Information Technology Specialist (ITS) Cybersecurity Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **What is a virtualized application that consists of its dependencies called?**
   - **A. Virtual machine**
   - **B. Container**
   - **C. Hypervisor**
   - **D. Router**

2. **What is the primary focus of penetration testing?**
   - **A. Network performance assessment**
   - **B. Identifying vulnerabilities**
   - **C. Data recovery**
   - **D. Malware detection**

3. **Which term describes software that controls network access permissions related to user actions?**
   - **A. Firewall**
   - **B. VPN**
   - **C. Access Control List (ACL)**
   - **D. Antivirus software**

4. **What is the goal of a cybersecurity awareness training program?**
   - **A. To fulfill compliance requirements**
   - **B. To educate employees about cybersecurity risks and promote safe behaviors online**
   - **C. To develop new security software**
   - **D. To analyze employee performance**

5. **What solution can help a company track and comply with security policies for mobile devices?**
   - **A. VPN software**
   - **B. Network monitoring tools**
   - **C. MDM software**
   - **D. Firewalls**

6. Which statement is true regarding advanced persistent threat (APT) attacks?

- **A. They are primarily used for network maintenance**
- **B. They are used to steal data**
- **C. They are a type of antivirus software**
- **D. They are ineffective against modern security measures**

7. Which built-in MacOS tool is designed for file encryption?

- **A. FileVault**
- **B. BitLocker**
- **C. Disk Utility**
- **D. Secure Enclave**

8. What does the term "cloud security" refer to?

- **A. The policies, controls, and technologies that protect data and applications in cloud computing environments**
- **B. The practices used to secure local servers and databases**
- **C. A subset of network security focused on securing cloud services only**
- **D. The encryption methods employed by cloud providers**

9. What type of attack uses publicly accessible open DNS servers to flood a target with DNS response traffic?

- **A. DNS Amplification**
- **B. DNS Spoofing**
- **C. DNS Hijacking**
- **D. DNS Reflection**

10. Which security framework focuses on continuous compliance and monitoring?

- **A. NIST Cybersecurity Framework**
- **B. CIS Controls**
- **C. ISO 27001**
- **D. COBIT**

Answers

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

Explanations

1. What is a virtualized application that consists of its dependencies called?

A. Virtual machine

B. Container

C. Hypervisor

D. Router

A virtualized application that consists of its dependencies is referred to as a container. Containers are designed to package an application along with all its necessary components, such as libraries and configuration files, directly with the application code. This allows the application to run reliably in different computing environments, as the container encapsulates everything needed for execution. The use of containers promotes consistency across development, testing, and production environments, thereby simplifying the deployment process and enhancing scalability. Containers are lightweight compared to virtual machines, as they share the same operating system kernel while still isolating the application processes. This separation enables efficient resource utilization and faster start-up times. This concept stands in contrast to a virtual machine, which simulates complete hardware and includes a full operating system, leading to heavier resource consumption. A hypervisor, on the other hand, is software that creates and manages virtual machines, rather than the applications themselves. Routers function in networking by directing traffic and are unrelated to application virtualization. Therefore, containers effectively fulfill the requirement of encapsulating applications with their respective dependencies.

2. What is the primary focus of penetration testing?

A. Network performance assessment

B. Identifying vulnerabilities

C. Data recovery

D. Malware detection

The primary focus of penetration testing is to identify vulnerabilities in a system, network, or application. This process simulates real-world attacks on an organization's IT infrastructure to discover exploitable weaknesses. By actively probing for vulnerabilities, penetration testers can provide valuable insights into security flaws that could be taken advantage of by malicious actors. This practice helps organizations strengthen their security posture by understanding where they are most vulnerable and implementing appropriate security measures to mitigate risks. While other options like network performance assessment, data recovery, and malware detection are important aspects of cybersecurity, they do not align with the core objective of penetration testing, which is specifically centered around vulnerability identification.

3. Which term describes software that controls network access permissions related to user actions?

A. Firewall

B. VPN

C. Access Control List (ACL)

D. Antivirus software

The term that accurately describes software responsible for controlling network access permissions related to user actions is Access Control List (ACL). ACLs are fundamental components of network security that define who can access specific resources and what actions they can perform, such as reading or modifying the data. They operate by checking permissions associated with user accounts or groups before granting access to network resources. In contrast, firewalls primarily focus on monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between a trusted internal network and untrusted external networks but do not specifically dictate user action permissions. VPNs (Virtual Private Networks) provide a secure connection over the internet by encrypting the data transmitted between a user's device and the server, ensuring privacy and confidentiality, but they do not manage users' permissions regarding network resources. Antivirus software is designed to detect, prevent, and remove malicious software from computers and networks, rather than controlling access permissions for users. Thus, ACLs distinctly serve the purpose of managing access permissions within network environments, making them the correct choice.

4. What is the goal of a cybersecurity awareness training program?

A. To fulfill compliance requirements

B. To educate employees about cybersecurity risks and promote safe behaviors online

C. To develop new security software

D. To analyze employee performance

The goal of a cybersecurity awareness training program is primarily to educate employees about cybersecurity risks and promote safe behaviors online. This training helps employees recognize potential threats, such as phishing scams or malware attacks, and understand the importance of following security protocols. By fostering a culture of cybersecurity awareness, organizations can significantly reduce the likelihood of breaches caused by human error. Effective training empowers employees with the knowledge to make informed decisions when handling sensitive information, using corporate resources, and adhering to best practices for cybersecurity. This proactive approach not only protects the organization but also helps employees feel more confident in their ability to contribute to overall security. Other options may touch on aspects related to cybersecurity but do not encapsulate the primary goal of these training programs. Compliance requirements, while important, are often a byproduct rather than the main focus of training. Developing new security software and analyzing employee performance are also valuable activities but do not directly reflect the intent of raising cybersecurity awareness among employees.

5. What solution can help a company track and comply with security policies for mobile devices?

A. VPN software

B. Network monitoring tools

C. MDM software

D. Firewalls

Mobile Device Management (MDM) software is specifically designed to help organizations manage, monitor, and secure mobile devices such as smartphones and tablets within their network. With MDM, companies can enforce security policies, configure devices, and ensure compliance with various regulations and standards. MDM solutions enable IT administrators to remotely manage device settings, enforce password policies, and implement encryption. This capability is crucial in maintaining the security of sensitive company data accessed or stored on mobile devices. Additionally, MDM tools can provide features such as application management, which allows the organization to control which apps can be installed and used on devices, thereby reducing the risk of malware or data breaches. In contrast, while VPN software secures data in transit and network monitoring tools help to monitor traffic and detect anomalies, they do not specifically manage or enforce compliance policies on mobile devices. Firewalls protect network boundaries but are not tailored to oversee mobile device security policies directly. Therefore, MDM stands out as the most effective solution for tracking and complying with security policies specifically for mobile devices.

6. Which statement is true regarding advanced persistent threat (APT) attacks?

A. They are primarily used for network maintenance

B. They are used to steal data

C. They are a type of antivirus software

D. They are ineffective against modern security measures

Advanced Persistent Threat (APT) attacks primarily aim to steal data, making the statement about their use for this purpose accurate. APT attacks are characterized by their long-term, targeted approach, where attackers gain unauthorized access to a network and remain undetected for an extended period. During this time, their goal is to collect sensitive information such as intellectual property, trade secrets, or personal data, which can be exploited for various malicious intents. Unlike traditional attacks, which tend to be opportunistic and can be executed quickly, APT attacks are sophisticated and methodical. Attackers often use multiple vectors to infiltrate networks and deploy advanced techniques to establish and maintain their presence. This persistent approach enables them to systematically extract valuable data over time while evading detection. The focus on data theft differentiates APT attacks from other options. The mention of network maintenance misrepresents their purpose, and characterizing them as antivirus software is inaccurate; APT attacks are inherently malicious rather than protective. Lastly, suggesting that APT attacks are ineffective against modern security measures ignores the reality of their design. Cybersecurity defenses may delay or thwart some attempts, but APTs are specifically engineered to circumvent security protocols and exploit weaknesses in systems.

7. Which built-in MacOS tool is designed for file encryption?

A. FileVault

B. BitLocker

C. Disk Utility

D. Secure Enclave

FileVault is the built-in macOS tool specifically designed for full disk encryption. It functions by encrypting the entire startup disk of a Mac, protecting the operating system and all user data stored on the disk. When FileVault is enabled, it uses XTS-AES-128 encryption with a 256-bit key to secure the contents of the disk. This ensures that even if someone gains physical access to the Mac, they cannot access the data without the correct user credentials. FileVault also integrates seamlessly with the macOS operating system, allowing users to log in using their existing credentials and providing recovery options through their Apple ID or a recovery key. This level of integration and security makes FileVault a primary choice for individuals and organizations looking to safeguard their sensitive data. Other options, while they may relate to security and encryption in some aspect, do not specifically offer full disk encryption tailored for macOS like FileVault does. Disk Utility can encrypt specific files or disk images but is not primarily focused on full disk encryption. BitLocker is a Windows-based encryption tool and does not apply to macOS systems. The Secure Enclave is a hardware-based security feature that enhances the protection of sensitive information but is not a tool for file encryption in the same way that

8. What does the term "cloud security" refer to?

A. The policies, controls, and technologies that protect data and applications in cloud computing environments

B. The practices used to secure local servers and databases

C. A subset of network security focused on securing cloud services only

D. The encryption methods employed by cloud providers

The term "cloud security" refers specifically to the policies, controls, and technologies that are designed to protect data and applications in cloud computing environments. This includes a comprehensive framework that encompasses various aspects such as data privacy, data integrity, identity and access management, threat detection, and incident response tailored for cloud infrastructures. Understanding cloud security is essential because it addresses the unique risks associated with storing and processing data in a cloud environment. Unlike traditional on-premise security measures, cloud security must deal with shared responsibility models between cloud service providers and customers, ensuring compliance with regulatory requirements, and adapting to the dynamic nature of cloud services. In contrast, the other choices focus on narrower aspects of security. While securing local servers and databases is important, it does not encompass the broader scope of cloud security, which involves specific challenges and protective measures for cloud environments. A subset of network security focused solely on cloud services would overlook the integrative nature of cloud security practices that also apply to on-premises components. Lastly, encryption methods are a specific tool within the broader domain of cloud security; while they are vital for protecting data, they do not capture the full range of policies and controls needed for a robust cloud security strategy.

9. What type of attack uses publicly accessible open DNS servers to flood a target with DNS response traffic?

A. DNS Amplification

B. DNS Spoofing

C. DNS Hijacking

D. DNS Reflection

The correct answer is DNS Amplification, which is a type of distributed denial-of-service (DDoS) attack that exploits the functionality of DNS servers. In this attack, the perpetrator sends a small query to an open DNS server, with the source address spoofed to appear as the target's IP address. The DNS server then responds to the query with a much larger response, flooding the target with a significant volume of DNS traffic. This amplification occurs because the response size is much greater than the original request, which enables attackers to use minimal resources to generate a substantial amount of outgoing traffic directed at the target. The use of publicly accessible open DNS servers is critical in these attacks since they allow attackers to bypass restrictions on who can make queries, enabling a much larger scale of attack. While DNS Reflection also involves amplifying traffic by using open DNS servers, it specifically entails reflecting the traffic back to a target, which is a key differentiator. Since the question directly highlights the flooding aspect generated through stored responses rather than the reflection mechanism, DNS Amplification is the more precise answer.

10. Which security framework focuses on continuous compliance and monitoring?

A. NIST Cybersecurity Framework

B. CIS Controls

C. ISO 27001

D. COBIT

The NIST Cybersecurity Framework is designed to help organizations manage and reduce cybersecurity risk by providing a set of standards, guidelines, and best practices. One of its core components is its focus on continuous compliance and monitoring, which emphasizes ongoing evaluation of cybersecurity policies and practices to adapt to changing threats and vulnerabilities. This framework encourages organizations to continuously assess their security posture by monitoring cybersecurity risks, ensuring that they are compliant with established standards and practices. The iterative nature means that organizations regularly revisit their security strategies and controls, enabling them to maintain an effective and resilient cybersecurity program. While the other frameworks like CIS Controls, ISO 27001, and COBIT provide various levels of guidance on security practices, they do not emphasize continuous compliance and monitoring as strongly as the NIST Cybersecurity Framework does. For example, while ISO 27001 is focused on establishing an Information Security Management System (ISMS) requiring periodic review and assessment, it does not intrinsically prioritize real-time monitoring or continuous compliance in the same structured way as NIST. Thus, the NIST Cybersecurity Framework stands out for its emphasis on an ongoing, adaptable approach to cybersecurity compliance and monitoring.