

CAS-003 Dumps

CompTIA Advanced Security Practitioner (CASP)

<https://www.certleader.com/CAS-003-dumps.html>



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

The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.

Which of the following BEST meets the needs of the board?

- A. KRI:- Compliance with regulations- Backlog of unresolved security investigations- Severity of threats and vulnerabilities reported by sensors- Time to patch critical issues on a monthly basis
KPI:- Time to resolve open security items- % of suppliers with approved security control frameworks- EDR coverage across the fleet- Threat landscape rating
- B. KRI:- EDR coverage across the fleet- Backlog of unresolved security investigations- Time to patch critical issues on a monthly basis- Threat landscape rating
KPI:- Time to resolve open security items- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors
- C. KRI:- EDR coverage across the fleet- % of suppliers with approved security control framework- Backlog of unresolved security investigations- Threat landscape rating
KPI:- Time to resolve open security items- Compliance with regulations- Time to patch critical issues on a monthly basis- Severity of threats and vulnerabilities reported by sensors
- D. KPI:- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors- Threat landscape rating
KRI:- Time to resolve open security items- Backlog of unresolved security investigations- EDR coverage across the fleet- Time to patch critical issues on a monthly basis

Answer: A

NEW QUESTION 3

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

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

Answer: B

NEW QUESTION 4

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

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

DCIM Images folder

Audio books folder Torrentz

My TAX.xls

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

Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

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

Answer: A

NEW QUESTION 5

An engineer needs to provide access to company resources for several offshore contractors. The contractors require:

Access to a number of applications, including internal websites
Access to database data and the ability to manipulate it

The ability to log into Linux and Windows servers remotely

Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

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

Answer: DE

NEW QUESTION 6

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 7

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

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

Answer: B

NEW QUESTION 8

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 9

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

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

Answer: B

NEW QUESTION 10

DRAG DROP

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

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

Kerberos

oAuth

OTP

SAML

- A. Mastered
B. Not Mastered

Answer: A

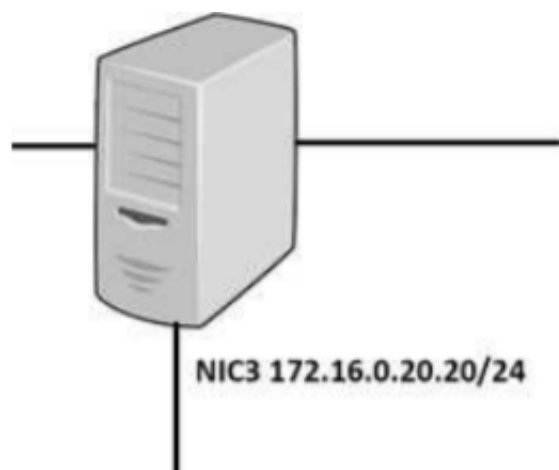
Explanation:

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

NEW QUESTION 10

DRAG DROP

A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.



The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

The DB server should not initiate outbound connections on NIC2

| | | |
|---|---|---|
| Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434 | Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389 | Permit UDP from 192.168.1.20 to 172.30.10.3 |
| Deny TCP from 10.0.10.20/24 to ANY | Deny IP from ANY to ANY | Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434 |
| Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434 | Permit IP from 172.30.10.3 to 192.168.1.20 | Deny IP from 10.0.10.20 to ANY |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

The DB server should not initiate outbound connections on NIC2

| | | |
|---|---|---|
| Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389 | Permit UDP from 192.168.1.20 to 172.30.10.3 | Permit IP from 172.30.10.3 to 192.168.1.20 |
| Deny IP from 10.0.10.20 to ANY | Deny IP from ANY to ANY | Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434 |
| Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434 | Deny TCP from 10.0.10.20/24 to ANY | Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434 |

NEW QUESTION 12

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 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 18

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

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

Answer: B

NEW QUESTION 23

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 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 28

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

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

Answer: EF

NEW QUESTION 30

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

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

Answer: B

NEW QUESTION 32

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

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

Answer: AC

NEW QUESTION 36

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

Duplicate IP addresses
Rogue network devices

Infected systems probing the company's network

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

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

Answer: BC

NEW QUESTION 40

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

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

Answer: B

NEW QUESTION 41

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

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

Answer: C

NEW QUESTION 45

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 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 46

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

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

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

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

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

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

Answer: BCE

NEW QUESTION 49

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

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

Answer: AB

NEW QUESTION 53

An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible.

Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

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

Answer: AEF

NEW QUESTION 58

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

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

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

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

Answer: B

NEW QUESTION 62

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 65

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 70

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

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

Answer: A

NEW QUESTION 72

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

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

Answer: B

NEW QUESTION 75

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

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

Answer: A

NEW QUESTION 80

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 81

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

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

Answer: C

NEW QUESTION 84

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 85

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

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

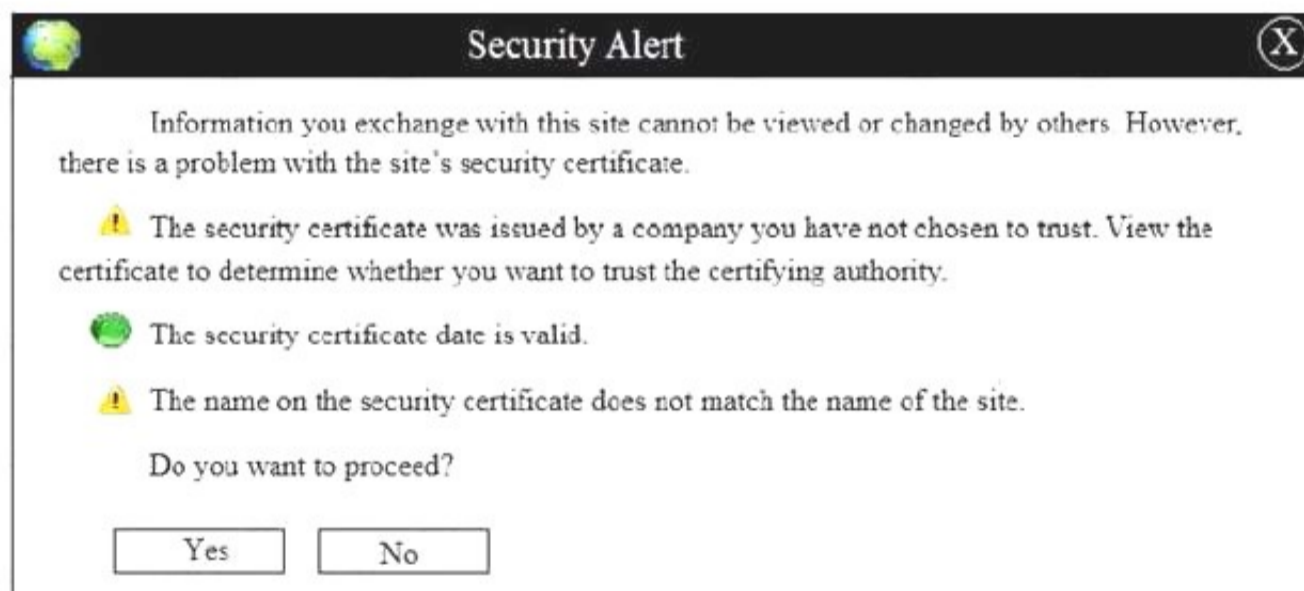
- A. Conduct a penetration test on each function as it is developed
- B. Develop a set of basic checks for common coding errors
- C. Adopt a waterfall method of software development
- D. Implement unit tests that incorporate static code analyzers

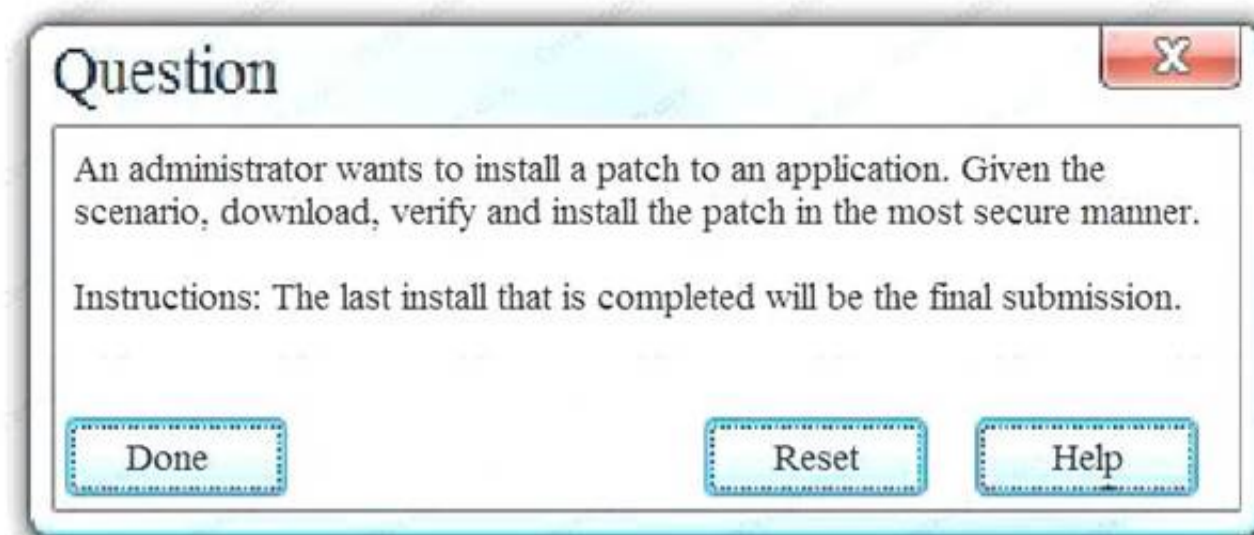
Answer: D

NEW QUESTION 89

Exhibit:

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





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

Answer: B

NEW QUESTION 93

Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

    char username[8];

    printf("Enter your username: ");

    gets(username)

    printf("\n");

    if (username == NULL) {

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

    }

    if strcmp(username, "admin") {

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

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

    } else {

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

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

    }

}
```

Which of the following vulnerability types in the MOST concerning?

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

Answer: B

NEW QUESTION 96

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 97

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

| Timestamp | SourceIP | CustName | PreferredContact | ProdName | Comments |
|--------------------|--------------|----------|------------------|----------|------------------------|
| Monday 10:00:04 | 10.14.34.55 | aaaaa | Phone | Widget1 | None left |
| Monday 10:00:04 | 10.14.34.55 | bbbbb | Phone | Widget1 | None left |
| Monday 10:00:05 | 10.14.34.55 | cccc | Phone | Widget1 | ../../../../etc/passwd |
| Monday 10:01:03 | 10.14.34.55 | ddddd | Phone | Widget1 | None left |
| Monday 10:01:04 | 10.14.34.55 | eeee | Phone | Widget1 | None left |
| Monday 10:01:05 | 10.14.34.55 | ffff | Phone | Widget1 | 1=1 |
| Monday 10:03:05 | 172.16.34.20 | Joe | Phone | Widget30 | Love the Widget! |
| Monday 10:04:01 | 10.14.34.55 | ggggg | Phone | Widget1 | <script> |
| Monday 10:05:05 | 10.14.34.55 | hhhhh | Phone | Widget1 | wget cookie |
| Monday 10:05:05 | 10.14.34.55 | iiii | Phone | Widget1 | None left |
| Monday 10:05:06 | 10.14.34.55 | llll | Phone | Widget1 | None left |

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

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

Answer: A

NEW QUESTION 100

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

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

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

Answer: B

NEW QUESTION 104

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

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

Answer: B

NEW QUESTION 106

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

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

Answer: BF

NEW QUESTION 109

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

The SIEM must be able to identify traffic baseline anomalies

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

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

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

Answer: BD

NEW QUESTION 113

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

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

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

Answer: A

NEW QUESTION 115

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

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

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

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

Answer: A

NEW QUESTION 120

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 123

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

An HOTP service is installed on the RADIUS server.

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

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

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

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

Answer: B

NEW QUESTION 127

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 132

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

Involve business owners and stakeholders Create an applicable scenario

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

Which of the following exercises has the CEO requested?

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

Answer: C

NEW QUESTION 135

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

stolen any funds.

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

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

Answer: D

NEW QUESTION 136

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

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

Answer: A

NEW QUESTION 141

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

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

Answer: D

NEW QUESTION 146

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

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

Answer: C

NEW QUESTION 148

A 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 150

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

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

Answer: A

NEW QUESTION 152

A company has gone through a round of phishing attacks. More than 200 users have had their workstation infected because they clicked on a link in an email. An incident analysis has determined an executable ran and compromised the administrator account on each workstation. Management is demanding the information security team prevent this from happening again. Which of the following would BEST prevent this from happening again?

- A. Antivirus
- B. Patch management
- C. Log monitoring
- D. Application whitelisting

E. Awareness training

Answer: A

NEW QUESTION 156

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

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

Answer: A

NEW QUESTION 161

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 162

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 164

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

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

The analyst then reviews the associated output:

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

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

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

Answer: B

NEW QUESTION 168

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 shredder, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.

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

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

Answer: C

NEW QUESTION 170

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

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

Answer: AC

NEW QUESTION 175

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

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

Answer: B

NEW QUESTION 179

During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter

Port state 161/UDP open 162/UDP open 163/TCP open

The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

- A. Patch and restart the unknown services.
- B. Segment and firewall the controller's network
- C. Disable the unidentified service on the controller.
- D. Implement SNMPv3 to secure communication.
- E. Disable TCP/UDP PORTS 161 THROUGH 163

Answer: D

NEW QUESTION 180

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

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

Answer: B

NEW QUESTION 185

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

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

First time detected 10 nov 2015 09:00 GMT_0600

Last time detected 10 nov 2015 09:00 GMT_0600

CVSS base: 5

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

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

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

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

Answer: A

NEW QUESTION 186

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

Scruscx: 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 187

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

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

Answer: C

NEW QUESTION 192

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 193

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

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

Answer: B

NEW QUESTION 196

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 200

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

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

Answer: B

Explanation:

The most common open source operating system is LINUX.

Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control

security policies, including United States Department of Defense–style mandatory access controls (MAC).

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

be caused by malicious or flawed applications. Incorrect Answers:

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

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

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

References:

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

NEW QUESTION 201

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

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

Answer: A

Explanation:

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

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

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

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

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

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

NEW QUESTION 205

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 208

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

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

Answer: B

Explanation:

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

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers,

corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

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

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

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

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

NEW QUESTION 209

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 exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: The code in 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 213

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

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

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

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

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

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

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

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

- A. An authorized administrator has logged into the root account remotely.
- B. The administrator should disable remote root logins.
- C. Isolate the system immediately and begin forensic analysis on the host.
- D. A remote attacker has compromised the root account using a buffer overflow in sshd.
- E. A remote attacker has guessed the root password using a dictionary attack.
- F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
- G. A remote attacker has compromised the private key of the root account.
- H. Change the root password immediately to a password not found in a dictionary.

Answer: CE

Explanation:

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

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

Incorrect Answers:

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

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

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

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

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

NEW QUESTION 216

Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the

following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

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

Answer: B

Explanation:

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

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

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

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

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

References:

[http://searchvHYPERLINK \"http://searchvirtualdesktop.techtarget.com/definition/virtualdesktop\" irtualdesktop.techtarget.com/definition/virtual-desktop](http://searchvHYPERLINK \)

NEW QUESTION 217

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

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

Answer: A

Explanation:

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

Incorrect Answers:

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

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

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

NEW QUESTION 220

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

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

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

Answer: AD

Explanation:

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

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

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

Incorrect Answers:

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

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

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

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

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

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

NEW QUESTION 224

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 226

A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be filexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

- A. A partition-based software encryption product with a low-level boot protection and authentication
- B. A container-based encryption product that allows the end users to select which files to encrypt
- C. A full-disk hardware-based encryption product with a low-level boot protection and authentication
- D. A file-based encryption product using profiles to target areas on the file system to encrypt

Answer: D

Explanation:

The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.

File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer.

Profiles can be used to determine areas on the file system to encrypt such as Document folders. Incorrect Answers:

A: A partition-based software encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts. B: An encryption product that allows the end users to select which files to encrypt is not the best solution. A solution that automatically encrypts the necessary data is a better solution.

C: A full-disk hardware-based encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts.

NEW QUESTION 229

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

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

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

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

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 230

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 233

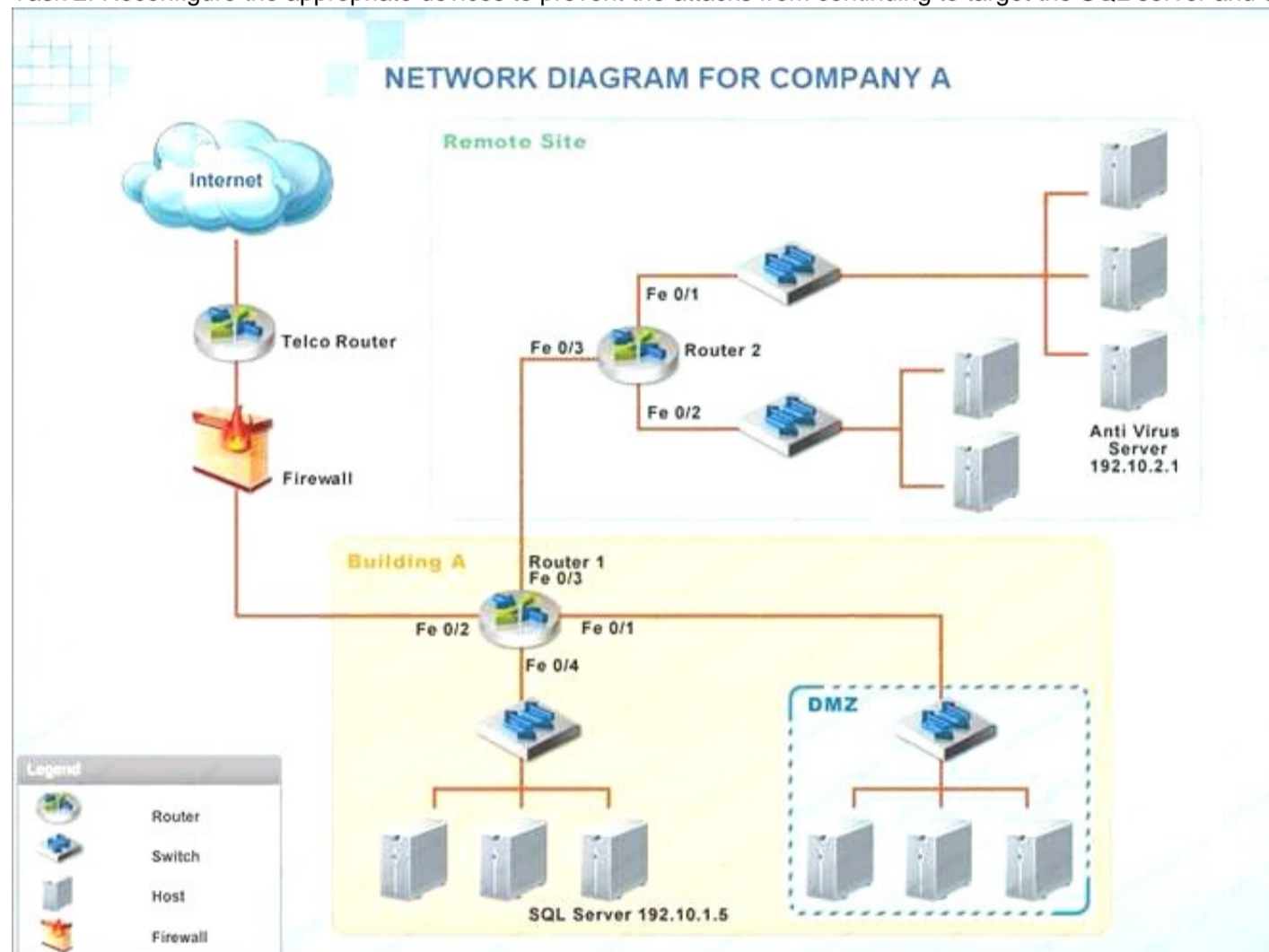
Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP

address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.

Instructions: Click on the simulation button to refer to the Network Diagram for Company A. Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.



```

Router1
Log Command Prompt

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

```

```

Router2
Log Command Prompt

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

```

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

A. Check the answer below

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

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

| | | | |
|---------------|---------------|-------------------------------------|--------------------------|
| 192.10.3.0/24 | 192.10.1.0/24 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 192.10.3.0/24 | 192.10.2.0/24 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

B. Check the answer below

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

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

| | | | |
|---------------|---------------|--------------------------|--------------------------|
| 192.10.3.0/24 | 192.10.1.0/24 | <input type="checkbox"/> | <input type="checkbox"/> |
| 192.10.3.0/24 | 192.10.2.0/24 | <input type="checkbox"/> | <input type="checkbox"/> |

Answer: A

NEW QUESTION 236

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

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

Firewall Interface

Instructions:

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

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



A. Check the answer below

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

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

B. This rule is not workin

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

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

E. This needs to be set to Permit.

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

Task 2)

All web servers have been changed to communicate solely over SS

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

G. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).

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

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ

H. This rule is not workin

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

J. It is not working because the protocol is wron

K. It should be TCP, not UDP.

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

Task 4) Other than allowing all

hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.The network time rule is shown in the image below.

However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rule

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

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

M. Check the answer below

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

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

N. This rule is not workin

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

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

Q. This needs to be set to Permit.

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

Task 2)

All web servers have been changed to communicate solely over SS

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

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

T. This rule is not workin

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

. It is not working because the protocol is wron

. It should be TCP, not UDP.

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

Task 4)

Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed. The network time rule is shown in the image

below. However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul

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

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

Answer: A

NEW QUESTION 241

A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is \$40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was \$100,000. Which of the following is the monetary value earned during the first year of operation?

- A. \$60,000
- B. \$100,000
- C. \$140,000
- D. \$200,000

Answer: A

Explanation:

ALE before implementing application caching: $ALE = ARO \times SLE$

$ALE = 5 \times \$40,000$ $ALE = \$200,000$

ALE after implementing application caching: $ALE = ARO \times SLE$

$ALE = 1 \times \$40,000$ $ALE = \$40,000$

The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.

Monetary value earned = $\$200,000 - \$40,000 - \$100,000$ Monetary value earned = \$60,000

Incorrect Answers:

B: \$100,000 would be the answer if the ARO after implementing application caching was 0.

C: \$140,000 is the expected loss in the first year. The ALE after implementing application caching + the cost of the countermeasures.

D: The answer cannot be \$200,000 because in the first year of operation the ALE after implementing application caching is \$40,000 and the cost of the countermeasures is \$100,000.

References: <http://www.pearsonitcertification.com/articles/article.aspx?p=418007> HYPERLINK

"<http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4>"&HYPERLINK

"<http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4>"seqNum=4

NEW QUESTION 242

A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must

be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

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

Answer: CD

Explanation:

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

Company profile, strategy, mission, and reputation

Financial status, including reviews of audited financial statements

Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks

Process expertise, methodology, and effectiveness Quality initiatives and certifications

Technology, infrastructure stability, and applications Security and audit controls

Legal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors

Insurance

Disaster recovery and business continuity policies C and D form part of Security and audit controls. Incorrect Answers:

A: A Physical Penetration Test recognizes the security weaknesses and strengths of the physical security. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.

B: A penetration test is a software attack on a computer system that looks for security weaknesses. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.

E: A security code review is an examination of an application that is designed to identify and assess threats to an organization. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.

References: https://en.wikipedia.org/wiki/Due_diligence [ht](#)HYPERLINK

"<http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5>"[p://www.ftpress.com/articles/](http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5)

[article.aspx?p=465313](http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5)HYPERLINK "<http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5>"&HYPERLINK

"<http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5>"seqNum=5 <http://seclists.org/pen-test/2004/Dec/11>

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 169

NEW QUESTION 246

After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

- A. Least privilege
- B. Job rotation
- C. Mandatory vacation
- D. Separation of duties

Answer: B

Explanation:

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

Incorrect Answers:

A: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.

C: Mandatory vacation is used to discover misuse and allow the organization time to audit a suspected employee while they are away from work.

D: Separation of duties requires more than one person to complete a task. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 245

NEW QUESTION 249

A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

- A. During the Identification Phase
- B. During the Lessons Learned phase
- C. During the Containment Phase
- D. During the Preparation Phase

Answer: B

Explanation:

The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.

Incorrect Answers:

A: The Identification Phase is the second step in the Incident Response process that deals with the detection of events and incidents.

C: The Containment Phase is the third step in the Incident Response process that deals with the planning, training, and execution of the incident response plan.

D: The Preparation Phase is the first step in the Incident Response process that deals with policies and procedures required to attend to the potential of security incidents.

References:

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

NEW QUESTION 254

Which of the following provides the BEST risk calculation methodology?

- A. Annual Loss Expectancy (ALE) x Value of Asset
- B. Potential Loss x Event Probability x Control Failure Probability
- C. Impact x Threat x Vulnerability
- D. Risk Likelihood x Annual Loss Expectancy (ALE)

Answer: B

Explanation:

Of the options given, the BEST risk calculation methodology would be Potential Loss x Event Probability x Control Failure Probability. This exam is about computer and data security so 'loss' caused by risk is not necessarily a monetary value.

For example:

Potential Loss could refer to the data lost in the event of a data storage failure. Event probability could be the risk a disk drive or drives failing.

Control Failure Probability could be the risk of the storage RAID not being able to handle the number of failed hard drives without losing data.

Incorrect Answers:

A: Annual Loss Expectancy (ALE) is a monetary value used to calculate how much is expected to be lost in one year. For example, if the cost of a failure (Single Loss Expectancy (SLE)) is \$1000 and the failure is expected to happen 5 times in a year (Annualized Rate of Occurrence (ARO)), then the Annual Loss Expectancy is \$5000. ALE is not the best calculation for I.T. risk calculation.

C: Impact x Threat x Vulnerability looks like a good calculation at first glance. However, for a risk calculation there needs to be a definition of the likelihood (probability) of the risk.

D: Annual Loss Expectancy (ALE) is a monetary value used to calculate how much is expected to be lost in one year. ALE is not the best calculation for I.T. risk calculation.

References:

<https://iaonline.theiia.org/understanding-the-risk-management-process>

NEW QUESTION 258

A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and require two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

- A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
- B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
- C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.
- D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
- E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Answer: AD

Explanation:

Privacy could be compromised because patient records can be from a doctor's personal device. This can then be shown to persons not authorized to view this information. Similarly, the doctor's personal device could have malware on it.

Incorrect Answers:

B: Device encryption is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.

C: The guest WiFi network is isolated from the internal network with appropriate security controls and the doctors and specialists can interact with the hospital's system via a remote desktop type interface.

E: Remote wiping is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.

References:

<http://www.gwava.com/blog/top-10-byod-business-concerns>

NEW QUESTION 263

The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

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

Answer: C

Explanation:

Mitigation means that a control is used to reduce the risk. In this case, the control is training. Incorrect Answers:

A: To avoid could mean not performing an activity that might bear risk.

B: To accept the risk means that the benefits of moving forward outweigh the risk. D: To transfer the risk means that the risk is deflected to a third party.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 88, 218

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

NEW QUESTION 266

A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

- A. The malware file's modify, access, change time properties.
- B. The timeline analysis of the file system.
- C. The time stamp of the malware in the swap file.
- D. The date/time stamp of the malware detection in the antivirus log

Answer: B

Explanation:

Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state

changes that have occurred on a computer.

Incorrect Answers:

A: This option will not help to determine when the system became infected.

C: A swap file is a space on a hard disk used as the virtual memory extension of a computer's real memory, which allows your computer's operating system to pretend that you have more RAM than you actually do.

D: This will tell you when the antivirus detected the malware, not when the system became infected. References:

<http://www.basistech.com/autopsy-feature-graphical-timeline-analysis-for-cyber-forensics/> <http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-or-pagefile>

"<http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-or-pagefile>" om/definition/swap-file-swap-space-or-pagefile

NEW QUESTION 270

The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

A. The corporate network is the only network that is audited by regulators and customers.

B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.

C. Home networks are unknown to attackers and less likely to be targeted directly.

D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Answer: B

Explanation:

Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. Data aggregation increases the impact and scale of a security breach. The amount of data aggregation on the corporate network is much more than on an employee's home network, and is therefore more valuable.

Incorrect Answers:

A: Protecting its corporate network boundary is the only network that is audited by regulators and customers is not a good enough reason. Protecting its corporate network boundary because the amount of data aggregation on the corporate network is much more than on an employee's home network is.

C: Home networks are not less likely to be targeted directly because they are unknown to attackers, but because the amount of data aggregation available on the corporate network is much more.

D: Whether employees are browsing from their personal computers or logged into the corporate network, they could still be attacked. However, the amount of data aggregation on the corporate network is much more than on an employee's home network, and is therefore more valuable. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 101

<http://searchsqlserver.techtarget.com/definition/data-aggregation>

NEW QUESTION 271

A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

A. Demonstration of IPS system

B. Review vendor selection process

C. Calculate the ALE for the event

D. Discussion of event timeline

E. Assigning of follow up items

Answer: DE

Explanation:

Lessons learned process is the sixth step in the Incident Response process. Everybody that was involved in the process reviews what happened and why it happened. It is during this step that they determine what changes should be introduced to prevent future problems.

Incorrect Answers:

A: Demonstration of the IPS system would not take place as part of the Incident Response process. B: Reviewing the vendor selection process is not part of the Incident Response process.

C: Calculating the ALE for the event is part of Quantitative Risk Assessment, not Incident Response. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 215, 249

NEW QUESTION 272

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.

B. Require each user to log passwords used for file encryption to a decentralized repository.

C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.

D. Allow encryption only by tools that use public keys from the existing escrowed corporate PK

Answer: D

Explanation:

Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network.

An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manner, a user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing the data in a way that only authorized people can access the data.

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of data.

A. The data can only be decrypted by the private key.

In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is holding the private key of the PKI.

By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.

Incorrect Answers:

A: File encryption should be enabled to enable the archiving of the data.

B: Requiring each user to log passwords used for file encryption is not a good solution. Apart from there being no mechanism to enforce this, you should not need

to know users' passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords.

C: You cannot and should not be able to archive old passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords. References:

<http://searchfinancialsecurity.techtarget.com/definition/electronicdiscovery>" [financialsecurity.techtarget.com/definithyperlink](http://searchfinancialsecurity.techtarget.com/definition/electronicdiscovery)
"http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery"ion/electronicdiscovery <https://en.wikipedia.org/wiki/Escrow>

NEW QUESTION 274

Customers are receiving emails containing a link to malicious software. These emails are subverting spam filters. The email reads as follows:

Delivered-To: customer@example.com Received: by 10.14.120.205

Mon, 1 Nov 2010 11:15:24 -0700 (PDT)

Received: by 10.231.31.193

Mon, 01 Nov 2010 11:15:23 -0700 (PDT)

Return-Path: <IT@company.com>

Received: from 127.0.0.1 for <customer@example.com>; Mon, 1 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)

Received: by smtpex.example.com (SMTP READY) with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500

Received: from 172.18.45.122 by 192.168.2.55; Mon, 1 Nov 2010 13:15:14 -0500

From: Company <IT@Company.com>

To: "customer@example.com" <customer@example.com> Date: Mon, 1 Nov 2010 13:15:11 -0500

Subject: New Insurance Application Thread-Topic: New Insurance Application

Please download and install software from the site below to maintain full access to your account. www.examplesite.com

Additional information: The authorized mail servers IPs are 192.168.2.10 and 192.168.2.11. The network's subnet is 192.168.2.0/25.

Which of the following are the MOST appropriate courses of action a security administrator could take to eliminate this risk? (Select TWO).

- A. Identify the origination point for malicious activity on the unauthorized mail server.
- B. Block port 25 on the firewall for all unauthorized mail servers.
- C. Disable open relay functionality.
- D. Shut down the SMTP service on the unauthorized mail server.
- E. Enable STARTTLS on the spam filter

Answer: BD

Explanation:

In this question, we have an unauthorized mail server using the IP: 192.168.2.55.

Blocking port 25 on the firewall for all unauthorized mail servers is a common and recommended security step. Port 25 should be open on the firewall to the IP addresses of the authorized email servers only (192.168.2.10 and 192.168.2.11). This will prevent unauthorized email servers sending email or receiving and relaying email.

Email servers use SMTP (Simple Mail Transfer Protocol) to send email to other email servers. Shutting down the SMTP service on the unauthorized mail server is effectively disabling the mail server functionality of the unauthorized server.

Incorrect Answers:

A: You shouldn't worry about identifying the origination point for the malicious activity on the unauthorized mail server. There isn't much you could do about the remote origination point even if you did identify it. You have an 'unauthorized' mail server. That is what you should be dealing with. C: In this question, the email was received by the unauthorized email server (192.168.2.55) ready to be collected by the recipient. The email was not relayed (forwarded) to other email servers. Disabling open relay functionality will not stop the emails. You need to disable all email (SMTP) functionality of the unauthorized server, not just relaying.

E: STARTTLS enables TLS encryption on communications with the spam filter. It will do nothing to prevent the usage of the unauthorized email server.

References: https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol" https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol"ocol

<https://www.arclab.com/en/kb/email/how-to-read-and-analyze-the-email-header-fields-spfdkim.html>

NEW QUESTION 276

It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?

- A. Update the blog page to HTTPS
- B. Filter metacharacters
- C. Install HIDS on the server
- D. Patch the web application
- E. Perform client side input validation

Answer: B

Explanation:

A general rule of thumb with regards to XSS is to "Never trust user input and always filter metacharacters." Incorrect Answers:

A: Updating the blog page to HTTPS will not resolve this issue.

C: HIDS are designed to monitor a computer system, not the network. IT will, therefore, not resolve this issue.

D: Simply installing a web application patch will not work, as the patch may be susceptible to XSS. Testing of the patch has to take place first.

E: Performing client side input validation is a valid method, but it is not the MOST effective. References:

<https://community.qualys.com/docs/DOC-1186>

<http://www.computerweekly.com/tip/The-true-test-of-a-Webapplication-patch>"ekly.com/tip/The-truHYPERLINK

"http://www.computerweekly.com/tip/The-truetest-

of-a-Web-application-patch"e-test-of-a-Web-application-patch

httpHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-cross-sitehttps:// certkingdom.com

scripting"/"://www.techreHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-crosssite- scripting/"pHYPERLINK "http://www.techrepublic.com/blog/it-

security/what-is-cross-sitescripting/" ublic.com/blog/it-security/what-is-cross-site-scripting/

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 137

NEW QUESTION 278

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 exploits. 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.org/reading-room/whitepapers/forensics/ids-fileforensics- 35952](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 281

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 encryption

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 286

A firm's Chief Executive Officer (CEO) is concerned that IT staff lacks the knowledge to identify complex vulnerabilities that may exist in a payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted that code base confidentiality is of critical importance to allow the company to exceed the competition in terms of the product's reliability, stability, and performance. Which of the following would provide the MOST thorough testing and satisfy the CEO's requirements?

- A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.
- B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.
- C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.
- D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

Answer: C

Explanation:

Gray box testing has limited knowledge of the system as an attacker would. The base code would remain confidential. This would further be enhanced by a Non-disclosure agreement (NDA) which is designed to protect confidential information.

Incorrect Answers:

A: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. They do not typically cover vulnerabilities and penetration / vulnerability testing. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.

B: A business partnership security agreement (BPA) is a legally binding document that is designed to provide safeguards and compel certain actions among business partners in relation to specific security-related activities. Black box testing is integrity-based testing that uses random user inputs. Code confidentiality is maintained but testing is limited.

D: White box testing requires full access to the code base as it involves validating the program logic. This does not test against vulnerabilities. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 167-168, 238-239

https://en.wikipedia.org/wiki/Non-disclosure_agreement"sure_agreement https://en.wikipedia.org/wiki/Nondisclosure_agreement"HYPERLINK

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

NEW QUESTION 287

Company policy requires that all company laptops meet the following baseline requirements: Software requirements:

Antivirus

Anti-malware Anti-spyware Log monitoring

Full-disk encryption

Terminal services enabled for RDP Administrative access for local users Hardware restrictions:

Bluetooth disabled FireWire disabled WiFi adapter disabled

Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

- A. Group policy to limit web access
- B. Restrict VPN access for all mobile users
- C. Remove full-disk encryption
- D. Remove administrative access to local users
- E. Restrict/disable TELNET access to network resources
- F. Perform vulnerability scanning on a daily basis
- G. Restrict/disable USB access

Answer: DG

Explanation:

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.

Therefore, one method of preventing such attacks is to remove administrative access for local users. A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer.

We can prevent this from happening by restricting or disabling access to USB devices.

Incorrect Answers:

A: Using a group policy to limit web access is not a practical solution. Users in a company often require Web access so restricting it will affect their ability to do their jobs.

B: Rootkits or Bootkits would not be caught by connecting to the network over a VPN so disabling VPN access will not help.

C: Removing full-disk encryption will not prevent Bootkits.

E: Bootkits are not caught by connecting to network resources using Telnet connection so disabling Telnet access to resources will not help.

F: Performing vulnerability scanning on a daily basis might help you to quickly detect Bootkits. However, vulnerability scanning does nothing to actually prevent the Bootkits.

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

NEW QUESTION 292

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CAS-003 Exam with Our Prep Materials Via below:

<https://www.certleader.com/CAS-003-dumps.html>