Free Questions for ICS-SCADA by braindumpscollection

Shared by Woods on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- None of these

B- Function code

C- Unit ID

D- Slave command

Answer:

B

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 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 NOT ICS specific malware?

Options:

A- Flame

B- Ha vex

C- Code Red

D- Stuxnet

Answer:

C

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 4

Question Type: MultipleChoice

Which of the TCP flags represents data in the packet?

Options:

A- RST

B- ACK

C- PSH

D- FIN

Answer:

C

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 5

Question Type: MultipleChoice

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

Options:

A- Initial

B- Pre-release

C- Zero day

D- First

Answer:

C

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

Question Type: **MultipleChoice**

Which publication from NIST provides guidance on Industrial Control Systems?

Options:

A- NIST SP 800-90

B- NIST SP 800-82

C- NIST SP 800-77

D- NIST SP 800-44

Answer:

B

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 7

Question Type: MultipleChoice

Which of the ICS/SCADA generations is considered distributed?

Options:

A- Fourth

B- Second

C- Third

D- First

E- Knapp, J. Langill, 'Industrial Network Security,' Syngress, 2014.

Answer:

C

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 8

Question Type: MultipleChoice

Which of the IEC 62443 security levels is identified by a hacktivist/terrorist target?

Options:

A- 1

B- 3

C- 4

D- 2

Answer:

C

Explanation:

IEC 62443 defines multiple security levels (SLs) tailored to address different types of threats and attackers in industrial control systems.

Security Level 4 (SL4) is designed to protect against sophisticated attacks by adversaries such as hacktivists or terrorists. SL4 involves threats that are targeted with specific intent against the organization, using advanced skills and means.

This level assumes that the adversary is capable of sustained and focused efforts with significant resources, including state-level actors or well-funded groups, aiming at causing widespread disruption or damage.

Reference

IEC 62443-3-3: System security requirements and security levels.

'Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems,' by Eric Knapp.

Question 9

Question Type: **MultipleChoice**

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

Options:

A- AH

B- Both AH and ESP

C- ESP

D- ICV

Answer:

B

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 10

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 11

Question Type: **MultipleChoice**

How many IPsec modes are there?

Options:

A- Four

B- Three

C- None of these

D- Two

Answer:

D

Explanation:

IPsec (Internet Protocol Security) primarily operates in two modes: Transport mode and Tunnel mode.

Transport mode: Encrypts only the payload of each packet, leaving the header untouched. This mode is typically used for end-to-end communication between two systems.

Tunnel mode: Encrypts both the payload and the header of each IP packet, which is then encapsulated into a new IP packet with a new header. Tunnel mode is often used for network-to-network communications (e.g., between two gateways) or between a remote client and a gateway.

Reference

'Security Architecture for the Internet Protocol,' RFC 4301.

'IPsec Modes of Operation,' by Internet Engineering Task Force (IETF).