CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

NEW QUESTION 1
An engineer needs to provide access to company resources for several offshore contractors. The contractors require:
Access to a number of applications, including internal websites Access to database data and the ability to manipulate it
The ability to log into Linux and Windows servers remotely
Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

A. VTC
B. VRRP
C. VLAN
D. VDI
E. VPN
F. Telnet

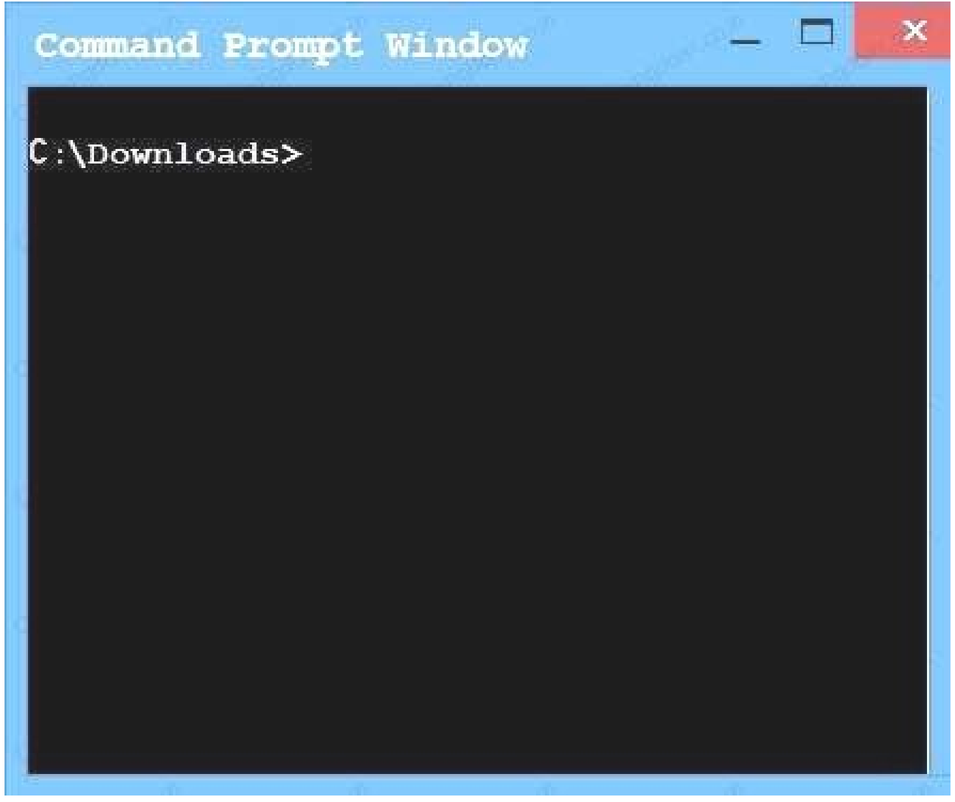
Answer: DE

NEW QUESTION 2
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?

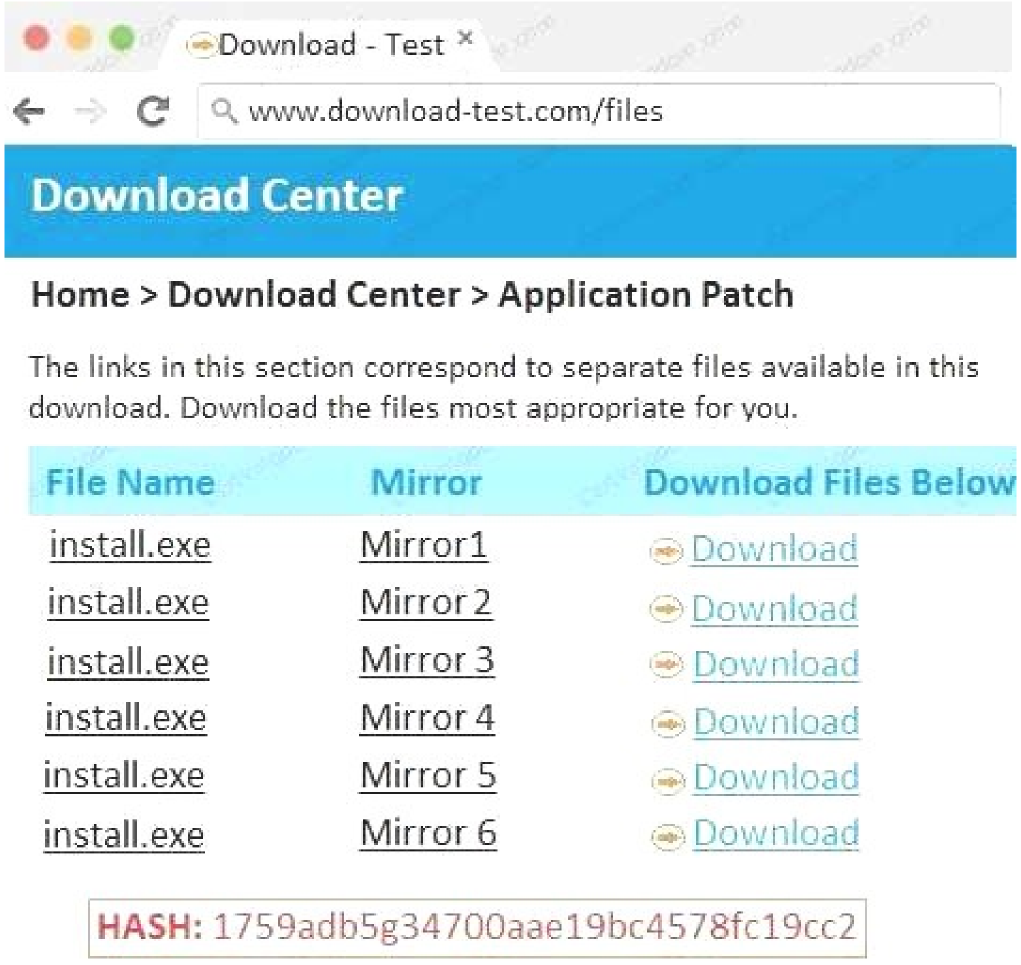
A. Avoid
B. Mitigate
C. Transfer
D. Accept

Answer: B

NEW QUESTION 3
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>
```



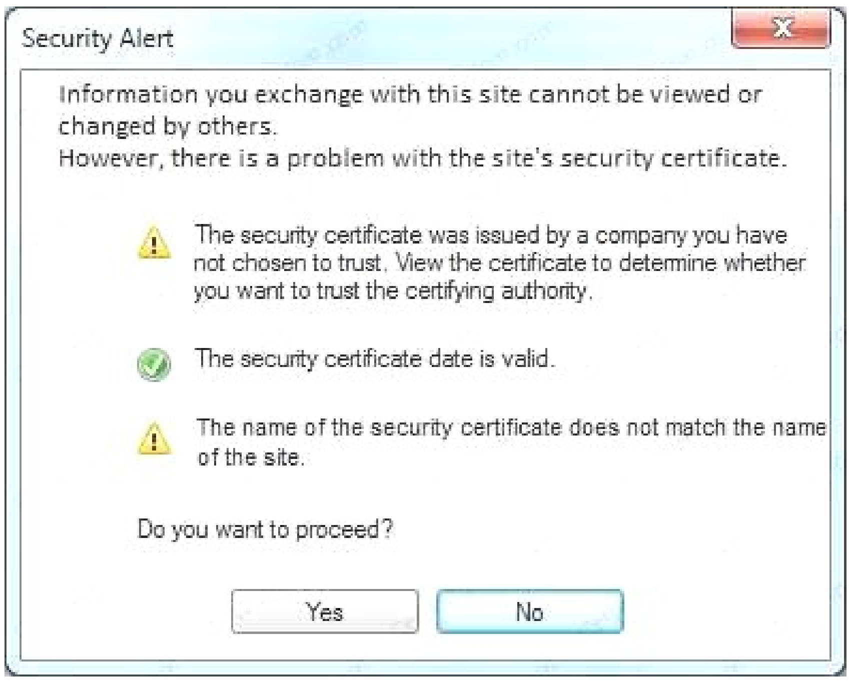
Download Center

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

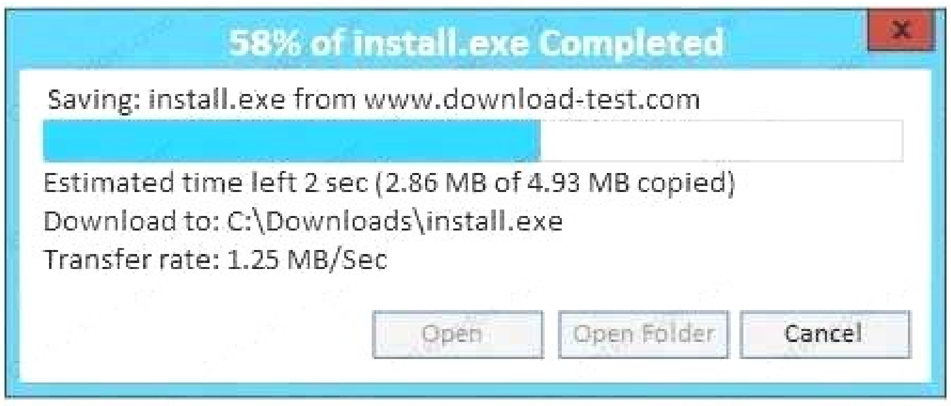
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate.

⚠ 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.

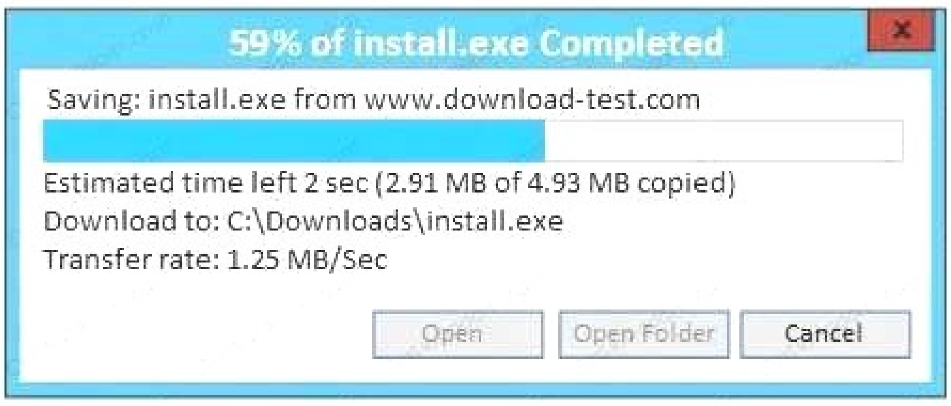
Do you want to proceed?



58% of install.exe Completed

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

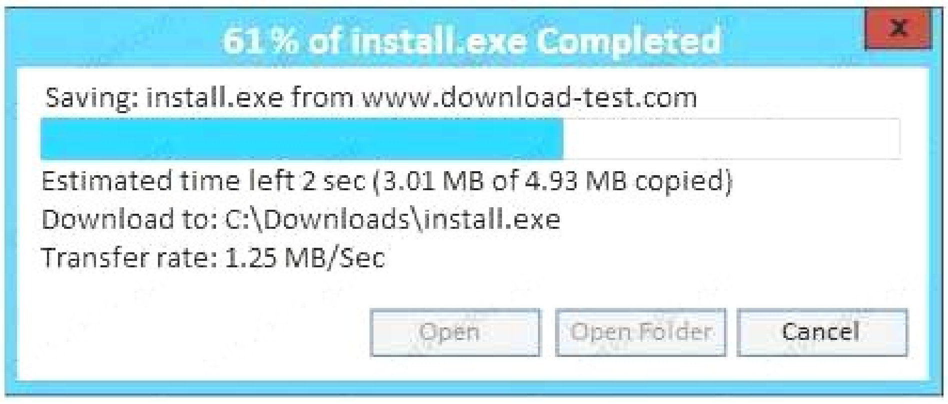
Estimated time left 2 sec (2.86 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec



59% of install.exe Completed

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

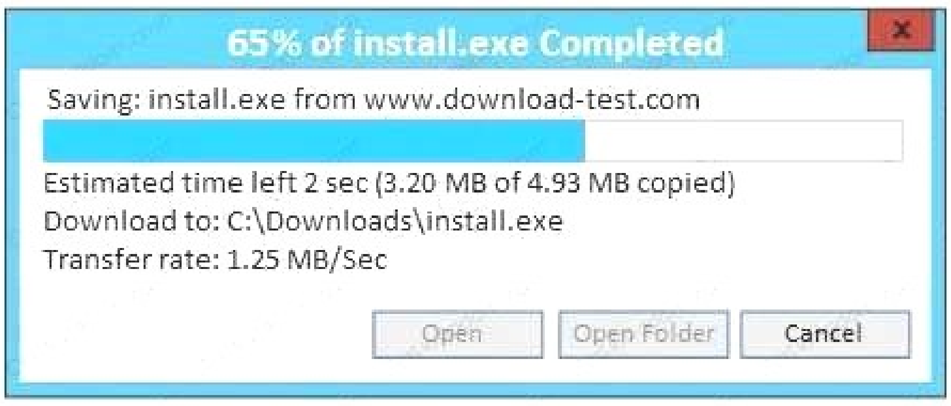
Estimated time left 2 sec (2.91 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec



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

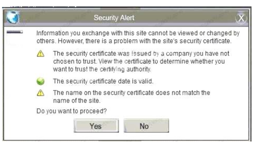
Saving: install.exe from www.download-test.com

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.

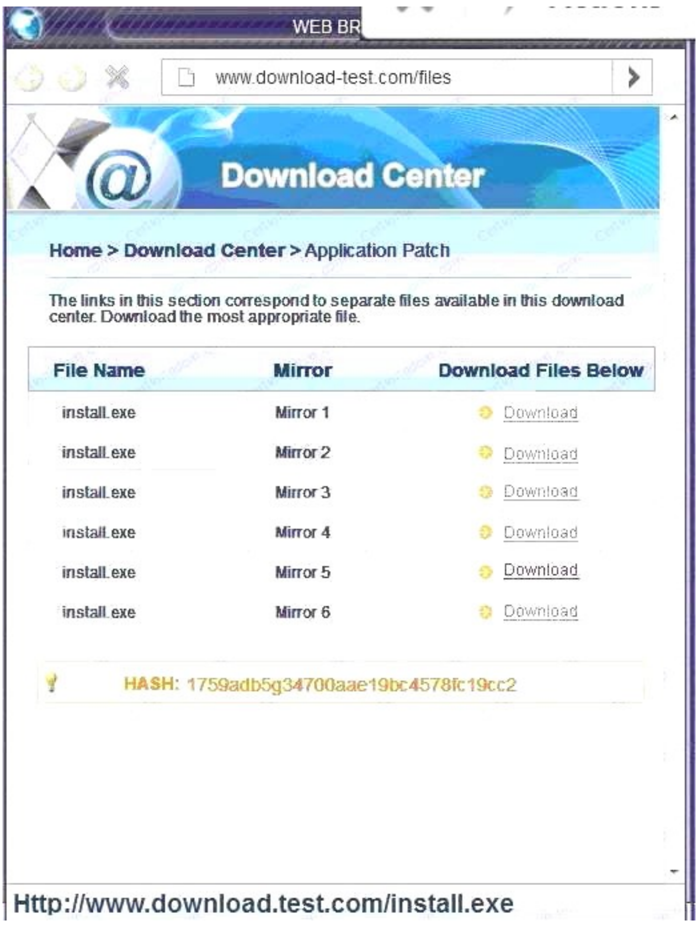
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

● 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.

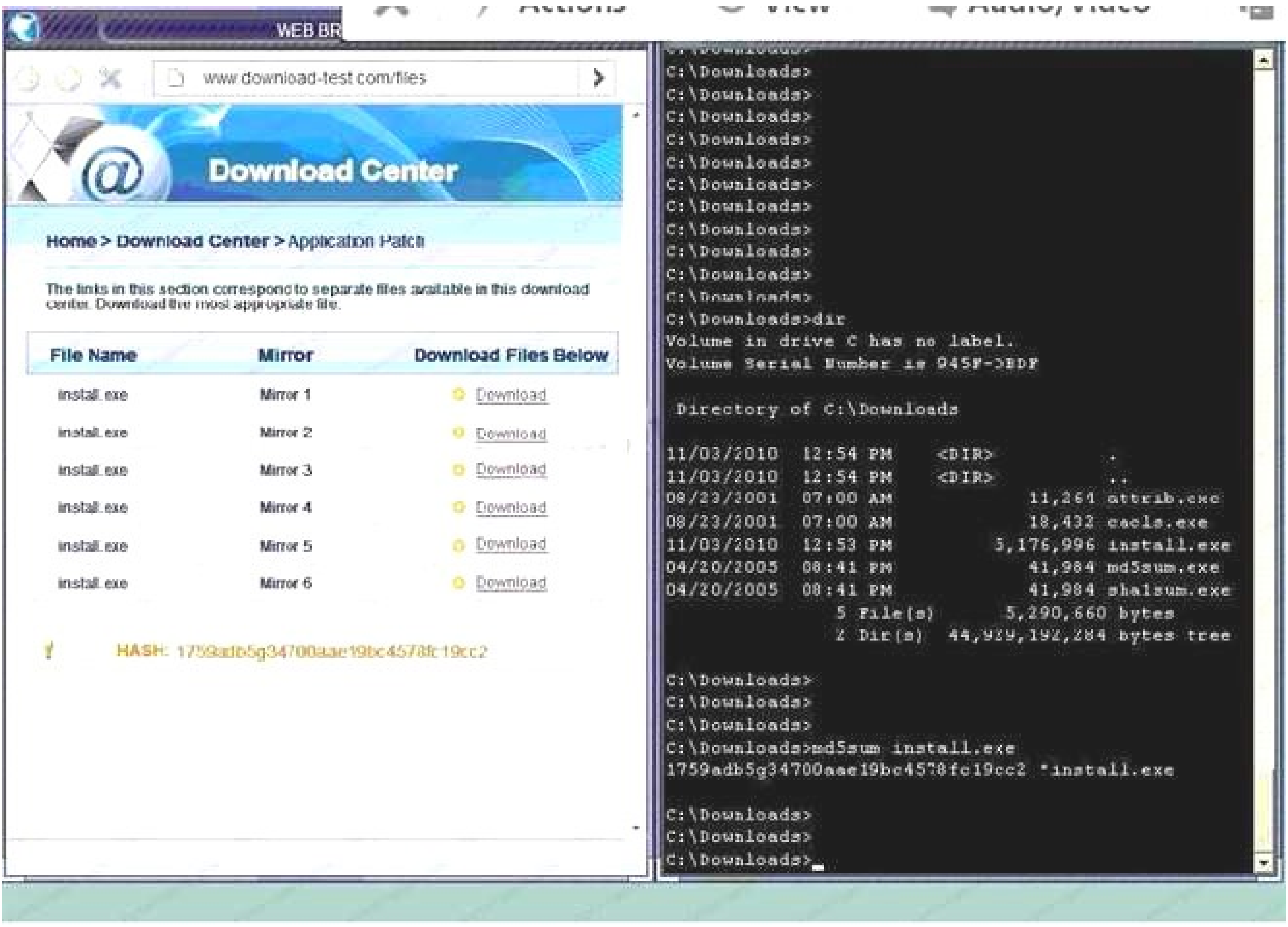
File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

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.

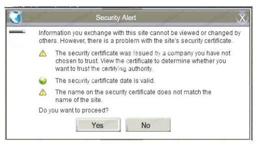
File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

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 945F-3EDF

 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.

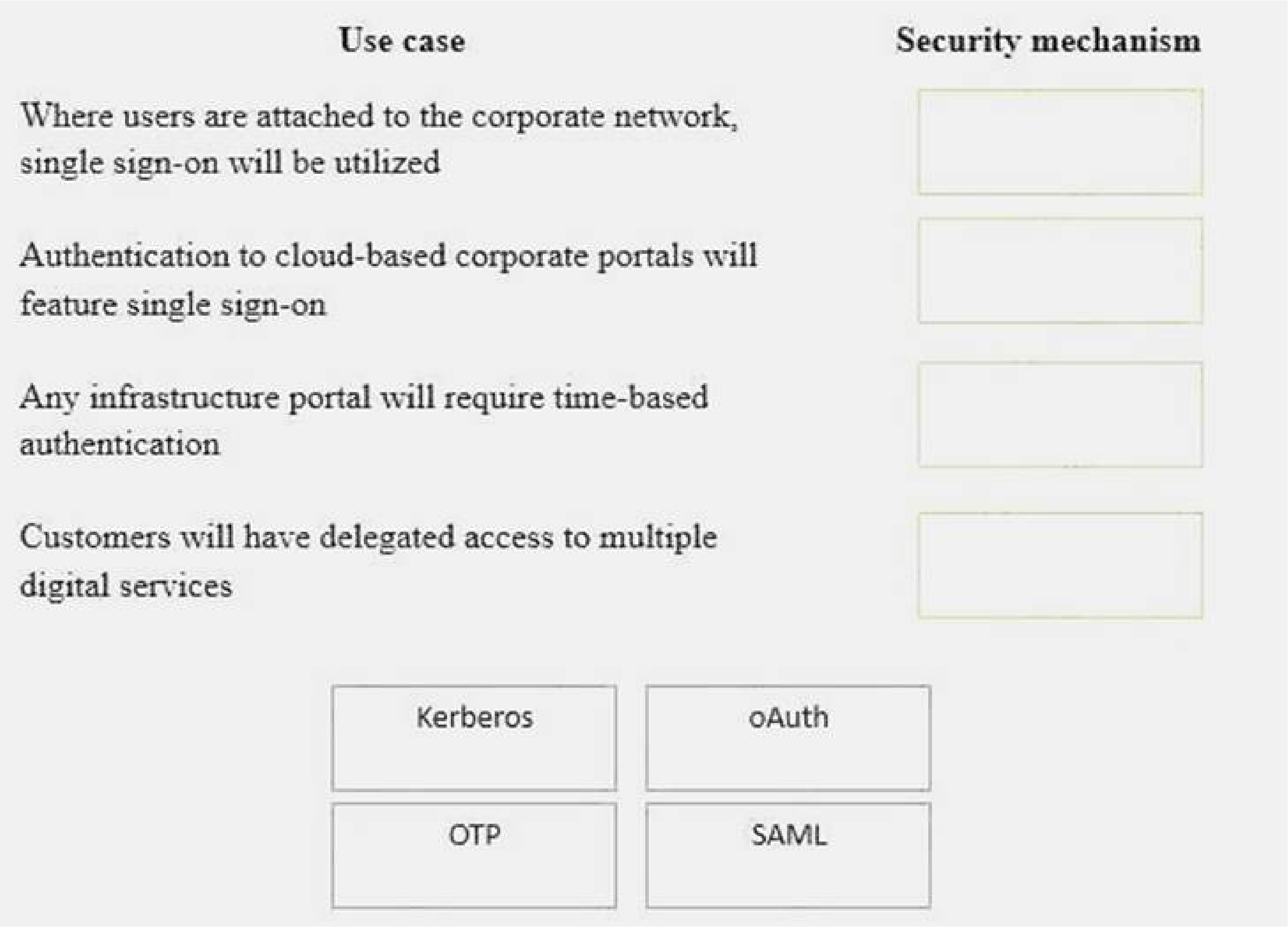
⚠ The name on the security certificate does not match the name of the site.

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 4
DRAG DROP
A security consultant is considering authentication options for a financial institution. The following authentication options are available security mechanism to the appropriate use case. Options may be used once.



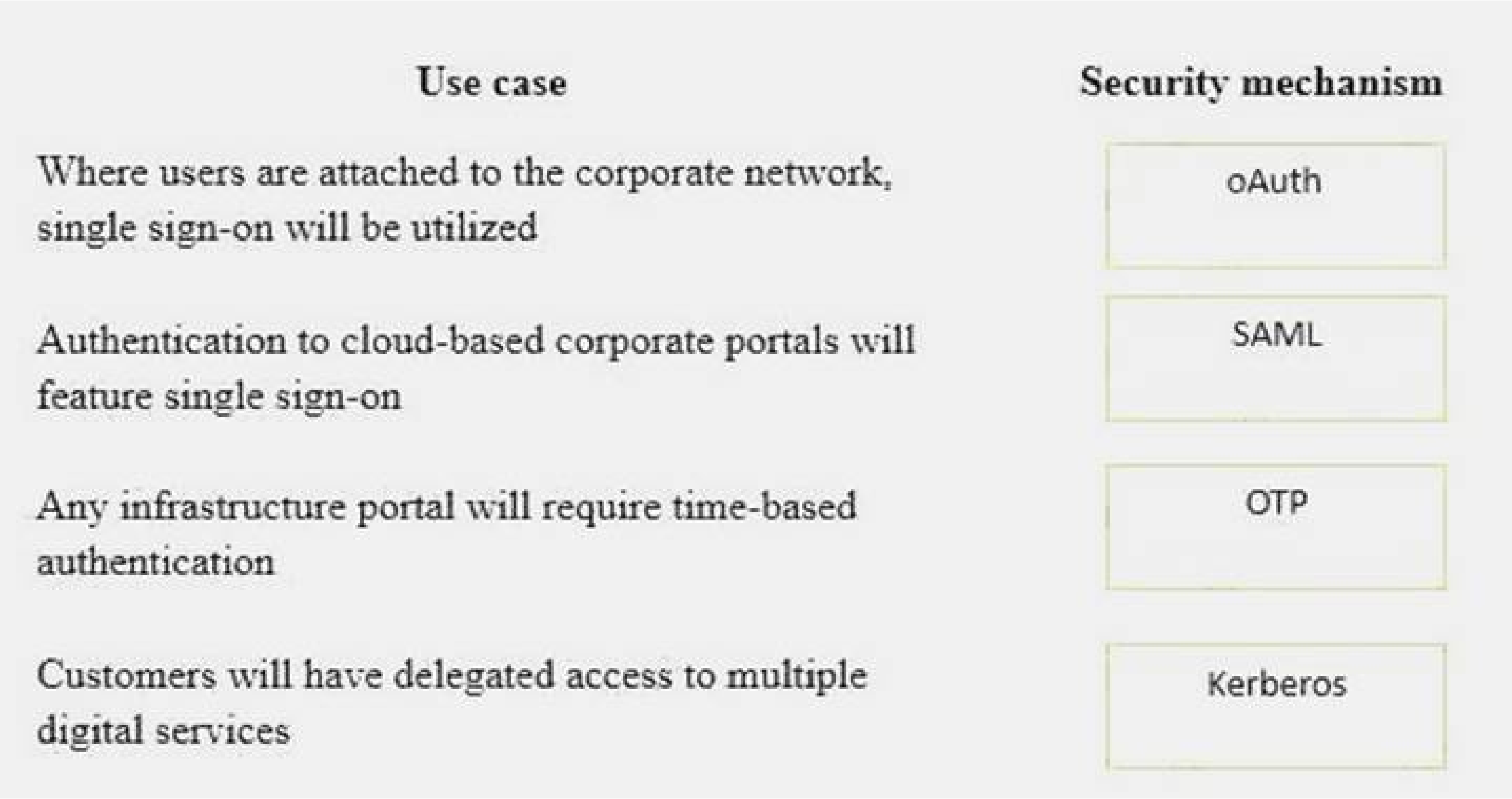
Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	
Authentication to cloud-based corporate portals will feature single sign-on	
Any infrastructure portal will require time-based authentication	
Customers will have delegated access to multiple digital services	

Kerberos
oAuth
OTP
SAML

A. Mastered
B. Not Mastered

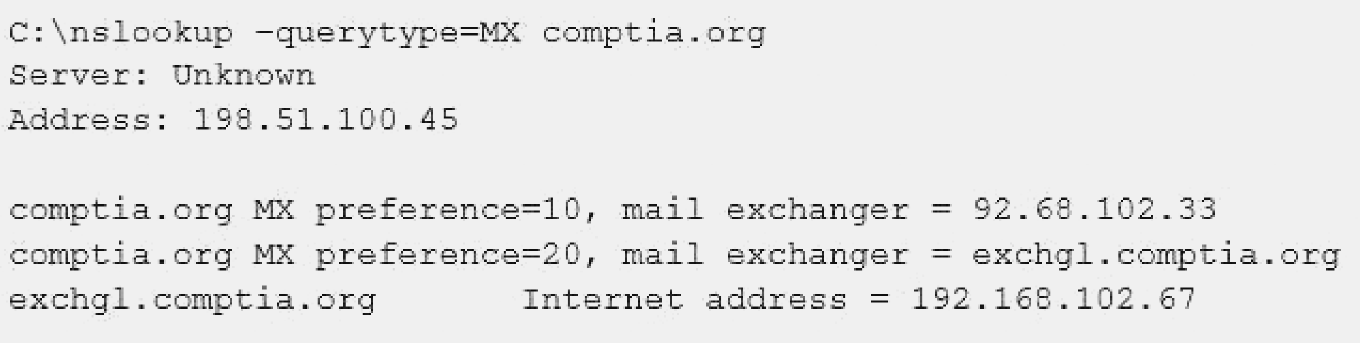
Answer: A

Explanation:



Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	oAuth
Authentication to cloud-based corporate portals will feature single sign-on	SAML
Any infrastructure portal will require time-based authentication	OTP
Customers will have delegated access to multiple digital services	Kerberos

NEW QUESTION 5
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:



```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured
B. Comptia.org is running an older mail server, which may be vulnerable to exploqts
C. The DNS SPF records have not been updated for Comptia.org
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

Answer: B

NEW QUESTION 6
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploqted so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions.
Which of the following approaches is described?

A. Blue team
B. Red team
C. Black box
D. White team

Answer: C

NEW QUESTION 7
A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

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

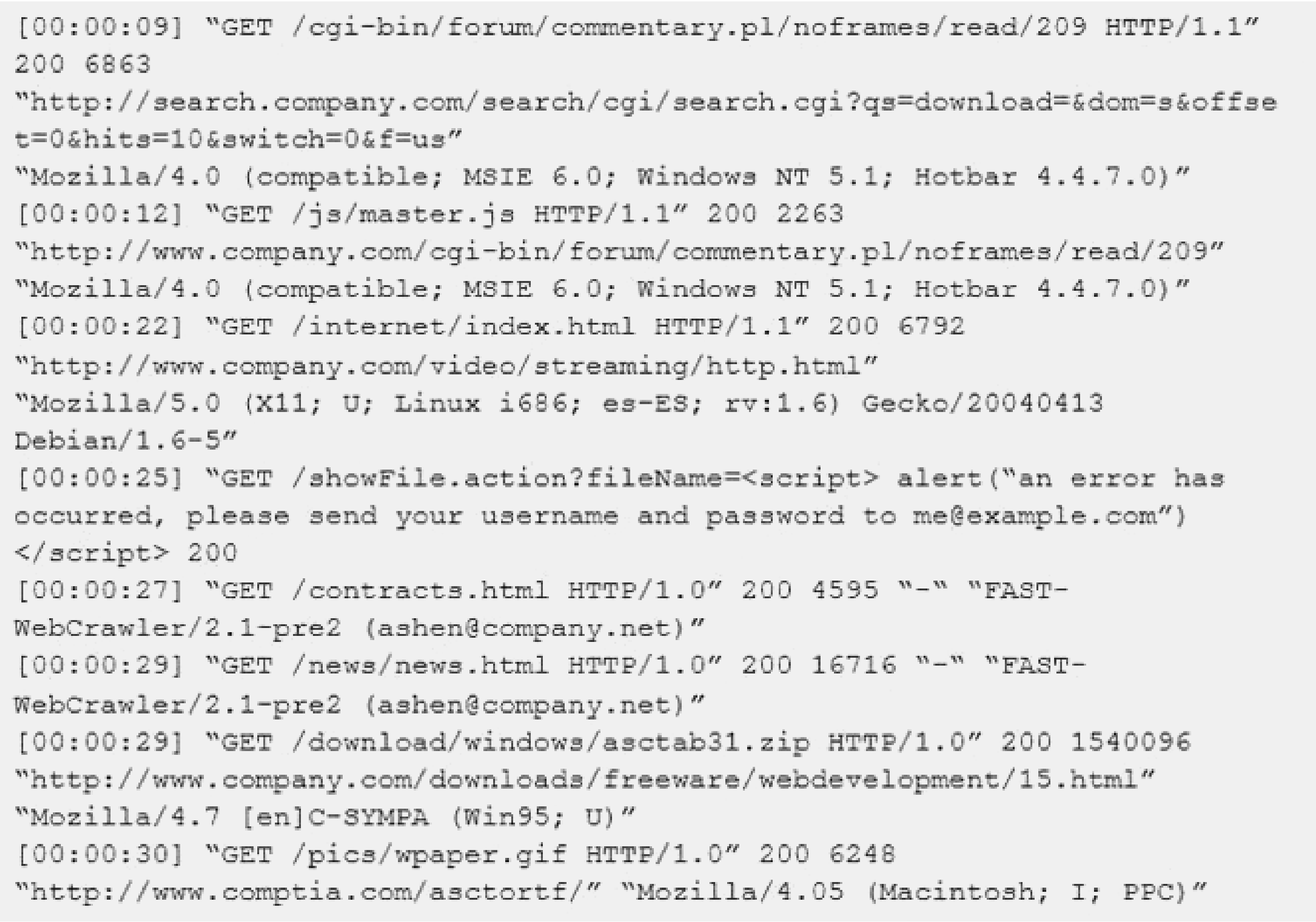
Answer: EF

NEW QUESTION 8
An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents.
The following observations have been identified:
The ICS supplier has specified that any software installed will result in lack of support.
There is no documented trust boundary defined between the SCADA and corporate networks.
Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.
Which of the following capabilities would BEST improve the security position?

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

Answer: A

NEW QUESTION 9
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 10
The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristicsfor anomaly detection
D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

Answer: B

NEW QUESTION 10
After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company’s IT department has seen a large number of the following incidents:
Duplicate IP addresses Rogue network devices
Infected systems probing the company’s network
Which of the following should be implemented to remediate the above issues? (Choose two.)

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

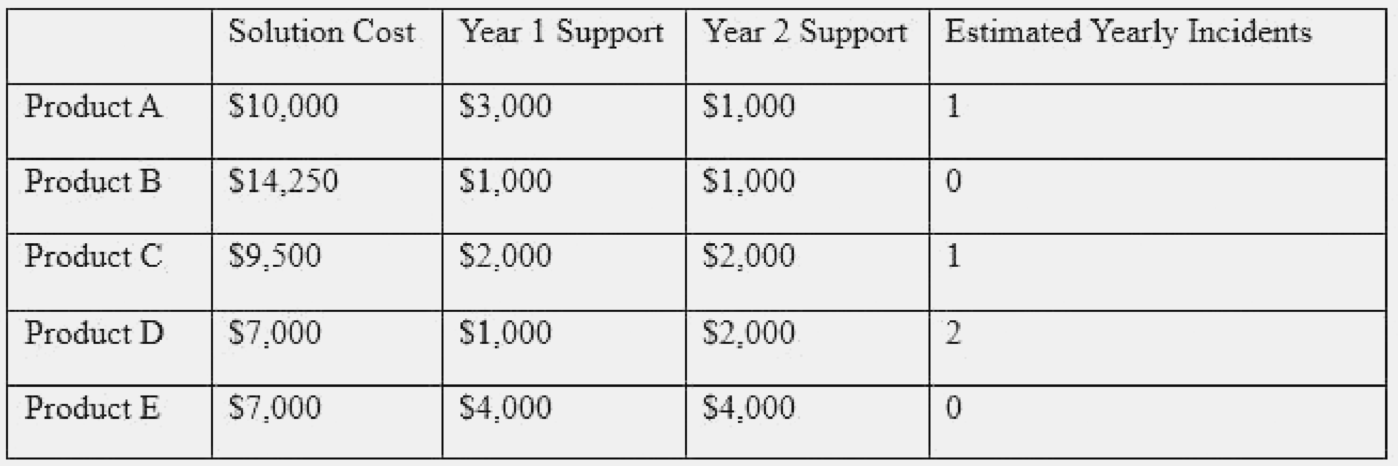
Answer: BC

NEW QUESTION 12
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 14
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 18
The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day explogt utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO's request?

A. 1. Perform the ongoing research of the best practices2. Determine current vulnerabilities and threats3. Apply Big Data techniques4. Use antivirus control
B. 1. Apply artificial intelligence algorithms for detection2. Inform the CERT team3. Research threat intelligence and potential adversaries4. Utilize threat intelligence to apply Big Data techniques
C. 1. Obtain the latest IOCs from the open source repositories2. Perform a sweep across the network to identify positive matches3. Sandbox any suspicious files4. Notify the CERT team to apply a future proof threat model
D. 1. Analyze the current threat intelligence2. Utilize information sharing to obtain the latest industry IOCs3. Perform a sweep across the network to identify positive matches4. Apply machine learning algorithms

Answer: C

NEW QUESTION 19
A forensics analyst suspects that a breach has occurred. Security logs show the company's OS patch system may be compromised, and it is serving patches that contain a zero-day explogt and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server. Which of the following should the analyst use to confirm this suspicion?

A. File size
B. Digital signature
C. Checksums
D. Anti-malware software
E. Sandboxing

Answer: B

NEW QUESTION 22
A company is acquiring incident response and forensic assistance from a managed security service provider in the event of a data breach. The company has selected a partner and must now provide required documents to be reviewed and evaluated. Which of the following documents would BEST protect the company and ensure timely assistance? (Choose two.)

A. RA
B. BIA
C. NDA
D. RFI
E. RFQ
F. MSA

Answer: CF

NEW QUESTION 24
A company is developing requirements for a customized OS build that will be used in an embedded environment. The company procured hardware that is capable of reducing the likelihood of successful buffer overruns while executables are processing. Which of the following capabilities must be included for the OS to take advantage of this critical hardware-based countermeasure?

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

Answer: B

NEW QUESTION 25
A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development. Which of the following SDLC best practices should the development team have followed?

A. Implementing regression testing
B. Completing user acceptance testing
C. Verifying system design documentation
D. Using a SRTM

Answer: D

NEW QUESTION 27
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

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

Answer: A

NEW QUESTION 29
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

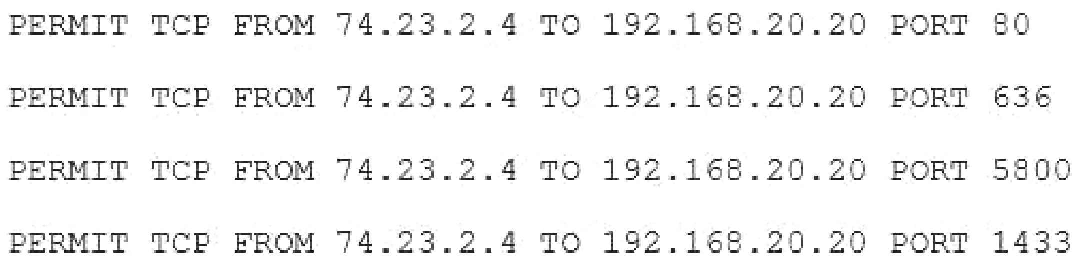
Answer: A

NEW QUESTION 31
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (?IO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

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

Answer: C

NEW QUESTION 33
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a third-party service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:



```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?

A. LDAP
B. WAYF
C. OpenID

D. RADIUS
E. SAML

Answer: D

NEW QUESTION 38
A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:
Store taxation-related documents for five years Store customer addresses in an encrypted format Destroy customer information after one year Keep data only in the customer's home country
Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

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

Answer: BCH

NEW QUESTION 42
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 45
A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.
Which of the following methods could be used in addition to an integrated development environment to reduce the severity of the issue?

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

Answer: D

NEW QUESTION 48
A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh.
Which of the following is the BEST way to address these issues and mitigate risks to the organization?

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

Answer: B

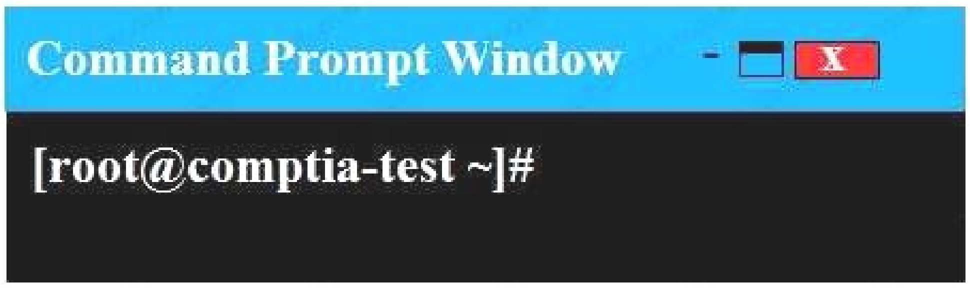
NEW QUESTION 52
A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.
Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

A. Access control list
B. Security requirements traceability matrix
C. Data owner matrix
D. Roles matrix
E. Data design document
F. Data access policies

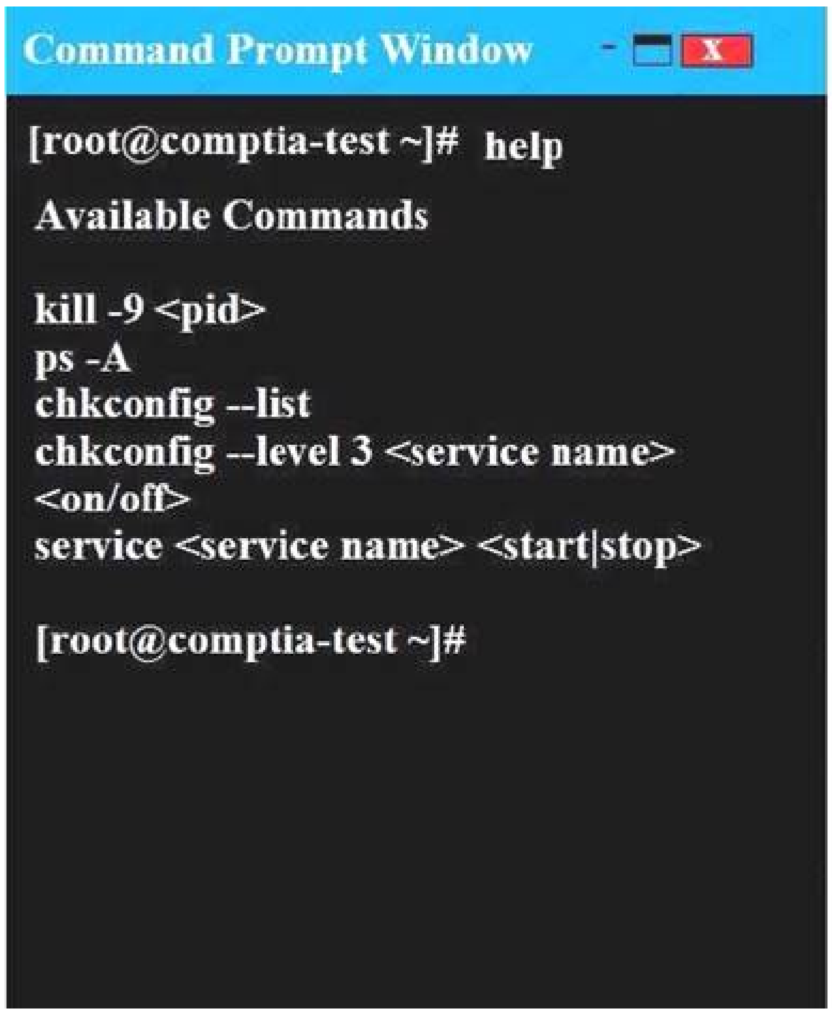
Answer: DF

NEW QUESTION 55
As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.
This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and

it does not need to print.
The command window will be provided along with root access. You are connected via a secure shell with root access.
You may query help for a list of commands. Instructions:
You need to disable and turn off unrelated services and processes.
It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
[root@comptia-test ~]#
```



```
[root@comptia-test ~]#  help
 Available Commands

 kill -9 <pid>
 ps -A
 chkconfig --list
 chkconfig --level 3 <service name>
 <on/off>
 service <service name> <start|stop>

 [root@comptia-test ~]#
```

A. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Serveriptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save Database Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>
B. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>

Answer: A

NEW QUESTION 56
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 60
A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

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

Answer: D

NEW QUESTION 61

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

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

Answer: B

NEW QUESTION 64
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

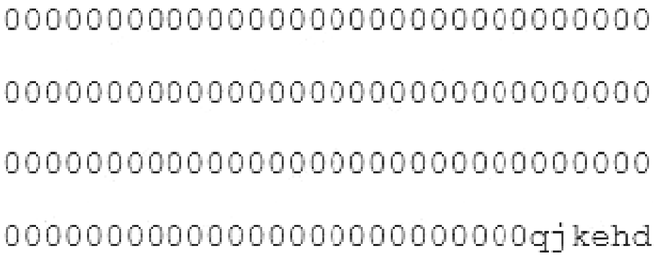
Answer: A

NEW QUESTION 68
A security researches is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.
Based on the information available to the researcher, which of the following is the MOST likely threat profile?

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

Answer: D

NEW QUESTION 70
A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.
To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:



```
00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000qj kehd
```

Which of the following should be included in the auditor’s report based in the above findings?

A. The hard disk contains bad sectors
B. The disk has been degaussed.
C. The data represents part of the disk BIOS.
D. Sensitive data might still be present on the hard drive

Answer: A

NEW QUESTION 73
An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:
URL: http://192.168.0.100/ERP/accountId=5&action=SELECT
Which of the following is the MOST likely vulnerability in this ERP platform?

A. Brute forcing of account credentials
B. Plan-text credentials transmitted over the Internet
C. Insecure direct object reference
D. SQL injection of ERP back end

Answer: C

NEW QUESTION 74
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:
1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced

3. Protection of sensitive files
4. Access to the corporate applications
Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

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

Answer: DEF

NEW QUESTION 79
A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.
Which of the following solutions BEST meets all of the architect's objectives?

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

Answer: A

NEW QUESTION 81
A user asks a security practitioner for recommendations on securing a home network. The user recently purchased a connected home assistant and multiple IoT devices in an effort to automate the home. Some of the IoT devices are wearables, and other are installed in the user's automobiles. The current home network is configured as a single flat network behind an ISP-supplied router. The router has a single IP address, and the router performs NAT on incoming traffic to route it to individual devices.
Which of the following security controls would address the user's privacy concerns and provide the BEST level of security for the home network?

A. Ensure all IoT devices are configured in a geofencing mode so the devices do not work when removed from the home networ
B. Disable the home assistant unless actively using it, and segment the network so each IoT device has its own segment.
C. Install a firewall capable of cryptographically separating network traffic require strong authentication to access all IoT devices, and restrict network access for the home assistant based on time-of-day restrictions.
D. Segment the home network to separate network traffic from users and the IoT devices, ensure security settings on the home assistant support no or limited recording capability, and install firewall rules on the router to restrict traffic to the home assistant as much as possible.
E. Change all default passwords on the IoT devices, disable Internet access for the IoT devices and the home assistant, obtain routable IP addresses for all devices, and implement IPv6 and IPSec protections on all network traffic.

Answer: B

NEW QUESTION 82
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 86
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancements to the company's cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

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

Answer: B

NEW QUESTION 89
A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition
B. Encryption of the SSD at the file level

C. FDE of each logical volume on the SSD
D. FDE of the entire SSD as a single disk

Answer: A

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

NEW QUESTION 93
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 96
A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.
Which of the following is the BEST course of action?

A. Investigate the network traffic and block UDP port 3544 at the firewall
B. Remove the system from the network and disable IPv6 at the router
C. Locate and remove the unauthorized 6to4 relay from the network
D. Disable the switch port and block the 2001::/32 traffic at the firewall

Answer: A

Explanation:
The 2001::/32 prefix is used for Teredo tunneling.
Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols, it can perform its function even from behind network address translation (NAT) devices such as home routers.
Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets. Teredo routes these datagrams on the IPv4 Internet and through NAT devices. Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.
Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32).
In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can then investigate the traffic within the network. Incorrect Answers:
B: Disabling IPv6 at the router will not help if the IPv6 traffic is encapsulated in IPv4 frames using Teredo. The question also states that there is no IPv6 routing into or out of the network.
C: 6to4 relays work in a similar way to Teredo. However, the addresses used by 6to4 relays start with 2002:: whereas Teredo addresses start with 2001. Therefore, a 6to4 relay is not being used in this question so this answer is incorrect.
D: This question is asking for the BEST solution. Disabling the switch port would take the system connected to it offline and blocking traffic destined for 2001::/32 at the firewall would prevent inbound Teredo communications (if you block the traffic on the inbound interface). However, blocking port UDP 3544 would suffice and investigating the traffic is always a better solution than just disconnecting a system from the network.
References: https://en.wikipedia.HYPERLINK
"https://en.wikipedia.org/wiki/Teredo_tunneling"org/wiki/Teredo_tunHYPERLINK "https://en.wikipedia.org/wiki/Teredo_tunneling"neling

NEW QUESTION 97
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 98
An application present on the majority of an organization’s 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

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

Answer: B

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

NEW QUESTION 102
select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson
Which of the following types of attacks is the user attempting?

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

Answer: D

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

NEW QUESTION 104
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 105
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 106
A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:

```
10.235.62.11 – - [02/Mar/2014:06:13:04] “GET
/site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1” 200 5724
```

Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.
B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.
D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Answer: C

Explanation:
The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.
In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must explogt a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
Incorrect Answers:
A: The code in this question does not contain non-printable characters.
B: The code in this question is not an example of cross site scripting (XSS).
D: The code in this question is an example of a SQL injection attack. It is not simply someone attempting to log on as administrator.
References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 107
The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

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

Answer: A

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

NEW QUESTION 110
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 113
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 114
A penetration tester is inspecting traffic on a new mobile banking application and sends the following web request:
POST http://www.example.com/resources/NewBankAccount HTTP/1.1 Content-type: application/json

```
{
“account”: [
{ “creditAccount”:”Credit Card Rewards account”}
{ “salesLeadRef”:”www.example.com/badcontent/explogtme.exe”}
],
“customer”: [
{ “name”:”Joe Citizen”}
{ “custRef”:”3153151”}
]
}
```

The banking website responds with: HTTP/1.1 200 OK

```
{
“newAccountDetails”:
[
{ “cardNumber”:”1234123412341234”}
{ “cardExpiry”:”2020-12-31”}
{ “cardCVV”:”909”}
],
“marketingCookieTracker”:“JSESSIONID=000000001” “returnCode”:“Account added successfully”
}
```

Which of the following are security weaknesses in this example? (Select TWO).

A. Missing input validation on some fields
B. Vulnerable to SQL injection
C. Sensitive details communicated in clear-text
D. Vulnerable to XSS
E. Vulnerable to malware file uploads
F. JSON/REST is not as secure as XML

Answer: AC

Explanation:
The SalesLeadRef field has no input validation. The penetration tester should not be able to enter “www.example.com/badcontent/explogtme.exe” in this field. The credit card numbers are communicated in clear text which makes it vulnerable to an attacker. This kind of information should be encrypted.
Incorrect Answers:
B: There is nothing to suggest the system is vulnerable to SQL injection.
D: There is nothing to suggest the system is vulnerable to XSS (cross site scripting).
E: Although the tester was able to post a URL to malicious software, it does not mean the system is vulnerable to malware file uploads.
F: JSON/REST is no less secure than XML.

NEW QUESTION 117
Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:
POST /login.aspx HTTP/1.1 Host: comptia.org

Content-type: text/html txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true
Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

A. Remove all of the post data and change the request to /login.aspx from POST to GET
B. Attempt to brute force all usernames and passwords using a password cracker
C. Remove the txtPassword post data and change alreadyLoggedIn from false to true
D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

Answer: C

Explanation:
The text “txtUsername=ann&txtPassword=ann” is an attempted login using a username of ‘ann’ and also a password of ‘ann’.
The text “alreadyLoggedIn=false” is saying that Ann is not already logged in.
To test whether we can bypass the authentication, we can attempt the login without the password
and we can see if we can bypass the ‘alreadyloggedin’ check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.
Incorrect Answers:
A: GET /login.aspx would just return the login form. This does not test whether the website is susceptible to a simple authentication bypass.
B: We do not want to guess the usernames and passwords. We want to see if we can get into the site without authentication.
D: We need to submit the data so we cannot toggle submit from true to false.

NEW QUESTION 118
ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

A. Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.
B. Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).
C. Organize VM hosts into containers based on security zone and restrict access using an ACL.
D. Require multi-factor authentication when accessing the console at the physical VM hos

Answer: C

Explanation:
Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the
containers to provide access to the hosts within the container. Incorrect Answers:
A: Hypervisor layer firewalling is used to restrict the network traffic that can access the host. It does not prevent a user from directly accessing the console of the host.
B: Maintaining a separate virtual switch for each security zone and ensuring VM hosts bind to only the correct virtual NIC(s) will restrict the network access of the VM hosts. It does not prevent a user from directly accessing the console of the host.
D: Multi-factor authentication is a secure way of authenticating a user. However, that’s all it does: authenticates someone. In other words, it only proves that the person is who they say they are. You would still need an ACL to determine whether that person is allowed or not allowed to access the console of the host.

NEW QUESTION 120
ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

A. Establish a list of users that must work with each regulation
B. Establish a list of devices that must meet each regulation
C. Centralize management of all devices on the network
D. Compartmentalize the network
E. Establish a company framework
F. Apply technical controls to meet compliance with the regulation

Answer: BDF

Explanation:
Payment card industry (PCI) compliance is adherence to a set of specific security standards that were
developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.
There are six main requirements for PCI compliance. The vendor must: Build and maintain a secure network
Protect cardholder data
Maintain a vulnerability management program Implement strong access control measures Regularly monitor and test networks Maintain an information security policy
To achieve PCI and SOX compliance you should:
Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.
Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.
Apply technical controls to meet compliance with the regulation. Secure the data as required. Incorrect Answers:
A: It is not necessary to establish a list of users that must work with each regulation. All users should be trained to manage sensitive dat
A. However, PCI and SOX compliance is more about the security of the data on the computers that contain the data.
C: Central management of all devices on the network makes device management easier for administrators. However, it is not a requirement for PCI and SOX compliance.
E: A company framework is typically related to the structure of employee roles and departments. It is not a requirement for PCI and SOX compliance.
References:
http://searchcompliance.techtarget.com/definition/PCI-compliaHYPERLINK "http://searchcompliance.techtarget.com/definition/PCI-compliance"nce

NEW QUESTION 123
A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

A. Online password testing

B. Rainbow tables attack
C. Dictionary attack
D. Brute force attack

Answer: B

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

NEW QUESTION 126
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 130
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 131
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.

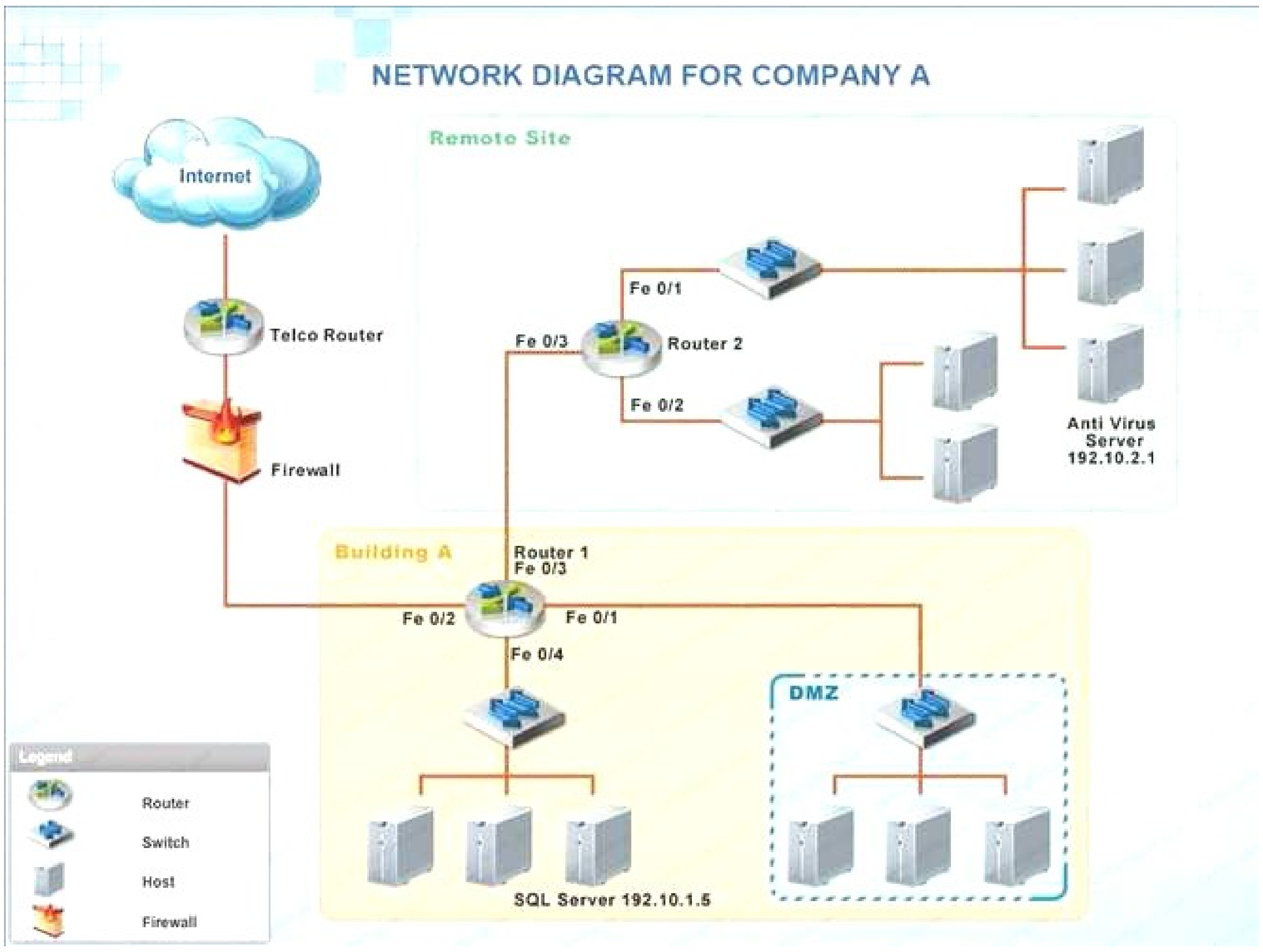
NEW QUESTION 134
A network engineer wants to deploy user-based authentication across the company’s wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user’s network access be controlled based on the user’s 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).

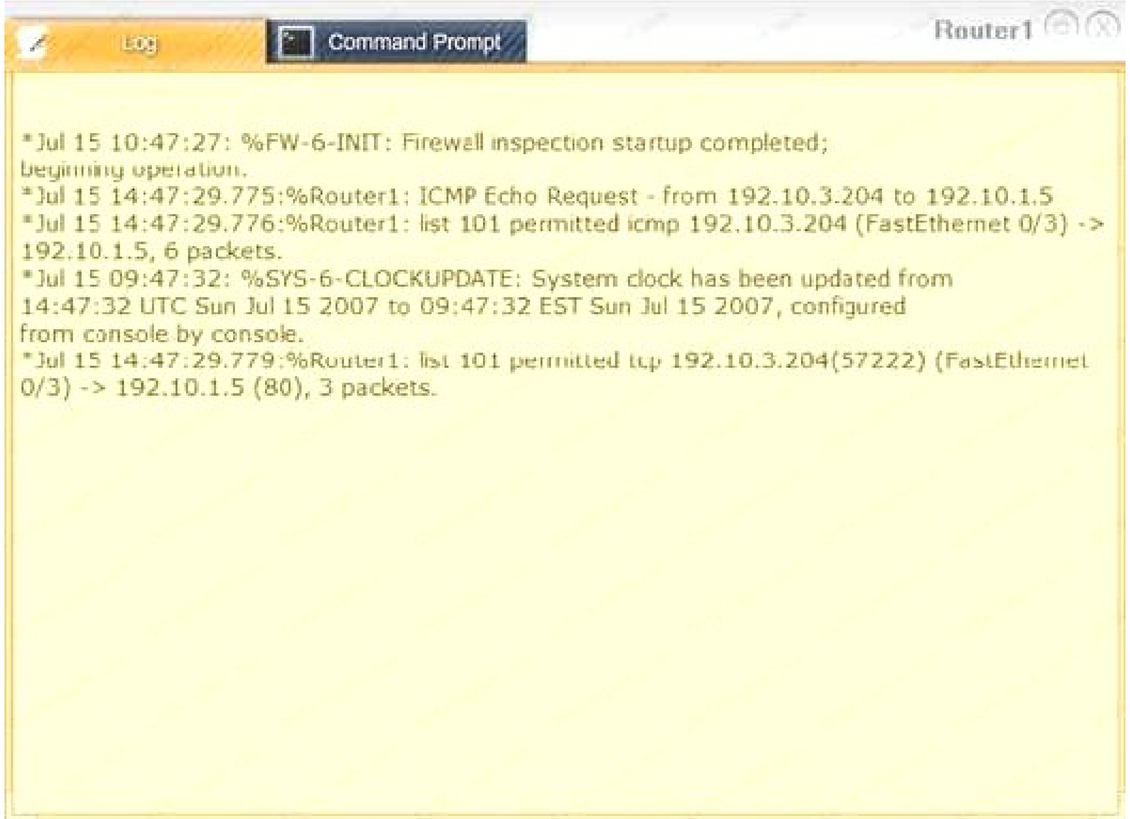
A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

Answer: CD

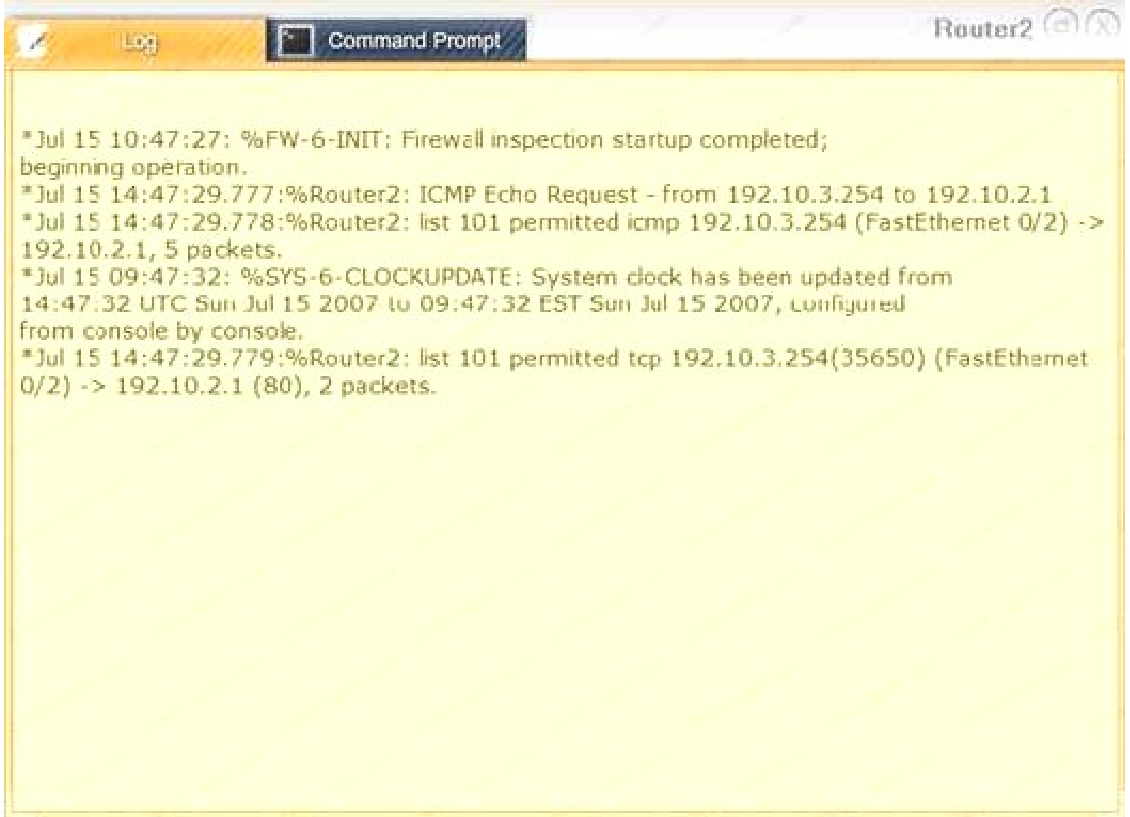
Explanation:
RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.
LDAP and RADIUS have something in common. They‘re both mainly protocols (more than a database) which uses attributes to carry information back and forth. 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 137
Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP
address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.
Instructions: Click on the simulation button to refer to the Network Diagram for Company A. Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.
Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.
Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.

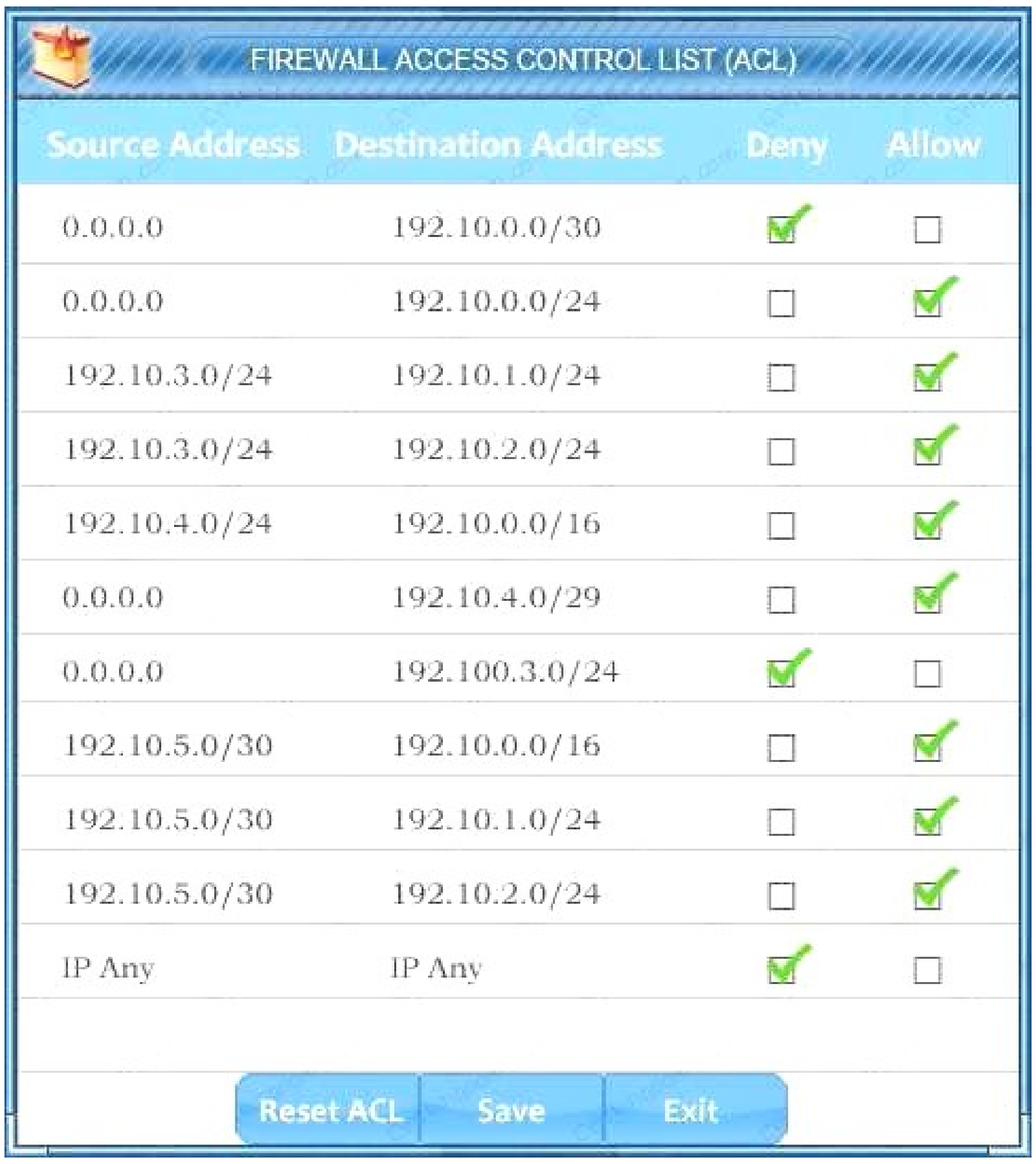




```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.775:%Router1: ICMP Echo Request - from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1: list 101 permitted icmp 192.10.3.204 (FastEthernet 0/3) ->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet
0/3) -> 192.10.1.5 (80), 3 packets.
```



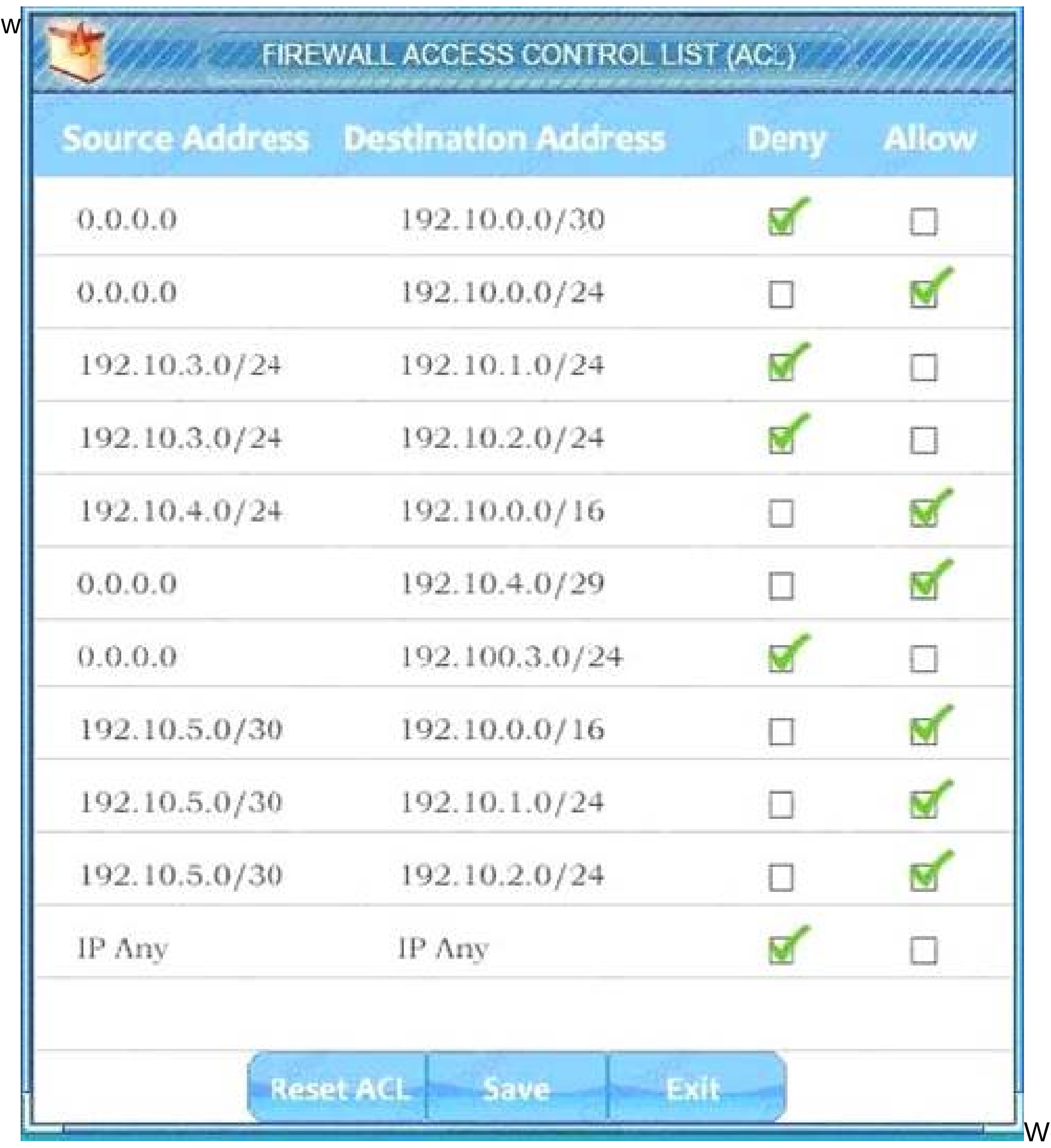
```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.777:%Router2: ICMP Echo Request - from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2: list 101 permitted icmp 192.10.3.254 (FastEthernet 0/2) ->
192.10.2.1, 5 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47.32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router2: list 101 permitted tcp 192.10.3.254(35650) (FastEthernet
0/2) -> 192.10.2.1 (80), 2 packets.
```



FIREWALL ACCESS CONTROL LIST (ACL)

Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	☑	□
0.0.0.0	192.10.0.0/24	□	☑
192.10.3.0/24	192.10.1.0/24	□	☑
192.10.3.0/24	192.10.2.0/24	□	☑
192.10.4.0/24	192.10.0.0/16	□	☑
0.0.0.0	192.10.4.0/29	□	☑
0.0.0.0	192.100.3.0/24	☑	□
192.10.5.0/30	192.10.0.0/16	□	☑
192.10.5.0/30	192.10.1.0/24	□	☑
192.10.5.0/30	192.10.2.0/24	□	☑
IP Any	IP Any	☑	□

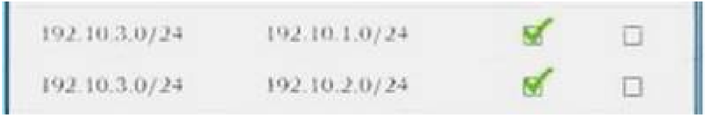
A. Check the answer below



FIREWALL ACCESS CONTROL LIST (ACL)

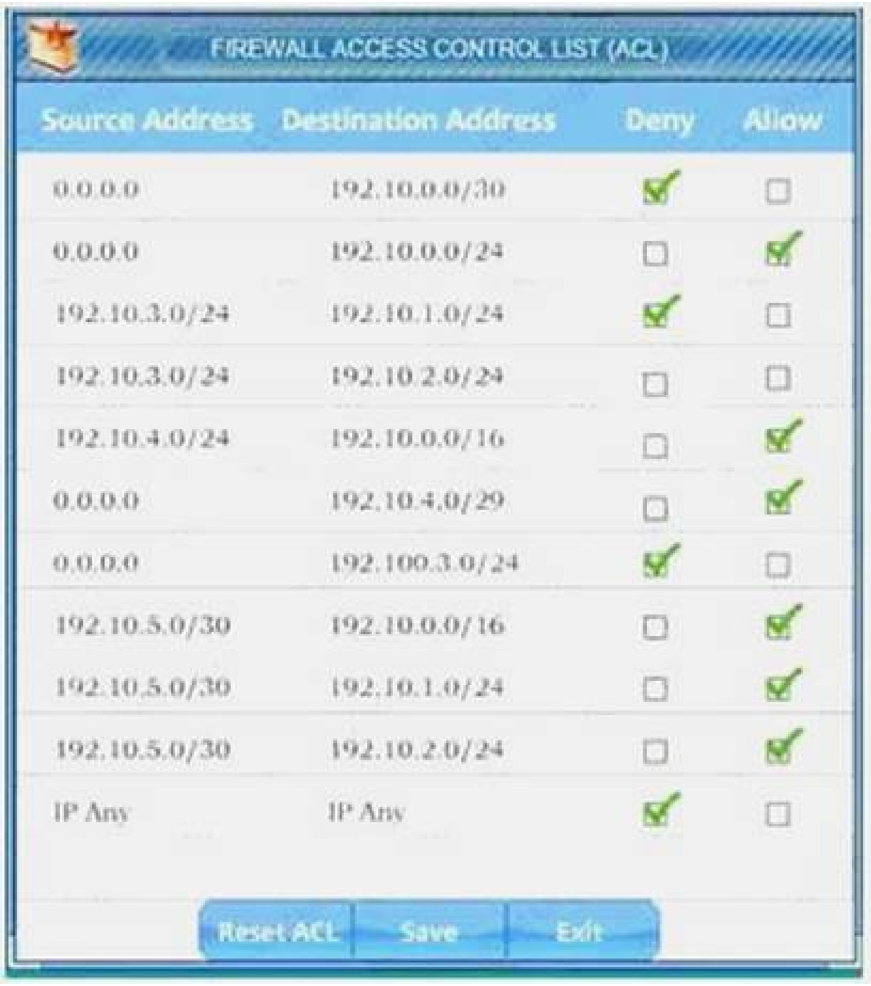
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	☑	□
0.0.0.0	192.10.0.0/24	□	☑
192.10.3.0/24	192.10.1.0/24	☑	□
192.10.3.0/24	192.10.2.0/24	☑	□
192.10.4.0/24	192.10.0.0/16	□	☑
0.0.0.0	192.10.4.0/29	□	☑
0.0.0.0	192.100.3.0/24	☑	□
192.10.5.0/30	192.10.0.0/16	□	☑
192.10.5.0/30	192.10.1.0/24	□	☑
192.10.5.0/30	192.10.2.0/24	□	☑
IP Any	IP Any	☑	□

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:



192.10.3.0/24	192.10.1.0/24	☑	□
192.10.3.0/24	192.10.2.0/24	☑	□

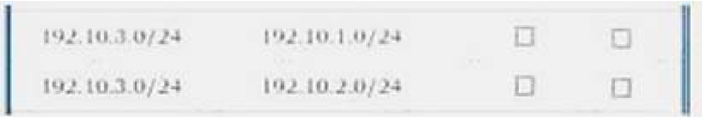
B. Check the answer below



FIREWALL ACCESS CONTROL LIST (ACL)

Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	☑	□
0.0.0.0	192.10.0.0/24	□	☑
192.10.3.0/24	192.10.1.0/24	☑	□
192.10.3.0/24	192.10.2.0/24	□	□
192.10.4.0/24	192.10.0.0/16	□	☑
0.0.0.0	192.10.4.0/29	□	☑
0.0.0.0	192.100.3.0/24	☑	□
192.10.5.0/30	192.10.0.0/16	□	☑
192.10.5.0/30	192.10.1.0/24	□	☑
192.10.5.0/30	192.10.2.0/24	□	☑
IP Any	IP Any	☑	□

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:



192.10.3.0/24	192.10.1.0/24	□	□
192.10.3.0/24	192.10.2.0/24	□	□

Answer: A

NEW QUESTION 141
The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer dat

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

Answer: D

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

NEW QUESTION 142
A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

A. Physical penetration test of the datacenter to ensure there are appropriate controls.
B. Penetration testing of the solution to ensure that the customer data is well protected.
C. Security clauses are implemented into the contract such as the right to audit.
D. Review of the organizations security policies, procedures and relevant hosting certifications.
E. Code review of the solution to ensure that there are no back doors located in the softwar

Answer: CD

Explanation:
Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following:
Company profile, strategy, mission, and reputation

Financial status, including reviews of audited financial statements
Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks
Process expertise, methodology, and effectiveness Quality initiatives and certifications
Technology, infrastructure stability, and applications Security and audit controls
Legal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors
Insurance
Disaster recovery and business continuity policies C and D form part of Security and audit controls. Incorrect Answers:
A: A Physical Penetration Test recognizes the security weaknesses and strengths of the physical security. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.
B: A penetration test is a software attack on a computer system that looks for security weaknesses. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.
E: A security code review is an examination of an application that is designed to identify and assess threats to an organization. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.
References: https://en.wikipedia.org/wiki/Due_diligence httHYPERLINK
"http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5"p://www.ftpress.com/articles/
article.aspx?p=465313HYPERLINK "http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5"&HYPERLINK
"http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5"seqNum=5 http://seclists.org/pen-test/2004/Dec/11
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 169

NEW QUESTION 143
An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

A. Ensure the SaaS provider supports dual factor authentication.
B. Ensure the SaaS provider supports encrypted password transmission and storage.
C. Ensure the SaaS provider supports secure hash file exchange.
D. Ensure the SaaS provider supports role-based access control.
E. Ensure the SaaS provider supports directory services federatio

Answer: E

Explanation:
A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network. Single sign-on will mitigate the risk of managing separate user credentials. Incorrect Answers:
A: Dual factor authentication will provide identification of users via a combination of two different components. It will not, however, mitigate the risk of managing separate user credentials.
B: The transmission and storage of encrypted passwords will not mitigate the risk of managing separate user credentials.
C: A hash file is a file that has been converted into a numerical string by a mathematical algorithm, and has to be unencrypted with a hash key to be understood. It will not, however, mitigate the risk of managing separate user credentials.
D: Role-based access control (RBAC) refers to the restriction of system access to authorized users. It will not, however, mitigate the risk of managing separate user credentials.
References:
https://msdn.microsoft.com/en-us/library/aa905332.aspx https://en.wikipedia.org/wiki/Two-factor_authentication https://en.wikipedia.org/wiki/Encryption
http://www.wisegeek.com/what-are-hash-files.htm https://en.wikipedia.org/wiki/Role-based_access_control

NEW QUESTION 144
A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO's requirement?

A. GRC
B. IPS
C. CMDB
D. Syslog-ng
E. IDS

Answer: A

Explanation:
GRC is a discipline that aims to coordinate information and activity across governance, risk management and compliance with the purpose of operating more efficiently, enabling effective information sharing, more effectively reporting activities and avoiding wasteful overlaps. An integrated GRC (iGRC) takes data feeds from one or more sources that detect or sense abnormalities, faults or other patterns from security or business applications.
Incorrect Answers:
B: IPS is a typical sensor type that is included in an iGRC.
C: A configuration management database (CMDB) is defined as a repository that acts as a data warehouse for IT organizations.
D: syslog-ng sends incoming log messages from specified sources to the correct destinations. E: IDS is a typical sensor type that is included in an iGRC.
References: https://en.wikipedia.org/wHYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover
nance.2C_risk_and_compliancy"iki/Governance,_risk_managemeHYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover nance.2C_risk_and_compliancy"nt,_and_HYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover
nance.2C_risk_and_compliancy"compliance#Integrated_governance.2C_risk_and_compliancy https://wiki.archlinux.org/index.php/Syslog-ng

NEW QUESTION 148
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation
B. Security test and evaluation

C. Risk assessment
D. Ongoing authorization

Answer: D

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

NEW QUESTION 151
A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks
B. Job rotation
C. Least privilege
D. Employee termination procedures

Answer: B

Explanation:
Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.
Incorrect Answers:
A: To verify that a potential employee has a clean background and that any negative history is exposed prior to employment, a background check is used.
C: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.
D: The employee termination procedures will not identify the employees involved in these activities and reduce the risk of this activity occurring in the future.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 243, 245, 246

NEW QUESTION 156
During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

A. Notify senior management, secure the scene, capture volatile storage, capture non-volatile storage, implement chain of custody, and analyze original media.
B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.
C. Implement chain of custody, take inventory, secure the scene, capture volatile and non-volatile storage, and document the findings.
D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

Answer: D

Explanation:
The scene has to be secured first to prevent contamination. Once a forensic copy has been created,
an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.
Incorrect Answers:
A: To prevent contamination, the scene should be secured first. B: The scene should be secured before taking inventory.
C: Implementing a chain of custody can only occur once evidence has been accessed. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254

NEW QUESTION 157
A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

A. Subjective and based on an individual's experience.
B. Requires a high degree of upfront work to gather environment details.
C. Difficult to differentiate between high, medium, and low risks.
D. Allows for cost and benefit analysis.
E. Calculations can be extremely complex to manag

Answer: A

Explanation:

Using likelihood and consequence to determine risk is known as qualitative risk analysis.
With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system. After qualitative analysis has been performed, you can then perform quantitative risk analysis. A
Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk.
Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.
Incorrect Answers:
B: Qualitative risk analysis does not require a high degree of upfront work to gather environment details. This answer applies more to quantitative risk analysis.
C: Although qualitative risk analysis does not use numeric values to quantify likelihood or consequence compared to quantitative analysis, we can all differentiate between the terms high, medium, and low when talking about risk.
D: Qualitative risk analysis does not allow for cost and benefit analysis, quantitative risk analysis does.
E: Calculations for qualitative risk analysis are not extremely complex to manage; they can be quantitative risk analysis.
References: https://www.passionatepm.com/blog/quHYPERLINK "https://www.passionatepm.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmpconcept- 1"alitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1

NEW QUESTION 162
A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems
B. Implement an application layer firewall to protect the payroll system interface
C. Monitor the system's security log for unauthorized access to the payroll application
D. Perform reconciliation of all payroll transactions on a daily basis

Answer: A

Explanation:
The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.
We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.
Incorrect Answers:
B: An application layer firewall may provide some protection to the application. However, the operating system is vulnerable due to being unpatched. It is unlikely that an application layer firewall will protect against the operating system vulnerabilities.
C: Monitoring the system's security log for unauthorized access to the payroll application will not actually provide any protection against unauthorized access. It would just enable you to see that unauthorized access has occurred.
D: Reconciling the payroll transactions on a daily basis would keep the accounts up to date but it would provide no protection for the system and so does not mitigate the vulnerability of missing OS patches as required in this question.

NEW QUESTION 165
The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:

```
11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400
```

Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.
B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.
C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGPsinkhole should be configured to drop traffic at the source networks.
D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

Answer: A

Explanation:
The exhibit displays logs that are indicative of an active fraggle attack. A Fraggle attack is similar to a smurf attack in that it is a denial of service attack, but the difference is that a fraggle attack makes
use of ICMP and UDP ports 7 and 19. Thus when the senior engineer uses a network analyzer to identify the attack he should contact the company's ISP to block those malicious packets. Incorrect Answers:
B: The logs are indicative of an ongoing fraggle attack. Even though a fraggle attack id also a DOS attack the best form of action to take would be to ask the ISP to block the malicious packets.
C: Configuring a sinkhole to block a denial of service attack will not address the problem since the type of attack as per the logs indicates a fraggle attack.
D: A smurf attack spoofs the source address with the address of the victim, and then sends it out as a broadcast ping. Each system in the network will then respond, and flood the victim with echo replies. The logs do not indicate a smurf attack.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 165, 168
https://en.wikipedia.org/wiki/Fraggle_attacHYPERLINK "https://en.wikipedia.org/wiki/Fraggle_attack"k

NEW QUESTION 167
An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following

methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

A. Use the pass the hash technique
B. Use rainbow tables to crack the passwords
C. Use the existing access to change the password
D. Use social engineering to obtain the actual password

Answer: A

Explanation:
With passing the hash you can grab NTLM credentials and you can manipulate the Windows logon sessions maintained by the LSA component. This will allow you to operate as an administrative user and not impact the integrity of any of the systems when running your tests.
Incorrect Answers:
B: Making use of rainbow tables and cracking passwords will have a definite impact on the integrity of the other systems that are to be penetration tested.
C: Changing passwords will impact the integrity of the other systems and is not a preferable method to conduct penetration testing.
D: Social engineering is not the preferred way to accomplish the goal of penetration testing and
gaining administrative credentials on the client's network. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17, 351

NEW QUESTION 171
A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

A. Increase the frequency of antivirus downloads and install updates to all workstations.
B. Deploy a cloud-based content filter and enable the appropriate category to prevent further infections.
C. Deploy a WAF to inspect and block all web traffic which may contain malware and explogts.
D. Deploy a web based gateway antivirus server to intercept viruses before they enter the networ

Answer: B

Explanation:
The undetected malware gets delivered to the company via drive-by and malware hosing websites. Display filters and Capture filters when deployed on the cloud-based content should provide the protection required.
Incorrect Answers:
A: The company already has an antivirus application that is not detecting the malware, increasing the frequency of antivirus downloads and installing the updates will thus not address the issue of the drive-by downloads and malware hosting websites.
C: A WAF is designed to sit between a web client and a web server to analyze OSI Layer 7 traffic; this will not provide the required protection in this case. WAFs are not 100% effective.
D: A web-based gateway antivirus is not going to negate the problem of drive-by downloads and malware hosting websites.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 116, 405-406

NEW QUESTION 175
A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent
B. 5.5 percent
C. 45 percent
D. 82 percent

Answer: D

Explanation:
Return on investment = Net profit / Investment where: Net profit = gross profit – expenses
investment = stock + market outstanding[when defined as?] + claims or
Return on investment = (gain from investment – cost of investment) / cost of investment Thus (100 000 – 55 000)/50 000 = 0,82 = 82 %
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 337
http://www.financeformulas.net/Return_on_Investment.html

NEW QUESTION 178
Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).

A. Check log files for logins from unauthorized IPs.
B. Check /proc/kmem for fragmented memory segments.
C. Check for unencrypted passwords in /etc/shadow.
D. Check timestamps for files modified around time of compromise.
E. Use lsof to determine files with future timestamps.
F. Use gpg to encrypt compromised data files.
G. Verify the MD5 checksum of system binaries.
H. Use vmstat to look for excessive disk I/

Answer: ADG

Explanation:

The MD5 checksum of the system binaries will allow you to carry out a forensic analysis of the compromised Linux system. Together with the log files of logins into the compromised system from unauthorized IPs and the timestamps for those files that were modified around the time that the compromise occurred will serve as useful forensic tools.
Incorrect Answers:
B: Checking for fragmented memory segments' is not a forensic analysis tool to be used in this case. C: The ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account. This is a useful tool for Linux passwords and shadow file formats and is in essence used to keep user account information.
E: Isof is used on Linux as a future timestamp tool and not a forensic analysis tool. F: Gpg is an encryption tool that works on Mac OS X.
H: vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length delay. The process and memory reports are instantaneous in either case. This is more of an administrator tool.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 387
httpsHYPERLINK "https://en.wikipedia.org/wiki/List_of_digital_forensics_tools"://en.wikipedia.org/wiki/List_of_digit al_forensics_tools

NEW QUESTION 180
A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.
Proposal:
External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.
The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?

A. -$30,000
B. $120,000
C. $150,000
D. $180,000

Answer: A

Explanation:
Return on investment = Net profit / Investment where: Net profit = gross profit - expenses.
or
Return on investment = (gain from investment – cost of investment) / cost of investment Subscriptions = 5,000 x 12 = 60,000 per annum
10 incidents @ 10,000 = 100.000 per annum reduce by 50% = 50,000 per annum
Thus the rate of Return is -10,000 per annum and that makes for -$30,000 after three years. References:
http://www.finHYPERLINK "http://www.financeformulas.net/Return_on_Investment.html"anceformulas.net/Return_on_Invest ment.html

NEW QUESTION 184
A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

A. Agile
B. SDL
C. Waterfall
D. Joint application development

Answer: A

Explanation:
In agile software development, teams of programmers and business experts work closely together, using an iterative approach.
Incorrect Answers:
B: The Microsoft developed security development life cycle (SDL) is designed to minimize the security-related design and coding bugs in software. An organization that implements SDL has a central security team that performs security functions.
C: The waterfall model is a sequential software development processes, in which progress is seen as flowing steadily downwards through the phases of conception, initiation, analysis, design, construction, testing, production/implementation and maintenance.
D: The vendor is still responsible for developing the solution, Therefore this is not an example of joint application development.
References:
BOOK pp. 371, 374
https://en.wikipedia.org/wiki/Waterfall_model

NEW QUESTION 189
An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

A. Guest users could present a risk to the integrity of the company's information.
B. Authenticated users could sponsor guest access that was previously approved by management.
C. Unauthenticated users could present a risk to the confidentiality of the company's information.
D. Meeting owners could sponsor guest access if they have passed a background chec

Answer: C

Explanation:
The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with unauthorized users.
Incorrect Answers:

A: Integrity of information is centered on the modification or alternation of information. Information remains unchanged and is in its true original form during transmission and storage. The issue of guests at a Web conference is related to confidentiality of information.
B: The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with guests.
D: The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with guests, whether they have passed background checks or not.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 3

NEW QUESTION 192
An intruder was recently discovered inside the data center, a highly sensitive are

A. To gain access, the intruder circumvented numerous layers of physical and electronic security measure
B. Company leadership has asked for a thorough review of physical security controls to prevent this from happening agai
C. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE).
D. Facilities management
E. Human resources
F. Research and development
G. Programming
H. Data center operations
I. Marketing
J. Information technology

Answer: AEG

Explanation:
A: Facilities management is responsible for the physical security measures in a facility or building. E: The breach occurred in the data center, therefore the Data center operations would be greatly concerned.
G: Data centers are important aspects of information technology (IT) in large corporations. Therefore the IT department would be greatly concerned.
Incorrect Answers:
B: Human Resources security is concerned with employees joining an organization, moving between different positions in the organization, and leaving the organization.
C: Research and Development is concerned with security at the design and development stage of a system.
D: Programming security is concerned with application code and application vulnerabilities. F: Marketing is not concerned with security.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 281, 326-328

NEW QUESTION 193
A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, “BYOD clients must meet the company’s infrastructure requirements to permit a connection.” The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management
B. IT governance
C. Change management
D. Transference of risk

Answer: B

Explanation:
It governance is aimed at managing information security risks. It entails educating users about risk and implementing policies and procedures to reduce risk.
Incorrect Answers:
A: Asset management is the process of organizing, t racking, and supporting the assets of a company. However, bring your own device (BYOD) entail the use of personal devices, which are not company assets.
C: Change management is the process of managing changes to the system and programs to ensure that changes occur in an ordered process. It should minimize the risk of unauthorized changes and help reverse any unauthorized change.
D: Transference of risk is the process of having a third party carry the risk for a company, through insurance, for example.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 80-81, 133-134, 209-210, 218, 231-233

NEW QUESTION 194
An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).

A. Implement hashing of data in transit
B. Session recording and capture
C. Disable cross session cut and paste
D. Monitor approved credit accounts
E. User access audit reviews
F. Source IP whitelisting

Answer: CEF

Explanation:
Data sovereignty is a legal concern where the data is governed by the laws of the country in which the data resides. In this scenario the company does not want the data to fall under the law of the country of the organization to whom back office process has be outsourced to. Therefore we must ensure that data can only be accessed on local servers and no copies are held on computers of the outsource partner. It is important therefore to prevent cut and paste operations.
Privacy concerns can be addressed by ensuring the unauthorized users do not have access to the dat
A. This can be accomplished though user access auditing, which needs to be reviewed on an ongoing basis; and source IP whitelisting, which is a list of IP addresses that are explicitly allowed access to the system.
Incorrect Answers:
A: Hashing is used to ensure data integrity. In other words, it ensures that the data has not been altered and is in its true, original state. This does not address data sovereignty and privacy concerns. B: Session recording and capture would represent an additional potential threat for privacy concerns should an unauthorized user access the recorded session data.
D: The monitoring of approved credit accounts is a processing issue. It is not related to data sovereignty or privacy concerns.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17-19, 204, 247

NEW QUESTION 198
The helpdesk department desires to roll out a remote support application for internal use on all company computers. This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access. The risk management team has been asked to review vendor responses to the RFQ. Which of the following questions is the MOST important?

A. What are the protections against MITM?
B. What accountability is built into the remote support application?
C. What encryption standards are used in tracking database?
D. What snapshot or “undo” features are present in the application?
E. What encryption standards are used in remote desktop and file transfer functionality?

Answer: B

Explanation:
Incorrect Answers:
A: Man-in-the-Middle (MiTM) attacks are carried out when an attacker places himself between the sender and the receiver in the communication path, where they can intercept and modify the communication. However, the risk of a MITM is slim whereas the support staff WILL be accessing personal information.
C: Database encryption to prevent unauthorized access could be important (depending on other security controls in place). However, the risk of an unauthorized database access is slim whereas the support staff WILL be accessing personal information.
D: What snapshot or “undo” features are present in the application is a relatively unimportant question. The application may have no snapshot or “undo” features. Accounting for data access is more important than the risk of support user wanting to undo a mistake.
E: Encryption to prevent against MITM or packet sniffing attacks is important. However, the risk of such attacks is slim whereas the support staff WILL be accessing personal information. This makes the accountability question more important.
References: https://www.priv.gHYPERLINK
"https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp"c.ca/information/guide/2012/gl_acc_201204_e.asp2/gl_acc_201204_e.asp

NEW QUESTION 200
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-003 Practice Exam Features:

* CAS-003 Questions and Answers Updated Frequently

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

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

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

100% Actual & Verified — Instant Download, Please Click
Order The CAS-003 Practice Test Here