Free Questions for ICS-SCADA by certsdeals

Shared by Christian on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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 2

Question Type: **MultipleChoice**

What type of protocol is represented by the number 6?

Options:

A- IUDP

B- IGRP

C- ICMP

D- TCP

Answer:

D

Explanation:

The protocol number 6 represents TCP (Transmission Control Protocol) in the Internet Protocol suite. TCP is a core protocol of the Internet Protocol suite and operates at the transport layer, providing reliable, ordered, and error-checked delivery of a stream of bytes between applications running on hosts communicating via an IP network. Reference:

RFC 793, 'Transmission Control Protocol,' which specifies the detailed operation of TCP.

Question 3

Question Type: **MultipleChoice**

What does the SPI within IPsec identify?

Options:

A- Security Association

B- Key Exchange

C- Decryption algorithm

D- All of these

Answer:

A

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 4

Question Type: MultipleChoice

What is the extension of nmap scripts?

Options:

A- .nsn

B- .nse

C- .nsv

D- .ns

Answer:

B

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 5

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 6

Question Type: MultipleChoice

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

Options:

A- tcpdump

B- Wireshark

C- Capsa

D- Commview

Answer:

A

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 7

Question Type: MultipleChoice

Which type of Intrusion Prevention System can monitor and validate encrypted data?

Options:

A- Memory

B- Network

C- Host

D- Anomaly

Answer:

B

Explanation:

A Network Intrusion Prevention System (NIPS) is capable of monitoring and validating encrypted data if it is integrated with technologies that allow it to decrypt the traffic.

Typically, network IPS can be set up with SSL/TLS decryption capabilities to inspect encrypted data as it traverses the network. This allows the IPS to analyze the content of encrypted packets and apply security policies accordingly.

Monitoring encrypted traffic is critical in detecting hidden malware, unauthorized data exfiltration, and other security threats concealed within SSL/TLS encrypted sessions.

Reference

'Network Security Technologies and Solutions,' by Yusuf Bhaiji, Cisco Press.

'Decrypting SSL/TLS Traffic with IPS,' by Palo Alto Networks.