PassQueen
a.k.a dumpsqueen.com

ICS/SCADA Cyber Security Exam

ECCouncil ICS-SCADA

Version Demo

Total Demo Questions: 9

Total Premium Questions: 95

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A baseline-monitoring system reports a possible unauthorized PLC logic change. Which two findings most strongly support escalating the event for forensic triage? (Select two.)

A. A program download occurred outside an approved maintenance window

B. The PLC logic checksum differs from the approved baseline

C. An operator shift change occurred at the control room

D. A scheduled historian backup completed successfully

E. The historian performed normal periodic data queries

ANSWER: A B

Explanation:

A program download outside an approved maintenance window is significant because controller logic changes should be tied to authorized change activity. **A logic checksum that differs from the approved baseline** indicates that the controller program may have been altered and requires validation against approved engineering records.

An expected operator shift change is not evidence of a logic modification. A routine backup completion does not by itself indicate compromise, and normal periodic historian queries are unrelated to PLC program integrity.

QUESTION NO: 2

Which of the following are required functions of information management?

A. All of these

B. Data enrichment

C. Normalization

D. Correlation

ANSWER: A

Explanation:

All of these is correct because effective security information management depends on data enrichment, normalization, and correlation working together. Data enrichment adds useful context to incoming records, such as asset identity, network location, ownership, threat-intelligence indicators, or process relevance. This context makes operational and security events more meaningful to analysts and supports appropriate prioritization in an ICS/SCADA environment. Normalization converts data from different devices, protocols, and log formats into a consistent schema, allowing events from industrial controllers, servers, network equipment, and security tools to be searched and evaluated consistently. Correlation then connects related normalized and enriched events across sources and time, helping reveal a larger security condition or incident that may not be visible from any individual event. These capabilities are foundational to centralized log and event management, including SIEM use cases. NIST describes the importance of log normalization and analysis in centralized log management in NIST SP 800-92, Guide to Computer Security Log Management. NIST's SIEM guidance also identifies collecting, aggregating, normalizing, and correlating event information as key capabilities in NIST SP 1800-11.

QUESTION NO: 3

What is the extension of nmap scripts?

A. .nsn

B. .nse

C. .nsv

D. .ns

ANSWER: B

Explanation:

The correct extension is **.nse**. Nmap's scripting capability is called the Nmap Scripting Engine (NSE), and script files used by this engine are stored with the `.nse` filename extension. NSE scripts are written in the Lua programming language and enable Nmap to perform tasks beyond basic port scanning, including service and version interrogation, vulnerability detection, authentication testing, discovery, and network enumeration. Nmap includes a substantial script library, commonly installed in an `scripts` directory, and users can invoke scripts using the `--script` option. For example, a user may run a category of scripts or specify an individual file whose name ends in `.nse`. This extension identifies the file as an Nmap Scripting Engine script and allows it to be selected, indexed, and executed by Nmap's script subsystem. The official NSE documentation describes both the script engine and the standard naming convention for script files, while the Nmap reference guide documents use of the `--script` option during scans. See the Nmap Scripting Engine documentation and the Nmap Reference Guide.

QUESTION NO: 4

When applying the IEC 62443 zones and conduits concept to an ICS network, which two actions are appropriate? (Select two.)

A. Group assets with common security requirements into zones

B. Define and enforce required communications through conduits

C. Use one flat network for all enterprise and control assets

D. Place every ICS asset in a single security zone

E. Permit unrestricted communications between all zones

ANSWER: A B

Explanation:

Grouping assets with common security requirements into zones is appropriate because zones are logical or physical groupings of assets that share similar security needs. **Defining and enforcing required communications through conduits** is also appropriate because conduits control and protect the traffic exchanged between zones.

A flat network removes the boundaries needed to apply differentiated controls. Placing every asset in a single zone ignores differing security requirements, while allowing unrestricted interzone communication defeats the purpose of controlled conduits.

QUESTION NO: 5

How many IPsec rules are there in Microsoft Firewall configuration?

A. 2

B. 5

C. 3

D. 4

ANSWER: B

Explanation:

5 is correct because Windows Firewall with Advanced Security configures IPsec through Connection Security Rules, and its New Connection Security Rule Wizard provides five rule types: isolation, authentication exemption, server-to-server, tunnel, and custom. These rule types define how IPsec protection is applied between computers or networks. For example, an isolation rule can require authenticated connections for selected endpoints, a server-to-server rule protects communications between designated hosts, and a tunnel rule establishes protected traffic between gateways. Authentication-exemption rules identify traffic that must remain reachable without IPsec authentication, while custom rules provide granular configuration for scenarios that do not fit the predefined templates. Therefore, the Microsoft Firewall IPsec rule configuration model is represented by five available Connection Security Rule types, rather than by the inbound or outbound firewall action choices used to filter ordinary traffic. Microsoft's documentation identifies these Connection Security Rule categories in the Windows Firewall with Advanced Security management model. See Microsoft's Windows Firewall configuration documentation and Windows Firewall with Advanced Security overview.

QUESTION NO: 6

A critical PLC has a vendor-confirmed vulnerability, but the required firmware update cannot be applied until the next planned outage. Which two actions provide the most appropriate compensating controls? (Select two.)

A. Restrict PLC communications to explicitly required hosts, ports, and protocols

B. Require engineering access through a secured jump host

C. Move the PLC to the enterprise user VLAN

D. Enable automatic firmware updates without operational testing

E. Disable PLC and firewall logging to preserve storage capacity

ANSWER: A B

Explanation:

Restricting communications to explicitly required hosts and services and **requiring controlled engineering access through a secured jump host** reduce exposure while the PLC remains unpatched. Allowlisting at the zone boundary limits the systems that can reach the PLC, while a jump host can enforce strong authentication, authorization, logging, and approved access paths for engineering activities.

Connecting the PLC to an enterprise VLAN increases its exposure. Automatic firmware updates are generally unsuitable for control assets because updates require testing and operational approval. Disabling logging removes evidence needed to detect and investigate misuse.

QUESTION NO: 7

What type of communication protocol does Modbus RTU use?

A. UDP

B. ICMP

C. Serial

D. SSTP

ANSWER: C

Explanation:

Serial is correct because Modbus RTU is the binary serial-line variant of the Modbus application protocol. It communicates by framing Modbus messages as binary data and transmitting them over serial physical interfaces, most commonly RS-485 and, in some deployments, RS-232. In a typical Modbus RTU serial network, one controller initiates requests and field devices return responses; device addressing and strict timing between message frames allow multiple devices to share the same serial bus. The RTU format uses a compact binary representation of function codes and data, followed by a cyclic redundancy check for detecting transmission errors. This makes Modbus RTU particularly common in industrial control environments, including PLCs, remote terminal units, drives, meters, and sensors. The Modbus Organization's serial-line specification defines Modbus RTU as an implementation over a two-wire serial line and describes its frame structure and timing requirements. Although Modbus can also be carried over Ethernet using Modbus TCP, that is a distinct transport implementation; the "RTU" designation specifically identifies the serial, binary framing mode. See the MODBUS over Serial Line Specification and Implementation Guide and the Modbus Organization specifications.

QUESTION NO: 8

A security team is preparing to collect packet captures from an operational network during an intermittent communications problem. Which two practices best preserve useful evidence while minimizing operational risk? (Select two.)

A. Use a network TAP or configured mirror port to collect traffic without placing the analyzer inline

B. Inject test packets continuously while capturing traffic

C. Synchronize the capture system time and document the collection period

D. Save only decoded packet summaries and discard the original capture

E. Reconfigure PLC network settings before beginning the capture

ANSWER: A C

Explanation:

Use a network TAP or configured mirror port to collect traffic without placing the analyzer inline and **synchronize the capture system time and document the collection period** are correct. Passive collection avoids disrupting production communications, while accurate timestamps support correlation with alarms, logs, and operator actions.

Injecting test packets can affect fragile devices and changes the evidence being collected. Capturing only decoded summaries may omit packet details needed for later analysis. Reconfiguring PLC network settings during an intermittent problem can worsen the outage and alter the environment.

QUESTION NO: 9

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

A. 1

B. 3

C. 4

D. 2

ANSWER: B

Explanation:

3 is the appropriate IEC 62443 security level for a hacktivist/terrorist threat target. Security Level 3 addresses protection against intentional violations carried out using sophisticated means by an adversary with moderate resources, relevant industrial-automation and control-system knowledge, and moderate motivation. Hacktivist and terrorist actors may deliberately target industrial operations to cause disruption, gain publicity, advance an ideological objective, or create physical and economic consequences. Such attacks can involve more than opportunistic tools: adversaries may conduct reconnaissance, exploit known weaknesses, use tailored malware or remote-access compromise paths, and understand

enough of the targeted environment to affect operations. Therefore, an IACS zone or conduit assessed as needing resistance to this type of capable, intentional threat is commonly aligned with Security Level 3. IEC 62443 uses security levels as risk-based capability targets rather than labels for specific organizations, so the selection should be supported by the system’s threat assessment and consequences of compromise. The IEC 62443 standards family is described by ISA/IEC 62443, while IEC provides the official catalogue entry for the foundational security-level concepts in IEC 62443-1-1.