

CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)



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

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 3

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

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

Answer: A

NEW QUESTION 4

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

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

DCIM Images folder

Audio books folder Torrentz

My TAX.xls

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

Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

- A. MicroSD 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 encrypted

Answer: A

NEW QUESTION 5

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

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

Answer: F

NEW QUESTION 6

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 7

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 8

An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.

Which of the following procedures should the security responder apply to the situation? (Choose two.)

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

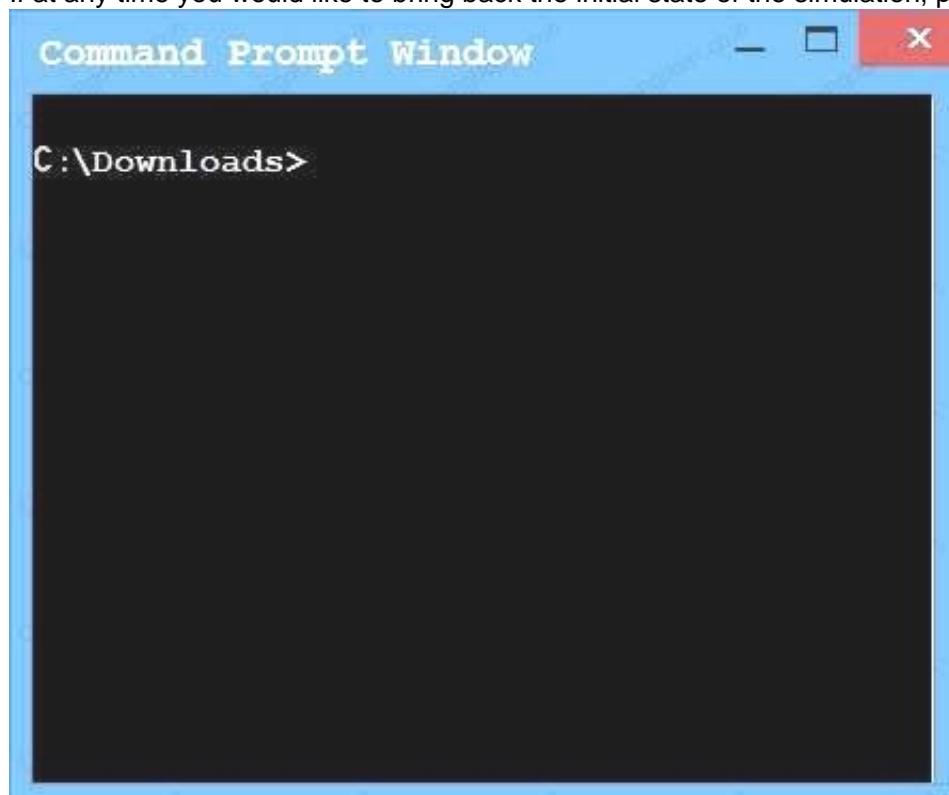
Answer: BF

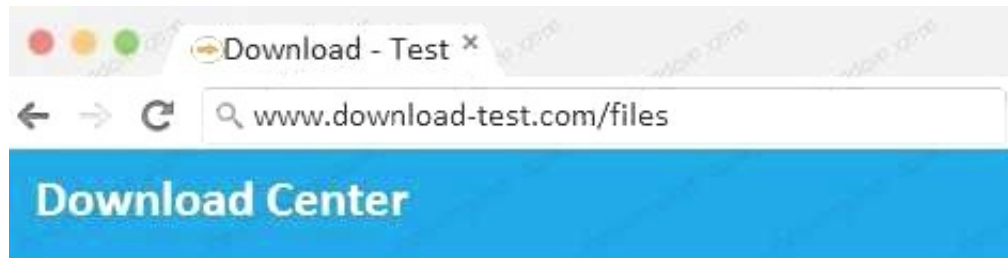
NEW QUESTION 9

An administrator wants to install a patch to an application. INSTRUCTIONS

Given the scenario, download, verify, and install the patch in the most secure manner. The last install that is completed will be the final submission.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



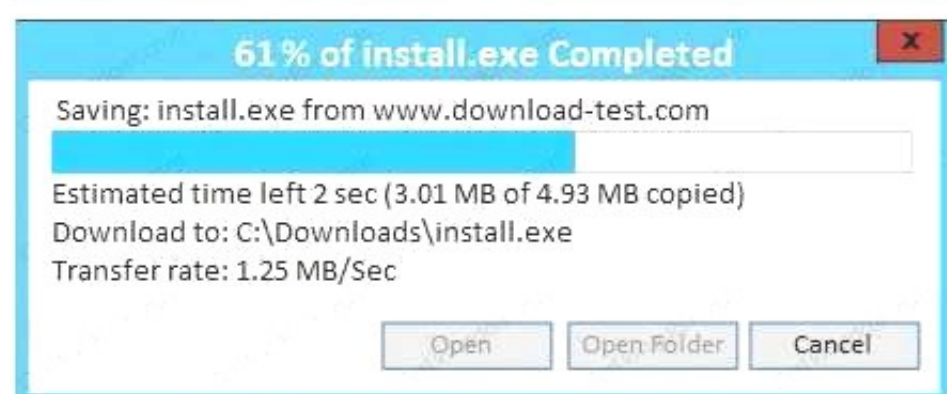
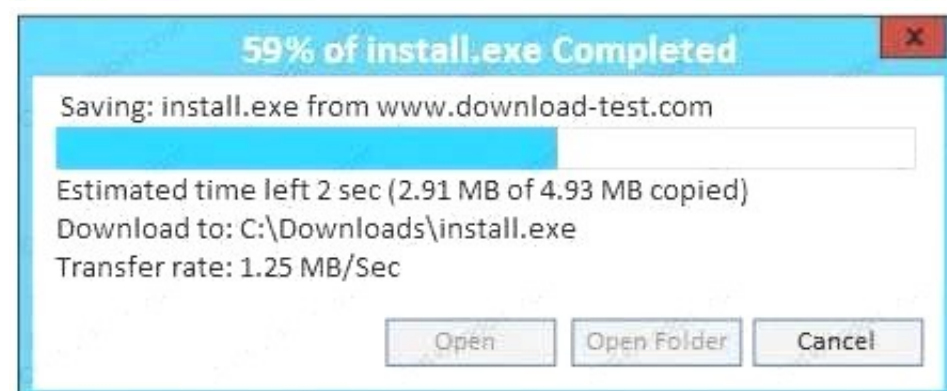
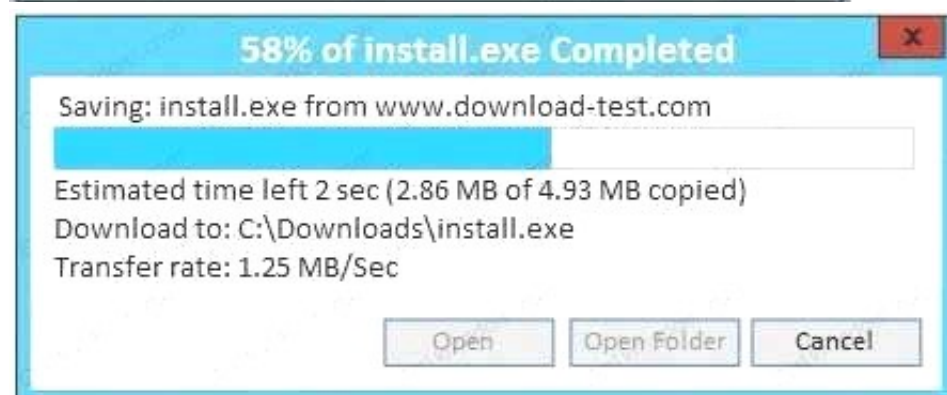


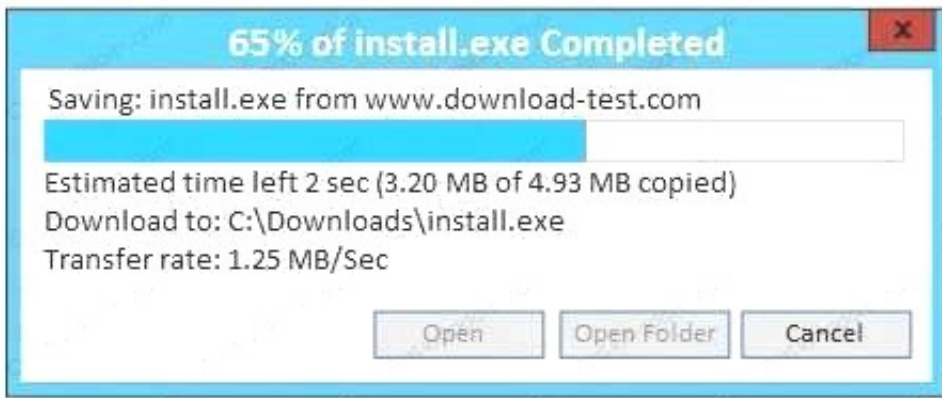
Home > Download Center > Application Patch

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

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

HASH: 1759adb5g34700aae19bc4578fc19cc2

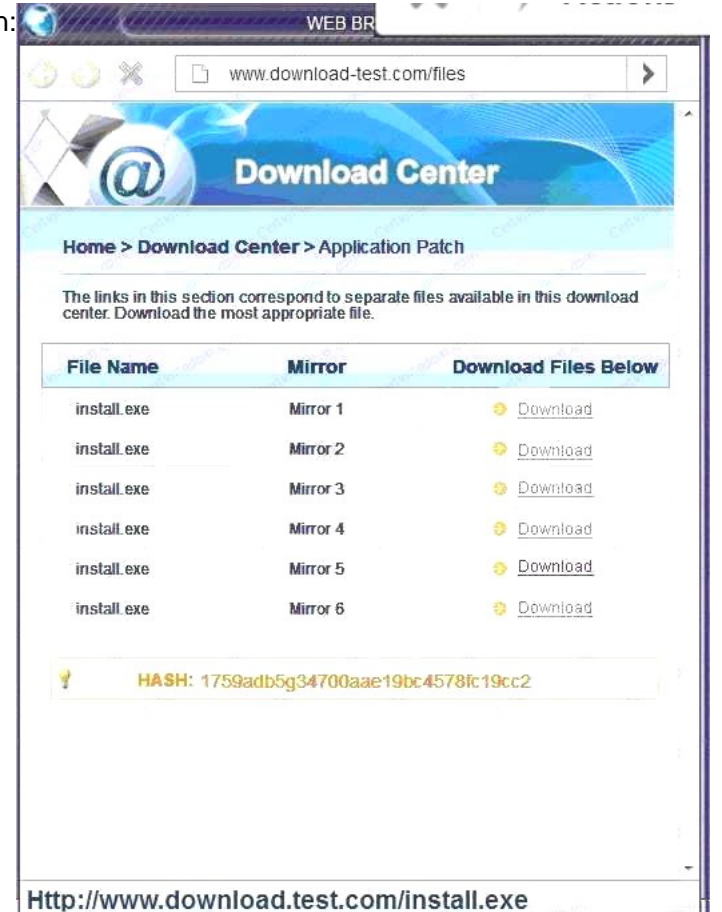




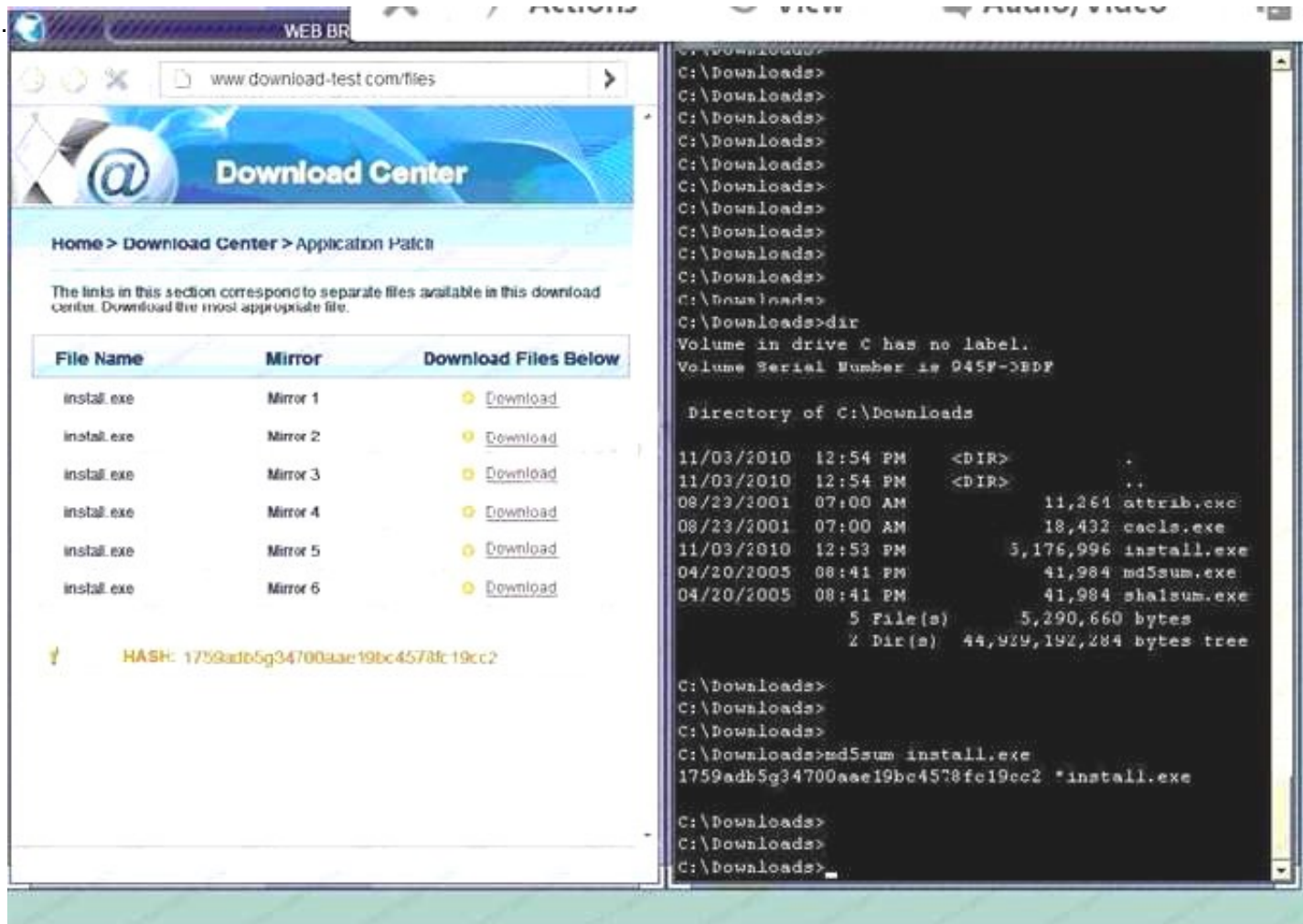
A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



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



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



Finally,

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

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



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

Answer: A

NEW QUESTION 10

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:
The data is for internal consumption only and shall not be distributed to outside individuals
The systems administrator should not have access to the data processed by the server
The integrity of the kernel image is maintained
Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

- A. SELinux
- B. DLP
- C. HIDS
- D. Host-based firewall
- E. Measured boot
- F. Data encryption
- G. Watermarking

Answer: CEF

NEW QUESTION 10

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 12

Given the following output from a local PC:

```
C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
Link-local IPv6 Address . . . . . : fe80::4551:67ba:77a6:62e1%11
IPv4 Address. . . . . : 172.30.0.28
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

- A. Allow 172.30.0.28:80 -> ANY
- B. Allow 172.30.0.28:80 -> 172.30.0.0/16
- C. Allow 172.30.0.28:80 -> 172.30.0.28:443
- D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Answer: B

NEW QUESTION 17

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 18

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 21

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 22

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 23

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

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

Answer: CD

NEW QUESTION 27

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 28

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 31

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

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

Answer: AC

NEW QUESTION 32

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 35

A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

- A. Call the CIO and ask for an interview, posing as a job seeker interested in an open position
- B. Compromise the email server to obtain a list of attendees who responded to the invitation who is on the IT staff
- C. Notify the CIO that, through observation at events, malicious actors can identify individuals to befriend
- D. Understand the CIO is a social drinker, and find the means to befriend the CIO at establishments the CIO frequents

Answer: D

NEW QUESTION 36

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

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

Answer: C

NEW QUESTION 38

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

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

Answer: D

NEW QUESTION 40

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

- A. Blue teaming
- B. Phishing simulations

- C. Lunch-and-learn
- D. Random audits
- E. Continuous monitoring
- F. Separation of duties

Answer: BE

NEW QUESTION 41

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

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

Answer: A

NEW QUESTION 46

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 49

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 52

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 53

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

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

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

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

Answer: D

NEW QUESTION 54

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

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

Answer: D

NEW QUESTION 56

An organization is preparing to develop a business continuity plan. The organization is required to meet regulatory requirements relating to confidentiality and availability, which are well-defined. Management has expressed concern following initial meetings that the organization is not fully aware of the requirements associated with the regulations. Which of the following would be MOST appropriate for the project manager to solicit additional resources for during this phase of the project?

- A. After-action reports
- B. Gap assessment
- C. Security requirements traceability matrix
- D. Business impact assessment
- E. Risk analysis

Answer: B

NEW QUESTION 60

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 61

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 63

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

- A. Exempt mobile devices from the requirement, as this will lead to privacy violations

- B. Configure the devices to use an always-on IPSec VPN
- C. Configure all management traffic to be tunneled into the enterprise via TLS
- D. Implement a VDI solution and deploy supporting client apps to devices
- E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Answer: BE

NEW QUESTION 65

A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: “<object object_ref=... />” and “<state state_ref=... />”. Which of the following tools BEST supports the use of these definitions?

- A. HTTP interceptor
- B. Static code analyzer
- C. SCAP scanner
- D. XML fuzzer

Answer: D

NEW QUESTION 66

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 71

A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization: `localStorage.setItem(“session-cookie”, document.cookie);` Which of the following should the security engineer recommend?

- A. SessionStorage should be used so authorized cookies expire after the session ends
- B. Cookies should be marked as “secure” and “HttpOnly”
- C. Cookies should be scoped to a relevant domain/path
- D. Client-side cookies should be replaced by server-side mechanisms

Answer: C

NEW QUESTION 74

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 78

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 81

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

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

D. Community IaaS

Answer: C

NEW QUESTION 84

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 Zone SRC 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST ANY ANY 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action ANY ANY 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action USER 10.1.1.0/24 10.1.2.0/24 ANY UNTRUST ANY 443 TCP 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 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
- P. 6 from top, edit the Action to be Permi
- Q. SRC Zone SRC 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 Zone ANY 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action USER 10.1.1.0/24 10.1.2.0/24 ANY UNTRUST ANY 443 TCP PERMIT

Answer: A

NEW QUESTION 85

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 89

Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

    char username[8];

    printf("Enter your username: ");

    gets(username)

    printf("\n");

    if (username == NULL) {

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

    }

    if strcmp(username, "admin") {

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

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

    } else {

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

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

    }

}
```

Which of the following vulnerability types is the MOST concerning?

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

Answer: B

NEW QUESTION 91

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

Timestamp	SourceIP	CustName	PreferredContact	ProdName	Comments
Monday 10:00:04	10.14.34.55	aaaaa	Phone	Widget1	None left
Monday 10:00:04	10.14.34.55	bbbbbb	Phone	Widget1	None left
Monday 10:00:05	10.14.34.55	cccc	Phone	Widget1	../../../../etc/passwd
Monday 10:01:03	10.14.34.55	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 95

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 97

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 102

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 105

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 108

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 111

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

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

Answer: B

NEW QUESTION 116

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 118

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

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

Answer: C

NEW QUESTION 123

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

- A. The filtering of sensitive data out of data flows at geographic boundaries.

- B. Removing potential bottlenecks in data transmission paths.
- C. The transfer of corporate data onto mobile corporate devices.
- D. The migration of data into and out of the network in an uncontrolled manne

Answer: D

NEW QUESTION 126

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 128

A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients' health information, management has identified the following requirements:

Data must be encrypted at rest.

The device must be disabled if it leaves the facility. The device must be disabled when tampered with

Which of the following technologies would BEST support these requirements? (Select two.)

- A. eFuse
- B. NFC
- C. GPS
- D. Biometric
- E. USB 4.1
- F. MicroSD

Answer: CD

NEW QUESTION 129

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 131

A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?

- A. Check for any relevant or required overlays.
- B. Review enhancements within the current control set.
- C. Modify to a high-baseline set of controls.
- D. Perform continuous monitorin

Answer: C

NEW QUESTION 136

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 139

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 140

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

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

Answer: B

NEW QUESTION 141

A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:

1. Information should be sourced from the trusted master data source.
 2. There must be future requirements for identity proofing of devices and users.
 3. A generic identity connector that can be reused must be developed.
 4. The current project scope is for internally hosted applications only.
- Which of the following solution building blocks should the security architect use to BEST meet the requirements?

- A. LDAP, multifactor authentication, oAuth, XACML
- B. AD, certificate-based authentication, Kerberos, SPML
- C. SAML, context-aware authentication, oAuth, WAYF
- D. NAC, radius, 802.1x, centralized active directory

Answer: A

NEW QUESTION 142

Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

- A. Lack of adequate in-house testing skills.
- B. Requirements for geographically based assessments
- C. Cost reduction measures
- D. Regulatory insistence on independent review

Answer: D

NEW QUESTION 143

Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: nonsensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive. Which of the following actions should the engineer take regarding the data?

- A. Label the data as extremely sensitive.
- B. Label the data as sensitive but accessible.
- C. Label the data as non-sensitive.
- D. Label the data as sensitive but export-controlle

Answer: C

NEW QUESTION 148

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

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

Answer: D

NEW QUESTION 152

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

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

Answer: A

NEW QUESTION 154

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

0000000000000000000000000000qjkeh 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 156

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

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

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

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

Answer: C

NEW QUESTION 158

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 161

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

Which of the following security controls would address the user's privacy concerns and provide the BEST level of security for the home network?

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

Answer: B

NEW QUESTION 165

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 166

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 170

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 173

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 178

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

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

Answer: B

NEW QUESTION 183

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 187

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 190

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

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

Answer: AC

NEW QUESTION 193

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 198

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

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

Answer: B

NEW QUESTION 202

A cybersecurity analyst is conducting packet analysis on the following:

Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:48:c2:5f:39:3c
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a

Which of the following is occurring in the given packet capture?

- A. ARP spoofing
- B. Broadcast storm
- C. Smurf attack
- D. Network enumeration
- E. Zero-day exploit

Answer: A

NEW QUESTION 205

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

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

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

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

Answer: B

NEW QUESTION 209

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 file-based mandatory access controls to prevent abnormal application modifications or executions.

References:

https://en.wikipedia.org/wiki/Security-Enhanced_Linux

NEW QUESTION 213

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

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

Answer: B

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

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

Incorrect Answers:

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

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

https://en.wikipedia.org/wiki/Data_deduplication

NEW QUESTION 214

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

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

Answer: A

Explanation: In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.

Therefore, the solution is to encrypt each individual partition separately. Incorrect Answers:

B: The question is asking for the BEST way to ensure confidentiality of individual operating system data.

A: Individual file encryption could work but if files are ever added to the operating systems (for updates etc.), you would have to manually encrypt the new files as well. A better solution would be to encrypt the entire partition. That way any new files added to the operating system would be automatically encrypted.

C: You cannot perform full disk encryption on an individual volume. Full disk encryption encrypts the entire disk.

D: FDE of the entire SSD as a single disk would encrypt the boot loaders which would prevent the operating systems from booting.

NEW QUESTION 216

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

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

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

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

Answer: C

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

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

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

Incorrect Answers:

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

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

resources or make changes to dat

A. The exploit

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

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

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

"https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use"Time_of_check_to_time_of_use

NEW QUESTION 217

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

A. The data may not be in a usable format.

B. The new storage array is not FCoE based.

C. The data may need a file system check.

D. The new storage array also only has a single controller

Answer: B

Explanation: Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol.

When moving the disks to another storage array, you need to ensure that the array supports FCoE, not just regular Fiber Channel. Fiber Channel arrays and Fiber Channel over Ethernet arrays use different network connections, hardware and protocols. Fiber Channel arrays use the Fiber Channel protocol over a dedicated Fiber Channel network whereas FCoE arrays use the Fiber Channel

protocol over an Ethernet network. Incorrect Answers:

A: It is unlikely that the data will not be in a usable format. Fiber Channel LUNs appear as local disks on a Windows computer. The computer then creates an NTFS volume on the fiber channel LUN. The storage array does not see the NTFS file system or the data stored on it. FCoE arrays only see the underlying block level storage.

C: The data would not need a file system check. FCoE arrays use block level storage and do not check the file system. Any file system checks would be performed by a Windows computer. Even if this happened, the data would be accessible after the check.

D: The new storage array also having a single controller would not be a problem. Only one controller is required.

References: https://en.wikipedia.org/wiki/Fibre_CHANNEL HYPERLINK

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

NEW QUESTION 221

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

NEW QUESTION 223

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

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

Answer: A

Explanation: The 2001::/32 prefix is used for Teredo tunneling.

Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols, it can perform its function even from behind network address translation (NAT) devices such as home routers.

Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets.

Teredo routes these datagrams on the IPv4 Internet and through NAT devices. Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.

Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32).

In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can then investigate the traffic within the network. Incorrect Answers:

B: Disabling IPv6 at the router will not help if the IPv6 traffic is encapsulated in IPv4 frames using Teredo. The question also states that there is no IPv6 routing into or out of the network.

C: 6to4 relays work in a similar way to Teredo. However, the addresses used by 6to4 relays start with 2002:: whereas Teredo addresses start with 2001.

Therefore, a 6to4 relay is not being used in this question so this answer is incorrect.

D: This question is asking for the BEST solution. Disabling the switch port would take the system connected to it offline and blocking traffic destined for 2001::/32 at the firewall would prevent inbound Teredo communications (if you block the traffic on the inbound interface). However, blocking port UDP 3544 would suffice and investigating the traffic is always a better solution than just disconnecting a system from the network.

References: https://en.wikipedia.org/wiki/Teredo_tunneling

"https://en.wikipedia.org/wiki/Teredo_tunneling"org/wiki/Teredo_tunHYPERLINK "https://en.wikipedia.org/wiki/Teredo_tunneling"neling

NEW QUESTION 227

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

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

Answer: C

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

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

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

The TPM is the hardware root of trust.

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

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

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

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

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

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

NEW QUESTION 232

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 233

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

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

Answer: B

Explanation: If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: This question is asking for the MOST comprehensive way to resolve the issue. A HIPS (Host Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.

C: This question is asking for the MOST comprehensive way to resolve the issue. Running the application in terminal services may reduce the threat landscape. However, it doesn't resolve the issue. Patching the application to eliminate the threat is a better solution.

D: This question is asking for the MOST comprehensive way to resolve the issue. A NIPS (Network Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.

References: <http://searchsecurity.techtarget.com/definition/buffer-overflow>

NEW QUESTION 238

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

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

Answer: A

Explanation: In this question, we need to protect the workstations when connected to either the office or home network. Therefore, we need a solution that stays with the workstation when the user takes the computer home.

A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.

Incorrect Answers:

B: Unified threat management (UTM) is a primary network gateway defense solution for organizations. In theory, UTM is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system: network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention and on-appliance reporting. However, UTM is designed to protect a network; it will not protect the user's workstations when connected to their home networks as required in this question.

C: Antivirus software will protect against attacks aided by known viruses. However, it will not protect against unknown attacks as required in this question.

D: NIPS stands for Network Intrusion Prevention Systems. A NIPS is designed to protect a network; it will not protect the user's workstations when connected to their home networks as required in this question.

E: Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. DLP does not protect against malicious attacks. References:

http://en.wikipedia.org/wiki/Intrusion_prevention_system"iki/Intrusion_prevention_system

NEW QUESTION 241

An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, [mail.example.org](mailto:example.org), archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

- A. Intermediate Root Certificate
- B. Wildcard Certificate
- C. EV x509 Certificate
- D. Subject Alternative Names Certificate

Answer: D

Explanation: Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate. When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.

Incorrect Answers:

A: An Intermediate Root Certificate is used to trust an intermediate CA (Certification Authority). The Intermediate root CA can issue certificates but the Intermediate Root Certificate itself cannot be used to secure multiple domains on a web server.

B: A wildcard certificate can be used to secure multiple domain names within the same higher level domain. For example: a wildcard certificate "*.example.com" can secure an unlimited number of domains that end in 'example.com' such as domain1.example.com, domain2.example.com etc. A wildcard certificate cannot be used to secure the domains listed in this question.

C: The certificate used to secure the domains will be an x509 certificate but it will not be a standard EV certificate. EV stands for extended validation. With a non-EV certificate, the issuing CA just ensures that you own the domains that you want to secure. With an EV certificate, further checks are carried out such as checks on your company. EV certificates take longer to issue due to the extra checks but the EV certificate provides extra guarantees to your customers that you are who you say you are. However, a standard EV certificate only secures a single domain.

NEW QUESTION 243

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 248

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 249

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

- A. Jailbroken mobile device

- B. Reconnaissance tools
- C. Network enumerator
- D. HTTP interceptor
- E. Vulnerability scanner
- F. Password cracker

Answer: DE

Explanation: Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.

To assess the security of the application server itself, you should use a vulnerability scanner.

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

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

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

Incorrect Answers:

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

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

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

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

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

"http://www.webopedia.com/TERM/V/vulnerability_scanning.html"rability_scanning.html

NEW QUESTION 251

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 256

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

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

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

Answer: AD

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

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

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

Incorrect Answers:

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

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

itself.

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

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

References: https://en.wikipedia.org/wiki/Static_program_analysis

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

NEW QUESTION 261

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

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

Answer: EF

Explanation: In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

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

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

Incorrect Answers:

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

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

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

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

References: https://en.wikipedia.org/wiki/Initialization_vector

NEW QUESTION 266

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

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

Answer: D

Explanation: JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.

Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help?

The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.

However there are some drawbacks to session identifiers:

They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.

They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a database to figure out who this session is for and if they are allowed to perform the requested operation.

JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format.

JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.

How To Store JWTs In The Browser

Short Answer:: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along the token for authentication purposes, but won't expose it to the JavaScript environment. Incorrect Answers:

A: A one-time key does not enable stateless communication.

B: SSL between the mobile application and the web services gateway will provide a secure encrypted connection between the two. However, SSL does not enable stateless communication.

C: A cookie is stateful, not stateless as required in the question. References:

<https://stormpath.com/blog/build-secure-user-interfaces-using-jwt> HYPERLINK "<https://stormpath.com/blog/build-secure-user-interfaces-using-jwts/>"s/

NEW QUESTION 269

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

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

Answer: A

Explanation: References:

<http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms>"sHYPERLINK

"<http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms>"tackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-

and-encryption-aHYPERLINK "<http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms>"lgorithms

NEW QUESTION 274

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

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

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

Answer: A

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

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

Incorrect Answers:

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

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

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

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

NEW QUESTION 275

An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are: Each lab must be on a separate network segment.

Labs must have access to the Internet, but not other lab networks.

Student devices must have network access, not simple access to hosts on the lab networks. Students must have a private certificate installed before gaining access.

Servers must have a private certificate installed locally to provide assurance to the students. All students must use the same VPN connection profile.

Which of the following components should be used to achieve the design in conjunction with directory services?

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

Answer: C

Explanation: IPsec VPN with mutual authentication meets the certificates requirements. RADIUS can be used with the directory service for the user authentication.

ACLs (access control lists) are the best solution for restricting access to network hosts. Incorrect Answers:

A: This solution has no provision for restricting access to hosts on the lab networks. B: This solution has no provision for restricting access to hosts on the lab networks. D: This solution has no provision for restricting access to hosts on the lab networks.

NEW QUESTION 280

A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated.

Users of the web application will not be added to the company's directory services. Passwords must not be stored in the code.

Which of the following meets these requirements?

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

Answer: A

Explanation: Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication.

OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.

Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam. Incorrect Answers:

B: The question states that users of the web application must be uniquely identified and authenticated. A shared client certificate for all users does not meet this requirement.

C: The question states that users of the web application will not be added to the company's directory services. SAML with federated directory services would require that the users are added to the directory services.

D: The question states that users of the web application must be uniquely identified and authenticated. Kerberos and browsers that support SAML provides no authentication mechanism. References:

<https://en.wikipedia.org/wiki/OpenID>

NEW QUESTION 284

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 288

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

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

Answer: A

Explanation: There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.

By eliminating all passwords and instead using digital signatures for authentication and authorization of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAML-enabled SaaS applications are easier and quicker to user provision in complex enterprise

environments, are more secure and help simplify identity management across large and diverse user communities.

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal. Incorrect Answers:

B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.

C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.

D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.

References:

<https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml-based-single-sign-on>

https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language"guage

NEW QUESTION 293

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CAS-003 Practice Exam Features:

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

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-003 Practice Test Here](#)