CySA+ Exam Questions 1

Study online at https://quizlet.com/_fjwtoz

You suspect that a service called explorer.exe on a Windows server is malicious and you need to terminate it. Which of the following tools would NOT be able to terminate it? sc wmic secpol.msc services.msc	secpol.msc (OBJ-3.1: The security policy auditor (secpol.msc) will allow an authorized administrator the option to change a great deal about an operating system, but it cannot explicitly stop a process or service that is already running. The sc.exe command allows an analyst to control services, including terminating them. The Windows Management Instrumentation (wmic) can terminate a service by using the following: wmic service <ServiceName> call StopService. The services.msc tool can also be used to enable, start, or terminate a running service.)
Which of the following tools could be used to detect unexpected output from an application being managed or monitored? A log analysis tool A behavior-based analysis tool A signature-based detection tool Manual analysis	A behavior-based analysis tool (OBJ-3: A behavior-based analysis tool can be used to capture/analyze normal behavior and then alert when an anomaly occurs. Configuring a behavior-based analysis tool requires more effort to properly set up, but it requires less work and manual monitoring once it is running. Signature-based detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future. Manual analysis requires a person to read all the output and determine if it is erroneous. A log analysis tool would only be useful to analyze the logs, but it would not be able to detect unexpected output by itself. Instead, the log analysis tool would need to use a behavior-based or signature-based detection system.)
A popular game allows for in-app purchases to acquire extra lives in the game. When a player purchases the extra lives, the number of lives is written to a configuration file on the gamer's phone. A hacker loves the game, but hate having to buy lives all the time, so they developed an exploit that allows a player to purchase 1 life for $0.99 and then modifies the content of the configuration file to claim 100 lives were purchased prior to the application reading the number of lives purchased from the file. Which of the following type of vulnerabilities did the hacker exploit? Sensitive data exposure Dereferencing Broken authentication Race condition	Race condition (OBJ-4.4: Race conditions occur when the outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer. In this scenario, the hacker's exploit is racing to modify the configuration file before the application reads the number of lives from it. Sensitive data exposure is a fault that allows privileged information (such as a token, password, or PII) to be read without being subject to the proper access controls. Broken authentication refers to an app that fails to deny access to malicious actors. Dereferencing attempts to access a pointer that references an object at a particular memory location.)
You have been given access to a Windows system located on an Active Directory domain as part of a white box penetration test. Which of the following commands would provide information about other systems on this network? net use net user net group net config	net use (OBJ-1: The net use command will list network shares that the workstation is using. This will help to identify file servers and print servers on the network. The net group command can only be used on domain controllers. The net config command will allow servers and workstations services to be controlled once they have already been identified. The net user command would show any user accounts on the local Windows workstation you are using.)
Which type of monitoring would utilize a network tap? Router-based Active	Passive (OBJ-1: Network taps are devices that allow a copy of network traffic to be captured for analysis. They conduct passive network monitoring and visibility without interfering with the network traffic

Passive SNMP	itself. Active monitoring relies on the scanning of targeted systems, not a network tap. Router-based monitoring would involve looking over the router's logs and configuration files. SNMP is used to monitor network devices, but is considered a form of active monitoring and doesn't rely on network taps.)
An organization wants to get an external attacker's perspective on their security status. Which of the following services should they purchase? Vulnerability scan Asset management Penetration test Patch management	Penetration test (OBJ-1.4: Penetration tests provide an organization with an external attacker's perspective on their security status. The NIST process for penetration testing divides tests into four phases: planning, discovery, attack, and reporting. The results of penetration tests are valuable security planning tools, as they describe the actual vulnerabilities that an attacker might exploit to gain access to a network. A vulnerability scan provides an assessment of your security posture from an internal perspective. Asset management refers to a systematic approach to the governance and realization of value from the things that a group or entity is responsible for, over their whole life cycles. It may apply both to tangible assets and to intangible assets. Patch management is the process that helps acquire, test, and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones.)
Which of the following type of solutions would you classify a FPGA as? Hardware security module Anti-tamper Trusted platform module Root of trust	Anti-tamper (OBJ-2: A field programmable gate array (FPGA) is an anti-tamper mechanism that makes use of a type of programmable controller and a physically unclonable function (PUF). The PUF generates a digital fingerprint based on the unique features of the device. This means that tampering with a device, such as by removing the chip or adding an unknown input/output mechanism, can be detected, and a remedial action like using zero-filling cryptographic keys can be performed automatically. A hardware security module (HSM) is an appliance for generating and storing cryptographic keys. It is a solution that may be less susceptible to tampering and insider threats than a traditional software-based storage solution. A trusted platform module (TPM) is a specification for hardware-based storage of digital certificates, cryptographic keys, hashed passwords, and other user and platform identification information. A hardware root of trust (RoT) or trust anchor is a secure subsystem that is able to provide attestation to declare something as true.)
Which of the following types of data breaches would require that the US Department of Health and Human Services and the media be notified if more than 500 individuals are affected by a data breach? Credit card information Protected health information Personally identifiable information Trade secret information	Protected health information (OBJ-2: Protected health information (PHI) is defined as any information that identifies someone as the subject of medical and insurance records, plus their associated hospital and laboratory test results. This type of data is protected by the Health Insurance Portability and Accountability Act (HIPPA) and requires notification of the individual, the Secretary of the US Department of Health and Human Services (HHS), and the media (if more than 500 individuals are affected) in the case of a data breach. Personally identifiable information (PII) is any data that can be used to identify, to contact, or to impersonate an individual. Credit card information is protected under the PCI DSS information security standard. Trade secret information is protected by the organization that owns those secrets.)
A cybersecurity analyst just finished conducting an initial vulnerability scan and is reviewing their results. To avoid wasting their time on results that are not really a vulnerability, the analyst wants to remove any false positives before they begin to remediate the findings. Which of the following is an indicator that something in	Items classified by the system as Low or as For Informational Purposes Only (OBJ-2: When conducting a vulnerability scan, it is common for the

their results would be a false positive? A finding that shows the scanner compliance plug-ins are not up-to-date Items classified by the system as Low or as For Informational Purposes Only A scan result showing a version that is different from the automated asset inventory A 'HTTPS entry that indicates the web page is securely encrypted	report to include some findings that are classified as "low" priority or "for informational purposes only". These are most likely false positives and can be ignored by the analyst when first starting their remediation efforts. "A HTTPS entry that indicates the web page is securely encrypted" is not a false positive, but a true negative (a non-issue). A scan result showing a version that is different from the automated asset inventory is something that should be investigated and is likely a true positive. A finding that shows the scanner compliance plug-ins are not up-to-date would likely also be a true positive that should be investigated.)
What containment techniques is the strongest possible response to an incident? Segmentation Isolating affected systems Isolating the attacker Enumeration	Isolating affected systems (OBJ-3: Isolation involves removing an affected component from whatever larger environment it is a part of. This can be everything from removing a server from the network after it has been the target of a DoS attack, to placing an application in a sandbox virtual machine (VM) outside of the host environments it usually runs on. Segmentation-based containment is a means of achieving the isolation of a host or group of hosts using network technologies and architecture. Segmentation uses VLANs, routing/subnets, and firewall ACLs to prevent a host or group of hosts from communicating outside the protected segment. Removal is not an industry term used but would be a synonym for isolation. Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system. Isolating the attacker would only stop their direct two-way communication and control of the affected system, but it would not be the strongest possible response since there could be malicious code still running on your victimized machine.)
Which type of media sanitization would you classify degaussing as? Clearing Purging Destruction Erasing	Purging (OBJ-3: Degaussing is classified as a form of purging. Purging eliminates information from being feasibly recovered even in a laboratory environment. Purging includes degaussing, encryption of the data with the destruction of its encryption key, and other non-destructive techniques. Some generic magnetic storage devices can be reused after the degaussing process has taken place, such as VHS tapes and some older backup tapes. For this reason, though, the technique of degaussing is classified as purging and not destruction, even though hard drives are rendered unusable after being degaussed. Clearing data prevents data from being retrieved without the use of state of the art laboratory techniques. Clearing often involves overwriting data one or more times with repetitive or randomized data. Destroying data is designed not merely to render the information unrecoverable, but also to hinder any reuse of the media itself. Destruction is a physical process that may involve shredding media to pieces, disintegrating it to parts, pulverizing it to powder, or incinerating it to ash. Erasing or deleting is considered a normal operation of a computer, which erases the pointer to the data file on a storage device. Erasing and deleting are easily reversed, and the data can be recovered with commercially available or open-source tools.)
Review the following packet captured at your NIDS: -=-23:12:23.154234 IP 86.18.10.3:54326 > 71.168.10.45:3389 Flags [P.], Seq 1834:1245, ack1, win 511, options [nop,nop, TS val 263451334 erc 482862734, length 125 -=-After reviewing the packet above, you discovered there is an unauthorized service running on the host. Which of the following	DENY TCP ANY HOST 71.168.10.45 EQ 3389

ACL entries should be implemented to prevent further access to the unauthorized service while maintaining full access to the approved services running on this host? DENY TCP ANY HOST 71.168.10.45 EQ 3389 DENY IP HOST 71.168.10.45 ANY EQ 25 DENY IP HOST 86.18.10.3 EQ 3389 DENY TCP ANY HOST 86.18.10.3 EQ 25	(OBJ-3: Since the question asks you to prevent access to the unauthorized service, we need to block port 3389 from accepting connections on 71.168.10.45 (the host). This option will deny ANY workstation from connecting to this machine (host) over the Remote Desktop Protocol service that is unauthorized (port 3389).)
You just finished conducting a remote scan of a class C network block using the following command "nmap -sS 202.15.73.0/24". The results only showed a single web server. Which of the following techniques would allow you to gather additional information about the network? Use a UDP scan Perform a scan from on-site Scan using the -p 1-65535 flag Use an IPS evasion technique	Perform a scan from on-site (OBJ-1: You should request permission to conduct an on-site scan of the network. If the organization's network is set up correctly, scanning from off-site will be much more difficult as many of the devices will be hidden behind the firewall. By conducting an on-site scan, you can conduct the scan from behind the firewall and receive more detailed information on the various servers and services that are running on the internal network. While nmap does provide some capabilities to scan through a firewall, it is not as detailed as being on-site.)
Which of the following technologies could be used to ensure that users who login to a network are physically in the same building as the network they are attempting to authenticate on? Port security NAC GPS location Geo-IP	GPS location NAC (OBJ-1.3: Network Access Control is used to identify an endpoint's characteristics when conducting network authentication. The GPS location of the device will provide the longitude and latitude of the user, which could be compared against the GPS coordinates of the building. Port security enables an administrator to configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port. This would not help to locate the individual based on their location, though. Geo-IP, or geolocation and country lookup of a host-based on its IP address, would identify the country of origin of the user, but not whether or not they are within the confines of the building. Geo-IP is also easily tricked if the user logs in over a VPN connection.)
Mark works as a Department of Defense contracting officer and needs to ensure that any network devices he purchases for his organization's network are secure. He utilizes a process to verify the chain of custody for every chip and component that is used in the device's manufacturer. What program should Mark utilize? Gray market procurement Trusted Foundry White market procurement Chain of procurement	Trusted Foundry (OBJ-1.4: The US Department of Defense (DoD) has set up a Trusted Foundry Program, operated by the Defense Microelectronics Activity (DMEA). Accredited suppliers have proved themselves capable of operating a secure supply chain, from design through to manufacture and testing. The Trusted Foundry program to help assure the integrity and confidentiality of circuits and manufacturing. The purpose is to help verify that agents of foreign governments are not able to insert malicious code or chips into the hardware being used by the military systems. This is part of ensuring hardware source authenticity and ensure purchasing is made from reputable suppliers to prevent the use of counterfeited or compromised devices.)
You are conducting a quick nmap scan of a target network. You want to conduct a SYN scan, but you don't have raw socket privileges on your workstation. Which of the following commands should you use to conduct the SYN scan from your workstation? nmap -sS nmap -O	nmap -sT (OBJ-1: The nmap TCP connect scan (-sT) is used when the SYN scan (-sS) is not an option. You should use the -sT flag when you d not have raw packet privileges on your workstation or if you are scanning an IPv6 network. This flag tells nmap to establish a connection with the target machine by issuing the connect system call instead of using a SYN scan directly. Normally, a fast scan

nmap -sT nmap -sX	using the -sS (SYN scan) flag is more often conducted, but it requires raw socket access on the scanning workstation. The -sX flag would conduct a Xmas scan where the FIN, PSH, and URG flags are used in the scan. The -O flag would conduct an operating system detection scan of the target system.)
What SCAP component could be to create a checklist to be used by different security teams within an organization and then report results in a standardized fashion? XCCDF CCE CPE CVE	XCCDF (OBJ-2: XCCDF <extensible configuration checklist description format> is a language that is used in creating checklists for reporting results. The Common Vulnerabilities and Exposures CVE system provides a reference-method for publicly known information-security vulnerabilities and exposures. The Common Configuration Enumeration CCE provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. Common Platform Enumeration CPE is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.)
You are conducting a vulnerability assessment when you discover a critical web application vulnerability on one of your Apache servers. Which of the following files would contain the logs for this Apache server if your organization is using the default naming convention? httpd_log apache_log access_log http_log	access_log (OBJ-2: On Apache web servers, the logs are stored in a file named access_log. By default, the file can be located at /var/log/httpd/access_log. This file records all requests processed by the Apache server. The httpd_log file is used by the WebSphere Application Server for z/OS, which is a very outdated server from the early 2000s. The http_log file is actually a header class file in C used by the Apache web server's pre-compiled code that provides the logging library but does not contain any actual logs itself. The file called apache_log is actually an executable program that parses Apache log files within in Postgres database.)
Barrett needs to verify settings on a macOS computer to be sure that the configuration he expects is what is currently set on the system. What type of file is commonly used to store configuration settings for a macOS system? The registry .profile files plists .config files	plists (OBJ-3: Preference and configuration files in macOS use property lists (plists) to specify the attributes, or properties, of an app or process. An example is the preferences plist for the Finder in the Library/Preferences/ folder of a user's home folder. The file is named com.apple.finder.plist. The registry is used to store registration configuration settings on Windows systems. A profile (.profile) file is a start-up file of an UNIX user, like the autoexec.bat file of DOS. A configuration (.config) file is a configuration file used by various applications containing plain text parameters that define settings or preferences for building or running a program. This is commonly used in Windows systems.)
What sanitization technique uses only logical techniques to remove data, such as overwriting a hard drive with a random series of ones and zeroes? Purge Degauss Destroy Clear	Clear (OBJ-3: Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques. Clearing involves overwriting data once (and seldom more than three times) with repetitive data (such as all zeros) or resetting a device to factory settings. Purging data is meant to eliminate information from being feasibly recovered even in a laboratory environment. Destroy requires physical destruction of the media, such as pulverization, melting, incineration, and disintegration. Degaussing is the process of decreasing or eliminating a remnant magnetic field. Degaussing is an effective method of sanitization for magnetic media, such as hard drives and floppy disks.)
You are searching a Linux server for a possible backdoor during a forensic investigation. Which part of the file system should you	

search for evidence of a backdoor related to a Linux service? /etc/passwd /etc/xinetd.conf /etc/shadow $HOME/.ssh/	/etc/xinetd.conf OBJ-3: Linux services are started by xinetd, but some new versions use sytemctl. Therefore, the /etc/xinetd.conf should be analyzed for any evidence of a backdoor being started as part of the Linux services. Both the /etc/passwd and /etc/shadow files contain configurations that are specifically associated with individual user accounts. The /home/.ssh directory contains SSH keys for SSH-based logins.
You are deploying OpenSSL in your organization and must select a cipher suite. Which of the following ciphers should NOT be used with OpenSSL? DES AES RSA ECC	DES (OBJ-4: DES is outdated and should not be used for any modern applications. The AES, RSA, and ECC are all current secure alternatives that could be used with OpenSSL. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!)
Which of the following lists represents the four tiers of the NIST cybersecurity framework, when ordered from least mature to most mature? Partial, Risk Informed, Repeatable, Adaptive Partial, Repeatable, Risk Informed, Adaptive Partial, Risk Informed, Managed, Adaptive Partial, Managed, Risk Informed, Adaptive	Partial, Risk Informed, Repeatable, Adaptive (OBJ-4: From least mature to most mature, the NIST cybersecurity framework is Partial (tier 1), Risk Informed (tier 2), Repeatable (tier 3), and Adaptive (tier 4). This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!)
What phase of the software development lifecycle is sometimes known as the acceptance, installation, and deployment phase? Development Training and transition Operations and maintenance Disposition	Training and transition (OBJ-4: The training and transition phase ensures that end users are trained on the software and that the software has entered general use. Because of these activities, this phase is sometimes called the acceptance, installation, and deployment phase. Disposition is focused on the retirement of an application or system. Operations and maintenance is focused on the portion of the lifecycle where the application or system goes into use to provide value to the end-users. Development is the portion of the lifecycle focused on designing and coding the application or system.)
Sarah has reason to believe that systems on her network have been compromised by an APT. She has noticed a large number of file transfers outbound to a remote site via TLS-protected HTTPS sessions from unknown systems. Which of the following techniques would most likely detect the APT? Network traffic analysis	Endpoint forensics (OBJ-1: An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. APTs usually send traffic that is encrypted so that they are harder to detect

Network forensics Endpoint behavior analysis Endpoint forensics	through network traffic analysis or network forensics. This means that you need to focus on the endpoints to detect an APT. Unfortunately, APTs are very sophisticated, so endpoint behavioral analysis is unlikely to easily detect them, so Sarah will need to conduct endpoint forensics as her most likely method to detect an APT and their associated infections on her systems.)
Joseph would like to prevent hosts from connecting to known malware distribution domains. What type of solution should be used without deploying endpoint protection software or an IPS system? Route poisoning Anti-malware router filters Subdomain whitelisting DNS blackholing	DNS blackholing (OBJ-1.3: DNS blackholing is a process that uses a list of known domains/IP addresses belonging to malicious hosts and uses an internal DNS server to create a fake reply. Route poisoning prevents networks from sending data somewhere when the destination is invalid. Routers do not usually have an anti-malware filter, and this would be reserved for a unified threat management system. Subdomain whitelisting would not apply here because it would imply that you are implicitly denying all traffic and only allow whitelisted subdomains to be accessed from the hosts that would affect their operational utility to the organization.)
Which of the following types of scans are useful for probing firewall rules? TCP SYN TCP ACK TCP RST XMAS TREE	TCP ACK (OBJ-1.2: TCP ACK scans can be used to determine what services are allowed through a firewall. An ACK scan sends TCP packets with only the ACK bit set. Whether ports are open or closed, the target is required to respond with a RST packet. Firewalls that block the probe, usually make no response or send back an ICMP destination unreachable error. This distinction allows Nmap to report whether the ACK packets are being filtered. A TCP SYN scan can sometimes be used to determine what ports are filtered, but if the firewall is configured to drop packets for disallowed ports instead of sending a RST packet, then a TCP SYN scan will not be able to determine if a firewall was there or if the port was simply unavailable. A TCP RST packet is sent by a target in response to a TCP ACK scan, but a TCP RST is not a valid type of scan itself. A XMAS Tree scan will set the FIN, PSH, and URG flags in the TCP packet. This is a very noisy type of scan and not useful for probing firewall rules)
An analyst's vulnerability scanner did not have the latest set of signatures installed. Due to this, several unpatched servers may have vulnerabilities that were undetected by their scanner. You have directed the analyst to update their vulnerability scanner with the latest signatures at least 24 hours before conducting any scans, but the results of their scans still appear to be the same. Which of the following logical controls should you use to address this situation? Create a script to automatically update the signatures every 24 hours Ensure the analyst manually validates that the updates are being performed as directed Test the vulnerability remediations in a sandbox before deploying them into production Configure the vulnerability scanners to run in credentialed mode	Create a script to automatically update the signatures every 24 hours (OBJ-2: Since the analyst appears to not be installing the latest vulnerability signatures according to your instructions, it would be best to create a script and automate the process to eliminate human error. The script will always ensure that the latest signatures are downloaded and installed in the scanner every 24 hours without any human intervention. While you may want the analyst to manually validate the updates were performed as part of their procedures, this is still error-prone and likely to not be conducted properly. Regardless of whether the scanners are being run in uncredentialed or credentialed mode, they will still miss vulnerabilities if they are using out-of-date signatures. Finally, the option to test the vulnerability remediations in a sandbox is a good suggestion, but it won't solve this scenario since we are concerned with the scanning portion or vulnerability management and not remediation in this question.)
Your organization's primary operating system vendor just released a critical patch for your servers. Your system administrators have recently deployed this patch and verified the installation was successful. This critical patch was designed to remediate a vulnera-	The vulnerability assessment scan is returning a false positive This critical patch did not remediate the vulnerability (OBJ-2: There are two reasonable choices presented: (1) the vulnerability assessment scan is returning a false positive, or (2)

bility that can allow a malicious actor to remotely execute code on the server over the Internet. You ran a vulnerability scan of the network and determined that all of the servers are still being reported as having the vulnerability. You verified all your scan configurations are correct. Which of the following might be the reason that the scan report still showing the servers as vulnerability? (SELECT ALL THAT APPLY) The vulnerability assessment scan is returning a false positive This critical patch did not remediate the vulnerability You conducted the vulnerability scan without waiting long enough after the patch was installed The wrong IP address r	this critical patch did not remediate the vulnerability. It is impossible to know which based on the description in the question. If the patch was installed successfully as the question states, then it is possible that the critical patch was coded incorrectly and did not actually remediate the vulnerability. While most operating system vendors do test their patches prior to release to prevent this, with extremely critical patches, they are sometimes rushed into production and the patch does not actually remediate the vulnerability on all systems. When this occurs, the vendor will issue a subsequent patch will be released to fix it and superseded the original patch. The other option is that the vulnerability assessment tool is incorrectly configured and is returning a false positive. This can occur when the signature used to detect the vulnerability is too specific or too generic to actually detect whether the system was patched for the vulnerability or not. The other options are incorrect, as you do not have to wait a certain period of time after installation before scanning, and it is assumed that you are scanning the same IP range both times as you have verified your scan configuration.)
You have run a vulnerability scan and received the following output:-=- CVE-2011-3389 QID 42366 - SSLv3.0/TLSv1.0 Protocol weak CBC mode Server side vulnerability Check with: openssl s_client -connect login.diontraining.com:443 - tls -cipher "AES:CAMELLISA:SEED:3DES:DES" -=- Which of the following categories should this be classified as? PKI transfer vulnerability Active Directory encryption vulnerability Web application cryptography vulnerability VPN tunnel vulnerability	Web application cryptography vulnerability (OBJ-2: This vulnerability should be categories as a web application cryptographic vulnerability. This is shown by the weak SSLv3.0/TLSv1.0 protocol being used in cipher block chaining (CBC) mode. Specifically, the use of the 3DES and DES algorithms during negotiation is a significant vulnerability. A stronger protocol should be used, such as forcing the use of AES.)
In a CVSS metric, which of the following is NOT one of the factors that comprise the base score for a given vulnerability? Access vector Authentication Access complexity Availability	Authentication (OBJ-2: In CVSS 3.1, the base metric is comprised of 8 factors: access vector (AV), access complexity (AC), privileges required (PR), user interaction (UI), scope (S), confidentiality (C), integrity (I), and availability (A).)
Jay is replacing his organization's current vulnerability scanner with a new tool. As he begins to create the scanner's configurations and scanning policy, he notices a conflict in the settings recommended between different documents. Which of the following sources must Jay follow when trying to resolve these conflicts? NIST guideline documents Vendor best practices Corporate policy Configuration settings from the prior system	Corporate policy (OBJ-2: Policies are formalized statements that apply to a specific area or task. Policies are mandatory and employees who violate a policy may be disciplined. Guidelines are general, non-mandatory recommendations. Best practices are considered procedures that are accepted as being correct or most effective, but are not mandatory to be followed. Configuration settings from the prior system could be helpful, but again, this is not a mandatory compliance area like a policy would be. Therefore, Jay should first follow the policy before the other three options if there is a conflict between them.)

Which of the following methods could not be used to retrieve the key from a forensic copy of a BitLocker encrypted drive? Analyzing the hibernation file Analyzing the memory dump file Retrieving the key from the MBR Performing a FireWire attack on mounted drives	Retrieving the key from the MBR (OBJ-3: BitLocker information is not stored in the Master Boot Record (MBR). Therefore, you cannot retrieve the key from the MBR. BitLocker keys can also be retrieved via hibernation files or memory dumps. The recovery key may also be retrieved by conducting a FireWire attack on the mounted drive using a side-channel attack known as a DMA attack. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal is not to score 100% on the exam; it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!)
You are a cybersecurity analyst and your company has just enabled key-based authentication on its SSH server. Review the following log file: -=- BEGIN LOG ---------- Sep 09 13:15:24 diontraining sshd[3423]: Failed password for root from 192.168.3.2 port 45273 ssh2 Sep 09 15:43:15 diontraining sshd[3542]: Failed password for root from 192.168.2.24 port 43543 ssh2 Sep 09 15:43:24 diontraining sshd[3544]: Failed password for jdion from 192.168.2.24 port 43589 ssh2 Sep 09 15:43:31 diontraining sshd[3546]: Failed password for tmartinez from 192.168.2.24 port 43619 ssh2 Sep 09 15:43:31 diontraining sshd[3546]: Failed password for jdion from 192.168.2.24 port 43631 ssh2 Sep 09 15:43:37 diontraining sshd[3548]: Failed password for root from 192.168.2.24 port 43657 ssh2 ——————————-- END LOG-=-Which of the following actions should be p	Disable password authentication for SSH (OBJ-3: It is common for attackers to attempt to log in remotely using the ssh service and the root or other user accounts. The best way to protect your server is to disable password authentication over ssh. Since your company just enabled key-based authentication on the SSH server, all legitimate users should be logging in using their RSA key pair on their client machines, not usernames and passwords. Based on the logs, you see the server is running SSHv2, so there is no need to disable SSHv1 (it may already be disabled). You don't want to fully disable remote root SSH logons, either, since this would make it difficult for administrators to conduct their work. Finally, based on the logs, it doesn't appear that anonymous SSH logons are an issue, either, as we don't see any anonymous attempts in the logs.)
Jamie's organization is attempting to budget for the next fiscal year. Jamie has calculated that a data breach will cost them $120,000 for each occurrence. Based on her analysis, she believes that a data breach will occur once every four years and have a risk factor is 30%. What is the ALE for a data breach within Jamie's organization? $9,000 $36,000 $90,000 $360,000	$9,000 (OBJ-3: The single loss expectancy (SLE) is the amount that would be lost in a single occurrence (AV) times the risk factor (RF). The annual loss expectancy (ALE) is the total cost of a risk to an organization on an annual basis. This is determined by multiplying the SLE by the annual rate of occurrence (ARO).SLE = AV x RF = $120,000 x 0.3 = $36,000ALE = SLE x ARO = $36,000 x 0.25 = $9,000)
Which of the following should a domain administrator utilize to best protect their Windows workstations from buffer overflow attacks? Install an anti-malware tool Install an anti-spyware tool Enable DEP in Windows	Enable DEP in Windows (OBJ-3: Windows comes with DEP, which is a built-in memory protection resource. This prevents code from being run in pages that are marked for nonexecutable. DEP, by default, only protects Windows programs and services classified as essential, but it can be used for all programs and services, or all programs and services except the ones on an exception list. Anti-virus and anti-malware cannot prevent buffer overflow attacks from zero-days, but DEP can. Bounds checking is an effective way to prevent buffer overflows, but this must be written into the programs

Conduct bound checking before executing a program	being installed. Therefore, bounds checking is not something a domain administrator can do on their own; it must be done by each software manufacturer.)
Which tool should a malware analyst utilize to track the changes made to the registry and the file system while running a suspicious executable on a Windows system? ProcDump DiskMon Process Monitor Autoruns	Process Monitor (OBJ-3: Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry, and process/thread activity. Autoruns shows you what programs are configured to run during system bootup or login. ProcDump is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike. DiskMon is an application that logs and displays all hard disk activity on a Windows system. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role.)
Which of the following security policies could help detect fraudulent cases that occur even when other security controls are already in place? Separation of duties Least privilege Dual control Mandatory vacations	Mandatory vacations (OBJ-4: Mandatory vacation policies require employees to take time away from their job and help to detect fraud or malicious activities. Even if other controls such as separation of duties, least privilege, and dual control are used, an employee could still collude with others to conduct fraud. By utilizing mandatory vacation policies, this fraud can often be discovered since a new person will be conducting the duties assigned to the person on vacation. Separation of duties is the concept of having more than one person required to complete a particular task to prevent fraud and error. Dual control, instead, requires both people to perform the action together. For example, a nuclear missile system uses dual control and requires two people to each turn a different key simultaneously to allow for a missile launch to occur. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.)
What describes the infrastructure needed to support the other architectural domains in the TOGAF framework? Business architecture Applications architecture Data architecture Technical architecture	Technical architecture (OBJ-4: TOGAF is a prescriptive framework that divides the enterprise architecture into four domains. Technical architecture describes the infrastructure needed to support the other architectural domains. Business architecture defines governance and organization and explains the interaction between enterprise architecture and business strategy. Applications architecture includes the applications and systems an organization deploys, the interactions between those systems, and their relation to business processes.)
A web developer wants to protect their new web application from a man-in-the-middle attack. Which of the following controls would best prevent an attacker from stealing tokens stored in cookies? Forcing the use of TLS for the web application Forcing the use of SSL for the web application Setting the secure attribute on the cookie Hashing the cookie value	Setting the secure attribute on the cookie (OBJ-4: When a cookie has the Secure attribute, the user agent includes the cookie in an HTTP request only if the request is transmitted over a secure channel (typically HTTPS). Although seemingly useful for protecting cookies from active network attackers, the Secure attribute protects only the cookie's confidentiality. Forcing the web application to use TLS or SSL does not force the cookie to be sent over TLS/SSL, so you still would need to set the Secure attribute on the cookie. Hashing the cookie provides integrity of the cookie, not confidentiality; therefore, it will not solve the issue presented by this question.)

CySA+ Exam Questions 1

Study online at https://quizlet.com/_fjwtoz

Which of the following is not normally part of an endpoint security suite? IPS Software firewall Anti-virus VPN	VPN (OBJ-4: Endpoint security includes software host-based firewalls, host-based intrusion protection systems (HIPS), and anti-virus software. A VPN is not typically considered an endpoint security tool because it is a network security tool.)
James is working with the software development team to integrate some real-time security reviews into some of their SDLC processes. Which of the following would best meet this requirement? Pair Programming Pass-around code review Tool-assisted review Formal code review	Pair Programming (Pair programming is a real-time process that would meet this requirement. It utilizes two developers working on one workstation, where one developer reviews the code being written in real-time by the other developer. While the other three options can also provide a security review, none of them are considered "real-time" since they are asynchronous processes that are performed after the coding has already been completed})
Which one of the following is an open-source forensic tool suite? FTK EnCase SIFT Helix	SIFT (The SIFT (SANS investigative forensics toolkit) Workstation is a group of free, open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated. FTK, EnCase, and Helix are all commercially available tools.)
Which of the following is not considered a component that belongs to the category of identity management infrastructure? Human resource system LDAP Provisioning engine Auditing system	Human resource system (OBJ-4: The human resource system may be a data source for identity management, but it is not part of the infrastructure itself. LDAP servers, provisioning engines, and auditing systems are all part of identity management infrastructures. Most organizations rely on a LDAP Directory to store users, groups, roles, and relationships between those entities. A provisioning engine is responsible for the process of coordinating the creation of user accounts, email authorizations in the form of rules and roles, and other tasks such as provisioning of physical resources associated with enabling new users. The auditing system is responsible for verifying the identities present in the organization's systems are valid and correct.)