Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

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

NEW QUESTION 1
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.
Which of the following is the MOST appropriate order of steps to be taken?

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

Answer: A

NEW QUESTION 2
A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.
The person extracts the following data from the phone and EXIF data from some files:
DCIM Images folder
Audio books folder Torrentz
My TAX.xls
Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s
Location: 3500 Lacey Road USA
Which of the following BEST describes the security problem?

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

Answer: A

NEW QUESTION 3
A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

A. SaaS
B. PaaS
C. IaaS
D. Hybrid cloud
E. Network virtualization

Answer: B

NEW QUESTION 4
An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

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

Answer: D

NEW QUESTION 5
A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

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

Answer: B

NEW QUESTION 6
A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.
Which of the following exercise types should the analyst perform?

A. Summarize the most recently disclosed vulnerabilities.
B. Research industry best practices and latest RFCs.
C. Undertake an external vulnerability scan and penetration test.
D. Conduct a threat modeling exercis

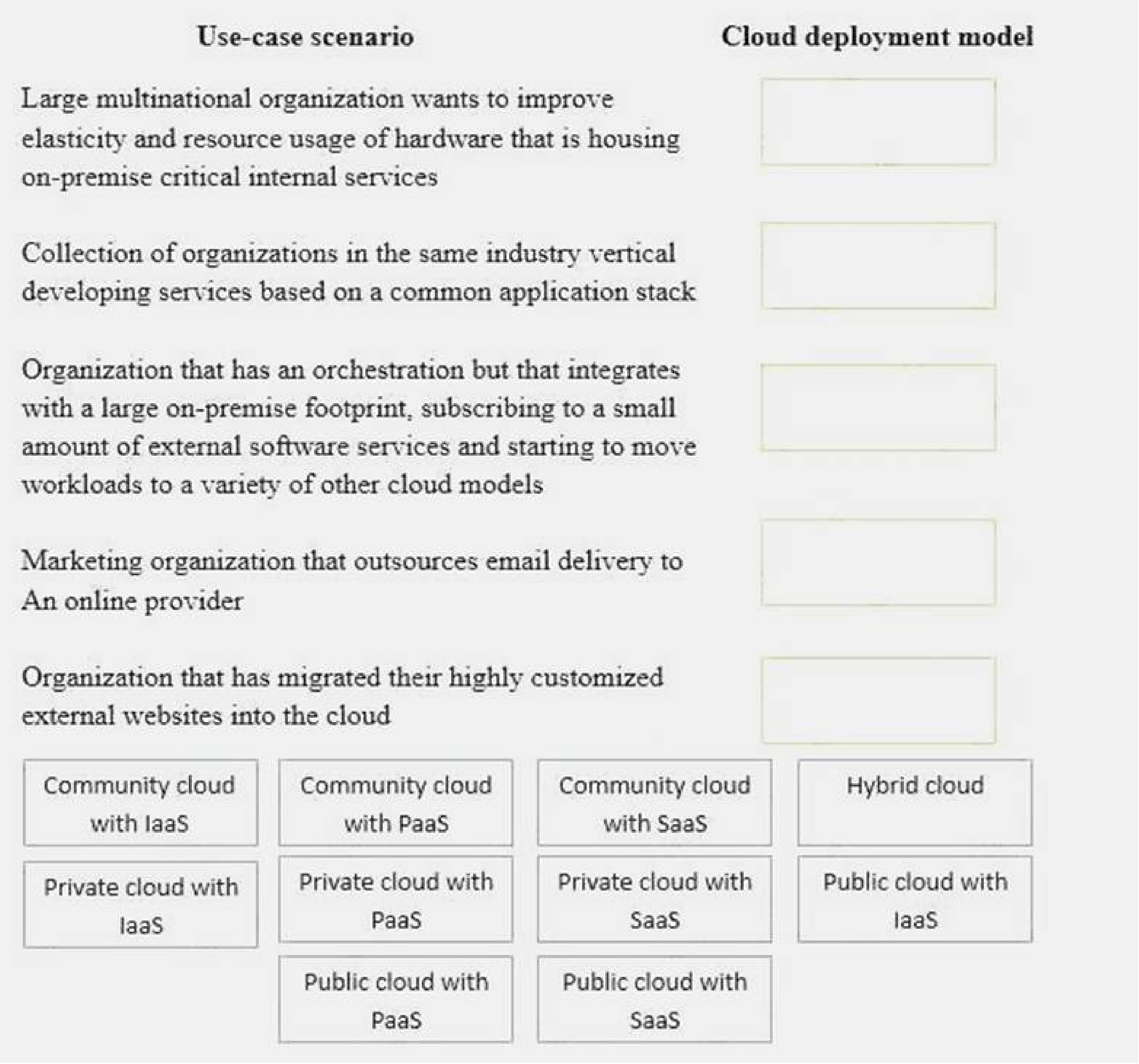
Answer: D

NEW QUESTION 7
An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.
Which of the following procedures should the security responder apply to the situation? (Choose two.)

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

Answer: BF

NEW QUESTION 8
DRAG DROP
Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.



Use-case scenario

Cloud deployment model

Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services

Collection of organizations in the same industry vertical developing services based on a common application stack

Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models

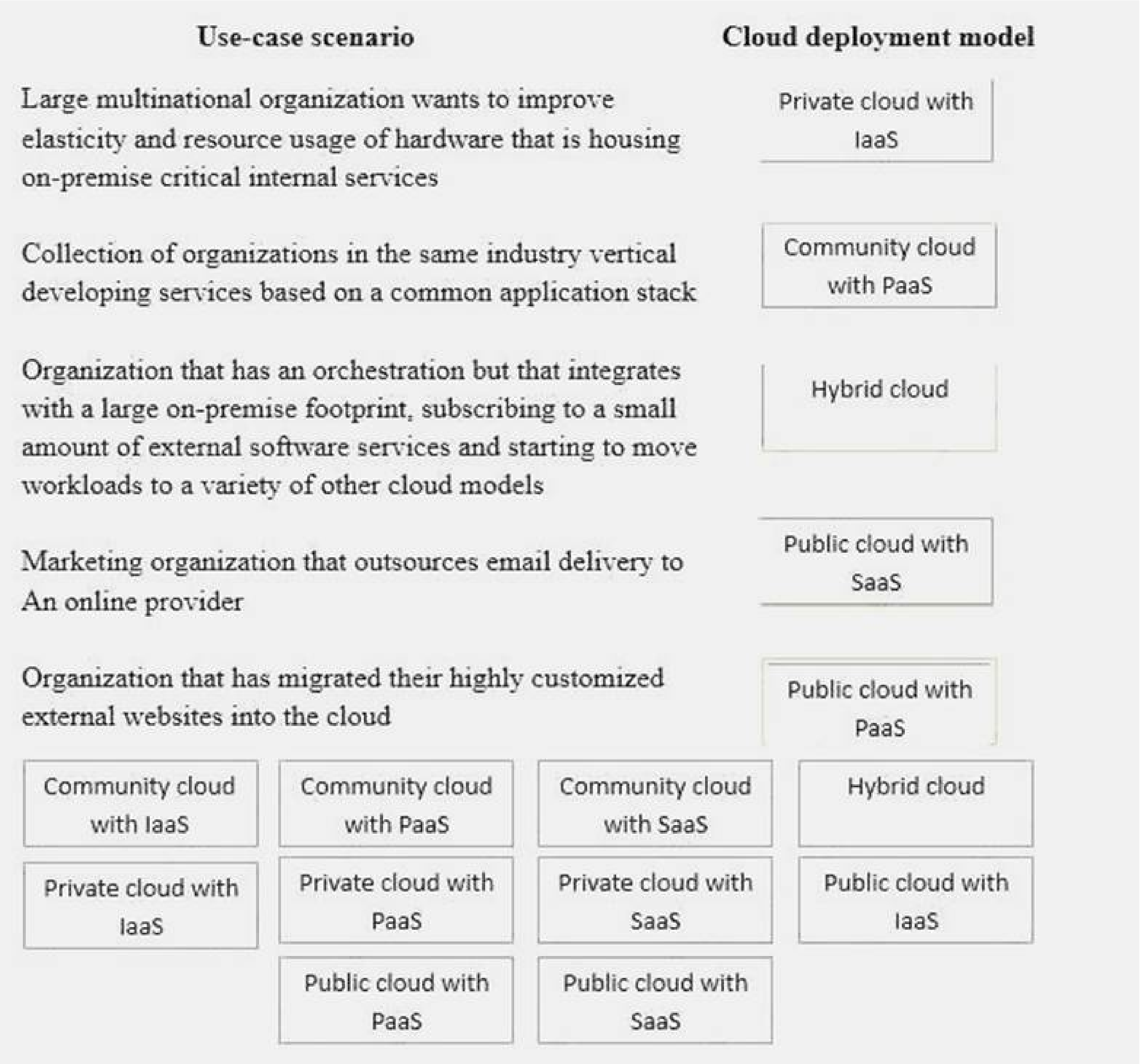
Marketing organization that outsources email delivery to An online provider

Organization that has migrated their highly customized external websites into the cloud

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	Private cloud with IaaS
Collection of organizations in the same industry vertical developing services based on a common application stack	Community cloud with PaaS
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	Hybrid cloud
Marketing organization that outsources email delivery to An online provider	Public cloud with SaaS
Organization that has migrated their highly customized external websites into the cloud	Public cloud with PaaS

Community cloud with IaaS
Community cloud with PaaS
Community cloud with SaaS
Hybrid cloud
Private cloud with IaaS
Private cloud with PaaS
Private cloud with SaaS
Public cloud with IaaS
Public cloud with PaaS
Public cloud with SaaS

NEW QUESTION 9
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
An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

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

Answer: CF

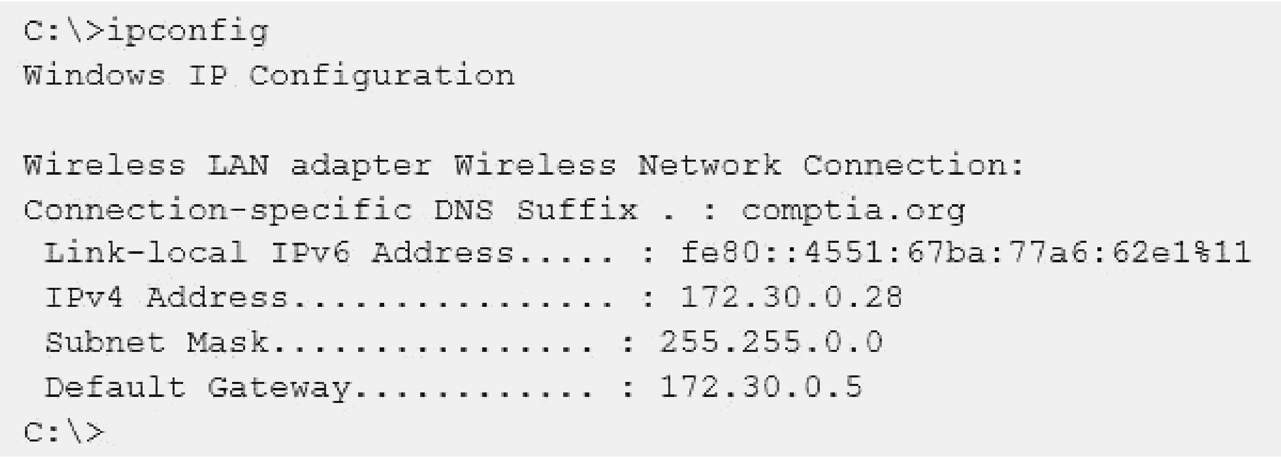
NEW QUESTION 10
A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO)

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 15
Given the following output from a local PC:



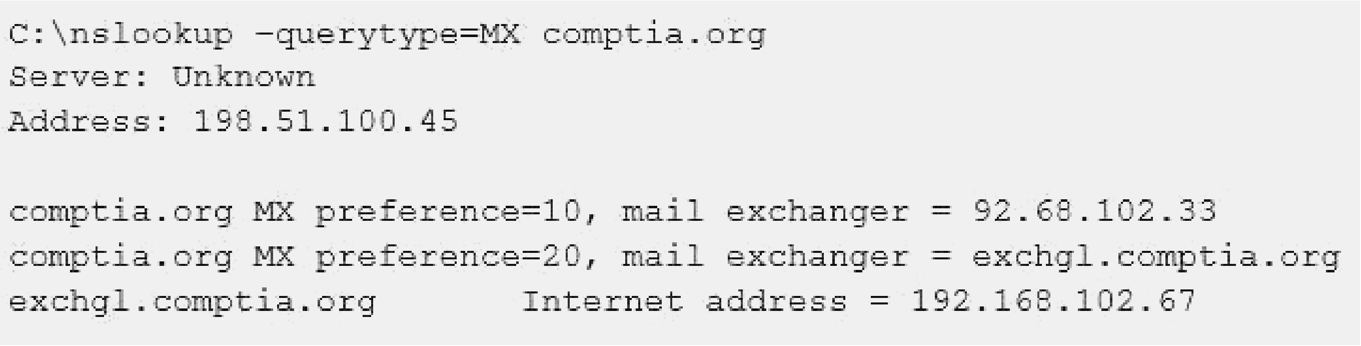
```
C:\>ipconfig
Windows IP Configuration

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 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 explogts
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 20
A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

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

Answer: D

NEW QUESTION 22
During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization’s reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

A. Air gaps
B. Access control lists
C. Spanning tree protocol
D. Network virtualization
E. Elastic load balancing

Answer: D

NEW QUESTION 24
An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the
assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

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

Answer: F

NEW QUESTION 29
A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

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

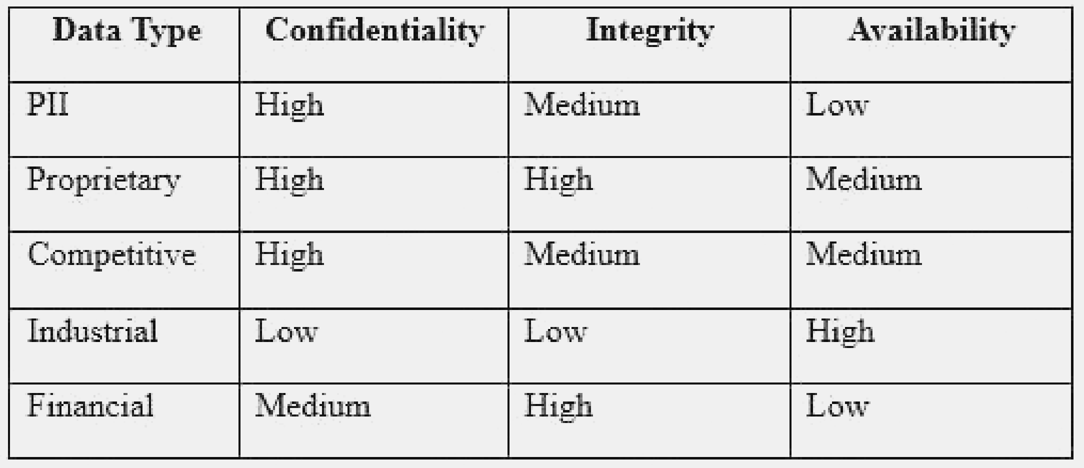
Answer: E

NEW QUESTION 32
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 explogted 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 37
An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.



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

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

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

Answer: B

NEW QUESTION 40
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

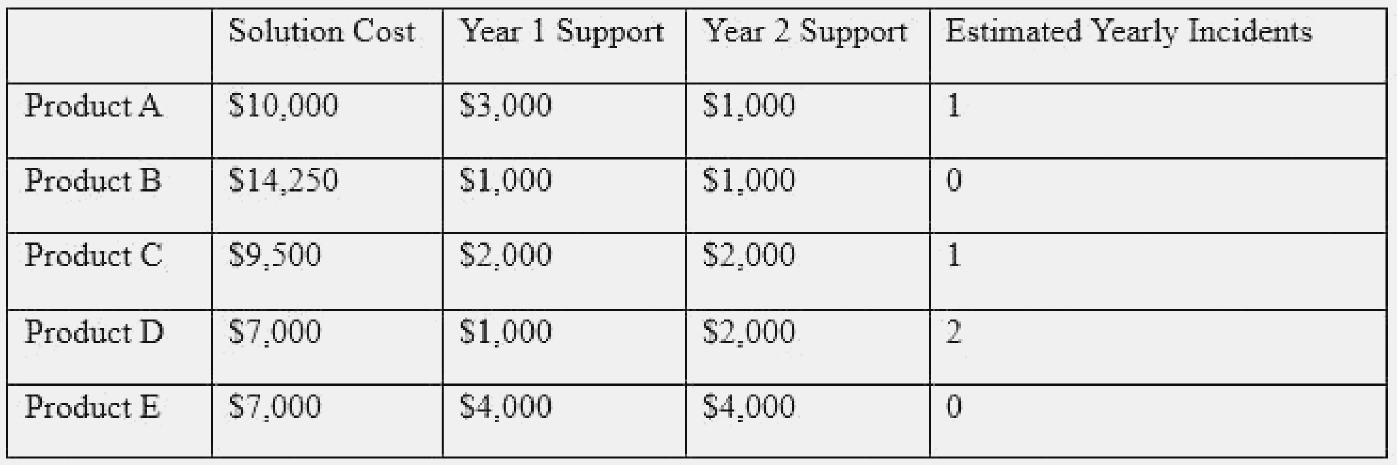
Answer: CD

NEW QUESTION 42
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 explogted 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 47
After investigating virus outbreaks that have cost the company $1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:



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

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

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

Answer: E

NEW QUESTION 48
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 49
An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

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

Answer: CE

NEW QUESTION 52
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 53
The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

A. Review the CVE database for critical explogts over the past year
B. Use social media to contact industry analysts
C. Use intelligence gathered from the Internet relay chat channels
D. Request information from security vendors and government agencies
E. Perform a penetration test of the competitor’s network and share the results with the board

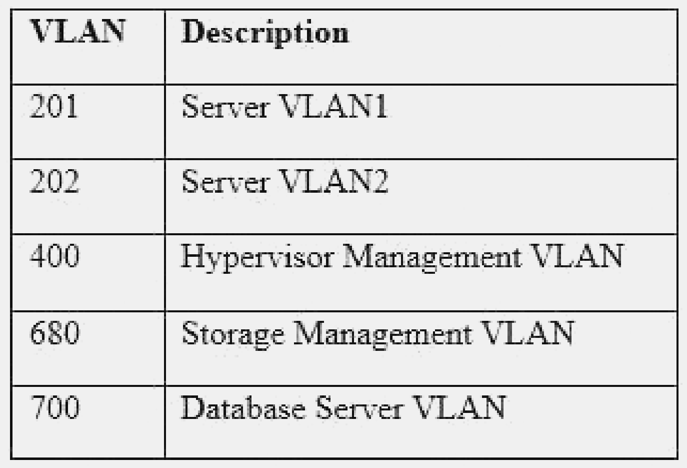
Answer: AD

NEW QUESTION 54
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 56
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 57
A forensics analyst suspects that a breach has occurred. Security logs show the company’s OS patch system may be compromised, and it is serving patches that contain a zero-day explogt and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server. Which of the following should the analyst use to confirm this suspicion?

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

Answer: B

NEW QUESTION 61
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

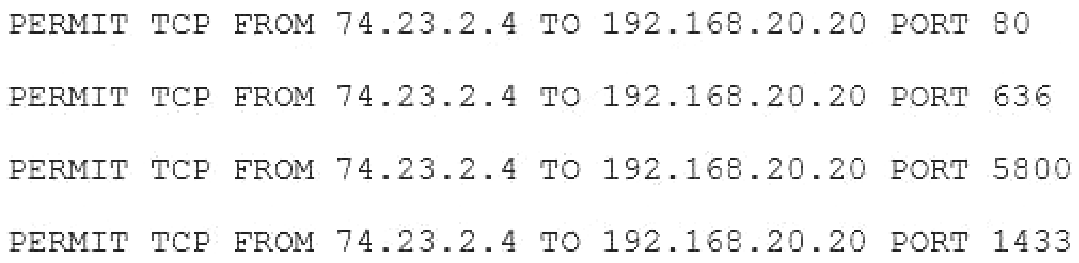
Answer: C

NEW QUESTION 65
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 70
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a third-party service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:



```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

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

A. LDAP
B. WAYF
C. OpenID
D. RADIUS
E. SAML

Answer: D

NEW QUESTION 71
An architect was recently hired by a power utility to increase the security posture of the company’s power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources.
Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

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

Answer: BE

NEW QUESTION 75
A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:
Store taxation-related documents for five years Store customer addresses in an encrypted format Destroy customer information after one year Keep data only in the customer’s home country
Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

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

Answer: BCH

NEW QUESTION 77

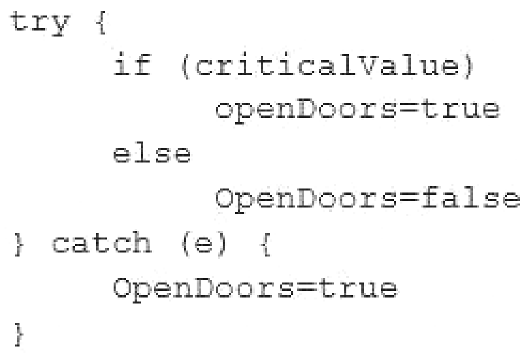
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is
performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements.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

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

Answer: A

NEW QUESTION 81

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



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

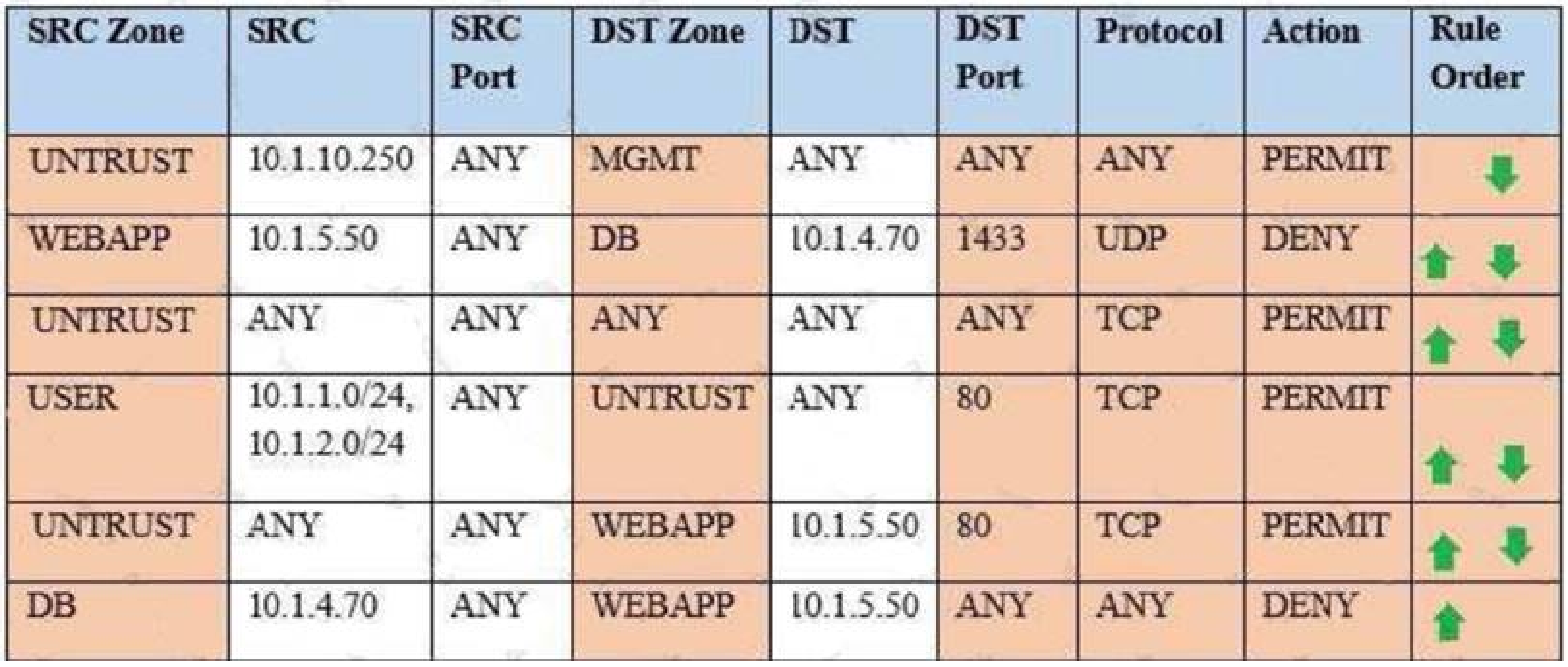
Which of the following is the BEST course of action for a security analyst to recommend to the software developer?

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

Answer: B

NEW QUESTION 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 SRCSRC Port DST Zone DSTDST 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 ZoneSRCSRC Port DST Zone DSTDST 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 ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action UNTRUST ANYANY WEBAPP 10.1.5.50 ANY TCP PERMITTask 4: Ensure the final rule is an explicit denyEnter this at the bottom of the access list i.
I. the line at the bottom of the rule: SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action ANY ANY ANY ANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco
J. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT
K. Task 1: A rule was added to prevent the management platform from accessing the interne
L. This rule is not workin
M. Identify the rule and correct this issue.In Rule n
N. 1 edit the Action to Deny to block internet access from the management platfor
O. SRC ZoneSRCSRC Port DST Zone DSTDST 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 ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n
R. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi
S. SRC ZoneANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco
T. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRCSRC PortDST Zone DSTDST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT

Answer: A

NEW QUESTION 87
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 91
To meet a SLA, which of the following document should be drafted, defining the company’s internal interdependent unit responsibilities and delivery timelines.

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

Answer: B

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

NEW QUESTION 94
A company’s existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh.
Which of the following is the BEST way to address these issues and mitigate risks to the organization?

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

Answer: B

NEW QUESTION 96
A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization’s file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.
Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

A. Access control list
B. Security requirements traceability matrix
C. Data owner matrix
D. Roles matrix

E. Data design document
F. Data access policies

Answer: DF

NEW QUESTION 99
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an explogt.
Which of the following would provide greater insight on the potential impact of this attempted attack?

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

Answer: B

NEW QUESTION 103
A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points. Which of the following solutions BEST meets the engineer’s goal?

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

Answer: C

NEW QUESTION 105
The Chief Information Officer (CIO) wants to increase security and accessibility among the organization’s cloud SaaS applications. The applications are configured to use passwords, and twofactor authentication is not provided natively. Which of the following would BEST address the CIO’s concerns?

A. Procure a password manager for the employees to use with the cloud applications.
B. Create a VPN tunnel between the on-premises environment and the cloud providers.
C. Deploy applications internally and migrate away from SaaS applications.
D. Implement an IdP that supports SAML and time-based, one-time password

Answer: B

NEW QUESTION 110
While attending a meeting with the human resources department, an organization’s information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use.
Additionally, each password has specific complexity requirements and different expiration time frames. Which of the following would be the BEST solution for the information security officer to recommend?

A. Utilizing MFA
B. Implementing SSO
C. Deploying 802.1X
D. Pushing SAML adoption
E. Implementing TACACS

Answer: B

NEW QUESTION 111
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

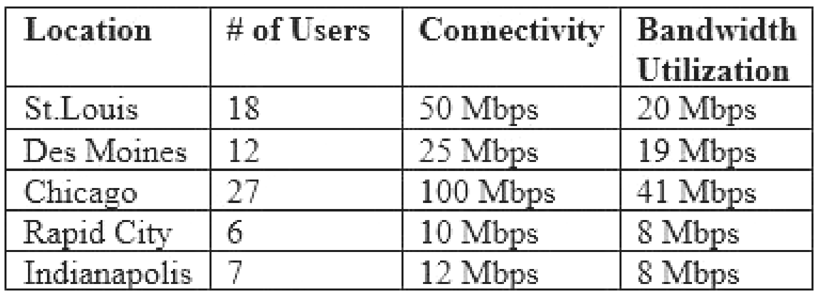
NEW QUESTION 115
A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients’ health information, management has identified the following requirements:
Data must be encrypted 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

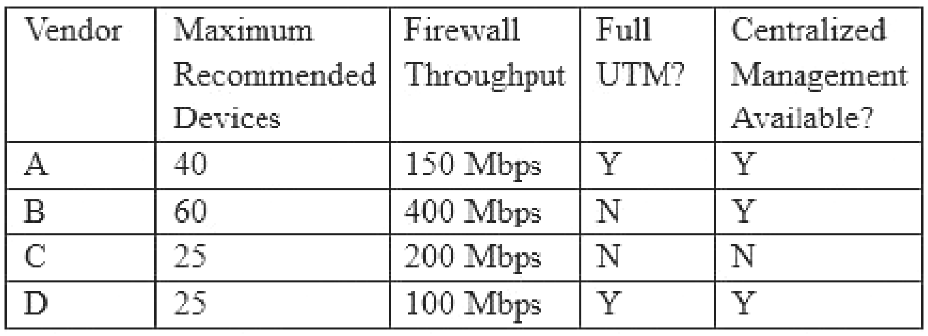
D. Biometric
E. USB 4.1
F. MicroSD

Answer: CD

NEW QUESTION 116
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 120
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 122
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 125
A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:
Configuration file 1: Operator ALL=/sbin/reboot Configuration file 2:
Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss Configuration file 3:
Operator:x:1000:1000::/home/operator:/bin/bash
Which of the following explains why an intended operator cannot perform the intended action?

A. The sudoers file is locked down to an incorrect command

B. SSH command shell restrictions are misconfigured
C. The passwd file is misconfigured
D. The SSH command is not allowing a pty session

Answer: D

NEW QUESTION 127
The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code. Which of the following is an SDLC best practice that should have been followed?

A. Versioning
B. Regression testing
C. Continuous integration
D. Integration testing

Answer: B

NEW QUESTION 130
An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

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

Answer: C

NEW QUESTION 133
A penetration tester noticed special characters in a database table. The penetration tester configured the browser to use an HTTP interceptor to verify that the front-end user registration web form accepts invalid input in the user’s age field. The developer was notified and asked to fix the issue. Which of the following is the MOST secure solution for the developer to implement?

A. IF $AGE == “!@#%^&*()_+<>?”:{}[]” THEN ERROR
B. IF $AGE == [1234567890] {1,3} THEN CONTINUE
C. IF $AGE != “a-bA-Z!@#$%^&*()_+<>?”{}[]”THEN CONTINUE
D. IF $AGE == [1-0] {0,2} THEN CONTINUE

Answer: B

NEW QUESTION 136
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:
1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications
Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

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

Answer: DEF

NEW QUESTION 141
The government is concerned with remote military missions being negatively being impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:
End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.
Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications
A host-based whitelist of approved websites and applications that only allow mission-related tools and sites
The use of satellite communication to include multiple proxy servers to scramble the source IP address
Which of the following is of MOST concern in this scenario?

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

Answer: A

NEW QUESTION 144
Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back. Which of the following BEST describes how the manager should respond?

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

Answer: D

NEW QUESTION 148
During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently. All paper records are scheduled to be shredded in a crosscut shredded, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.
Which of the following would ensure no data is recovered from the system droves once they are disposed of?

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

Answer: C

NEW QUESTION 152
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 153
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 158
There have been several explogts to critical devices within the network. However, there is currently no process to perform vulnerability analysis. Which the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

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

Answer: B

NEW QUESTION 160
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security anal... reviewing vulnerability scan result from a recent web server scan.
Portions of the scan results are shown below: Finding# 5144322
First time detected 10 nov 2015 09:00 GMT_0600
Last time detected 10 nov 2015 09:00 GMT_0600
CVSS base: 5
Access path: http://myorg.com/mailinglist.htm
Request: GET http://mailinglist.aspx?content=volunteer Response: C:\Docments\MarySmith\malinglist.pdf
Which of the following lines indicates information disclosure about the host that needs to be remediated?

A. Response: C:\Docments\marysmith\malinglist.pdf
B. Finding#5144322
C. First Time detected 10 nov 2015 09:00 GMT_0600
D. Access path: http//myorg.com/mailinglist.htm
E. Request: GET http://myorg.come/mailinglist.aspx?content=volunteer

Answer: A

NEW QUESTION 164
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
Scrusex: 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 time) After reviewing the alert, which of the following is the BEST analysis?

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

Answer: B

NEW QUESTION 169
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After invest the new vulnerability, it was determined that the web services providing are being impacted by this new threat. Which of the following data types a MOST likely at risk of exposure based on this new threat? (Select TWO)

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

Answer: AC

NEW QUESTION 170
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 174
An investigation showed a worm was introduced from an engineer’s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to a company policy and technical controls. Which of the following would be the MOST secure control implement?

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

Answer: A

NEW QUESTION 177
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, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can
be caused by malicious or flawed applications. Incorrect Answers:
A: An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. ACLs do not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.

C: A firewall is used to control data leaving a network or entering a network based on source and destination IP address and port numbers. IPTables is a Linux firewall. However, it does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
D: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. It does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
References:
https://en.wikipedia.org/wiki/SeHYPERLINK "https://en.wikipedia.org/wiki/Security- Enhanced_Linux"curity-Enhanced_Linux

NEW QUESTION 180
A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

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

Answer: A

Explanation:
In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server
to authenticate to the client.
This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.
Incorrect Answers:
B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.
C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.
D: The question states that the security authentication on the Windows domain is set to the highest
level. This will be NTLMv2, not NTLM (version1). References: https://en.wikipedia.org/wiki/NT_LAN_Manager

NEW QUESTION 181
A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

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

Answer: A

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

NEW QUESTION 184
A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

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

Answer: D

Explanation:
Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code. Incorrect Answers:
A: Client side input validation could be used to validate the input into input fields. Client side input validation is where the validation is performed by the web browser. However this question is asking for the BEST answer. A user with malicious intent could bypass the client side input validation whereas it would be much more difficult to bypass regular expression matching implemented in the application code.
B: A stored procedure is SQL code saved as a script. A SQL user can run the stored procedure rather than typing all the SQL code contained in the stored procedure. A stored procedure is not used for
validating input.
C: Any stored credit card details should be encrypted for security purposes. Also a secure method of transmission such as SSL or TLS should be used to encrypt

the data when transmitting the credit card number over a network such as the Internet. However, encrypting credit card details is not a way of securing the input fields in an application.

NEW QUESTION 187
A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.
Which of the following is the BEST course of action?

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

Answer: A

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

NEW QUESTION 189
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://searHYPERLINK "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 192
select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson
Which of the following types of attacks is the user attempting?

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

Answer: D

Explanation:
The code in the question is SQL code. The attack is a SQL injection attack.

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

NEW QUESTION 196
At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

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

Answer: DF

Explanation:
The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.
The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.
Incorrect Answers:
A: If a lack of memory was the cause of the problem, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops. Therefore adding guests with more memory will not solve the problem so this answer is incorrect.
B: This question is asking for the MOST likely cause of the problem. A backup running on the thin clients at 9am every morning as soon as the lab desktops start up is an unlikely cause of the problem. It is much more likely that the lab desktops starting up at the same time is causing high disk I/O.
C: The lab desktops starting up would not cause memory issues on the thin clients so adding memory will not solve the issue.
E: The lab desktops starting up would not cause network bandwidth issues so increasing the bandwidth will not solve the issue.
G: The lab desktops starting up would not saturate the network.
H: If the lab desktops are using more memory than is available to the host systems, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops.

NEW QUESTION 197
A developer has implemented a piece of client-side JavaScript code to sanitize a user’s provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:

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

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

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

Answer: C

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

NEW QUESTION 198
The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show
the following:

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

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

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

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

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

Answer: AF

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

NEW QUESTION 199
A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.
B. Database record encryption should be used when storing sensitive information on virtual servers.
C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel networ

Answer: A

Explanation:
VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration. When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.
Incorrect Answers:
B: Database record encryption is used for encrypting database records only. This question does not state that the only sensitive data is database records. The data is at risk as it travels across the network when virtual machines are migrated between hosts. Data is unencrypted when it is transmitted over the network.
C: Full disk encryption is a good idea to secure data stored on disk. However, the data is unencrypted when it is transmitted over the network.
D: The sensitive data is on the VDI virtual machines. Storing the sensitive information on an isolated fiber channel network would make the information inaccessible from the virtual machines.

NEW QUESTION 203
ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

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

Answer: C

Explanation:

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

NEW QUESTION 204
ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

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

Answer: BDF

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

NEW QUESTION 208
An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd
B. /etc/shadow
C. /etc/security
D. /etc/password
E. /sbin/logon
F. /bin/bash

Answer: AB

Explanation:
In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users' passwords means to store the passwords in an encrypted format.
Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd''. As this file is used by many tools (such as ``ls'') to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk.
Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible
format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc.
Incorrect Answers:
C: The /etc/security file contains group information. It does not contain usernames or passwords. D: There is no /etc/password file. Usernames are stored in the /etc/passwd file.
E: There is no /sbin/logon file. Usernames are stored in the /etc/passwd file.
F: /bin/bash is a UNIX shell used to run a script. It is not where usernames or passwords are stored. References:
http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.HYPERLINK "http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html"html

NEW QUESTION 210
A security administrator has noticed that an increased number of employees’ workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?

A. Implement an Acceptable Use Policy which addresses malware downloads.

B. Deploy a network access control system with a persistent agent.
C. Enforce mandatory security awareness training for all employees and contractors.
D. Block cloud-based storage software on the company networ

Answer: D

Explanation:
The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users to do not bring unauthorized data that could potentially contain malware into the network.
We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage services such as Dropbox or OneDrive.
Incorrect Answers:
A: An Acceptable Use Policy is always a good ide
A. However, it just tells the users how they ‘should’
use the company systems. It is not a technical control to prevent malware.
B: A network access control system is used to control access to the network. It does not prevent malware on client computers.
C: Mandatory security awareness training for all employees and contractors is always a good idea. However, it just educates the users about potential security risks. It is not a technical control to prevent malware.

NEW QUESTION 211
ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

A. TOTP
B. PAP
C. CHAP
D. HOTP

Answer: D

Explanation:
The question states that the HMAC counter-based codes and are valid until they are used. These are “one-time” use codes.
HOTP is an HMAC-based one-time password (OTP) algorithm.
HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.
Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP. Software tokens are available for (nearly) all major mobile/smartphone platforms.
Incorrect Answers:
A: TOTP is Time-based One-time Password. This is similar to the one-time password system used in this question. However, TOTPs expire after a period of time. In this question, the passwords (codes) expire after first use regardless of the timing of the first use.
B: PAP (Password Authentication Protocol) is a simple authentication protocol in which the user name and password is sent to a remote access server in a plaintext (unencrypted) form. PAP is not what is described in this question.
C: CHAP (Challenge-Handshake Authentication Protocol) is an authentication protocol that provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. CHAP is not what is described in this question.
References:
https://en.wikipedia.org/wiki/HMAC-based_One-time_HYPERLINK "https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm"Password_Algorithm

NEW QUESTION 213
A security tester is testing a website and performs the following manual query: https://www.comptia.com/cookies.jsp?products=5%20and%201=1
The following response is received in the payload: “ORA-000001: SQL command not properly ended” Which of the following is the response an example of?

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

Answer: A

Explanation:
This is an example of Fingerprinting. The response to the code entered includes “ORA-000001” which tells the attacker that the database software being used is Oracle.
Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished “passively” by sniffing network packets passing between hosts, or it can be accomplished “actively” by transmitting specially created packets to the target machine and analyzing the response.
Incorrect Answers:
B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not an example of XSS.
C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.
D: Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.
References: http://www.yourdictionary.com/fingerprinting

NEW QUESTION 215
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 217
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 218
Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

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

Answer: A

Explanation:
There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.
By eliminating all passwords and instead using digital signatures for authentication and authorization
of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAMLenabled SaaS applications are easier and quicker to user provision in complex enterprise
environments, are more secure and help simplify identity management across large and diverse user communities.
Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal. Incorrect Answers:

B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.
C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.
D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.
References:
https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml- based-single-sign-on
https://en.wikipedia.org/wiki/Security_Assertion_Markup_LanHYPERLINK "https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language"guage

NEW QUESTION 223
An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations
B. Review the security policies and standards
C. Perform a network penetration test
D. Review the firewall rule set and IPS logs

Answer: B

Explanation:
IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified.
Incorrect Answers:
A: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing switch and router configurations are not part of this process. C: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Performing a network penetration test is not part of this process.
D: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing the firewall rule set and IPS logs are not part of this process. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 270, 332

NEW QUESTION 227
A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

A. Memorandum of Agreement
B. Interconnection Security Agreement
C. Non-Disclosure Agreement
D. Operating Level Agreement

Answer: B

Explanation:
The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.
Incorrect Answers:
A: A memorandum of agreement (MOA) is a document composed between parties to cooperate on an agreed upon project or meet an agreed objective.
C: A nondisclosure agreement (NDA) is designed to protect confidential information.
D: An operating level agreement (OLA) defines the responsibilities of each partner's internal support group.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 238

NEW QUESTION 229
The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.
B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
C. Publish a policy that addresses the security requirements for working remotely with company equipment.
D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Answer: C

Explanation:
The question states that "the organization has not addressed telecommuting in the past". It is therefore unlikely that a company policy exists for telecommuting workers.
There are many types of company policies including Working time, Equality and diversity, Change management, Employment policies, Security policies and Data Protection policies.
In this question, a new method of working has been employed: remote working or telecommuting. Policies should be created to establish company security requirements (and any other requirements) for users working remotely.
Incorrect Answers:
A: The data should already be secure on the corporate systems. If an information classification scheme is used as part of the security, it should already have been created. Remote working does not add the requirement for an information classification scheme.
B: The personnel work from remote locations with corporate assets; their personal computers are not used. Therefore, we do not require database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
D: You should identify and document the proper procedures for telecommuting. However, the security requirements for working remotely with company equipment should be addressed first. Furthermore, you would not necessarily work with mid-level managers to identify and document the proper procedures for telecommuting if the company has a technology steering committee.

NEW QUESTION 233
A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user's communicatio
B. Next, place a legal hold on the user's email account.
C. Perform an e-discover using the applicable search term
D. Next, back up the user's email for a future investigation.
E. Place a legal hold on the user's email accoun
F. Next, perform e-discovery searches to collect applicable emails.
G. Perform a back up of the user's email accoun
H. Next, export the applicable emails that match the search terms.

Answer: C

Explanation:
A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government
investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.
Incorrect Answers:
A: Chain of custody (CoC) refers to the chronological documentation showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.
B: Potentially relevant data has to be placed on hold before e-discovery takes place. D: This option could still allow the email to be tampered with.
References: https://en.wikipedia.org/wiki/Electronic_discovery#Types_of_ESI https://en.wikipediHYPERLINK "https://en.wikipedia.org/wiki/Chain_of_custody"a.org/wiki/Chain_of_custody https://en.wikipedia.org/wiki/Legal_hold

NEW QUESTION 236
The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server’s baseline communications profile.
B. Configure the server logs to collect unusual activity including failed logins and restarted services.
C. Correlate data loss prevention logs for anomalous communications from the server.
D. Setup a packet capture on the firewall to collect all of the server communication

Answer: A

Explanation:
Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day explogts. Having knowledge of each host’s communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zeroday and APT (advance persistent threat) malware and agents. Data intelligence allows forensic
analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network. Incorrect Answers:
B: The attack has already happened; the server has already been compromised. Configuring the server logs to collect unusual activity including failed logins and restarted services might help against future attacks but it will not provide information on an attack that has already happened.
C: It is unlikely the DLP logs would contain anomalous communications from the server that would identify where the server collected the information.
D: The attack has already happened; the server has already been compromised. Setting up a packet capture on the firewall to collect all of the server communications might help against future attacks but it will not provide information on an attack that has already happened.
References:
https://www.sans.HYPERLINK "https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics- 35952"org/reading-room/whitepapers/forensics/ids-fiHYPERLINK
"https://www.sans.org/reading-room/whitepapers/forensics/ids-file-forensics-35952"le-forensics- 35952, p. 6

NEW QUESTION 239
During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of the following is the MOST likely cause of the noncompliance?

A. The devices are being modified and settings are being overridden in production.
B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
C. The desktop applications were configured with the default username and password.
D. 40 percent of the devices use full disk encryptio

Answer: A

Explanation:
The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops during the six months that they’ve had them.
Incorrect Answers:
B: A patch management system would not cause the devices to be noncompliant after issuing the latest patches. Devices are non-compliant because their patches are out-of-date, not because the
patches are too recent.
C: The desktop applications being configured with the default username and password would not be the cause of non-compliance. The hosts are hardened at the OS level so application configuration would not affect this.

D: Devices using full disk encryption would not be the cause of non-compliance. The hosts are hardened at the OS level. Disk encryption would have no effect on the patch level or configuration of the host.

NEW QUESTION 244
During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

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

Answer: D

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

NEW QUESTION 246
Company policy requires that all unsupported operating systems be removed from the network. The security administrator is using a combination of network based tools to identify such systems for the purpose of disconnecting them from the network. Which of the following tools, or outputs from the tools in use, can be used to help the security administrator make an approximate determination of the operating system in use on the local company network? (Select THREE).

A. Passive banner grabbing
B. Password cracker C.http://www.company.org/documents_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4
C. 443/tcp open http
D. dig host.company.com
E. 09:18:16.262743 IP (tos 0x0, ttl 64, id 9870, offset 0, flags [none], proto TCP (6), length 40)192.168.1.3.1051 > 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0
F. Nmap

Answer: AFG

Explanation:
Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.
The output displayed in option F includes information commonly examined to fingerprint the OS. Nmap provides features that include host discovery, as well as service and operating system detection.
Incorrect Answers:
B: A password cracker is used to recover passwords from data that have been stored in or transmitted by a computer system.
C: This answer is invalid as port 443 is used for HTTPS, not HTTP.
D: This web address link will not identify unsupported operating systems for the purpose of disconnecting them from the network.
E: The dig (domain information groper) command is a network administration command-line tool for
querying Domain Name System (DNS) name servers. References: https://en.wikipedia.org/wiki/Dig_(command) https://en.wikipedia.org/wiki/Password_cracking https://en.wikipediHYPERLINK
"https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers"a.org/wiki/List_of_TCP_and_U DP_port_numbers
http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabbHYPERLINK "http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic"ing-using-os.html?view=classic
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 174, 175

NEW QUESTION 247
The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?

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

Answer: C

Explanation:
Integer overflow errors can occur when a program fails to account for the fact that an arithmetic operation can result in a quantity either greater than a data type's maximum value or less than its minimum value.
Incorrect Answers:
A: Race conditions are a form of arrack that normally targets timing, and sometimes called asynchronous attacks. The objective is to explogt the delay between the time of check (TOC) and the time of use (TOU).
B: Click-jacking is when attackers deceive Web users into disclosing confidential information or taking control of their computer while clicking on seemingly harmless web pages.
D: Use after free errors happen when a program carries on making use of a pointer after it has been freed.
E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.

References: https://www.owasp.org/index.php/IntegerHYPERLINK "https://www.owasp.org/index.php/Integer_overflow"_overfHYPERLINK "https://www.owasp.org/index.php/Integer_overflow"low
https://www.owasp.org/index.php/Using_freed_memory
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 151, 153, 163

NEW QUESTION 249
A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

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

Answer: A

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

NEW QUESTION 251
The IT Security Analyst for a small organization is working on a customer's system and identifies a
possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.
B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.
C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.
D. Refer the issue to management for handling according to the incident response proces

Answer: D

Explanation:
The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.
Incorrect Answers:
A: Contacting the local authorities so an investigation can be started as quickly as possible would not be the first step. Apart from the fact an investigation could take any amount of time; this action does nothing to actually stop the unauthorized access.
B: Shutting down the production network interfaces on the server and changing all of the DBMS account passwords may be a step in the company's incident response procedure. However, as the IT Security Analyst does not know what the customer's incident response process is, he should notify management so they can make that decision.
C: Disabling the front-end web server may or may not stop the unauthorized access to the database server. However, taking a company web server offline may have a damaging impact on the company so the IT Security Analyst should not make that decision without consulting the management. Using email to determine how the customer would like to proceed is not appropriate method of communication. For something this urgent, a face-to-face meeting or at least a phone call would be more appropriate.

NEW QUESTION 255
The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:

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

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

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

D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

Answer: A

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

NEW QUESTION 256
An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

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

Answer: A

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

NEW QUESTION 257
......