PassQueen
a.k.a dumpsqueen.com

CIW v5 Security Essentials

CIW 1D0-571

Version Demo

Total Demo Questions: 8

Total Premium Questions: 85

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Principles	26
Topic 2, Perimeter Security	17
Topic 3, Operating System Security	17
Topic 4, Network Security	14
Topic 5, Security Policies	11
Total	85

QUESTION NO: 1

You have been assigned to configure a DMZ that uses multiple firewall components. Specifically, you must configure a router that will authoritatively monitor and, if necessary, block traffic. This device will be the last one that inspects traffic before it passes to the internal network. Which term best describes this device?

A. Screening router

B. Bastion host

C. Proxy server

D. Choke router

ANSWER: D

Explanation:

Choke router is correct because it is the filtering router positioned at the critical, tightly controlled boundary between a DMZ and the trusted internal network. In a multi-component DMZ design, this router acts as the final enforcement point for traffic attempting to move from systems exposed to less-trusted networks toward internal resources. Its rules authoritatively permit only required, explicitly authorized connections and block traffic that does not meet the organization's policy. The "choke" concept reflects concentrating this transit through a controlled path so that traffic can be inspected, filtered, logged, and stopped before it reaches the internal network. This placement supports defense in depth: even if a public-facing system in the DMZ is compromised, the attacker must still traverse a separately administered boundary with restrictive controls before reaching internal assets. NIST describes firewalls as controls that enforce an organization's network security policy by monitoring and controlling incoming and outgoing network traffic; a choke router applies that enforcement at the internal side of the DMZ boundary. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and Cisco guidance on DMZ security design.

QUESTION NO: 2

Which of the following errors most commonly occurs when responding to a security breach?

A. Shutting down network access using the firewall, rather than the network router

B. Adhering to the company policy rather than determining actions based on the IT manager's input

C. Making snap judgments based on emotions, as opposed to company policy

D. Taking too much time to document the attack

ANSWER: C

Explanation:

Making snap judgments based on emotions, as opposed to company policy is the most common and consequential error described here. A security incident can create intense pressure to act immediately, particularly when responders fear data loss, service outages, or reputational damage. However, decisions driven by panic, anger, or assumptions can lead to unnecessary disruption, destruction of volatile evidence, missed containment steps, and actions that conflict with legal, regulatory, or organizational obligations. A documented incident-response policy provides predefined authority, escalation paths, communication procedures, evidence-handling practices, and containment and recovery processes. Following that plan enables responders to make deliberate, coordinated, and auditable decisions even under stressful conditions. NIST emphasizes that incident response should be based on established policies and procedures, with preparation occurring before an incident so that personnel can respond consistently and effectively. The organization's incident-response capability should also define roles and decision-making authority, reducing reliance on improvised individual judgment during a breach. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the CISA incident response resources.

QUESTION NO: 3

You have been asked to encrypt a large file using a secure encryption algorithm so you can send it via e-mail to your supervisor. Encryption speed is important. The key will not be transmitted across a network. Which form of encryption should you use?

A. Asymmetric

B. PGP

C. Hash

D. Symmetric

ANSWER: D

Explanation:

Symmetric encryption is the appropriate choice because it uses one shared secret key for both encryption and decryption and is designed to process large amounts of data efficiently. Since encryption speed is explicitly important, a modern symmetric cipher such as AES is well suited to encrypting a large file before it is sent by email. The condition that the key will not be transmitted over a network removes the principal key-distribution concern associated with shared-key encryption: the sender and supervisor can establish or exchange the secret through a trusted, out-of-band method. Symmetric cryptography is therefore commonly used for bulk data encryption, including files, disks, backups, and high-volume communications. NIST identifies AES as a symmetric block cipher standardized for protecting electronic data, with approved key sizes that provide strong practical security when implemented and managed correctly. In real-world secure messaging systems, asymmetric cryptography may help establish or protect a session key, but the file's actual data is typically encrypted with a symmetric algorithm because of its performance characteristics. See NIST FIPS 197: Advanced Encryption Standard (AES) and NIST Guide to Encryption and Key Management.

QUESTION NO: 4

Consider the following series of commands from a Linux system: iptables -A input -p icmp -s 0/0 -d 0/0 -j REJECT Which explanation best describes the impact of the resulting firewall ruleset?

A. Individuals on remote networks will no longer be able to use SSH to control internal network resources.

B. Internal hosts will not be able to ping each other using ICMP.

C. Stateful multi-layer inspection has been enabled.

D. Individuals on remote networks will not be able to use ping to troubleshoot connections.

E. The command fails because the built-in INPUT chain name is case-sensitive, so no rule is added.

ANSWER: E

Explanation:

The command fails under a standard iptables configuration because built-in chain names are case-sensitive. The built-in chain that processes packets addressed to the local host is named `INPUT`, not `input`. Therefore, unless an administrator has separately created a user-defined chain literally named `input`, iptables cannot find the specified chain and does not append the ICMP rejection rule. The usual result is an error indicating that the chain or target does not exist, and the active firewall ruleset remains unchanged. This distinction matters because an apparently small capitalization error can mean a security control was never deployed. To create the intended inbound rule, the command would need to name the built-in chain as `INPUT`, for example: `iptables -A INPUT -p icmp -s 0/0 -d 0/0 -j REJECT`. The iptables manual identifies the built-in chains using uppercase names, including `INPUT`, and documents that `-A` appends a rule to the named chain. See the iptables manual page and the Netfilter documentation.

QUESTION NO: 5

Which of the following standards is used for digital certificates?

A. DES

B. Diffie-Hellman

C. X.509

D. RC5

ANSWER: C

Explanation:

X.509 is the standard used to define the format and structure of public-key digital certificates. An X.509 certificate binds a subject's identity, such as a person, organization, server, or device, to a public key. It includes essential fields such as the certificate issuer, subject name, public-key information, serial number, validity period, certificate version, and the issuer's digital signature. These standardized fields allow software and services to consistently validate certificates and build a chain of trust to a trusted certificate authority. X.509 certificates are the certificate type commonly used by TLS/SSL to authenticate websites and establish encrypted HTTPS connections. They are also used in many enterprise public key infrastructure deployments for purposes including user authentication, device authentication, email security, and code signing. The ITU-T Recommendation X.509 specifies the public-key certificate framework, while the IETF's RFC 5280 profiles X.509 certificates and certificate revocation lists for Internet use. See the ITU-T X.509 recommendation and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

QUESTION NO: 6

At the beginning of an IPsec session, which activity occurs during the Internet Key Exchange (IKE)?

A. Determining the number of security associations

B. Negotiating the authentication method

C. Determining the network identification number

D. Negotiating the version of IP to be used

ANSWER: B

Explanation:

Negotiating the authentication method is correct because IKE establishes the security parameters that IPsec peers will use before protected traffic is sent. During IKE negotiation, the peers authenticate one another and agree on the cryptographic and security settings needed to create an IPsec Security Association. Authentication can be performed using methods such as pre-shared keys, digital certificates, or signature-based authentication, depending on the configured policy. This initial exchange also provides a secure basis for deriving keying material and establishing the protected IPsec connection.

In IKEv2, the IKE_SA_INIT and IKE_AUTH exchanges establish the IKE Security Association, negotiate cryptographic algorithms, exchange nonces and keying material, identify the peers, and authenticate them. The resulting authenticated IKE Security Association is then used to negotiate Child Security Associations that protect the actual IP traffic. This authentication negotiation is therefore a fundamental activity at the beginning of an IPsec session. See the IKEv2 specification in RFC 7296 and the IPsec/IKE overview in Cisco's IKEv2 documentation.

QUESTION NO: 7

A Web application stores a session identifier in a user's browser after successful authentication. Which mechanism is most commonly used to store this identifier?

A. A cookie

B. A digital certificate

C. A DNS record

D. A firewall rule

ANSWER: A

Explanation:

A cookie is correct because web applications commonly use an HTTP cookie to maintain a session identifier between requests. The browser returns the cookie to the server with later requests, allowing the server to associate the requests with the authenticated session. Session cookies should be protected using attributes such as Secure, HttpOnly, and SameSite, and the session identifier should be unpredictable and regenerated after authentication. The HTTP cookie mechanism is defined in RFC 6265.

QUESTION NO: 8

Which of the following is most likely to address a problem with an operating system's ability to withstand an attack that attempts to exploit a buffer overflow?

A. Firewall

B. Software update

C. Intrusion detection system

D. Network scanner

ANSWER: B

Explanation:

Software update is correct because buffer-overflow vulnerabilities are commonly defects in operating-system components, services, libraries, or drivers that mishandle data written to memory. When a vendor discovers and fixes such a flaw, it distributes the remediation through a security patch, hotfix, or other software update. Applying the update replaces or modifies the vulnerable code so that excessive or malformed input is correctly checked and cannot be used to overwrite memory in the manner the exploit requires. Maintaining a timely patch-management process is therefore a primary control for improving an operating system's resilience to known buffer-overflow attacks. Updates may also introduce or improve exploit mitigations, such as address-space layout randomization and data-execution prevention, which make successful memory-corruption exploitation more difficult. Organizations should obtain updates from the operating-system vendor, test them according to their change-management process, and deploy them promptly based on risk and vulnerability severity. The U.S. Cybersecurity and Infrastructure Security Agency identifies timely patching as essential to mitigating known vulnerabilities, and Microsoft documents memory-protection features that help defend against memory-corruption exploits. See CISA's Known Exploited Vulnerabilities Catalog and Microsoft's Data Execution Prevention documentation.