Eccouncil ICS-SCADA Practice Questions

Shared by Hewitt on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What share does the WannaCry ransomware use to connect with the target?

Options:

A- $IPC
B- $Admin
C- $SPOOL
D- $C

Answer:

A

Explanation:

The WannaCry ransomware utilizes the $IPC (Inter-Process Communication) share to connect with and infect target machines. This hidden network share supports the operation of named pipes, which facilitates the communication necessary for WannaCry to execute its payload across networks. Reference:

CISA Analysis Report, 'WannaCry Ransomware'.

WannaCry ransomware uses the SMB (Server Message Block) protocol to propagate through networks and connect to target systems. Specifically, it exploits a vulnerability in SMBv1, known as EternalBlue (MS17-010).

IPC Share: The $IPC (Inter-Process Communication) share is a hidden administrative share used for inter-process communication. WannaCry uses this share to gain access to other machines on the network.

SMB Exploitation: By exploiting the SMB vulnerability, WannaCry can establish a connection to the $IPC share, allowing it to execute the payload on the target machine.

Propagation: Once connected, it deploys the DoublePulsar backdoor and then spreads the ransomware payload.

Given these details, the correct answer is $IPC.

Reference

'WannaCry Ransomware Attack,' Wikipedia, WannaCry.

'MS17-010: Security Update for Windows SMB Server,' Microsoft, MS17-010.

Question 2

Question Type: MultipleChoice

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

Options:

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

Answer:

D

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 3

Question Type: MultipleChoice

Which of the following is the stance on risk that by default allows traffic with a default permit approach?

Options:

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

Answer:

D

Explanation:

In network security, the stance on managing and assessing risk can vary widely depending on the security policies of an organization.

A 'Permissive' stance, often referred to as a default permit approach, allows all traffic unless it has been specifically blocked. This approach can be easier to manage from a usability standpoint but is less secure as it potentially allows unwanted or malicious traffic unless explicitly filtered.

This is in contrast to a more restrictive policy, which denies all traffic unless it has been explicitly permitted, typically seen in more secure environments.

Reference

'Network Security Basics,' by Cisco Systems.

'Understanding Firewall Policies,' by Fortinet.

Question 4

Question Type: MultipleChoice

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

Options:

A- Footprinting

B- Surveillance
C- Cover your tracks
D- Enumeration

Answer:

D

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 5

Question Type: MultipleChoice

Which of the monitor alerts is considered most dangerous?

Options:

A- True Positive
B- False Positive
C- False Negative
D- True Negative

Answer:

C

Explanation:

In the context of monitoring and alerts within cybersecurity, the classification of alerts includes true positives, false positives, true negatives, and false negatives.

A false negative is considered the most dangerous type of alert because it occurs when an actual security threat is present but the monitoring system fails to detect and alert it. This allows malicious activities to occur undetected, potentially leading to significant damage or data loss.

The risk with false negatives is that they provide a false sense of security, assuming that systems are secure while in reality, they are compromised.

Reference

'Security and Network Monitoring Basics,' Cisco Systems.

'Understanding Alert Classifications in Cybersecurity,' Journal of Information Security.

Question 6

Question Type: MultipleChoice

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

Options:

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

Answer:

A

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 7

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 8

Question Type: MultipleChoice

With respect to the IEC 62443, how many steps are in the Defense in Depth process?

Options:

A- 8
B- 4
C- 6
D- 2

Answer:

C

Explanation:

IEC 62443 is a series of standards designed to secure Industrial Automation and Control Systems (IACS). It provides a framework for implementing cybersecurity measures in the context of industrial environments.

The Defense in Depth (DiD) approach outlined in IEC 62443 involves multiple layers of security measures to protect industrial networks. This method ensures that if one layer fails, others are in place to continue protection.

Specifically, the IEC 62443 framework describes six fundamental steps in setting up a Defense in Depth strategy, covering aspects from physical security to network segmentation and device hardening.

Reference

International Electrotechnical Commission, IEC 62443 Series.

'Understanding IEC 62443 for Industrial Cybersecurity,' by ISA99 Committee.

The IEC 62443 standard outlines a comprehensive framework for securing industrial automation and control systems (IACS). The Defense in Depth concept within this standard includes six steps designed to ensure robust security.

Step 1: Identification and Authentication Control (IAC): Ensuring only authorized users and devices can access the system.

Step 2: Use Control (UC): Managing permissions and access controls to restrict actions users can perform.

Step 3: System Integrity (SI): Ensuring the system remains in a trustworthy state, protected from unauthorized changes.

Step 4: Data Confidentiality (DC): Protecting sensitive data from unauthorized access and disclosure.

Step 5: Restricted Data Flow (RDF): Controlling and monitoring data flows to prevent unauthorized data transmission.

Step 6: Timely Response to Events (TRE): Implementing mechanisms to detect, respond to, and recover from security incidents.

These steps collectively form the Defense in Depth strategy prescribed by IEC 62443.

Reference

'IEC 62443 - Industrial Automation and Control Systems Security,' International Electrotechnical Commission, IEC 62443.

'Defense in Depth,' Cybersecurity and Infrastructure Security Agency (CISA), Defense in Depth.

Question 9

Question Type: MultipleChoice

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

Options:

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

Answer:

C

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 10

Question Type: MultipleChoice

Which of the following are NOT components of an ICS/SCADA network device?

Options:

A- Low processing threshold
B- Legacy systems
C- High bandwidth networks
D- Weak network stack

Answer:

C

Explanation:

Industrial Control Systems (ICS) and SCADA networks typically operate in environments where the available bandwidth is limited. They are often characterized by:

Low processing threshold: ICS/SCADA devices generally have limited processing capabilities due to their specialized and often legacy nature.

Legacy systems: Many ICS/SCADA systems include older technology that might not support newer security protocols or high-speed data transfer.

Weak network stack: These systems may have incomplete or less robust network stacks that can be susceptible to specific types of network attacks.

High bandwidth networks are not typical of ICS/SCADA environments, as these systems do not usually require or support high-speed data transmission due to their operational requirements and the older technology often used in such environments.

Reference

'Navigating the Challenges of Industrial Control Systems,' by ISA-99 Industrial Automation and Control Systems Security.

'Cybersecurity for Industrial Control Systems,' by the Department of Homeland Security.

Question 11

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.