Navy Officer Candidate School (OCS) Cyber Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://navyocscyber.examzify.com

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. Define a protocol in networking.

A. A physical connection between devices

B. An agreement about communication between two parties

C. A type of network application

D. The hardware used to transmit data

2. What process combines data and code into a single object?

A. Segmentation

B. Encapsulation

C. Layering

D. Packetizing

3. In network security, which is generally considered more challenging, defense or offense?

A. Offense

B. Neither

C. Defense

D. Both equally

4. What is the key characteristic of spear phishing?

A. Widespread attacks without specific targets

B. Carefully designed emails targeting a particular individual or organization

C. Generic messages sent to random email addresses

D. Using social media to extract information

5. Which component of an OS allows interaction through graphical icons and visual indicators?

A. Shell

B. API

C. GUI

D. Kernel

6. What is the purpose of a kill chain model?

A. To decrease production time

B. To describe stages of network intrusion

C. To manage human resources effectively

D. To analyze financial performance

7. What is the primary function of Http?

A. Encrypting data

B. Defining webpage styles

C. Serving as the language of the web

D. Managing server requests

8. How does malware typically affect files on a computer system?

A. It repairs corrupted files

B. It collects data from files

C. It locks or deletes files and modifies them

D. It organizes files for better access

9. What does the operating system do to manage running programs?

A. It allocates hard drive space for each program

B. It schedules CPU time for program execution

C. It compiles programs into machine code

D. It connects programs to the internet

10. Which of the following statements is true about TCP?

A. It sends packets in random order

B. It does not guarantee data delivery

C. It is connection-oriented and verifies packet delivery

D. It operates independently of internet protocols

Answers

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

Explanations

1. Define a protocol in networking.

A. A physical connection between devices

B. An agreement about communication between two parties

C. A type of network application

D. The hardware used to transmit data

A protocol in networking is fundamentally an agreement about communication between two parties. It establishes the rules and conventions that govern how data is transmitted and received over a network. This includes aspects such as syntax (the structure or format of the messages), semantics (the meaning of the messages), and timing (when messages can be sent and how fast they can be transmitted). Protocols ensure that devices, applications, or systems can communicate with each other effectively, even if they are made by different manufacturers or operating in different environments. For instance, the TCP/IP protocol suite defines how data should be packetized, addressed, transmitted, routed, and received, which is crucial for various types of communications over the internet. In contrast, other options refer to different aspects of networking; a physical connection between devices refers to the hardware layer rather than the communication rules, a type of network application doesn’t encompass the fundamental purpose of protocols, and hardware used to transmit data does not define the interaction rules between devices. Understanding protocols is key to grasping how networking functions as they underpin the entire framework for data exchange.

2. What process combines data and code into a single object?

A. Segmentation

B. Encapsulation

C. Layering

D. Packetizing

The process that combines data and code into a single object is known as encapsulation. This concept is fundamental in object-oriented programming and software design, where encapsulation allows objects to bundle their data (attributes) with the methods (functions) that operate on that data. This tight coupling of data and functionality promotes better organization, easier maintenance, and enhanced reusability of code, as it controls access and defines how the data can be manipulated. In encapsulation, the internal state of an object is hidden from the outside world, only allowing access through well-defined interfaces or methods. This helps in protecting the integrity of the data and enforcing rules about how it can be accessed or modified. This differs significantly from segmentation, layering, and packetizing. Segmentation typically refers to dividing data into smaller pieces for easier management or transmission, layering involves organizing systems in structured levels for modularity (commonly found in network protocols), and packetizing refers to the process of encapsulating data into discrete packets for network transmission. Each of these processes serves a different purpose and scenario in computing and networking, but none involve the direct integration of data and code like encapsulation does.

3. In network security, which is generally considered more challenging, defense or offense?

A. Offense

B. Neither

C. Defense

D. Both equally

In network security, defense is generally considered more challenging than offense due to the nature of the threats and the responsibilities involved. Defensive strategies require a deep understanding of various attack vectors, constant monitoring for vulnerabilities, and the implementation of comprehensive security measures to protect against a wide range of potential attacks. Defenders must account for an ever-evolving landscape of threats, including sophisticated malware, social engineering tactics, and zero-day vulnerabilities. This necessitates regular updates to security protocols and the continuous education of security personnel to adapt to new challenges. Effective defense involves creating layers of security, such as firewalls, intrusion detection systems, and access controls, all of which must work in harmony to prevent breaches. On the other hand, offense, while requiring skill and creativity, often has a more focused objective: exploiting existing vulnerabilities. Offensive activities can leverage known techniques and tools that have been proven effective in the past, which can sometimes simplify the task of launching an attack. In summary, defense is inherently more complex and resource-intensive, as it must anticipate and mitigate against various potential threats, whereas offensive strategies can often rely on established methods and may have a narrower focus. This depth and breadth of responsibility in defending against a myriad of attack methods is what makes it the more challenging aspect of

4. What is the key characteristic of spear phishing?

A. Widespread attacks without specific targets

B. Carefully designed emails targeting a particular individual or organization

C. Generic messages sent to random email addresses

D. Using social media to extract information

Spear phishing is characterized by carefully designed emails that target a specific individual or organization. This method involves conducting thorough research on the target to craft a message that appears credible and personalized. By doing this, the attacker increases the likelihood that the recipient will engage with the content, whether by clicking on a malicious link or providing sensitive information. This level of targeting distinguishes spear phishing from more generalized phishing attacks, which simply cast a wide net without focusing on particular individuals or organizations. This targeted approach often leverages details gleaned from social media or company websites to make the communication appear legitimate, which enhances the attack's chances of success. Understanding this nuance is vital in cybersecurity, as it helps individuals and organizations develop more effective defenses against these types of nuanced threats.

5. Which component of an OS allows interaction through graphical icons and visual indicators?

A. Shell

B. API

C. GUI

D. Kernel

The component of an operating system that allows interaction through graphical icons and visual indicators is the Graphical User Interface (GUI). The GUI serves as a bridge between the user and the system, allowing users to interact with the computer using visual elements like buttons, icons, windows, and menus, which makes it more intuitive and user-friendly compared to command-line interfaces. A GUI simplifies complex operations by allowing users to perform actions through clicks and drags rather than typing commands. This not only enhances usability for people with varying levels of technical skills but also improves efficiency when performing tasks, as users can visually navigate the operating system. In contrast to other components, the shell primarily provides a command-line interface, the API facilitates communication between software applications, and the kernel manages the system resources. While all these components play essential roles in the operation of an operating system, the GUI is specifically designed for visual interaction.

6. What is the purpose of a kill chain model?

A. To decrease production time

B. To describe stages of network intrusion

C. To manage human resources effectively

D. To analyze financial performance

The purpose of a kill chain model is to describe stages of network intrusion. This model is instrumental in cybersecurity as it outlines the series of steps that an adversary typically follows to execute an attack successfully. Understanding this framework allows security professionals to identify, detect, and mitigate threats at various stages of the intrusion process. The kill chain model breaks down a cyberattack into discrete phases, such as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. By analyzing these stages, organizations can implement defensive measures tailored to interrupt the chain at critical points, ultimately thwarting the attack before it achieves its objectives. This proactive approach is crucial for developing effective cybersecurity strategies and enhancing overall network security.   The other options do not relate to the primary focus of the kill chain model, which is centered specifically on cybersecurity and network threats.

7. What is the primary function of Http?

A. Encrypting data

B. Defining webpage styles

C. Serving as the language of the web

D. Managing server requests

The primary function of HTTP, or Hypertext Transfer Protocol, is to serve as the foundational protocol for transferring data on the web. It allows for the communication between web browsers (clients) and web servers, enabling users to access and interact with websites. When you enter a URL or click on a link, your browser uses HTTP to send a request to the server where that resource is hosted. The server then responds, transmitting the requested web page’s data back to the browser, which renders it for the user. Understanding this function is crucial because HTTP is integral to the web's operation; it dictates how messages are formatted and transmitted, and how web servers and browsers respond to various commands. This protocol does not inherently involve encrypting data, defining webpage styles, or managing server requests in the manner described in the incorrect options, though it may work alongside other protocols and technologies that do handle those aspects.

8. How does malware typically affect files on a computer system?

A. It repairs corrupted files

B. It collects data from files

C. It locks or deletes files and modifies them

D. It organizes files for better access

Malware typically affects files on a computer system by locking or deleting them and also modifying them, which is accurately reflected in the chosen answer. This behavior is a common characteristic of various types of malware, including ransomware, which encrypts files and demands payment for their release, and file-corrupting viruses that damage files, making them unusable. Locking files means that the user is unable to access or modify them without first disabling the malware or paying a ransom. Deletion refers to the outright removal of files, potentially leading to the permanent loss of critical data. Modification can involve changing the content within files or altering file attributes, which can disrupt normal operations and lead to data integrity issues. This manipulation of files can have severe consequences for users and organizations, impacting productivity and data security. The other options do not align with the typical functions of malware. Repairing corrupted files is not a capability of malware; rather, this activity is associated with legitimate software tools. Collecting data from files might occur through specific types of malware, such as spyware, but it doesn't encompass the overall damaging effects malware has on file systems. Organizing files is typically a function of file management systems and is not a characteristic of malware, which is primarily geared toward harmful activities.

9. What does the operating system do to manage running programs?

A. It allocates hard drive space for each program

B. It schedules CPU time for program execution

C. It compiles programs into machine code

D. It connects programs to the internet

The operating system plays a crucial role in managing running programs, and one of its primary functions is to schedule CPU time for program execution. This involves determining which program gets to use the CPU and for how long, effectively coordinating the processing and execution of multiple programs simultaneously. By scheduling CPU time, the operating system ensures that each program runs efficiently without unnecessary delays, thereby optimizing the overall performance of the system. This management allows for multitasking, enabling users to switch between different applications seamlessly. Other functions, such as allocating hard drive space, compiling programs into machine code, or connecting programs to the internet, while important, do not directly relate to the core task of managing the execution of programs in a multitasking environment. Each of these functions serves a specific purpose within the broader ecosystem of a computer's operations, but they do not encompass the essential role of organizing and prioritizing execution time for active tasks.

10. Which of the following statements is true about TCP?

A. It sends packets in random order

B. It does not guarantee data delivery

C. It is connection-oriented and verifies packet delivery

D. It operates independently of internet protocols

The statement that TCP is connection-oriented and verifies packet delivery is indeed accurate. TCP, or Transmission Control Protocol, is designed to ensure reliable communication between devices on a network. Being connection-oriented means that TCP establishes a connection between the sender and receiver before any data is transmitted. This process involves a three-way handshake, which helps ensure that both parties are ready for data transfer. Once the connection is established, TCP tracks packets of data using sequence numbers and acknowledgments. If a packet is lost or not acknowledged by the receiving end, TCP will retransmit those packets, ensuring data delivery and order. This reliability aspect of TCP makes it suitable for applications that require accurate data transfer, such as web browsing or file transfers. Other options present characteristics that do not apply to TCP. For example, TCP does not send packets in random order; rather, it ensures that packets arrive in the order they were sent. Additionally, it does guarantee data delivery, making option B inaccurate. Lastly, TCP functions within the framework of internet protocols, meaning it does not operate independently, which makes option D incorrect.