DUMPSARENA

GCIA – GIAC Certified Intrusion Analyst Practice Test

GIAC GCIA

Version Demo

Total Demo Questions: 50

Total Premium Questions: 505

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	170
Topic 2, Volume B	152
Topic 3, Volume C	124
Topic 4, Volume D	39
Total	505

QUESTION NO: 1

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

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

A. Event logs

B. Program logs

C. Web server logs

D. System logs

ANSWER: A B C D

Explanation:

Event logs, Program logs, Web server logs, and System logs should all be reviewed because each can provide relevant forensic artifacts for buffer-overflow exploitation or cookie-snooping activity. Event logs can establish a timeline of authentication activity, process creation, service failures, and security-relevant events. Program logs can record application exceptions, crashes, malformed input handling, and unexpected behavior that may coincide with an attempted or successful buffer overflow. System logs provide operating-system and service-level evidence such as kernel, daemon, application, and resource-error messages that help identify compromise symptoms and correlate them with other sources.

Web server logs are especially valuable when investigating cookie-related attacks because they may document suspicious HTTP requests, unusual session usage, anomalous client behavior, referrer or user-agent changes, and access to protected resources under a potentially hijacked session. They also support correlation with application and authentication events to determine the affected accounts, time window, source addresses, and requested resources. NIST incident-response guidance emphasizes collecting and correlating logs from hosts, applications, and network-facing services, while OWASP identifies web-server logging as an important source for detecting and investigating web attacks. See NIST SP 800-61 Rev. 2 and OWASP Logging Cheat Sheet.

QUESTION NO: 2

Peter works as a professional Computer Hacking Forensic Investigator for eLaw-Suit law firm. He is working on a case of a cyber crime. Peter knows that the good investigative report should not only communicate the relevant facts, but also present expert opinion. This report should not include the cases in which the expert acted as a lay witness. Which of the following type of witnesses is a lay witness?

A. One who can give a firsthand account of something seen, heard, or experienced.

B. One with special knowledge of the subject about which he or she is testifying.

C. One who observes an event.

D. One who is not qualified as an expert witness.

ANSWER: D

Explanation:

“One who is not qualified as an expert witness.” is the correct answer because a lay witness is a witness who does not testify under the specialized-expertise standard applicable to expert witnesses. Lay testimony is grounded in the witness’s own perceptions and personal knowledge, such as what the person saw, heard, did, or experienced during the relevant events. In a cybercrime matter, for example, a system user may testify about receiving a suspicious email or observing an unexpected account change without being qualified to offer technical forensic conclusions.

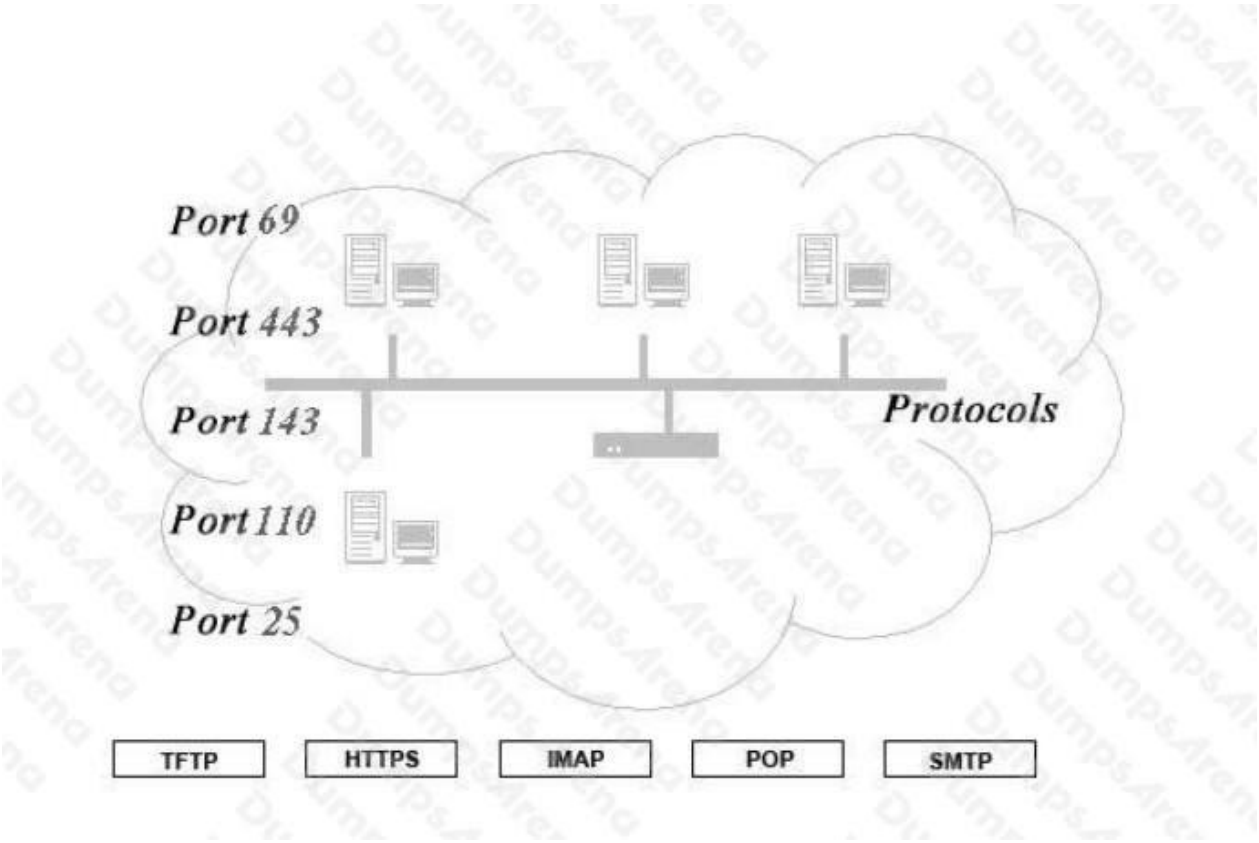
Under Federal Rule of Evidence 701, a non-expert witness may offer opinion testimony only when it is rationally based on that witness’s perception, helpful to understanding testimony or determining a fact, and not based on specialized knowledge within the scope of expert testimony. Expert testimony, by contrast, is governed by Rule 702 and requires specialized knowledge, skill, experience, training, or education, along with a reliable basis for the opinion. Thus, the defining distinction is

that a lay witness is not qualified and presented as an expert witness. See Federal Rule of Evidence 701 and Federal Rule of Evidence 702.

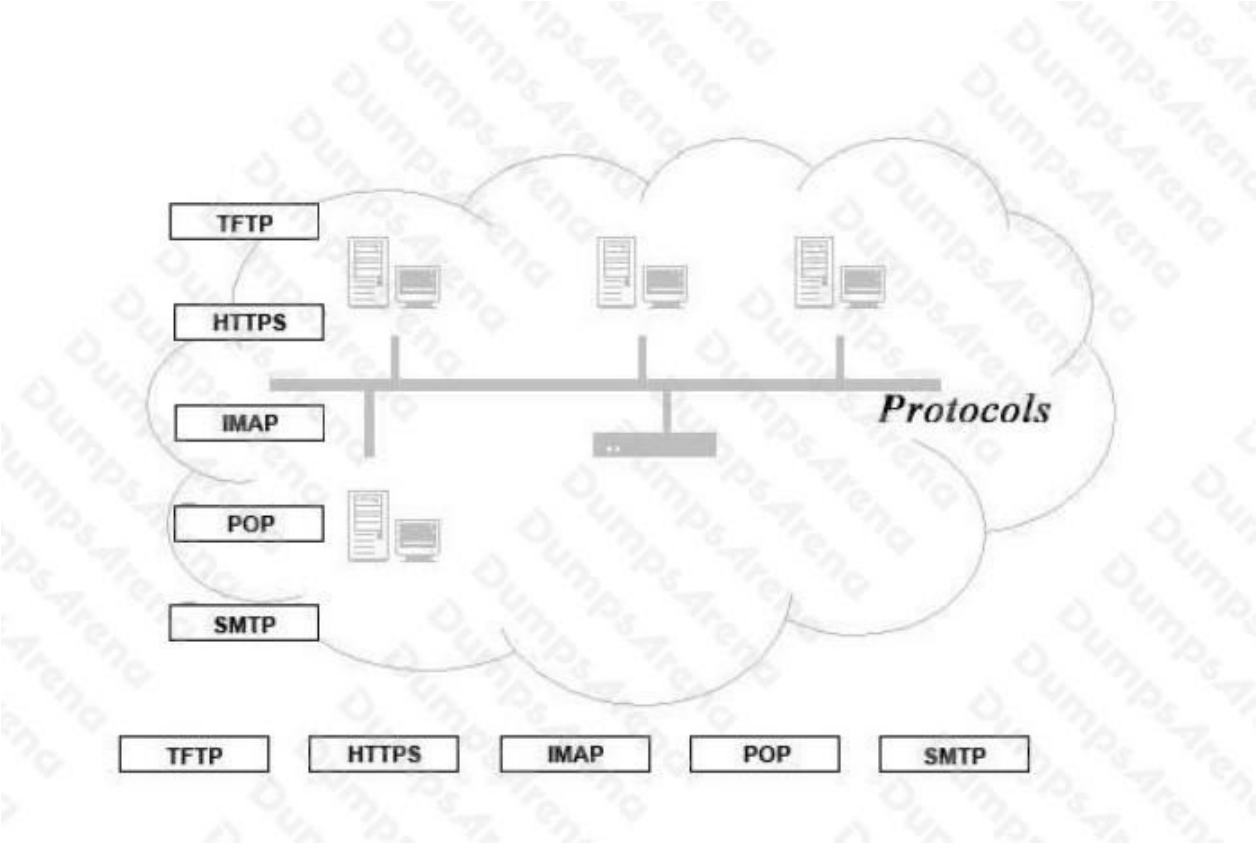
QUESTION NO: 3 - (DRAG DROP)

DRAG DROP Drag and drop the appropriate protocols to their respective port numbers they use by default.

Select and Place:



ANSWER:



Explanation:

The correct default-service mapping is TFTP with Port 69, HTTPS with Port 443, IMAP with Port 143, POP with Port 110, and SMTP with Port 25. These are the well-known service ports commonly used when analyzing network traffic, firewall rules, packet captures, and service scans. The Internet Assigned Numbers Authority maintains the authoritative Service Name and Transport Protocol Port Number Registry, including these assigned service-port relationships: IANA Service Name and Port Number Registry.

TFTP is a lightweight file-transfer service that conventionally listens on UDP port 69. HTTPS is HTTP protected by TLS and conventionally uses TCP port 443. For email access, IMAP conventionally uses TCP port 143, while POP conventionally uses TCP port 110. SMTP is the conventional protocol for relaying and submitting email between mail systems, using TCP port 25. The TFTP specification documents the port 69 service, and the SMTP specification describes SMTP's use of port 25. Recognizing these defaults lets an analyst quickly associate an observed destination port with the likely application protocol and assess whether the traffic is consistent with expected service behavior.

QUESTION NO: 4

Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information?

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

A. Slack space

B. Dumb space

C. Hidden partition

D. Unused Sectors

ANSWER: A C D

Explanation:

Slack space, hidden partition, and unused sectors are valid storage locations for information concealed through file-system steganography. Slack space is the residual area between the logical end of a file and the end of its allocated disk cluster; because normal file reads stop at the file's logical size, data placed there is not ordinarily displayed to users. A hidden partition can provide a separate disk area that is not exposed through ordinary operating-system views, allowing material to be stored apart from visible file-system content. Unused sectors, including unallocated disk space that is not currently assigned to active files, can likewise hold data without creating a conventional visible file entry. In practice, encryption is commonly used together with these locations so that discovery of the embedded bytes does not reveal their contents. Forensic examination must therefore account for allocated files, file slack, unallocated space, partition structures, and raw-sector data rather than relying only on directory listings. NIST's digital-forensics guidance describes collecting and examining file-system and media artifacts, including deleted and residual data: NIST SP 800-86. NIST also provides a practical overview of data recovery from storage media in its computer-forensics resource material: NIST Computer Forensics.

QUESTION NO: 5

Which of the following DOS commands is used to configure network protocols?

A. netsh

B. netsvc

C. netstat

D. ipconfig

ANSWER: A

Explanation:

`netsh` is the correct command because it is the Windows command-line scripting utility designed to display and modify the configuration of network interfaces, protocols, and related services. It provides separate command contexts for major networking components, allowing an administrator to configure settings such as IPv4 and IPv6 interface parameters, addresses, routes, DNS servers, WLAN profiles, firewall behavior, and IPsec policies. For example, the `netsh interface ipv4` context can be used to inspect or set IPv4 interface configuration, while other contexts manage wireless networking and advanced security-related networking features. This makes `netsh` appropriate when the task is to configure network protocol behavior rather than merely view current network information.

Although the question uses the historical term "DOS commands," `netsh` is a Windows command-line utility and remains relevant in modern Windows administration, especially for scripts, remote support procedures, and systems where graphical management tools are unavailable. Microsoft describes Netsh as a command-line tool for displaying or modifying the network configuration of a currently running computer. Its context-based structure is specifically intended to administer networking components and protocol settings. See the Microsoft Netsh overview and the Netsh command contexts documentation.

QUESTION NO: 6

Which of the following utilities is used to display the current TCP/IP configuration of a Windows NT computer?

A. NBTSTAT

B. IPCONFIG

C. CONFIG.SYS

D. FTP

ANSWER: B

Explanation:

IPCONFIG is the Windows command-line utility used to view a computer's current TCP/IP network configuration. When run without parameters, `ipconfig` displays the IP address, subnet mask, and default gateway configured for each applicable network adapter. This information is fundamental during network troubleshooting and intrusion analysis because it identifies the host's addressing, local network boundaries, and configured route to external networks. Additional switches provide more detailed information: for example, `ipconfig /all` displays adapter MAC addresses, DHCP status, DNS servers, lease details, and other configuration values; `ipconfig /displaydns` shows the local DNS resolver cache. The utility has been a standard TCP/IP diagnostic command in Windows environments, including Windows NT systems with TCP/IP installed. Microsoft documents that IPConfig displays all current TCP/IP network configuration values and can refresh DHCP and DNS-related settings. See the Microsoft IPConfig command reference and the Microsoft TCP/IP addressing overview.

QUESTION NO: 7

Fill in the blank with the appropriate facts regarding IP version 6 (*IPv6*).

IP addressing version 6 uses_____ -bit address. Its____ IP address assigned to a single host allows the host to send and receive data.

A. 128; unicast

ANSWER: A

Explanation:

The correct completion is **128; unicast**. IPv6 defines addresses as 128 bits long, providing a vastly larger address space than the 32-bit format used by IPv4. The 128-bit representation is normally written as eight groups of hexadecimal digits separated by colons, with established compression rules for consecutive zero-valued groups. This address length is a core property of the IPv6 Internet Protocol specification and is important when interpreting packet headers, logs, and network indicators during intrusion analysis.

A unicast IPv6 address identifies a single interface. Packets sent to that address are delivered to the identified interface, allowing the associated host to receive traffic directed specifically to it and to use that address as a source when sending traffic. IPv6 supports several address types, but unicast is the type used for one-to-one communication with a specific host or interface. The IPv6 base specification states that IPv6 addresses are 128 bits, while the IPv6 addressing architecture defines unicast addresses and their one-interface delivery behavior. See RFC 8200 and RFC 4291.

QUESTION NO: 9

Which of the following statements are true about routers?

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

A. Routers do not limit physical broadcast traffic.

B. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.

C. Routers act as protocol translators and bind dissimilar networks.

D. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.

ANSWER: B C D

Explanation:

Routers make forwarding decisions at the network layer. They examine a packet's destination network address, compare it to routing information, and select an appropriate next hop or outgoing interface. This path-selection role is fundamental to routing and allows routers to direct traffic across interconnected networks toward its intended destination. Routing decisions historically used classful address boundaries; modern routers more commonly use classless inter-domain routing prefixes, but the underlying concept remains that routers use the logical network portion of an address to determine where packets should be sent.

Routers also join networks that may use different data-link technologies. For example, a router can receive an internet protocol packet in an Ethernet frame and forward that packet through a different compatible encapsulation on another interface. In this sense, routers bind dissimilar network segments while forwarding network-layer traffic. A router separates broadcast domains as part of this inter-network function and applies routing-table knowledge to each packet's destination. RFC 1812 describes the requirements and forwarding behavior of internet protocol routers: RFC 1812. Cisco's overview of routing similarly explains that routers connect networks and choose paths for traffic: What Is a Router?.

QUESTION NO: 10

Which of the following algorithms produces a digital signature which is used to authenticate the bit-stream images?

A. MD6

B. MD5

C. BOINIC

D. HashClash

ANSWER: B

Explanation:

MD5 is the intended answer because it computes a fixed-length message digest for a bit-stream forensic image. At acquisition, the examiner calculates and records the MD5 digest of the original media and the acquired image. Recalculating the digest later and obtaining the same value provides evidence that the image bit stream has remained unchanged, supporting image authentication and integrity verification. In forensic terminology, this digest is often informally called a digital fingerprint or signature, although it is technically a cryptographic hash value rather than a public-key digital signature.

RFC 1321 defines MD5 as an algorithm that takes an arbitrary-length message and produces a 128-bit message digest, which is the property used for this comparison workflow. NIST's guidance for mobile-device forensics likewise describes calculating cryptographic hash values to verify that forensic copies have not changed. MD5 has known collision weaknesses and should not be relied on alone where adversarial collision resistance is required; modern practice commonly records a stronger hash such as SHA-256 as well. Nevertheless, MD5 is the recognized answer in the context of the question's traditional bit-stream-image authentication use case.

References: RFC 1321: The MD5 Message-Digest Algorithm; NIST SP 800-101 Rev. 1.

QUESTION NO: 11

Which of the following utilities can generate a local static route table? Each correct answer represents a complete solution. Choose two.

A. ROUTE

B. PING

C. NETSTAT

D. TRACERT

E. NBTSTAT

ANSWER: A C

Explanation:

ROUTE is a native Windows TCP/IP command-line utility for viewing and managing the local IP routing table. Its `print` function produces the current route-table output, while its `add` function creates routes; using the persistent-route parameter retains a static route across restarts. Thus, it can both establish and present locally configured static routing information.

Microsoft documents the command's route display, addition, deletion, and persistent-route capabilities in its ROUTE command reference.

NETSTAT can also generate a local routing-table listing. In Windows, the `-r` parameter displays the IP routing table, providing an analyst with a local view of active routes, including routes that have been statically configured. This is useful during intrusion analysis and host triage because it allows the examiner to identify the gateways, interfaces, and destination networks used by the system without sending network traffic. The command is documented in Microsoft's NETSTAT command reference, which specifies that `-r` displays the routing table. Together, these utilities provide the expected local route-table functionality: ROUTE manages and displays routes, and NETSTAT produces a routing-table report.

QUESTION NO: 12

Andrew works as an Administrator for a Windows 2000 based network. The network has a primary external DNS server, and a secondary DNS server located on the ISP's UNIX server, in order to provide fault tolerance. Users complain that they are unable to connect to the URL when using the secondary server. What should Andrew do to resolve the problem?

A. He should disable the fast zone transfer in the Advanced tab of the Properties window on the secondary server.

B. He should select the BIND secondaries check box in the Zone Transfer tab of the Properties window on the primary server.

C. He should select the BIND secondaries check box in the Advanced tab of the Properties window on the primary server.

D. He should enable the fast zone transfer in the Advanced tab of the Properties window on the primary server.

ANSWER: C

Explanation:

He should select the BIND secondaries check box in the Advanced tab of the Properties window on the primary server. The UNIX-hosted secondary is likely running a BIND implementation that does not support the Windows DNS fast zone-transfer format. A secondary DNS server can answer authoritatively only after it successfully receives and loads a current copy of the primary zone. Enabling BIND secondaries compatibility on the Windows 2000 primary causes the DNS server to use a zone-transfer behavior compatible with BIND secondary servers, allowing the UNIX server to obtain the zone data and serve the required URL records during normal operation or primary-server failure. This setting belongs on the Windows primary because it controls how that server sends zone data to secondary servers. Zone transfers are the mechanism by which a secondary obtains its authoritative zone copy; Microsoft's DNS documentation describes the primary-to-secondary transfer relationship and the importance of permitting compatible transfers. See Microsoft documentation on DNS zone transfers and Microsoft documentation on DNS zones.

QUESTION NO: 13

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

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

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

D. 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.

ANSWER: A C D

Explanation:

External threats originate outside the organization's trusted environment and involve actors or activity attempting to affect systems, services, networks, or data without authorized access. This includes Internet-based attacks directed at publicly reachable infrastructure or attempts to enter an internal environment through exposed services, credentials, or other access paths. Network flooding through exceptionally large volumes of requests is also an external threat scenario: denial-of-service and distributed denial-of-service activity is commonly launched from external systems and aims to exhaust bandwidth, connections, processing capacity, or application resources so legitimate users cannot obtain service. Perimeter security controls are an important defensive layer for managing this exposure. Firewalls and related boundary protections enforce rules on inbound and outbound traffic, reduce unnecessary Internet exposure, and limit access to permitted services and users. NIST describes firewalls as devices or programs that control traffic between networks or hosts with differing security postures, while CISA provides specific guidance for preparing for and responding to DDoS attacks. These controls should be combined with monitoring, rate limiting, resilient architecture, and incident-response processes for effective protection. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and CISA DDoS Protection Resources.

QUESTION NO: 14

Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet.

Which of the following security threats may occur if DMZ protocol attacks are performed? Each correct answer represents a complete solution. Choose all that apply.

A. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.

B. Attacker can gain access to the Web server in a DMZ and exploit the database.

C. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.

D. Attacker can exploit any protocol used to go into the internal network or intranet of the com pany

ANSWER: A B D

Explanation:

A DMZ is a segmented network zone intended to expose selected public-facing services while limiting direct reachability to internal systems. An attacker who compromises a Web server in the DMZ may be able to exploit a database when the application's permitted database connection, credentials, trust relationship, or an exposed administrative path provides a route to that backend resource. This illustrates why public-facing application components and internal data services must be tightly separated and access-controlled.

DMZ protection can also be bypassed by a zero-day payload when the payload exploits a previously unknown vulnerability or otherwise lacks a detection signature or prevention rule. Defense-in-depth controls reduce exposure but do not guarantee detection of unknown attacks. In addition, every protocol explicitly permitted from the DMZ toward internal systems creates a potential attack path. If an attacker compromises a DMZ host, they can attempt to misuse, tunnel over, or exploit vulnerabilities in those allowed services to pivot toward the intranet. NIST describes DMZ architectures as a means of separating publicly accessible services from protected networks and stresses controlling traffic between network zones. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and CISA's overview of zero-day vulnerabilities.

QUESTION NO: 15

Peter 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. Peter 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. Names of the victims

B. Date and time of incident

C. Nature of harassment

D. Location of each incident

ANSWER: A B C D

Explanation:

Complete incident documentation should capture the names of the victims, the date and time of incident, the nature of harassment, and the location of each incident. Together, these facts create a reliable contemporaneous record that allows an employer or investigator to identify the people involved, establish a timeline, understand the conduct being reported, locate relevant physical or digital evidence, and identify potential witnesses. Describing the nature of harassment is particularly important because a record must preserve what was said, done, displayed, transmitted, or otherwise experienced; a date and location alone do not document the alleged conduct. Maintaining this information also supports a prompt, thorough, and impartial response, while preserving details that may become less clear over time. The U.S. Equal Employment Opportunity Commission explains that employers should take steps to prevent and correct harassment and that complaints should be addressed appropriately. Its guidance recognizes the importance of effective complaint processes and investigations. See the EEOC harassment resources and the EEOC Enforcement Guidance on Harassment in the Workplace.

QUESTION NO: 16

Which of the following password cracking attacks is based on a pre-calculated hash table to retrieve plain text passwords?

A. Brute Force attack

B. Hybrid attack

C. Dictionary attack

D. Rainbow attack

ANSWER: D

Explanation:

Rainbow attack is correct because it uses rainbow tables: precomputed data structures that trade storage and advance computation for faster recovery of candidate plaintext passwords from password hashes. Rather than calculating every possible password hash only after obtaining a target hash, an attacker creates chains of hash and reduction operations ahead of time. The table stores selected chain endpoints, allowing the attacker to determine whether a target hash may occur in a chain and then regenerate that chain to identify the corresponding plaintext candidate. This substantially reduces online or post-compromise cracking time for unsalted, fast password hashes, although it requires considerable preparation and storage. Unique, randomly generated salts make precomputed tables far less useful because the same password produces a different hash for each salt value; modern password storage should also use deliberately slow, adaptive password-hashing functions. NIST specifically recommends salted password hashing with an approved password-hashing scheme, and OWASP describes salts as a defense against precomputed hash attacks such as rainbow tables. See NIST SP 800-63B and the OWASP Password Storage Cheat Sheet.

QUESTION NO: 17

What are the limitations of the POP3 protocol?

Each correct answer represents a complete solution. Choose three.

A. E-mails can be retrieved only from the Inbox folder of a mailbox. E-mails stored in any other folder are not accessible.

B. It is only a retrieval protocol. It is designed to work with other applications that provide the ability to send e-mails.

C. It does not support retrieval of encrypted e-mails.

D. It uses less memory space.

ANSWER: A B

Explanation:

POP3 is intentionally a simple mailbox-access protocol. Its standard transaction model exposes a single server-side maildrop: after authentication, a client lists, retrieves, and optionally deletes messages from that maildrop. It has no standardized commands for browsing or selecting arbitrary mailbox folders, so a POP3 client generally accesses only the mailbox's Inbox-equivalent maildrop rather than mail saved in other server-side folders. This limited server-side mailbox model is one reason IMAP is preferred when users need folder access and synchronized mail across devices.

POP3 also provides retrieval functions only. Its defined operations cover authentication, message status, listing, retrieval, deletion marking, and session updates; sending mail is outside the protocol's scope. A mail client therefore uses SMTP or another submission service to send messages. These protocol boundaries are documented in RFC 1939. POP3 can retrieve encrypted message content because it transfers message data as message octets, and POP3 sessions can also be protected with TLS; secure email transport guidance is described in RFC 8314.

QUESTION NO: 18

Which of the following are open-source vulnerability scanners?

A. Nessus

B. NetRecon

C. Hackbot

D. Nikto

ANSWER: A C D

Explanation:

In the historical GIAC/SANS context in which this question is commonly used, **Nessus**, **Hackbot**, and **Nikto** are open-source vulnerability-scanning tools. Nessus was originally distributed as an open-source scanner (notably the Nessus 2.x line), with a plugin-based design that allowed the community to inspect and extend vulnerability checks. Consequently, it is included in legacy security-training material as an open-source scanner, even though later Nessus releases are distributed under Tenable's proprietary licensing model. Hackbot is likewise categorized in legacy security-tool references as an open-source vulnerability-assessment scanner. Nikto remains a well-known open-source web-server scanner. It performs tests for potentially dangerous files, outdated server software, insecure configurations, and other common web-server exposures; its source and signatures are publicly maintained. Open-source scanners are especially useful to analysts because their checks, signatures, and implementation can be reviewed and adapted to the organization's assessment requirements. The current Nikto project and source code are available through the Nikto GitHub repository. Tenable's Nessus product history and available releases can be reviewed at the Tenable Nessus product page.

QUESTION NO: 19

Which of the following UDP ports are used by the Simple Network Management Protocol (SNMP)? Each correct answer represents a complete solution. Choose two.

A. UDP port 69

B. UDP port 161

C. UDP port 137

D. UDP port 162

ANSWER: B D

Explanation:

SNMP conventionally uses UDP port 161 for communication between an SNMP manager and an SNMP agent. The manager sends requests, such as GET, GETNEXT, GETBULK, and SET messages, to the agent's UDP port 161; the agent normally returns its response to the manager's originating UDP source port. This traffic is central to polling and administering monitored network devices, servers, and other managed systems.

UDP port 162 is used for SNMP notifications, specifically unsolicited traps and inform messages sent by an SNMP agent to a receiving management station or notification receiver. Traps are sent without acknowledgement, whereas SNMP informs are acknowledged, but both are conventionally delivered to UDP port 162. During network monitoring or intrusion analysis, traffic on these ports can identify SNMP management activity and may merit review for exposed community strings, unauthorized management requests, or anomalous notifications. The Internet Assigned Numbers Authority lists snmp as UDP port 161 and snmptrap as UDP port 162. RFC 3417 also specifies the transport mapping used by SNMP, including these well-known UDP ports: RFC 3417.

QUESTION NO: 20

Which of the following types of firewall ensures that the packets are part of the established session?

A. Switch-level firewall

B. Application-level firewall

C. Stateful inspection firewall

D. Circuit-level firewall

ANSWER: C

Explanation:

Stateful inspection firewall is correct because it maintains a state table containing details of active network connections, such as source and destination IP addresses, ports, protocol information, and TCP connection state. When a packet arrives, the firewall does not evaluate it solely as an isolated packet; it compares the packet against the state table to determine whether it belongs to a legitimate, established session. For example, a return packet for an outbound TCP connection can be accepted when its flow matches an entry created for that connection, without requiring a separate broad inbound rule. This connection-aware filtering is the defining characteristic of stateful inspection and makes it useful for enforcing policies that permit valid responses while limiting unsolicited traffic. TCP state tracking commonly recognizes stages such as connection establishment, established communication, and teardown, although modern stateful firewalls can track connection state for other protocols as well. NIST describes stateful inspection firewalls as examining packet headers and maintaining information about the state of network connections, while the Cisco security configuration guidance documents the use of established-session matching in stateful firewall policy. See NIST SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy and Cisco IOS XE Firewall Policy Configuration Guide.

QUESTION NO: 21

Which of the following components are usually found in an Intrusion detection system (IDS)? Each correct answer represents a complete solution. Choose two.

A. Sensor

B. Gateway

C. Firewall

D. Modem

E. Console

ANSWER: A E

Explanation:

An IDS is commonly organized around sensors and a console (or central management/analysis console). A **Sensor** observes activity at a monitored location, such as a network segment or host, collects relevant events or traffic, and produces alerts or event data when it identifies potentially malicious or policy-relevant behavior. Network IDS sensors are placed at strategic visibility points so analysts can inspect traffic entering, leaving, or traversing a network.

A **Console** provides the centralized interface for receiving and reviewing sensor output. It supports alert triage, investigation, correlation, configuration, reporting, and response workflows. In distributed IDS deployments, sensors may operate remotely while the console gives security personnel a consolidated operational view. This division between collection/detection sensors and centralized management or analysis is a standard IDS architecture concept. NIST describes intrusion-detection technologies as monitoring and analyzing events for signs of incidents, while network-based technologies monitor network traffic at selected points. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems and the CISA overview of intrusion detection and prevention systems.

QUESTION NO: 22

What is the size of a subnet in IPv6?

A. 2^{64} addresses

B. 2^{32} addresses

C. 2^{62} addresses

D. 2^{128} addresses

ANSWER: A

Explanation:

The correct answer is **2^{64} addresses**. In normal IPv6 LAN design, a subnet uses a /64 prefix: the first 64 bits identify the network prefix and the remaining 64 bits form the interface identifier portion of the address. Because 64 bits remain available for addressing interfaces, the subnet contains 2^{64} possible IPv6 addresses (18,446,744,073,709,551,616). This convention is fundamental to IPv6 operations, including Stateless Address Autoconfiguration (SLAAC), which expects a 64-bit interface identifier on prefixes used for address autoconfiguration. The IPv6 addressing architecture describes addresses as a prefix plus an interface identifier, and the /64 boundary is the standard subnet size for ordinary IPv6 networks. Although IPv6 routing and point-to-point designs can use different prefix lengths in specialized circumstances, certification questions asking for the size of an IPv6 subnet conventionally refer to the standard /64 subnet. See RFC 4291, IP Version 6 Addressing Architecture and RFC 7421, Analysis of the 64-bit Boundary in IPv6 Addressing.

QUESTION NO: 23

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

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

A. Dig

B. Host

C. NSLookup

D. DSniff

ANSWER: A B C

Explanation:

`Dig`, `Host`, and `NSLookup` can each request a DNS zone transfer when querying an authoritative server that permits transfers for the requested zone. A full zone transfer is normally requested using the AXFR query type over TCP port 53. For example, `dig @authoritative-server example.com AXFR` explicitly submits an AXFR request. The `host` utility supports this activity through its zone-listing capability, such as `host -l example.com authoritative-server`, which requests the zone data. Microsoft's `nslookup` also supports zone listing in its interactive mode, including use of the `ls` command against an authoritative server. These tools are useful during authorized DNS assessment because a successful AXFR response may disclose hostnames, service records, addressing information, and other naming details that help establish an inventory of exposed systems. Whether the transfer succeeds is determined by the DNS server's zone-transfer access-control configuration; properly administered authoritative servers restrict AXFR/IXFR requests to approved secondary DNS servers. See the BIND 9 manual pages for `dig` and `host` documentation, and Microsoft's nslookup documentation for the Windows utility.

QUESTION NO: 24

Host-based IDS (HIDS) is an Intrusion Detection System that runs on the system to be monitored. HIDS monitors only the data that it is directed to, or originates from the system on which HIDS is installed. Besides monitoring network traffic for detecting attacks, it can also monitor other parameters of the system such as running processes, file system access and integrity, and user logins for identifying malicious activities. Which of the following tools are examples of HIDS? Each correct answer represents a complete solution. Choose all that apply.

A. HPing

B. BlackIce Defender

C. Tripwire

D. Legion

ANSWER: B C

Explanation:

BlackIce Defender and Tripwire are examples of host-based intrusion detection capabilities because they operate on, and collect security-relevant information from, the protected endpoint. BlackIce Defender was a host-resident personal firewall and intrusion-detection product. Its endpoint location allows it to inspect traffic involving the local host and identify suspicious activity directed at that system. This is consistent with the HIDS model, in which detection data is gathered from an individual machine rather than solely from a network sensor.

Tripwire is a classic host-based file-integrity monitoring solution. It establishes a trusted baseline for selected files and directories, then detects and reports changes to monitored objects. Unauthorized or unexpected changes to operating-system files, application binaries, configurations, or other critical data can indicate compromise, persistence, or policy violations. File-integrity monitoring is specifically valuable to intrusion analysts because it provides evidence of changes occurring on the endpoint, including changes that network-only monitoring may not observe. Tripwire's documented integrity-monitoring approach is described at Tripwire File Integrity Manager. More generally, NIST identifies file-integrity checking as an important host-based detection capability in NIST SP 800-94.

QUESTION NO: 25

You work as a Network Administrator in a company. The NIDS is implemented on the network. You want to monitor network traffic. Which of the following modes will you configure on the network interface card to accomplish the task?

A. Promiscuous

B. Audit mode

C. Full Duplex

D. Half duplex

ANSWER: A

Explanation:

Promiscuous mode is the appropriate NIC configuration for a network intrusion detection system that must inspect network traffic. Under ordinary operation, a network interface processes frames addressed to its own MAC address, broadcast frames, and applicable multicast frames. When placed in promiscuous mode, the interface passes all frames it receives to the operating system for analysis, including frames addressed to other hosts. This enables a NIDS sensor connected to a network tap or a properly configured switch mirror/SPAN port to capture and inspect packets traversing the monitored network segment.

Promiscuous mode is therefore a fundamental capture setting for packet-analysis and intrusion-detection tools such as tcpdump, Wireshark, and NIDS sensors. It does not itself grant visibility into every packet on a switched network: the sensor must also receive a copy of the desired traffic through suitable network infrastructure configuration. Once the traffic reaches the sensor interface, promiscuous mode ensures the operating system and NIDS can examine frames regardless of their destination MAC address. For further background, see the Wireshark User's Guide: Capture Options and the pcap manual documentation.

QUESTION NO: 26

Adam works as a professional Computer Hacking Forensic Investigator, a project has been assigned to him to investigate and examine files present on suspect's computer. Adam uses a tool with the help of which he can examine recovered deleted files, fragmented files, and other corrupted data. He can also examine the data, which was captured from the network, and access the physical RAM, and any processes running in virtual memory with the help of this tool. Which of the following tools is Adam using?

A. Vedit

B. WinHex

C. HxD

D. Evidor

ANSWER: B

Explanation:

WinHex is correct because it is a forensic-capable hexadecimal editor and disk editor designed to inspect data at a low level, including data that conventional file-system views may not expose. Its forensic functionality supports examining storage media and files regardless of whether data is deleted, damaged, fragmented, or otherwise difficult to interpret through ordinary applications. This is particularly valuable during an investigation because the examiner can inspect raw sectors, file-system structures, and file contents directly, preserving visibility into artifacts that may not have a normal filename or directory entry.

WinHex also provides memory-analysis capabilities. X-Ways describes WinHex as offering RAM editing and support for examining memory-related data, which aligns with the scenario's reference to physical RAM and processes represented in virtual memory. Its ability to inspect binary data makes it suitable for analyzing captured network data as well, since packet captures and other network artifacts can be reviewed at the byte level when needed. These capabilities make WinHex an appropriate all-purpose forensic examination tool for the described combination of deleted-file recovery, fragmented-data analysis, network-capture review, and memory examination. See the WinHex product overview and the WinHex manual.

QUESTION NO: 27

Which of the following statements is true about ICMP packets?

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

A. The PING utility uses them to verify connectivity between two hosts.

B. They guarantee the delivery of datagrams.

C. They are encapsulated within IP datagrams.

D. They use UDP datagrams.

E. They are used to report errors if a problem in IP processing occurs.

ANSWER: A C E

Explanation:

"The PING utility uses them to verify connectivity between two hosts." is correct because ping sends ICMP Echo Request messages and evaluates the corresponding Echo Replies. This provides a practical indication that a remote system can be reached and is responding at the network layer; the replies can also provide round-trip timing and packet-loss information.

"They are encapsulated within IP datagrams." is correct because ICMP is a network-layer control protocol carried directly by IP. An IP packet identifies ICMP through the IP Protocol field value of 1, after which the ICMP message contains its type, code, checksum, and message-specific fields. ICMP is therefore part of normal IP operation and diagnostics rather than an application-layer service.

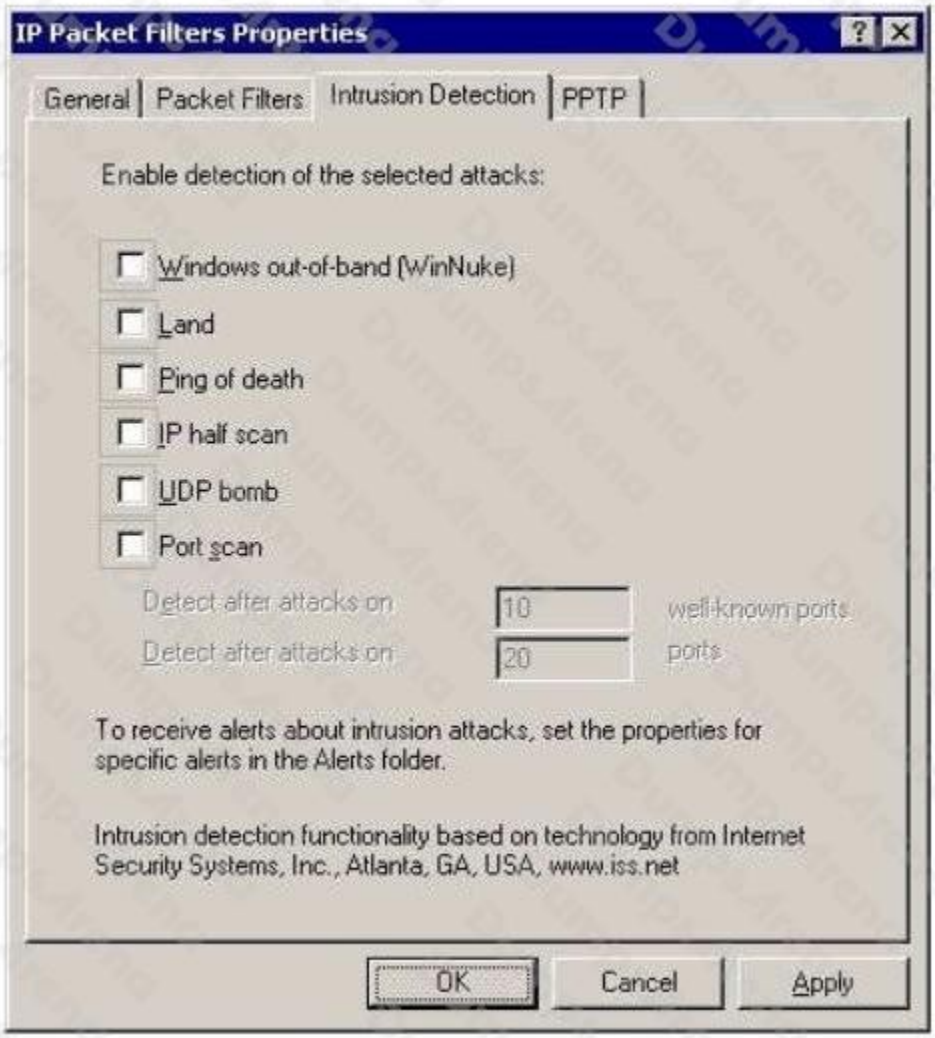
"They are used to report errors if a problem in IP processing occurs." is correct because ICMP defines error-reporting messages that communicate conditions encountered while forwarding or processing IP traffic. Examples include Destination Unreachable, Time Exceeded, and Parameter Problem messages. These messages give a sender or diagnostic tool useful feedback about an IP-delivery or routing condition. The foundational ICMP message format and error-reporting purpose are specified in RFC 792; modern IPv4 router behavior and ICMP error-generation requirements are detailed in RFC 1812.

QUESTION NO: 28 - (HOTSPOT)

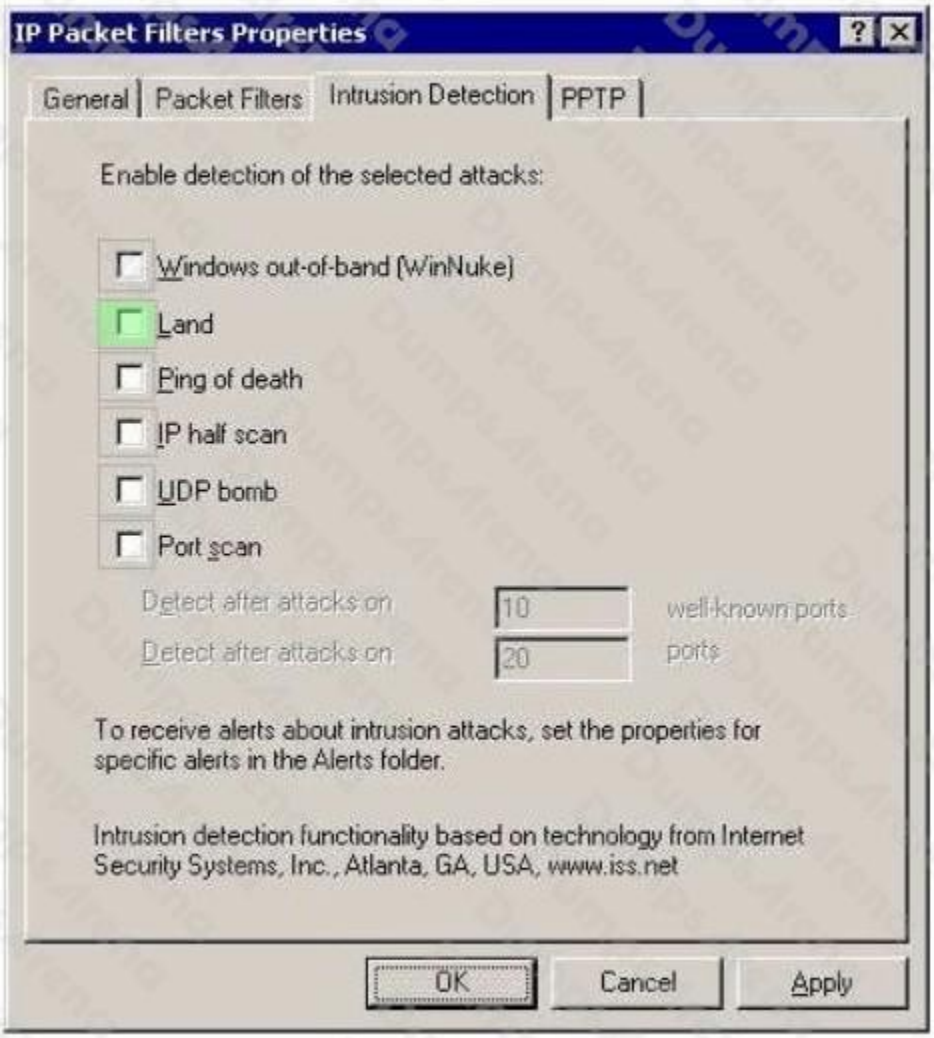
HOTSPOT

You work as a Network Administrator for McRobert Inc. The company's Windows 2000-based network is configured with Internet Security and Acceleration (ISA) Server 2000. You are configuring intrusion detection on the server. You want to get notified when a TCP SYN packet is sent with a spoofed source IP address and port number that match the destination IP address and port number. Mark the alert that you will enable on the Intrusion Detection tab page of the IP Packet Filters Properties dialog box to accomplish the task.

Hot Area:


IP Packet Filters Properties
General
Packet Filters
Intrusion Detection
PPTP
Enable detection of the selected attacks:
Windows out-of-band (WinNuke)
Land
Ping of death
IP half scan
UDP bomb
Port scan
Detect after attacks on
10
well-known ports
Detect after attacks on
20
ports
To receive alerts about intrusion attacks, set the properties for specific alerts in the Alerts folder.
Intrusion detection functionality based on technology from Internet Security Systems, Inc., Atlanta, GA, USA, www.iss.net
OK
Cancel
Apply

ANSWER:



Explanation:

The correct alert to enable is **Land**. A LAND attack uses a deliberately forged TCP SYN packet in which the source address and source port are set to the same values as the packet's destination address and destination port. In practical terms, the attacker constructs a connection request that appears to originate from, and be sent back to, the target host itself. This is the precise signature described in the question: a TCP SYN packet with spoofed source IP and port values matching its destination IP and port values.

ISA Server 2000's intrusion-detection settings include a dedicated LAND detection control because this malformed packet pattern is distinctive and can be recognized at the packet-filtering layer. Enabling the Land alert causes the server's intrusion-detection functionality to identify and generate an alert for traffic matching that source-equals-destination TCP SYN condition. This lets the administrator be notified of attempted LAND attacks and investigate the event through ISA alerting and logging facilities.

LAND is a classic denial-of-service technique, historically associated with vulnerable TCP/IP implementations that could mishandle a connection request addressed back to the originating endpoint. The defining characteristic remains the same regardless of the affected platform: matching source and destination IP addresses, together with matching source and destination TCP ports, on an initial SYN segment. For background on the attack pattern, see the MITRE ATT&CK Network Denial of Service technique and the CISA Alerts and Advisories page for defensive incident-monitoring guidance.

QUESTION NO: 29

Which of the following ports is used by Layer 2 Tunneling Protocol (L2TP)?

A. UDP port 1701

B. UDP port 67

C. TCP port 23

D. TCP port 25

ANSWER: A

Explanation:

UDP port 1701 is the well-known port assigned to the Layer 2 Tunneling Protocol (L2TP). L2TP is used to create tunnels that carry Layer 2 frames across an IP network, commonly as part of remote-access VPN deployments. RFC 2661 specifies that an L2TP control connection uses UDP destination port 1701; this port is also used for L2TP data messages once the tunnel/session is established. In a common L2TP/IPsec implementation, IPsec first protects the L2TP traffic, but the encapsulated L2TP protocol itself remains associated with UDP 1701. For traffic analysis, recognizing UDP 1701 helps identify L2TP negotiation and tunneling activity, while also accounting for the IPsec encapsulation that may protect the traffic in transit. The Internet Assigned Numbers Authority registers 1701/UDP under the service name *l2tp*, confirming its standardized assignment. See RFC 2661: Layer Two Tunneling Protocol "L2TP" and the IANA Service Name and Transport Protocol Port Number Registry.

QUESTION NO: 30

Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?

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

A. portsentry

B. libnids

C. nmap

D. scanlogd

ANSWER: A B D

Explanation:

portsentry, **libnids**, and **scanlogd** can be used in identifying stealth-oriented port-scanning activity. PortSentry is a host-based intrusion-detection utility designed to watch configured ports and react when connection attempts or probe activity indicate a scan. It supports detection modes that help identify reconnaissance before an attacker establishes a normal application session.

scanlogd is specifically intended to identify port-scan patterns from packet traffic, including scans designed to avoid the obvious connection patterns produced by conventional TCP connection attempts. Its analysis of TCP flags, source addresses, and probing behavior makes it useful for recognizing stealth scan activity in packet logs or live network monitoring.

libnids provides packet-capture and network-intrusion-detection building blocks, including IP defragmentation and TCP stream reassembly. These capabilities enable an intrusion-detection application built with the library to inspect otherwise evasive traffic patterns and implement scan-detection logic. This makes it suitable for use in a detection solution rather than merely generating scan traffic. See the SANS research library for intrusion-detection context and the PortSentry manual page for operational details.

QUESTION NO: 31

You are the Administrator for a Windows 2000 based network that uses DHCP to dynamically assign IP addresses to the clients and DNS servers. You want to ensure that the DNS servers can communicate with another DNS server. Which type of query will you run to achieve this?

A. PATHPING

B. NSLOOKUP

C. PING

D. Recursive

E. Iterative

ANSWER: E

Explanation:

Iterative is correct because it describes the query process used when a DNS server must obtain information from other DNS servers to resolve a name. In an iterative resolution, the querying DNS server contacts another DNS server—such as a root, top-level-domain, or authoritative server—and receives either the requested resource record or a referral identifying the next DNS server to contact. The querying server then continues the lookup by contacting the referred server as needed. This server-to-server referral process allows DNS infrastructure to locate authoritative information across the DNS namespace while maintaining a clear chain of delegation.

In a Windows DNS environment, a DNS server commonly performs iterative queries when it does not already have the answer in its zones or cache and must resolve a name through the hierarchy. This behavior is fundamental to normal DNS name resolution between DNS servers and is the appropriate query type for validating that one DNS server can obtain DNS information from another. Microsoft's DNS overview describes how DNS servers query other servers in the namespace: DNS overview. Additional technical detail on recursive resolvers and iterative lookups is available from Cloudflare's DNS server types guide.

QUESTION NO: 32

Which of the following is designed to protect the Internet resolvers (clients) from forged DNS data that are created by the DNS cache poisoning?

A. Split-horizon DNS

B. Stub resolver

C. Domain Name System Extension (DNSSEC)

D. BINDER

ANSWER: C

Explanation:

Domain Name System Extension (DNSSEC) is correct because it adds cryptographic origin authentication and data-integrity protection to DNS responses. DNSSEC enables a validating resolver to verify a chain of trust from a configured trust anchor, generally the DNS root, through signed delegations to the requested zone. DNS records are digitally signed, and the resolver validates those signatures using the corresponding DNSKEY records and DS records published in the DNS hierarchy. If an attacker attempts to inject forged resource records into a recursive resolver's cache, a validating resolver will reject the data when the signatures cannot be validated or the authenticated denial-of-existence information does not verify.

This protection directly addresses the core cache-poisoning problem: ordinary DNS historically provides no built-in way for a resolver to prove that a received answer genuinely originated from the authoritative zone and was not altered in transit. DNSSEC does not encrypt DNS queries or responses; rather, it provides authenticated DNS data so clients using a validating recursive resolver can receive trustworthy answers. RFC 4033 defines DNSSEC's security goals and explains that it protects resolvers from accepting forged DNS data. See RFC 4033: DNS Security Introduction and Requirements and the ICANN DNSSEC overview.

QUESTION NO: 33

Nathan works as a Computer Hacking Forensic Investigator for SecureEnet Inc. He uses Visual TimeAnalyzer software to track all computer usage by logging into individual users account or specific projects and compile detailed accounts of time spent within each program. Which of the following functions are NOT performed by Visual TimeAnalyzer?

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

A. It monitors all user data such as passwords and personal documents.

B. It gives parents control over their children's use of the personal computer.

C. It tracks work time, pauses, projects, costs, software, and internet usage.

D. It records specific keystrokes and run screen captures as a background process.

ANSWER: A D

Explanation:

Visual TimeAnalyzer is intended for activity and time analysis: it associates computer use with applications, projects, work periods, breaks, software use, and internet use so that the collected activity can be reviewed as time-accounting information. Its core purpose is therefore to create usage and productivity records rather than to collect the contents of everything a user types or stores. “It monitors all user data such as passwords and personal documents.” is not a Visual TimeAnalyzer function. Capturing passwords is particularly sensitive credential collection and is associated with input-capture/keylogging behavior, not ordinary application-usage time tracking. Likewise, “It records specific keystrokes and run screen captures as a background process.” describes surveillance capabilities outside the product’s time-analysis role. Keystroke logging and screen capture are distinct collection techniques that can be used by malicious software or specialized monitoring products; they should not be inferred merely because a program reports time spent in applications or on projects. MITRE documents input capture, including keylogging, as a separate technique in Input Capture: Keylogging, and identifies screen capture separately at Screen Capture. The correct selections are therefore the statements concerning monitoring passwords/personal documents and recording keystrokes/screen captures.

QUESTION NO: 35 - (SIMULATION)

Fill in the blank with the appropriate term.

_____is the practice of monitoring and potentially restricting the flow of information outbound from one network to another

ANSWER: See the explanation for the answer

Explanation:

Answer: Egress filtering

Egress filtering is the practice of monitoring and potentially restricting outbound traffic or information as it flows from one network to another. It is commonly used to limit unauthorized data exfiltration and to prevent internal hosts from sending unwanted or spoofed traffic externally.

QUESTION NO: 36

Which of the following organizations is dedicated to computer security research and information sharing?

A. FBI

B. NIPC

C. Honeynet Project

D. IEEE

ANSWER: C

Explanation:

The **Honeynet Project** is the correct answer because it is an international, nonprofit security-research organization specifically established to improve the security community's understanding of threats through research, shared tools, published analysis, and education. Its work centers on honeypots and related defensive technologies: controlled systems and services designed to observe malicious activity safely and generate useful intelligence about attacker techniques, malware, and intrusion behavior. This directly supports both elements in the question: conducting computer-security research and disseminating the resulting knowledge to defenders, researchers, incident responders, and the broader public.

The project publishes research material, maintains open-source security tools, and encourages collaboration among contributors in many countries. Such sharing helps analysts recognize current attack patterns, develop detection content, and improve incident-handling practices. The organization describes its mission as researching the latest attacks and developing open-source security tools to improve Internet security. Its public reports and technical resources make its findings available for practical defensive use rather than limiting them to a closed membership or a single government function. See the Honeynet Project and its About page for its mission, research focus, and community-oriented work.

QUESTION NO: 37

Which of the following proxy servers can be used for spamming?

A. Caching proxy server

B. Web proxy server

C. Open proxy server

D. Anonymizing proxy server

ANSWER: C

Explanation:

An **Open proxy server** is correct because it accepts proxy requests from arbitrary, untrusted Internet users rather than restricting access to authorized clients. An attacker can route traffic through such a service to conceal the traffic's actual source address and shift abuse reports toward the proxy operator. This makes an exposed proxy attractive for spam campaigns, including sending unsolicited messages through services reachable via the proxy or using it as an intermediary in a broader spam-delivery infrastructure. In intrusion analysis, open proxies are significant indicators of compromised or poorly administered systems because they can be discovered and abused remotely at scale.

The security issue is the absence of effective access controls: a proxy should require authentication, restrict permitted source networks, and limit permitted destinations and connection methods. HTTP proxy behavior includes support for forwarding requests and, where enabled, establishing tunnels using the CONNECT method; these capabilities must be carefully controlled to prevent misuse. RFC 9110 documents the CONNECT tunneling mechanism at RFC 9110, Section 9.3.6. NIST also recommends restricting proxy access and configuring boundary protections to enforce organizational policy in SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 38

Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?

Each correct answer represents a part of the solution. Choose all that apply.

A. Text Semagrams

B. Linguistic steganography

C. Technical steganography

D. Perceptual masking

ANSWER: A B

Explanation:

Text Semagrams and **Linguistic steganography** correctly describe the suspected method. Steganography conceals the existence of a message by embedding it in apparently ordinary material rather than merely encrypting its contents. In text-based steganography, a semagram conveys hidden information through nonlinguistic or visual properties, such as symbols, typography, spacing, formatting, graphical marks, or other visible signs within a document. The presence of unusual special symbols, graphics, and signs in files that otherwise appear to be text is therefore consistent with text semagrams carrying concealed data.

Linguistic steganography is the broader category encompassing techniques that hide messages in text or language-related representations. It can use wording, syntax, formatting, character choices, and visual text features to encode a covert message while preserving an innocent-looking cover document. Text semagrams fit within this broader text/linguistic steganography classification because their hidden signal is represented through the form and presentation of textual material. A forensic investigator should preserve the original files and examine character encoding, fonts, whitespace, document metadata, and rendering differences to identify the covert channel. For background on the purpose and use of steganography, see Encyclopaedia Britannica: Steganography and NCSC: Data security.

QUESTION NO: 39

Which of the following OSI layers is responsible for protocol conversion, data encryption/ decryption, and data compression?

A. Network layer

B. Data-link layer

C. Presentation layer

D. Transport layer

ANSWER: C

Explanation:

The correct answer is **Presentation layer**. Layer 6 of the OSI model is responsible for ensuring that data exchanged by applications is represented in a form the receiving system can interpret. This includes translation or protocol conversion between differing data formats and character encodings, such as converting text represented in one encoding into a mutually understandable representation. The presentation layer also provides transformation services that reduce or protect the data before it is delivered to the application-facing layer. Compression reduces the number of bits that must be transmitted or stored, while encryption converts readable plaintext into protected ciphertext; decryption restores that ciphertext to usable plaintext for an authorized recipient. These functions support interoperability and secure, efficient data exchange without requiring every application to implement its own incompatible representation handling. In practical TCP/IP networking, OSI presentation-layer functions are often implemented within application protocols, libraries, or software rather than as a distinct network-layer protocol. Nevertheless, in the conceptual OSI model, protocol translation, encryption/decryption, and compression are classic Presentation layer responsibilities. See the ISO OSI Basic Reference Model and the Cloudflare overview of the OSI model.

QUESTION NO: 40

John works as a Network Security Administrator for NetPerfect Inc. The manager of the company has told John that the company's phone bill has increased drastically. John suspects that the company's phone system has been cracked by a malicious hacker. Which attack is used by malicious hackers to crack the phone system?

A. War dialing

B. Sequence++ attack

C. Phreaking

D. Man-in-the-middle attack

ANSWER: C

Explanation:

Phreaking is correct because it specifically describes the unauthorized exploration, manipulation, or abuse of telephone systems and telecommunications services. A phreaker may obtain illicit access to a private branch exchange (PBX), voicemail platform, calling account, long-distance service, or other telephony infrastructure in order to place unauthorized calls. A sudden and substantial rise in a company's phone charges is a classic indicator of telecom fraud, particularly when compromised systems are used to make expensive international or premium-rate calls. In a modern enterprise environment, this can involve traditional PBX equipment, Voice over IP (VoIP) services, SIP trunks, softphones, or voicemail systems exposed to weak credentials or insecure remote administration. The term remains useful because it identifies the target and purpose of the activity: compromise or fraudulent use of telephone services. Effective investigation should include reviewing call-detail records, identifying unusual destinations and calling times, validating PBX and VoIP account access logs, and immediately restricting suspicious outbound calling. The FCC provides guidance on reviewing telephone billing and recognizing unauthorized charges at Understanding Your Telephone Bill. CISA also provides defensive guidance relevant to protecting enterprise voice and communications systems at CISA Communications Sector.

QUESTION NO: 42

Which of the following statements best describes the string matching method of signature analysis?

A. String matching searches specific strings that may indicate an attack.

B. String matching examines multiple fields from different protocols, such as source address, destination port, or TCP flags.

C. In string matching, each packet is wrapped in predefined layers of different protocols.

D. In string matching, an incoming packet is compared, byte by byte, with a single signature, a string of code.

ANSWER: D

Explanation:

In string matching signature analysis, an inspection engine compares packet or reassembled application-layer data against a defined sequence of bytes or characters associated with known malicious activity. The description "In string matching, an incoming packet is compared, byte by byte, with a single signature, a string of code." captures the fundamental matching process: the signature contains a content pattern, and the engine searches the relevant traffic buffer for that pattern. In practical intrusion-detection rules, the comparison is often performed against normalized or reassembled data rather than only one raw packet, and a rule may contain more than one content condition. Nevertheless, byte-oriented comparison to a signature string is the defining concept being tested. This technique is widely used to identify known exploit fragments, malware indicators, suspicious commands, protocol tokens, and other recognizable payload content. For example, Snort rule syntax provides the `content` option specifically to search packet payloads for a specified string, with modifiers that control how and where the engine performs that search. This makes string matching a core signature-analysis capability for network intrusion detection and inspection. See the Snort content option documentation and the Suricata payload keyword documentation.

QUESTION NO: 43

Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server. Which of the following files will he review to accomplish the task?

Each correct answer represents a part of the solution. Choose all that apply.

A. Checkpoint files

B. EDB and STM database files

C. Temporary files

D. cookie files

ANSWER: A B C

Explanation:

For a legacy Microsoft Exchange environment, **Checkpoint files**, **EDB and STM database files**, and **Temporary files** are relevant artifacts for examining a suspicious email. The Exchange database files are the central source of mailbox-store evidence. In older Exchange versions, the EDB file contains structured mailbox data and metadata, while the STM file can contain native MIME content, making these files particularly useful when reconstructing message content, headers, recipients, attachments, and mailbox context. Checkpoint files record the transaction-log generation that has been committed to the database and help an examiner understand database recovery state and establish a coherent relationship between database and related recovery artifacts. Temporary files can preserve transient data created during message processing, conversion, attachment handling, indexing, or client/server operations; therefore, they may contain useful remnants when the primary message is unavailable or incomplete. Together, these artifacts support correlation of email evidence and recovery-oriented forensic analysis. Microsoft documents the role of Exchange databases, transaction logs, and checkpoint files in maintaining mailbox data and recovery consistency in its Exchange disaster recovery documentation. For background on Exchange mailbox databases and their storage role, see Microsoft's mailbox database documentation.

QUESTION NO: 44

Which of the following techniques is used to log network traffic?

A. Cracking

B. IP address spoofing

C. Tunneling

D. Sniffing

ANSWER: D

Explanation:

Sniffing is the technique used to capture and log network traffic for later inspection. A network sniffer places a network interface into a mode that can receive observed packets, then records packet headers and, when available, payload data. Analysts use sniffing during incident response, intrusion analysis, network troubleshooting, and security monitoring to establish what systems communicated, which protocols and ports were used, when activity occurred, and whether traffic contains indicators of compromise.

Packet-capture tools such as tcpdump and Wireshark are common implementations of this technique. Captured traffic can be written to standard packet-capture files, allowing an analyst to revisit the evidence, filter it by address or protocol, reconstruct sessions, and correlate it with firewall, IDS, or endpoint logs. In a switched environment, collection may require a network tap, a SPAN/mirror port, or capture directly on an endpoint or sensor so that the relevant packets are visible to the capture interface. This evidentiary logging role is precisely what sniffing provides. For further technical detail, see the Wireshark documentation and the tcpdump manual page.

QUESTION NO: 45

Adam works as a Network Administrator for passguide Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

A. Internet bot

B. Honey Pot

C. SPI

D. Distributive firewall

ANSWER: C

Explanation:

SPI is the correct choice because stateful packet inspection tracks the state and context of network connections rather than evaluating each packet in isolation. A stateful firewall maintains a connection table and can determine whether an inbound packet belongs to a legitimate, established session. This provides useful protection against many denial-of-service techniques that use unsolicited, malformed, or invalid-state packets to consume resources or disrupt services. For example, state tracking enables the firewall to enforce valid TCP session behavior and apply limits or rules to suspicious connection attempts, including patterns associated with SYN-flood-style attacks. Stateful inspection also lets administrators define policies based on connection state, source, destination, ports, and protocol behavior, which makes perimeter filtering significantly more effective than simple stateless packet filtering. In operational environments, SPI should be configured alongside connection-rate limits, logging, alerting, and upstream DDoS mitigation because very large volumetric attacks can exhaust available bandwidth before traffic reaches the firewall. Nevertheless, for the network-security control described in this question, stateful packet inspection is the most directly useful mechanism for identifying and blocking invalid or unauthorized traffic flows associated with DoS activity. See CISA guidance on denial-of-service attacks and Cisco's discussion of stateful firewall inspection.

QUESTION NO: 46

Which of the following is included in a memory dump file?

A. List of loaded drivers

B. Security ID

C. Stop message and its parameters

D. The kernel-mode call stack for the thread that stopped the process from execution

ANSWER: A C D

Explanation:

A Windows memory dump captures diagnostic information from the system state at the time of a serious failure, enabling analysts and debuggers to reconstruct what the operating system was doing. A list of loaded drivers is included because third-party and Microsoft kernel drivers are central to crash analysis: their names, versions, and loaded modules help associate faulting code with a driver or subsystem. The stop message and its parameters are also core crash artifacts. They identify the bug-check condition and provide values that help determine the specific failing operation, memory address, or context involved.

The kernel-mode call stack for the thread that stopped the process from execution is likewise valuable diagnostic content. Stack frames show the sequence of kernel functions active when the stop occurred and can identify the component involved in the failure path. Microsoft's documentation specifically describes small memory dumps as containing the stop message and parameters, a list of loaded drivers, and the kernel-mode call stack for the thread that stopped. Larger kernel or complete dumps can preserve substantially more memory, but these baseline crash-analysis artifacts remain essential. See Microsoft's Small Memory Dump documentation and Varieties of Kernel-Mode Dump Files.

QUESTION NO: 47

Mark works as a Network administrator for SecureEnet Inc. His system runs on Mac OS X. He wants to boot his system from the Network Interface Controller (NIC). Which of the following snag keys will Mark use to perform the required function?

A. D

B. N

C. Z

D. C

ANSWER: B

Explanation:

N is the applicable startup key for an Intel-based Mac configured to start from a network-based NetBoot service. The key is held immediately after powering on or restarting the Mac; firmware then searches for an available compatible network startup source rather than proceeding directly to the normal local startup disk. In the context of older Mac OS X administration material, this is commonly described as booting from the network interface controller, although it requires supporting network infrastructure such as a NetBoot server and appropriate DHCP/Boot Service discovery configuration.

Apple's Mac startup-key documentation identifies holding **N** at startup as the command to start from a NetBoot server when available. This behavior is distinct from selecting a locally attached boot volume and is specifically intended for centrally managed deployment, recovery, imaging, and diagnostic workflows in environments using Apple's legacy network-boot services. The question's reference to Mac OS X and the use of "NIC" align with that legacy NetBoot startup procedure. See Apple's Mac startup key combinations reference and its NetBoot deployment documentation for the relevant startup and network-boot context.

QUESTION NO: 48

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Public key

B. Digital certificates

C. Twofish

D. RSA

ANSWER: A D

Explanation:

NTFS Encrypting File System uses public-key cryptography to protect the encryption key associated with each encrypted file. In the EFS design, the file's contents are encrypted with a randomly generated file-encryption key, and that key is then protected for the authorized user through public-key operations. RSA is the public-key algorithm EFS uses for this key-protection function. Consequently, both *Public key* and *RSA* accurately identify cryptography used by EFS. The use of public-key protection enables EFS to associate access to encrypted material with the private key held by an authorized user or designated recovery agent, rather than relying solely on a shared secret. Microsoft's EFS technical documentation describes the file encryption key and the public-key-encrypted data-decryption field that allows an authorized private-key holder to recover that key. Microsoft also documents that EFS certificates contain an RSA key pair used by EFS. See Microsoft's File Encryption documentation and Microsoft's Cipher/EFS documentation.

QUESTION NO: 49

Which of the following commands will you use with the tcpdump command to capture the traffic from a filter stored in a file?

A. tcpdump -A file_name

B. tcpdump -D file_name

C. tcpdump -X file_name

D. tcpdump -F file_name

ANSWER: D

Explanation:

`tcpdump -F file_name` is correct because the `-F` flag directs tcpdump to read its packet-selection expression, commonly called a capture filter, from the specified file rather than requiring the expression on the command line. The file contains a filter written in the same libpcap filter language used for normal tcpdump capture expressions, such as `tcp port 443` or `host 192.0.2.10 and not port 22`. This is especially useful for longer, reusable, or operationally standardized filters, because it avoids shell-quoting issues and allows the filter to be reviewed and version-controlled separately from the command invocation. For example, if `web.filter` contains `tcp port 80 or tcp port 443`, running `tcpdump -F web.filter` captures packets matching that expression. tcpdump's documentation specifies that `-F file` reads the filter expression from a file; it also notes that lines beginning with `#` are treated as comments. This behavior is based on the packet-filter syntax provided by libpcap, which tcpdump uses to compile capture expressions before packet capture begins. See the tcpdump manual page and the pcap-filter manual page.

QUESTION NO: 50

Which of the following is the difference between SSL and S-HTTP?

A. SSL operates at the network layer and S-HTTP operates at the application layer.

B. SSL operates at the transport layer and S-HTTP operates at the application layer.

C. SSL operates at the application layer and S-HTTP operates at the transport layer.

D. SSL operates at the application layer and S-HTTP operates at the network layer.

ANSWER: B

Explanation:

SSL operates at the transport layer and S-HTTP operates at the application layer. SSL, now superseded in practice by TLS, provides security services to application protocols over a reliable transport connection, normally TCP. Its record protocol protects data passed from an application and delivers protected records to TCP, allowing protocols such as HTTP, SMTP, and IMAP to use the same underlying transport-security mechanism. In layered-model terminology used in security training and exam questions, this placement is commonly described as the transport layer, although SSL/TLS is more precisely positioned between application protocols and TCP.

S-HTTP (Secure Hypertext Transfer Protocol) was designed specifically as an extension to HTTP. Its security features are embedded in HTTP messages and headers, so it is an application-layer protocol rather than a general-purpose transport security protocol. This distinction is central: SSL/TLS can secure multiple application protocols without changing their message formats, whereas S-HTTP applies protection within the HTTP application protocol itself. The historical SSL specification describes the SSL Record Protocol as receiving data from higher-level protocols and transmitting it to TCP; the S-HTTP specification defines it as an HTTP security enhancement. See RFC 6101 and RFC 2660.