PLTW Cybersecurity EOC Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What does a .bat file extension indicate?

- **A. Open a Security Protocol**
- **B. Open a Batch file script**
- **C. Open a Web page**
- **D. Open an Audio file**

2. What does SSL stand for?

- **A. Secure Socket Layer**
- **B. System Security Log**
- **C. Simple Secure Link**
- **D. Scalable Security Layer**

3. Which best describes a man-in-the-middle (MITM) attack?

- **A. An attack that involves physically accessing a system**
- **B. An attack where the attacker secretly intercepts and relays communication between two parties**
- **C. A cyber defense strategy using multiple safety measures**
- **D. An unauthorized access attempt on a secured server**

4. To duplicate a file, which command should you use?

- **A. cp**
- **B. mv**
- **C. rm**
- **D. touch**

5. Which encryption method uses the same key for both the encryption and decryption processes?

- **A. Public key encryption**
- **B. Symmetric key encryption**
- **C. Asymmetric key encryption**
- **D. Multi-factor encryption**

6. What does a Smurf Attack specifically target?

- **A. Individual computers**
- **B. Broadcast networks**
- **C. User keystrokes**
- **D. Data encryption**

7. What role does user education play in cybersecurity?

- **A. It promotes the purchasing of security software**
- **B. It helps individuals recognize threats and follow best practices to protect information**
- **C. It ensures compliance with security policies**
- **D. It reduces the financial costs of security breaches**

8. What is the function of Cloud9?

- **A. To provide virtual reality experiences**
- **B. To access data without harming local devices**
- **C. To manage cloud resources**
- **D. To develop standalone applications**

9. Which command is used to create a new directory?

- **A. mkdir**
- **B. rmdir**
- **C. cd**
- **D. cp**

10. Describe what a botnet is.

- **A. A software that enhances network performance**
- **B. A tool for securing computer systems**
- **C. A network of infected computers controlled by an attacker to perform malicious activities**
- **D. A collection of authorized user devices**

Answers

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

Explanations

1. What does a .bat file extension indicate?

A. Open a Security Protocol

B. Open a Batch file script

C. Open a Web page

D. Open an Audio file

A .bat file extension indicates that the file is a batch file script. Batch files are used primarily in Windows operating systems to execute a series of commands automatically. When a .bat file is run, the operating system processes each command in the file sequentially. These commands can include anything from launching programs, copying files, deleting files, or changing directory paths. The use of batch files is particularly useful for automating repetitive tasks, simplifying complex command sequences, or setting up environments for applications. This makes them an efficient tool for users who frequently perform similar operations. In contrast, the other options do not correspond to the .bat file extension. A .bat file does not relate to security protocols, web pages, or audio files, which have their own specific extensions and purposes. Therefore, recognizing .bat files as batch file scripts is crucial in understanding their functionality within the Windows environment.

2. What does SSL stand for?

A. Secure Socket Layer

B. System Security Log

C. Simple Secure Link

D. Scalable Security Layer

SSL stands for Secure Socket Layer. This is a standard security protocol that is used to establish an encrypted link between a web server and a browser. SSL is critical for ensuring that sensitive data transmitted over the internet, such as personal information, credit card numbers, and login credentials, is kept secure and private from eavesdroppers and attackers. The naming convention reflects its purpose: "Secure" indicates the encryption and protection of data, "Socket" refers to the way connections are established in networking, and "Layer" signifies that it operates at a specific layer within an internet protocol suite. The use of SSL has evolved, and it has been largely replaced by Transport Layer Security (TLS) in recent years, but the term SSL is still widely used in discussions about secure internet communications. Other options present alternative interpretations or combinations of terminology that do not accurately reflect the established meaning associated with this widely used security protocol.

3. Which best describes a man-in-the-middle (MITM) attack?

A. An attack that involves physically accessing a system

B. An attack where the attacker secretly intercepts and relays communication between two parties

C. A cyber defense strategy using multiple safety measures

D. An unauthorized access attempt on a secured server

A man-in-the-middle (MITM) attack is characterized by the attacker secretly intercepting and relaying communication between two parties who believe they are directly communicating with each other. In this type of attack, the attacker can alter or eavesdrop on the communication without either party being aware that their conversation has been compromised. This deceptive positioning allows the attacker to access sensitive information, such as login credentials or personal data, and manipulate the communication for malicious purposes. This definition aligns precisely with the nature of MITM attacks, emphasizing the covert interception of data which is fundamental to their operation. Understanding this mechanism is crucial for recognizing vulnerabilities in communication protocols and the importance of using encryption to secure data transfers, as it can prevent such attacks from occurring.

4. To duplicate a file, which command should you use?

A. cp

B. mv

C. rm

D. touch

The command used to duplicate a file in a Linux or Unix-based operating system is 'cp', which stands for "copy." When you use this command followed by the source file and the destination where you want the copy to be created, it creates an exact duplicate of the original file. For example, if you have a file named "document.txt" and you want to create a copy called "document_copy.txt," you would use the command: `cp document.txt document_copy.txt`. This results in two separate files, enabling you to edit or manipulate the duplicate without affecting the original. In contrast, the other commands serve different purposes: 'mv' is used to move or rename files, 'rm' is for removing files, and 'touch' primarily creates empty files or updates the timestamps on existing files. Therefore, for duplicating files, 'cp' is the appropriate and effective command to use.

5. Which encryption method uses the same key for both the encryption and decryption processes?

A. Public key encryption

B. Symmetric key encryption

C. Asymmetric key encryption

D. Multi-factor encryption

The correct answer is symmetric key encryption because this method relies on a single shared key to perform both the encryption and decryption processes. In symmetric key encryption, both the sender and the receiver must have access to the same key and keep it secret from unauthorized users. This approach is efficient in terms of speed and performance, making it suitable for encrypting large amounts of data. In contrast, public key encryption uses a pair of keys—a public key for encryption and a private key for decryption. This allows secure communications without needing to share a secret key in advance. Asymmetric key encryption refers to this type of encryption method, characterized by separate keys for encryption and decryption. Multi-factor encryption is not a standard type of encryption on its own; rather, it usually refers to the use of multiple authentication factors to enhance security. Thus, symmetric key encryption distinctly utilizes the same key throughout both stages of the process, distinguishing it clearly from the other methods mentioned.

6. What does a Smurf Attack specifically target?

A. Individual computers

B. Broadcast networks

C. User keystrokes

D. Data encryption

A Smurf Attack specifically targets broadcast networks by exploiting the Internet Control Message Protocol (ICMP). In this type of Distributed Denial of Service (DDoS) attack, the attacker sends ICMP Echo Request packets (commonly known as pings) to the broadcast address of a subnet. Each device on that subnet responds to the ping, creating a massive amount of traffic directed towards the target network's IP address. The use of the broadcast address amplifies the attack, as a single request can result in replies from multiple devices, overwhelming the target with traffic and causing denial of service. This makes broadcast networks particularly vulnerable to Smurf Attacks, as they can easily be flooded with responses, leading to network congestion and disruption of legitimate services. Understanding the nature of such attacks is crucial for implementing effective network security and mitigation strategies.

7. What role does user education play in cybersecurity?

A. It promotes the purchasing of security software

B. It helps individuals recognize threats and follow best practices to protect information

C. It ensures compliance with security policies

D. It reduces the financial costs of security breaches

User education plays a crucial role in cybersecurity by empowering individuals to recognize threats and adhere to best practices for safeguarding their information. This knowledge enables users to identify various types of cyber threats, such as phishing attempts, malware, and social engineering scams. Educated users are more likely to employ strong passwords, use multi-factor authentication, and be cautious about what information they share online, thereby enhancing the overall security posture of both individuals and organizations. By understanding the potential risks and adopting sound security practices, individuals can significantly decrease the likelihood of falling victim to cyber-attacks. This proactive approach to personal and organizational cybersecurity is essential, as human error is often a significant contributing factor in many security incidents. Therefore, user education serves as a foundational strategy in building a culture of security awareness and responsibility, ultimately protecting sensitive data from unauthorized access and breaches.

8. What is the function of Cloud9?

A. To provide virtual reality experiences

B. To access data without harming local devices

C. To manage cloud resources

D. To develop standalone applications

Cloud9 is an integrated development environment (IDE) that operates in the cloud, allowing developers to write, run, and debug their code directly in the browser. The primary function of Cloud9 is to provide a workspace where users can access data and run applications without the need to install software or manage local device resources. This means that users can work on complex programming tasks without risking harm to their local machines, as all processing is done on Cloud9's servers. This cloud-based approach enhances collaboration, as multiple users can work on the same codebase simultaneously, and it allows easy access to development tools from any device with internet connectivity. Thus, the ability to access data without harming local devices is a pivotal aspect of Cloud9's functionality, making it easy for developers to focus on their projects without the limitations imposed by their local setups.

9. Which command is used to create a new directory?

A. mkdir

B. rmdir

C. cd

D. cp

The command used to create a new directory is "mkdir," which stands for "make directory." This command is widely used in various command-line interfaces, including Unix/Linux and Windows systems. When executed, it allows users to set up a new folder within the current working directory or a specified path. Utilizing "mkdir" is essential for organizing files and directories, as it promotes better file management and accessibility. For instance, if you want to create a project folder, you would type “mkdir ProjectName” in the command line, and a new directory with that name will be established. The other commands serve different purposes. "rmdir" is used to remove directories, "cd" is employed to change the current directory, and "cp" is used to copy files or directories. Understanding the distinct functions of these commands highlights why "mkdir" is specifically suited for creating a new directory.

10. Describe what a botnet is.

A. A software that enhances network performance

B. A tool for securing computer systems

C. A network of infected computers controlled by an attacker to perform malicious activities

D. A collection of authorized user devices

A botnet is best defined as a network of infected computers that are controlled by an attacker to perform malicious activities. This means that an attacker infects multiple computers with malware, enabling them to be remotely managed and utilized for various harmful tasks. Such tasks may include launching distributed denial-of-service (DDoS) attacks, sending spam emails, or stealing sensitive information from unsuspecting users. The magnitude and the anonymity that a botnet provides makes it a popular tool for cybercriminals, as they can orchestrate large attacks without the need for direct access to a large number of computers. Each compromised device, often referred to as a "bot" or "zombie," acts under the control of the cybercriminal, allowing for coordinated and powerful attacks. Understanding the nature and function of botnets is essential in cybersecurity, as they pose a significant threat to both individuals and organizations, demonstrating the importance of network security measures and the need for vigilance against malware infections.