GIAC

Exam GSNA

GIAC Systems and Network Auditor

Version: 3.0

[Total Questions: 368]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	68

Topic 1, Volume A

Question No : 1 - (Topic 1)

George works as an office assistant in Soft Well Inc. The company uses the Windows Vista operating system. He wants to disable a program running on a computer. Which of the following Windows Defender tools will he use to accomplish the task?

A. Allowed items
B. Quarantined items
C. Options
D. Software Explorer

Answer: D

Explanation:
Software Explorer is used to remove, enable, or disable a program running on a computer. Answer: A is incorrect. Allowed items contains a list of all the programs that a user has chosen not to monitor with Windows Defender. Answer: C is incorrect. Options is used to choose how Windows Defender should monitor all the programs running on a computer. Answer: B is incorrect. Quarantined items is used to remove or restore a program blocked by Windows Defender.

Question No : 2 - (Topic 1)

You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem. Which of the following utilities will you use to diagnose the problem?

A. PING
B. IPCONFIG
C. TRACERT
D. NSLOOKUP

Answer: D

Explanation: NSLOOKUP is a tool for diagnosing and troubleshooting Domain Name System (DNS) problems. It performs its function by sending queries to the DNS server and obtaining detailed responses at the command prompt. This information can be useful for diagnosing and resolving name resolution issues, verifying whether or not the resource

records are added or updated correctly in a zone, and debugging other server-related problems. This tool is installed along with the TCP/IP protocol through the Control Panel. Answer: A is incorrect. The ping command-line utility is used to test connectivity with a host on a TCP/IP-based network. This is achieved by sending out a series of packets to a specified destination host. On receiving the packets, the destination host responds with a series of replies. These replies can be used to determine whether or not the network is working properly. Answer: B is incorrect. IPCONFIG is a command-line utility used to display current TCP/IP network configuration values and update or release the Dynamic Host Configuration Protocol (DHCP) allocated leases. It is also used to display, register, or flush Domain Name System (DNS) names. Answer: C is incorrect. TRACERT is a route-tracing Windows utility that displays the path an IP packet takes to reach the destination. It shows the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.

Question No : 3 - (Topic 1)

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to run a command that forces all the unwritten blocks in the buffer cache to be written to the disk. Which of the following Unix commands can you use to accomplish the task?

A. swapon
B. tune2fs
C. swapoff
D. sync

Answer: D

Explanation: The sync command is used to flush filesystem buffers. It ensures that all disk writes have been completed before the processor is halted or rebooted. Generally, it is preferable to use reboot or halt to shut down a system, as they may perform additional actions such as resynchronizing the hardware clock and flushing internal caches before performing a final sync. Answer: B is incorrect. In Unix, the tune2fs command is used to adjust tunable filesystem parameters on the second extended filesystems. Answer: A is incorrect. In Unix, the swapon command is used to activate a swap partition. Answer: C is incorrect. In Unix, the swapoff command is used to de-activate a swap partition.

Question No : 4 - (Topic 1)

Which of the following statements about a session are true? (Choose two)

A. The creation time can be obtained using the getSessionCreationTime() method of the HttpSession.
B. The getAttribute() method of the HttpSession interface returns a String.
C. The time for the setMaxInactiveInterval() method of the HttpSession interface is specified in seconds.
D. The isNew() method is used to identify if the session is new.

Answer: C,D

Explanation: The setMaxInactiveInterval() method sets the maximum time in seconds before a session becomes invalid. The syntax of this method is as follows: public void setMaxInactiveInterval(int interval) Here, interval is specified in seconds. The isNew() method of the HttpSession interface returns true if the client does not yet know about the session, or if the client chooses not to join the session. This method throws an IllegalStateException if called on an invalidated session. Answer: B is incorrect. The getAttribute(String name) method of the HttpSession interface returns the value of the named attribute as an object. It returns a null value if no attribute with the given name is bound to the session. This method throws an IllegalStateException if it is called on an invalidated session. Answer: A is incorrect. The creation time of a session can be obtained using the getCreationTime() method of the HttpSession.

Question No : 5 - (Topic 1)

Which of the following statements is true about a relational database?

A. It is difficult to extend a relational database.
B. The standard user and application program interface to a relational database is Programming Language (PL).
C. It is a collection of data items organized as a set of formally-described tables.
D. It is a set of tables containing data fitted into runtime defined categories.

Answer: C

Explanation: A relational database is a collection of data items organized as a set of

formally-described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database tables. Answer: B is incorrect. The standard user and application program interface to a relational database is the structured query language (SQL). Answer: A is incorrect. In addition to being relatively easy to create and access, a relational database has the important advantage of being easy to extend. Answer: D is incorrect. A relational database is a set of tables containing data fitted into predefined categories. Each table (which is sometimes called a relation) contains one or more data categories in columns. Each row contains a unique instance of data for the categories defined by the columns.

Question No : 6 - (Topic 1)

An auditor assesses the database environment before beginning the audit. This includes various key tasks that should be performed by an auditor to identify and prioritize the users, data, activities, and applications to be monitored. Which of the following tasks need to be performed by the auditor manually?

A. Classifying data risk within the database systems
B. Monitoring data changes and modifications to the database structure, permission and user changes, and data viewing activities
C. Analyzing access authority
D. Archiving, analyzing, reviewing, and reporting of audit information

Answer: A,C

Explanation: The Internal Audit Association lists the following as key components of a database audit: Create an inventory of all database systems and use classifications. This should include production and test data. Keep it up-to-date. Classify data risk within the database systems. Monitoring should be prioritized for high, medium, and low risk data. Implement an access request process that requires database owners to authorize the "roles" granted to database accounts (roles as in Role Based Access and not the native database roles). Analyze access authority. Users with higher degrees of access permission should be under higher scrutiny, and any account for which access has been suspended should be monitored to ensure access is denieA, Dttempts are identified. Assess application coverage. Determine what applications have built-in controls, and prioritize database auditing accordingly. All privileged user access must have audit priority. Legacy and custom applications are the next highest priority to consider, followed by the packaged applications. Ensure technical safeguards. Make sure access controls are set properly.

Audit the activities. Monitor data changes and modifications to the database structure, permission and user changes, and data viewing activities. Consider using network-based database activity monitoring appliances instead of native database audit trails. Archive, analyze, review, and report audit information. Reports to auditors and IT managers must communicate relevant audit information, which can be analyzed and reviewed to determine if corrective action is required. Organizations that must retain audit data for long-term use should archive this information with the ability to retrieve relevant data when needed. The first five steps listed are to be performed by the auditor manually. Answer: B, D are incorrect. These tasks are best achieved by using an automated solution.

Question No : 7 - (Topic 1)

You work as a Network Administrator for XYZ CORP. The company has a TCP/IP-based network environment. The network contains Cisco switches and a Cisco router. You run the following command for a router interface: show interface serial0 You get the following output: Serial0 is administratively down, line protocol is down What will be your conclusion after viewing this output?

A. There is a physical problem either with the interface or the cable attached to it.
B. The router has no power.
C. There is a problem related to encapsulation.
D. The interface is shut down.

Answer: D

Explanation: According to the question, the output displays that the interface is administratively down. Administratively down means that the interface is shut down. In order to up the interface, you will have to open the interface with the no shutdown command. Answer: A is incorrect. Had there been a physical problem with the interface, the output would not have displayed "administratively down". Instead, the output would be as follows: serial0 is down, line protocol is down Answer: B is incorrect. You cannot run this command on a router that is powered off. Answer: C is incorrect. Encapsulation has nothing to do with the output displayed in the question.

Question No : 8 - (Topic 1)

You work as a Network Administrator for XYZ CORP. The company has a Linux-based network. You need to configure a firewall for the company. The firewall should be able to keep track of the state of network connections traveling across the network. Which of the following types of firewalls will you configure to accomplish the task?

A. A network-based application layer firewall
B. Host-based application firewall
C. An application firewall
D. Stateful firewall

Answer: D

Explanation:

A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected. Answer: B is incorrect. A host-based application firewall can monitor any application input, output, and/or system service calls made from, to, or by an application. This is done by examining information passed through system calls instead of, or in addition to, a network stack. A host-based application firewall can only provide protection to the applications running on the same host. An example of a host-based application firewall that controls system service calls by an application is AppArmor or the Mac OS X application firewall. Host-based application firewalls may also provide network-based application firewalling. Answer: A is incorrect. A network-based application layer firewall, also known as a proxy-based or reverse-proxy firewall, is a computer networking firewall that operates at the application layer of a protocol stack. Application firewalls specific to a particular kind of network traffic may be titled with the service name, such as a Web application firewall. They may be implemented through software running on a host or a stand-alone piece of network hardware. Often, it is a host using various forms of proxy servers to proxy traffic before passing it on to the client or server. Because it acts on the application layer, it may inspect the contents of the traffic, blocking specified content, such as certain websites, viruses, and attempts to exploit known logical flaws in client software. Answer: C is incorrect. An application firewall is a form of firewall that controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall. The application firewall is typically built to monitor one or more specific applications or services (such as a web or database service), unlike a stateful network firewall, which can provide some access controls for nearly any kind of network traffic. There are two primary categories of application firewalls: Network-based application firewalls Host-based application firewalls

Question No : 9 - (Topic 1)

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You have been assigned the task to design the authentication system for the remote users of the company. For security purposes, you want to issue security tokens to the remote users. The token should work on the one-time password principle and so once used, the next password gets generated. Which of the following security tokens should you issue to accomplish the task?

A. Virtual tokens
B. Event-based tokens
C. Bluetooth tokens
D. Single sign-on software tokens

Answer: B

Explanation: An event-based token, by its nature, has a long life span. They work on the one-time password principle and so once used, the next password is generated. Often the user has a button to press to receive this new code via either a token or via an SMS message. All CRYPTOCard's tokens are event-based rather than time-based. Answer: C is incorrect. Bluetooth tokens are often combined with a USB token, and hence work in both a connecteA, D disconnected state. Bluetooth authentication works when closer than 32 feet (10 meters). If the Bluetooth is not available, the token must be inserted into a USB input device to function. Answer: A is incorrect. Virtual tokens are a new concept in multi-factor authentication first introduced in 2005 by security company Sestus. Virtual tokens work by sharing the token generation process between the Internet website and the user's computer and have the advantage of not requiring the distribution of additional hardware or software. In addition, since the user's device is communicating directly with the authenticating website, the solution is resistant to man-in-the-middle attacks and similar forms of online fraud. Answer: D is incorrect. Single sign-on software tokens are used by the multiple, related, but independent software systems. Some types of single sign-on (SSO) solutions, like enterprise single sign-on, use this token to store software that allows for seamless authentication and password filling. As the passwords are stored on the token, users need not remember their passwords and therefore can select more secure passwords, or have more secure passwords assigned.

Question No : 10 - (Topic 1)

Adam works on a Linux system. He is using Sendmail as the primary application to transmit e-mails. Linux uses Syslog to maintain logs of what has occurred on the system. Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?

A. /var/log/mailog
B. /var/log/logmail
C. /log/var/mailog
D. /log/var/logd

Answer: A

Explanation: /var/log/mailog ?le generally contains the source and destination IP addresses, date and time stamps, and other information that may be used to check the information contained within an e-mail header. Linux uses Syslog to maintain logs of what has occurred on the system. The configuration file /etc/syslog.conf is used to determine where the Syslog service (Syslogd) sends its logs. Sendmail can create event messages and is usually configured to record the basic information such as the source and destination addresses, the sender and recipient addresses, and the message ID of e-mail. The syslog.conf will display the location of the log file for e-mail. Answer: B, C, D are incorrect. All these files are not valid log files.

Question No : 11 - (Topic 1)

Sarah works as a Web Developer for XYZ CORP. She is creating a Web site for her company. Sarah wants greater control over the appearance and presentation of Web pages. She wants the ability to precisely specify the display attributes and the appearance of elements on the Web pages. How will she accomplish this?

A. Use the Database Design wizard.
B. Make two templates, one for the index page and the other for all other pages.
C. Use Cascading Style Sheet (CSS).
D. Make a template and use it to create each Web page.

Answer: C

Explanation: Sarah should use the Cascading Style Sheet (CSS) while creating Web pages. This will give her greater control over the appearance and presentation of the Web pages and will also enable her to precisely specify the display attributes and the appearance of elements on the Web pages.

Question No : 12 - (Topic 1)

You work as the Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are a root user on the Red Hat operating system. You want to keep an eye on the system log file /var/adm/messages. Which of the following commands should you use to read the file in real time?

A. tail -n 3 /var/adm/messages
B. tail -f /var/adm/messages
C. cat /var/adm/messages
D. tail /var/adm/messages

Answer: B

Explanation: Using the -f option causes tail to continue to display the file in real time, showing added lines to the end of the file as they occur.

Question No : 13 - (Topic 1)

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: Piggybacking refers to access of a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary in jurisdictions around the world. While completely outlawed in some jurisdictions, it is permitted in others. The process of sending data along with the acknowledgment is called piggybacking. Answer: C is incorrect. Bluebugging is an attack used only in a Bluetooth network. Bluebugging is a form of bluetooth attack often caused by a lack of awareness. Bluebugging tools allow attacker to "take control" of the victim's phone via the usage of the victim's Bluetooth phone headset. It does this by pretending to be the users bluetooth headset and therefore "tricking" the phone to obey its call commands. Answer: D is incorrect. A worm is a software program that uses computer networks and security holes to replicate itself from one computer to another. It usually performs malicious actions, such as using the resources of computers as well as shutting down computers. Answer: B is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as a network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to the network. The effects of a DoS attack are as follows: Saturates network resources Disrupts connections between two computers, thereby preventing communications between services Disrupts services to a specific computer Causes failure to access a Web site Results in an increase in the amount of spam A Denial-of-Service attack is very common on the Internet because it is much easier to accomplish. Most of the DoS attacks rely on the weaknesses in the TCP/IP protocol.

Question No : 14 - (Topic 1)

Which of the following tools works both as an encryption-cracking tool and as a keylogger?

A. Magic Lantern
B. KeyGhost Keylogger
C. Alchemy Remote Executor
D. SocketShield

Answer: A

Explanation: Magic Lantern works both as an encryption-cracking tool and as a keylogger. Answer: C is incorrect. Alchemy Remote Executor is a system management tool that allows

Network Administrators to execute programs on remote network computers without leaving their workplace. From the hacker's point of view, it can be useful for installing keyloggers, spyware, Trojans, Windows rootkits and such. One necessary condition for using the Alchemy Remote Executor is that the user/attacker must have the administrative passwords of the remote computers on which the malware is to be installed. Answer: B is incorrect. The KeyGhost keylogger is a hardware keylogger that is used to log all keystrokes on a computer. It is a tiny device that clips onto the keyboard cable. Once the KeyGhost keylogger is attached to the computer, it quietly logs every key pressed on the keyboard into its own internal Flash memory (just as with smart cards). When the log becomes full, it overwrites the oldest keystrokes with the newest ones. Answer: D is incorrect. SocketShield provides a protection shield to a computer system against malware, viruses, spyware, and various types of keyloggers. SocketShield provides protection at the following two levels: 1.Blocking: In this level, SocketShield uses a list of IP addresses that are known as purveyor of exploits. All http requests for any page in these domains are simply blocked. 2.Shielding: In this level, SocketShield blocks all the current and past IP addresses that are the cause of unauthorized access.

Question No : 15 - (Topic 1)

You have just installed a Windows 2003 server. What action should you take regarding the default shares?

A. Disable them only if this is a domain server.
B. Disable them.
C. Make them hidden shares.
D. Leave them, as they are needed for Windows Server operations.

Answer: B

Explanation: Default shares should be disabled, unless they are absolutely needed. They pose a significant security risk by providing a way for an intruder to enter your machine. Answer: A is incorrect. Whether this is a domain server, a DHCP server, a file server, or database server does not change the issue with shared drives/folders. Answer: C is incorrect. They cannot be hidden. Shared folders are, by definition, not hidden but rather available to users on the network. Answer: D is incorrect. These are not necessary for Windows Server operations.

Question No : 16 - (Topic 1)

John works as a contract Ethical Hacker. He has recently got a project to do security checking for www.we-are-secure.com. He wants to find out the operating system of the we-are-secure server in the information gathering step. Which of the following commands will he use to accomplish the task? (Choose two)

A. nc 208.100.2.25 23
B. nmap -v -O www.we-are-secure.com
C. nc -v -n 208.100.2.25 80
D. nmap -v -O 208.100.2.25

Answer: B,D

Explanation: According to the scenario, John will use "nmap -v -O 208.100.2.25" to detect the operating system of the we-are-secure server. Here, -v is used for verbose and -O is used for TCP/IP fingerprinting to guess the remote operating system. John may also use the DNS name of we-are-secure instead of using the IP address of the we-are-secure server. So, he can also use the nmap command "nmap -v -O www.we-are-secure.com ". Answer: C is incorrect. "nc -v -n 208.100.2.25 80" is a Netcat command, which is used to banner grab for getting information about the

Question No : 17 - (Topic 1)

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 risks are the risks that an auditor will not be able to find what they

are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist. Detection risk includes two types of risk: Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample. Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objectives (detection faults). Answer: A is incorrect. Residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). In the economic context, residual means "the quantity left over at the end of a process; a remainder". Answer: B is incorrect. Inherent risk, in auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of inherent risk depends on the professional judgment of the auditor, and it is done after assessing the business environment of the entity being audited. Answer: C is incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as primary risks, but can turn out to be so if not estimated and planned properly.

Question No : 18 - (Topic 1)

John works as a Network Administrator for We-are-secure Inc. The We-are-secure server is based on Windows Server 2003. One day, while analyzing the network security, he receives an error message that Kernel32.exe is encountering a problem. Which of the following steps should John take as a countermeasure to this situation?

A. He should download the latest patches for Windows Server 2003 from the Microsoft site, so that he can repair the kernel.
B. He should restore his Windows settings.
C. He should observe the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new malicious process is running, he should kill that process.
D. He should upgrade his antivirus program.

Answer: C,D

Explanation: In such a situation, when John receives an error message revealing that Kernel32.exe is encountering a problem, he needs to come to the conclusion that his

antivirus program needs to be updated, because Kernel32.exe is not a Microsoft file (It is a Kernel32.DLL file.). Although such viruses normally run on stealth mode, he should examine the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new process (malicious) is running on the server, he should exterminate that process. Answer: A, B are incorrect. Since kernel.exe is not a real kernel file of Windows, there is no need to repair or download any patch for Windows Server 2003 from the Microsoft site to repair the kernel. Note: Such error messages can be received if the computer is infected with malware, such as Worm_Badtrans.b, Backdoor.G_Door, Glacier Backdoor, Win32.Badtrans.29020, etc.

Question No : 19 - (Topic 1)

You work as a Network Administrator for Infonet Inc. The company's network has an FTP server. You want to secure the server so that only authorized users can access it. What will you do to accomplish this?

A. Disable anonymous authentication.
B. Stop the FTP service on the server.
C. Disable the network adapter on the server.
D. Enable anonymous authentication.

Answer: A

Explanation: You will have to disable anonymous authentication. This will prevent unauthorized users from accessing the FTP server. Anonymous authentication (anonymous access) is a method of authentication for Websites. Using this method, a user can establish a Web connection to the IIS server without providing a username and password. Hence, this is an insecure method of authentication. This method is generally used to permit unknown users to access the Web or FTP server directories. Answer: D is incorrect. Enabling anonymous authentication will allow all the users to access the server. Answer: B is incorrect. Stopping the FTP service on the server will prevent all the users from accessing the FTP server. Answer: C is incorrect. Disabling the network adapter on the FTP server will disconnect the server from the network.

Question No : 20 - (Topic 1)

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system. He wants to sniff the we-are-secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?

A. IPChains
B. Tripwire
C. Hunt
D. Ethercap

Answer: C

Explanation:

In such a scenario, John will use Hunt which is capable of performing both the hacking techniques, sniffing and session hijacking. Answer: D is incorrect. Ethercap is a network sniffer and packet generator. It may be an option, but John wants to do session hijacking as well. Hence, he will not use Ethercap. Answer: A is incorrect. IPChains is a firewall. Answer: B is incorrect. Tripwire is a file and directory integrity checker.

Question No : 21 - (Topic 1)

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Single Loss Expectancy (SLE)
B. Annualized Rate of Occurrence (ARO)
C. Exposure Factor (EF)
D. Safeguard

Answer: B

Explanation: The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. Answer: C is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer: A is incorrect. The Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE = Asset Value ($) X Exposure Factor (EF) Answer: D is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a

specific threat or a group of threats.

Question No : 22 - (Topic 1)

Mark implements a Cisco unified wireless network for Tech Perfect Inc. Which functional area of the Cisco unified wireless network architecture includes intrusion detection and prevention?

A. Network services
B. Wireless clients
C. Network unification
D. Wireless access points

Answer: A

Explanation: Network services is the last functional area of the Cisco unified wireless network architecture. This functional area includes the self-depending network, enhanced network support, such as location services, intrusion detection and prevention, firewalls, network admission control, and all other services. Answer: C is incorrect. Network unification is a functional area of the Cisco unified wireless network architecture. This functional area includes the following wireless LAN controllers: 1.The 6500 series catalyst switch 2.Wireless services module (WiSM) 3.Cisco wireless LAN controller module (WLCM) 4.Cisco catalyst 3750 series integrated WLC 5.Cisco 4400 series WLC 6.Cisco 2000 series WLC Answer: B is incorrect. Wireless clients is a functional area of the Cisco unified wireless network. The client devices are connected to a user. Answer: D is incorrect. A wireless access point (WAP) is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth, or related standards. The WAP usually connects to a wired network, and it can transmit data between wireless devices and wired devices on the network. Each access point can serve multiple users within a defined network area. As people move beyond the range of one access point, they are automatically handed over to the next one. A small WLAN requires a single access point. The number of access points in a network depends on the number of network users and the physical size of the network.

Question No : 23 - (Topic 1)

What are the different categories of PL/SQL program units?

A. Default
B. Unnamed
C. Primary
D. Named

Answer: B,D

Explanation: A named block is a PL/SQL block that Oracle stores in the database and can be called by name from any application. A named block is also known as a stored procedure. Named blocks can be called from any PL/SQL block. It has a declaration section, which is known as a header. The header may include the name of a block, type of the block, and parameter. The name and list of formal parameters are known as the signature of a subroutine. Once a named PL/SQL block is compiled, it gets permanently stored as p-code after compilation in the shared pool of the system global area. Therefore, the named block gets compiled only once. An anonymous block is a PL/SQL block that appears in a user's application and is neither named nor stored in the database. This block does not allow any mode of parameter. Anonymous block programs are effective in some situations. They are basically used when building scripts to seed data or perform one-time processing activities. They are also used when a user wants to nest activity in another PL/SQL block's execution section. Anonymous blocks are compiled each time they are executed.

Question No : 24 - (Topic 1)

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network. John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

A. Non-operational audit
B. Dependent audit
C. Independent audit
D. Operational audit

Answer: C

Explanation: An independent audit is an audit that is usually conducted by external or outside resources. It is the process of reviewing detailed audit logs for the following purposes: To examine the system activities and access logs To assess the adequacy of

system methods To assess the adequacy of system controls To examine compliance with established enterprise network system policies To examine compliance with established enterprise network system procedures To examine effectiveness of enabling, support, and core processes Answer: B is incorrect. It is not a valid type of security audit. Answer: D is incorrect. It is done to examine the operational and ongoing activities within a network. Answer: B is incorrect. It is not a valid type of security audit. Answer: D is incorrect. It is done to examine the operational and ongoing activities within a network. Answer: A is incorrect. It is not a valid type of security audit.

Question No : 25 - (Topic 1)

Which of the following statements about the traceroute utility are true?

A. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.
B. It records the time taken for a round trip for each packet at each router.
C. It is an online tool that performs polymorphic shell code attacks.
D. It generates a buffer overflow exploit by transforming an attack shell code so that the new attack shell code cannot be recognized by any Intrusion Detection Systems.

Answer: A,B

Explanation: Traceroute is a route-tracing utility that displays the path an IP packet takes to reach its destination. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host. This tool also records the time taken for a round trip for each packet at each router that can be used to find any faulty router along the path. Answer: C, D are incorrect. Traceroute does not perform polymorphic shell code attacks. Attacking tools such as ADMutate areused to perform polymorphic shell code attacks.

Question No : 26 - (Topic 1)

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to use Kismet as a wireless sniffer to sniff the We-are-secure network. Which of the following IEEE-based traffic can be sniffed

with Kismet?

A. 802.11g
B. 802.11n
C. 802.11b
D. 802.11a

Answer: A,B,C,D

Explanation: Kismet can sniff IEEE 802.11a, 802.11b, 802.11g, and 802.11n-based wireless network traffic.

Question No : 27 - (Topic 1)

eBox Platform is an open source unified network server (or a Unified Network Platform) for SMEs. In which of the following forms can eBox Platform be used?

A. Unified Communications Server
B. Network Infrastructure Manager
C. Gateway
D. Sandbox

Answer: A,B,C

Explanation: eBox Platform is an open source unified network server (or a Unified Network Platform) for SMEs. eBox Platform can act as a Gateway, Network Infrastructure Manager, Unified Threat Manager, Office Server, Unified Communications Server or a combination of them. Besides, eBox Platform includes a development framework to ease the development of new Unix-based services. Answer: D is incorrect. eBox Platform cannot act as a sandbox. A sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs, from unverified third-parties, suppliers, and untrusted users.

Question No : 28 - (Topic 1)

You work as a Java Programmer for JavaSkills Inc. You are working with the Linux

operating system. Nowadays, when you start your computer, you notice that your OS is taking more time to boot than usual. You discuss this with your Network Administrator. He suggests that you mail him your Linux bootup report. Which of the following commands will you use to create the Linux bootup report?

A. touch bootup_report.txt
B. dmesg > bootup_report.txt
C. dmesg | wc
D. man touch

Answer: B

Explanation: According to the scenario, you can use dmesg > bootup_report.txt to create the bootup file. With this command, the bootup messages will be displayed and will be redirected towards bootup_report.txt using the > command.

Question No : 29 - (Topic 1)

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

A. Safeguards
B. Detective controls
C. Corrective controls
D. Preventive controls

Answer: C

Explanation: Corrective controls are used after a security breach. After security has been breached, corrective controls are intended to limit the extent of any damage caused by the incident, e.g. by recovering the organization to normal working status as efficiently as possible. Answer: D is incorrect. Before the event, preventive controls are intended to prevent an incident from occurring, e.g. by locking out unauthorized intruders. Answer: B is incorrect. During the event, detective controls are intended to identify and characterize an incident in progress, e.g. by sounding the intruder alarm and alerting the security guards or the police. Answer: A is incorrect. Safeguards are those controls that provide some amount of protection to an asset.

Question No : 30 - (Topic 1)

Ryan wants to create an ad hoc wireless network so that he can share some important files with another employee of his company. Which of the following wireless security protocols should he choose for setting up an ad hoc wireless network?

(Choose two)

A. WPA2 -EAP
B. WPA-PSK
C. WEP
D. WPA-EAP

Answer: B,C

Explanation: Ryan can either choose WEP or WPA-PSK wireless protocol to set an ad hoc wireless network.
Answer: A is incorrect. WPA2-EAP cannot be chosen for an ad hoc wireless network, as it requires RADIUS (Remote Authentication Dial- In User Service) server for authentication.
Answer: D is incorrect. WPA-EAP cannot be chosen for an ad hoc wireless network, as it requires RADIUS (Remote Authentication Dial-In User Service) server for authentication.

Question No : 31 - (Topic 1)

You run the wc -c file1.txt command. If this command displays any error message, you want to store the error message in the error.txt file. Which of the following commands will you use to accomplish the task?

A. wc -c file1.txt >>error.txt
B. wc -c file1.txt 1>error.txt
C. wc -c file1.txt 2>error.txt
D. wc -c file1.txt >error.txt

Answer: C

Explanation: According to the scenario, you will use the wc -c file1.txt 2>error.txt command to accomplish the task. The 2> operator is an error redirector, which, while running a command, redirects the error (if it exists) on the specified file. Answer: B, D are incorrect. The > or 1> redirector can be used to redirect the output of the wc -c file1.txt file to the error.txt file; however, you want to write the errors in the error.txt file, not the whole

output. Answer: A is incorrect. The >> operator will redirect the output of the command in the same manner as the > or 1> operator. Although the >> operator will not overwrite the error.txt file, it will append the error.txt file.

Question No : 32 - (Topic 1)

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 supports the following group management functions: Full group administration such as add, modify, delete, and copy Rename groups Copy groups from one computer to another View both direct and indirect (nested) group members for one or more groups [only for Active Directory] View all group members, including for multiple groups/entire domain [only for Active Directory] Answer: D is incorrect. All group members can neither be viewed nor managed until the new server is linked to Active Directory.

Question No : 33 - (Topic 1)

Which of the following is a technique for creating Internet maps? (Choose two)

A. AS PATH Inference
B. Object Relational Mapping

C. Active Probing
D. Network Quota

Answer: A,C

Explanation: There are two prominent techniques used today for creating Internet maps: Active probing: It is the first works on the data plane of the Internet and is called active probing. It is used to infer Internet topology based on router adjacencies. AS PATH Inference: It is the second works on the control plane and infers autonomous system connectivity based on BGP data.

Question No : 34 - (Topic 1)

Which of the following types of firewall functions at the Session layer of OSI model?

A. Packet filtering firewall
B. Circuit-level firewall
C. Switch-level firewall
D. Application-level firewall

Answer: B

Explanation: Circuit-level firewall operates at the Session layer of the OSI model. This type of firewall regulates traffic based on whether or not a trusted connection has been established.

Question No : 35 - (Topic 1)

You work as a Web Deployer for UcTech Inc. You write the <security constraint> element for an application in which you write the <auth-constraint> sub-element as follows: <auth-constraint> <role-name>*</role-name> </auth-constraint> Who will have access to the application?

A. Only the administrator
B. No user
C. All users