CREST Practitioner Security Analyst (CPSA) Practice (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Which statement accurately describes the characteristics of Token Ring?**
   - **A. It is a wireless network technology**
   - **B. It shares bandwidth with all stations in a ring topology**
   - **C. It uses a centralized control for data transmission**
   - **D. It utilizes switch technology to control traffic**

2. **Which of the following protocols is not connection-oriented?**
   - **A. TCP**
   - **B. UDP**
   - **C. FTP**
   - **D. SMTP**

3. **Which of the following is a method used to exploit a buffer overflow vulnerability?**
   - **A. Code injection**
   - **B. SQL queries**
   - **C. Shell scripting**
   - **D. Data validation**

4. **Which version does not share a classification with Windows XP?**
   - **A. NT 5.1**
   - **B. NT 5.0**
   - **C. NT 5.2**
   - **D. NT 6.1**

5. **What is a potential consequence of a buffer overflow in C programming?**
   - **A. Memory leak**
   - **B. Code Injection**
   - **C. Invalid pointer exceptions**
   - **D. Access control violations**

6. Which act is known as the Family Educational Rights and Privacy Act?

A. FERPA

B. FISMA

C. GLBA

D. HIPAA

7. What is the filename of the physical storage file for Active Directory?

A. Ntds.dat

B. Ntds.dit

C. Ntds.txt

D. Ntds.bin

8. Which of the following command options will allow a user from a specific host to log in without root permissions?

A. host +

B. host user

C. -host

D. host +@netgroup

9. What is the purpose of port 103?

A. X.400 Standard

B. File Transfer Services

C. Web Browsing

D. Email Services

10. Which protocol operates on port 119?

A. NNTP (Network News Transfer Protocol)

B. SMTP

C. POP3

D. DNS

Answers

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

Explanations

1. Which statement accurately describes the characteristics of Token Ring?

A. It is a wireless network technology

B. It shares bandwidth with all stations in a ring topology

C. It uses a centralized control for data transmission

D. It utilizes switch technology to control traffic

The correct characterization of Token Ring is that it shares bandwidth with all stations in a ring topology. In a Token Ring network, devices are interconnected in a circular manner, and data is transmitted in a token-passing method. Each device waits for an opportunity to send data when it obtains a token, which ensures that only one device transmits at a time, thus preventing collisions. This token-passing mechanism allows all stations in the network to have equal access to the shared bandwidth, promoting orderly transmission and improving efficiency. In contrast, the other options do not accurately reflect the characteristics of Token Ring. For instance, Token Ring is a wired network technology utilizing physical cabling, not wireless, which excludes the first option. The second option, which implies a centralized control for data transmission, does not apply here, as Token Ring relies on decentralized control via the token-passing protocol rather than a central controller. The mention of switch technology in the last option refers to Ethernet networks, where switches manage traffic more efficiently, a characteristic not inherent to Token Ring, which operates based on the ring topology structure.

2. Which of the following protocols is not connection-oriented?

A. TCP

B. UDP

C. FTP

D. SMTP

The correct answer is UDP, which stands for User Datagram Protocol. UDP is classified as a connectionless protocol, meaning it does not establish a dedicated end-to-end connection before data transmission. It allows data to be sent without the overhead of connection setup and teardown, facilitating faster communications. In UDP, data packets, or datagrams, are sent without ensuring that the recipient is ready to receive them, making it suitable for applications that require speed and efficiency over reliability, such as streaming audio or video. In contrast, other protocols listed, such as TCP (Transmission Control Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol), are connection-oriented. These protocols require a connection to be established before any data is sent, ensuring a reliable transmission with mechanisms for error checking and data sequencing. This connection-oriented approach guarantees that the data is delivered accurately and in the correct order, which is essential for many applications like file transfers and email communication.

3. Which of the following is a method used to exploit a buffer overflow vulnerability?

A. Code injection

B. SQL queries

C. Shell scripting

D. Data validation

A method used to exploit a buffer overflow vulnerability is code injection. Buffer overflow vulnerabilities occur when a program attempts to write more data to a fixed-length buffer than it can hold, causing adjacent memory space to be overwritten. This can lead to unpredictable behavior, including the execution of arbitrary code. Through code injection, an attacker can manipulate the program's execution flow by inserting malicious code directly into the buffer. When the program resumes execution, it may inadvertently run the attacker's code, leading to unauthorized actions taken on the system, such as privilege escalation or remote command execution. This technique takes advantage of programming weaknesses and poor memory management practices, making it a critical vector for cybersecurity threats. The other options, such as SQL queries, shell scripting, and data validation, do not directly pertain to exploiting buffer overflow vulnerabilities in the same manner as code injection does. SQL queries are primarily related to database interactions, shell scripting involves scripting for automation, and data validation is a defensive programming practice meant to prevent such vulnerabilities from being exploited in the first place.

4. Which version does not share a classification with Windows XP?

A. NT 5.1

B. NT 5.0

C. NT 5.2

D. NT 6.1

The correct answer identifies the version that does not share a classification with Windows XP. Windows XP is classified as NT 5.1, meaning it belongs to the NT 5 family. The designation NT 5.0 corresponds to Windows 2000, which is a predecessor of Windows XP, but not the same classification. Windows NT 5.2 corresponds to Windows Server 2003, which is also within the NT 5 family but generally characterized as a server operating system. NT 6.1 corresponds to Windows 7, representing a major shift in the Windows operating system's architecture and features, moving beyond the classifications and functionalities of the NT 5.x series. Thus, NT 5.0 is distinctly different from Windows XP, as it indicates a separate version entirely, while the others either classify under the same version or continue the NT lineage that includes Windows XP.

5. What is a potential consequence of a buffer overflow in C programming?

A. Memory leak

B. Code Injection

C. Invalid pointer exceptions

D. Access control violations

A buffer overflow occurs when a program writes more data to a buffer than it can hold, which can lead to unintended behavior. The most significant consequence of this vulnerability is code injection. When a buffer overflow takes place, an attacker can overwrite the stack, heap, or return addresses to inject malicious code into a program's memory space. This injected code can then be executed, compromising the security of the application and potentially leading to unauthorized access or other malicious actions. This type of vulnerability is particularly dangerous in C programming due to the language's low-level memory management and lack of built-in bounds checking. The ability to craft the overflow to point to specific locations in memory allows attackers to execute arbitrary code, gaining control over the execution flow of the application and leading to various security breaches.

6. Which act is known as the Family Educational Rights and Privacy Act?

A. FERPA

B. FISMA

C. GLBA

D. HIPAA

The Family Educational Rights and Privacy Act is commonly referred to as FERPA. This federal law was enacted to protect the privacy of student education records and provides specific rights to students and their parents regarding access to these records. Under FERPA, educational institutions must obtain written consent from students or parents before disclosing personally identifiable information from education records, ensuring the confidentiality of sensitive data related to a student's educational experience. In contrast, the other options refer to different acts with separate focuses: FISMA, or the Federal Information Security Management Act, pertains to the management and protection of federal information systems; GLBA, or the Gramm-Leach-Bliley Act, deals with financial privacy in the banking and financial sector; and HIPAA, the Health Insurance Portability and Accountability Act, is centered around the protection of health information. Thus, only FERPA is involved with the rights and privacy of educational records, making it the correct choice.

7. What is the filename of the physical storage file for Active Directory?

A. Ntds.dat

B. Ntds.dit

C. Ntds.txt

D. Ntds.bin

The filename of the physical storage file for Active Directory is Ntds.dit. This file is crucial because it contains the directory data, including user accounts, group policies, and other vital information stored in Active Directory. The ".dit" extension denotes that it is a database file, specifically designed for storing structured data efficiently. Ntds.dit is specifically optimized for the operations and functions of directory services, providing fast access and ensuring data integrity. It is used by Windows Server operating systems to manage directory services and ensure that network resources are readily available and manageable. Understanding the specific role of Ntds.dit helps to grasp how Active Directory maintains its information and serves users and systems within a network environment. The other filenames listed do not correspond to the actual physical storage requirements of Active Directory.

8. Which of the following command options will allow a user from a specific host to log in without root permissions?

A. host +

B. host user

C. -host

D. host +@netgroup

The command option that allows a user from a specific host to log in without root permissions is the option that specifies access permissions for a defined user originating from that host. This option establishes a direct connection between the host and the user, facilitating user access control based on their identity and location. In many environments, configuration files and security settings, such as within SSH or system access policies, can be mapped to user-to-host conditions that determine login capabilities. By using a specific user's designation — as indicated in the option — system administrators can more effectively manage access without necessarily granting root privileges. The other options provided do not accurately define this specific and limited access. For example, simply stating "host +" does not specify a user, making it too broad a permissions statement. "-host" indicates the removal of host-related permissions and is not suitable for granting access. Lastly, "host +@netgroup" implies access based on a netgroup rather than a specific user, which changes the context of permission management significantly. In summary, focusing on user-specific permissions originating from defined hosts is key to ensuring that individuals can access systems without granting them full administrative rights.

9. What is the purpose of port 103?

A. X.400 Standard

B. File Transfer Services

C. Web Browsing

D. Email Services

Port 103 is primarily associated with the X.400 standard, which is a protocol suite used for electronic messaging. This standard facilitates the exchange of mail over the internet and is part of the larger framework of telecommunications messaging services often utilized by organizations requiring robust and standardized email communication. The use of port 103 enables systems to establish a connection for carrying out operations related to the X.400 messaging protocol, thereby ensuring effective message delivery and mail management. The other options pertain to different protocols or services not related to port 103. For example, file transfer services typically utilize ports like 20 and 21 for FTP, while web browsing primarily occurs over port 80 (HTTP) or port 443 (HTTPS). Email services usually operate on ports like 25 (SMTP) or 110 (POP3), distinctly differing from the purposes served by port 103. Understanding these associations clarifies the specific function of port 103 in the realm of electronic communications.

10. Which protocol operates on port 119?

A. NNTP (Network News Transfer Protocol)

B. SMTP

C. POP3

D. DNS

NNTP, or Network News Transfer Protocol, is the correct choice for the protocol that operates on port 119. This protocol is primarily used for the distribution, retrieval, and posting of Usenet articles and is essential in managing networked news groups. By using port 119, NNTP facilitates the transport of news messages and allows users to access and interact with news articles seamlessly. Understanding the context of other protocols can help clarify this point. SMTP, or Simple Mail Transfer Protocol, operates on port 25 and is used for sending emails. POP3, or Post Office Protocol version 3, operates on port 110 and is primarily used for retrieving emails from a server. DNS, or Domain Name System, typically operates on port 53 and is used for resolving domain names into IP addresses. Each of these protocols serves distinct purposes in the realm of network communications, whereas NNTP specifically handles the transmission of Usenet content over the internet.