DUMPSBOSS.

GIAC Systems and Network Auditor

GIAC GSNA

Version Demo

Total Demo Questions: 47

Total Premium Questions: 474

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	114
Topic 2, Volume B	110
Topic 3, Volume C	108
Topic 4, Volume D	122
Total	474

QUESTION NO: 1

You configure a wireless router at your home. To secure your home Wireless LAN (WLAN), you implement WEP. Now you want to connect your client computer to the WLAN.

Which of the following is the required information that you will need to configure the client computer? (Choose two)

A. SSID of the WLAN

B. WEP key

C. IP address of the router

D. MAC address of the router

ANSWER: A B

Explanation:

To join a WLAN protected with Wired Equivalent Privacy (WEP), the client must be configured with the network's Service Set Identifier (SSID) and the matching WEP key. The SSID identifies the particular wireless network that the client should locate and attempt to join. A client uses this identifier when selecting or manually creating the wireless-network profile.

The WEP key provides the shared secret needed to protect and access the WLAN. The access point and client must use matching WEP security settings, including the same key material and, where applicable, the configured transmit key index. With these values configured, the client can associate to the access point and communicate using the WLAN's configured legacy encryption mechanism.

WEP is obsolete and has serious cryptographic weaknesses; current security guidance is to use WPA3-Personal where supported, or WPA2-Personal with AES/CCMP for legacy compatibility, rather than deploying WEP. Nevertheless, for the WLAN described, the SSID and WEP key are the required client-side connection details. See the NIST Guidelines for Securing Wireless LANs and CISA wireless-security guidance.

QUESTION NO: 2

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Disaster recovery plan

B. Continuity of Operations Plan

C. Business continuity plan

D. Contingency plan

ANSWER: D

Explanation:

Contingency plan is correct because it is a forward-looking plan for responding when actual conditions differ from the assumptions used in normal operations or planning. It documents predefined strategies, actions, responsibilities, decision points, and activation triggers for a particular disruptive event, emergency, security incident, or other adverse state of affairs. The purpose is to ensure the organization can make an organized, timely response rather than inventing its response under pressure. A mature contingency plan also establishes monitoring and notification procedures, identifies the resources needed to execute the response, and defines conditions for initiating, escalating, and ending planned actions. In an information-system context, NIST describes contingency planning as preparing for recovery and restoration of systems and operations after a disruption, with plans based on defined scenarios and recovery requirements. This fits the question's focus on specific actions addressing variances from assumptions and a defined problem or emergency. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and the CISA business continuity planning resources.

QUESTION NO: 3

Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer? (Choose two)

A. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.

B. Attacker can use the Ping Flood DoS attack if WZC is used.

C. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.

D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

ANSWER: A C

Explanation:

“Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.” is correct because Windows XP Wireless Zero Configuration can actively search for wireless networks, including networks recorded in its preferred-network configuration. These probe requests can expose network identifiers to nearby observers using wireless-monitoring tools. An attacker can use knowledge of those identifiers to impersonate a network the client expects and induce an unsafe association. NIST identifies rogue access points and unauthorized wireless associations as significant enterprise WLAN risks and recommends controls that prevent clients from connecting to untrusted networks.

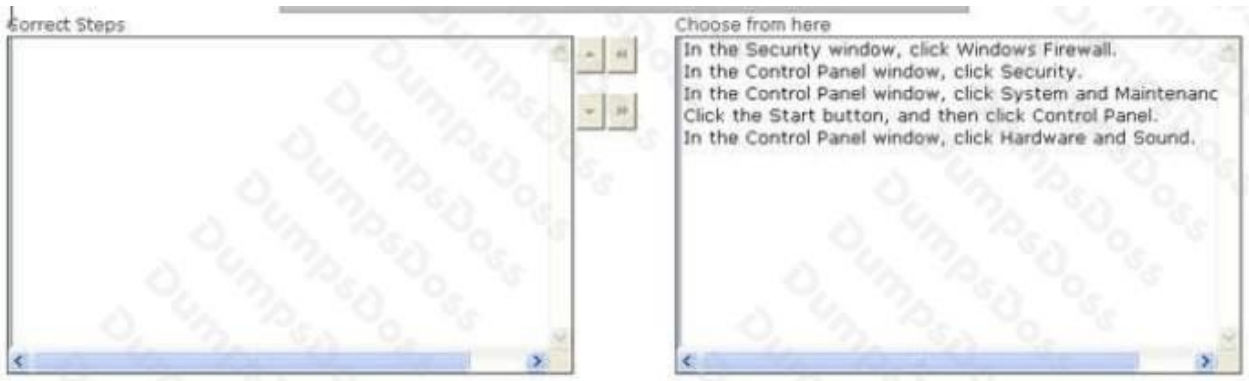
“Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.” is also correct. If a client automatically selects an available preferred network, an attacker can advertise the expected network name and provide a stronger signal than the legitimate access point. This evil-twin scenario can cause the computer to associate with the attacker-controlled access point, enabling traffic interception or further attempts to compromise the client. Wireless clients should use strong mutual authentication, validate network identity, and avoid automatic connection behavior where possible. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks and Microsoft’s Windows XP end-of-support notice.

QUESTION NO: 4 - (DRAG DROP)

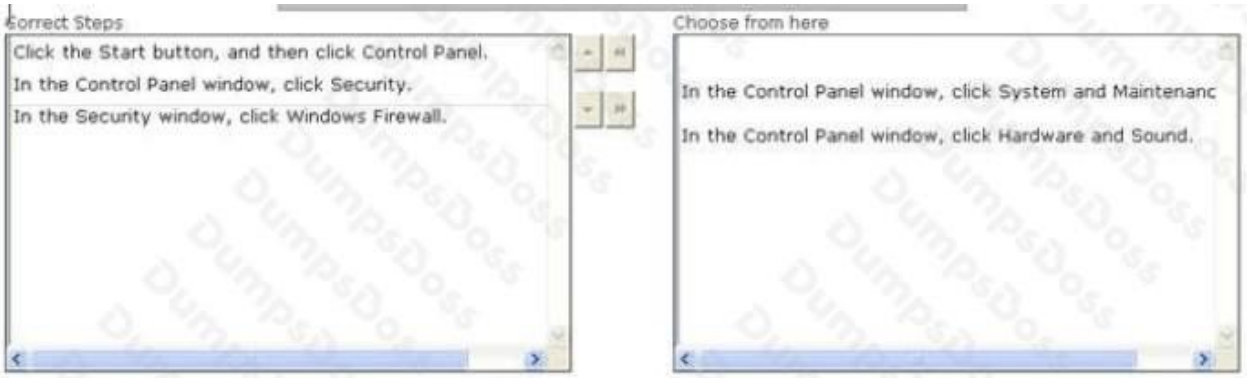
DRAG DROP

You work as a Network Administrator for SoftWorld Inc. All client computers in the company run Windows Vista. You want to view the status of Windows Firewall. Choose in the correct order the steps you will take to accomplish the task.

Select and Place:



ANSWER:



Explanation:

To view Windows Firewall status in the Windows Vista Control Panel category view, begin by opening the Control Panel from the Start menu. This is the standard entry point for Windows configuration utilities and administrative settings. Once Control Panel is open, select **Security**, because Windows Vista groups firewall-related settings under its security category. The Security page provides access to the system's security controls and their current protection state.

Next, select **Windows Firewall** from the Security window. This opens the Windows Firewall dialog, which displays whether the firewall is on or off and provides the associated configuration controls. The sequence is therefore: click the Start button and open Control Panel; open Security; then open Windows Firewall. Following this navigation path reaches the specific firewall interface directly and allows the administrator to inspect the firewall's operational status.

Windows Firewall is a host-based firewall that helps control inbound network traffic and applies protection according to the active network context. Reviewing its status is a core administrative and audit activity because the enabled state of the firewall is part of the system's security posture. Microsoft's documentation describes Windows Firewall as a component used to help protect devices by filtering network traffic; see Windows Firewall overview. Microsoft also provides security guidance and product lifecycle information for legacy Windows versions through its Windows Vista lifecycle page.

QUESTION NO: 5

What is the purpose of Cellpadding attribute of

A. Cellpadding is used to set the width of cell border and its content.

B. Cellpadding is used to set the width of a table.

C. Cellpadding is used to set the space between the cell border and its content.

D. Cellpadding is used to set the space between two cells in a table.

ANSWER: C

Explanation:

Cellpadding is used to set the space between the cell border and its content. In traditional HTML table markup, the `cellpadding` attribute specifies the inset space within every table cell: the distance from a cell's border to the text, image, or other content placed inside that cell. This internal spacing improves readability by preventing content from appearing directly against the border. Its value was conventionally expressed as a number of CSS pixels, and it applied across the table's cells unless more-specific styling was used.

For modern HTML, `cellpadding` is obsolete and authors should use CSS padding on `td` and `th` elements instead. For example, `td, th { padding: 8px; }` creates the same type of internal cell spacing while separating document structure from presentation. MDN documents `HTMLTableElement.cellPadding` as the legacy API reflecting this attribute and recommends CSS for styling: MDN Web Docs: HTMLTableElement.cellPadding. The HTML Standard also identifies presentational table attributes as obsolete and directs authors toward CSS: WHATWG HTML Standard: Obsolete features.

QUESTION NO: 6

Anonymizers are the services that help make a user's own Web surfing anonymous. An

anonymizer removes all the identifying information from a user's computer while the user surfs the Internet. It ensures the privacy of the user in this manner. After the user anonymizes a Web access with an anonymizer prefix, every subsequent link selected is also automatically accessed anonymously.

Which of the following are limitations of anonymizers?

A. ActiveX controls

B. Plugins

C. Secure protocols

D. Java applications

E. JavaScript

ANSWER: A B C D E

Explanation:

ActiveX controls, Plugins, Secure protocols, Java applications, and JavaScript are all recognized limitations of traditional URL-based web anonymizers. These services generally work by fetching and rewriting web content through an intermediary proxy. That model can be disrupted when browser-side code or embedded components establish their own connections, require direct access to client resources, or cannot be safely rewritten and relayed by the anonymizing service. ActiveX controls are especially significant because they may receive broad access to local system resources. Plugins and Java applications can introduce connections or execution behavior outside the anonymizer's normal URL-rewriting path, reducing the assurance that traffic remains mediated by the anonymizing service. JavaScript may be disabled by URL-based anonymizers because scripts can expose browser characteristics, create direct requests, or break rewritten links. Secure protocols also present a fundamental constraint: end-to-end HTTPS protections require the browser to validate and communicate securely with the destination, which conflicts with a simple intermediary rewriting model unless the intermediary performs explicit TLS interception. Modern proxy designs handle HTTPS differently, but the stated limitations accurately describe the historical web anonymizer model addressed by this question. OWASP describes how browser-executed content can create security and privacy concerns in its third-party components guidance, while Mozilla documents the browser security model and restrictions around active web content in its web security documentation.

QUESTION NO: 7

You work as an Exchange Administrator for XYZ CORP. The network design of the company is given below:

Employees are required to use Microsoft Outlook Web Access to access their emails remotely. You are required to accomplish the following goals: Ensure fault tolerance amongst the servers. Ensure the highest level of security and encryption for the Outlook Web Access clients. What will you do to accomplish these goals?

A. Install one front-end Exchange 2000 server and continue to run Microsoft Outlook Web Access on the existing server. Place the new server on the perimeter network. Configure unique URLs for each server. Configure Certificate Services. Create a rule on the firewall to direct port 443 to the servers.

B. Install two front-end Exchange 2000 servers. Place the new servers on the internal network and configure load balancing between them. Configure Certificate Services. Create a rule on the firewall to redirect port 443 to the servers.

C. Install two front-end Exchange 2000 servers. Place the new servers on the perimeter network and configure load balancing between them. Configure Certificate Services. Create a rule on the firewall to redirect port 443 to the servers.

D. Install two Exchange 2000 servers. Place the new servers on the perimeter network. Configure unique URLs for each server. Configure Certificate Services. Create a rule on the firewall to direct port 443 to the servers.

ANSWER: C

Explanation:

Install two front-end Exchange 2000 servers. Place the new servers on the perimeter network and configure load balancing between them. Configure Certificate Services. Create a rule on the firewall to redirect port 443 to the servers. satisfies both stated requirements. Two front-end servers behind a load-balancing solution provide service continuity: if one front-end server becomes unavailable, client requests can be directed to the remaining server. The front-end role is designed to receive client web requests and proxy them to mailbox servers, making it appropriate to scale and protect remote Outlook Web Access access independently of the internal messaging systems.

Locating the front-end servers in a perimeter network separates Internet-facing systems from the internal network. A firewall can publish only encrypted web access by forwarding transmission control protocol port 443 to the load-balanced front-end service. Certificate Services supplies the server certificate needed for secure sockets layer encryption, protecting authentication and mailbox traffic between remote browser clients and the published Outlook Web Access endpoint. This design combines redundant client access, encrypted remote sessions, and network segmentation. Microsoft's historical Exchange front-end/back-end topology guidance describes the front-end role and its use for Internet client access: Microsoft Exchange front-end and back-end server topology. Microsoft also documents the role of certificates in securing web-server connections: Set up TLS on IIS.

QUESTION NO: 8

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. NetStumbler

C. Absinthe

D. Kismet

ANSWER: B

Explanation:

NetStumbler is correct because it is a Windows wireless-network discovery utility designed to identify nearby IEEE 802.11b, 802.11a, and 802.11g access points. It actively probes for wireless networks and presents operational details useful during wireless assessments, including the access point's SSID, BSSID (MAC address), channel, signal-to-noise information, and signal strength. Those capabilities support site-survey and wardriving activities, finding potentially unauthorized access points, and identifying coverage or radio-frequency interference conditions. NetStumbler can also log collected observations, allowing the information to be reviewed or graphed for analysis of wireless signal behavior over time or location. Its historical documentation specifically describes the tool as a Windows application for detecting wireless LANs and lists support for 802.11a/b/g network discovery. Because the question describes this combination of Windows platform support, active WLAN discovery, access-point metadata display, signal-strength monitoring, and graphing/alarm-oriented assessment use, NetStumbler precisely matches the requested tool. Further background and the original project documentation are available from NetStumbler and the tool's archived NetStumbler website.

QUESTION NO: 9

You have to move the whole directory /foo to /bar. Which of the following commands will you use to accomplish the task?

A. mv /bar /foo

B. mv -R /foo /bar

C. mv /foo /bar

D. mv -r /bar /foo

ANSWER: C

Explanation:

`mv /foo /bar` is the standard command for moving a directory in Unix and Linux systems. The `mv` utility accepts a source pathname followed by a destination pathname and operates on directories directly; no recursive flag is needed. If `/bar` already exists and is a directory, this command places the source directory beneath it as `/bar/foo`, preserving the source directory's name and contents. If `/bar` does not exist, the command renames or moves `/foo` so that its new pathname is `/bar`. In either case, the entire directory tree is handled as one move operation. This behavior is especially useful for administrators because it retains the directory's contained files and subdirectories without requiring separate copy or traversal commands. The exact result depends on whether the destination pathname already exists as a directory, so auditors should verify destination state before execution when a specific final pathname matters. The POSIX specification describes `mv` source-to-target behavior at The Open Group mv specification; implementation details are also documented in the GNU Coreutils mv manual.

QUESTION NO: 10

Which of the following statements is NOT true about FAT16 file system?

A. FAT16 file system works well with large disks because the cluster size increases as the disk partition size increases.

B. FAT16 file system supports file-level compression.

C. FAT16 does not support file-level security.

D. FAT16 file system supports Linux operating system.

ANSWER: A B

Explanation:

The statements "FAT16 file system works well with large disks because the cluster size increases as the disk partition size increases" and "FAT16 file system supports file-level compression" are not true. FAT16 has a limited number of addressable clusters because its file-allocation-table entries are 16 bits. To accommodate larger volumes, implementations increase cluster size. Although this permits a larger partition to be formatted, it increases slack space: even a very small file consumes an entire cluster. As volume and cluster sizes grow, this inefficient allocation becomes increasingly significant, so FAT16 is not considered a good file system for large disks.

FAT16 also has no native file-level compression capability. File-level compression is a filesystem feature in which individual files or folders can be stored in compressed form while remaining transparently accessible to applications. Microsoft's file-system feature comparison identifies compression as an NTFS capability rather than a FAT capability. FAT-family volumes may contain files compressed externally by an application or archive utility, but that is not FAT16-provided file-level compression. These limitations are among the reasons FAT16 is primarily associated with smaller or legacy-compatible volumes. See Microsoft's file system functionality comparison and FAT file-system documentation.

QUESTION NO: 11

Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system.

Which of the following are the most likely threats to his computer? (Choose two)

A. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.

B. Attacker can use the Ping Flood DoS attack if WZC is used.

C. An attacker, by creating a fake wireless network with a high-power antenna, can cause Victor's computer to associate with the attacker's network to gain access.

D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

ANSWER: A C

Explanation:

“Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.” is correct because a client’s wireless discovery and connection behavior can disclose identifying information about networks it has previously sought or trusted. An attacker monitoring radio traffic can use that intelligence to impersonate a known network and entice the client to connect. This is particularly significant for legacy wireless clients and configurations that automatically reconnect to preferred networks without sufficient user verification.

“An attacker, by creating a fake wireless network with a high-power antenna, can cause Victor's computer to associate with the attacker's network to gain access.” is also correct. A rogue or evil-twin access point can advertise an expected network name and provide a signal that appears more attractive to the wireless client. If the device associates with the attacker-controlled access point, the attacker may intercept traffic, conduct credential-harvesting attacks, or manipulate the victim’s network communications. NIST wireless-security guidance emphasizes the risks from rogue access points and the need to securely configure wireless clients and authenticate network connections. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks and Microsoft documentation on Windows Wi-Fi configuration.

QUESTION NO: 12

Which of the following commands can be used to intercept and log the Linux kernel messages?

A. syslogd

B. klogd

C. sysklogd

D. syslog-ng

ANSWER: A B

Explanation:

In the traditional Linux logging architecture, `klogd` and `syslogd` work together to collect and record kernel events. `klogd` is the kernel logging daemon: it reads messages emitted by the Linux kernel, historically through the kernel log interface such as `/proc/kmsg`, and passes those messages into the system logging facility. This makes `klogd` the component specifically associated with intercepting kernel messages.

`syslogd` is the system logging daemon that receives those messages and applies its configured routing and storage rules, commonly writing them to files such as `/var/log/messages` or `/var/log/syslog`, forwarding them to another host, or both. Therefore, it is part of the command pair used to log kernel messages in a traditional deployment. The `klogd` manual describes its role as intercepting and logging Linux kernel messages, while the `syslogd` documentation describes its role in receiving and processing system log records. See the klogd manual page and the syslogd manual page.

QUESTION NO: 13

Which of the following commands can be used to format text files?

A. wc

B. ps

C. tail

D. pr

ANSWER: D

Explanation:

The `pr` command is used to format text files for presentation, particularly for printing. It can paginate output by splitting content into pages, add headers containing items such as the date, filename, and page number, and arrange text into multiple columns. These capabilities make it appropriate when plain-text file content needs a print-oriented layout rather than merely being displayed or inspected. For example, `pr -2 filename` produces a two-column formatted version of a file, while other options can control page length, header behavior, and column separation. In an audit or administration context, this can be useful when preparing readable hard-copy or print-preview output from reports and log-derived text. The GNU Core Utilities documentation identifies `pr` as the utility for "convert[ing] text files for printing," including pagination and columnation features. The POSIX specification likewise defines `pr` as a utility that writes files to standard output in paginated form. See the GNU Coreutils pr invocation documentation and the POSIX pr utility specification.

QUESTION NO: 14

Sam works as a Network Administrator for Blue Well Inc. All client computers in the company run the Windows Vista operating. Sam creates a new user account. He wants to create a temporary password for the new user such that the user is forced to change his password when he logs on for the first time.

Which of the following options will he choose to accomplish the task?

A. User cannot change password

B. Delete temporary password at next logon

C. User must change password at next logon

D. Password never expires

ANSWER: C

Explanation:

User must change password at next logon is the appropriate setting because it marks the administrator-assigned password as temporary. When the new user first authenticates with that initial password, Windows requires the user to create a new password before normal access can continue. This ensures that the administrator who created the account does not retain knowledge of the user's ongoing credential, which supports individual accountability and sound password-management practice. In the Windows user-account interface, this setting is selected while creating or editing a local or domain user account after entering the initial password. The user is then prompted to choose a password that meets the applicable password policy, such as length, complexity, and password-history requirements. Microsoft documents the equivalent Active Directory Users and Computers account property as requiring the user to change the password at the next logon; it is intended for precisely this first-use or password-reset workflow. For related Windows account-management guidance, see Microsoft's Active Directory account management documentation and Microsoft's password policy documentation.

QUESTION NO: 15

You work as a Network Administrator for XYZ CORP. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest network. You configure a new Windows Server 2008 server in the network. The new server is not yet linked to Active Directory. You are required to accomplish the following tasks: Add a new group named "Sales". Copy the "Returns" group from the older server to the new one. Rename the "Returns" group to "Revenue". View all group members, including for multiple groups/entire domain. You use Hyena to simplify and centralize all of these tasks. Which of the assigned tasks will you be able to accomplish?

A. Copy the "Returns" group to the new server.

B. Rename the "Returns" group to "Revenue".

C. Add the new group named "Sales".

D. View and manage all group members, including for multiple groups/entire domain.

ANSWER: A B C

Explanation:

Hyena provides group-management capabilities for local computer groups as well as Active Directory groups, depending on the target and available directory connectivity. Therefore, the administrator can add the new group named "Sales" on the new server, because creating and administering local groups is part of Hyena's group administration functionality. Hyena also supports copying a group from one computer to another, allowing the existing "Returns" group configuration to be copied from the older server to the new server. In addition, Hyena supports renaming groups, so changing the copied or existing group name from "Returns" to "Revenue" is an available administrative task.

These functions are appropriate even though the new server has not yet been linked to Active Directory, because they can be performed against local group objects on the server. The domain-wide capability to enumerate all members across multiple groups or throughout the domain is an Active Directory-oriented feature; it requires the server or management context to have access to Active Directory. Hyena's product documentation identifies group administration, copying groups between computers, and group renaming among its supported group-management functions. See SystemTools Hyena Group Management and SystemTools Hyena product overview.

QUESTION NO: 16

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active

Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company has recently provided laptops to its sales team members. You have configured access points in the network to enable a wireless network. The company's security policy states that all users using laptops must use smart cards for authentication.

Which of the following authentication techniques will you use to implement the security policy of the company?

A. IEEE 802.1X using EAP-TLS

B. IEEE 802.1X using PEAP-MS-CHAP

C. Pre-shared key

D. Open system

ANSWER: A

Explanation:

IEEE 802.1X using EAP-TLS is the appropriate authentication technique because EAP-TLS performs certificate-based mutual authentication between the wireless client and the authentication server, typically Network Policy Server/Internet Authentication Service with Active Directory Certificate Services in a Windows environment. A smart card securely stores the user's private key and its associated certificate. During EAP-TLS authentication, the user unlocks that private key with the smart-card PIN, and the client proves possession of the key without transmitting the private key or the PIN across the wireless network.

This approach directly enforces the requirement that laptop users authenticate through smart cards, while also allowing the wireless infrastructure to validate trusted client certificates and the client to validate the server certificate. IEEE 802.1X supplies port-based network access control for the wireless connection, and EAP-TLS supplies the certificate and smart-card authentication method. The organization must deploy an appropriate public key infrastructure, issue smart-card logon certificates to users, configure the RADIUS authentication service, and configure wireless clients and access points for 802.1X/EAP-TLS. Microsoft describes certificate requirements and configuration considerations for EAP-TLS in its NPS certificate documentation and its certificate services guidance.

QUESTION NO: 17

Which of the following are the drawbacks of the NTLM Web authentication scheme?

A. The password is sent in hashed format to the Web server.

B. It works only with Microsoft Internet Explorer.

C. The password is sent in clear text format to the Web server.

D. It can be brute forced easily.

ANSWER: B D

Explanation:

“It works only with Microsoft Internet Explorer.” reflects the historical web-browser interoperability limitation commonly associated with NTLM-based Integrated Windows Authentication. NTLM was proprietary to Microsoft, and seamless, built-in support in the browser was traditionally associated with Internet Explorer. In modern environments, browser support has evolved, but this remains the expected limitation in the legacy framing of the question and is relevant when auditing older applications and authentication designs.

“It can be brute forced easily.” is also a drawback because NTLM authentication relies on password-derived cryptographic material. An attacker who captures NTLM challenge-response data may attempt offline password guessing, testing candidate passwords until one produces the matching response. The practical difficulty depends heavily on password length, complexity, and the available cracking resources; weak or reused passwords substantially increase the risk. Microsoft describes NTLM as a challenge-response protocol and recommends using stronger, modern authentication mechanisms where possible. Auditors should therefore identify NTLM usage, assess password and account controls, and look for mitigations against credential capture and relay. See Microsoft NTLM documentation and Microsoft’s NTLM overview.

QUESTION NO: 18

Which of the following tools hides information about IIS Webservers so that they can be prevented from various attacks performed by an attacker?

A. httprint

B. ServerMask

C. Whisker

D. WinSSLMiM

ANSWER: B

Explanation:

ServerMask is correct because it was specifically designed as an IIS server-information concealment and hardening tool. Its purpose is to reduce information disclosure that enables web-server fingerprinting, such as revealing IIS- or ASP/ASP.NET-specific HTTP response headers, default error responses, cookie characteristics, and implementation details exposed through URLs or generated content. By limiting these identifiers or making them less useful, ServerMask reduces the reconnaissance value available to an attacker attempting to identify the server platform and select targeted exploits. This is a defensive-depth measure: concealing server details does not replace prompt patching, secure configuration, input validation, authentication controls, or monitoring, but it can reduce unnecessary exposure and make automated targeting less reliable. OWASP identifies web-server fingerprinting and the collection of headers, error pages, and other server characteristics as important information-gathering activities during testing: OWASP Web Security Testing Guide: Fingerprint Web Server. Microsoft likewise documents IIS configuration controls for managing request handling and reducing exposure through web-server configuration: IIS Request Filtering configuration reference. Therefore, ServerMask directly matches the tool described.

QUESTION NO: 19

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities.

Which of the following vulnerabilities can be fixed using Nessus?

A. Vulnerabilities that allow a remote cracker to control sensitive data on a system

B. Misconfiguration (e.g. open mail relay, missing patches, etc.)

C. Vulnerabilities that allow a remote cracker to access sensitive data on a system

D. Vulnerabilities that help in Code injection attacks

ANSWER: A B C

Explanation:

Nessus is used to identify, document, and prioritize security weaknesses so administrators can remediate them; the scanner itself generally does not apply the corrective change. Vulnerabilities that allow a remote cracker to control sensitive data on a system are an important class of remotely exploitable findings that Nessus plugins can detect through service discovery, version checks, and vulnerability-specific tests. Findings that allow a remote cracker to access sensitive data on a system are likewise within the core purpose of vulnerability assessment, because exposed services, vulnerable software versions, and insecure configurations can permit unauthorized disclosure.

Misconfiguration (e.g. open mail relay, missing patches, etc.) is also a standard Nessus assessment category. Nessus can identify missing security updates, insecure service configurations, and policy or compliance deviations, including through authenticated scans where credentials permit more complete inspection of host patch and configuration state. The resulting findings give the administrator the evidence needed to install patches, change configuration settings, disable unnecessary services, or otherwise remediate the issue. Tenable describes Nessus as a vulnerability-assessment solution that detects vulnerabilities, misconfigurations, and compliance issues: Tenable Nessus. Guidance on vulnerability management also emphasizes identifying and remediating known vulnerabilities: CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 20

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to see the username, real name, home directory, encrypted password, and other information about a user.

Which of the following Unix configuration files can you use to accomplish the task?

A. /etc/passwd

B. /etc/printcap

C. /etc/hosts

D. /etc/inittab

ANSWER: A

Explanation:

`/etc/passwd` is the traditional Unix account database and is the correct file for viewing core user-account attributes. Its colon-separated records identify the login name and include the password field, numeric user and group identifiers, the GECOS field (commonly used for the user's real name and related descriptive information), the home-directory path, and the login shell. Consequently, it is the standard configuration file associated with reviewing a user's identity and account configuration in Unix systems. Historically, the password field in this file held the encrypted password hash. On modern Unix and Linux systems that implement shadow passwords, this field generally contains a placeholder such as `x`, while the actual password hash is protected in `/etc/shadow`; however, `/etc/passwd` remains the authoritative public account-record file and is the intended answer for the traditional Unix formulation of this question. The Linux manual page documents the

precise fields and their purposes, including the GECOS, home-directory, and shell fields. See passwd(5) — Linux manual page and shadow(5) — Linux manual page.

QUESTION NO: 21

You work as a Database Administrator for BigApple Inc. The Company uses Oracle as its database. You enabled standard database auditing. Later, you noticed that it has a huge impact on performance of the database by generating a large amount of audit data.

How will you keep control on this audit data?

A. By implementing principle of least privilege.

B. By removing some potentially dangerous privileges.

C. By setting the REMOTE_LOGIN_PASSWORDFILE instance parameter to NONE.

D. By limiting the number of audit records generated to only those of interest.

ANSWER: D

Explanation:

By limiting the number of audit records generated to only those of interest is correct because an effective Oracle audit configuration targets events, users, objects, and actions that provide meaningful security or compliance evidence. Narrowing the audit scope reduces both the number of records written and the associated processing, storage, and review burden, while retaining useful accountability information. For standard auditing, administrators can choose specific statement privileges or object actions to audit rather than broadly auditing all activity. Where available, auditing can also be configured to record activity by session instead of every access, reducing duplicate records for repeated operations in one session. Oracle's guidance emphasizes planning auditing around the information required and configuring audit policies selectively; this supports a manageable audit trail and more effective monitoring. Audit data should also be retained, reviewed, and purged or archived according to an established audit-trail management policy, but the primary way to prevent unnecessary audit-volume growth at collection time is to audit only significant events. See Oracle Database Security Guide: Introduction to Auditing and Oracle Database Security Guide: Administering the Audit Trail.

QUESTION NO: 22

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

Under which of the following controls does audit control come?

A. Protective controls

B. Reactive controls

C. Detective controls

D. Preventive controls

ANSWER: C

Explanation:

Detective controls is correct because audit trails and audit logs record events that have occurred, creating evidence that enables an organization to identify suspicious, unauthorized, erroneous, or policy-violating activity. Their core security value is visibility: analysts, auditors, and incident responders can review recorded actions, correlate events across systems, and determine what happened, when it happened, and which account or process was involved. This supports detection of control failures and investigation after an event is logged, rather than stopping the action at the point it occurs.

Effective logging also supports accountability and forensic reconstruction. For example, logs may capture authentication attempts, privileged actions, configuration changes, access to sensitive data, and security-relevant system events. To provide useful detective capability, records should be protected from unauthorized alteration, retained according to organizational requirements, and monitored or reviewed in a timely manner. NIST identifies audit and accountability controls as mechanisms for creating, protecting, retaining, reviewing, analyzing, and reporting audit records, which directly supports detection and investigation. See NIST SP 800-53 Rev. 5, Audit and Accountability and NIST SP 800-92, Guide to Computer Security Log Management.

QUESTION NO: 23 - (HOTSPOT)

HOTSPOT

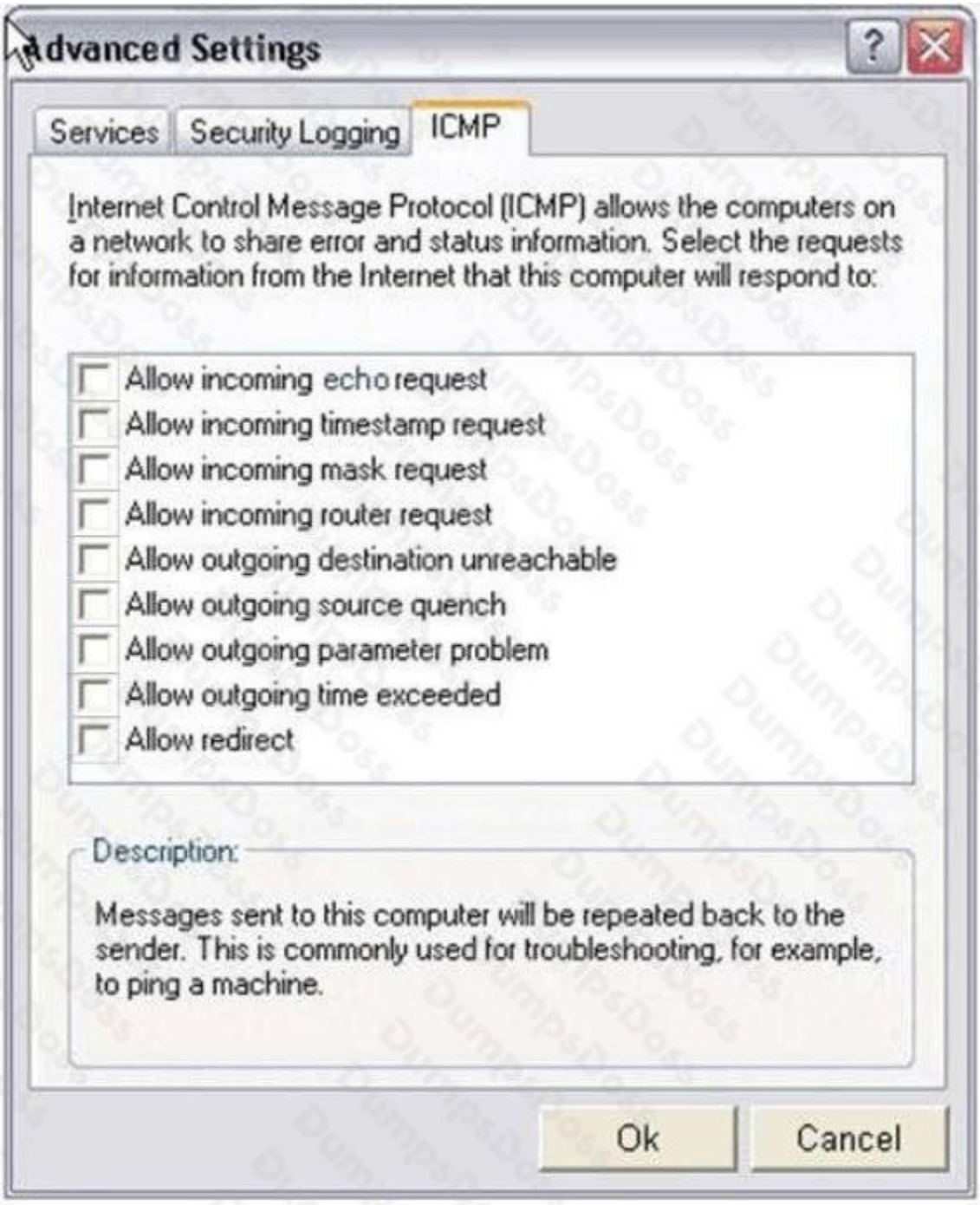
You work as a Network Administrator of a Windows 2000 Active Directory-based single domain network. You have configured your Windows XP Professional computer at home to have a static IP address assigned by your Internet service provider (ISP). It is always connected to the Internet through a modem. You have enabled the Internet Connection Firewall for the Internet connection. You use the PING command to check the connectivity of your home computer from office, but you receive the following error message:

Request timed out.

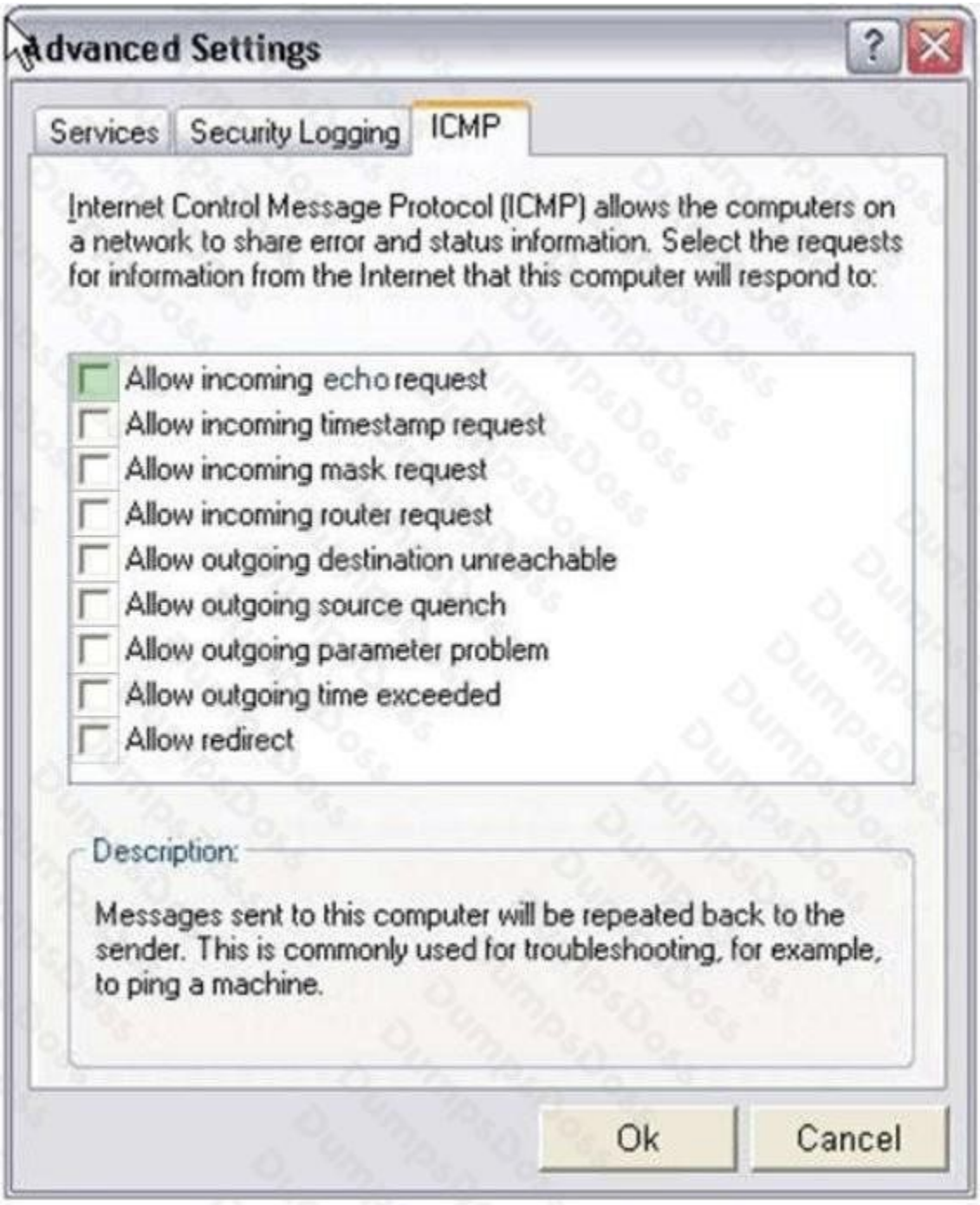
On examining the log file of the Internet Connection Firewall on your home computer, you find DROP ICMP messages. You want to ping your home computer without compromising on security.

Select the option in the Internet Connection Firewall Advanced Settings dialog box, which will be required to be checked to accomplish the task.

Hot Area:


Advanced Settings
Services
Security Logging
ICMP
Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:
Allow incoming echo request
Allow incoming timestamp request
Allow incoming mask request
Allow incoming router request
Allow outgoing destination unreachable
Allow outgoing source quench
Allow outgoing parameter problem
Allow outgoing time exceeded
Allow redirect
Description:
Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.
Ok
Cancel

ANSWER:



Explanation:

The correct setting is **Allow incoming echo request** on the ICMP tab. The Ping utility tests basic IP-layer reachability by sending an ICMP Echo Request to a destination host. For the home Windows XP computer to be successfully pinged from the office, its firewall must accept that inbound request and permit the computer to return the matching ICMP Echo Reply. This setting creates the narrowly targeted exception necessary for that diagnostic traffic, rather than broadly relaxing Internet Connection Firewall protections.

The dialog's description confirms the purpose of the selected setting: messages sent to the computer are repeated back to the sender, which is commonly used to troubleshoot connectivity by pinging a machine. Because the firewall log records dropped ICMP traffic and the remote Ping operation times out, allowing this specific inbound ICMP request directly addresses the observed condition. The setting applies only to echo-request handling; it does not require enabling unrelated ICMP message types. This lets the administrator verify that the home system and its ISP-assigned static address are reachable while keeping the rest of the firewall's inbound filtering in place. Microsoft's description of Windows Firewall configuration explains that firewall rules control inbound traffic, and the Internet Engineering Task Force defines ICMP Echo and Echo Reply behavior in RFC 792. Therefore, the marker belongs on the checkbox beside "Allow incoming echo request."

QUESTION NO: 24

The employees of CCN Inc. require remote access to the company's proxy servers. In order to provide solid wireless security, the company uses LEAP as the authentication protocol.

Which of the following is supported by the LEAP protocol?

A. Dynamic key encryption

B. Public key certificate for server authentication

C. Strongest security level

D. Password hash for client authentication

ANSWER: A D

Explanation:

LEAP (Lightweight Extensible Authentication Protocol) supports **dynamic key encryption** and **password hash for client authentication**. LEAP was Cisco's proprietary wireless EAP method and uses a username and password with a challenge-response exchange rather than relying on a client-side public-key certificate. Following successful authentication, LEAP derives session keying material that can be used to provide dynamically generated WEP keys. Dynamic keys improve on static WEP deployments by giving authenticated wireless clients fresh encryption keys instead of leaving one shared key in place indefinitely.

For client authentication, LEAP's challenge-response design uses password-derived hash information. This enables the authentication server and supplicant to validate knowledge of the shared password without transmitting the cleartext password across the wireless network. LEAP also provides mutual authentication through its challenge-response exchanges, but its password-based design has historically made password strength and credential-management practices especially important. Cisco describes LEAP as an EAP-based wireless authentication mechanism with dynamic WEP key generation in its LEAP technical overview. The EAP framework used by methods such as LEAP is defined in RFC 3748.

QUESTION NO: 25

Which of the following is an Internet mapping technique that relies on various BGP collectors that collect information such as routing updates and tables and provide this information publicly?

A. Path MTU discovery (PMTUD)

B. AS Route Inference

C. AS PATH Inference

D. Firewalking

ANSWER: C

Explanation:

AS PATH Inference is correct because it derives an Autonomous System-level view of Internet connectivity from the AS_PATH attribute found in publicly collected BGP routing information. BGP route collectors, including Route Views and RIPE RIS, receive routing updates and routing table data from participating networks and make much of that data available for research and operational analysis. Each advertised BGP route includes an AS path: an ordered sequence of autonomous systems that the route advertisement has traversed. By examining these sequences across many advertised prefixes and collectors, analysts can infer likely inter-AS adjacencies and construct AS-level topology maps. This method is particularly useful for broad Internet mapping because it leverages control-plane information already exchanged by networks rather than requiring probes to every destination. The inferred topology represents routing-policy visibility and should be interpreted accordingly, since it does not necessarily expose every physical link or the exact forwarding path used by packets. Route Views describes its public collection of BGP routing data at https://www.routeviews.org/routeviews/, while RIPE NCC documents access to Routing Information Service data at https://ris.ripe.net/docs/.

QUESTION NO: 26

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to find out when a particular user was last logged in. To accomplish this, you need to analyze the log configuration files.

Which of the following Unix log configuration files can you use to accomplish the task?

A. /var/log/btmp

B. /var/log/messages

C. /var/log/lastlog

D. /var/log/wtmp

ANSWER: C

Explanation:

`/var/log/lastlog` is the appropriate file for determining when a particular local user last logged in. On Linux and many Unix-like systems, the lastlog database stores one fixed-size record per user ID. That record includes the time of the user's most recent successful login, along with associated terminal and remote-host information where available. Administrators normally query this binary database with the `lastlog` command, such as `lastlog -u username`, rather than reading it directly. The command maps the account name to its UID and retrieves the corresponding record, making it well suited to an audit question focused on the latest login for one user. Because the database retains the most recent login record per account, it provides a direct answer even when older session-history records have been rotated. The system's configured location can vary on some Unix platforms, but `/var/log/lastlog` is the conventional Linux location cited in the question. See the lastlog command manual and the lastlog file-format manual for the record purpose, format, and usage details.

QUESTION NO: 27

You are responsible for a large network that has its own DNS servers. You periodically check the log to see if there are any problems.

Which of the following are likely errors you might encounter in the log? (Choose three)

A. The DNS server could not create FTP socket for address [IP address of server]

B. The DNS server could not create an SMTP socket

C. Active Directory Errors

D. The DNS server could not create a Transmission Control Protocol (TCP) socket

E. The DNS server could not initialize the Remote Procedure Call (RPC) service

ANSWER: C D E

Explanation:

Active Directory Errors, "The DNS server could not create a Transmission Control Protocol (TCP) socket," and "The DNS server could not initialize the Remote Procedure Call (RPC) service" are valid classes of errors that can appear in Microsoft DNS Server logging and event records. DNS depends on network sockets to listen for and answer name-resolution traffic, including TCP-based DNS queries and zone transfers. A failure to create or bind a required TCP socket can prevent the service from accepting that traffic on the affected address or port. DNS also uses RPC-related functionality for administrative and service operations; initialization failures can therefore be recorded when required RPC services or dependencies are unavailable. For Active Directory-integrated zones, DNS stores zone data in Active Directory and relies on directory services and replication. Directory access, replication, or configuration problems can consequently surface as DNS-related Active Directory errors. Reviewing these events helps an auditor identify failures that can affect name resolution, zone availability, and centralized DNS management. Microsoft documents DNS Server operational requirements and troubleshooting considerations at DNS Server overview and explains Active Directory-integrated DNS zones at Active Directory Domain Services documentation.

QUESTION NO: 28

What does CSS stand for?

A. Cascading Style Sheet

B. Coded System Sheet

C. Cyclic Style Sheet

D. Cascading Style System

ANSWER: A

Explanation:

Cascading Style Sheet is the correct expansion of CSS. CSS is the standard stylesheet language used to describe how HTML or XML documents are presented, including layout, colors, typography, spacing, and responsive behavior. Although the acronym is commonly expanded in the singular as “Cascading Style Sheet,” the technology and its specification are generally referred to as “Cascading Style Sheets.” The word “cascading” describes the rule-resolution process: when more than one declaration could apply to an element, the browser evaluates origin, importance, specificity, scoping proximity, and source order to determine the final computed style. This allows site-wide styles, component-specific styles, and limited inline styling to work together predictably. CSS may be included in a document using a `<style>` element, linked as an external `.css` resource, or applied through an element’s `style` attribute. Its separation of presentation from document content supports maintainable, consistent web design. The CSS standard is maintained through specifications published by the CSS Working Group; see the W3C CSS overview. Practical syntax, selectors, cascading, and style application are documented by the MDN CSS reference.

QUESTION NO: 30

You work as a Software Developer for UcTech Inc. You want to create a new session.

Which of the following methods can you use to accomplish the task?

A. getNewSession(true)

B. getSession(false)

C. getSession()

D. getSession(true)

E. getNewSession()

ANSWER: C D

Explanation:

`getSession()` is appropriate because the servlet request API returns the session already associated with the request when one exists and automatically creates a new `HttpSession` when no session is associated with that request. It therefore supports application code that needs a session without first performing a separate existence check.

`getSession(true)` has the same session-creation behavior. The boolean argument controls whether creation is permitted when the request has no current session; supplying `true` directs the container to create and return a new session in that circumstance. Both calls return an `HttpSession`, which an application can use to store session-scoped attributes, obtain the session identifier, or configure session-related behavior. In a servlet, these methods are invoked on the `HttpServletRequest` object, such as `request.getSession()`.

The Jakarta Servlet API defines these methods and specifies that a session is created when necessary for `getSession()` and `getSession(true)`. See the HttpServletRequest API documentation and the Jakarta Servlet specification.

QUESTION NO: 31

Which of the following statements about Secure Sockets Layer (SSL) are true? (Choose two)

A. It provides connectivity between Web browser and Web server.

B. It provides mail transfer service.

C. It provides communication privacy, authentication, and message integrity.

D. It uses a combination of public key and symmetric encryption for security of data.

ANSWER: C D

Explanation:

“It provides communication privacy, authentication, and message integrity” is correct because SSL’s successor, TLS, is designed to create a protected communications channel. During the handshake, the protocol authenticates the server (and can optionally authenticate the client) through certificates and public-key cryptography. The resulting protected session provides confidentiality for transmitted data and integrity protection that enables endpoints to detect unauthorized modification. These are the essential security objectives traditionally associated with SSL/TLS for services such as HTTPS.

“It uses a combination of public key and symmetric encryption for security of data.” is also correct. SSL/TLS uses asymmetric, public-key cryptography during authentication and key establishment, allowing a client to validate the server certificate and securely negotiate shared session secrets. Once the session is established, the protocol uses symmetric encryption with those session keys to protect application data efficiently. This hybrid approach combines the authentication and key-establishment benefits of public-key cryptography with the performance advantages of symmetric encryption for ongoing data transfer. Although SSL itself is obsolete and should not be deployed in modern systems, these statements accurately describe the security model commonly taught for SSL and implemented by modern TLS. See RFC 8446, The Transport Layer Security Protocol Version 1.3 and OWASP Transport Layer Security guidance.

QUESTION NO: 32

Choose the benefits of deploying switches over hubs in your infrastructure. (Choose two)

A. Layer 2 switches allow for the creation of Virtual LANs providing options for further segmentation and security.

B. Switches lower the number of collisions in the environment.

C. Switches create an environment best suited for half duplex communications. This improves network performance and the amount of available bandwidth.

D. Layer 2 switches increase the number of broadcast domains in the environment.

ANSWER: A B

Explanation:

Layer 2 switches allow for the creation of Virtual LANs providing options for further segmentation and security. A managed Layer 2 switch can assign ports to distinct VLANs, logically separating systems even when they share the same physical switching infrastructure. This segmentation supports security and audit objectives by limiting the Layer 2 scope in which broadcasts and other local traffic are forwarded, and by allowing network access policies to be applied between segments through appropriate routing and filtering controls. VLAN capability is a meaningful operational and security advantage over a traditional hub. Cisco’s VLAN overview describes VLANs as logical networks that can partition a switched network: Cisco: What Is a VLAN?.

Switches lower the number of collisions in the environment. Unlike a hub, which places attached devices in one shared collision domain, a switch creates a separate collision domain for each switch port. With normal full-duplex Ethernet operation, a host and its switch port can send and receive simultaneously without collisions; this improves effective bandwidth use and network performance. This behavior is especially relevant when replacing legacy shared-media or hub-based deployments. Cisco explains the relationship between switched Ethernet, collision domains, and full-duplex operation in its Ethernet switching documentation: Cisco: Ethernet Switching.

QUESTION NO: 33

Data mining is a process of sorting through data to identify patterns and establish relationships. Which of the following data mining parameters looks for patterns where one event is connected to another event?

A. Sequence or path analysis

B. Forecasting

C. Clustering

D. Association

ANSWER: D

Explanation:

Association is correct because association analysis identifies relationships, co-occurrences, or dependencies among items and events in a dataset. Its purpose is to reveal that the presence or occurrence of one item or event is statistically linked to another, commonly expressed as an association rule such as “when event X occurs, event Y also tends to occur.” In an audit, security, or operational-data context, this can help identify related activity—for example, a particular account change frequently occurring alongside a specific system event. Association-rule mining evaluates these relationships using measures such as support, which indicates how often the combination occurs, and confidence, which indicates the conditional frequency of one event given another. This directly matches the wording “one event is connected to another event,” without requiring that one occur later in time or that the result be a future prediction. The National Institute of Standards and Technology describes association-rule learning as a data-mining technique for finding relationships among variables, while IBM’s overview of association rules similarly explains their use in discovering frequent relationships in data. See the NIST discussion of data-mining techniques and IBM documentation on association rules.

QUESTION NO: 35

You want to monitor the network infrastructure of a software-based company. The network infrastructure of the company consists of the following:

- Windows TCP/IP services
- Web and mail servers
- URLs Applications (MS Exchange, SQL etc.)

Which of the following network monitoring solutions can you use to accomplish the task?

A. Axence nVision

B. CommandCenter NOC

C. Netmon

D. Cymphonix Network Composer

ANSWER: A

Explanation:

Axence nVision is the appropriate solution because its network-monitoring capability is designed to supervise the mixed infrastructure identified in the question from a single management platform. Its monitoring module supports availability and performance checks for Windows hosts and TCP/IP services, while also providing checks relevant to web resources, mail services, URLs, and commonly deployed server applications. This aligns directly with an environment that includes Microsoft Exchange and SQL Server alongside general network services.

For an auditor or network administrator, the value of this coverage is not merely that individual devices can be reached, but that defined service checks can establish whether critical business services are operating normally and can generate alerts when thresholds or availability conditions are breached. Axence nVision also extends monitoring to network devices and

traffic-related information, supporting broader infrastructure visibility where servers, services, and network equipment must be assessed together. The vendor describes nVision as a network-management product with network monitoring, inventory, and related administrative functions; its monitoring documentation specifically identifies service, URL, and application monitoring capabilities. See Axence nVision product information and Axence nVision documentation.

QUESTION NO: 36

In addition to denying and granting access, what other services does a firewall support?

A. Network Address Translation (NAT)

B. Secondary connections

C. Control Internet access based on keyword restriction

D. Data caching

ANSWER: A C D

Explanation:

Firewalls commonly provide additional network-security and traffic-management services beyond making permit/deny decisions. **Network Address Translation (NAT)** allows a firewall to translate private internal IP addresses to one or more routable external addresses. This both conserves public IPv4 addresses and prevents external systems from directly seeing the internal addressing scheme. NAT is frequently implemented at the network perimeter alongside firewall policy enforcement.

Control Internet access based on keyword restriction is a form of application-layer web filtering. Firewalls or integrated secure web gateway/proxy capabilities can enforce organizational browsing policies by evaluating requested web content, URLs, categories, or keywords and restricting access when policy criteria are met.

Data caching is also a service associated particularly with proxy firewalls. A proxy can retain copies of frequently requested web objects locally and serve subsequent requests from its cache when appropriate. This can reduce repeated external downloads, lower bandwidth use, and improve response times for clients. These functions illustrate that firewalls, especially next-generation and proxy-based implementations, can combine packet filtering with address translation, content-access controls, and application-proxy services. See the IETF NAT terminology and considerations and UK NCSC guidance on network security controls.

QUESTION NO: 37

A Cisco router can have multiple connections to networks. These connections are known as interfaces for Cisco Routers. For naming each interface, Cisco generally uses the type of interface as part of the name.

Which of the following are true about the naming conventions of Cisco Router interfaces?

A. An interface connected to a serial connection always starts with an S.

B. An interface connected to a Token Ring segment always starts with To.

C. An Ethernet interface that is fast always starts with an F.

D. An interface connected to an Ethernet segment of the network always starts with an En.

ANSWER: A B C

Explanation:

Cisco IOS identifies an interface by its media or technology type followed by its location and port numbering. Thus, the interface type is a meaningful part of the interface identifier used in configuration and operational commands such as `show interfaces` and `interface`. An interface connected to a serial connection always starts with an S because the interface

type is named `Serial`, commonly displayed in abbreviated form such as `Serial0/0` or `Se0/0`. An interface connected to a Token Ring segment always starts with To because Cisco names that technology `TokenRing`; IOS commonly abbreviates this type as `To`, as in `TokenRing0`. An Ethernet interface that is fast always starts with an F because its type is `FastEthernet`, typically abbreviated as `Fa`, for example `FastEthernet0/1` or `Fa0/1`. The number of slash-separated components after the type depends on the platform's hardware layout, such as slot, subslot, and port, but does not change the technology-based prefix. Cisco documents interface naming and interface-type command usage in its IOS Interface Command Reference and provides interface configuration guidance in the Cisco Interfaces and Modules support documentation.

QUESTION NO: 38 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate command.

You want to search the most recent command that starts with the string 'user'. For this, you will enter the _____ command to get the desired result.

ANSWER: See the explanation for the answer

Explanation:

The appropriate command is:

```
!user
```

In Bash history expansion, `!user` reruns the most recent command in the history list whose command line begins with `user`.

QUESTION NO: 39

Which of the following tools uses Internet Control Message Protocol (ICMP)?

A. Port scanner

B. Brutus

C. Fragroute

D. Ping scanner

ANSWER: D

Explanation:

Ping scanner is correct because it discovers reachable systems by sending ICMP Echo Request messages and identifying hosts that return ICMP Echo Reply messages. This is commonly called an ICMP ping sweep: the scanner sends probes to a range of IP addresses and compiles a list of addresses that appear responsive. ICMP is a supporting protocol for IP networks, defined for carrying control, error-reporting, and diagnostic messages rather than application data. Echo Request and Echo Reply are its well-known diagnostic message types, which make them suitable for basic host discovery and reachability testing.

In an audit or assessment, a ping scanner can establish an initial inventory of active systems before more detailed examination. Results must be interpreted carefully because network firewalls, host firewalls, and system configurations may block or rate-limit ICMP messages; therefore, lack of an Echo Reply does not conclusively establish that a host is absent. Nevertheless, the defining operation of a ping scanner is its use of ICMP echo traffic to test whether hosts respond. The ICMP message format and Echo message behavior are specified in RFC 792. Practical host-discovery implementations that use ICMP Echo Request probes are also documented by Nmap Host Discovery documentation.

QUESTION NO: 40

You are the security manager of Microliss Inc. Your enterprise uses a wireless network infrastructure with access points ranging 150-350 feet. The employees using the network complain that their passwords and important official information have been traced. You discover the following clues: The information has proved beneficial to an other company. The other company is located about 340 feet away from your office. The other company is also using wireless network. The bandwidth of your network has degraded to a great extent. Which of the following methods of attack has been used?

A. A piggybacking attack has been performed.

B. A DOS attack has been performed.

C. The information is traced using Bluebugging.

D. A worm has exported the information.

ANSWER: A

Explanation:

A piggybacking attack has been performed. The nearby company is within the stated wireless access-point range and can therefore use Microliss's wireless service without authorization if the network's radio coverage and access controls permit it. This unauthorized use consumes shared wireless airtime and Internet capacity, which accounts for the substantial bandwidth degradation. If the wireless traffic is unencrypted, or if authentication and segmentation controls are weak, the unauthorized user may also capture or access sensitive business data, including credentials and official information. In this scenario, the physical proximity, use of another organization's wireless network, apparent access to proprietary information, and reduction in available bandwidth collectively support unauthorized use of the organization's WLAN connection—commonly termed wireless piggybacking. NIST advises organizations to use strong WLAN authentication and encryption, securely configure access points, and continuously monitor wireless activity to identify unauthorized clients and access points. These controls reduce the opportunity for an outside party to associate with or exploit an enterprise WLAN. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks and CISA guidance on network availability and denial-of-service conditions.

QUESTION NO: 41

Which of the following attacks allows the bypassing of access control lists on servers or routers, and helps an attacker to hide? (Choose two)

A. DNS cache poisoning

B. DDoS attack

C. IP spoofing attack

D. MAC spoofing

ANSWER: C D

Explanation:

IP spoofing attack and **MAC spoofing** can both be used to misrepresent a system's identity and potentially defeat access controls that rely solely on a claimed source address. In IP spoofing, an attacker crafts packets with a forged source IP address. If a router, firewall, or server ACL trusts that source IP address, the forged value may cause the traffic to appear to originate from an authorized host. Source-address validation at network boundaries is an important control specifically because it reduces the ability to send packets using addresses not legitimately assigned to the originating network. RFC 2827 describes this ingress-filtering practice: RFC 2827, Network Ingress Filtering.

MAC spoofing changes the layer-two hardware address presented by a network interface. On a local Ethernet or wireless segment, this can make an attacker appear to be a device whose MAC address is trusted by a switch port-security policy, wireless control, or MAC-based ACL. It can also make network activity harder to attribute to the attacker's actual interface. Cisco's port-security documentation describes the use of secure MAC addresses to restrict access and the importance of

addressing MAC-address violations: Cisco Port Security. Both techniques therefore support identity concealment and can exploit ACLs that depend only on source IP or MAC identifiers.

QUESTION NO: 42

Which of the following are the countermeasures against WEP cracking?

A. Using the longest key supported by hardware.

B. Changing keys often.

C. Using a non-obvious key.

D. Using a 16 bit SSID.

ANSWER: A B C

Explanation:

Using the longest key supported by hardware, changing keys often, and using a non-obvious key are all measures that can raise the effort required to attack a legacy Wired Equivalent Privacy deployment. A longer supported key increases the amount of key material used by the mechanism, while a non-obvious, randomly generated key avoids easily guessed values and reduces exposure to simple password-guessing practices. Regular key changes limit the period in which a captured key remains useful and can reduce the value of traffic collected under one static key. These practices are mitigations only: the fundamental design weaknesses in Wired Equivalent Privacy, including weaknesses involving its stream-cipher usage and integrity protections, mean that a sufficiently capable attacker can still recover keys after collecting enough wireless traffic. Therefore, an auditor should treat these controls as temporary risk reduction for an unavoidable legacy environment, not as a basis for approving the protocol for new or continuing sensitive deployments. Current best practice is migration to modern wireless protections rather than reliance on Wired Equivalent Privacy. NIST states that Wired Equivalent Privacy should not be used and recommends stronger wireless security configurations; see NIST SP 800-153. The Wi-Fi Alliance's overview of current security generations also provides useful context for modern protection choices: Wi-Fi Security.

QUESTION NO: 43

Adam works as a Security Analyst for Umbrella Inc. He is retrieving large amount of log data from syslog servers and network devices such as Router and switches. He is facing difficulty in analyzing the logs that he has retrieved. To solve this problem, Adam decides to use software called Sawmill. Which of the following statements are true about Sawmill?

A. It incorporates real-time reporting and real-time alerting.

B. It is used to analyze any device or software package, which produces a log file such as Web servers, network devices (switches & routers etc.), syslog servers etc.

C. It is a software package for the statistical analysis and reporting of log files.

D. It comes only as a software package for user deployment.

ANSWER: A B C

Explanation:

Sawmill is designed as a log-analysis and reporting platform, so "It is a software package for the statistical analysis and reporting of log files" accurately describes its core purpose. It ingests log data, parses it into structured information, and presents statistical reports that help analysts investigate activity, trends, and events without manually reviewing very large raw-log files.

"It is used to analyze any device or software package, which produces a log file such as Web servers, network devices (switches & routers etc.), syslog servers etc." is also correct in the practical sense intended by the question. Sawmill supports analysis of logs from a broad range of sources through log formats and profiles, including web infrastructure and network/security devices. This makes it applicable to the syslog and network-device data described in the scenario.

“It incorporates real-time reporting and real-time alerting” is correct because Sawmill’s feature set includes monitoring-oriented reporting and alert capabilities, allowing operational or security-relevant log activity to be surfaced promptly. These capabilities complement its historical statistical reporting by helping an analyst move from collected log data to timely visibility. See the vendor’s Sawmill product site and its feature overview for product capability details.

QUESTION NO: 44

You work as a Network Administrator for XYZ CORP. The company has a Windows Active

Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks: The wireless network communication should be secured. The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps: Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication.

What will happen after you have taken these steps?

A. Both tasks will be accomplished.

B. The laptop users will be able to use smart cards for getting authenticated.

C. The wireless network communication will be secured.

D. None of the tasks will be accomplished.

ANSWER: C

Explanation:

The wireless network communication will be secured. In the Windows Server 2003-era wireless architecture described, IEEE 802.1X provides port-based network access control: the wireless client must complete EAP authentication through the access point before receiving normal network access. PEAP protects the EAP exchange by establishing a TLS tunnel between the client and authentication server, and the successful authentication can provide keying material used to protect the wireless connection. WEP then applies link-layer encryption to the WLAN traffic. Thus, the stated 802.1X, PEAP, and WEP configuration achieves the question’s wireless-access protection objective in the legacy context of this scenario. Microsoft describes 802.1X as providing authenticated network access and notes its role in wireless access control in its Network Access documentation. The IEEE 802.1X standard defines the port-based access-control framework and its authentication architecture; see the IEEE 802.1X standard page. In a current deployment, an auditor should require WPA2-Enterprise or WPA3-Enterprise rather than WEP, because WEP is obsolete and cryptographically weak; however, the expected outcome for this historical configuration is that the wireless communication is protected.

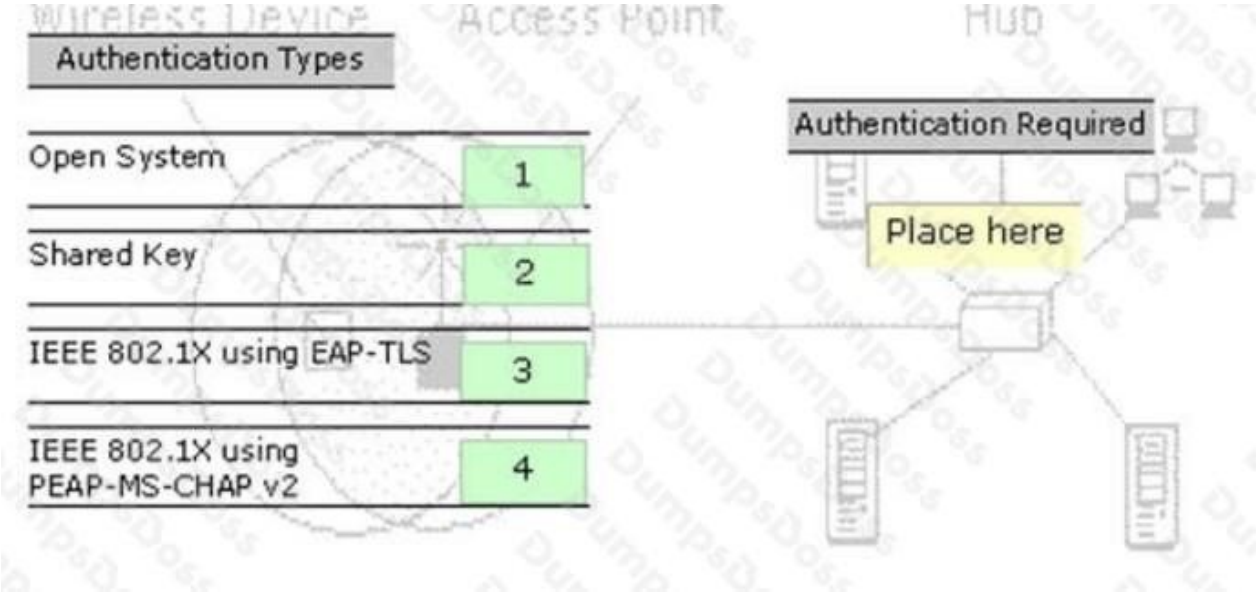
QUESTION NO: 45 - (DRAG DROP)

DRAG DROP

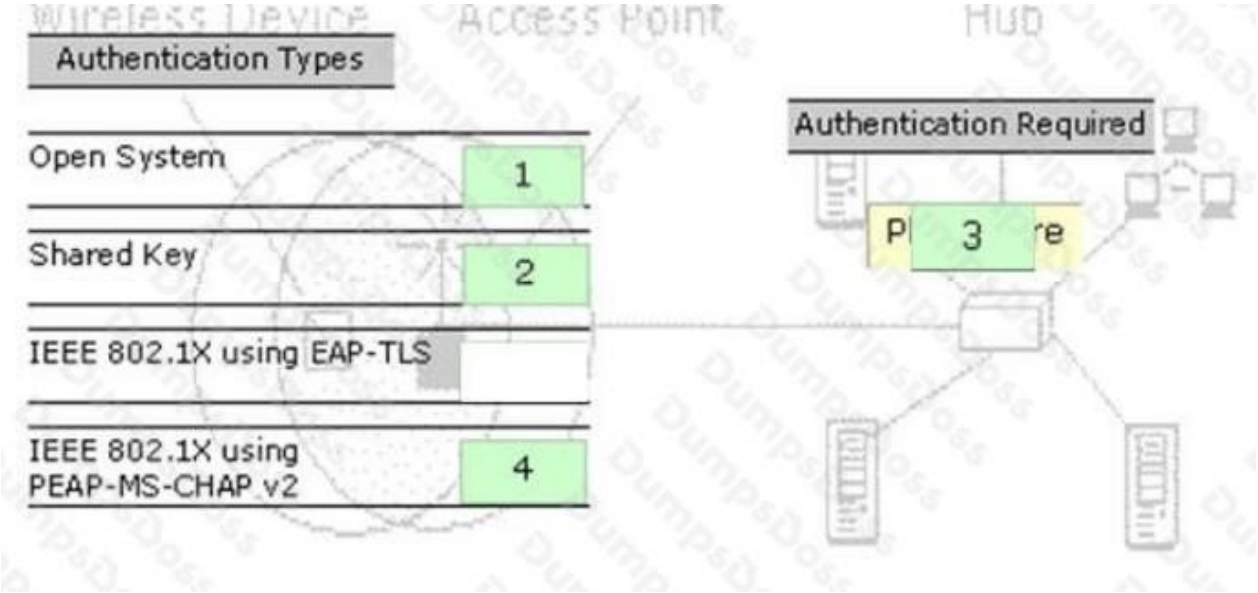
You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active

Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company has recently provided laptops to its sales team members. You have configured access points in the network to enable a wireless network. The company's security policy states that all users using laptops must use smart cards for authentication. Select and place the authentication method you are required to configure to implement the security policy of the company.

Select and Place:



ANSWER:



Explanation:

IEEE 802.1X using EAP-TLS is the appropriate authentication method because the policy requires laptop users to authenticate with smart cards before receiving access to the wireless network. IEEE 802.1X provides port-based network access control: a wireless client requesting access acts as the supplicant, the access point acts as the authenticator, and a RADIUS server validates the supplied credentials. This allows the organization to make successful authentication a condition of joining the protected wireless network.

EAP-TLS is specifically suited to smart-card authentication because it uses Transport Layer Security with digital certificates. The user certificate and corresponding private key can be stored on the smart card, so the user must possess the card and unlock it with the appropriate PIN to complete authentication. The authentication infrastructure also presents a server certificate, enabling mutual certificate-based authentication between the client and the network. This provides strong protection for enterprise wireless access and aligns with Active Directory certificate services in a Windows Server environment.

Microsoft documents the use of smart cards with certificate-based authentication in its Smart Card Overview. The IEEE 802.1X framework is defined by the Extensible Authentication Protocol standard, while EAP-TLS certificate authentication is specified in RFC 5216. Therefore, selecting IEEE 802.1X using EAP-TLS implements the required smart-card-based wireless authentication control.

QUESTION NO: 46

Which of the following commands can be used to find out where commands are located?

A. type

B. which

C. env

D. ls

ANSWER: A B

Explanation:

`type` and `which` are both appropriate commands for identifying how a command name is resolved by the shell and, where applicable, the executable's location. In common POSIX-style shells, `type` reports whether a name resolves to an alias, shell builtin, shell function, keyword, or an external executable. When the name is an external command, its output ordinarily includes the pathname found through the user's `PATH`. This makes it particularly useful during audit work because a command that appears to be a standard utility may instead be overridden by a shell alias or function.

`which` is used to display the pathname of the executable that would be located for a command name according to the search path. It is commonly available on Unix-like systems and is useful for quickly confirming which installed copy of a utility the environment will invoke. Auditors can use these commands to verify command resolution, identify unexpected executable locations, and investigate path-order issues that could affect administrative scripts or security tooling. The Bash reference documents `type` as identifying how each name would be interpreted, while the POSIX specification describes `command -v`-style command identification behavior and path resolution concepts. See the GNU Bash Builtins reference and the POSIX command utility specification.

QUESTION NO: 47

You work as a Network Auditor for XYZ CORP. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it.

Which of the following risks may occur due to the existence of these problems?

A. Residual risk

B. Inherent risk

C. Secondary risk

D. Detection risk

ANSWER: D

Explanation:

Detection risk is the correct answer because it is the risk that audit procedures will not identify a material error, control deficiency, fault, or other relevant condition that actually exists. In this scenario, the auditor is having difficulty locating faults and associated entities in the Windows-based environment. That limitation directly affects the auditor's ability to obtain sufficient and appropriate evidence and to detect conditions the audit is intended to uncover. If searches, queries, evidence collection, or review procedures do not reveal relevant assets, events, or faults, the audit may incorrectly report that no issue was found even though one is present.

In audit-risk practice, detection risk is managed by designing and performing procedures that are appropriate to the audit objective, including using reliable data sources, validating search scope and completeness, testing query logic, and applying additional procedures where evidence is incomplete or uncertain. It can arise from sampling limitations as well as nonsampling issues, such as applying an unsuitable procedure or misinterpreting evidence. The core concern here is therefore the possibility that the audit work fails to find an existing condition. See the PCAOB guidance on audit risk and detection risk and the ISACA discussion of understanding audit risk.