DUMPSsheet

Free Questions for ICS-SCADA by dumpssheet

Shared by Cross on 17-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In physical to logical asset protections, what threat can be directed against the network?

Options:

A- Elevation of privileges

B- Flood the switch

C- All of these

D- Crack the password

Answer:

C

Explanation:

In the context of physical to logical asset protection in network security, several threats can be directed against the network, including:

Elevation of Privileges: Where unauthorized users gain higher-level permissions improperly.

Flood the Switch: Typically involves a DoS attack where the switch is overwhelmed with traffic, preventing normal operations.

Crack the Password: An attack aimed at gaining unauthorized access by breaking through password security. All these threats can potentially compromise the network's security and the safety of its physical and logical assets. Reference:

CompTIA Security+ Guide to Network Security Fundamentals.

Question 2

Question Type: MultipleChoice

What is the maximum size in bytes of an ethernet packet?

Options:

A- 1200

B- 1400

C- 1500

D- 1300

Answer:

C

Explanation:

The maximum transmission unit (MTU) for Ethernet, which is the largest size of an Ethernet packet or frame that can be sent over the network, is typically 1500 bytes. This size does not include the Ethernet frame's preamble and start frame delimiter but does include all other headers and the payload. Ethernet's MTU of 1500 bytes is a standard for most Ethernet networks, especially those conforming to the IEEE 802.3 standard. Reference:

IEEE 802.3-2012, 'Standard for Ethernet'.

Question 3

Question Type: MultipleChoice

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

Options:

A- Integrity

B- Confidentiality

C- Availability

D- Authentication

Answer:

B

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 4

Question Type: **MultipleChoice**

How many IPsec rules are there in Microsoft Firewall configuration?

Options:

A- 2

B- 5

C- 3

D- 4

Answer:

D

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 5

Question Type: **MultipleChoice**

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

Options:

A- Permissive

B- Paranoid

C- Promiscuous

D- Prudent

Answer:

B

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 6

Question Type: **MultipleChoice**

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

Options:

A- 205

B- 405

C- 505

D- 502

Answer:

D

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 7

Question Type: MultipleChoice

Which of the CVSS metrics refer to the exploit quotient of the vulnerability?

Options:

A- Temporal

B- Environmental

C- IBase

D- All of these

Answer:

A

Explanation:

The Common Vulnerability Scoring System (CVSS) uses several metrics to assess the severity of vulnerabilities. Among them, the Temporal metric group specifically reflects the exploit quotient of a vulnerability.

Temporal metrics consider factors that change over time after a vulnerability is initially assessed. These include:

Exploit Code Maturity: This assesses the likelihood of the vulnerability being exploited based on the availability and maturity of exploit code.

Remediation Level: The level of remediation available for the vulnerability, which influences the ease of mitigation.

Report Confidence: This metric measures the reliability of the reports about the vulnerability.

These temporal factors directly affect the exploitability and potential threat posed by a vulnerability, adjusting the base score to provide a more current view of the risk.

Reference

Common Vulnerability Scoring System v3.1: User Guide.

'Understanding CVSS,' by FIRST (Forum of Incident Response and Security Teams).