PassQueen
a.k.a dumpsqueen.com

Global Industrial Cyber Security Professional ()

GIAC GICSP

Version Demo

Total Demo Questions: 7

Total Premium Questions: 76

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An engineer identifies an intermittent, unauthorized 2.4 GHz transmission near a process area. The engineer must first determine whether the source is Wi-Fi, Bluetooth, Zigbee, or another radio-frequency device before selecting a containment action. Which tool is most useful?

A. Spectrum analyzer

B. Packet analyzer

C. Vulnerability scanner

D. Cable tester

ANSWER: A

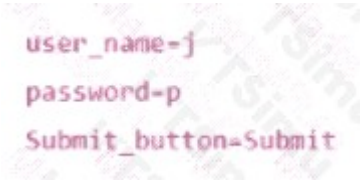
Explanation:

A spectrum analyzer is most useful because it displays radio-frequency energy across a frequency range and can help characterize the timing, bandwidth, and channel occupancy of the unknown transmission. This provides visibility into emitters even when their traffic cannot yet be associated with a known network protocol or endpoint.

A packet analyzer requires access to traffic in a supported protocol and may not observe an unknown emitter. A vulnerability scanner actively probes networked systems and is not appropriate for identifying RF emissions. A cable tester validates wired cabling and does not analyze wireless spectrum.

QUESTION NO: 2

Use sqlmap to dump tables from http://locjlhost/index.php? page-login, php.The data necessary for this is as follows:



How many tables does sqlmap find in the dojo control database? Hint: The option to dump tables is –tables

A. 3

B. 86

C. 82

D. 84

E. 1

F. 83

G. 4

ANSWER: D

Explanation:

84 is correct. In sqlmap, the `--tables` switch enumerates the tables available in the selected database after the target, injection point, and database context have been established. The relevant result is the total reported by sqlmap for the dojo control database in the supplied lab environment: 84 tables. This is an enumeration result rather than a count inferred from

the number of databases or from the number of rows in any one table. After identifying an injectable parameter, an operator would normally use `--dbs` to identify databases, select the intended database with `-D`, and then use `--tables` to retrieve the schema's table list and its reported count. Enumerating database objects is useful during authorized testing because it establishes the exposed application data model and supports appropriately scoped subsequent validation. sqlmap documents table enumeration and database selection in its usage reference: sqlmap Wiki: Enumeration. The project's official repository also provides the tool and its current documentation: sqlmap on GitHub. This activity must be performed only against systems and training environments for which explicit authorization has been granted.

QUESTION NO: 3

A facility uses badge readers on the entrance to a control room. Security staff observe that an unauthorized person can enter by following an authorized employee through the door before it closes. Which physical-security control most directly addresses this weakness?

A. Install a mantrap or other anti-tailgating entry control

B. Install a higher-resolution surveillance camera

C. Replace the door lock with a stronger keyed lock

D. Post additional warning signs at the entrance

ANSWER: A

Explanation:

A mantrap or other anti-tailgating entry control most directly addresses the weakness because it restricts passage so that individuals must be separately authenticated before entering the protected area. Badge-reader records alone show that a credential was used but may not establish that every person entering was authorized.

A higher-resolution camera can improve investigation and detection but does not necessarily prevent entry. A stronger door lock delays forced entry but does not stop an authorized person from holding the door open. Additional warning signs may deter some behavior but do not provide reliable access enforcement.

QUESTION NO: 4

An organization needs to provide a vendor with remote access to an engineering workstation during a scheduled maintenance window. The workstation is on the Level 2 supervisory network, and the vendor does not require access to any other control-system asset. Which design best supports this requirement?

A. A jump host in an industrial DMZ with time-limited, authenticated access

B. A direct VPN connection from the vendor network to the Level 2 workstation

C. A permanent local account on the engineering workstation for the vendor

D. An enterprise user workstation configured to share its remote-desktop session

ANSWER: A

Explanation:

A jump host in an industrial DMZ with time-limited, authenticated access is the best design. The vendor first connects to a controlled intermediary in the DMZ, where access can be approved, monitored, recorded, and restricted to the maintenance window. A tightly controlled connection from that host to the specific engineering workstation can then be permitted through the relevant security boundary.

Direct VPN access into Level 2 bypasses an important segmentation and monitoring point. A permanent vendor account creates unnecessary standing access, while allowing the vendor to connect through a general enterprise workstation does

not provide the same purpose-built control boundary. The design should also use least privilege, multifactor authentication where feasible, session logging, and prompt removal of access when the work is complete.

QUESTION NO: 5

Which control helps prevent threats to Integrity?

A. Firewall egress filtering

B. Logging IDS alerts

C. Centralized LDAP authentication

D. Implementing digital signatures

ANSWER: D

Explanation:

Implementing digital signatures helps prevent integrity threats by cryptographically binding a signed object to both its contents and the signer's private key. A recipient can validate the signature using the corresponding public key; validation detects whether the signed data, such as a firmware image, configuration file, command package, or software update, was modified after signing. This makes digital signatures especially valuable in industrial environments, where unauthorized changes to control logic or device firmware can create operational and safety consequences. Digital signatures also provide origin authentication: when certificate validation and key management are properly implemented, the verifier can establish that the item was signed by an authorized publisher. In practice, this control should be applied before deployment or execution and supported by secure key storage, certificate lifecycle management, and a trusted process for approving signers. NIST describes digital signatures as mechanisms used to detect unauthorized modification of data and authenticate the signatory. CISA likewise identifies code signing as a means to verify software integrity and publisher identity. See NIST FIPS 186-5, Digital Signature Standard and CISA Code Signing Best Practices.

QUESTION NO: 6

What is a use of Network Address Translation?

A. To maximize Firewall functionality

B. To make access list configuration easier

C. To hide private network addresses

D. To enable network routing functionality

ANSWER: C

Explanation:

Network Address Translation is used to hide private network addresses by translating internally used private IPv4 addresses into one or more externally routable public addresses when traffic crosses a network boundary. Private-address ranges are not globally routable on the public Internet, so NAT lets systems in an internal enterprise or industrial-control-network segment communicate outward without exposing their private addressing scheme directly. A common implementation, Port Address Translation, permits numerous internal hosts to share a single public IPv4 address by distinguishing their connections with transport-layer port information. This capability has been widely used both to conserve scarce public IPv4 addresses and to separate internal addressing from external addressing. In an ICS architecture, NAT may be deployed at carefully managed boundaries, such as between an industrial DMZ and another network, where its address-obfuscation and address-management functions can support segmentation design. NAT is not itself a complete security control; it should be used alongside firewalls, access-control rules, monitoring, and well-defined conduits. The Internet Engineering Task Force describes traditional NAT behavior and its translation of address and port mappings in RFC 3022. NIST also discusses the importance of segmented network architectures and controlled communications for operational technology environments in NIST SP 800-82 Rev. 3.

QUESTION NO: 7

A safety instrumented system independently trips a process when pressure exceeds a defined safe limit. A proposed change would place the safety-system controller on the same routable network segment as the basic process-control PLC to simplify engineering access. What is the primary security concern?

A. The shared segment can create a common-mode path affecting both control and safety functions

B. The safety controller cannot use Ethernet communications under any circumstances

C. The basic-control PLC must always be configured as the safety controller’s backup

D. The safety trip will no longer require a defined pressure setpoint

ANSWER: A

Explanation:

The primary concern is that the change reduces independence between the basic process-control system and the safety function. A compromise, network fault, or unauthorized engineering action affecting the shared segment could create a common-mode path to both the normal control function and the protective shutdown function. Safety functions should be protected through appropriate separation, controlled conduits, and tightly managed engineering access.

The issue is not that a safety controller cannot communicate over a network or that it can never be maintained remotely. Rather, its security architecture must preserve the independence and availability needed for it to perform its protective role when the basic control system behaves unexpectedly or is compromised.