PassQueen
a.k.a dumpsqueen.com

GIAC Certified Perimeter Protection Analyst

GIAC GPPA

Version Demo

Total Demo Questions: 32

Total Premium Questions: 322

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Mark has been assigned a project to configure a wireless network for a company. The network should contain a Windows 2003 server and 30 Windows XP client computers. Mark has a single dedicated Internet connection that has to be shared among all the client computers and the server. The configuration needs to be done in a manner that the server should act as a proxy server for the client computers.

Which of the following programs can Mark use to fulfill this requirement?

A. Wingate

B. Microsoft Internet Security & Acceleration Server (ISA)

C. Sniffer

D. SOCKS

ANSWER: A

Explanation:

Wingate is the appropriate choice because it is proxy-server and Internet-connection-sharing software designed to run on a centrally managed Windows host and provide controlled Internet access to multiple client systems. Installed on the Windows Server 2003 system, it can accept requests from the Windows XP clients, proxy supported application traffic on their behalf, and use the server's dedicated Internet connection as the shared outbound connection. This arrangement centralizes access policy, authentication, logging, and connection management rather than requiring each workstation to have its own direct Internet-facing configuration. For a network with approximately 30 client computers, a server-based proxy deployment also provides an administratively practical way to manage users and monitor usage from one point. WinGate documentation describes its proxy services and its role in allowing client machines to access Internet services through a WinGate server. Its product materials also describe gateway capabilities for sharing an Internet connection and applying policy to client traffic. See the WinGate Documentation Wiki and the vendor's WinGate features overview.

QUESTION NO: 2

You work as a Network Administrator for ABC Inc. The company has a TCP/IP network. You have been assigned a task to configure a stateful packet filtering firewall to secure the network of the company. You are encountering some problems while configuring the stateful packet filtering firewall.

Which of the following can be the reasons for your problems?

Each correct answer represents a complete solution. (Choose all that apply.)

A. It contains additional overhead of maintaining a state table.

B. It has limited logging capabilities.

C. It has to open up a large range of ports to allow communication.

D. It is complex to configure.

ANSWER: A D

Explanation:

Stateful packet filtering adds operational complexity because the firewall must inspect traffic in the context of active connections rather than evaluating every packet independently. It tracks details such as source and destination addresses, ports, protocol state, sequence information where applicable, and connection timeouts. The resulting state table consumes memory and processing resources, particularly on busy perimeter devices handling many simultaneous flows. Administrators must size the firewall appropriately and tune session limits and timeout values so that legitimate traffic remains reliable while stale or abusive sessions do not exhaust resources.

It is also complex to configure because rules must account for connection direction, permitted session initiation, return traffic, protocol behavior, address translation interactions, and exception handling. A policy that is logically sound can still cause unexpected connectivity issues if its ordering, state matching, or timeout assumptions are not aligned with the applications using the network. NIST describes stateful inspection as maintaining state information for network connections and emphasizes the importance of carefully defining and managing firewall policy rules. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and CISA: Understanding Firewall Basics.

QUESTION NO: 3

Which of the following attacks generates falsified information within an IP header?

A. Web spoofing attack

B. DNS spoofing attack

C. IP spoofing attack

D. ARP spoofing attack

ANSWER: C

Explanation:

IP spoofing attack is correct because it involves creating IP packets with a forged source IP address in the Internet Protocol header. The source-address field identifies the apparent origin of a packet; altering it causes the recipient or an intermediate system to see a packet as originating from an address selected by the attacker rather than its actual sender. This technique can be used to conceal an attacker's identity, impersonate a trusted host where network conditions permit, or support reflection and denial-of-service attacks. Since the falsified value is specifically placed in the IP header, this is accurately described as IP spoofing. Effective perimeter defenses commonly apply ingress and egress filtering, validating that source addresses arriving on an interface are plausible for the network from which they were received. The Internet Engineering Task Force's guidance on network ingress filtering describes filtering forged source addresses as a key anti-spoofing control. See RFC 2827, Network Ingress Filtering and the CISA overview of denial-of-service attacks.

QUESTION NO: 4

Which of the following DNS operations transfers an entire DNS zone from a primary name server to a secondary name server?

A. AXFR

B. PTR

C. MX

D. SOA

ANSWER: A

Explanation:

AXFR is correct because it is the DNS full zone-transfer operation. A secondary authoritative server uses AXFR to request the complete set of resource records for a zone from the primary server. This supports replication of authoritative DNS data and redundancy for name-resolution services.

From a perimeter-security perspective, unrestricted zone transfers can disclose hostnames, addressing information, mail-server records, and other useful reconnaissance data. DNS administrators should restrict zone-transfer requests to explicitly authorized secondary servers and use transaction security controls where appropriate. RFC 5936 defines AXFR, and RFC 1034 describes the DNS domain and zone model. See RFC 5936, DNS Zone Transfer Protocol and RFC 1034, Domain Names - Concepts and Facilities.

QUESTION NO: 5

Poplu works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Poplu started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution.

Which of the following data should be recorded in this documentation?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Date and time of incident

B. Names of the victims

C. Nature of harassment

D. Location of each incident

ANSWER: A B C D

Explanation:

Effective sexual-harassment incident documentation should establish the basic facts needed for a prompt, fair internal investigation and for any subsequent administrative or legal process. Recording the **Date and time of incident** creates a chronological record, helps identify potentially relevant schedules, messages, access records, or witnesses, and supports assessment of whether conduct was isolated or repeated. Recording the **Names of the victims** identifies the affected person or persons and allows the organization to provide notice, protection, support, and an opportunity to provide a complete account. The **Nature of harassment** must be documented with sufficiently specific factual detail about the conduct, communications, or behavior reported; this is central to determining the scope and seriousness of the allegation. The **Location of each incident** identifies where events occurred and may help preserve physical, digital, video, or access-control evidence and locate witnesses. Together, these details create a reliable factual record while enabling the employer to investigate and take appropriate corrective action. The U.S. Equal Employment Opportunity Commission describes harassment as unlawful when conduct becomes a condition of employment or is severe or pervasive enough to create a hostile work environment, making accurate incident facts particularly important. See the EEOC sexual harassment guidance and the EEOC enforcement guidance on workplace harassment.

QUESTION NO: 6

You have to ensure that your Cisco Router is only accessible via telnet and ssh from the following hosts and subnets:

10.10.2.103

10.10.0.0/24

Which of the following sets of commands will you use to accomplish the task?

A. access-list 10 permit 10.10.2.103 access-list 10 permit 10.10.0.0 0.0.0.255 access-list 10 deny any line vty 0 4 access-group 10 in

B. access-list 10 permit host 10.10.2.103 access-list 10 permit 10.10.0.0 0.0.0.255 access-list 10 deny any line vty 0 4 access-class 10 out

C. access-list 10 permit host 10.10.2.103 access-list 10 permit 10.10.0.0 0.0.0.255 access-list 10 deny any line vty 0 4 access-class 10 in

D. access-list 10 permit host 10.10.2.103 access-list 11 permit host 10.10.0.0 255.255.255.0 access-list 12 deny any line vty 0 4 access-group 10, 11, 12 in

ANSWER: C

Explanation:

`access-list 10 permit host 10.10.2.103 access-list 10 permit 10.10.0.0 0.0.0.255 access-list 10 deny any line vty 0 4 access-class 10 in` is correct because it creates a standard IPv4 access control list that permits exactly the specified individual source host and the specified /24 source network, then applies that ACL to incoming connections on the router's virtual terminal lines. The `host` keyword represents a single IPv4 address, so it precisely matches 10.10.2.103. In Cisco ACL syntax, 10.10.0.0 with the wildcard mask 0.0.0.255 matches all addresses from 10.10.0.0 through 10.10.0.255, which is the requested /24 subnet. The explicit `deny any` ensures remaining source addresses are denied; an implicit deny would also exist at the end of an ACL. Crucially, `access-class 10 in` is configured under `line vty` and filters inbound management-session attempts, including Telnet and SSH, based on the source IP address. Cisco documents the use of `access-class` to restrict access to VTY lines and distinguishes it from interface ACL application: Cisco access-class command reference. Cisco's ACL overview also describes wildcard-mask matching used by standard ACLs: Configuring Commonly Used IP ACLs.

QUESTION NO: 7

You work as a Network Administrator for ABC Inc. The company has a Windows Server 2008based network. You have created a test domain for testing IPv6 addressing. Which of the following types of addresses are supported by IPv6?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Broadcast

B. Multicast

C. Anycast

D. Unicast

ANSWER: B C D

Explanation:

IPv6 supports **Unicast**, **Anycast**, and **Multicast** address types. A unicast address identifies a single network interface, so traffic sent to that address is delivered to one intended destination. IPv6 defines multiple unicast scopes and uses, including global unicast addresses for Internet-routable communication and link-local addresses for communication on the local network segment. Anycast addresses can be assigned to more than one interface, typically on different hosts; a packet sent to an anycast address is routed to the nearest interface according to the network routing topology. This supports resilient and efficient delivery to services deployed at multiple locations. Multicast addresses identify a group of interfaces, allowing a sender to transmit one packet that is delivered to every member of the specified group. IPv6 relies on multicast for important control and discovery functions, including Neighbor Discovery, and uses solicited-node multicast addresses to support efficient address resolution. These three address categories are defined by the IPv6 addressing architecture and are foundational to IPv6 host and routing behavior. See the IPv6 Addressing Architecture (RFC 4291) and Microsoft's IPv6 overview.

QUESTION NO: 8

A Security Administrator is reviewing controls to reduce the risk of SYN flood attacks against an Internet-facing TCP service.

Which of the following measures can help protect the service?

Each correct answer represents a complete solution. (Choose three.)

A. Enable SYN cookies.

B. Tune the backlog for pending TCP connections.

C. Apply SYN rate limits or connection thresholds at the perimeter.

D. Block all TCP SYN packets.

ANSWER: A B C

Explanation:

SYN cookies help a TCP stack avoid allocating connection-state resources until the client completes the TCP three-way handshake. Increasing or tuning the backlog for pending connections can provide additional capacity for legitimate connection attempts during short bursts. A perimeter firewall or load balancer can also apply rate limits or connection thresholds to excessive SYN traffic, helping reduce the load that reaches the protected service.

Blocking all TCP SYN packets would prevent legitimate clients from establishing new TCP connections and is not an appropriate defensive solution. SYN flood attacks attempt to exhaust resources by creating many incomplete connection attempts. RFC 4987 describes TCP SYN flooding and common mitigations, including SYN cookies and filtering techniques. See RFC 4987, TCP SYN Flooding Attacks and Common Mitigations.

QUESTION NO: 9

Which of the following protocols does IPsec use to perform various security functions in the network?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Internet Key Exchange

B. Authentication Header

C. Encapsulating Security Payload

D. Skinny Client Control Protocol

ANSWER: A B C

Explanation:

IPsec uses Internet Key Exchange, Authentication Header, and Encapsulating Security Payload to provide its key security functions. Internet Key Exchange (IKE) establishes and manages Security Associations, authenticates peers, and negotiates the cryptographic algorithms and keying material that protect IPsec communications. In contemporary IPsec deployments, IKEv2 is the standard key-management protocol. Authentication Header (AH) supplies connectionless integrity, data-origin authentication, and optional anti-replay protection for IP packets. Encapsulating Security Payload (ESP) supplies those protections as well as confidentiality through encryption, making ESP the commonly deployed IPsec payload-protection protocol. AH and ESP can operate in transport or tunnel mode, while IKE supports the negotiation and lifecycle management needed for protected IPsec traffic. Together, these protocols form the IPsec architecture's mechanisms for peer authentication, key establishment, integrity verification, replay defense, and—when ESP encryption is selected—confidentiality. The Internet Engineering Task Force defines the IPsec architecture and its security services in RFC 4301; the current IKEv2 specification is available in RFC 7296.

QUESTION NO: 10

You work as a Network Administrator for ABC Inc. The company wants to reduce the possibility of source IP address spoofing on an Internet-facing router.

Which of the following features should be configured to verify that a route back to the source address exists through the interface on which a packet is received?

A. Unicast Reverse Path Forwarding

B. Port Address Translation

C. Spanning Tree Protocol

D. Dynamic Host Configuration Protocol

ANSWER: A

Explanation:

Unicast Reverse Path Forwarding (uRPF) is correct because it validates the source address of an arriving packet by consulting the routing table. In strict mode, the router verifies that the best return route to the packet's source address uses the same interface on which the packet arrived. If the route does not match, the router can discard the packet as potentially spoofed. This makes uRPF a useful perimeter control against traffic that claims an invalid or unreachable source address.

uRPF must be applied carefully on networks that use asymmetric routing, because legitimate packets may arrive on an interface other than the one selected by the return route. RFC 3704 describes ingress filtering and reverse-path validation techniques for reducing IP source-address spoofing. See RFC 3704, Ingress Filtering for Multihomed Networks.

QUESTION NO: 11

Which of the following tools can be used for passive OS fingerprinting?

A. nmap

B. dig

C. tcpdump

D. ping

ANSWER: C

Explanation:

tcpdump can be used for passive OS fingerprinting because it captures and displays packets that systems already transmit on the network, without sending probing traffic to the target. Operating systems often produce distinguishable TCP/IP characteristics in ordinary traffic, particularly during TCP connection establishment. An analyst can inspect fields such as the initial TTL, TCP window size, TCP option ordering, maximum segment size, window-scaling values, selective-acknowledgment support, and the presence or behavior of timestamps. Taken together, these characteristics can indicate the likely operating-system family or network stack implementation.

tcpdump is therefore useful both as a direct packet-inspection utility and as a collection mechanism for passive fingerprinting analysis. For example, capturing SYN packets with an appropriate filter allows the analyst to observe the target host's advertised TCP parameters while remaining nonintrusive. This approach is valuable during network monitoring, incident response, and perimeter analysis because it does not require an active scan or a response from the observed host beyond its normal communications. The tcpdump manual documents its packet-capture and filtering capabilities, while the p0f project provides additional background on passive fingerprinting techniques: tcpdump manual and p0f passive fingerprinting.

QUESTION NO: 12

Which of the following Linux file systems is a journaled file system?

A. ext4

B. ext3

C. ext

D. ext2

ANSWER: A

Explanation:

`ext4` is a journaled Linux file system. Journaling records intended metadata updates, and optionally file-data updates depending on the configured data mode, in a dedicated journal before the changes are committed to the main file-system structures. This write-ahead record helps the file system recover consistently after an unexpected shutdown, power loss, or system crash. During the next mount, the journal can be replayed so that incomplete updates are resolved without requiring a full consistency scan of every file-system structure. ext4 supports several journaling modes, including ordered mode, which

is commonly the default and ensures relevant file data is written before its associated metadata is committed to the journal. It also supports journal checksums and other reliability and scalability improvements. The Linux kernel's ext4 documentation describes its journaling behavior and recovery design in detail, while the ext4 manual page identifies the journal as a core on-disk feature: Linux kernel ext4 documentation and ext4(5) manual page.

QUESTION NO: 13

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

• It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.

• It is commonly used for the following purposes:

a) War driving

b) Detecting unauthorized access points

c) Detecting causes of interference on a WLAN

d) WEP ICV error tracking

e) Making Graphs and Alarms on 802.11 Data, including Signal Strength

This tool is known as _____.

A. THC-Scan

B. Kismet

C. Absinthe

D. NetStumbler

ANSWER: D

Explanation:

NetStumbler is the correct answer because it is a Windows wireless-network discovery utility designed to identify nearby IEEE 802.11 wireless LANs. It collects and presents the information named in the question, including access-point SSID, BSSID/MAC address, radio channel, and received signal level. Its graphical display and logging capabilities make it particularly useful during authorized wireless-site surveys and troubleshooting, where an analyst needs to identify coverage patterns, observe signal changes, and recognize sources of WLAN interference.

NetStumbler is also historically associated with wardriving: while moving through an area, an authorized tester can use it to record detected wireless networks and their signal characteristics. In a perimeter-protection context, the same discovery data can support identification of unexpected or unauthorized access points and help validate the organization's wireless inventory. The tool's ability to expose wireless-network metadata and track radio observations explains the references to signal graphs, alarms, and WEP integrity-check-value error monitoring. NetStumbler's project information is available at NetStumbler. For background on how Windows manages and exposes wireless LAN interfaces, see Microsoft's Native Wi-Fi API documentation.

QUESTION NO: 14

You work as a Network Administrator for ABC Inc. The company wants to harden the management plane of its perimeter routers and firewalls.

Which of the following controls should be implemented?

Each correct answer represents a complete solution. (Choose three.)

A. Use SSH for command-line administration.

B. Restrict management access to approved source networks.

C. Use SNMPv3 with authentication and privacy.

D. Enable Telnet for remote administration.

ANSWER: A B C

Explanation:

Using **SSH** for command-line administration protects management credentials and commands from network interception. Restricting administrative access with an access-control list limits management connections to approved source addresses or a dedicated management network. Using **SNMPv3** provides authentication and privacy features for management monitoring, unlike older SNMP versions that commonly expose community strings and management information in clear text.

Telnet should not be enabled for administrative access because it transmits the session, including credentials, without encryption. Secure management-plane configuration should also include strong authentication, authorization, accounting, logging, and timely patching of management services. NIST recommends protecting network-device management interfaces and using secure protocols in NIST SP 800-41 Rev. 1. RFC 3414 defines the User-based Security Model used by SNMPv3; see RFC 3414.

QUESTION NO: 15

Which of the following types of IP actions are supported by an IDP rulebase? (Choose three.)

A. Initiate rules of the rulebase

B. Notify

C. Drop/block session

D. Close connection

ANSWER: B C D

Explanation:

An IDP rulebase supports response actions that both create visibility into detected attacks and actively stop the traffic associated with a match. **Notify** is an alerting action: it records and reports the event so that security personnel and monitoring systems can investigate the policy match. **Drop/block session** is a protective enforcement action that prevents the matched traffic flow from continuing through the device. This is appropriate when the signature indicates malicious or policy-prohibited activity and the goal is to contain it immediately.

Close connection is also an active response. It terminates the applicable TCP connection by sending reset traffic, helping end an already-established session rather than merely handling a single packet. Together, notification, session blocking, and connection closing represent the main operational categories of IDP response: observe and log the event, prevent continued passage of the malicious flow, and actively terminate a connection when protocol state permits. The selected actions therefore provide both detection visibility and practical perimeter protection. Juniper's IDP policy documentation describes policy actions and their use in responding to matching attack objects; see Juniper IDP policy overview and Juniper IDP policy actions.

QUESTION NO: 16

Which of the following statements are true about an IPv6 network?

Each correct answer represents a complete solution. (Choose all that apply.)

A. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.

B. It provides improved authentication and security.

C. It uses 128-bit addresses.

D. It increases the number of available IP addresses.

E. It uses longer subnet masks than those used in IPv4.

ANSWER: A B C D

Explanation:

IPv6 uses 128-bit addressing, producing an address space vastly larger than IPv4's 32-bit address space. This expanded space supports substantially more globally unique addresses and enables common deployment practices such as assigning a /64 prefix to a typical LAN. IPv6 also defines an IP-layer security architecture and was designed with IPsec integration in mind, including support for authentication and confidentiality services when those protections are deployed. In addition, IPv6 defines IPv4-embedded address representations for transition and interoperability scenarios. In IPv4-mapped and formerly IPv4-compatible forms, the IPv4 address occupies the low-order 32 bits of the 128-bit IPv6 representation. This lets IPv6-capable systems and software represent or handle IPv4 endpoint addresses in an IPv6-oriented context. The IPv6 addressing architecture, including the 128-bit address format and IPv4-embedded forms, is specified in RFC 4291. IPv6's security architecture and the relationship between IPv6 and IPsec are described by the IPv6 Node Requirements (RFC 6434).

QUESTION NO: 17

WinDump, tcpdump, and Wireshark specify which fields of information libpcap should record.

Which of the following filters do they use in order to accomplish the task?

A. FIR filter

B. IM filter

C. Web filter

D. Berkeley Packet Filter

ANSWER: D

Explanation:

Berkeley Packet Filter is correct. Libpcap-based capture tools such as tcpdump, WinDump, and Wireshark use the Berkeley Packet Filter (BPF) mechanism to define capture filters. A capture-filter expression, such as `tcp port 443` or `host 192.0.2.10`, is compiled into BPF instructions and provided to the packet-capture subsystem. The filtering can be applied in the operating system kernel, allowing packets that do not satisfy the expression to be discarded before they are copied to the user-space application. This reduces unnecessary packet processing, memory use, and capture overhead, which is particularly important on busy network links. BPF filtering is distinct from display filtering: capture filtering controls the packets libpcap records or delivers to the application, while display filtering is applied afterward to packets already captured. The libpcap manual documents that a filter expression is compiled into a packet-filter program and attached to a capture handle. Wireshark likewise identifies its capture-filter syntax as being based on the libpcap filter language. See the pcap-filter manual page and Wireshark's pcap-filter documentation.

QUESTION NO: 18

Which of the following devices are used to implement Network Address Translation (NAT)?

A. Routers and switches

B. Routers and firewalls

C. Firewalls and file servers

D. Switches and firewalls

ANSWER: B

Explanation:

Routers and firewalls is correct because NAT is normally performed at the boundary between networks by a device that routes traffic between IP networks. NAT translates address information in packet headers, allowing privately addressed internal hosts to communicate with external networks through one or more public addresses. A router can apply source NAT, destination NAT, and port address translation while forwarding traffic between interfaces. A firewall commonly provides the same NAT capabilities, often coupling its translation rules with security-policy enforcement so that published services and outbound connections can be controlled at the perimeter.

This placement is important: the device implementing NAT must see traffic as it enters or leaves the relevant address domains and must maintain translation state so return packets are mapped to the proper internal endpoint. Cisco's overview describes NAT as translating private internal addresses to public addresses as packets move between networks, a function implemented on routing devices. The NIST firewall guidance also identifies network address translation as a common firewall capability. See Cisco: What Is Network Address Translation? and NIST SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 19

The simplest form of a firewall is a packet filtering firewall. A packet filtering firewall filters packets at the Network layer and Transport layer.

What are the types of information that are filtered at the Network layer of the OSI reference model?

Each correct answer represents a complete solution. (Choose all that apply.)

A. TCP and UDP port numbers

B. IP addresses

C. TCP/IP protocols

D. TCP control flags

ANSWER: B C

Explanation:

At the OSI Network layer, packet-filtering decisions are based on fields in the Internet Protocol header. **IP addresses** are Network-layer identifiers: the source address identifies the originating IP host or network, and the destination address identifies the intended IP host or network. A firewall can use either or both values to permit or deny traffic according to defined address-based policy rules.

TCP/IP protocols are also identifiable at this layer through the IP header's Protocol field. That field specifies the next encapsulated protocol, such as TCP, UDP, or ICMP, enabling a packet filter to apply rules based on the IP protocol carried within the packet. Although TCP and UDP are commonly associated with Transport-layer communication, their protocol identifiers are conveyed by the Network-layer IP header and can therefore be selected by an IP packet-filtering rule.

RFC 791 defines IPv4 header fields including Source Address, Destination Address, and Protocol, and describes the Protocol field as indicating the next-level protocol used in the data portion of an IP datagram. See RFC 791: Internet Protocol. For a practical description of packet-filtering rules using source/destination addresses and protocol values, see the Netfilter Packet Filtering HOWTO.

QUESTION NO: 20

Mark works as a Network Security Administrator for BlueWells Inc. The company has a Windowsbased network. Mark is giving a presentation on Network security threats to the newly recruited employees of the company. His presentation is about the External threats that the company recently faced in the past.

Which of the following statements are true about external threats?

Each correct answer represents a complete solution. (Choose three.)

A. These threats can be countered by implementing security controls on the perimeters of the network, such as firewalls, which limit user access to the Internet.

B. These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access.

C. These are the threats that originate from within the organization.

D. These are the threats intended to flood a network with large volumes of access requests.

ANSWER: A B D

Explanation:

External threats originate outside an organization's trusted environment and involve attempts by unaffiliated attackers or Internet-based sources to affect systems, services, data, or network availability. The statement "These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access." correctly identifies the defining source and objective of an external attack. Perimeter controls are a key defensive layer because they regulate traffic crossing the boundary between internal networks and untrusted networks. Accordingly, "These threats can be countered by implementing security controls on the perimeters of the network, such as firewalls, which limit user access to the Internet." correctly describes the role of firewalls and related boundary protections in reducing exposure and enforcing access policy. Finally, "These are the threats intended to flood a network with large volumes of access requests." describes denial-of-service activity, which commonly comes from external hosts, including distributed sources, and targets the availability of public-facing or Internet-reachable services. NIST identifies denial-of-service attacks as attacks that prevent or impair authorized use of networks, systems, or applications. See NIST's denial-of-service definition and CISA guidance on denial-of-service attacks.

QUESTION NO: 21

Paul works as a Technical Representative in a CSIRT for ABC Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Paul wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis.

Which of the following is the correct order for searching data on a Windows based system?

A. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system.

B. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces.

C. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces.

D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps.

ANSWER: C

Explanation:

The correct sequence is "Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces." It represents a structured Windows forensic-search workflow that begins by addressing volatile information, which is most susceptible to loss when a system state changes. The examiner then proceeds through local disk-resident artefacts, including file slack and the broader file system, before examining configuration and user-activity evidence held in the Windows Registry. Memory-dump and system-state material can then provide further context about the running environment and operating-system configuration, while internet traces are reviewed as user-activity artefacts that can help reconstruct browsing, download, and potential data-exfiltration activity. Applying a defined sequence helps ensure that evidence sources

are considered consistently and that relationships between files, Registry entries, system configuration, memory information, and browser artefacts can be correlated during analysis. This approach is consistent with established incident-response and digital-forensics guidance emphasizing preservation of volatile evidence and systematic collection and examination of relevant system artefacts. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and NIST guidance on handling digital media and evidence.

QUESTION NO: 22

Which of the following types of vulnerability scanners performs a black-box test?

A. Port scanner

B. Web application security scanner

C. CGI scanner

D. Network scanner

ANSWER: B

Explanation:

Web application security scanner is correct because these tools commonly assess an application from the perspective of an external, unauthenticated or minimally authenticated user, without relying on access to its source code or internal implementation. The scanner discovers the reachable attack surface by crawling pages, following links, identifying forms and parameters, and sending carefully constructed HTTP requests. It then evaluates the application's observable responses for indicators of security weaknesses, such as injection flaws, cross-site scripting, broken session handling, and insecure server configuration. This approach is characteristically black-box: the assessment is based on inputs supplied to the running application and outputs returned by it, rather than a review of how the application was built. In perimeter protection work, such scanning is valuable because it reflects what an Internet-facing attacker can discover and exercise against a deployed web service. OWASP describes black-box web application testing as testing without knowledge of the application's internal structure and provides a methodology for this form of assessment in the OWASP Web Security Testing Guide. Additional practical guidance on web application scanning is available from CISA's web application security resources.

QUESTION NO: 23

You work as a Network Administrator for ABC Inc. The company has a Windows Server 2008- based network. You have created a test domain for testing IPv6 addressing.

Which of the following types of addresses are supported by IPv6?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Broadcast

B. Multicast

C. Anycast

D. Unicast

ANSWER: B C D

Explanation:

IPv6 supports unicast, multicast, and anycast addressing. A unicast address identifies a single network interface, so packets sent to that address are delivered to one specific interface. IPv6 unicast includes several operationally important scopes and forms, such as global unicast addresses for routable communication, link-local addresses used on the local network segment, and unique local addresses for private internal use. Multicast identifies a group of interfaces, allowing a sender to transmit one packet that is delivered to every interface that has joined the applicable multicast group. IPv6 relies on multicast for functions such as Neighbor Discovery and router discovery, rather than using broadcast traffic. Anycast allows the same

address to be assigned to multiple interfaces, generally on different nodes; traffic sent to that address is routed to the nearest instance according to the routing topology. This is useful for providing resilient, geographically distributed services while presenting a single destination address. These three address types are defined by the IPv6 addressing architecture and are the applicable IPv6 delivery models. See RFC 4291, IP Version 6 Addressing Architecture and Microsoft's IPv6 overview.

QUESTION NO: 24

A remote-access VPN offers secured and encrypted connections between mobile or remote users and their corporate network across public networks.

Which of the following does the remote access VPN use for offering these types of connections? Each correct answer represents a complete solution. (Choose two.)

A. TLS

B. SSL

C. SSH

D. IPsec

ANSWER: B D

Explanation:

Remote-access VPNs commonly use SSL and IPsec to protect communications between a remote user and an organizational network over an untrusted network. SSL VPN is the traditional term for a remote-access VPN that establishes an encrypted session using the SSL/TLS security protocol family. It is widely used to provide browser-based access to internal web resources or client-based access to broader sets of network resources. The VPN gateway authenticates the remote user and applies authorization policy before permitting access through the protected session.

IPsec is also a standard remote-access VPN technology. An IPsec remote-access deployment generally uses an IPsec client and a VPN gateway to authenticate peers, negotiate cryptographic security associations, and encapsulate protected IP traffic. This allows the remote endpoint to communicate securely with corporate network resources as though it were connected through a protected network path. NIST describes both IPsec and SSL/TLS VPN technologies as common approaches for securing remote access, while noting that each can be deployed with appropriate authentication and endpoint controls. See NIST SP 800-113, Guide to SSL VPNs and RFC 4301, Security Architecture for IP.

QUESTION NO: 25

Which of the following is used for debugging the network setup itself by determining whether all necessary routing is occurring properly, allowing the user to further isolate the source of a problem?

A. Netfilter

B. iptables

C. WinPcap

D. tcpdump

ANSWER: D

Explanation:

tcpdump is the correct answer because it captures and displays packets observed on a network interface, allowing an analyst to verify what traffic is actually entering and leaving a host. During routing troubleshooting, packet captures can establish whether a host is transmitting traffic toward its configured gateway, whether return traffic arrives on the expected interface, and whether fields such as source and destination addresses, protocol values, ports, and TCP flags match expectations. Filtering capabilities are particularly useful: an analyst can focus on a specific host, subnet, port, or protocol

rather than examining unrelated traffic. Comparing captures at multiple points in a path helps isolate where packets stop appearing or begin to take an unexpected route. This evidence-based approach distinguishes a routing or reachability problem from an application, host-firewall, or service issue. tcpdump is a command-line packet analyzer built on the libpcap capture interface and is widely used in perimeter and network operations for rapid diagnostic capture. Its packet-selection expressions and output controls are documented in the tcpdump manual page; the underlying capture-library behavior is described by the libpcap documentation.

QUESTION NO: 26

John works as a Network Administrator for Web Perfect Inc. The company has a wireless LAN network. John has configured shared key authentication on a client. The client and the AP start exchanging the frames to enable authentication.

Which of the following vulnerabilities may occur while the client and the AP exchange the challenge text over the wireless link?

A. Land attack

B. DoS attack

C. Vulnerability attack

D. Man-in-the-middle attack

ANSWER: D

Explanation:

Man-in-the-middle attack is correct because IEEE 802.11 shared-key authentication using WEP sends the access point's challenge text in cleartext and then receives that same challenge encrypted with the WEP RC4 keystream. An attacker within radio range can capture both versions of the same data. Comparing the plaintext challenge with its encrypted form can reveal the keystream associated with the initialization vector used in that exchange. This exposure allows an active attacker to forge or alter appropriately protected traffic for that keystream context, inject frames, and impersonate a participant in the wireless exchange. In practical terms, the attacker can position themselves between the client and access point at the wireless layer and manipulate communications rather than merely observe them. This is a fundamental design weakness of WEP shared-key authentication: proving knowledge of the shared key inadvertently provides material useful for attacks against WEP-protected frames. Modern wireless deployments should avoid WEP and use WPA2 or WPA3 with robust authentication and encryption instead. See Cisco's discussion of the weaknesses in WEP shared-key authentication in its Wireless LAN Security Overview and the IEEE 802.11 Wi-Fi terminology and security context.

QUESTION NO: 27

You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo.

Which of the following folders on the local computer will you review to accomplish the task?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Temporary Internet Folder

B. History folder

C. Download folder

D. Cookies folder

ANSWER: A B D

Explanation:

Temporary Internet Folder, History folder, and Cookies folder are appropriate sources of local forensic evidence when a person uses browser-based email such as Hotmail or Yahoo Mail. Browser caches, historically called Temporary Internet Files/Temporary Internet Folder in Windows and Internet Explorer contexts, can retain locally stored copies or fragments of web pages, images, scripts, and downloaded content associated with webmail activity. These artifacts can help establish that a mailbox was accessed and may preserve useful contextual information from the web session.

The History folder or browser-history database records visited URLs and access times. This can identify visits to webmail providers, sign-in pages, message views, attachment links, and other web-based mail actions. Cookie storage is also relevant because cookies may retain identifiers, account-related preferences, authentication-state artifacts, and timestamps that associate a browser profile with a particular webmail service or user activity. Examiners should acquire and analyze these artifacts using forensically sound methods, while recognizing that their locations and formats vary by browser and operating system. The NIST Guide to Integrating Forensic Techniques into Incident Response describes collecting and examining browser-related evidence, and the CISA computer forensics guidance emphasizes preserving relevant local artifacts during an investigation.

QUESTION NO: 28

You are the Administrator for a corporate network. You are concerned about denial of service attacks.

Which of the following would be most helpful against Denial of Service (DOS) attacks?

A. Honey pot

B. Network surveys

C. Stateful Packet Inspection (SPI) firewall

D. Packet filtering firewall

ANSWER: C

Explanation:

Stateful Packet Inspection (SPI) firewall is the best answer because it evaluates traffic in the context of an active connection, rather than judging each packet independently. By maintaining a state table, an SPI firewall can recognize whether packets are part of legitimate, established sessions and can enforce protocol-appropriate connection behavior. This is particularly useful for reducing exposure to certain network-layer and transport-layer denial-of-service techniques, including unsolicited packets and malformed or invalid connection attempts. It can also apply connection limits, timeout policies, and rate-related controls, depending on the implementation, helping prevent a perimeter device or internal host from processing unnecessary traffic.

For TCP traffic, stateful inspection enables the firewall to observe the expected connection setup and subsequent packet flow, making it a meaningful defensive control at the network boundary. It should be deployed as one layer of a broader availability strategy that includes upstream DDoS protection, capacity planning, monitoring, and an incident-response process. NIST describes denial-of-service attacks as attempts to impair availability and identifies filtering and network defenses as relevant mitigations. See NIST's Denial-of-Service definition and CISA guidance on DDoS.

QUESTION NO: 29

You work as a Network Administrator for ABC Inc. The company wants to implement egress filtering at its Internet perimeter.

Which of the following controls are appropriate for an egress-filtering policy? Each correct answer represents a complete solution. (Choose three.)

A. Permit only authorized internal source address ranges.

B. Allow only outbound services required for business operations.

C. Log denied outbound connections.

D. Allow all outbound traffic without inspection.

ANSWER: A B C

Explanation:

Egress filtering controls traffic leaving an organization and should limit outbound communication to authorized sources, destinations, services, and protocols. Permitting only valid internal source address ranges helps prevent compromised or misconfigured systems from sending traffic with unauthorized source addresses. Restricting outbound services to approved business requirements reduces opportunities for malware command-and-control, data exfiltration, and unauthorized remote-access channels.

Logging denied outbound traffic provides visibility into attempted policy violations and can identify systems requiring investigation. A well-designed policy should account for required services such as DNS, web access, mail relays, software updates, and approved remote access while blocking unnecessary traffic. BCP 38 discusses filtering traffic with incorrect source addresses, and NIST discusses firewall policy enforcement in RFC 2827 and NIST SP 800-41 Rev. 1.

QUESTION NO: 30

Rick works as the Security Manager for ABC Inc. He wants to continue the evaluation of rules according to the ordered list to identify matches even if a match is found.

Which of the following rulebases will he use to accomplish the task?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Backdoor rulebase

B. Nonterminal rulebase

C. Terminal rulebase

D. IDP rulebase

ANSWER: B D

Explanation:

A nonterminal rulebase is specifically designed to continue processing after a rule matches. Rules are evaluated in their configured sequence, but a match does not end the rulebase evaluation. This permits the device to identify and apply the effects of additional applicable rules, which is useful when multiple controls, such as logging, marking, or layered enforcement actions, must be accumulated for the same traffic.

An IDP rulebase also supports continued evaluation for matching traffic. Intrusion-detection and prevention processing commonly requires traffic to be assessed against multiple relevant signatures, attack objects, or policy criteria rather than treating one match as the sole result. Continuing evaluation enables the IDP engine to identify all applicable threats and apply the configured prevention and inspection behavior. This behavior aligns with the general distinction between terminal and nonterminal policy processing and with IDP policies that evaluate traffic against configured rules and attack definitions. Juniper's IDP policy documentation describes how IDP policies define inspection and actions for traffic: Juniper IDP Policies. For additional context on ordered security-policy evaluation, see Palo Alto Networks Security Policy Rule Evaluation.

QUESTION NO: 31

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN.

What steps can be used as a countermeasure of ARP spoofing?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Using smash guard utility.

B. Using ARP Guard utility.

C. Using static ARP entries on servers, workstation and routers.

D. Using ARP watch utility.

E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets.

ANSWER: B C D E

Explanation:

Using ARP Guard utility, using static ARP entries on servers, workstation and routers, using ARP watch utility, and using IDS Sensors to check continually for large amount of ARP traffic on local subnets are valid defenses or detective controls for ARP spoofing. ARP Guard-type tools can monitor ARP behavior and identify or block suspicious address-to-MAC association changes. Static ARP entries provide fixed, administrator-defined IP-to-MAC mappings for important systems, such as gateways and servers, preventing those hosts from relying on unsolicited dynamic ARP updates for the protected mappings. ARP watch utilities provide visibility by tracking observed ARP mappings and alerting administrators when a MAC address associated with an IP address changes unexpectedly. IDS sensors add network-wide detection by inspecting local-subnet traffic for anomalous ARP patterns, including excessive ARP replies, conflicting bindings, and ARP activity indicative of poisoning attempts. These measures can be combined with switch-based validation controls, such as Dynamic ARP Inspection, which validates ARP packets against trusted address-binding information. Cisco describes this validation approach in its Dynamic ARP Inspection documentation. ARP mapping-change monitoring is also documented in the arpwatch manual page.

QUESTION NO: 32

You work as a Network Administrator for a bank. For securing the bank's network, you configure a firewall and an IDS. In spite of these security measures, intruders are able to attack the network. After a close investigation, you find that your IDS is not configured properly and hence is unable to generate alarms when needed.

What type of response is the IDS giving?

A. False Negative

B. False Positive

C. True Positive

D. True Negative

ANSWER: A

Explanation:

False Negative is correct because an actual malicious intrusion is occurring, but the intrusion detection system fails to raise an alarm. In IDS terminology, the “positive” condition means the system identifies activity as malicious, while the real-world condition is that an attack is genuinely present. Since the IDS does not detect or alert on that real attack—here because it is improperly configured—the result is a false negative. False negatives are especially serious in a bank environment because they create undetected exposure: security personnel may have no prompt to investigate, contain, or remediate the intrusion while attackers continue operating in the network. Proper IDS deployment therefore requires tuning detection rules, validating sensor visibility and traffic coverage, maintaining signatures or analytics, and regularly testing alerting with representative attack activity. NIST describes intrusion-detection technologies and emphasizes the need for sound configuration, monitoring, and ongoing maintenance to produce useful detection results. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and the MITRE ATT&CK knowledge base for context on detecting adversary behaviors.