Free Questions for ICS-SCADA

Shared by Gonzales on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- c

B- a

C- r

D- s

Answer:

C

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 2

Question Type: MultipleChoice

Who developed the ModBus protocol?

Options:

A- Siemens

B- BAG

C- Modicon

D- Motorola

Answer:

C

Explanation:

The Modbus protocol was developed by Modicon, now a brand of Schneider Electric.

It was originally designed in 1979 for use with its programmable logic controllers (PLCs) in industrial applications.

Modbus is a serial communications protocol that has become a de facto standard communication protocol and is now commonly used to connect industrial electronic devices. The main reasons for its use are its simplicity and the fact that it is open-source, which allows manufacturers to build their own implementations of the standard.

Reference

'Modbus Protocol Reference Guide,' Modicon, Inc., 1979.

'A Guide to the Modbus Protocol,' Schneider Electric.

Question 3

Question Type: **MultipleChoice**

Which of the ICS/SCADA generations is considered networked?

Options:

A- Fourth

B- Third

C- Second

D- First

Answer:

B

Explanation:

Industrial Control Systems (ICS) have evolved through several generations, each characterized by different technological capabilities and integration levels.

The third generation of ICS/SCADA systems is considered networked. This generation incorporates more advanced digital and networking technologies, allowing for broader connectivity and communication across different systems and components within industrial environments.

Third-generation SCADA systems are often characterized by their use of standard communication protocols and networked solutions, improving interoperability and control but also increasing the attack surface for potential cyber threats.

Reference

'Evolution of Industrial Control Systems and Cybersecurity Implications,' IEEE Transactions on Industry Applications.

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

Question 4

Question Type: MultipleChoice

What form of attack uses a vector that infects a software package?

Options:

A- Spam

B- All of these

C- Quicksand

D- Watering Hole

Answer:

D

Explanation:

A 'watering hole' attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit.

The goal is to infect a website that members of a targeted community frequently use with malware. Once a user visits the compromised website, malware can be delivered to the user's system, exploiting vulnerabilities on their device.

This attack vector is used in scenarios where attackers want to breach secure environments indirectly by targeting less secure points in a network's ecosystem, such as third-party software used within the organization.

Reference

'Watering Hole Attacks: Detect, Disrupt, and Prevent,' by Kaspersky Lab.

'Emerging Threats in Cybersecurity: Understanding Watering Hole Attacks,' published in the Journal of Network Security.

Question 5

Question Type: **MultipleChoice**

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

Options:

A- Lulzec

B- Anonymous

C- Hacktivism

D- Suicide Hackers

Answer:

C

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'.

Question 6

Question Type: MultipleChoice

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

Options:

A- Integrity

B- Authentication

C- Availability

D- Confidentiality

Answer:

C

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 7

Question Type: MultipleChoice

Which of the following are valid TCP flags?

Options:

A- None of these

B- IGP,ACK,SYN,PSH,URG

C- BGP,FIN,PSH,SYN,ACK

D- FIN,PSH,URG,RST,SYN

Answer:

D

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 8

Question Type: **MultipleChoice**

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

Options:

A- AFRINIC

B- LACNIC

C- RIPENCC

D- ARIN

Answer:

B

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.