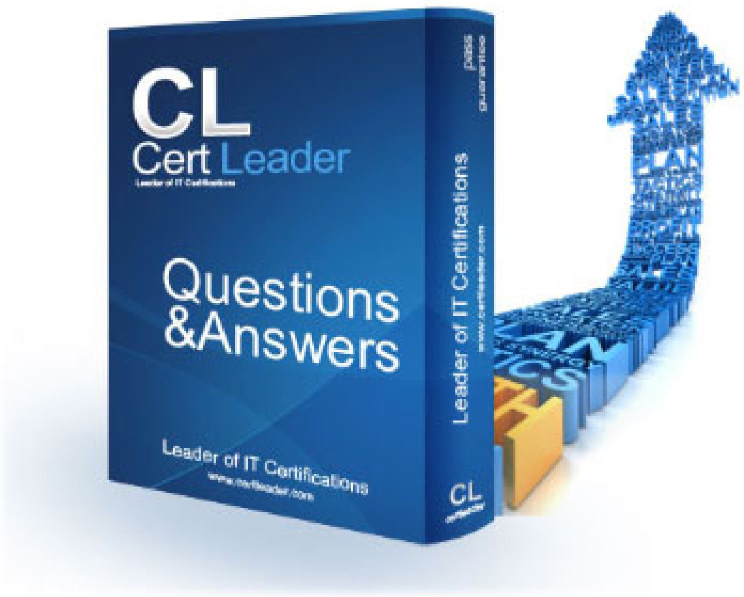
CAS-003 Dumps

CompTIA Advanced Security Practitioner (CASP)

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



NEW QUESTION 1
A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.
Which of the following is the BEST solution?

A. Use an entropy-as-a-service vendor to leverage larger entropy pools.
B. Loop multiple pseudo-random number generators in a series to produce larger numbers.
C. Increase key length by two orders of magnitude to detect brute forcing.
D. Shift key generation algorithms to ECC algorithm

Answer: A

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

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

Answer: B

NEW QUESTION 4
A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.
The person extracts the following data from the phone and EXIF data from some files:
DCIM Images folder
Audio books folder Torrentz
My TAX.xls
Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s
Location: 3500 Lacey Road USA
Which of the following BEST describes the security problem?

A. MicroSD in not encrypted and also contains personal data.
B. MicroSD contains a mixture of personal and work data.
C. MicroSD in not encrypted and contains geotagging information.
D. MicroSD contains pirated software and is not encrypte

Answer: A

NEW QUESTION 5
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 6
During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

A. Code repositories
B. Security requirements traceability matrix
C. Software development lifecycle

D. Data design diagram
E. Roles matrix
F. Implementation guide

Answer: F

NEW QUESTION 7
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 8
A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:
TCP 80 open
TCP 443 open
TCP 1434 filtered
The penetration tester then used a different tool to make the following requests:
GET / script/login.php?token=45$MHT000MND876
GET / script/login.php?token=@#984DCSPQ%091DF
Which of the following tools did the penetration tester use?

A. Protocol analyzer
B. Port scanner
C. Fuzzer
D. Brute forcer
E. Log analyzer
F. HTTP interceptor

Answer: C

NEW QUESTION 9
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 10
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 10
A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase
the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle.
Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

A. Install and configure an IPS.
B. Enforce routine GPO reviews.
C. Form and deploy a hunt team.
D. Institute heuristic anomaly detection.
E. Use a protocol analyzer with appropriate connector

Answer: AD

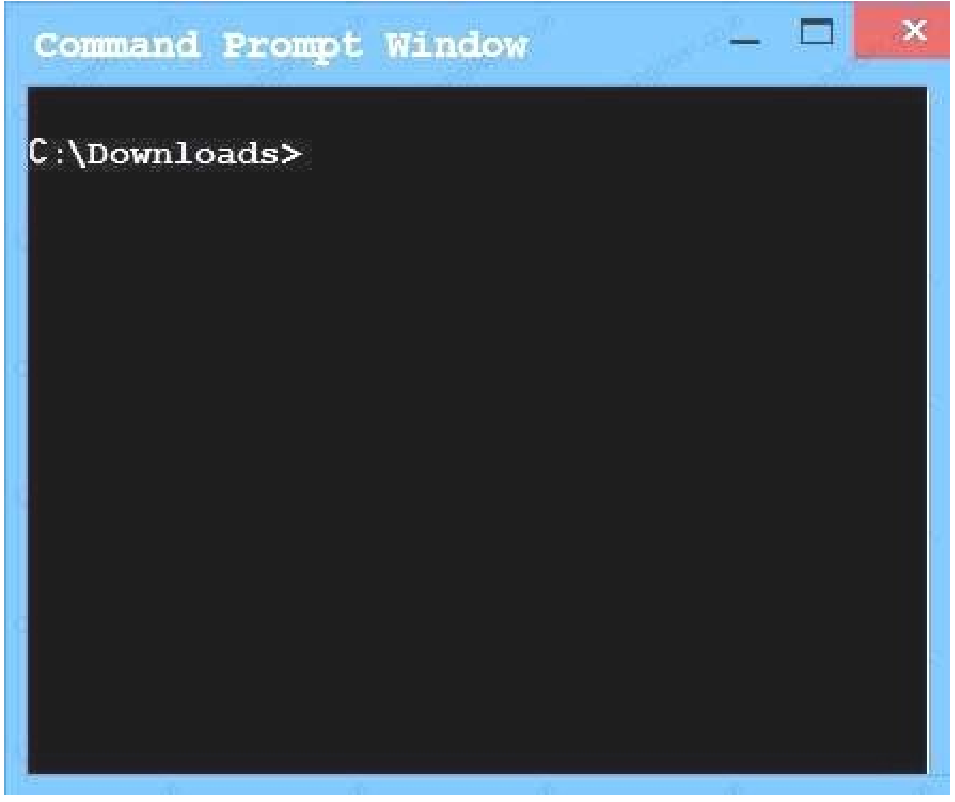
NEW QUESTION 13

An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.
Which of the following procedures should the security responder apply to the situation? (Choose two.)

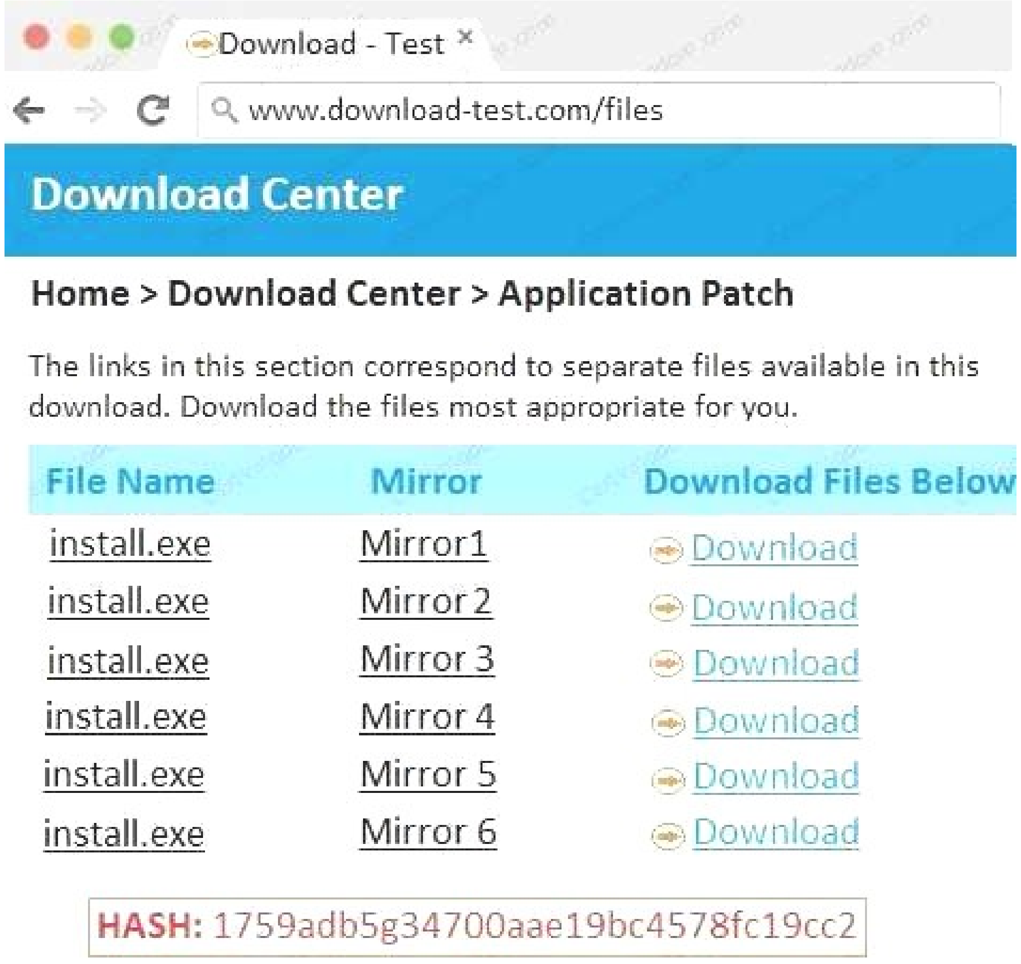
A. Contain the server.
B. Initiate a legal hold.
C. Perform a risk assessment.
D. Determine the data handling standard.
E. Disclose the breach to customers.
F. Perform an IOC sweep to determine the impac

Answer: BF

NEW QUESTION 15
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.



```
C:\Downloads>
```



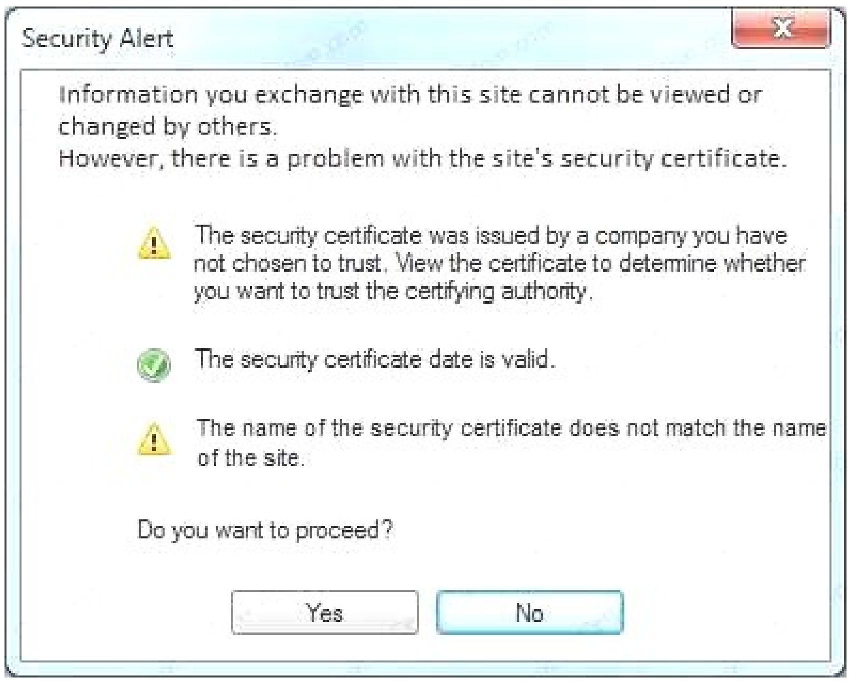
Download Center

Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download. Download the files most appropriate for you.

File Name	Mirror	Download Files Below
install.exe	Mirror1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2


Security Alert

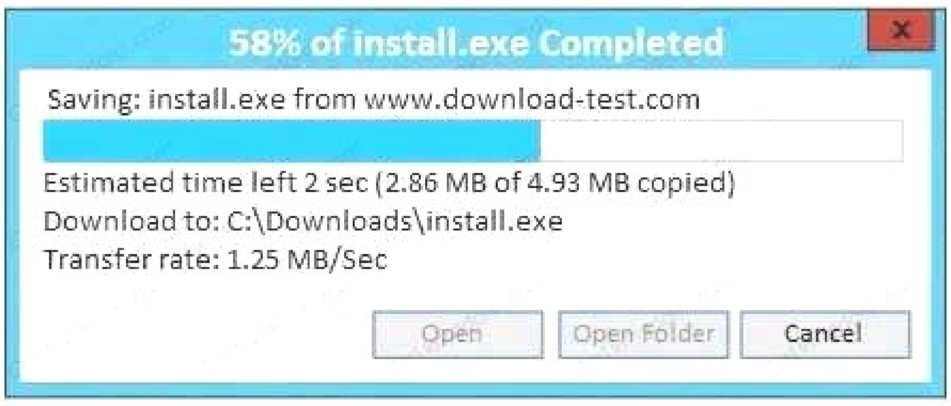
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

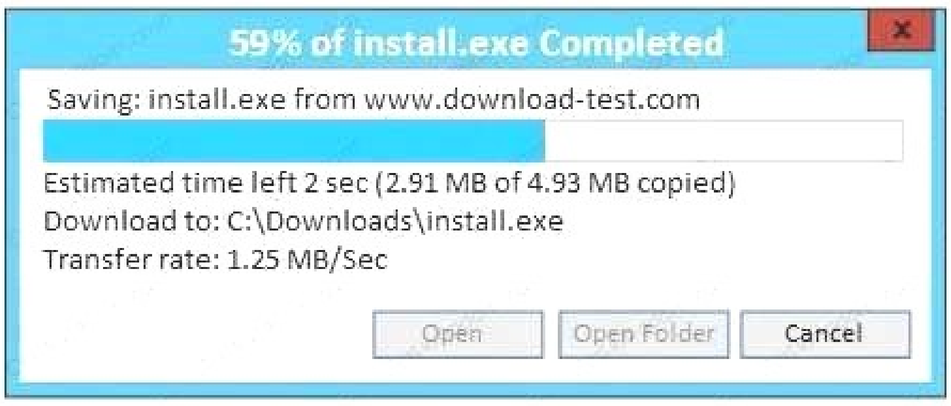
⚠ The name of the security certificate does not match the name of the site.

Do you want to proceed?


58% of install.exe Completed

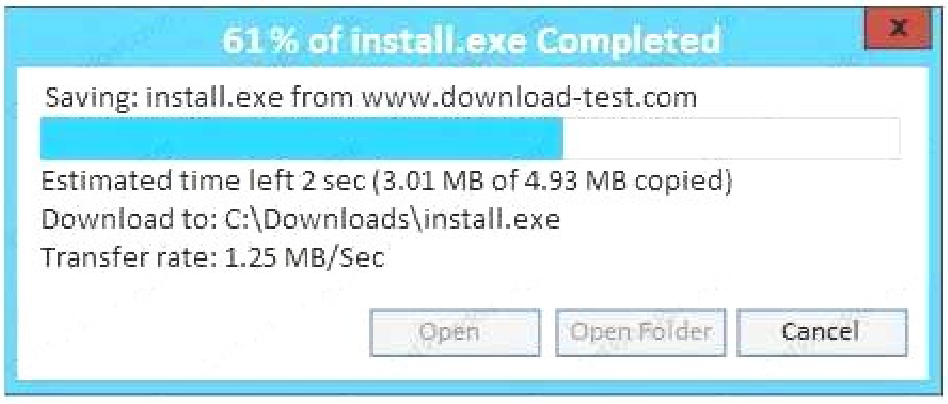
Saving: install.exe from www.download-test.com

Estimated time left 2 sec (2.86 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec


59% of install.exe Completed

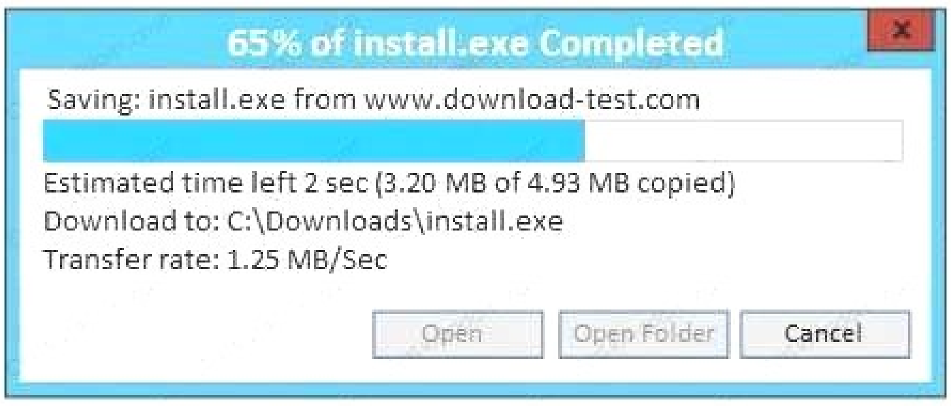
Saving: install.exe from www.download-test.com

Estimated time left 2 sec (2.91 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec


61% of install.exe Completed

Saving: install.exe from www.download-test.com

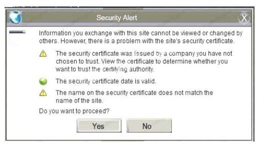
Estimated time left 2 sec (3.01 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec


65% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (3.20 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec

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.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

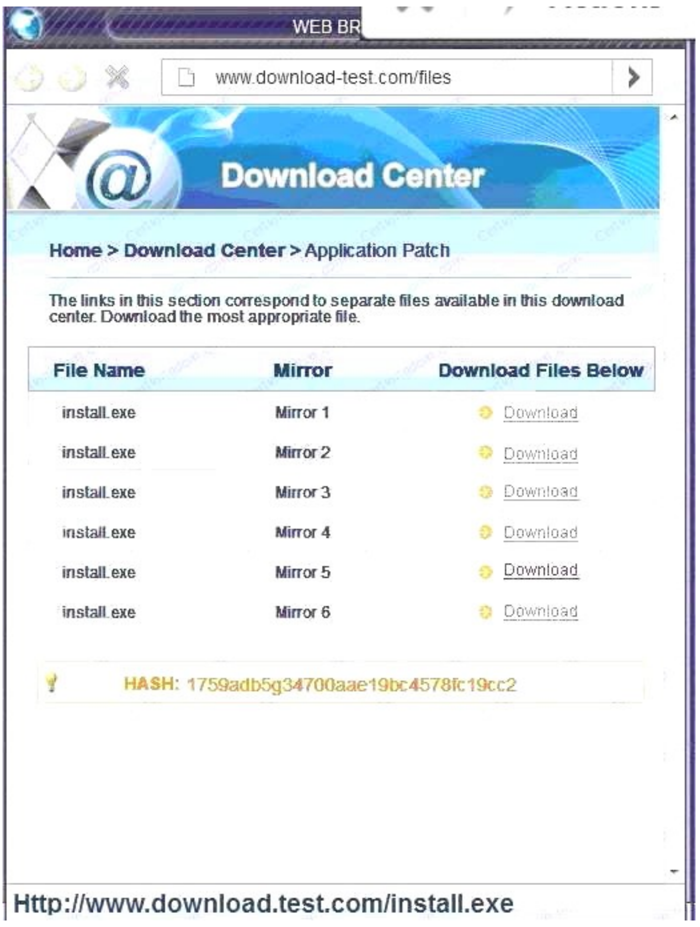
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

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



Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download center. Download the most appropriate file.

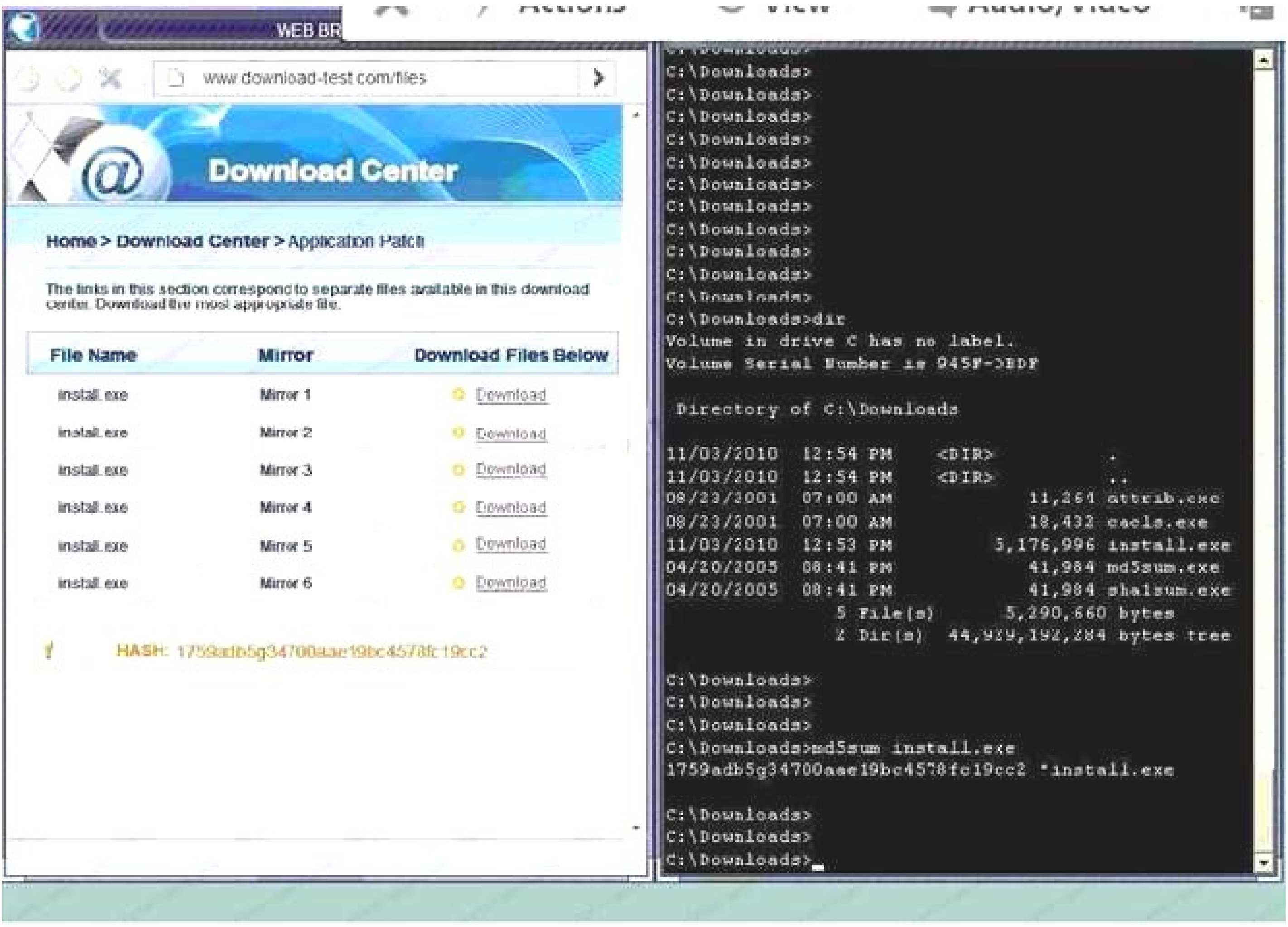
File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2

Http://www.download.test.com/install.exe

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.



Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download center. Download the most appropriate file.

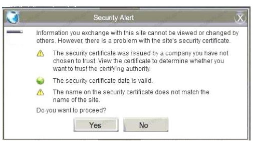
File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2

```
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 045F-3BDF

 Directory of C:\Downloads

11/03/2010  12:54 PM    <DIR>          .
11/03/2010  12:54 PM    <DIR>          ..
08/23/2001  07:00 AM            11,264 attrib.exe
08/23/2001  07:00 AM            18,432 cacls.exe
11/03/2010  12:53 PM         5,176,996 install.exe
04/20/2005  08:41 PM            41,984 md5sum.exe
04/20/2005  08:41 PM            41,984 sha1sum.exe
               5 File(s)      5,290,660 bytes
               2 Dir(s)  44,929,192,284 bytes free

C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>md5sum install.exe
1759adb5g34700aae19bc4578fc19cc2 *install.exe

C:\Downloads>
C:\Downloads>
C:\Downloads>_
```

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.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

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 19

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 23
An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

A. Secure storage policies
B. Browser security updates
C. Input validation
D. Web application firewall
E. Secure coding standards
F. Database activity monitoring

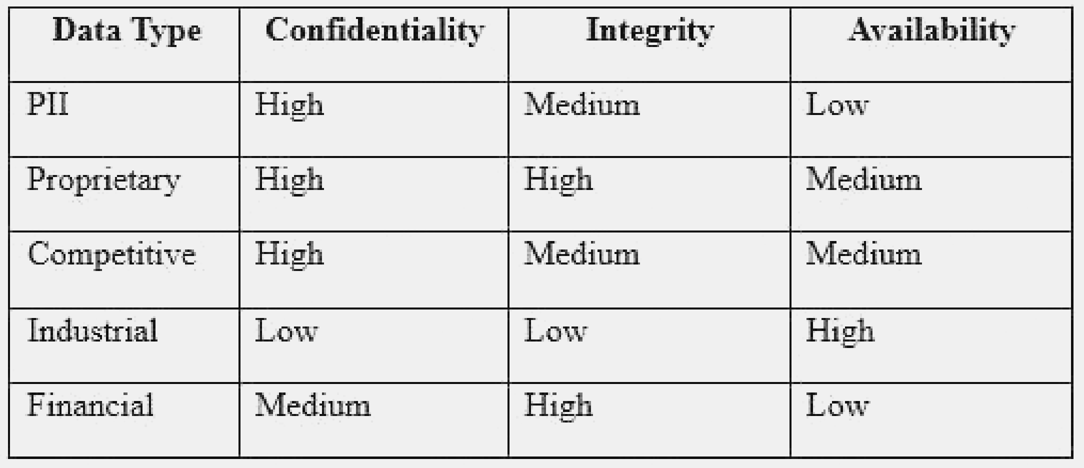
Answer: CF

NEW QUESTION 24
A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

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

Answer: D

NEW QUESTION 26
An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.



Data Type	Confidentiality	Integrity	Availability
PII	High	Medium	Low
Proprietary	High	High	Medium
Competitive	High	Medium	Medium
Industrial	Low	Low	High
Financial	Medium	High	Low

Based on the data classification table above, which of the following BEST describes the overall classification?

A. High confidentiality, high availability
B. High confidentiality, medium availability
C. Low availability, low confidentiality
D. High integrity, low availability

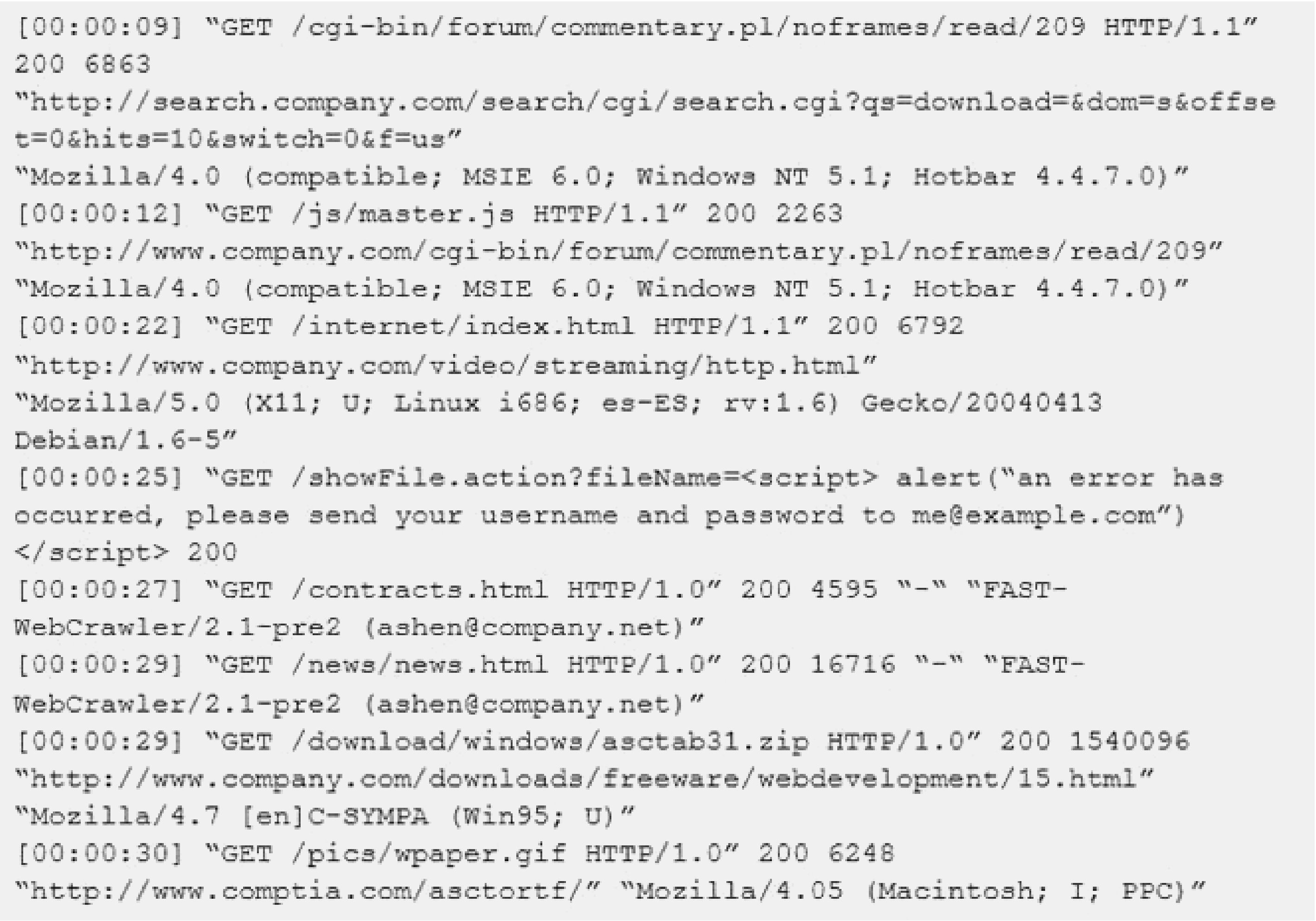
Answer: B

NEW QUESTION 30
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 32
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)"
```

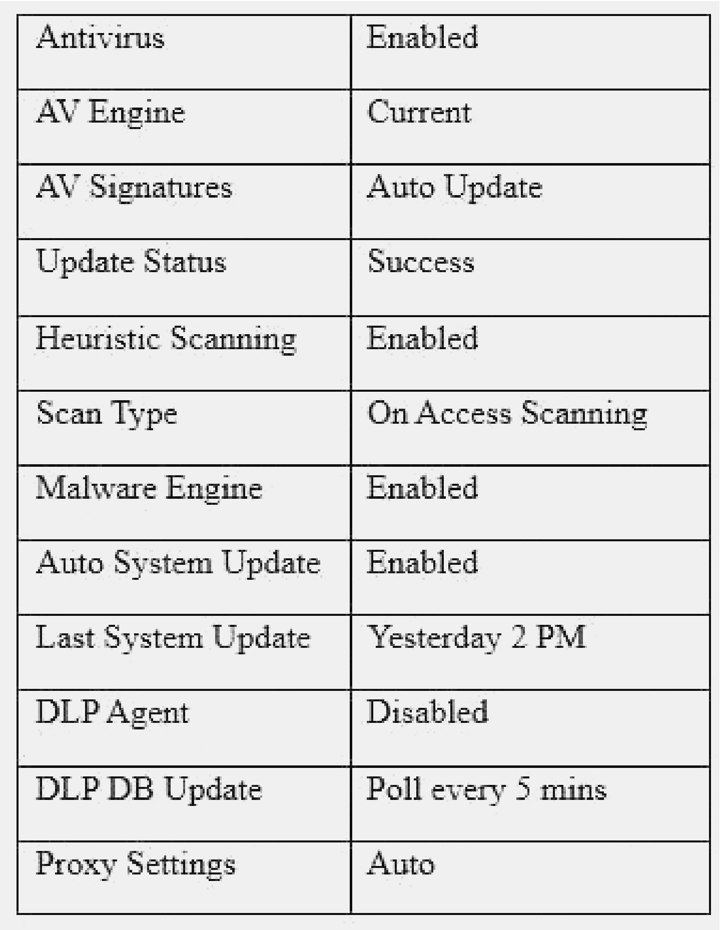
Which of the following types of attack vector did the penetration tester use?

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

Answer: B

NEW QUESTION 36

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 39

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

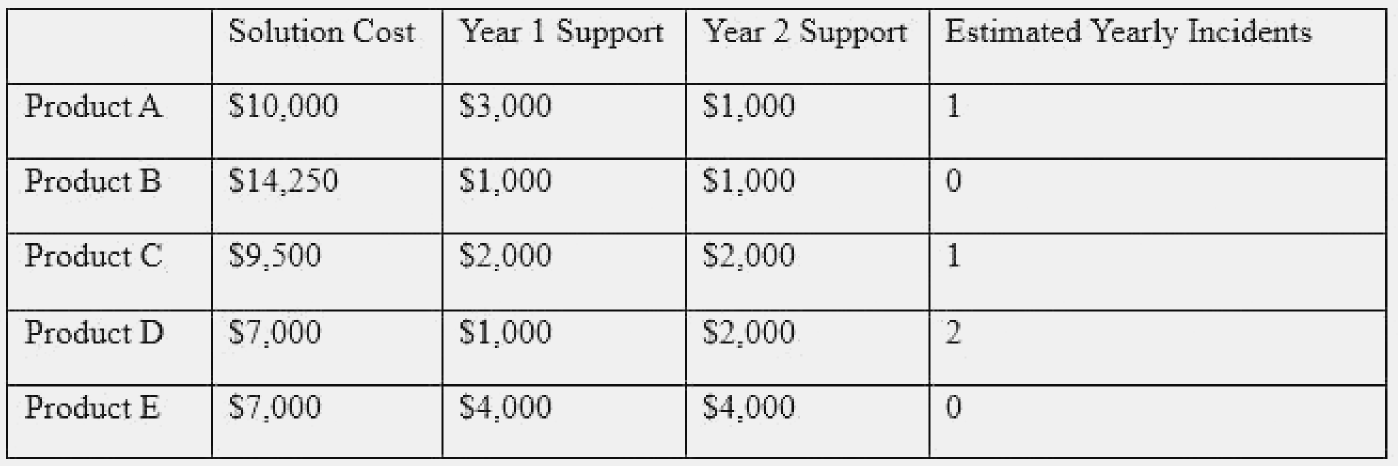
Answer: B

NEW QUESTION 44
A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:
High-impact controls implemented: 6 out of 10 Medium-impact controls implemented: 409 out of 472 Low-impact controls implemented: 97 out of 1000
The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:
Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000
Average medium-impact control implementation cost: $6,250; Probable ALE for each mediumimpact control gap: $11,000
Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

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

Answer: C

NEW QUESTION 48
After investigating virus outbreaks that have cost the company $1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:



	Solution Cost	Year 1 Support	Year 2 Support	Estimated Yearly Incidents
Product A	$10,000	$3,000	$1,000	1
Product B	$14,250	$1,000	$1,000	0
Product C	$9,500	$2,000	$2,000	1
Product D	$7,000	$1,000	$2,000	2
Product E	$7,000	$4,000	$4,000	0

Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?

A. Product A
B. Product B
C. Product C
D. Product D
E. Product E

Answer: E

NEW QUESTION 51
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 53
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 58
An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

A. Magic link sent to an email address
B. Customer ID sent via push notification
C. SMS with OTP sent to a mobile number
D. Third-party social login
E. Certificate sent to be installed on a device
F. Hardware tokens sent to customers

Answer: CE

NEW QUESTION 63
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

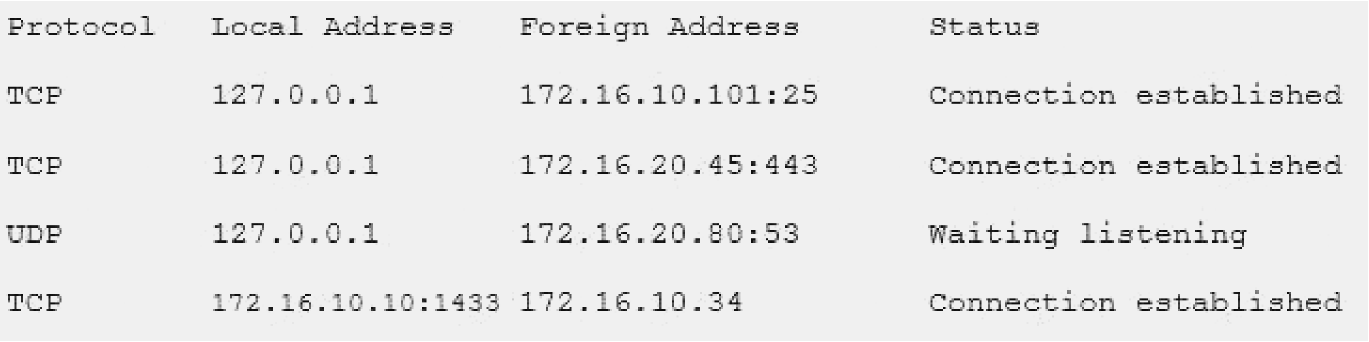
Answer: BCE

NEW QUESTION 67
A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)

A. Restrict access to the network share by adding a group only for developers to the share's ACL
B. Implement a new COTS solution that does not use hard-coded credentials and integrates with directory services
C. Obfuscate the username within the script file with encoding to prevent easy identification and the account used
D. Provision a new user account within the enterprise directory and enable its use for authentication to the target application
E. Share the username and password with all developers for use in their individual scripts
F. Redesign the web applications to accept single-use, local account credentials for authentication

Answer: AB

NEW QUESTION 71
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 73
A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However, the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?

A. The OS version is not compatible
B. The OEM is prohibited

C. The device does not support FDE
D. The device is rooted

Answer: D

NEW QUESTION 75
An agency has implemented a data retention policy that requires tagging data according to type before storing it in the data repository. The policy requires all business emails be automatically deleted after two years. During an open records investigation, information was found on an employee's work computer concerning a conversation that occurred three years prior and proved damaging to the agency's reputation. Which of the following MOST likely caused the data leak?

A. The employee manually changed the email client retention settings to prevent deletion of emails
B. The file that contained the damaging information was mistagged and retained on the server for longer than it should have been
C. The email was encrypted and an exception was put in place via the data classification application
D. The employee saved a file on the computer's hard drive that contained archives of emails, which were more than two years old

Answer: D

NEW QUESTION 78
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 80
A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

A. When it is mandated by their legal and regulatory requirements
B. As soon as possible in the interest of the patients
C. As soon as the public relations department is ready to be interviewed
D. When all steps related to the incident response plan are completed
E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

Answer: A

NEW QUESTION 82
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 87
During a security event investigation, a junior analyst fails to create an image of a server's hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

A. Continuity of operations
B. Chain of custody
C. Order of volatility
D. Data recovery

Answer: C

NEW QUESTION 89
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 92

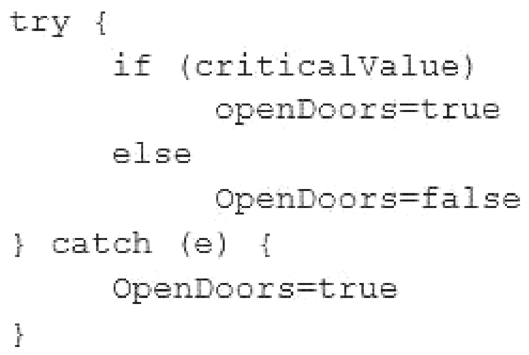
A company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

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 97

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



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

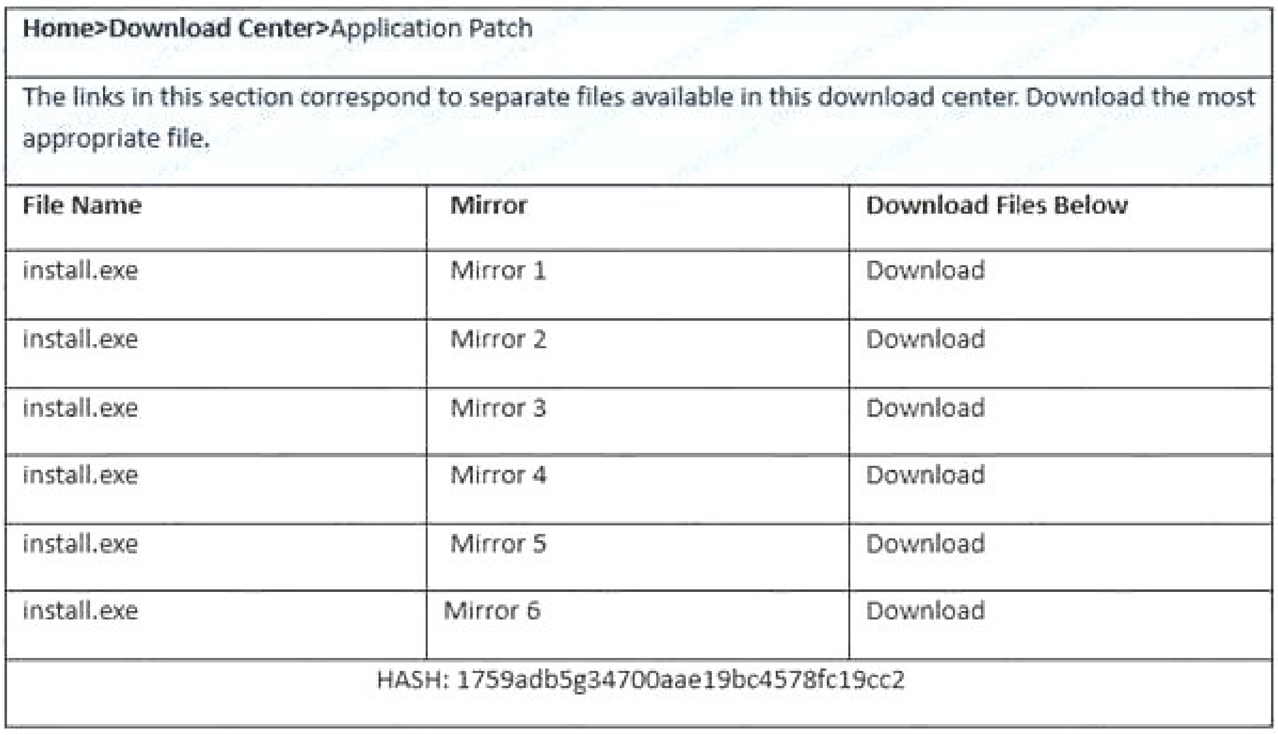
Which of the following is the BEST course of action for a security analyst to recommend to the software developer?

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

Answer: B

NEW QUESTION 99

Exhibit:

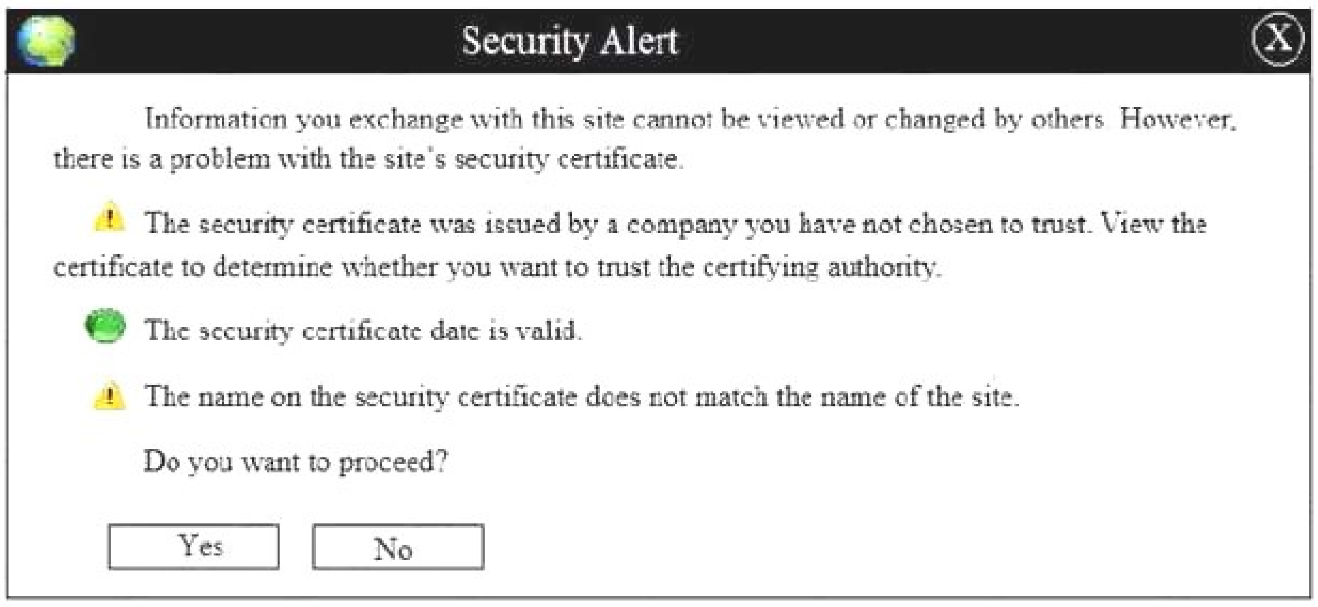


Home>Download Center>Application Patch

The links in this section correspond to separate files available in this download center. Download the most appropriate file.

File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2



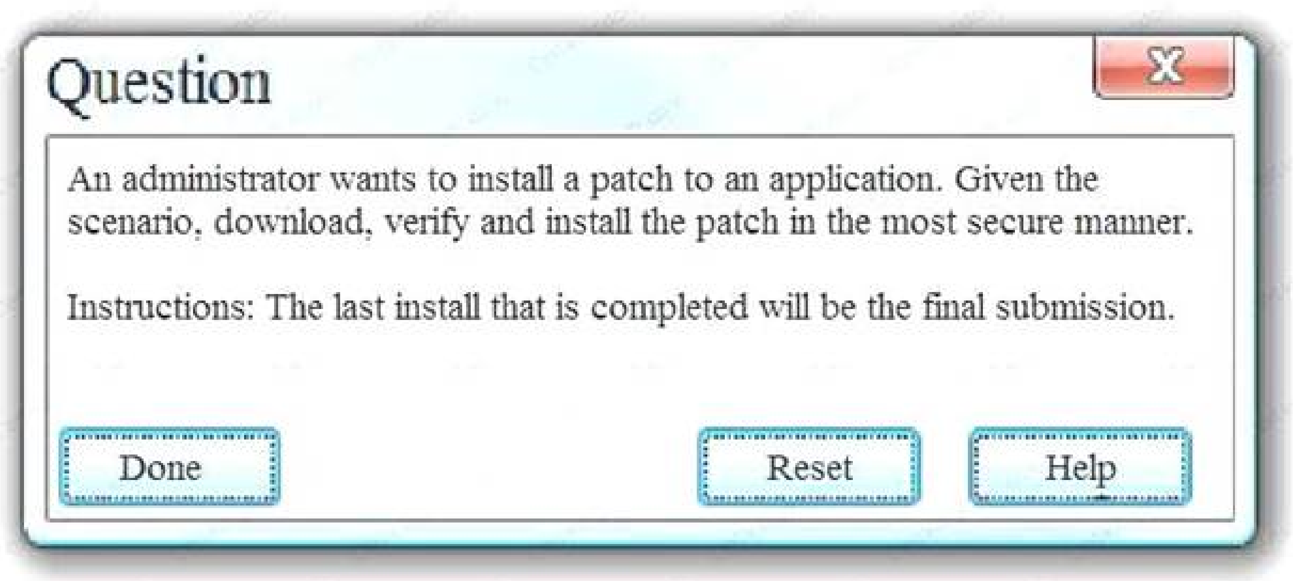
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate does not match the name of the site.

Do you want to proceed?



An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner.

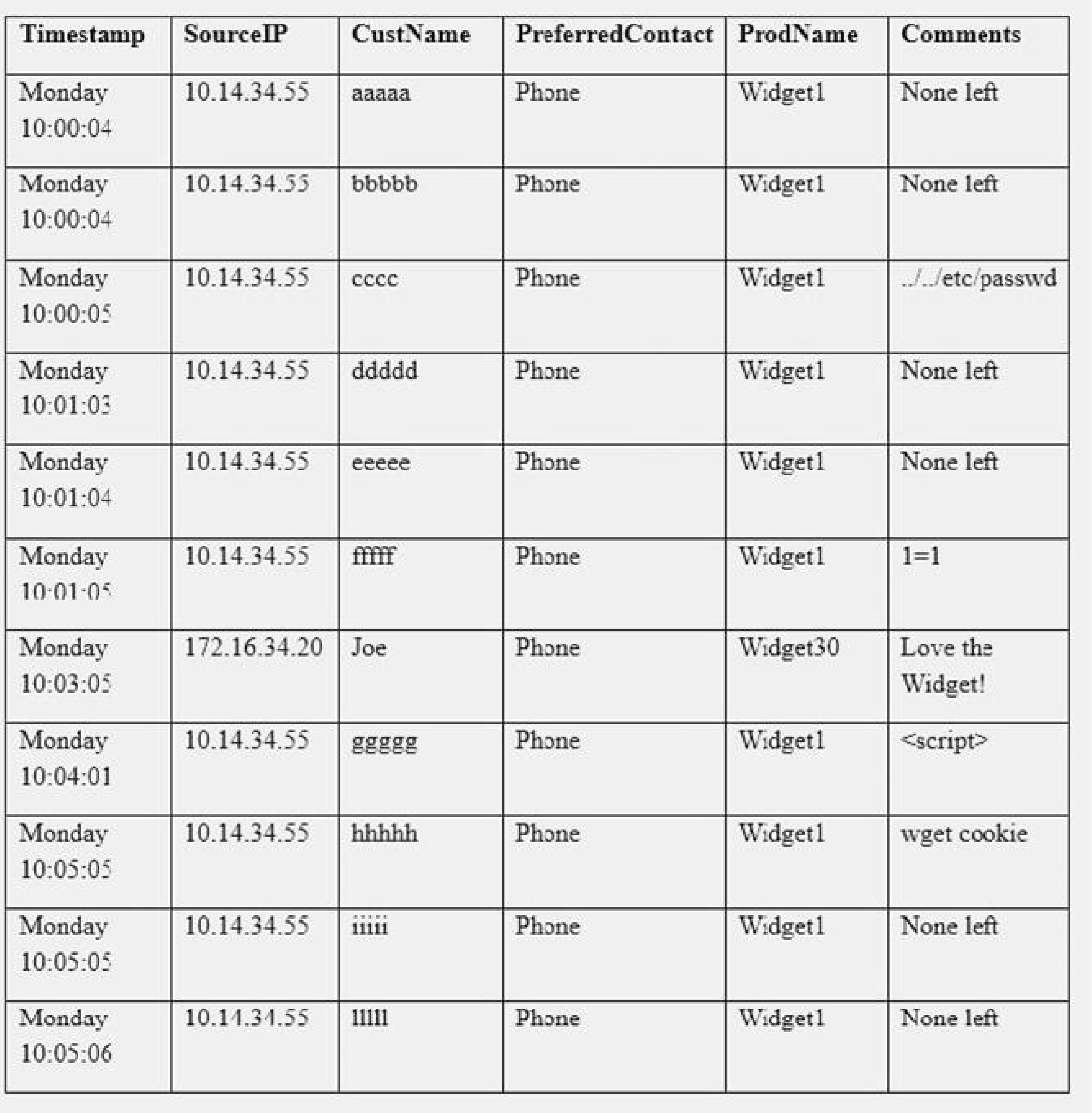
Instructions: The last install that is completed will be the final submission.

A. Step 1: Verify that the certificate is valid or no
B. In case of any warning message, cancel the download.Step 2: If certificate issue is not there then, download the file in your system.Step 3: Match the hash value of the downloaded file with the one which you selected on the websit
C. Step 4: Install the file if the hash value matches.
D. Step 1: Verify that the certificate is valid or no
E. In case of any warning message, cancel the download.Step 2: If certificate issue is not there then, download the file in your syste
F. Step 3: Calculate the hash value of the downloaded file.Step 4: Match the hash value of the downloaded file with the one which you selected on the websit
G. Step 5: Install the file if the hash value matches.

Answer: B

NEW QUESTION 102

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:



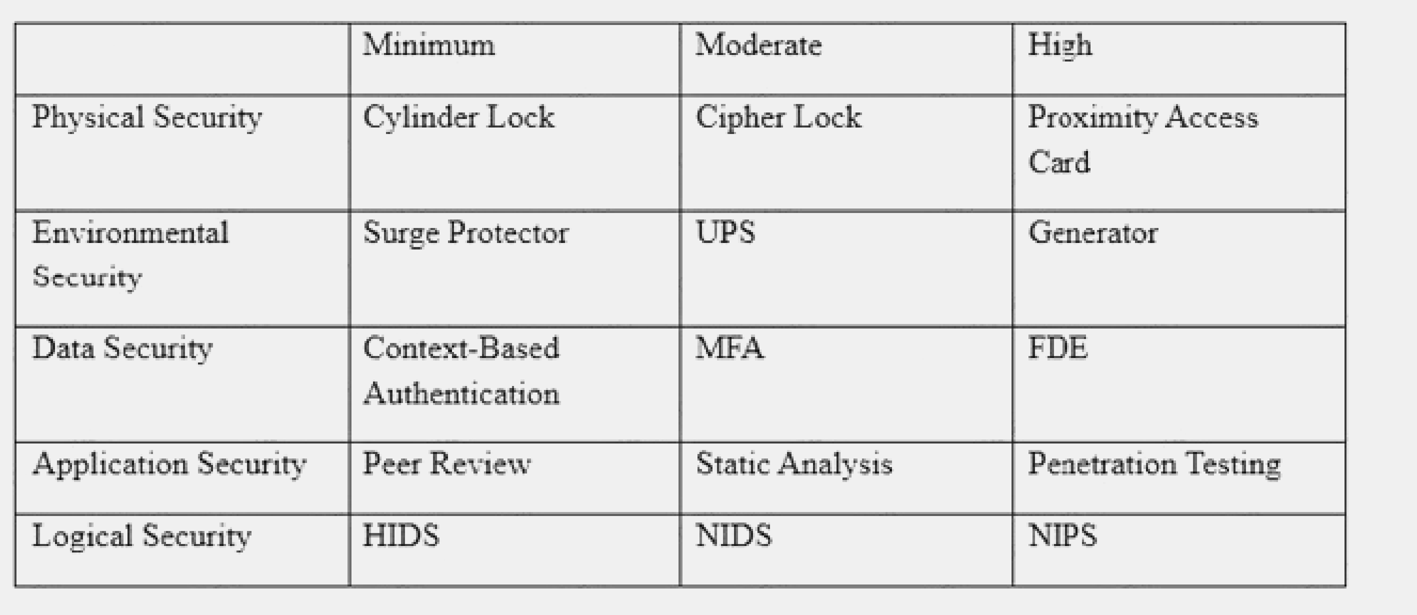
Timestamp	SourceIP	CustName	PreferredContact	ProdName	Comments
Monday 10:00:04	10.14.34.55	aaaaa	Phone	Widget1	None left
Monday 10:00:04	10.14.34.55	bbbbb	Phone	Widget1	None left
Monday 10:00:05	10.14.34.55	cccc	Phone	Widget1	../../etc/passwd
Monday 10:01:03	10.14.34.55	ddddd	Phone	Widget1	None left
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 106
An organization has established the following controls matrix:



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

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

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

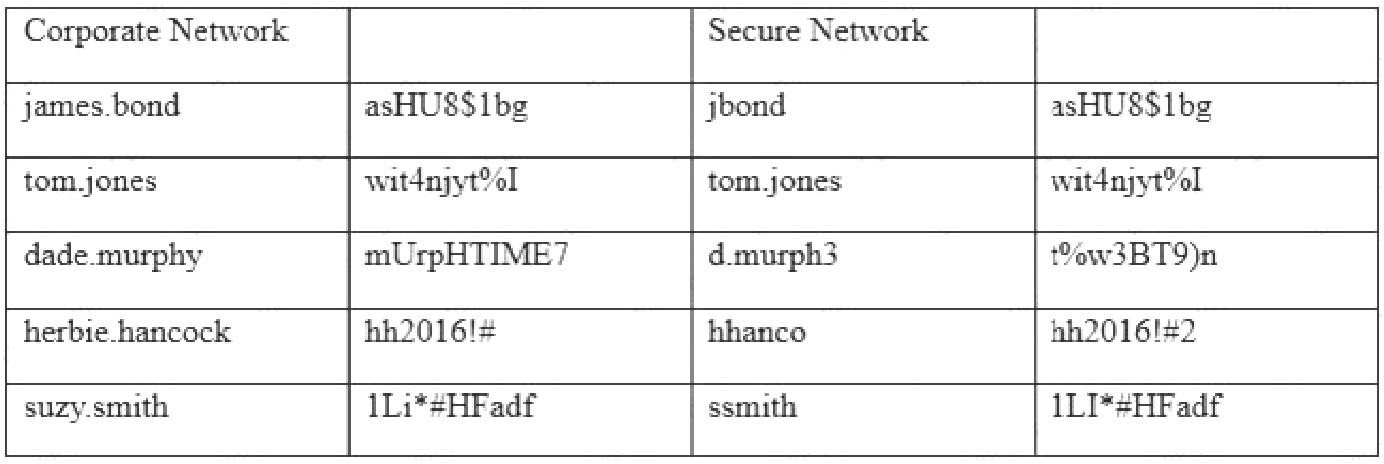
Answer: D

NEW QUESTION 109
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 114
An information security officer is responsible for one secure network and one office network. Recent intelligence suggests there is an opportunity for attackers to gain access to the secure network due to similar login credentials across networks. To determine the users who should change their information, the information security officer uses a tool to scan a file with hashed values on both networks and receives the following data:



Corporate Network		Secure Network	
james.bond	asHU8$1bg	jbond	asHU8$1bg
tom.jones	wit4njyt%I	tom.jones	wit4njyt%I
dade.murphy	mUrpHTIME7	d.murph3	t%w3BT9)n
herbie.hancock	hh2016!#	hhanco	hh2016!#2
suzy.smith	1Li*#HFadf	ssmith	1LI*#HFadf

Which of the following tools was used to gather this information from the hashed values in the file?

A. Vulnerability scanner
B. Fuzzer
C. MD5 generator
D. Password cracker
E. Protocol analyzer

Answer: C

NEW QUESTION 119
A Chief Information Security Officer (CISO is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization’s systems. The CISO knows improvements can be made to the guides.
Which of the following would be the BEST source of reference during the revision process?

A. CVE database
B. Internal security assessment reports
C. Industry-accepted standards
D. External vulnerability scan reports
E. Vendor-specific implementation guides

Answer: A

NEW QUESTION 122
Security policies that are in place at an organization prohibit USB drives from being utilized across the entire enterprise, with adequate technical controls in place to block them. As a way to still be able to work from various locations on different computing resources, several sales staff members have signed up for a web-based storage solution without the consent of the IT department. However, the operations department is required to use the same service to transmit certain business partner documents.
Which of the following would BEST allow the IT department to monitor and control this behavior?

A. Enabling AAA
B. Deploying a CASB
C. Configuring an NGFW
D. Installing a WAF
E. Utilizing a vTPM

Answer: B

NEW QUESTION 126
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 131
A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points. Which of the following solutions BEST meets the engineer’s goal?

A. Schedule weekly reviews of al unit test results with the entire development team and follow up between meetings with surprise code inspections.
B. Develop and implement a set of automated security tests to be installed on each development team leader’s workstation.
C. Enforce code quality and reuse standards into the requirements definition phase of the waterfall development process.
D. Deploy an integrated software tool that builds and tests each portion of code committed by developers and provides feedback.

Answer: C

NEW QUESTION 134
An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user’s accounts is sensitive, and therefore, the organization wants to comply with the following requirements:
Active full-device encryption Enabled remote-device wipe Blocking unsigned applications
Containerization of email, calendar, and contacts
Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements?

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

Answer: B

NEW QUESTION 139
An organization’s network engineering team recently deployed a new software encryption solution
to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data readwrite requests in storage, impacting business operations.
Which of the following alternative approaches would BEST address performance requirements while meeting the intended security objective?

A. Employ hardware FDE or SED solutions.
B. Utilize a more efficient cryptographic hash function.
C. Replace HDDs with SSD arrays.
D. Use a FIFO pipe a multithreaded software solutio

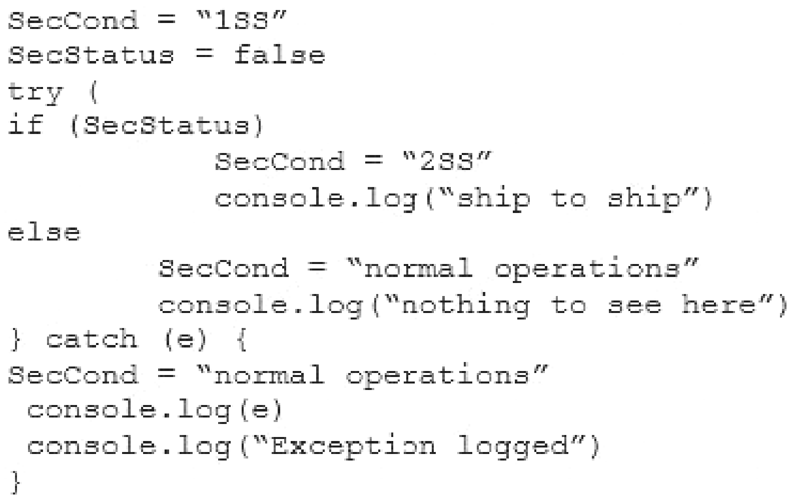
Answer: A

NEW QUESTION 143
Which of the following is the GREATEST security concern with respect to BYOD?

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

Answer: D

NEW QUESTION 145
Given the following code snippet:



```
SecCond = “1SS”
SecStatus = false
try (
if (SecStatus)
           SecCond = “2SS”
           console.log(“ship to ship”)
else
        SecCond = “normal operations”
        console.log(“nothing to see here”)
} catch (e) {
SecCond = “normal operations”
 console.log(e)
 console.log(“Exception logged”)
}
```

Which of the following failure modes would the code exhibit?

A. Open
B. Secure
C. Halt

D. Exception

Answer: D

NEW QUESTION 147
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 149
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 152
An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations. Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

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

Answer: B

NEW QUESTION 156
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 161
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 164
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 165
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 166
A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:
Configuration file 1: Operator ALL=/sbin/reboot Configuration file 2:
Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss Configuration file 3:
Operator:x:1000:1000::/home/operator:/bin/bash
Which of the following explains why an intended operator cannot perform the intended action?

A. The sudoers file is locked down to an incorrect command
B. SSH command shell restrictions are misconfigured
C. The passwd file is misconfigured
D. The SSH command is not allowing a pty session

Answer: D

NEW QUESTION 169
An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

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

Answer: C

NEW QUESTION 171
Company.org has requested a black-box security assessment be performed on key cyber terrain. On area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing. Which of the following commands should the assessor use to determine this information?

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

Answer: A

NEW QUESTION 174
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 176
An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:
Encrypt all traffic between the network engineer and critical devices. Segregate the different networking planes as much as possible.
Do not let access ports impact configuration tasks.
Which of the following would be the BEST recommendation for the network security engineer to present?

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

Answer: B

NEW QUESTION 180
A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers. Which of the following is the BEST statement for the engineer to take into consideration?

A. Single-tenancy is often more expensive and has less efficient resource utilizatio
B. Multi-tenancy may increase the risk of cross-customer exposure in the event of service vulnerabilities.
C. The managed service provider should outsource security of the platform to an existing cloud compan
D. This will allow the new log service to be launched faster and with well-tested security controls.
E. Due to the likelihood of large log volumes, the service provider should use a multi-tenancy model for the data storage tier, enable data deduplication for storage cost efficiencies, and encrypt data at rest.
F. The most secure design approach would be to give customers on-premises appliances, install agents on endpoints, and then remotely manage the service via a VPN.

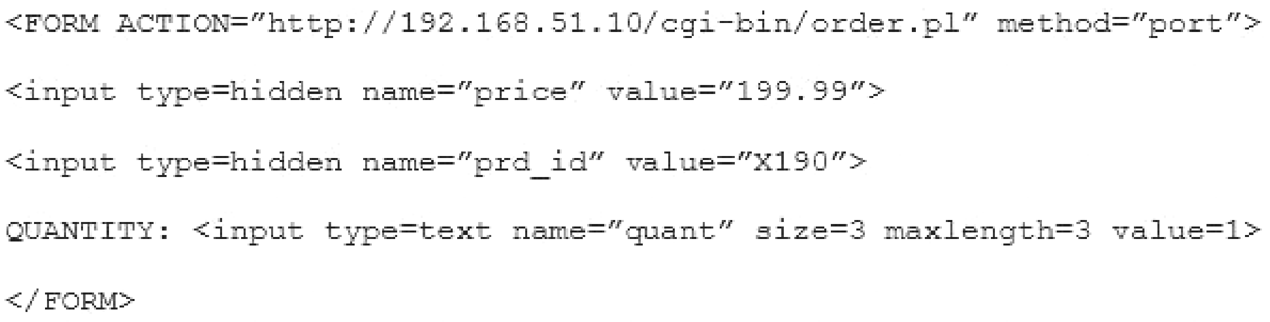
Answer: A

NEW QUESTION 184
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 189
Given the following code snippet:



```
<FORM ACTION="http://192.168.51.10/cgi-bin/order.pl" method="port">

<input type=hidden name="price" value="199.99">

<input type=hidden name="prd_id" value="X190">

QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=1>

</FORM>
```

Of which of the following is this snippet an example?

A. Data execution prevention
B. Buffer overflow
C. Failure to use standard libraries
D. Improper filed usage
E. Input validation

Answer: D

NEW QUESTION 194
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^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/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 199
A company has decided to lower costs by conducting an internal assessment on specific devices and various internal and external subnets. The assessment will be done during regular office hours, but it must not affect any production servers. Which of the following would MOST likely be used to complete the assessment? (Select two.)

A. Agent-based vulnerability scan
B. Black-box penetration testing
C. Configuration review
D. Social engineering
E. Malware sandboxing
F. Tabletop exercise

Answer: AC

NEW QUESTION 201
Which of the following is a feature of virtualization that can potentially create a single point of failure?

A. Server consolidation
B. Load balancing hypervisors
C. Faster server provisioning
D. Running multiple OS instances

Answer: A

NEW QUESTION 205
A cybersecurity analyst has received an alert that well-known "call home" messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the massages. After determining the alert was a true positive, which of the following represents OST likely cause?

A. Attackers are running reconnaissance on company resources.
B. An outside command and control system is attempting to reach an infected system.
C. An insider trying to exfiltrate information to a remote network.
D. Malware is running on a company system

Answer: B

NEW QUESTION 209
A cybersecurity analyst is hired to review the security the posture of a company. The cybersecurity analyst notice a very high network bandwidth consumption due to SYN floods from a small number of IP addresses. Which of the following would be the BEST action to take to support incident response?

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

Answer: B

NEW QUESTION 213
Which of the following system would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect ... secrecy?

A. Endpoints
B. VPN concentrators
C. Virtual hosts
D. SIEM
E. Layer 2 switches

Answer: B

NEW QUESTION 216
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After invest the new vulnerability, it was determined that the web services providing are being impacted by this new threat. Which of the following data types a MOST likely at risk of exposure based on this new threat? (Select TWO)

A. Cardholder data
B. intellectual property

C. Personal health information
D. Employee records
E. Corporate financial data

Answer: AC

NEW QUESTION 217
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines. Which of the following represents a FINAL step in the prediction of the malware?

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

Answer: C

NEW QUESTION 218
Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

A. Enable multipath to increase availability
B. Enable deduplication on the storage pools
C. Implement snapshots to reduce virtual disk size
D. Implement replication to offsite datacenter

Answer: B

Explanation:
Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.
It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.
Incorrect Answers:
A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.
D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:
https://en.wikipedia.org/wiki/Data_deduplication

NEW QUESTION 219
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 221
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 222
After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.
SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);
The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the $USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being explogted to manipulate the price of a shopping cart's items?

A. Input validation
B. SQL injection
C. TOCTOU
D. Session hijacking

Answer: C

Explanation:
In this question, TOCTOU is being explogted to allow the user to modify the temp file that contains the price of the item.
In software development, time of check to time of use (TOCTOU) is a class of software bug caused by
changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition.
A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.
Incorrect Answers:
A: 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. The explogt in this question is not an example of input validation.
B: SQL injection is a type of security explogt in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to dat
A. The explogt
in this question is not an example of a SQL injection attack.
D: Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by obtaining the session ID and masquerading as the authorized user. The explogt in this question is not an example of session hijacking.
References: https://en.wikipedia.org/wikiHYPERLINK
"https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use"/Time_of_check_to_time_of_use

NEW QUESTION 224
The administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Whichof the following issues may potentially occur?

A. The data may not be in a usable format.
B. The new storage array is not FCoE based.
C. The data may need a file system check.
D. The new storage array also only has a single controlle

Answer: B

Explanation:
Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol.
When moving the disks to another storage array, you need to ensure that the array supports FCoE, not just regular Fiber Channel. Fiber Channel arrays and Fiber Channel over Ethernet arrays use different network connections, hardware and protocols. Fiber Channel arrays use the Fiber Channel protocol over a dedicated Fiber Channel network whereas FCoE arrays use the Fiber Channel
protocol over an Ethernet network. Incorrect Answers:
A: It is unlikely that the data will not be in a usable format. Fiber Channel LUNs appear as local disks on a Windows computer. The computer then creates an NTFS volume on the fiber channel LUN. The storage array does not see the NTFS file system or the data stored on it. FCoE arrays only see the underlying block level storage.
C: The data would not need a file system check. FCoE arrays use block level storage and do not check the file system. Any file system checks would be performed by a Windows computer. Even if this happened, the data would be accessible after the check.
D: The new storage array also having a single controller would not be a problem. Only one controller is required.

References: https://en.wikipedia.org/wiki/Fibre_HYPERLINK "https://en.wikipedia.org/wiki/Fibre_Channel_over_Ethernet"Channel_over_Ethernet

NEW QUESTION 229
Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

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

Answer: E

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

NEW QUESTION 231
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 232
A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

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

Answer: A

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

NEW QUESTION 234
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 238
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 240
The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show
the following:

```
90.76.165.40 – - [08/Mar/2014:10:54:04] “GET calendar.php?create%20table%20hidden HTTP/1.1” 200 5724
90.76.165.40 – - [08/Mar/2014:10:54:05] “GET ../../../root/.bash_history HTTP/1.1” 200 5724 90.76.165.40 – - [08/Mar/2014:10:54:04] “GET
index.php?user=<script>Create</script> HTTP/1.1” 200 5724
```

The security administrator also inspects the following file system locations on the database server using the command ‘ls -al /root’

```
drwxrwxrwx 11 root root 4096 Sep 28 22:45 .
drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..
-rws------ 25 root root 4096 Mar 8 09:30 .bash_history
-rw------- 25 root root 4096 Mar 8 09:30 .bash_history
-rw------- 25 root root 4096 Mar 8 09:30 .profile
-rw------- 25 root root 4096 Mar 8 09:30 .ssh
```

Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

A. Privilege escalation
B. Brute force attack
C. SQL injection
D. Cross-site scripting
E. Using input validation, ensure the following characters are sanitized: <>
F. Update crontab with: find / \(-perm -4000 \) –type f –print0 | xargs -0 ls –l | email.sh
G. Implement the following PHP directive: $clean_user_input = addslashes($user_input)
H. Set an account lockout policy

Answer: AF

Explanation:
This is an example of privilege escalation.
Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been ‘escalated’.
Now that we know the system has been attacked, we should investigate what was done to the system.
The command “Update crontab with: find / \(-perm -4000 \) –type f –print0 | xargs -0 ls –l | email.sh” is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user executing that executable file gets the permissions of the individual or group that owns the file.
Incorrect Answers:
B: A brute force attack is used to guess passwords. This is not an example of a brute force attack. C: 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). This is not an example of a SQL Injection attack.
D: 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. This is not an example of an XSS attack.
E: Sanitizing just the <> characters will not prevent such an attack. These characters should not be sanitized in a web application.
G: Adding slashes to the user input will not protect against the input; it will just add slashes to it.
H: An account lockout policy is useful to protect against password attacks. After a number of incorrect passwords, the account will lockout. However, the attack in this question is not a password attack so a lockout policy won’t help.

NEW QUESTION 242
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 244
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 248
An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

A. Implementing federated network access with the third party.
B. Using a HSM at the network perimeter to handle network device access.
C. Using a VPN concentrator which supports dual factor via hardware tokens.
D. Implementing 802.1x with EAP-TTLS across the infrastructur

Answer: D

Explanation:
IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital
certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.
EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the
server certificates. Incorrect Answers:
A: Federated network access provides user access to networks by using a single logon. The logon is authenticated by a party that is trusted to all the networks. It does not ensure that all devices that connect to its networks have been previously approved.
B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. It does not ensure that all devices that connect to its networks have been previously approved.
C: A VPN concentrator provides VPN connections and is typically used for creating site-to-site VPN architectures. It does not ensure that all devices that connect to its networks have been previously approved.
References: http://en.wikipedia.org/wiki/IEEE_802.1X
https://www.juniper.net/techpubs/software/aHYPERLINK "https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html"aa_802/HYPERLINK "https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP- 024.html"sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html

NEW QUESTION 249
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 250
A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

A. Use AES in Electronic Codebook mode
B. Use RC4 in Cipher Block Chaining mode
C. Use RC4 with Fixed IV generation
D. Use AES with cipher text padding
E. Use RC4 with a nonce generated IV
F. Use AES in Counter mode

Answer: EF

Explanation:
In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.
Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.
AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.
Incorrect Answers:
A: AES in Electronic Codebook mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.
B: RC4 in Cipher Block Chaining mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 (not in Cipher Block Chaining mode) or AES in Counter Mode.
C: You cannot use fixed IV generation for RC4 when encrypting streaming video.
D: AES with cipher text padding cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.
References: https://en.wikipedia.org/wiki/Initialization_vector

NEW QUESTION 252
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 255
A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway.
Which of the following controls MUST be implemented to enable stateless communication?

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

Answer: D

Explanation:
JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.
Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help?
The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.
However there are some drawbacks to session identifiers:
They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.
They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a database to figure out who this session is for and if they are allowed to perform the requested operation.
JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format.
JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.
How To Store JWTs In The Browser
Short Answer:: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along
the token for authentication purposes, but won't expose it to the JavaScript environment. Incorrect Answers:
A: A one-time key does not enable stateless communication.
B: SSL between the mobile application and the web services gateway will provide a secure encrypted connection between the two. However, SSL does not enable stateless communication.
C: A cookie is stateful, not stateless as required in the question. References:
https://stormpath.com/blog/build-secure-user-interfaces-using-jwtHYPERLINK "https://stormpath.com/blog/build-secure-user-interfaces-using-jwts/"s/

NEW QUESTION 259
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 security tester is testing a website and performs the following manual query: https://www.comptia.com/cookies.jsp?products=5%20and%201=1
The following response is received in the payload: "ORA-000001: SQL command not properly ended" Which of the following is the response an example of?

A. Fingerprinting
B. Cross-site scripting
C. SQL injection
D. Privilege escalation

Answer: A

Explanation:

This is an example of Fingerprinting. The response to the code entered includes “ORA-000001” which tells the attacker that the database software being used is Oracle.
Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished “passively” by sniffing network packets passing between hosts, or it can be accomplished “actively” by transmitting specially created packets to the target machine and analyzing the response.
Incorrect Answers:
B: 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 an example of XSS.
C: 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). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.
D: Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.
References: http://www.yourdictionary.com/fingerprinting

NEW QUESTION 264
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 267
Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 1
B. 3
C. 6

Answer: C

Explanation:
You would need three wildcard certificates:
*. east.company.com
*. central.company.com
*. west.company.com
The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: *. company.com will cover “<anything>.company.com” but it won’t
cover “<anything>.<anything>.company.com”.
You can only have one wildcard in a domain. For example: *.company.com. You cannot have
..company.com. Only the leftmost wildcard (*) is counted. Incorrect Answers:
A: You cannot secure public facing server farms without any SSL certificates.
B: You need three wildcard certificates, not one. A wildcard covers only one level of subdomain. D: You do not need six wildcard certificates to secure three domains.
References:
https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certifiHYPERLINK "https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567"cate-567

NEW QUESTION 271
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 275
A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated.
Users of the web application will not be added to the company's directory services. Passwords must not be stored in the code.
Which of the following meets these requirements?

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

Answer: A

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

NEW QUESTION 279
The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.
Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

A. Revise the corporate policy to include possible termination as a result of violations
B. Increase the frequency and distribution of the USB violations report
C. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offense
D. Implement group policy objects

Answer: D

Explanation:
A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.
One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.
This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.
Incorrect Answers:
A: Threatening the users with termination for violating the acceptable use policy may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
B: Increasing the frequency and distribution of the USB violations report may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
C: Offenders not being able to deny the offense will make it easier to prove the offense. However, it
does not prevent the offense in the first place and therefore is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
References:
http://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/

NEW QUESTION 280
Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

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

Answer: A

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

NEW QUESTION 282
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
......