Palo Alto Networks (PANW) Certified Cybersecurity Entry-level Technician (PCCET) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Don’t worry about getting everything right, your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations, and take breaks to retain information better.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning.

7. Use Other Tools

Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly — adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. Which action is associated with Web 3.0?

A. Checking CNN's website for news

B. Posting on Facebook

C. Adding information to Wikipedia

D. Asking Apple's Siri a question

2. What does TCP stand for in network communication?

A. Transmission Control Protocol

B. Transfer Control Protocol

C. Transmission Congestion Protocol

D. Transfer Congestion Protocol

3. Which stage of an attack is typically east-west traffic?

A. Reconnaissance

B. Weaponization

C. Lateral spread

D. Actions on the objective

4. Who is the most likely target of social engineering?

A. Executive management, because it has the most permissions

B. Senior IT engineers, because the attacker hopes to get them to disable the security infrastructure

C. Junior people, because they are easier to stress and probably not as well trained

D. The accounting department, because it can wire money directly to the attacker's account

5. Which business objective includes details about how the Security Operations organization will achieve its goals?

A. Budget

B. Mission

C. Governance

D. Planning

6. Which device processes logical addresses?

A. Hub

B. Switch

C. WiFi access point

D. Router

7. What is the theoretical maximum number of devices in a class B?

A. 2^24-2 = 16777214

B. 2^20-2 = 1048574

C. 2^16-2 = 65534

D. 2^8-2 = 254

8. Organizations are using which resource to expand their on-premises private cloud compute capacity?

A. Software Defined Data Centers

B. Public Cloud

C. Virtual Storage

D. Virtual Networks

9. What does the acronym CIDR represent?

A. Classful Inter Dependant Routing

B. Classless Inter-Domain Routing

C. Classless Inter Dependant Routing

D. Classful Inter Domain Routing

10. What does CVE stand for?

A. Computer Vulnerabilities and their Exploits

B. Common Vulnerabilities and their Exploits

C. Common Vulnerabilities and Exposures

D. Computer Vulnerabilities and Exposures

Answers

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

Explanations

1. Which action is associated with Web 3.0?

A. Checking CNN's website for news

B. Posting on Facebook

C. Adding information to Wikipedia

D. Asking Apple's Siri a question

Web 3.0 represents a new era of the internet characterized by decentralized networks, enhanced user interaction, and the ability to understand and process information in a more intelligent way. Asking Apple's Siri a question exemplifies Web 3.0 capabilities as it involves the use of an AI-driven virtual assistant that can interpret voice commands, understand context, and deliver personalized responses. This interaction signifies a shift toward more intelligent systems that can engage in dialog and provide service in a way that goes beyond traditional web interactions. In contrast, options like checking CNN's website for news, posting on Facebook, and adding information to Wikipedia are more representative of earlier web functions. These actions involve more static content consumption or social media interaction rather than the intelligent, semantic web capabilities highlighted in Web 3.0. The evolution toward AI and decentralized data interaction is central to understanding the advancements that define this new phase of the internet.

2. What does TCP stand for in network communication?

A. Transmission Control Protocol

B. Transfer Control Protocol

C. Transmission Congestion Protocol

D. Transfer Congestion Protocol

TCP stands for Transmission Control Protocol in network communication. It is one of the primary protocols in the Internet Protocol Suite, widely used for transmitting data over networks. TCP is responsible for ensuring reliable, ordered, and error-checked delivery of data packets between applications running on hosts communicating over an IP network. The significance of TCP lies in its ability to establish a robust connection between a client and a server, managing the transfer of data in a way that guarantees all packets are received and in the correct sequence. This is crucial for applications that require high integrity of data, such as web browsing and email. In contrast, the other options do not accurately define TCP or its purpose. For example, "Transfer Control Protocol," "Transmission Congestion Protocol," and "Transfer Congestion Protocol" do not exist as standardized networking terms and fail to capture the essence and functionality of TCP as established in network communication protocols.

3. Which stage of an attack is typically east-west traffic?

A. Reconnaissance

B. Weaponization

C. Lateral spread

D. Actions on the objective

In a cybersecurity context, east-west traffic refers to the movement of data within a network, particularly between devices on the same local area network (LAN) as opposed to traffic that originates from outside the network and travels into it. The stage of an attack known as lateral spread is characterized by attackers moving through the network after they have gained an initial foothold, attempting to access other devices, resources, or sensitive data. During the lateral spread stage, attackers often exploit vulnerabilities or utilize compromised credentials to navigate across the network from one system to another, which constitutes east-west traffic. This movement is aimed at broadening their access and control over the network, allowing them to compromise additional systems, extract valuable information, or establish persistence by creating backdoors. The other stages identified in the question serve different purposes: - Reconnaissance involves gathering information about the target before an attack occurs and typically generates north-south traffic (inbound or outbound). - Weaponization is about creating a malicious payload or exploit that will be used in the attack, and while it may involve some internal communication for preparation, it doesn't focus on movement within the network like lateral spread does. - Actions on the objective refers to the final efforts made by the attacker after achieving their goal

4. Who is the most likely target of social engineering?

A. Executive management, because it has the most permissions

B. Senior IT engineers, because the attacker hopes to get them to disable the security infrastructure

C. Junior people, because they are easier to stress and probably not as well trained

D. The accounting department, because it can wire money directly to the attacker's account

The most likely target of social engineering is often junior employees, as they tend to be less experienced and might not be as well-equipped to recognize or respond to manipulative tactics used by attackers. Such individuals may lack the training or awareness needed to suspect that a seemingly legitimate request, like sharing credentials or clicking on a malicious link, could be part of a manipulation attempt. Social engineering relies heavily on exploiting human psychology, and junior personnel may be more prone to stress and pressure, making them more susceptible to the instigator's tactics. They may feel the urgency to comply due to their position or inexperience, leading to a higher chance of falling victim to the scheme. While other options present valid targets for social engineering attacks, they generally involve more specialized knowledge or established protocols that may be harder to bypass. For instance, targeting executive management or senior IT engineers often requires in-depth research and sophistication that attackers might not always have at their disposal. Meanwhile, the accounting department, while a potential target for financial fraud, may involve more extensive verification processes that could deter immediate compliance compared to junior employees.

5. Which business objective includes details about how the Security Operations organization will achieve its goals?

A. Budget

B. Mission

C. Governance

D. Planning

The business objective that includes details about how the Security Operations organization will achieve its goals is the planning aspect. Planning involves developing strategies and establishing specific actions needed to meet the organization's security objectives. This includes defining priorities, allocating resources, setting timelines, and outlining the procedures to be followed. By creating a comprehensive plan, the Security Operations team can effectively address potential threats, align with business goals, and ensure that all team members understand their roles and responsibilities in achieving these objectives. While other options like mission and governance are related to the overall framework within which the security operations function, planning is distinctly focused on the actionable steps required to fulfill the organization's security goals. Budget, on the other hand, focuses primarily on financial aspects, which, while important, do not detail the processes and strategies necessary for achieving security objectives.

6. Which device processes logical addresses?

A. Hub

B. Switch

C. WiFi access point

D. Router

The device that processes logical addresses is the router. Routers operate at the network layer (Layer 3) of the OSI model, which is responsible for routing data between different networks based on logical addressing, typically using IP addresses. When data packets are sent across networks, routers determine the best path to take based on the destination IP address. They examine the packet's logical address and make forwarding decisions to direct the traffic toward the appropriate network. This capability is essential for facilitating communication between disparate networks, such as connecting a home network to the internet or connecting different segments of an organization's internal network. In contrast, hubs and switches operate at lower layers. Hubs simply transmit data to all connected devices without processing any addressing information; they operate at the physical layer. Switches, while more intelligent than hubs, still primarily deal with data link layer addressing (such as MAC addresses) to forward frames within the same local area network rather than handling logical (IP) addresses that span multiple networks. WiFi access points also serve to connect wireless devices to a network but do not perform any routing functions or logical address processing. Thus, routers uniquely fulfill the role of processing logical addresses in network communications.

7. What is the theoretical maximum number of devices in a class B?

A. 2^24-2 = 16777214

B. 2^20-2 = 1048574

C. 2^16-2 = 65534

D. 2^8-2 = 254

In a Class B network, the subnet mask is typically 255.255.0.0, which uses the first 16 bits for the network portion and the remaining 16 bits for the host portion. The host portion is where devices (hosts) on the network are addressed. To determine the maximum number of usable host addresses in a Class B network, you calculate the total number of combinations available with the 16 bits designated for hosts, which is 2^16 (65536). However, in any network, two addresses are reserved: one for the network address and one for the broadcast address. Therefore, the actual number of usable addresses is calculated as follows: Total usable addresses = Total addresses - Reserved addresses = 2^16 - 2 = 65536 - 2 = 65534 This calculation reveals that the maximum theoretical number of devices that can be supported in a Class B network is indeed 65534. Thus, the correct interpretation of the maximum number of devices aligns directly with the provided answer that shows these computations accurately.

8. Organizations are using which resource to expand their on-premises private cloud compute capacity?

A. Software Defined Data Centers

B. Public Cloud

C. Virtual Storage

D. Virtual Networks

The public cloud is a resource increasingly utilized by organizations to expand their on-premises private cloud compute capacity. It allows businesses to leverage the additional resources available in the public cloud, effectively allowing for greater flexibility and scalability. By integrating public cloud services, organizations can manage sudden spikes in demand, maintain operational efficiency, and avoid the costs associated with over-provisioning on-premises infrastructure. This hybrid approach of combining on-premises private clouds with public cloud resources facilitates a more dynamic IT environment, as organizations can quickly access and utilize vast amounts of compute storage and processing power from public cloud providers without the need for significant upfront investment in hardware. This can optimize costs and resource management, support disaster recovery strategies, and enhance overall business agility. The other options, while relevant to cloud computing, do not specifically address the method of extending private cloud capacity. Software Defined Data Centers are about the technologies that create virtualized environments, virtual storage refers to physical storage management in a more abstract way, and virtual networks pertain to networking layers rather than compute capacity directly.

9. What does the acronym CIDR represent?

A. Classful Inter Dependant Routing

B. Classless Inter-Domain Routing

C. Classless Inter Dependant Routing

D. Classful Inter Domain Routing

The acronym CIDR stands for Classless Inter-Domain Routing. This method was introduced to improve the allocation of IP addresses and replace the older classful network design. CIDR allows for more efficient use of the available IP address space by enabling variable-length subnet masking (VLSM), which permits more granular control over how IP address space is divided. This capability helps reduce the overall number of entries in routing tables, making routing more efficient and scalable across the internet. By adopting a classless system, networks can be divided according to their actual needs rather than being limited to fixed class sizes, which often resulted in wasted IP addresses. Understanding CIDR is crucial for anyone involved in network design and management, as it significantly impacts how IP addressing and routing are handled in modern networking scenarios.

10. What does CVE stand for?

A. Computer Vulnerabilities and their Exploits

B. Common Vulnerabilities and their Exploits

C. Common Vulnerabilities and Exposures

D. Computer Vulnerabilities and Exposures

CVE stands for Common Vulnerabilities and Exposures. It refers to a list of publicly known cybersecurity vulnerabilities and exposures that provides a reference-method for publicly known information-security vulnerabilities and exposures. The CVE system aims to standardize the naming of these vulnerabilities, which allows security professionals to quickly identify and address them. By providing a unique identifier for each vulnerability, CVE facilitates easier sharing of data across various tools and services, leading to a more coordinated response to security risks. This uniformity helps organizations prioritize their security efforts and strategies effectively, as they can refer to the same common set of vulnerabilities. The introduction of CVE has proven essential for effective vulnerability management and threat intelligence, as it streamlines communication and enhances understanding across the cybersecurity community.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://panw-certifiedcybercecurityentryleveltechnician.examzify.com

We wish you the very best on your exam journey. You've got this!