CREST Practitioner Security Analyst (CPSA) Practice (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What does TKIP aim to replace?

A. AES

B. WEP

C. SSL

D. IPSec

2. The Payment Card Industry Data Security Standard is commonly referred to as what?

A. PCI DSS

B. PCI Standards

C. Payment Security Standards

D. Data Protection Standards

3. Which of the following protocols is Cisco's proprietary Layer 2 protocol used for gathering information about neighboring devices?

A. VTP

B. HSRP

C. CDP

D. STP

4. Which of the following acts is referred to as GDPR for the UK?

A. Data Protection Act 1998

B. Computer Misuse Act 1990

C. Human Rights Act 1998

D. Freedom of Information Act 2000

5. Which command in Oracle retrieves the current user?

A. SELECT user FROM dual

B. SELECT CURRENT_USER

C. SELECT username FROM all_users

D. SELECT instance_name FROM v$instance

6. Which protocol operates on Port 143?

A. Internet Message Transfer Protocol

B. Internet Message Access Protocol

C. Simple Mail Transfer Protocol

D. Post Office Protocol

7. What does IETF stand for?

A. Internet Engineering Task Framework

B. Internet Engineering Task Force

C. International Engineering Task Force

D. Internet Evaluation Task Force

8. What is the classification for Windows XP 64 bit?

A. NT 5.1

B. NT 5.2

C. NT 6.0

D. NT 4.0

9. What characterizes a DDoS attack?

A. An attack from a single computer

B. An attempt to exploit software vulnerabilities

C. An overwhelming flood of requests from multiple computers

D. A circumvention of security protocols

10. Which protocol is primarily used to prevent network loops by adopting a dynamic routing method?

A. STP

B. DHCP

C. VRRP

D. CDP

Answers

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

Explanations

1. What does TKIP aim to replace?

A. AES

B. WEP

C. SSL

D. IPSec

TKIP, or Temporal Key Integrity Protocol, was introduced as a part of the IEEE 802.11i standard to enhance the security of wireless networks. It specifically aims to replace WEP, which is Wired Equivalent Privacy, a protocol that was widely used but had significant security vulnerabilities. WEP utilized static encryption keys, making it susceptible to various attacks such as key reuse and IV (Initialization Vector) attacks. TKIP addresses these vulnerabilities by implementing a per-packet keying mechanism, which generates a unique encryption key for each data packet. This improvement provides a stronger level of security for wireless communication by ensuring that even if one key is compromised, it does not jeopardize the security of subsequent packets. In contrast, options like AES (Advanced Encryption Standard), SSL (Secure Sockets Layer), and IPSec (Internet Protocol Security) serve different roles and contexts in the security infrastructure. AES is a symmetric encryption standard that can be used independently of TKIP. SSL is a protocol for establishing secure connections over a computer network, often used in web communications, while IPSec is used primarily for securing IP communications by authenticating and encrypting each IP packet. None of these directly relate to the specific improvements TKIP brings to replace WEP's weaknesses.

2. The Payment Card Industry Data Security Standard is commonly referred to as what?

A. PCI DSS

B. PCI Standards

C. Payment Security Standards

D. Data Protection Standards

The widely recognized term for the Payment Card Industry Data Security Standard is indeed PCI DSS. This acronym stands for Payment Card Industry Data Security Standard, which outlines a collection of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI DSS is critical for safeguarding sensitive payment card data against theft and fraud, providing guidelines that help organizations protect cardholder information. The use of PCI DSS as the standard terminology is vital for clear communication within the payment card industry, as it encompasses specific requirements and practices that entities must follow to comply with this standard. Understanding this term is crucial for professionals in security and compliance roles, as it is a key aspect of data security related to payment processing.

3. Which of the following protocols is Cisco's proprietary Layer 2 protocol used for gathering information about neighboring devices?

A. VTP

B. HSRP

C. CDP

D. STP

The correct answer is CDP, which stands for Cisco Discovery Protocol. It is a proprietary Layer 2 protocol developed by Cisco to facilitate the discovery of neighboring devices in a network. CDP operates at the Data Link layer of the OSI model, allowing devices to exchange information such as device IDs, IP addresses, software versions, and capabilities. When a device running CDP is connected to the network, it periodically sends out CDP packets to identify its neighboring Cisco devices. Those devices, in turn, respond with their information, enabling the original device to build a comprehensive view of the network topology. This capability is especially useful for network management and troubleshooting, as it helps administrators understand how devices are interconnected. Other protocols listed serve different purposes: - VTP (VLAN Trunking Protocol) is used in managing VLANs across a network. - HSRP (Hot Standby Router Protocol) is for providing redundancy in IP routers. - STP (Spanning Tree Protocol) is used to prevent loops in network topologies. CDP uniquely focuses on gathering and sharing information about neighboring devices, making it the correct choice in this context.

4. Which of the following acts is referred to as GDPR for the UK?

A. Data Protection Act 1998

B. Computer Misuse Act 1990

C. Human Rights Act 1998

D. Freedom of Information Act 2000

The Data Protection Act 1998 corresponds to the framework established for data protection in the UK prior to the introduction of the General Data Protection Regulation (GDPR). However, it's important to note that while the Data Protection Act 1998 was in effect, it was replaced by the Data Protection Act 2018, which implements the GDPR into UK law. This new legislation builds upon the principles set out in the GDPR and adapts them for the context of UK law following Brexit. Therefore, while the Data Protection Act 1998 is not currently in line with GDPR standards, it is the legislation that initially established data protection rights in the UK. The other options listed represent different areas of law that do not directly pertain to data protection. The Computer Misuse Act focuses on computer-related offenses, the Human Rights Act pertains to human rights legislation, and the Freedom of Information Act deals with access to information held by public authorities. These laws serve different purposes and are not directly related to data protection in the context of GDPR.

5. Which command in Oracle retrieves the current user?

A. SELECT user FROM dual

B. SELECT CURRENT_USER

C. SELECT username FROM all_users

D. SELECT instance_name FROM v$instance

The command that retrieves the current user in Oracle is indeed the one that uses the dual table. The dual table is a special one-row, one-column table present by default in all Oracle databases. It is often used for selecting a single value or for performing calculations without needing an actual table. When you execute "SELECT user FROM dual", Oracle returns the username of the connected user. This is because the 'user' function, when queried, provides the current schema for the session. While other options contain valid SQL queries, they do not specifically return the current user in the same context. "SELECT CURRENT_USER" would also return the current user, but it is not the most common or idiomatic way to achieve this in Oracle, making it less favorable in certain contexts. The commands querying from all_users and v$instance are suited for different purposes, such as listing all users and retrieving instance information, respectively, and do not focus on returning the current user.

6. Which protocol operates on Port 143?

A. Internet Message Transfer Protocol

B. Internet Message Access Protocol

C. Simple Mail Transfer Protocol

D. Post Office Protocol

The protocol that operates on Port 143 is the Internet Message Access Protocol (IMAP). IMAP is designed for email retrieval, allowing users to access their mail stored on a remote server while keeping their email organized. This protocol facilitates complex email functionalities, such as managing multiple folders, synchronizing messages across different devices, and maintaining read/unread statuses. When working with email, IMAP is particularly relevant in scenarios where users require relevant access to their email from various locations and devices. Unlike other protocols, such as POP, IMAP enables the email to remain on the server, facilitating more versatile and efficient management of email accounts. In contrast, other protocols have different primary functions and port assignments. Internet Message Transfer Protocol (SMTP) generally operates on Port 25 and is used for sending or relaying email messages. Simple Mail Transfer Protocol serves a very specific purpose of delivering mails rather than fetching them. Post Office Protocol (POP) runs primarily on Port 110 and is designed for users who want to download emails from their server to the local computer for offline access. Understanding these distinctions helps clarify why the Internet Message Access Protocol is the correct answer associated with Port 143.

7. What does IETF stand for?

A. Internet Engineering Task Framework

B. Internet Engineering Task Force

C. International Engineering Task Force

D. Internet Evaluation Task Force

The correct answer is "Internet Engineering Task Force." This organization plays a crucial role in developing and promoting voluntary Internet standards, particularly those related to the Internet Protocol Suite (TCP/IP). The IETF is composed of a large community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The name signifies its focus on tasks related to engineering in the context of Internet technology and standards. Specifically, the term “Task Force” indicates a group dedicated to a particular objective, which in this case involves the engineering and enhancement of Internet protocols. In contrast, the other options either misrepresent the organization's purpose, offer incorrect terminology, or use the wrong qualifiers. For instance, “Internet Engineering Task Framework” and “International Engineering Task Force” incorrectly replace "Force" with "Framework" and misstate the global aspect of the organization, which is primarily focused on the Internet rather than international engineering. The term “Internet Evaluation Task Force” is also inaccurate because it suggests a focus on evaluation rather than engineering of Internet protocols. Therefore, "Internet Engineering Task Force" accurately reflects the group’s mission and activities.

8. What is the classification for Windows XP 64 bit?

A. NT 5.1

B. NT 5.2

C. NT 6.0

D. NT 4.0

The classification for Windows XP 64 bit is NT 5.2. Windows XP itself is built on the Windows NT architecture, and the specific versioning of Windows XP recognizes different variations based on the architecture it supports. The standard 32-bit version of Windows XP is classified as NT 5.1, while Windows XP Professional x64 Edition specifically aligns with NT 5.2 due to its ability to support 64-bit processing. This distinction is essential for understanding the technical capabilities and system requirements associated with different versions of Windows. The other classifications mentioned do not correspond to the 64-bit version of Windows XP. NT 6.0 pertains to Windows Vista, and NT 4.0 reflects an earlier generation of Windows operating systems. Understanding these classifications is crucial for identifying compatibility and features when working with various versions of Windows operating systems.

9. What characterizes a DDoS attack?

A. An attack from a single computer

B. An attempt to exploit software vulnerabilities

C. An overwhelming flood of requests from multiple computers

D. A circumvention of security protocols

A DDoS (Distributed Denial of Service) attack is characterized by an overwhelming flood of requests coming from multiple computers, often coordinated to target a single system. This simultaneous barrage of traffic aims to exhaust the resources of the targeted server or network, causing it to slow down significantly or even crash, rendering it unavailable to legitimate users. The nature of this attack involves distributed sources, meaning that numerous compromised computers, often part of a botnet, launch the attacks in concert. This makes it difficult to mitigate, as the traffic comes from many different IP addresses, which complicates the task of filtering out malicious requests. In contrast, an attack from a single computer does not meet the definition of a DDoS attack since it lacks the distributed nature that characterizes such incidents. Similarly, while exploiting software vulnerabilities can be part of different attack strategies, it does not directly relate to the defining features of a DDoS attack. The circumvention of security protocols, while relevant to various types of attacks, does not specifically characterize the overwhelming nature of a DDoS assault.

10. Which protocol is primarily used to prevent network loops by adopting a dynamic routing method?

A. STP

B. DHCP

C. VRRP

D. CDP

The protocol primarily used to prevent network loops by adopting a dynamic routing method is Spanning Tree Protocol (STP). STP is designed to detect and eliminate loops in a network topology that could lead to broadcast storms and other issues that degrade network performance. It works by creating a logical tree structure that spans all the switches in a network while blocking redundant paths, ensuring that there is only one active path between any two network devices. In this context, dynamic routing methods involve protocols that automatically adjust the paths data packets take through the network as changes occur, such as link failures or additions. However, while dynamic routing protocols like OSPF or EIGRP do not directly prevent loops, STP specifically addresses the loop issue within switched Ethernet networks. The other protocols listed serve different functions: DHCP (Dynamic Host Configuration Protocol) is responsible for assigning IP addresses to devices on a network; VRRP (Virtual Router Redundancy Protocol) provides high availability and failover for routers; and CDP (Cisco Discovery Protocol) is a network discovery tool used to gather information about the directly connected Cisco devices. None of these protocols are designed primarily for loop prevention in the context of network topology management.