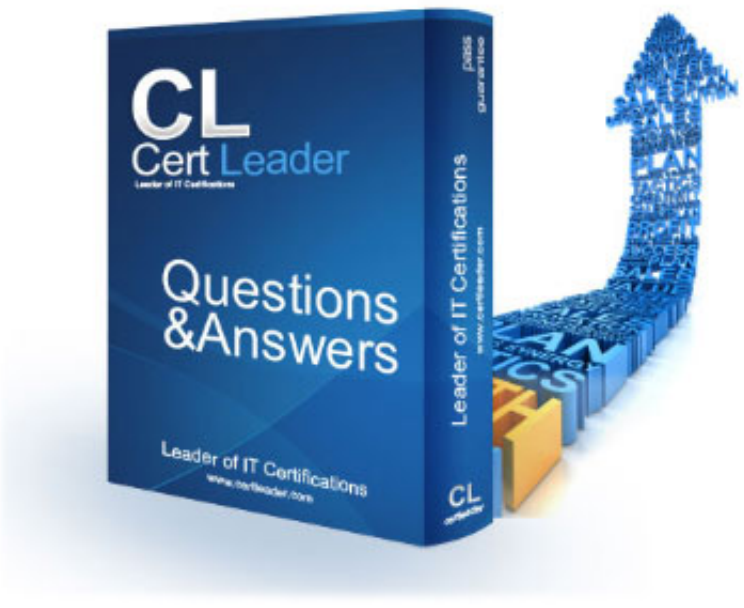
CAS-003 Dumps

CompTIA Advanced Security Practitioner (CASP)

https://www.certleader.com/CAS-003-dumps.html



NEW QUESTION 1
A security engineer has been hired to design a device that will enable the exfiltration of data from within a well-defended network perimeter during an authorized test. The device must bypass all firewalls and NIDS in place, as well as allow for the upload of commands from a centralized command and control answer. The total cost of the device must be kept to a minimum in case the device is discovered during an assessment. Which of the following tools should the engineer load onto the device being designed?

A. Custom firmware with rotating key generation
B. Automatic MITM proxy
C. TCP beacon broadcast software
D. Reverse shell endpoint listener

Answer: B

NEW QUESTION 2
An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:
1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of the company's geographical location
The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project's security consultant recommend as the NEXT step?

A. Develop a security exemption, as it does not meet the security policies
B. Mitigate the risk by asking the vendor to accept the in-country privacy principles
C. Require the solution owner to accept the identified risks and consequences
D. Review the entire procurement process to determine the lessons learned

Answer: C

NEW QUESTION 3
A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:
The data is for internal consumption only and shall not be distributed to outside individuals The systems administrator should not have access to the data processed by the server
The integrity of the kernel image is maintained
Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

A. SELinux
B. DLP
C. HIDS
D. Host-based firewall
E. Measured boot
F. Data encryption
G. Watermarking

Answer: CEF

NEW QUESTION 4
A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

A. ISA
B. BIA
C. SLA
D. RA

Answer: C

NEW QUESTION 5
Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
 Link-local IPv6 Address..... : fe80::4551:67ba:77a6:62e1%11
 IPv4 Address................ : 172.30.0.28
 Subnet Mask................. : 255.255.0.0
 Default Gateway............. : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

A. Allow 172.30.0.28:80 -> ANY
B. Allow 172.30.0.28:80 -> 172.30.0.0/16

C. Allow 172.30.0.28:80 -> 172.30.0.28:443
D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Answer: B

NEW QUESTION 6
A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

A. Set up a VDI environment that prevents copying and pasting to the local workstations ofoutsourced staff members
B. Install a client-side VPN on the staff laptops and limit access to the development network
C. Create an IPSec VPN tunnel from the development network to the office of the outsourced staff
D. Use online collaboration tools to initiate workstation-sharing sessions with local staff who have access to the development network

Answer: D

NEW QUESTION 7
A systems security engineer is assisting an organization's market survey team in reviewing requirements for an upcoming acquisition of mobile devices. The engineer expresses concerns to the survey team about a particular class of devices that uses a separate SoC for baseband radio I/O. For which of the following reasons is the engineer concerned?

A. These devices can communicate over networks older than HSPA+ and LTE standards, exposing device communications to poor encryptions routines
B. The organization will be unable to restrict the use of NFC, electromagnetic induction, and Bluetooth technologies
C. The associated firmware is more likely to remain out of date and potentially vulnerable
D. The manufacturers of the baseband radios are unable to enforce mandatory access controls within their driver set

Answer: B

NEW QUESTION 8
A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

A. Patch management
B. Antivirus
C. Application firewall
D. Spam filters
E. HIDS

Answer: E

NEW QUESTION 9
A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

A. OTA updates
B. Remote wiping
C. Side loading
D. Sandboxing
E. Containerization
F. Signed applications

Answer: EF

NEW QUESTION 10
A security incident responder discovers an attacker has gained access to a network and has overwritten key system files with backdoor software. The server was reimaged and patched offline. Which of the following tools should be implemented to detect similar attacks?

A. Vulnerability scanner
B. TPM
C. Host-based firewall
D. File integrity monitor
E. NIPS

Answer: CD

NEW QUESTION 10
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat

C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Answer: A

NEW QUESTION 11
A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

Antivirus	Enabled
AV Engine	Current
AV Signatures	Auto Update
Update Status	Success
Heuristic Scanning	Enabled
Scan Type	On Access Scanning
Malware Engine	Enabled
Auto System Update	Enabled
Last System Update	Yesterday 2 PM
DLP Agent	Disabled
DLP DB Update	Poll every 5 mins
Proxy Settings	Auto

Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)

A. Install HIPS
B. Enable DLP
C. Install EDR
D. Install HIDS
E. Enable application blacklisting
F. Improve patch management processes

Answer: BE

NEW QUESTION 15
An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability explogted in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

A. Deploy virtual desktop infrastructure with an OOB management network
B. Employ the use of vTPM with boot attestation
C. Leverage separate physical hardware for sensitive services and data
D. Use a community CSP with independently managed security services
E. Deploy to a private cloud with hosted hypervisors on each physical machine

Answer: AC

NEW QUESTION 16
After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:
Duplicate IP addresses Rogue network devices
Infected systems probing the company's network
Which of the following should be implemented to remediate the above issues? (Choose two.)

A. Port security
B. Route protection
C. NAC
D. HIPS
E. NIDS

Answer: BC

NEW QUESTION 21
A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

A. Call the CIO and ask for an interview, posing as a job seeker interested in an open position
B. Compromise the email server to obtain a list of attendees who responded to the invitation who is on the IT staff
C. Notify the CIO that, through observation at events, malicious actors can identify individuals to befriend
D. Understand the CIO is a social drinker, and find the means to befriend the CIO at establishments the CIO frequents

Answer: D

NEW QUESTION 26
A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:
High-impact controls implemented: 6 out of 10 Medium-impact controls implemented: 409 out of 472 Low-impact controls implemented: 97 out of 1000
The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:
Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000
Average medium-impact control implementation cost: $6,250; Probable ALE for each mediumimpact control gap: $11,000
Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the past
B. The enterprise security team has focused exclusively on mitigating high-level risks
C. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controls
D. The cybersecurity team has balanced residual risk for both high and medium controls

Answer: C

NEW QUESTION 30
A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit. Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence. The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?

A. Update and deploy GPOs
B. Configure and use measured boot
C. Strengthen the password complexity requirements
D. Update the antivirus software and definitions

Answer: D

NEW QUESTION 33
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:
The tool needs to be responsive so service teams can query it, and then perform an automated response action.
The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.
Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

Answer: BCE

NEW QUESTION 38
A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

A. Inform the customer that the service provider does not have any control over third-party blacklist entrie
B. The customer should reach out to the blacklist operator directly
C. Perform a takedown of any customer accounts that have entries on email blacklists because this is a strong indicator of hostile behavior
D. Work with the legal department and threaten legal action against the blacklist operator if the netblocks are not removed because this is affecting legitimate traffic
E. Establish relationship with a blacklist operators so broad entries can be replaced with more granular entries and incorrect entries can be quickly pruned

Answer: D

NEW QUESTION 42
A company is developing requirements for a customized OS build that will be used in an embedded environment. The company procured hardware that is capable of reducing the likelihood of successful buffer overruns while executables are processing. Which of the following capabilities must be included for the OS to take advantage of this critical hardware-based countermeasure?

A. Application whitelisting
B. NX/XN bit
C. ASLR
D. TrustZone
E. SCP

Answer: B

NEW QUESTION 47
A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: “<object object_ref=… />” and “<state state_ref=… />”. Which of the following tools BEST supports the use of these definitions?

A. HTTP interceptor
B. Static code analyzer
C. SCAP scanner
D. XML fuzzer

Answer: D

NEW QUESTION 50
A deployment manager is working with a software development group to assess the security of a
new version of the organization’s internally developed ERP tool. The organization prefers to not perform assessment activities following deployment, instead focusing on assessing security throughout the life cycle. Which of the following methods would BEST assess the security of the product?

A. Static code analysis in the IDE environment
B. Penetration testing of the UAT environment
C. Vulnerability scanning of the production environment
D. Penetration testing of the production environment
E. Peer review prior to unit testing

Answer: C

NEW QUESTION 51
An architect was recently hired by a power utility to increase the security posture of the company’s power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources.
Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

A. Isolate the systems on their own network
B. Install a firewall and IDS between systems and the LAN
C. Employ own stratum-0 and stratum-1 NTP servers
D. Upgrade the software on critical systems
E. Configure the systems to use government-hosted NTP servers

Answer: BE

NEW QUESTION 53
A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:
Store taxation-related documents for five years Store customer addresses in an encrypted format Destroy customer information after one year Keep data only in the customer’s home country
Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

A. Capacity planning policy
B. Data retention policy
C. Data classification standard
D. Legal compliance policy
E. Data sovereignty policy
F. Backup policy
G. Acceptable use policy
H. Encryption standard

Answer: BCH

NEW QUESTION 55
A company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

A. Use a protocol analyzer against the site to see if data input can be replayed from the browser
B. Scan the website through an interception proxy and identify areas for the code injection
C. Scan the site with a port scanner to identify vulnerable services running on the web server
D. Use network enumeration tools to identify if the server is running behind a load balancer

Answer: C

NEW QUESTION 58
A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches

C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

Answer: CD

NEW QUESTION 60
The code snippet below controls all electronic door locks to a secure facility in which the doors should only fail open in an emergency. In the code, “criticalValue” indicates if an emergency is underway:

```
try {
      if (criticalValue)
            openDoors=true
      else
            OpenDoors=false
} catch (e) {
      OpenDoors=true
}
```

Which of the following is the BEST course of action for a security analyst to recommend to the software developer?

A. Rewrite the software to implement fine-grained, conditions-based testing
B. Add additional exception handling logic to the main program to prevent doors from being opened
C. Apply for a life-safety-based risk exception allowing secure doors to fail open
D. Rewrite the software’s exception handling routine to fail in a secure state

Answer: B

NEW QUESTION 65
A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.
Which of the following methods could be used in addition to an integrated development environment to reduce the severity of the issue?

A. Conduct a penetration test on each function as it is developed
B. Develop a set of basic checks for common coding errors
C. Adopt a waterfall method of software development
D. Implement unit tests that incorporate static code analyzers

Answer: D

NEW QUESTION 68
To meet a SLA, which of the following document should be drafted, defining the company’s internal interdependent unit responsibilities and delivery timelines.

A. BPA
B. OLA
C. MSA
D. MOU

Answer: B

Explanation:
OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

NEW QUESTION 69
A security analyst sees some suspicious entries in a log file from a web server website, which has a form that allows customers to leave feedback on the company’s products. The analyst believes a malicious actor is scanning the web form. To know which security controls to put in place, the analyst first needs to determine the type of activity occurring to design a control. Given the log below:

Timestamp	SourceIP	CustName	PreferredContact	ProdName	Comments
Monday 10:00:04	10.14.34.55	aaaaa	Phone	Widget1	None left
Monday 10:00:04	10.14.34.55	bbbbb	Phone	Widget1	None left
Monday 10:00:05	10.14.34.55	cccc	Phone	Widget1	../../etc/passwd
Monday 10:01:03	10.14.34.55	ddddd	Phone	Widget1	None left
Monday 10:01:04	10.14.34.55	eeeee	Phone	Widget1	None left
Monday 10:01:05	10.14.34.55	fffff	Phone	Widget1	1=1
Monday 10:03:05	172.16.34.20	Joe	Phone	Widget30	Love the Widget!
Monday 10:04:01	10.14.34.55	ggggg	Phone	Widget1	<script>
Monday 10:05:05	10.14.34.55	hhhhh	Phone	Widget1	wget cookie
Monday 10:05:05	10.14.34.55	iiiii	Phone	Widget1	None left
Monday 10:05:06	10.14.34.55	lllll	Phone	Widget1	None left

Which of the following is the MOST likely type of activity occurring?

A. SQL injection
B. XSS scanning
C. Fuzzing
D. Brute forcing

Answer: A

NEW QUESTION 72
An organization has established the following controls matrix:

	Minimum	Moderate	High
Physical Security	Cylinder Lock	Cipher Lock	Proximity Access Card
Environmental Security	Surge Protector	UPS	Generator
Data Security	Context-Based Authentication	MFA	FDE
Application Security	Peer Review	Static Analysis	Penetration Testing
Logical Security	HIDS	NIDS	NIPS

The following control sets have been defined by the organization and are applied in aggregate fashion:
Systems containing PII are protected with the minimum control set. Systems containing medical data are protected at the moderate level. Systems containing cardholder data are protected at the high level.
The organization is preparing to deploy a system that protects the confidentially of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

A. Proximity card access to the server room, context-based authentication, UPS, and full-disk encryption for the database server.
B. Cipher lock on the server room door, FDE, surge protector, and static analysis of all application code.
C. Peer review of all application changes, static analysis of application code, UPS, and penetration testing of the complete system.
D. Intrusion detection capabilities, network-based IPS, generator, and context-based authenticatio

Answer: D

NEW QUESTION 76
A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh. Which of the following is the BEST way to address these issues and mitigate risks to the organization?

A. Purchase the SSL, decryption license for the firewalls and route traffic back to the proxies for enduser categorization and malware analysis.
B. Roll out application whitelisting to end-user desktops and decommission the existing proxies, freeing up network ports.
C. Use an EDP solution to address the malware issue and accept the diminishing role of the proxy for URL categorization in the short team.
D. Accept the current risk and seek possible funding approval in the next budget cycle to replace the existing proxies with ones with more capacity.

Answer: B

NEW QUESTION 79
A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded. Which of the following should be used to identify weak processes and other vulnerabilities?

A. Gap analysis
B. Benchmarks and baseline results
C. Risk assessment
D. Lessons learned report

Answer: D

NEW QUESTION 84
The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloud-based log aggregation solution for all traffic that is logged. Which of the following presents a long-term risk to user privacy in this scenario?

A. Confidential or sensitive documents are inspected by the firewall before being logged.
B. Latency when viewing videos and other online content may increase.
C. Reports generated from the firewall will take longer to produce due to more information from inspected traffic.
D. Stored logs may contain non-encrypted usernames and passwords for personal website

Answer: A

NEW QUESTION 88
A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials. Which of the following tools should be used? (Choose two.)

A. Fuzzer
B. SCAP scanner
C. Packet analyzer
D. Password cracker
E. Network enumerator
F. SIEM

Answer: BF

NEW QUESTION 89
A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers. Which of the following BEST describes the contents of the supporting document the engineer is creating?

A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.
B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.
C. A set of formal methods that apply to one or more of the programing languages used on the development project.
D. A methodology to verify each security control in each unit of developed code prior to committing the code.

Answer: D

NEW QUESTION 91
An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following requirements:
Active full-device encryption Enabled remote-device wipe Blocking unsigned applications
Containerization of email, calendar, and contacts
Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements?

A. Require frequent password changes and disable NFC.
B. Enforce device encryption and activate MAM.
C. Install a mobile antivirus application.
D. Configure and monitor devices with an MD

Answer: B

NEW QUESTION 96
While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use.
Additionally, each password has specific complexity requirements and different expiration time frames. Which of the following would be the BEST solution for the information security officer to recommend?

A. Utilizing MFA
B. Implementing SSO
C. Deploying 802.1X
D. Pushing SAML adoption
E. Implementing TACACS

Answer: B

NEW QUESTION 97
Which of the following is the GREATEST security concern with respect to BYOD?

A. The filtering of sensitive data out of data flows at geographic boundaries.
B. Removing potential bottlenecks in data transmission paths.
C. The transfer of corporate data onto mobile corporate devices.
D. The migration of data into and out of the network in an uncontrolled manne

Answer: D

NEW QUESTION 100
A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device.
Additionally, to protect patients' health information, management has identified the following requirements:
Data must be encrypted at rest.
The device must be disabled if it leaves the facility. The device must be disabled when tampered with
Which of the following technologies would BEST support these requirements? (Select two.)

A. eFuse
B. NFC
C. GPS
D. Biometric
E. USB 4.1
F. MicroSD

Answer: CD

NEW QUESTION 102
A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company's RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:
An HOTP service is installed on the RADIUS server.
The RADIUS server is configured to require the HOTP service for authentication.
The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor.
Which of the following should be implemented to BEST resolve the issue?

A. Replace the password requirement with the second facto
B. Network administrators will enter their username and then enter the token in place of their password in the password field.
C. Configure the RADIUS server to accept the second factor appended to the passwor
D. Network administrators will enter a password followed by their token in the password field.
E. Reconfigure network devices to prompt for username, password, and a toke
F. Network administrators will enter their username and password, and then they will enter the token.
G. Install a TOTP service on the RADIUS server in addition to the HOTP servic
H. Use the HOTP on older devices that do not support two-factor authenticatio
I. Network administrators will use a web portalto log onto these device

Answer: B

NEW QUESTION 103
Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the requirements that it be easy to manage and provide capacity for growth.
The tables below provide information on a subset of remote sites and the firewall options:

Location	# of Users	Connectivity	Bandwidth Utilization
St.Louis	18	50 Mbps	20 Mbps
Des Moines	12	25 Mbps	19 Mbps
Chicago	27	100 Mbps	41 Mbps
Rapid City	6	10 Mbps	8 Mbps
Indianapolis	7	12 Mbps	8 Mbps

Vendor	Maximum Recommended Devices	Firewall Throughput	Full UTM?	Centralized Management Available?
A	40	150 Mbps	Y	Y
B	60	400 Mbps	N	Y
C	25	200 Mbps	N	N
D	25	100 Mbps	Y	Y

Which of the following would be the BEST option to recommend to the CIO?

A. Vendor C for small remote sites, and Vendor B for large sites.
B. Vendor B for all remote sites
C. Vendor C for all remote sites
D. Vendor A for all remote sites
E. Vendor D for all remote sites

Answer: D

NEW QUESTION 108
A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.
Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?

A. Check for any relevant or required overlays.
B. Review enhancements within the current control set.
C. Modify to a high-baseline set of controls.
D. Perform continuous monitorin

Answer: C

NEW QUESTION 113
A security researches is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.
Based on the information available to the researcher, which of the following is the MOST likely threat profile?

A. Nation-state-sponsored attackers conducting espionage for strategic gain.
B. Insiders seeking to gain access to funds for illicit purposes.
C. Opportunists seeking notoriety and fame for personal gain.
D. Hackvisits seeking to make a political statement because of socio-economic factor

Answer: D

NEW QUESTION 116
A security analyst is inspecting pseudocode of the following multithreaded application:
1. perform daily ETL of data
1.1 validate that yesterday's data model file exists
1.2 validate that today's data model file does not exist
1.2 extract yesterday's data model
1.3 transform the format
1.4 load the transformed data into today's data model file
1.5 exit
Which of the following security concerns is evident in the above pseudocode?

A. Time of check/time of use
B. Resource exhaustion
C. Improper storage of sensitive data
D. Privilege escalation

Answer: A

NEW QUESTION 118
An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations. Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

A. Malicious insiders will not have the opportunity to tamper with data at rest and affect the integrity of the system.
B. Thin client workstations require much less security because they lack storage and peripherals that can be easily compromised, and the virtual workstations are protected in the cloud where security is outsourced.
C. All thin clients use TPM for core protection, and virtual workstations use vTPM for core protection with both equally ensuring a greater security advantage for a cloud-hosted environment.
D. Malicious users will have reduced opportunities for data extractions from their physical thin client workstations, this reducing the effectiveness of local attacks.

Answer: B

NEW QUESTION 120
A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:
1. Information should be sourced from the trusted master data source.
2. There must be future requirements for identity proofing of devices and users.
3. A generic identity connector that can be reused must be developed.
4. The current project scope is for internally hosted applications only.
Which of the following solution building blocks should the security architect use to BEST meet the requirements?

A. LDAP, multifactor authentication, oAuth, XACML
B. AD, certificate-based authentication, Kerberos, SPML
C. SAML, context-aware authentication, oAuth, WAYF
D. NAC, radius, 802.1x, centralized active directory

Answer: A

NEW QUESTION 124
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: nonsensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive. Which of
the following actions should the engineer take regarding the data?

A. Label the data as extremely sensitive.
B. Label the data as sensitive but accessible.
C. Label the data as non-sensitive.
D. Label the data as sensitive but export-controlle

Answer: C

NEW QUESTION 129
The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues. Which of the following is the MOST important information to reference in the letter?

A. After-action reports from prior incidents.
B. Social engineering techniques
C. Company policies and employee NDAs
D. Data classification processes

Answer: C

NEW QUESTION 131
The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other user's emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes. Which of the following tools would show this type of output?

A. Log analysis tool
B. Password cracker
C. Command-line tool
D. File integrity monitoring tool

Answer: A

NEW QUESTION 135
An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

A. Following new requirements that result from contractual obligations
B. Answering requests from auditors that relate to e-discovery
C. Responding to changes in regulatory requirements
D. Developing organizational policies that relate to hiring and termination procedures

Answer: C

NEW QUESTION 136
Company.org has requested a black-box security assessment be performed on key cyber terrain. On area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing. Which of the following commands should the assessor use to determine this information?

A. dnsrecon –d company.org –t SOA
B. dig company.org mx
C. nc –v company.org
D. whois company.org

Answer: A

NEW QUESTION 138

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant.
All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

A. System design documentation
B. User acceptance testing
C. Peer review
D. Static code analysis testing
E. Change control documentation

Answer: A

NEW QUESTION 141
An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:
Encrypt all traffic between the network engineer and critical devices. Segregate the different networking planes as much as possible.
Do not let access ports impact configuration tasks.
Which of the following would be the BEST recommendation for the network security engineer to present?

A. Deploy control plane protections.
B. Use SSH over out-of-band management.
C. Force only TACACS to be allowed.
D. Require the use of certificates for AAA.

Answer: B

NEW QUESTION 143
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:
1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications
Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

A. IPSec VPN
B. HIDS
C. Wireless controller
D. Rights management
E. SSL VPN
F. NAC
G. WAF
H. Load balancer

Answer: DEF

NEW QUESTION 144
A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.
Which of the following solutions BEST meets all of the architect's objectives?

A. An internal key infrastructure that allows users to digitally sign transaction logs
B. An agreement with an entropy-as-a-service provider to increase the amount of randomness in generated keys.
C. A publicly verified hashing algorithm that allows revalidation of message integrity at a future date.
D. An open distributed transaction ledger that requires proof of work to append entrie

Answer: A

NEW QUESTION 148
The government is concerned with remote military missions being negatively being impacted by the use of technology that may fail to protect operational security.
To remediate this concern, a number of solutions have been implemented, including the following:
End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.
Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications
A host-based whitelist of approved websites and applications that only allow mission-related tools and sites
The use of satellite communication to include multiple proxy servers to scramble the source IP address
Which of the following is of MOST concern in this scenario?

A. Malicious actors intercepting inbound and outbound communication to determine the scope of the mission
B. Family members posting geotagged images on social media that were received via email from soldiers
C. The effect of communication latency that may negatively impact real-time communication with mission control
D. The use of centrally managed military network and computers by soldiers when communicating with external parties

Answer: A

NEW QUESTION 149

Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back. Which of the following BEST describes how the manager should respond?

A. Determine if the data still exists by inspecting to ascertain if the laptop has already been wiped and if the storage team has recent backups.
B. Inform Ann that the laptop was for company data only and she should not have stored personal photos on a company asset.
C. Report the email because it may have been a spoofed request coming from an attacker who is trying to exfiltrate data from the company laptop.
D. Consult with the legal and/or human resources department and check company policies around employment and termination procedures.

Answer: D

NEW QUESTION 152
A cybersecurity analyst is hired to review the security the posture of a company. The cybersecurity analyst notice a very high network bandwidth consumption due to SYN floods from a small number of IP addresses. Which of the following would be the BEST action to take to support incident response?

A. Increase the company's bandwidth.
B. Apply ingress filters at the routers.
C. Install a packet capturing tool.
D. Block all SYN packet

Answer: B

NEW QUESTION 155
A technician receives the following security alert from the firewall's automated system: Match_Time: 10/10/16 16:20:43
Serial: 002301028176
Device_name: COMPSEC1 Type: CORRELATION
Scrusex: domain\samjones Scr: 10.50.50.150
Object_name: beacon detection Object_id: 6005
Category: compromised-host Severity: medium
Evidence: host repeatedly visited a dynamic DNS domain (17 time) After reviewing the alert, which of the following is the BEST analysis?

A. the alert is a false positive because DNS is a normal network function.
B. this alert indicates a user was attempting to bypass security measures using dynamic DNS.
C. this alert was generated by the SIEM because the user attempted too many invalid login attempts.
D. this alert indicates an endpoint may be infected and is potentially contacting a suspect hos

Answer: B

NEW QUESTION 156
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After invest the new vulnerability, it was determined that the web services providing are being impacted by this new threat. Which of the following data types a MOST likely at risk of exposure based on this new threat? (Select TWO)

A. Cardholder data
B. intellectual property
C. Personal health information
D. Employee records
E. Corporate financial data

Answer: AC

NEW QUESTION 161
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines. Which of the following represents a FINAL step in the prediction of the malware?

A. The workstations should be isolated from the network.
B. The workstations should be donated for refuse.
C. The workstations should be reimaged
D. The workstations should be patched and scanne

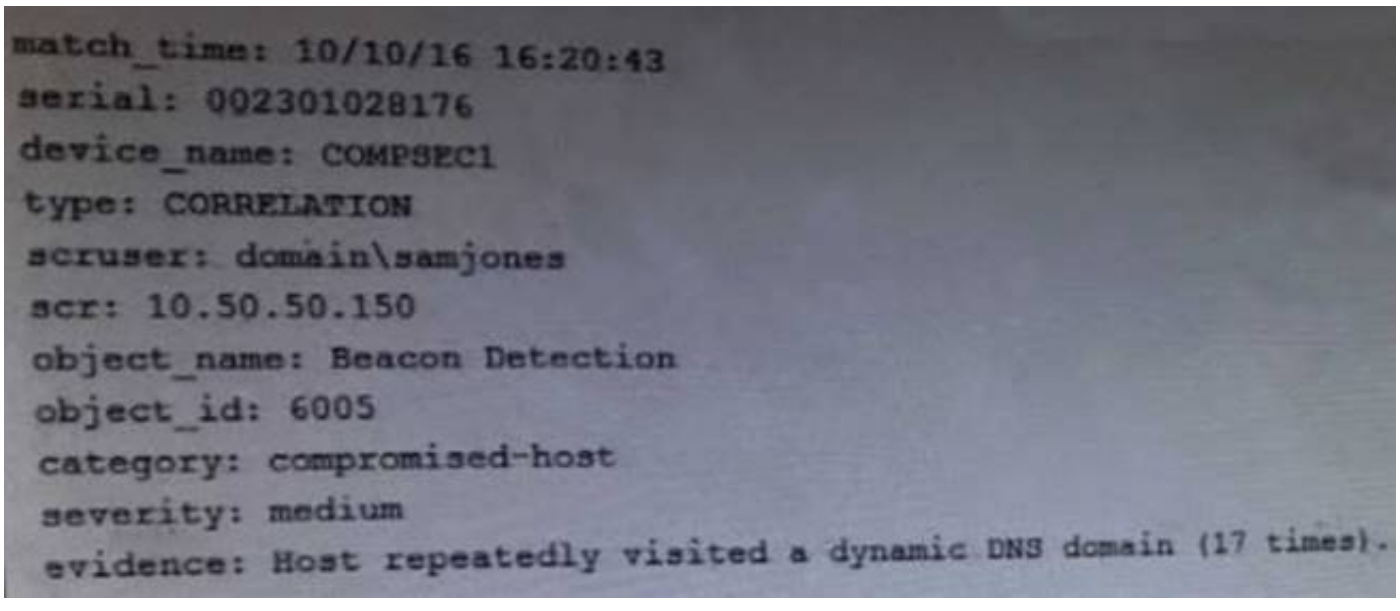
Answer: C

NEW QUESTION 165
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancements to the company's cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

A. OSSM
B. NIST
C. PCI
D. OWASP

Answer: B

NEW QUESTION 167
A technician receives the following security alert from the firewall's automated system:



After reviewing the alert, which of the following is the BEST analysis?

A. This alert is false positive because DNS is a normal network function.
B. This alert indicates a user was attempting to bypass security measures using dynamic DNS.
C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.
D. This alert indicates an endpoint may be infected and is potentially contacting a suspect hos

Answer: B

NEW QUESTION 168
An investigation showed a worm was introduced from an engineer's laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to a company policy and technical controls. Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.
B. Implement role-based group policies on the management network for client access.
C. Utilize a jump box that is only allowed to connect to client from the management network.
D. Deploy a company-wide approved engineering workstation for management acces

Answer: A

NEW QUESTION 172
A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

A. Refuse LM and only accept NTLMv2
B. Accept only LM
C. Refuse NTLMv2 and accept LM
D. Accept only NTLM

Answer: A

Explanation:
In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.
This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.
Incorrect Answers:
B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.
C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.
D: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not NTLM (version1). References: https://en.wikipedia.org/wiki/NT_LAN_Manager

NEW QUESTION 176
Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

A. Integer overflow
B. Click-jacking
C. Race condition
D. SQL injection
E. Use after free
F. Input validation

Answer: E

Explanation:
Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.
Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.
According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."
Incorrect Answers:
A: Integer overflow is the result of an attempt by a CPU to arithmetically generate a number larger than what can fit in the devoted memory storage space. Arithmetic operations always have the potential of returning unexpected values, which may cause an error that forces the whole program to shut down. This is not what is described in this question.
B: Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information
or taking control of their computer while clicking on seemingly innocuous web pages. This is not what is described in this question.
C: A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence to be done correctly. This is not what is described in this question.
D: SQL injection is a type of security explogt in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to dat
A. This is not
what is described in this question.
F: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. This is not what is described in this question.
References:
http://www.webopedia.com/TERM/U/use-after-free.HYPERLINK "http://www.webopedia.com/TERM/U/use-after-free.html"html htHYPERLINK "https://en.wikipedia.org/wiki/Clickjacking"tps://en.wikipedia.org/wiki/Clickjacking http://searchstorage.tHYPERLINK "http://searchstorage.techtarget.com/definition/racecondition" echtarget.com/definition/race-condiHYPERLINK "http://searchstorage.techtarget.com/definition/race-condition"tion

NEW QUESTION 180
An application present on the majority of an organization’s 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

A. Deploy custom HIPS signatures to detect and block the attacks.
B. Validate and deploy the appropriate patch.
C. Run the application in terminal services to reduce the threat landscape.
D. Deploy custom NIPS signatures to detect and block the attack

Answer: B

Explanation:
If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.
A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers,
corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
Incorrect Answers:
A: This question is asking for the MOST comprehensive way to resolve the issue. A HIPS (Host Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.
C: This question is asking for the MOST comprehensive way to resolve the issue. Running the application in terminal services may reduce the threat landscape. However, it doesn’t resolve the issue. Patching the application to eliminate the threat is a better solution.
D: This question is asking for the MOST comprehensive way to resolve the issue. A NIPS (Network Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.
References: http://searchsecurity.techtarget.com/definition/buffer-overflow

NEW QUESTION 184
select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson
Which of the following types of attacks is the user attempting?

A. XML injection
B. Command injection
C. Cross-site scripting
D. SQL injection

Answer: D

Explanation:
The code in the question is SQL code. The attack is a SQL injection attack.
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must explogt a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
Incorrect Answers:
A: The code in the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.
B: Command injection is an attack in which the goal is execution of arbitrary commands on the host
operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not the type of code you would use in an XSS attack.
References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 185
A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

A. Insecure direct object references, CSRF, Smurf
B. Privilege escalation, Application DoS, Buffer overflow
C. SQL injection, Resource exhaustion, Privilege escalation
D. CSRF, Fault injection, Memory leaks

Answer: A

Explanation:
Insecure direct object references are used to access dat
A. CSRF attacks the functions of a web site which could access dat
A. A Smurf attack is used to take down a system.
A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which will allow attackers to manipulate these references to access unauthorized data.
Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious Web site, email, blog, instant message, or program causes a user's Web browser to perform an unwanted action on a trusted site for which the user is currently authenticated. The impact of a successful cross-site request forgery attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function (funds Transfer, form submission etc.) via the target's browser without knowledge of the target user, at least until the unauthorized function has been committed.
A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.
Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.
Incorrect Answers:
B: Application DoS is an attack designed to affect the availability of an application. Buffer overflow is used to obtain information. Therefore, the order of importance in this answer is incorrect.
C: Resource exhaustion is an attack designed to affect the availability of a system. Privilege escalation is used to obtain information. Therefore, the order of importance in this answer is incorrect.
D: The options in the other answers (Insecure direct object references, privilege escalation, SQL injection) are more of a threat to data confidentiality than the options in this answer. References:
http://www.tutorialspoint.com/secuHYPERLINK "http://www.tutorialspoint.com/security_testing/insecure_direct_object_reference.htm"rity_testing /insecure_direct_object_reference.htm https://www.owasp.org/index.php/Cross-Site_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet"Request_Forgery_(CSRF)_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet"Prevention_Cheat_Sheet http://www.webopedia.com/TERM/S/smurf.html

NEW QUESTION 190
A security administrator wants to deploy a dedicated storage solution which is inexpensive, can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

A. SAN
B. NAS
C. Virtual SAN
D. Virtual storage

Answer: B

Explanation:
A NAS is an inexpensive storage solution suitable for small offices. Individual files can be encrypted by using the EFS (Encrypted File System) functionality provided by the NTFS file system.
NAS typically uses a common Ethernet network and can provide storage services to any authorized devices on that network.
Two primary NAS protocols are used in most environments. The choice of protocol depends largely on the type of computer or server connecting to the storage.
Network File System (NFS) protocol usually used by servers to access storage in a NAS environment. Common Internet File System (CIFS), also sometimes called Server Message Block (SMB), is usually used for desktops, especially those running Microsoft Windows.
Unlike DAS and SAN, NAS is a file-level storage technology. This means the NAS appliance maintains and controls the files, folder structures, permission, and attributes of the data it holds. A typical NAS deployment integrates the NAS appliance with a user database, such as Active Directory, so file permissions can be assigned based on established users and groups. With Active Directory
integration, most Windows New Technology File System (NTFS) permissions can be set on the files contained on a NAS device.
Incorrect Answers:
A: A SAN is expensive compared to a NAS and is more suitable for enterprise storage for larger
networks.
C: A Virtual SAN is the combined local storage of multiple hypervisor servers (VMware ESXi for example) to create one virtual storage pool. This is not the best solution for a small office.
D: Virtual storage is storage presented by an underlying SAN or group of servers. This is not the best solution for a small office.
References:
hHYPERLINK "http://infrastructuretechnologypros.com/understanding-storage-technology-part-2- alphabet-soup-storage/"ttp://infrastructuretechnoloHYPERLINK "http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soupstorage/" gypros.com/understanding-storage-technology-part-2-alphabet-soup-storage/

NEW QUESTION 193

At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

A. Add guests with more memory to increase capacity of the infrastructure.
B. A backup is running on the thin clients at 9am every morning.
C. Install more memory in the thin clients to handle the increased load while booting.
D. Booting all the lab desktops at the same time is creating excessive I/O.
E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.
F. Install faster SSD drives in the storage system used in the infrastructure.
G. The lab desktops are saturating the network while booting.
H. The lab desktops are using more memory than is available to the host system

Answer: DF

Explanation:
The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.
The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.
Incorrect Answers:
A: If a lack of memory was the cause of the problem, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops. Therefore adding guests with more memory will not solve the problem so this answer is incorrect.
B: This question is asking for the MOST likely cause of the problem. A backup running on the thin clients at 9am every morning as soon as the lab desktops start up is an unlikely cause of the problem. It is much more likely that the lab desktops starting up at the same time is causing high disk I/O.
C: The lab desktops starting up would not cause memory issues on the thin clients so adding memory will not solve the issue.
E: The lab desktops starting up would not cause network bandwidth issues so increasing the bandwidth will not solve the issue.
G: The lab desktops starting up would not saturate the network.
H: If the lab desktops are using more memory than is available to the host systems, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops.

NEW QUESTION 196
The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

A. HIPS
B. UTM
C. Antivirus
D. NIPS
E. DLP

Answer: A

Explanation:
In this question, we need to protect the workstations when connected to either the office or home network. Therefore, we need a solution that stays with the workstation when the user takes the computer home.
A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.
Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.
Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.
Incorrect Answers:
B: Unified threat management (UTM) is a primary network gateway defense solution for organizations. In theory, UTM is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system: network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention and on-appliance reporting. However, UTM is designed to protect a network; it will not protect the user’s workstations when connected to their home
networks as required in this question.
C: Antivirus software will protect against attacks aided by known viruses. However, it will not protect against unknown attacks as required in this question.
D: NIPS stands for Network Intrusion Prevention Systems. A NIPS is designed to protect a network; it will not protect the user’s workstations when connected to their home networks as required in this question.
E: Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. DLP does not protect against malicious attacks. References:
http://en.wikipedia.org/wHYPERLINK "http://en.wikipedia.org/wiki/Intrusion_prevention_system"iki/Intrusion_prevention_system

NEW QUESTION 198
Which of the following describes a risk and mitigation associated with cloud data storage?

A. Risk: Shared hardware caused data leakage Mitigation: Strong encryption at rest
B. Risk: Offsite replication Mitigation: Multi-site backups
C. Risk: Data loss from de-duplication Mitigation: Dynamic host bus addressing
D. Risk: Combined data archivingMitigation: Two-factor administrator authentication

Answer: A

Explanation:
With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small

risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.
The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.
Incorrect Answers:
B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.
C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the dat
A. Dynamic host bus addressing is not a risk mitigation.
D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

NEW QUESTION 200
Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

A. Deduplication
B. Data snapshots
C. LUN masking
D. Storage multipaths

Answer: C

Explanation:
A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).
LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.
Incorrect Answers:
A: Deduplication is the process of eliminating multiple copies of the same data to save storage space. It does not prevent an unauthorized HBA from viewing iSCSI target information.
B: Data snapshots are point in time copies of data often used by data backup applications. They do not prevent an unauthorized HBA from viewing iSCSI target information.
D: Storage multipaths are when you have multiple connections to a storage device. This provides path redundancy in the event of a path failure and can also (in active/active configurations) provide extra capacity by aggregating the bandwidth of the multiple storage paths. However, they do not prevent an unauthorized HBA from viewing iSCSI target information.
References:
http://searchviHYPERLINK "http://searchvirtualstorage.techtarget.com/definition/LUNmasking" rtualstorage.techtarget.com/definition/LUN-masking

NEW QUESTION 201
A vulnerability scanner report shows that a client-server host monitoring solution operating in the credit card corporate environment is managing SSL sessions with a weak algorithm which does not meet corporate policy. Which of the following are true statements? (Select TWO).

A. The X509 V3 certificate was issued by a non trusted public CA.
B. The client-server handshake could not negotiate strong ciphers.
C. The client-server handshake is configured with a wrong priority.
D. The client-server handshake is based on TLS authentication.
E. The X509 V3 certificate is expired.
F. The client-server implements client-server mutual authentication with different certificate

Answer: BC

Explanation:
The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported. The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.
Incorrect Answers:
A: If the X509 V3 certificate was issued by a non-trusted public CA, then the client would receive an error saying the certificate is not trusted. However, an X509 V3 certificate would not cause a weak algorithm.
D: TLS provides the strongest algorithm; even stronger than SSL version 3.
E: If the X509 V3 certificate had expired, then the client would receive an error saying the certificate is not trusted due to being expired. However, an X509 V3 certificate would not cause a weak algorithm.
F: SSL does not mutual authentication with different certificates. References:
http://www.slashroot.in/uHYPERLINK "http://www.slashroot.in/understanding-ssl-handshakeprotocol" nderstanding-ssl-hHYPERLINK "http://www.slashroot.in/understanding-ssl-handshakeprotocol" andshake-protocol

NEW QUESTION 202
Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

A. Jailbroken mobile device
B. Reconnaissance tools
C. Network enumerator
D. HTTP interceptor
E. Vulnerability scanner
F. Password cracker

Answer: DE

Explanation:
Communications between a mobile web application and a RESTful application server will use the
HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.

To assess the security of the application server itself, you should use a vulnerability scanner.
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be explogted and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.
Incorrect Answers:
A: A jailbroken mobile device is a mobile device with an operating system that has any built-in security restrictions removed. This enables you to install software and perform actions that the manufacturer did not intend. However, a jailbroken mobile device is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.
B: Reconnaissance in terms of IT security is the process of learning as much as possible about a target business usually over a long period of time with a view to discovering security flaws. It is not used by security administrators for security assessment of client-server applications.
C: Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It is not used to assess the security between the mobile web application and the RESTful application server.
F: A password cracker is used to guess passwords. It is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.
References: http://www.webopedia.com/TERM/V/vulneHYPERLINK
"http://www.webopedia.com/TERM/V/vulnerability_scanning.html"rability_scanning.html

NEW QUESTION 206
A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

A. Online password testing
B. Rainbow tables attack
C. Dictionary attack
D. Brute force attack

Answer: B

Explanation:
The passwords in a Windows (Active Directory) domain are encrypted.
When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".
To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then
the user is authenticated and granted access.
Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.
Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse
the hashing function to determine what the plaintext password might be.
The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.
Incorrect Answers:
A: Online password testing cannot be used to crack passwords on a windows domain.
C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.
D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:
http://netsecuriHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow- Tables.htm"ty.about.com/od/hackertoHYPERLINK
"http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"ols/a/Rainbow- TableHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"s.htm

NEW QUESTION 211
A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway.
Which of the following controls MUST be implemented to enable stateless communication?

A. Generate a one-time key as part of the device registration process.
B. Require SSL between the mobile application and the web services gateway.
C. The jsession cookie should be stored securely after authentication.
D. Authentication assertion should be stored securely on the clien

Answer: D

Explanation:
JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.
Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help?
The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.
However there are some drawbacks to session identifiers:
They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.
They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a

database to figure out who this session is for and if they are allowed to perform the requested operation.
JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format.
JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.
How To Store JWTs In The Browser
Short Answer:: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along
the token for authentication purposes, but won't expose it to the JavaScript environment. Incorrect Answers:
A: A one-time key does not enable stateless communication.
B: SSL between the mobile application and the web services gateway will provide a secure encrypted connection between the two. However, SSL does not enable stateless communication.
C: A cookie is stateful, not stateless as required in the question. References:
https://stormpath.com/blog/build-secure-user-interfaces-using-jwtHYPERLINK "https://stormpath.com/blog/build-secure-user-interfaces-using-jwts/"s/

NEW QUESTION 213
A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be filexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

A. A partition-based software encryption product with a low-level boot protection and authentication
B. A container-based encryption product that allows the end users to select which files to encrypt
C. A full-disk hardware-based encryption product with a low-level boot protection and authentication
D. A file-based encryption product using profiles to target areas on the file system to encrypt

Answer: D

Explanation:
The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.
File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer.
Profiles can be used to determine areas on the file system to encrypt such as Document folders. Incorrect Answers:
A: A partition-based software encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts. B: An encryption product that allows the end users to select which files to encrypt is not the best solution. A solution that automatically encrypts the necessary data is a better solution.
C: A full-disk hardware-based encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts.

NEW QUESTION 214
A storage as a service company implements both encryption at rest as well as encryption in transit of customers' dat

A. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement asolution that will strengthen the customer's encryption ke
B. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?
C. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }
D. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }
E. password = password + sha(password+salt) + aes256(password+salt)
F. key = aes128(sha256(password), password))

Answer: A

Explanation:
References:
http://HYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms"sHYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms"tackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-and-encryption-aHYPERLINK "http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms"lgorithms

NEW QUESTION 218
A security administrator has noticed that an increased number of employees' workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?

A. Implement an Acceptable Use Policy which addresses malware downloads.
B. Deploy a network access control system with a persistent agent.
C. Enforce mandatory security awareness training for all employees and contractors.
D. Block cloud-based storage software on the company networ

Answer: D

Explanation:
The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users to do not bring unauthorized data that could potentially contain malware into the network.
We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage services such as Dropbox or OneDrive.
Incorrect Answers:
A: An Acceptable Use Policy is always a good ide
A. However, it just tells the users how they 'should'
use the company systems. It is not a technical control to prevent malware.

B: A network access control system is used to control access to the network. It does not prevent malware on client computers.
C: Mandatory security awareness training for all employees and contractors is always a good idea. However, it just educates the users about potential security risks. It is not a technical control to prevent malware.

NEW QUESTION 221
A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

A. Remove contact details from the domain name registrar to prevent social engineering attacks.
B. Test external interfaces to see how they function when they process fragmented IP packets.
C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.
D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port scans against external network interfaces.

Answer: B

Explanation:
Fragmented IP packets are often used to evade firewalls or intrusion detection systems.
Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listing to a port).
One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. One method is a fragmented port scan. Fragmented packet Port Scan
The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP fragments, but many networks cannot afford the performance loss caused by the queuing.
Incorrect Answers:
A: Removing contact details from the domain name registrar does not improve the security of a network.
C: Enabling a honeynet to capture and facilitate future analysis of malicious attack vectors is a good way of gathering information to help you plan how you can defend against future attacks. However, it does not improve the security of the existing network.
D: Filter all internal ICMP message traffic does not force attackers to use full-blown TCP port scans against external network interfaces. They can use fragmented scans.
References:
http://www.auditmypc.com/port-scanning.asp

NEW QUESTION 224
A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated.
Users of the web application will not be added to the company's directory services. Passwords must not be stored in the code.
Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.
B. Use TLS with a shared client certificate for all users.
C. Use SAML with federated directory services.
D. Use Kerberos and browsers that support SAM

Answer: A

Explanation:
Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication. OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.
Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam. Incorrect Answers:
B: The question states that users of the web application must be uniquely identified and authenticated. A shared client certificate for all users does not meet this requirement.
C: The question states that users of the web application will not be added to the company's directory services. SAML with federated directory services would require that the users are added to the directory services.
D: The question states that users of the web application must be uniquely identified and authenticated. Kerberos and browsers that support SAML provides no authentication mechanism. References:
https://en.wikipedia.org/wiki/OpenID

NEW QUESTION 226
A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

A. Insider threat
B. Network reconnaissance
C. Physical security
D. Industrial espionage

Answer: C

Explanation:
If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office

door.
However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise,
agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
Incorrect Answers:
A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.
B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.
D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.
References: http://searchsecurity.techtarget.com/deHYPERLINK
"http://searchsecurity.techtarget.com/definition/physical-security"finition/physical-security

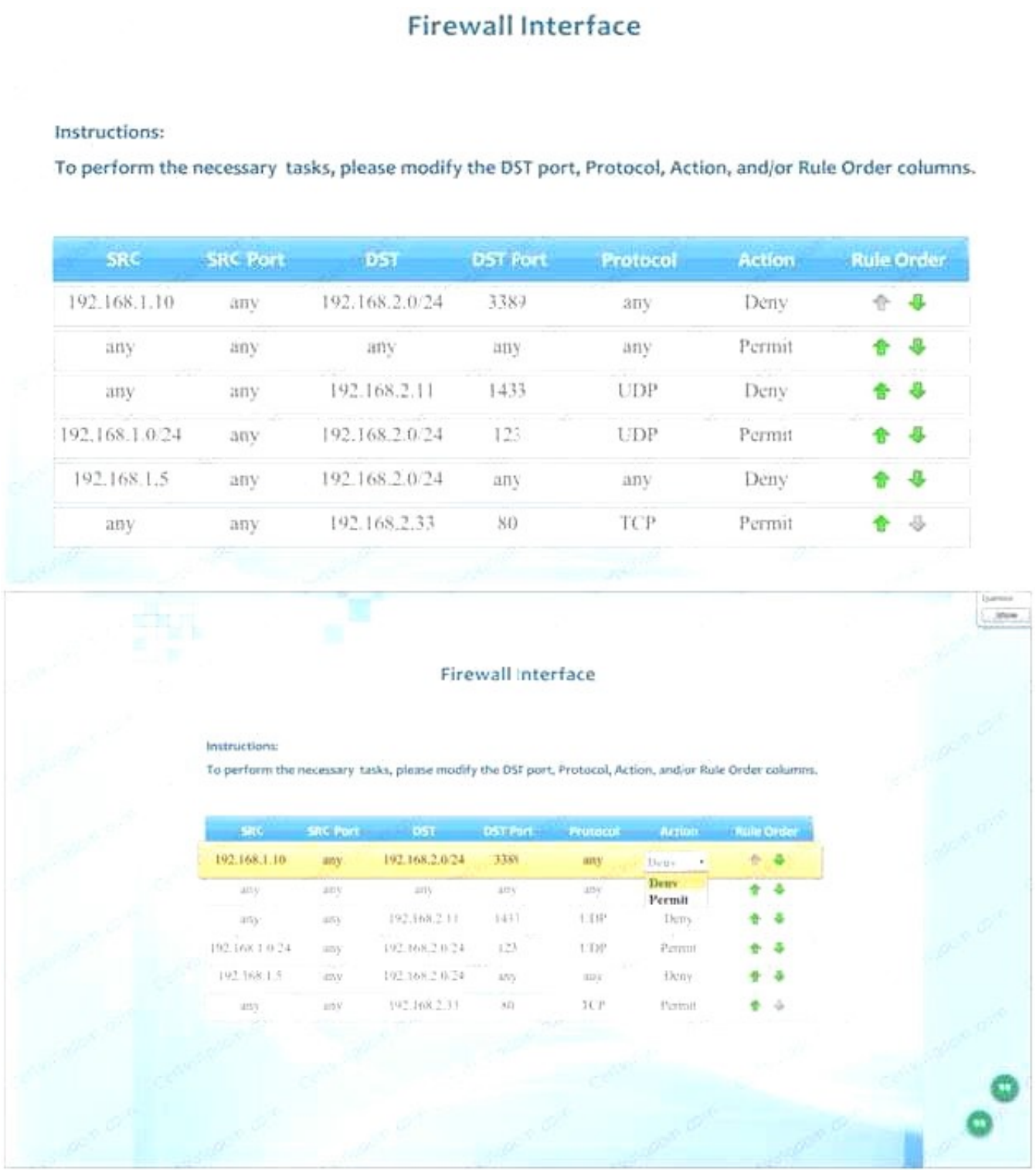
NEW QUESTION 228
Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

A. Establish a cloud-based authentication service that supports SAML.
B. Implement a new Diameter authentication server with read-only attestation.
C. Install a read-only Active Directory server in the corporate DMZ for federation.
D. Allow external connections to the existing corporate RADIUS serve

Answer: A

Explanation:
There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.
By eliminating all passwords and instead using digital signatures for authentication and authorization
of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAMLenabled SaaS applications are easier and quicker to user provision in complex enterprise
environments, are more secure and help simplify identity management across large and diverse user communities.
Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal. Incorrect Answers:
B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.
C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.
D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.
References:
https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml- based-single-sign-on
https://en.wikipedia.org/wiki/Security_Assertion_Markup_LanHYPERLINK "https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language"guage

NEW QUESTION 231
Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:
User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down
Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.
Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.
Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.
Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.



A. Check the answer below

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	
any	any	192.168.2.33	443	TCP	Permit	
any	any	192.168.2.11	1433	TCP	Deny	
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	
192.168.1.5	any	192.168.2.0/24	any	any	Deny	
any	any	any	any	any	Deny	

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
B. This rule is not workin
C. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
D. It is not working because the action is set to Den
E. This needs to be set to Permit.

192.168.1.10	any	192.168.2.0/24	3389	any	Deny	

Task 2)
All web servers have been changed to communicate solely over SS
F. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
G. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).

any	any	192.168.2.33	80	TCP	Permit	

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
H. This rule is not workin
I. Identify and correct this issue.The SQL Server rule is shown in the image belo
J. It is not working because the protocol is wron
K. It should be TCP, not UDP.

any	any	192.168.2.11	1433	UDP	Deny	

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.The network time rule is shown in the image below.
However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul
L. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).

any	any	any	any	any	Permit

M. Check the answer below

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	
any	any	192.168.2.33	443	TCP	Permit	
any	any	192.168.2.11	1433	TCP	Deny	
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	
192.168.1.5	any	192.168.2.0/24	any	any	Deny	
any	any	any	any	any	Deny	

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
N. This rule is not workin
O. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
P. It is not working because the action is set to Den
Q. This needs to be set to Permit.

192.168.1.10	any	192.168.2.0/24	3389	any	Deny

Task 2)
All web servers have been changed to communicate solely over SS
R. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
S. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
T. This rule is not workin
. Identify and correct this issue.The SQL Server rule is shown in the image belo
. It is not working because the protocol is wron
. It should be TCP, not UDP.

any	any	192.168.2.11	1433	UDP	Deny

Task 4)
Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed.The network time rule is shown in the image below.However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul
. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).

any	any	any	any	any	Permit

Answer: A

NEW QUESTION 234
The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

A. The company should mitigate the risk.
B. The company should transfer the risk.
C. The company should avoid the risk.
D. The company should accept the ris

Answer: B

Explanation:
To transfer the risk is to defilect it to a third party, by taking out insurance for example. Incorrect Answers:
A: Mitigation is not an option as the CIO's budget does not allow for the purchase of additional compensating controls.
C: Avoiding the risk is not an option as the business unit depends on the critical business function. D: Accepting the risk would not reduce financial loss.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 218

NEW QUESTION 236
A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

A. Establish a risk matrix
B. Inherit the risk for six months
C. Provide a business justification to avoid the risk
D. Provide a business justification for a risk exception

Answer: D

Explanation:
The Exception Request must include: A description of the non-compliance.
The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance.

The proposed plan for managing the risk associated with non-compliance.
The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance.
An endorsement of the request by the appropriate Information Trustee (VP or Dean). Incorrect Answers:
A: A risk matrix can be used to determine an overall risk ranking before determining how the risk will be dealt with.
B: Inheriting the risk for six months means that it has been decided the benefits of moving forward outweighs the risk.
C: Avoiding the risk is not recommended as the applications are still being used. References:
http://www.rit.edu/security/sHYPERLINK "http://www.rit.edu/security/sites/rit.edu.security/files/exception process.pdf"ites/rit.edu.security/files/exceptionHYPERLINK "http://www.rit.edu/security/sites/rit.edu.security/files/exception process.pdf"%20process.pdf
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 218

NEW QUESTION 237
The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.
D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Answer: A

Explanation:
Security in depth is the concept of creating additional layers of security. The traditional approach of securing the IT infrastructure is no longer enough. Today's threats are multifaceted and often persistent, and traditional network perimeter security controls cannot effectively mitigate them. Organizations need to implement more effective, multi-level security controls that are embedded with their electronic assets. They need to protect key assets from both external and internal threats. This security in depth approach is meant to sustain attacks even when perimeter and traditional controls have been breached.
In this question, using two firewalls to secure the DMZ from both external and internal attacks is the best approach. Having each firewall managed by a separate administrator will reduce the chance of a configuration error being made on both firewalls. The remote logging will enable incident reconstruction.
Incorrect Answers:
B: Depending on the number of interfaces on the firewall, you could protect from external and internal threats with a single firewall although two firewalls is a better solution. However, it is not practical to have separate interfaces on the same firewall managed by different administrators. The firewall rules work together in a hierarchy to determine what traffic is allowed through each interface.
C: A SaaS based firewall can be used to protect cloud resources. However, it is not the best solution for protecting the network in this question.
D: A virtualized firewall could be used. However, multiple instances of the same firewall should be identical. They should not be configured separately by different administrators.
References:
http://www.oracle.com/technetwork/topics/entarch/oracle-wp-securiHYPERLINK "http://www.oracle.com/technetwork/topics/entarch/oracle-wp-security-ref-arch-1918345.pdf"tyref- arch-1918345.pdf

NEW QUESTION 242
A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and require two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
C. The guest WiFi may be explogted allowing non-authorized individuals access to confidential patient data.
D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Answer: AD

Explanation:
Privacy could be compromised because patient records can be from a doctor's personal device. This can then be shown to persons not authorized to view this information. Similarly, the doctor's personal device could have malware on it.
Incorrect Answers:
B: Device encryption is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.
C: The guest WiFi network is isolated from the internal network with appropriate security controls and the doctors and specialists can interact with the hospital's system via a remote desktop type interface.
E: Remote wiping is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.
References:
http://www.gwava.com/blog/top-10-byod-business-concerns

NEW QUESTION 247
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation
B. Security test and evaluation
C. Risk assessment
D. Ongoing authorization

Answer: D

Explanation:

Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process
that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.
Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.
Incorrect Answers:
A: Independent verification and validation (IV&V) is executed by a third party organization not involved in the development of a product. This is not considered continuous monitoring of authorized information systems.
B: Security test and evaluation is not considered continuous monitoring of authorized information systems.
C: Risk assessment is the identification of potential risks and threats. It is not considered continuous monitoring of authorized information systems.
References:
http://www.fedramp.net/ongoHYPERLINK "http://www.fedramp.net/ongoing-assessment-andauthorization- continuous-monitoring"ing-assessment-andHYPERLINK "http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring"- authorization-continuous-monitoring
https://www.techopedia.com/definition/24836/independent-verification-and-validation--
iHYPERLINK "https://www.techopedia.com/definition/24836/independent-verification-andvalidation-- iv&v"vHYPERLINK "https://www.techopedia.com/definition/24836/independentverification-
and-validation--iv&v"&HYPERLINK "https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v"v
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 213, 219

NEW QUESTION 250
A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

A. an administrative control
B. dual control
C. separation of duties
D. least privilege
E. collusion

Answer: C

Explanation:
Separation of duties requires more than one person to complete a task. Incorrect Answers:
A: Administrative controls refer policies, procedures, guidelines, and other documents used by an organization.
B: Dual control forces employees who are planning anything illegal to work together to complete critical actions.
D: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.
E: Collusion is defined as an agreement which occurs between two or more persons to deceive, mislead, or defraud others of legal rights.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 245, 321
https://en.wikipedia.org/wiki/Collusion

NEW QUESTION 251
The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server's baseline communications profile.
B. Configure the server logs to collect unusual activity including failed logins and restarted services.
C. Correlate data loss prevention logs for anomalous communications from the server.
D. Setup a packet capture on the firewall to collect all of the server communication

Answer: A

Explanation:
Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day explogts. Having knowledge of each host's communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zeroday and APT (advance persistent threat) malware and agents. Data intelligence allows forensic
analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network. Incorrect Answers:
B: The attack has already happened; the server has already been compromised. Configuring the server logs to collect unusual activity including failed logins and restarted services might help against future attacks but it will not provide information on an attack that has already happened.
C: It is unlikely the DLP logs would contain anomalous communications from the server that would identify where the server collected the information.
D: The attack has already happened; the server has already been compromised. Setting up a packet capture on the firewall to collect all of the server communications might help against future attacks but it will not provide information on an attack that has already happened.
References:
https://www.sans.HYPERLINK "https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics- 35952"org/reading-room/whitepapers/forensics/ids-fiHYPERLINK
"https://www.sans.org/reading-room/whitepapers/forensics/ids-file-forensics-35952"le-forensics- 35952, p. 6

NEW QUESTION 252
Company policy requires that all company laptops meet the following baseline requirements: Software requirements:
Antivirus
Anti-malware Anti-spyware Log monitoring
Full-disk encryption
Terminal services enabled for RDP Administrative access for local users Hardware restrictions:
Bluetooth disabled FireWire disabled WiFi adapter disabled
Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from

reoccurring? (Select TWO).

A. Group policy to limit web access
B. Restrict VPN access for all mobile users
C. Remove full-disk encryption
D. Remove administrative access to local users
E. Restrict/disable TELNET access to network resources
F. Perform vulnerability scanning on a daily basis
G. Restrict/disable USB access

Answer: DG

Explanation:
A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.
Therefore, one method of preventing such attacks is to remove administrative access for local users. A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer. We can prevent this from happening by restricting or disabling access to USB devices.
Incorrect Answers:
A: Using a group policy to limit web access is not a practical solution. Users in a company often require Web access so restricting it will affect their ability to do their jobs.
B: Rootkits or Bootkits would not be caught by connecting to the network over a VPN so disabling VPN access will not help.
C: Removing full-disk encryption will not prevent Bootkits.
E: Bootkits are not caught by connecting to network resources using Telnet connection so disabling Telnet access to resources will not help.
F: Performing vulnerability scanning on a daily basis might help you to quickly detect Bootkits. However, vulnerability scanning does nothing to actually prevent the Bootkits.
References: https://en.wikipedia.org/wiki/Rootkit

NEW QUESTION 254
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CAS-003 Exam with Our Prep Materials Via below:

https://www.certleader.com/CAS-003-dumps.html