ECCouncil.ICS-SCADA Cyber Security.by.Lazyon.37q

Number: ICS-SCADA Cyber Security
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: ICS/SCADA Cyber Security

Exam Name: ICS/SCADA Cyber Security

Exam A

QUESTION 1
Which of the following can be used to view entire copies of web sites?

A. Wayback machine
B. Google Cache
C. Netcraft
D. Bing offline

Correct Answer: A
Section:
Explanation:
The Wayback Machine is an internet service provided by the Internet Archive that allows users to see archived versions of web pages across time, enabling them to browse past versions of a website as it appeared on specific dates.
It captures and stores snapshots of web pages, making it an invaluable tool for accessing the historical state of a website or recovering content that has since been changed or deleted.
Other options like Google Cache may also show snapshots of web pages, but the Wayback Machine is dedicated to this purpose and holds a vast archive of historical web data.
Reference
Internet Archive: https://archive.org
'Using the Wayback Machine,' Internet Archive Help Center.

QUESTION 2
Which publication from NIST provides guidance on Industrial Control Systems?

A. NIST SP 800-90
B. NIST SP 800-82
C. NIST SP 800-77
D. NIST SP 800-44

Correct Answer: B
Section:
Explanation:
NIST Special Publication 800-82, 'Guide to Industrial Control Systems (ICS) Security,' provides guidance on securing industrial control systems, including SCADA systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). It offers practices and recommendations for protecting and securing ICS systems against disruptions, malicious activities, and other threats to their integrity and availability.
Reference:
National Institute of Standards and Technology (NIST), 'Guide to Industrial Control Systems (ICS) Security'.

QUESTION 3
Which mode within IPsec provides a secure connection tunnel between two endpoints AND protects the sender and the receiver?

A. Protected
B. Tunnel
C. Transport
D. Covered

Correct Answer: B
Section:
Explanation:
IPsec (Internet Protocol Security) has two modes: Transport mode and Tunnel mode.
Tunnel mode is used to create a secure connection tunnel between two endpoints (e.g., two gateways, or a client and a gateway) and it encapsulates the entire IP packet.
This mode not only protects the payload but also the header information of the original IP packet, thereby providing a higher level of security compared to Transport mode, which only protects the payload.
Reference
Kent, S. and Seo, K., 'Security Architecture for the Internet Protocol,' RFC 4301, December 2005.
'IPsec Services,' Microsoft TechNet.

QUESTION 4
Which component of the IT Security Model is attacked with masquerade?

A. Integrity
B. Availability
C. Confidentiality
D. Authentication

Correct Answer: D
Section:
Explanation:
A masquerade attack involves an attacker pretending to be an authorized user of a system, thus compromising the authentication component of the IT security model. Authentication ensures that the individuals accessing the system are who they claim to be. By masquerading as a legitimate user, an attacker can bypass this security measure and gain unauthorized access to the system.
Reference:
William Stallings, 'Security in Computing'.

QUESTION 5
What is a vulnerability called that is released before a patch comes out?

A. Initial
B. Pre-release
C. Zero day
D. First

Correct Answer: C
Section:
Explanation:
A vulnerability that is exploited before the vendor has issued a patch or even before the vulnerability is known to the vendor is referred to as a 'zero-day' vulnerability. The term 'zero-day' refers to the number of days the software vendor has had to address and patch the vulnerability since it was made public---zero, in this case.
Reference:
Symantec Security Response, 'Zero Day Initiative'.

QUESTION 6
The NIST SP 800-53 defines how many management controls?

A. 6
B. 9
C. 5

D. 7

Correct Answer: B
Section:
Explanation:
NIST SP 800-53 is a publication that provides a catalog of security and privacy controls for federal information systems and organizations and promotes the development of secure and resilient federal information and information systems.
According to the NIST SP 800-53 Rev. 5, the framework defines a comprehensive set of controls, which are divided into different families. Among these families, there are specifically nine families categorized under management controls. These include categories such as risk assessment, security planning, program management, and others.
Reference
'NIST Special Publication 800-53 (Rev. 5) Security and Privacy Controls for Information Systems and Organizations.'
NIST website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

QUESTION 7
A Virtual Private Network (VPN) requires how many Security Associations?

A. 5
B. 4
C. 3
D. 2

Correct Answer: D
Section:
Explanation:
A Virtual Private Network (VPN) typically requires two Security Associations (SAs) for a secure communication session. One SA is used for inbound traffic, and the other for outbound traffic.
In the context of IPsec, which is often used to secure VPN connections, these two SAs facilitate the bidirectional secure exchange of packets in a VPN tunnel.
Each SA uniquely defines how traffic should be securely processed, including the encryption and authentication mechanisms. This ensures that data sent in one direction is handled independently from data sent in the opposite direction, maintaining the integrity and confidentiality of both communication streams.
Reference
'Understanding IPSec VPNs,' by Cisco Systems.
'IPsec Security Associations,' RFC 4301, Security Architecture for the Internet Protocol.

QUESTION 8
Which of the ICS/SCADA generations is considered distributed?

A. Fourth
B. Second
C. Third
D. First
E. Knapp, J. Langill, 'Industrial Network Security,' Syngress, 2014.

Correct Answer: C
Section:
Explanation:
The third generation of ICS/SCADA systems is considered distributed. This generation features systems that are networked and interconnected, typically using a variety of standard communication protocols. This distribution allows for broader connectivity and integration with other systems, enhancing operational flexibility and efficiency but also introducing more vectors for potential cyber threats.
Reference:
Joseph Weiss, 'Protecting Industrial Control Systems from Electronic Threats'.

The third generation of ICS/SCADA systems is considered distributed. These systems emerged in the late 1990s and early 2000s and were designed to overcome the limitations of earlier generations by leveraging networked architectures.
Distributed Architecture: Third-generation systems distributed control functions across multiple interconnected devices and systems, providing greater scalability and flexibility.
Network Integration: These systems integrated more extensively with IT networks, allowing for remote monitoring and control.
Standard Protocols: Adoption of standard communication protocols (e.g., Ethernet, TCP/IP) facilitated interoperability and integration with other systems.
Enhanced Redundancy: Improved fault tolerance and redundancy were implemented to ensure system reliability.
Due to these features, the third generation is known as the distributed generation.
Reference
'SCADA Systems,' SCADAHacker, SCADA Generations.

QUESTION 9
What is the size of the AH in bits with respect to width?

A. 24
B. 43
C. 16
D. 32

Correct Answer: D
Section:
Explanation:
The Authentication Header (AH) in the context of IPsec has a fixed header portion of 24 bits and a mutable part that can vary, but when considering the fixed structure of the AH itself, the width is typically considered to be 32 bits at its core structure for basic operations in providing integrity and authentication, without confidentiality.
Reference:
RFC 4302, 'IP Authentication Header'.

QUESTION 10
Which of the registrars contains the information for the domain owners in Latin America?

A. AFRINIC
B. LACNIC
C. RIPENCC
D. ARIN

Correct Answer: B
Section:
Explanation:
LACNIC, the Latin American and Caribbean Internet Addresses Registry, is the regional internet registry (RIR) responsible for allocating and administering IP addresses and Autonomous System Numbers (ASNs) in Latin America and the Caribbean.
Function: LACNIC manages the distribution of internet number resources (IP addresses and ASNs) in its region, maintaining the registry of domain owners and other related information.
Coverage: The organization covers over 30 countries in Latin America and the Caribbean, including countries like Brazil, Argentina, Chile, and Mexico.
Services: LACNIC provides a range of services including IP address allocation, ASN allocation, reverse DNS, and policy development for internet resource management in its region.
Given this role, LACNIC is the correct answer for the registrar that contains information for domain owners in Latin America.
Reference
'About LACNIC,' LACNIC, LACNIC Overview.
'Regional Internet Registries,' Wikipedia, Regional Internet Registries.

QUESTION 11
Which of the following are valid TCP flags?

A. None of these
B. IGP,ACK,SYN,PSH,URG
C. BGP,FIN,PSH,SYN,ACK
D. FIN,PSH,URG,RST,SYN

Correct Answer: D
Section:
Explanation:
TCP flags are used in the header of TCP segments to control the flow of data and to indicate the status of a connection. Valid TCP flags include:
FIN: Finish, used to terminate the connection.
PSH: Push, instructs the receiver to pass the data to the application immediately.
URG: Urgent, indicates that the data contained in the segment should be processed urgently.
RST: Reset, abruptly terminates the connection upon error or other conditions.
SYN: Synchronize, used during the initial handshake to establish a connection. These flags are integral to managing the state and flow of TCP connections.
Reference:
Douglas E. Comer, 'Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture'.

QUESTION 12
Which of the options in the netstat command show the routing table?

A. c
B. a
C. r
D. s

Correct Answer: C
Section:
Explanation:
The netstat command is a versatile networking tool used for various network-related information-gathering tasks, including displaying all network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
The specific option -r with the netstat command is used to display the routing table.
This information is critical for troubleshooting network issues and understanding how data is routed through a network, identifying possible points of failure or security vulnerabilities.
Reference
'Linux Network Administrator's Guide,' by O'Reilly Media.
Man pages for netstat in UNIX/Linux distributions.

QUESTION 13
A Security Association is a ___________ way connection?

A. One
B. None of these
C. Two
D. Three

Correct Answer: A
Section:
Explanation:

A Security Association (SA) in the context of IPsec is a one-way logical connection used for secure communication between two endpoints. IPsec requires two SAs to establish a secure, bidirectional communication channel---one for each direction (inbound and outbound). This arrangement ensures that each direction is independently secured, with its own set of security parameters.
Reference:
RFC 4301, 'Security Architecture for the Internet Protocol'.

QUESTION 14
Which of the following are required functions of information management?

A. All of these
B. Date enrichment
C. Normalization
D. Correlation

Correct Answer: A
Section:
Explanation:
Information management within the context of network security involves several critical functions that ensure data is correctly handled for security operations. These functions include:
Normalization: This process standardizes data formats from various sources to a common format, making it easier to analyze systematically.
Correlation: This function identifies relationships between disparate pieces of data, helping to identify patterns or potential security incidents.
Data enrichment: Adds context to the collected data, enhancing the information with additional details, such as threat intelligence.
All these functions are essential to effective information management in security systems, allowing for more accurate monitoring and faster response to potential threats.
Reference
'Data Enrichment and Correlation in SIEM Systems,' Security Information Management Best Practices.
'Normalization Techniques for Security Data,' Journal of Network Security.

QUESTION 15
What type of communication protocol does Modbus RTU use?

A. UDP
B. ICMP
C. Serial
D. SSTP

Correct Answer: C
Section:
Explanation:
Modbus RTU (Remote Terminal Unit) is a communication protocol based on a master-slave architecture that uses serial communication. It is one of the earliest communication protocols developed for devices connected over serial lines. Modbus RTU packets are transmitted in a binary format over serial lines such as RS-485 or RS-232.
Reference:
Modbus Organization, 'MODBUS over Serial Line Specification and Implementation Guide V1.02'.

QUESTION 16
Which of the ICS/SCADA generations is considered monolithic?

A. Second
B. First
C. Fourth
D. Third

Correct Answer: B
Section:
Explanation:
The first generation of ICS/SCADA systems is considered monolithic, primarily characterized by standalone systems that had no external communications or connectivity with other systems. These systems were typically fully self-contained, with all components hard-wired together, and operations were managed without any networked interaction.
Reference:

U S. Department of Homeland Security, 'Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies'.

QUESTION 17
Which of the following components is not part of the Authentication Header (AH)?

A. Replay
B. Authentication
C. Confidentiality
D. Integrity

Correct Answer: C
Section:
Explanation:
The Authentication Header (AH) is a component of the IPsec protocol suite that provides authentication and integrity to the communications. AH ensures that the contents of the communications have not been altered in transit (integrity) and verifies the sending and receiving parties (authentication). However, AH does not provide confidentiality, which would involve encrypting the payload data. Confidentiality is provided by the Encapsulating Security Payload (ESP), another component of IPsec.
Reference:
RFC 4302, 'IP Authentication Header'.

QUESTION 18
How many main score areas are there in the CVSS?2

A. 2
B. 4
C. 3
D. None of these

Correct Answer: C
Section:
Explanation:
The Common Vulnerability Scoring System (CVSS) is a framework for rating the severity of security vulnerabilities. CVSS provides three main score areas: Base, Temporal, and Environmental.
Base Score evaluates the intrinsic qualities of a vulnerability.
Temporal Score reflects the characteristics of a vulnerability that change over time.
Environmental Score considers the specific impact of the vulnerability on a particular organization, tailoring the Base and Temporal scores according to the importance of the affected IT asset.
Reference:
FIRST, 'Common Vulnerability Scoring System v3.1: Specification Document'.

QUESTION 19
Which of the following is NOT an exploit tool?

A. Canvas

B. Core Impact

C. Metasploit

D. Nessus

Correct Answer: D
Section:
Explanation:
Among the options listed, Nessus is primarily a vulnerability assessment tool, not an exploit tool. It is used to scan systems, networks, and applications to identify vulnerabilities but does not exploit them. On the other hand, Canvas, Core Impact, and Metasploit are exploit tools designed to actually perform attacks (safely and legally) to demonstrate the impact of vulnerabilities.
Reference:
Tenable, Inc., 'Nessus FAQs'.

QUESTION 20
When monitoring a network, you receive an ICMP type 8 packet. What does this represent?

A. Echo request

B. Echo start

C. Echo recall

D. Echo reply

Correct Answer: A
Section:
Explanation:
ICMP (Internet Control Message Protocol) is used in network devices, like routers, to send error messages and operational information indicating success or failure when communicating with another IP address.
An ICMP type 8 packet specifically is an 'Echo Request.' It is used primarily by the ping command to test the connectivity between two nodes.
When a device sends an ICMP Echo Request, it expects to receive an ICMP Echo Reply (type 0) from the target node. This mechanism helps in diagnosing the state and reachability of a network on the Internet or within a private network.
Reference
RFC 792 Internet Control Message Protocol: https://tools.ietf.org/html/rfc792
Internet Assigned Numbers Authority (IANA) ICMP Parameters:

QUESTION 21
What type of protocol is considered connection-oriented?

A. UDP

B. TCP

C. ICMP

D. ARP

Correct Answer: B
Section:
Explanation:
TCP (Transmission Control Protocol) is a connection-oriented protocol used in the majority of internet communications.
Connection-oriented protocols like TCP require a connection to be established between the communicating devices before data is transmitted. This ensures reliable and ordered delivery of data.
TCP manages this by establishing a handshake mechanism (TCP three-way handshake) to set up the connection prior to transmitting data and properly terminating the connection once the communication session has completed.
Reference
'TCP/IP Illustrated, Volume 1: The Protocols' by W. Richard Stevens.

Postel, J., 'Transmission Control Protocol,' RFC 793.

QUESTION 22
Which of the following steps is used to reveal the IP addressing?

A. Footprinting
B. Surveillance
C. Cover your tracks
D. Enumeration

Correct Answer: D
Section:
Explanation:
Enumeration is a step in the information-gathering phase of a penetration test or cyber attack where an attacker actively engages with the target to extract detailed information, including IP addressing.
Enumeration: During enumeration, the attacker interacts with network services to gather information such as user accounts, network shares, and IP addresses.
Techniques: Common techniques include using tools like Nmap, Netcat, and Nessus to scan for open ports, services, and to identify the IP addresses in use.
Purpose: The goal is to map the network's structure, find potential entry points, and understand the layout of the target environment.
Because enumeration involves discovering detailed information including IP addresses, it is the correct answer.
Reference
'Enumeration in Ethical Hacking,' GeeksforGeeks, Enumeration.
'Network Enumeration,' Wikipedia, Network Enumeration.

QUESTION 23
Which of the following are not a part of the temporal score in the CVSS? (Select all that apply.)

A. Attack Vector
B. User Interaction
C. Reporting Confidence
D. Remediation Level

Correct Answer: A, B
Section:
Explanation:
The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.
The temporal score in CVSS adjusts the base score of a vulnerability based on factors that change over time, such as the availability of exploits or the existence of patches.
The temporal score includes:
Remediation Level
Report Confidence
Attack Vector and User Interaction are part of the base score, not the temporal score, as they describe the fundamental characteristics of the vulnerability and do not typically change over time.
Reference
Common Vulnerability Scoring System v3.1: Specification Document.
'Understanding CVSS,' by FIRST (Forum of Incident Response and Security Teams).

QUESTION 24
Which of the IPsec headers contains the Security Parameters Index (SPI)?

A. AH
B. Both AH and ESP

C. ESP
D. ICV

Correct Answer: B
Section:
Explanation:
IPsec uses two main protocols to secure network communications: Authentication Header (AH) and Encapsulating Security Payload (ESP).
Both AH and ESP use a Security Parameters Index (SPI), which is a critical component of their headers. The SPI is a unique identifier that enables the receiver to select the correct security association for processing incoming packets.
AH provides authentication and integrity, while ESP provides confidentiality, in addition to authentication and integrity. Both protocols use the SPI to manage these functions securely.
Reference
'IPsec Security Architecture,' RFC 4302 (AH) and RFC 4303 (ESP).
'IPsec Explained,' by Juniper Networks.

QUESTION 25
Which of the TCP flags represents data in the packet?

A. RST
B. ACK
C. PSH
D. FIN

Correct Answer: C
Section:
Explanation:
The PSH (Push) flag in the TCP header instructs the receiving host to push the data to the receiving application immediately without waiting for the buffer to fill. This is used to ensure that data is not delayed, thus improving the efficiency of communication where real-time data processing is required. It effectively tells the system that the data in the packet should be considered urgent.
Reference:
Douglas E. Comer, 'Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture'.

QUESTION 26
Which of the following is NOT ICS specific malware?

A. Flame
B. Ha vex
C. Code Red
D. Stuxnet

Correct Answer: C
Section:
Explanation:
Code Red is not ICS specific malware; it was a famous worm that targeted computers running Microsoft's IIS web server. Unlike Flame, Havex, and Stuxnet, which were specifically designed to target industrial control systems or perform espionage related to ICS environments, Code Red was aimed at exploiting vulnerabilities in internet-facing software to perform denial-of-service attacks and other malicious activities.
Reference:
CERT Coordination Center, 'Code Red Worm Exploiting Buffer Overflow In IIS Indexing Service DLL'.

QUESTION 27
A protocol analyzer that produces raw output is which of the following?

A. tcpdump
B. Wireshark
C. Capsa
D. Commview

Correct Answer: A
Section:
Explanation:
tcpdump is a powerful command-line packet analyzer used primarily in UNIX and UNIX-like operating systems; it allows the capture and display of TCP/IP and other packets being transmitted or received over a network to which the computer is attached.
Unlike graphical tools like Wireshark, tcpdump provides raw output of the packet captures directly to the terminal or a specified file, making it ideal for deep dive network analysis, especially in environments where a graphical user interface is unavailable.
tcpdump uses the libpcap library to capture packet data, which allows it to support a wide range of command-line options to filter and display packet information according to user needs.
Reference
'tcpdump manual page,' by the Tcpdump Group.
'Practical Packet Analysis Using Wireshark to Solve Real-World Network Problems,' by Chris Sanders, No Starch Press.

QUESTION 28
With respect to data analysis, which of the following is not a step?

A. Enumeration
B. All of these
C. vulnerabilities
D. Scanning for targets

Correct Answer: A
Section:
Explanation:
In the context of data analysis, enumeration is not typically considered a step. Enumeration is more relevant in security assessments and network scanning contexts where specific details about devices, users, or services are cataloged. Data analysis steps typically include gathering data, preprocessing, analyzing, and interpreting results rather than enumeration, which is more about identifying and listing components in a system or network.
Reference:
'Data Science from Scratch' by Joel Grus, which outlines common steps in data analysis.

QUESTION 29
What is the extension of nmap scripts?

A. .nsn
B. .nse
C. .nsv
D. .ns

Correct Answer: B
Section:
Explanation:
Nmap scripts, which are used to enhance the functionality of Nmap for performing network discovery, security auditing, and other tasks, have the extension .nse. This stands for Nmap Scripting Engine, which allows users to write scripts to automate a wide variety of networking tasks.
Reference:

Nmap Network Scanning by Gordon Lyon (also known as Fyodor Vaskovich), detailing the use and examples of Nmap scripts.

QUESTION 30
What does the SPI within IPsec identify?

A. Security Association
B. Key Exchange
C. Decryption algorithm
D. All of these

Correct Answer: A
Section:
Explanation:
Within IPsec, the SPI (Security Parameter Index) is a critical component that uniquely identifies a Security Association (SA) for the IPsec session. The SPI is used in the IPsec headers to help the receiving party determine which SA has been agreed upon for processing the incoming packets. This identification is crucial for the proper operation and management of security policies applied to the encrypted data flows.
Reference:
RFC 4301, 'Security Architecture for the Internet Protocol,' which discusses the structure and use of the SPI in IPsec communications.

QUESTION 31
Which of the following ports are used for communications in Modbus TCP?

A. 205
B. 405
C. 505
D. 502

Correct Answer: D
Section:
Explanation:
Modbus TCP is a variant of the Modbus family of simple, networked protocols aimed at industrial automation applications. Unlike the original Modbus protocol, which runs over serial links, Modbus TCP runs over TCP/IP networks.
Port 502 is the standard TCP port used for Modbus TCP communications. This port is designated for Modbus messages encapsulated in a TCP/IP wrapper, facilitating communication between Modbus devices and management systems over an IP network.
Knowing the correct port number is crucial for network configuration, security settings, and troubleshooting communications within a Modbus-enabled ICS/SCADA environment.
Reference
Modbus Organization, 'MODBUS Application Protocol Specification V1.1b3'.
'Modbus TCP/IP -- A Comprehensive Network protocol,' by Schneider Electric.

QUESTION 32
Which of the following is the stance that by default has a default deny approach?

A. Permissive
B. Paranoid
C. Promiscuous
D. Prudent

Correct Answer: B
Section:

Explanation:

In the context of network security policies, a 'Paranoid' stance typically means adopting a default-deny posture. This security approach is one of the most restrictive, where all access is blocked unless explicitly allowed.
A default deny strategy is considered best practice for securing highly sensitive environments, as it minimizes the risk of unauthorized access and reduces the attack surface.
This approach contrasts with more open stances such as Permissive or Promiscuous, which are less restrictive and generally allow more traffic by default.
Reference
'Network Security: Policies and Guidelines for Effective Network Management,' by Jonathan Gossels.
'Best Practices for Implementing a Security Awareness Program,' by Kaspersky Lab.

QUESTION 33

How many IPsec rules are there in Microsoft Firewall configuration?

A. 2
B. 5
C. 3
D. 4

Correct Answer: D
Section:
Explanation:

In the configuration of Microsoft Windows Firewall with Advanced Security, you can define IPsec rules as part of your security policy. Typically, these rules can be organized into four main categories: Allow connection, Block connection, Allow if secure (which can specify encryption or authentication requirements), and Custom. While the interface and features can vary slightly between Windows versions, four fundamental types of rules regarding how traffic is handled are commonly supported.
Reference:
Microsoft documentation, 'Windows Firewall with Advanced Security'.

QUESTION 34

Which component of the IT Security Model is usually the least priority in ICS/SCADA Security?

A. Integrity
B. Confidentiality
C. Availability
D. Authentication

Correct Answer: B
Section:
Explanation:

In ICS/SCADA systems, the typical priority hierarchy of the IT Security Model components places Availability and Integrity above Confidentiality. This prioritization is due to the critical nature of operational continuity and data accuracy in industrial control systems, where system downtime or incorrect data can lead to significant operational disruptions or safety issues. Confidentiality, while important, is often considered of lesser priority compared to ensuring systems are operational (Availability) and data is accurate (Integrity).
Reference:
National Institute of Standards and Technology (NIST), 'Guide to Industrial Control Systems (ICS) Security'.

QUESTION 35

What is used in the Modbus protocol to tell the slave to read or write?

A. None of these
B. Function code
C. Unit ID

D. Slave command

Correct Answer: B
Section:
Explanation:
In the Modbus protocol, the function code is used to tell the slave device what kind of action to perform, such as reading or writing data.
Modbus function codes specify the type of operation to be performed on the registers. For example, function code 03 is used to read holding registers, and function code 06 is used to write a single register.
Each function code is a single byte in size and is positioned at the start of the PDU (Protocol Data Unit) in the Modbus message structure, directly influencing how the slave interprets and executes the request.
Reference
'Modbus Application Protocol Specification V1.1b,' Modbus Organization.
'The Modbus Protocol Explained,' by Schneider Electric.

QUESTION 36
Which component of the IT Security Model is the highest priority in ICS/SCADA Security?

A. Integrity
B. Authentication
C. Availability
D. Confidentiality

Correct Answer: C
Section:
Explanation:
In ICS/SCADA systems, the highest priority typically is Availability, due to the critical nature of the services and infrastructures they support. These systems often control vital processes in industries like energy, water treatment, and manufacturing. Any downtime can lead to significant disruptions, safety hazards, or economic losses. Thus, ensuring that systems are operational and accessible is a primary security focus in the context of ICS/SCADA security.
Reference:
National Institute of Standards and Technology (NIST), 'Guide to Industrial Control Systems (ICS) Security'.

QUESTION 37
Which of the following is the name of hacking for a cause?

A. Lulzec
B. Anonymous
C. Hacktivism
D. Suicide Hackers

Correct Answer: C
Section:
Explanation:
Hacktivism refers to the act of hacking, or breaking into computer systems, for a politically or socially motivated purpose. Hacktivists use their skills to promote a cause, influence public opinion, or bring attention to social injustices. The term combines 'hacking' and 'activism,' representing a form of activism that takes place within cyberspace.
Reference:
Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy'.