP typically uses port 80, DNS operates on port 53, and FTP usually utilizes ports 20 and 21. These differing uses highlight the specific purpose and function of port 161 in the context of network management.

10. What does confidentiality in cybersecurity focus on?

A. Access restriction for unauthorized users

B. Availability of information for authorized users

C. Data integrity verification

D. User authentication processes

Confidentiality in cybersecurity specifically emphasizes protecting information from unauthorized access. This means ensuring that only individuals or systems that have been granted permission can view or use certain data. The primary goal is to safeguard sensitive information, so it is kept private and secure from malicious actors or unintended users. Implementing access restrictions for unauthorized users is fundamental to maintaining confidentiality, as it controls who can interact with information and prevents breaches. In contrast, the other choices focus on different aspects of cybersecurity. While availability pertains to ensuring that authorized users can access information when needed, and data integrity involves verifying that information has not been altered or tampered with, these concepts are separate from the primary aim of confidentiality. User authentication processes also relate to how users are verified before gaining access but are more about assurance of identity rather than the broader concept of maintaining confidentiality of data.