



# CompTIA

## Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

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 2

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

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

**Answer: B**

#### NEW QUESTION 3

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 4

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

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

**Answer: D**

#### NEW QUESTION 5

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

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

**Answer: B**

#### NEW QUESTION 6

A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:  
TCP 80 open  
TCP 443 open

TCP 1434 filtered

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

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

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

Which of the following tools did the penetration tester use?

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

**Answer: C**

#### NEW QUESTION 7

A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase

the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle.

Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

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

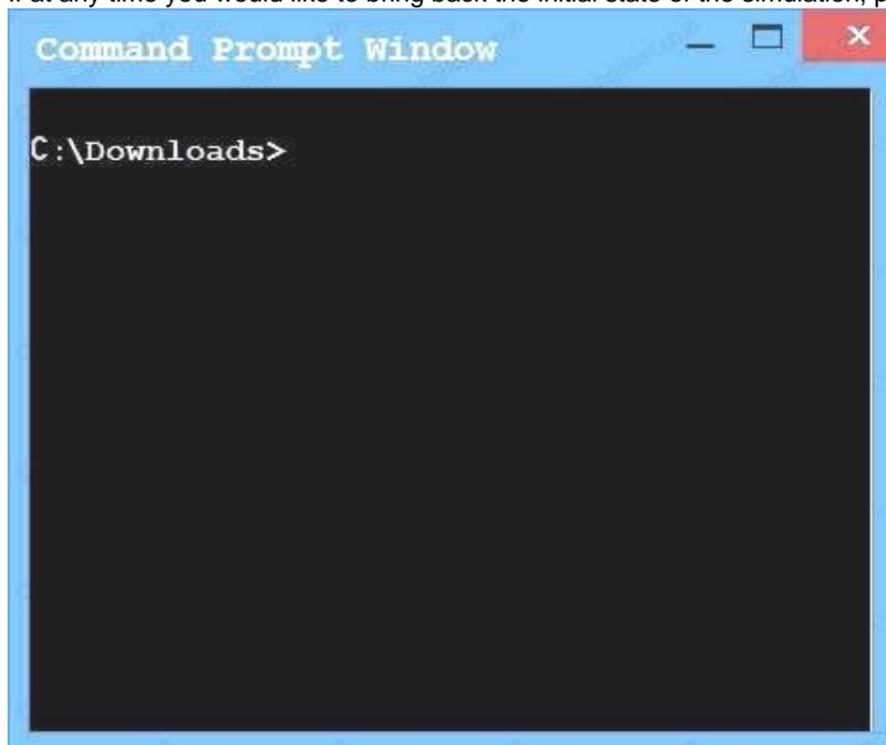
**Answer: AD**

#### NEW QUESTION 8

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

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

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



Download - Test x  
www.download-test.com/files  
**Download Center**

Home > Download Center > Application Patch

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

File Name	Mirror	Download Files Below
<a href="#">install.exe</a>	<a href="#">Mirror1</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 2</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 3</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 4</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 5</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 6</a>	<a href="#">Download</a>

**HASH:** 1759adb5g34700aae19bc4578fc19cc2

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate date is valid.
- The name of the security certificate does not match the name of the site.

Do you want to proceed?

58% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (2.86 MB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

Transfer rate: 1.25 MB/Sec

59% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (2.91 MB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

Transfer rate: 1.25 MB/Sec

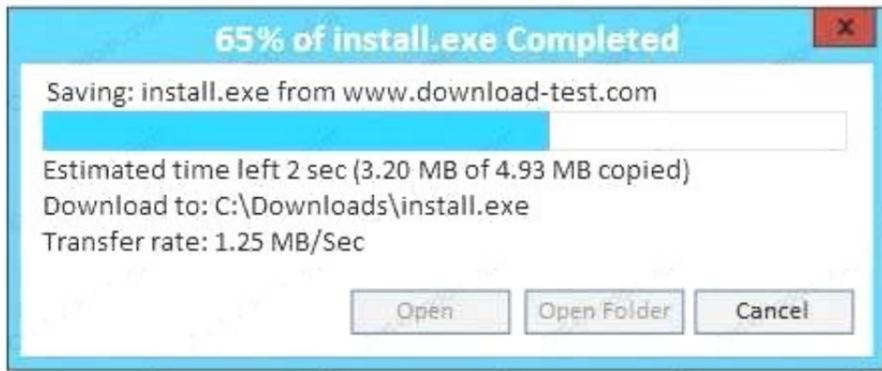
61% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (3.01 MB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

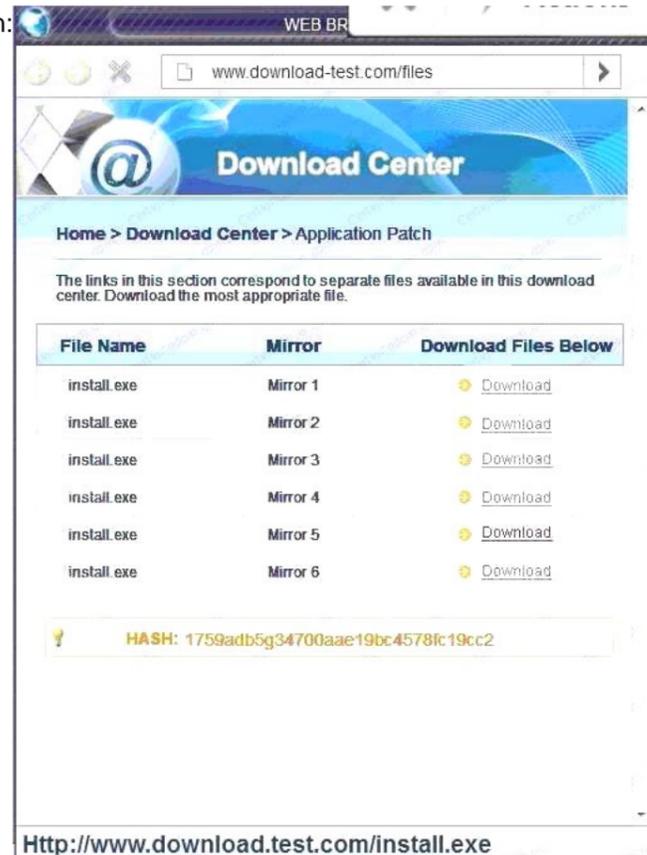
Transfer rate: 1.25 MB/Sec



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

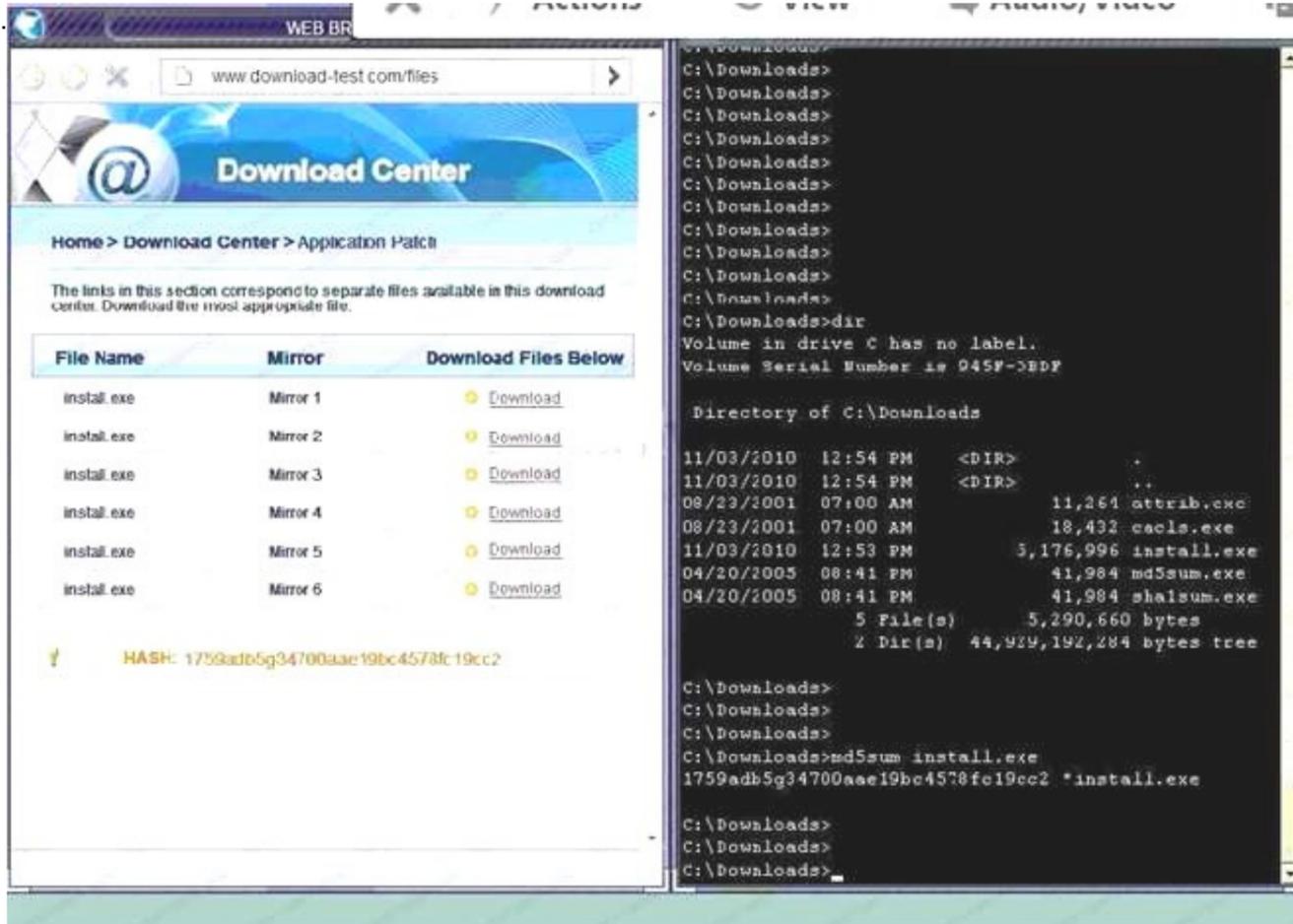


Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:



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

B. Make sure that the hash matches.



Finally,

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

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



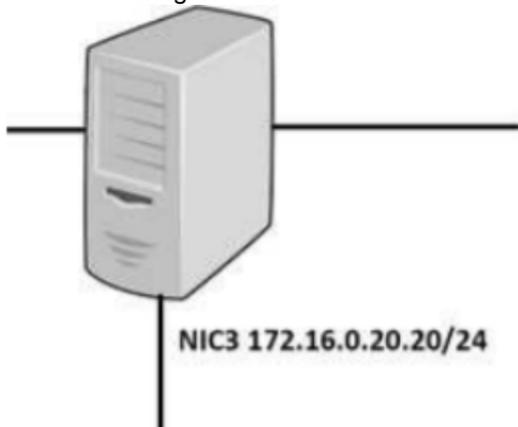
Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown. Since we need to do this in the most secure manner possible, they should not be used. Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as show D.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

**Answer:** A

**NEW QUESTION 9**

DRAG DROP

A security administrator must configure the database server shown below to 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	<input type="text"/>
The web server in the 10.10.10.0/25 network should connect to the DB via NIC1	<input type="text"/>
The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network	<input type="text"/>
The DB server should not initiate outbound connections on NIC2	<input type="text"/>

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

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

The DB server should not initiate outbound connections on NIC2

Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389

Permit UDP from 192.168.1.20 to 172.30.10.3

Permit IP from 172.30.10.3 to 192.168.1.20

Deny IP from 10.0.10.20 to ANY

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

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

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

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

- A. The public/private views on the Comptia.org DNS servers are misconfigured
- B. Comptia.org is running an older mail server, which may be vulnerable to exploits
- C. The DNS SPF records have not been updated for Comptia.org
- D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

**Answer: B**

#### NEW QUESTION 10

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

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

**Answer: D**

#### NEW QUESTION 15

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

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

Answer: F

#### NEW QUESTION 18

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

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

Answer: C

#### NEW QUESTION 21

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

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

Answer: EF

#### NEW QUESTION 23

A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

- A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
- B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
- C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
- D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Answer: A

#### NEW QUESTION 26

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

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

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

- A. SQLi

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

**Answer:** B

#### NEW QUESTION 28

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

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

**Answer:** AC

#### NEW QUESTION 29

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 33

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

- A. Blue teaming
- B. Phishing simulations
- C. Lunch-and-learn
- D. Random audits
- E. Continuous monitoring
- F. Separation of duties

**Answer:** BE

#### NEW QUESTION 38

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

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

**Answer:** AD

#### NEW QUESTION 43

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 48

A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However,

the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?

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

**Answer: D**

#### NEW QUESTION 49

A company is acquiring incident response and forensic assistance from a managed security service provider in the event of a data breach. The company has selected a partner and must now provide required documents to be reviewed and evaluated. Which of the following documents would BEST protect the company and ensure timely assistance? (Choose two.)

- A. RA
- B. BIA
- C. NDA
- D. RFI
- E. RFQ
- F. MSA

**Answer: CF**

#### NEW QUESTION 50

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

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

**Answer: A**

#### NEW QUESTION 51

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

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

**Answer: C**

#### NEW QUESTION 55

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

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

**Answer: A**

#### NEW QUESTION 59

A deployment manager is working with a software development group to assess the security of a new version of the organization's internally developed ERP tool. The organization prefers to not perform assessment activities following deployment, instead focusing on assessing security throughout the life cycle. Which of the following methods would BEST assess the security of the product?

- A. Static code analysis in the IDE environment
- B. Penetration testing of the UAT environment
- C. Vulnerability scanning of the production environment
- D. Penetration testing of the production environment
- E. Peer review prior to unit testing

**Answer: C**

#### NEW QUESTION 60

During a security event investigation, a junior analyst fails to create an image of a server's hard drive before removing the drive and sending it to the forensics

analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

- A. Continuity of operations
- B. Chain of custody
- C. Order of volatility
- D. Data recovery

**Answer: C**

**NEW QUESTION 61**

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

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

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

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

**Answer: D**

**NEW QUESTION 66**

A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

- A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
- B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
- C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
- D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
- E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
- F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

**Answer: CD**

**NEW QUESTION 67**

Exhibit:

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

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

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

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

MS-SQL server: 10.1.4.70

MGMT platform: 10.1.10.250

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

Task 2) The firewall must be configured so that the SQL server can only receive requests from the web server.  
 Task 3) The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.  
 Task 4) Ensure the final rule is an explicit deny.  
 Task 5) Currently the user zone can access internet websites over an unencrypted protocol. Modify a rule so that user access to websites is over secure protocols only.  
 Instructions: To perform the necessary tasks, please modify the DST port, SRC zone, Protocol, Action, and/or Rule Order columns. Type ANY to include all ports. Firewall ACLs are read from the top down.  
 Once you have met the simulation requirements, click Save. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

- A. Task 1: A rule was added to prevent the management platform from accessing the interne
- B. This rule is not workin
- C. Identify the rule and correct this issue.In Rule n
- D. 1 edit the Action to Deny to block internet access from the management platform.SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n
- E. 6 from top, edit the Action to be Permi
- F. SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n
- G. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi
- H. SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST ANY ANY WEBAPP 10.1.5.50 ANY TCP PERMITTask 4: Ensure the final rule is an explicit denyEnter this at the bottom of the access list i.
- I. the line at the bottom of the rule: SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action ANY ANY ANY ANY ANY ANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco
- J. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action USER 10.1.1.0/24 10.1.2.0/24 ANY UNTRUST ANY 443 TCP PERMIT
- K. Task 1: A rule was added to prevent the management platform from accessing the interne
- L. This rule is not workin
- M. Identify the rule and correct this issue.In Rule n
- N. 1 edit the Action to Deny to block internet access from the management platfor
- O. SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n
- P. 6 from top, edit the Action to be Permi
- Q. SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n
- R. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi
- S. SRC Zone ANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco
- T. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action USER 10.1.1.0/24 10.1.2.0/24 ANY UNTRUST ANY 443 TCP PERMIT

**Answer:** A

**NEW QUESTION 71**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 73**

An organization has established the following controls matrix:

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

The following control sets have been defined by the organization and are applied in aggregate fashion:  
 Systems containing PII are protected with the minimum control set. Systems containing medical data are protected at the moderate level. Systems containing cardholder data are protected at the high level.  
 The organization is preparing to deploy a system that protects the confidentiality of a database containing PII and medical data from clients. Based on the controls

classification, which of the following controls would BEST meet these requirements?

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

**Answer: D**

#### NEW QUESTION 76

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

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

**Answer: B**

#### NEW QUESTION 78

A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix. Which of the following MOST likely need to be configured to ensure the system are mitigated accordingly? (Select two.)

- A. Antivirus
- B. HIPS
- C. Application whitelisting
- D. Patch management
- E. Group policy implementation
- F. Firmware updates

**Answer: DF**

#### NEW QUESTION 81

A Chief Information Security Officer (CISO) is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides. Which of the following would be the BEST source of reference during the revision process?

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

**Answer: A**

#### NEW QUESTION 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 86

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

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

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

**Answer: B**

#### NEW QUESTION 91

A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators. Which of the following is MOST likely to produce the needed information?

- A. Whois
- B. DNS enumeration
- C. Vulnerability scanner
- D. Fingerprinting

**Answer: A**

#### NEW QUESTION 93

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 96

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

User IP space: 192.168.1.0/24

Server IP space: 192.168.192.0/25

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

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

**Answer: B**

#### NEW QUESTION 101

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 103

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

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

**Answer: D**

#### NEW QUESTION 106

Given the following code snippet:

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

Which of the following failure modes would the code exhibit?

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

**Answer: D**

#### NEW QUESTION 110

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

Data must be encrypted at rest.

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

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

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

**Answer: CD**

#### NEW QUESTION 115

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

Involve business owners and stakeholders Create an applicable scenario

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

Which of the following exercises has the CEO requested?

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

**Answer: C**

#### NEW QUESTION 119

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

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

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

**Answer: D**

#### NEW QUESTION 123

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

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

**Answer:** A

**NEW QUESTION 128**

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 131**

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 136**

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 138**

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

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

**Answer:** A

**NEW QUESTION 141**

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

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

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

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

**Answer:** C

**NEW QUESTION 146**

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:



- D. Social engineering
- E. Malware sandboxing
- F. Tabletop exercise

**Answer:** AC

#### NEW QUESTION 157

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

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

**Answer:** B

#### NEW QUESTION 161

There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis. Which of 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 162

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

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

First time detected 10 nov 2015 09:00 GMT\_0600

Last time detected 10 nov 2015 09:00 GMT\_0600

CVSS base: 5

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

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

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

- A. Response: C:\Documents\marysmith\maillinglist.pdf
- B. Finding#5144322
- C. First Time detected 10 nov 2015 09:00 GMT\_0600
- D. Access path: <http://myorg.com/maillinglist.htm>
- E. Request: GET <http://myorg.com/maillinglist.aspx?content=volunteer>

**Answer:** A

#### NEW QUESTION 164

A technician receives the following security alert from the firewall's automated system: Match\_Time: 10/10/16 16:20:43

Serial: 002301028176

Device\_name: COMPSEC1 Type: CORRELATION

Srcuser: domain\samjones Src: 10.50.50.150

Object\_name: beacon detection Object\_id: 6005

Category: compromised-host Severity: medium

Evidence: host repeatedly visited a dynamic DNS domain (17 time) After reviewing the alert, which of the following is the BEST analysis?

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

**Answer:** B

#### NEW QUESTION 169

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 173

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

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

**Answer: B**

**Explanation:**

The most common open source operating system is LINUX.

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

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

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

be caused by malicious or flawed applications. Incorrect Answers:

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

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

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

References:

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

**NEW QUESTION 178**

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

- A. vTPM
- B. HSM
- C. TPM
- D. INE

**Answer: A**

**Explanation:**

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

A vTPM is a virtual Trusted Platform Module.

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

Incorrect Answers:

B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. This solution would require hardware pass-through.

C: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. Virtual machines cannot access a hardware TPM.

D: INE (intelligent network element) is not used for storing cryptographic keys. References:

[https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module) <http://HYPERLINK>

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

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

**NEW QUESTION 180**

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

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

**Answer: A**

**Explanation:**

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

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

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

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

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

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

#### NEW QUESTION 181

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

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

**Answer:** A

#### Explanation:

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

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

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

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

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

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

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

C: 6to4 relays work in a similar way to Teredo. However, the addresses used by 6to4 relays start with 2002:: whereas Teredo addresses start with 2001. Therefore, a 6to4 relay is not being used in this question so this answer is incorrect.

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

References: [https://en.wikipedia.org/wiki/Teredo\\_tunneling](https://en.wikipedia.org/wiki/Teredo_tunneling)

"[https://en.wikipedia.org/wiki/Teredo\\_tunneling](https://en.wikipedia.org/wiki/Teredo_tunneling)"org/wiki/Teredo\_tunHYPERLINK "[https://en.wikipedia.org/wiki/Teredo\\_tunneling](https://en.wikipedia.org/wiki/Teredo_tunneling)"neling

#### NEW QUESTION 183

select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson  
Which of the following types of attacks is the user attempting?

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

**Answer:** D

#### Explanation:

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

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: The code in the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.

B: Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.

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

References: [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

#### NEW QUESTION 186

A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

- A. Insecure direct object references, CSRF, Smurf
- B. Privilege escalation, Application DoS, Buffer overflow
- C. SQL injection, Resource exhaustion, Privilege escalation
- D. CSRF, Fault injection, Memory leaks

**Answer:** A

#### Explanation:

Insecure direct object references are used to access data

A. CSRF attacks the functions of a web site which could access data

A. A Smurf attack is used to take down a system.

A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which will allow attackers to manipulate these references to access unauthorized data.

Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious Web site, email, blog, instant message, or program causes a user's Web browser to perform an unwanted action on a trusted site for which the user is currently authenticated. The impact of a successful cross-site request forgery attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing

an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function (funds Transfer, form submission etc.) via the target's browser without knowledge of the target user, at least until the unauthorized function has been committed.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

Incorrect Answers:

B: Application DoS is an attack designed to affect the availability of an application. Buffer overflow is used to obtain information. Therefore, the order of importance in this answer is incorrect.

C: Resource exhaustion is an attack designed to affect the availability of a system. Privilege escalation is used to obtain information. Therefore, the order of importance in this answer is incorrect.

D: The options in the other answers (Insecure direct object references, privilege escalation, SQL injection) are more of a threat to data confidentiality than the options in this answer. References:

[http://www.tutorialspoint.com/security\\_testing/insecure\\_direct\\_object\\_reference.htm](http://www.tutorialspoint.com/security_testing/insecure_direct_object_reference.htm) [https://www.owasp.org/index.php/Cross-Site\\_Request\\_Forgery\\_\(CSRF\)\\_Prevention\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet) <http://www.webopedia.com/TERM/S/smurf.html>

### NEW QUESTION 189

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

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

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

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

**Answer: C**

#### Explanation:

The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: The code in this question does not contain non-printable characters.

B: The code in this question is not an example of cross site scripting (XSS).

D: The code in this question is an example of a SQL injection attack. It is not simply someone attempting to log on as administrator.

References: [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

### NEW QUESTION 192

Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

- A. Deduplication
- B. Data snapshots
- C. LUN masking
- D. Storage multipaths

**Answer: C**

#### Explanation:

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Incorrect Answers:

A: Deduplication is the process of eliminating multiple copies of the same data to save storage space. It does not prevent an unauthorized HBA from viewing iSCSI target information.

B: Data snapshots are point in time copies of data often used by data backup applications. They do not prevent an unauthorized HBA from viewing iSCSI target information.

D: Storage multipaths are when you have multiple connections to a storage device. This provides path redundancy in the event of a path failure and can also (in active/active configurations) provide extra capacity by aggregating the bandwidth of the multiple storage paths. However, they do not prevent an unauthorized HBA from viewing iSCSI target information.

References:

<http://searchvirtualstorage.techtarget.com/definition/LUNmasking>

### NEW QUESTION 196

Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

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

**Answer: B**

**Explanation:**

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

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

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

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

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

References:

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

**NEW QUESTION 201**

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

- A. Synchronous copy of data
- B. RAID configuration
- C. Data de-duplication
- D. Storage pool space allocation
- E. Port scanning
- F. LUN masking/mapping
- G. Port mapping

**Answer: FG**

**Explanation:**

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Port mapping is used in 'Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

Incorrect Answers:

A: Synchronous copy of data is used to copy data. It is not a technical control for securing a SAN storage infrastructure.

B: RAID configuration is the configuration of the disks in the SAN. A RAID is an array of disks that provides a logical pool of storage by combining the storage capacity of the disks. RAID provides hardware redundancy in that the data will not be lost if an individual disk fails. RAID configuration is not a technical control for securing a SAN storage infrastructure.

C: Data de-duplication is the process of eliminating multiple copies of the same data to save storage space. It is not a technical control for securing a SAN storage infrastructure.

D: Storage pool space allocation is the process of allocating and making available portions of the storage pool to servers. It is not a technical control for securing a SAN storage infrastructure.

E: Port scanning is the process of probing a server or host for open ports. It is not a technical control for securing a SAN storage infrastructure.

References: <http://searchvirtualstorage.techtarget.com/definition/LUN-masking> [https://en.wikipedia.org/wiki/Fibre\\_Channel\\_zoning](https://en.wikipedia.org/wiki/Fibre_Channel_zoning)

**NEW QUESTION 205**

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 210

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

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

**Answer:** EF

#### Explanation:

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce. AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.

Incorrect Answers:

- A: AES in Electronic Codebook mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.  
B: RC4 in Cipher Block Chaining mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 (not in Cipher Block Chaining mode) or AES in Counter Mode.  
C: You cannot use fixed IV generation for RC4 when encrypting streaming video.  
D: AES with cipher text padding cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.

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

#### NEW QUESTION 214

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 218

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

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

**Answer:** A

**Explanation:**

References:

[http://HYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms"sHYPERLINK](http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms)

["http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-](http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms)

[algorithms"tackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-](http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-)

[and-encryption-aHYPERLINK "http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms"lgorithms](http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms)

**NEW QUESTION 223**

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

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

**Answer:** C

**Explanation:**

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

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

Incorrect Answers:

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

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

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

References: <http://searchsecurity.techtarget.com/definitio>

["http://searchsecurity.techtarget.com/definition/physical-security"inition/physical-security](http://searchsecurity.techtarget.com/definition/physical-security)

**NEW QUESTION 228**

Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:

User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down

Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

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

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

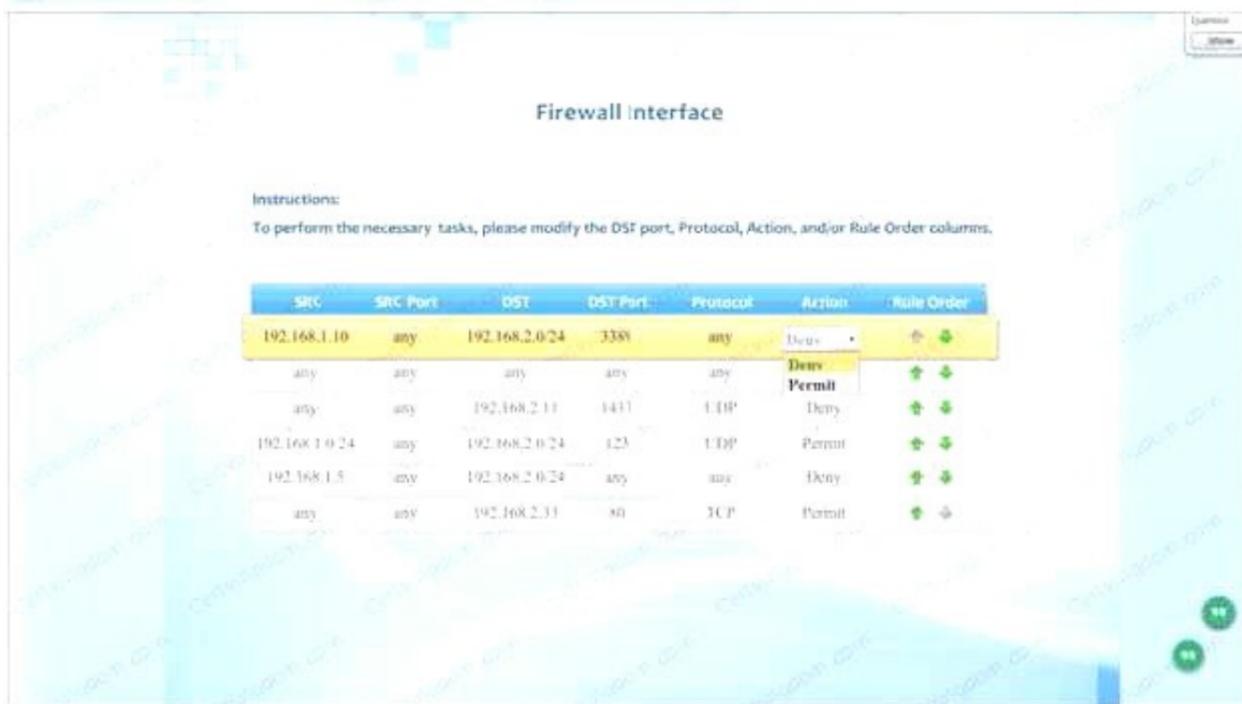
Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

### Firewall Interface

Instructions:

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

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



A. Check the answer below

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

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

B. This rule is not workin

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

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

E. This needs to be set to Permit.

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

Task 2)

All web servers have been changed to communicate solely over SS

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

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

any	any	192.168.2.33	80	TCP	Permit	↑ ↓
-----	-----	--------------	----	-----	--------	-----

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

H. This rule is not workin

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

J. It is not working because the protocol is wron

K. It should be TCP, not UDP.

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

Task 4) Other than allowing all

hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.The network time rule is shown in the image below. However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul

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

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

M. Check the answer below

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

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

N. This rule is not workin

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

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

Q. This needs to be set to Permit.

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

Task 2)

All web servers have been changed to communicate solely over SS

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

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

T. This rule is not workin

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

. It is not working because the protocol is wron

. It should be TCP, not UDP.

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

Task 4)

Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed.The network time rule is shown in the image below.However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul

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

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

**Answer:** A

### NEW QUESTION 230

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 235

The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business \$2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

- A. The company should mitigate the risk.
- B. The company should transfer the risk.
- C. The company should avoid the risk.
- D. The company should accept the risk.

**Answer:** B

**Explanation:**

To transfer the risk is to deflect it to a third party, by taking out insurance for example. Incorrect Answers:

A: Mitigation is not an option as the CIO's budget does not allow for the purchase of additional compensating controls.

C: Avoiding the risk is not an option as the business unit depends on the critical business function. D: Accepting the risk would not reduce financial loss.

References:

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

**NEW QUESTION 236**

An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

- A. Ensure the SaaS provider supports dual factor authentication.
- B. Ensure the SaaS provider supports encrypted password transmission and storage.
- C. Ensure the SaaS provider supports secure hash file exchange.
- D. Ensure the SaaS provider supports role-based access control.
- E. Ensure the SaaS provider supports directory services federation.

**Answer:** E

**Explanation:**

A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network. Single sign-on will mitigate the risk of managing separate user credentials. Incorrect Answers:

A: Dual factor authentication will provide identification of users via a combination of two different components. It will not, however, mitigate the risk of managing separate user credentials.

B: The transmission and storage of encrypted passwords will not mitigate the risk of managing separate user credentials.

C: A hash file is a file that has been converted into a numerical string by a mathematical algorithm, and has to be unencrypted with a hash key to be understood. It will not, however, mitigate the risk of managing separate user credentials.

D: Role-based access control (RBAC) refers to the restriction of system access to authorized users. It will not, however, mitigate the risk of managing separate user credentials.

References:

<https://msdn.microsoft.com/en-us/library/aa905332.aspx> [https://en.wikipedia.org/wiki/Two-factor\\_authentication](https://en.wikipedia.org/wiki/Two-factor_authentication) <https://en.wikipedia.org/wiki/Encryption>

<http://www.wisegeek.com/what-are-hash-files.htm> [https://en.wikipedia.org/wiki/Role-based\\_access\\_control](https://en.wikipedia.org/wiki/Role-based_access_control)

**NEW QUESTION 238**

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

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

**Answer:** B

**Explanation:**

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

Incorrect Answers:

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

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

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

References:

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

**NEW QUESTION 241**

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

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

**Answer:** B

**Explanation:**

The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.

Incorrect Answers:

A: A memorandum of agreement (MOA) is a document composed between parties to cooperate on an agreed upon project or meet an agreed objective.

C: A nondisclosure agreement (NDA) is designed to protect confidential information.

D: An operating level agreement (OLA) defines the responsibilities of each partner's internal support group.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 238

#### NEW QUESTION 245

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

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

**Answer: B**

#### Explanation:

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

Incorrect Answers:

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

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

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

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

"<http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-orpagefile>"

#### NEW QUESTION 249

An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

- A. Independent verification and validation
- B. Security test and evaluation
- C. Risk assessment
- D. Ongoing authorization

**Answer: D**

#### Explanation:

Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.

Incorrect Answers:

A: Independent verification and validation (IV&V) is executed by a third party organization not involved in the development of a product. This is not considered continuous monitoring of authorized information systems.

B: Security test and evaluation is not considered continuous monitoring of authorized information systems.

C: Risk assessment is the identification of potential risks and threats. It is not considered continuous monitoring of authorized information systems.

References:

<http://www.fedramp.net/ongoing> ["http://www.fedramp.net/ongoing-assessment-andauthorization-continuous-monitoring"](http://www.fedramp.net/ongoing-assessment-andauthorization-continuous-monitoring) [ing-assessment-and](http://www.fedramp.net/ongoing-assessment-andauthorization-continuous-monitoring) [authorization-continuous-monitoring](http://www.fedramp.net/ongoing-assessment-andauthorization-continuous-monitoring)

"<http://www.fedramp.net/ongoing-assessment-andauthorization-continuous-monitoring>"

<https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v>

[i](https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v) [v](https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v)

"<https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v>"

[and-validation--iv&v](https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v) [v](https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v)

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 213, 219

#### NEW QUESTION 253

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

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

**Answer: C**

#### Explanation:

The question states that "the organization has not addressed telecommuting in the past". It is therefore unlikely that a company policy exists for telecommuting workers.

There are many types of company policies including Working time, Equality and diversity, Change management, Employment policies, Security policies and Data Protection policies.

In this question, a new method of working has been employed: remote working or telecommuting. Policies should be created to establish company security requirements (and any other requirements) for users working remotely.

Incorrect Answers:

A: The data should already be secure on the corporate systems. If an information classification scheme is used as part of the security, it should already have been created. Remote working does not add the requirement for an information classification scheme.

B: The personnel work from remote locations with corporate assets; their personal computers are not used. Therefore, we do not require database views and

constrained interfaces so remote users will be unable to access PII from personal equipment.

D: You should identify and document the proper procedures for telecommuting. However, the security requirements for working remotely with company equipment should be addressed first. Furthermore, you would not necessarily work with mid-level managers to identify and document the proper procedures for telecommuting if the company has a technology steering committee.

#### NEW QUESTION 255

After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

- A. The binary files used by the application have been modified by malware.
- B. The application is unable to perform remote attestation due to blocked ports.
- C. The restored image backup was encrypted with the wrong key.
- D. The hash key summary of hardware and installed software no longer matches.

**Answer:** D

#### Explanation:

Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation. Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

Incorrect Answers:

A: It is very unlikely that the binary files used by the application have been modified by malware. Malware doesn't modify application binary files.

B: A backup image of the system was restored onto the new hardware. Therefore, the software configuration should be the same as before. It is unlikely that blocked ports preventing remote attestation is the cause of the problem.

C: A backup image of the system was restored onto the new hardware. If the restored image backup was encrypted with the wrong key, you wouldn't be able to restore the image.

References:

<https://technet.microsoft.com/en-us/library/bb457054.aspx>

#### NEW QUESTION 256

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

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

**Answer:** A

#### Explanation:

Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day exploits. Having knowledge of each host's communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zeroday and APT (advance persistent threat) malware and agents. Data intelligence allows forensic analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network. Incorrect Answers:

B: The attack has already happened; the server has already been compromised. Configuring the server logs to collect unusual activity including failed logins and restarted services might help against future attacks but it will not provide information on an attack that has already happened.

C: It is unlikely the DLP logs would contain anomalous communications from the server that would identify where the server collected the information.

D: The attack has already happened; the server has already been compromised. Setting up a packet capture on the firewall to collect all of the server communications might help against future attacks but it will not provide information on an attack that has already happened.

References:

<https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics-35952>

"<https://www.sans.org/reading-room/whitepapers/forensics/ids-file-forensics-35952>", p. 6

#### NEW QUESTION 261

Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

- A. Install a HIPS on the SIP servers
- B. Configure 802.1X on the network
- C. Update the corporate firewall to block attacking addresses
- D. Configure 802.11e on the network
- E. Configure 802.1q on the network

**Answer:** AD

#### Explanation:

Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host.

IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.  
Incorrect Answers:

B: 802.1X is used by devices to attach to a LAN or WLAN.

C: Updating the corporate firewall will not work as the DoS attacks are from an internal source. E: 802.1q is used for VLAN tagging.

References: [https://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](https://en.wikipedia.org/wiki/Intrusion_prevention_system)

[https://en.wikipedia.org/wiki/IEEE\\_802.11e-2005](https://en.wikipedia.org/wiki/IEEE_802.11e-2005)

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

#### NEW QUESTION 262

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

A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.

B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.

C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.

D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

**Answer: C**

#### Explanation:

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

Incorrect Answers:

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

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

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

References:

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

[https://en.wikipedia.org/wiki/Non-disclosure\\_agreement](https://en.wikipedia.org/wiki/Non-disclosure_agreement)

[https://en.wikipedia.org/wiki/Gray\\_box\\_testing](https://en.wikipedia.org/wiki/Gray_box_testing)

[https://en.wikipedia.org/wiki/Gray\\_box\\_testing](https://en.wikipedia.org/wiki/Gray_box_testing)

#### NEW QUESTION 265

A company provides on-demand cloud computing resources for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for customer access to the administrative website. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data from customer A was found on a hidden directory within the VM of company B. Company B is not in the same industry as company A and the two are not competitors. Which of the following has MOST likely occurred?

A. Both VMs were left unsecured and an attacker was able to exploit network vulnerabilities to access each and move the data.

B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.

C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.

D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.

**Answer: A**

#### Explanation:

In this question, two virtual machines have been accessed by an attacker. The question is asking what is MOST likely to have occurred.

It is common for operating systems to not be fully patched. Of the options given, the most likely occurrence is that the two VMs were not fully patched allowing an attacker to access each of them. The attacker could then copy data from one VM and hide it in a hidden folder on the other VM. Incorrect Answers:

B: The two VMs are from different companies. Therefore, the two VMs would use different twofactor tokens; one for each company. For this answer to be correct, the attacker would have to steal

both two-factor tokens. This is not the most likely answer.

C: Resource exhaustion is a simple denial of service condition which occurs when the resources necessary to perform an action are entirely consumed, therefore preventing that action from taking place. A resource exhaustion attack is not used to gain unauthorized access to a system.

D: The two VMs are from different companies so it can't be an employee from the two companies. It is possible (although unlikely) than an employee from the hosting company had administrative access to both VMs. Even if that were the case, the employee would not dump the memory to a mapped disk to copy the information. With administrative access, the employee could copy the data using much simpler methods.

References: [https://www.owasp.org/index.php/Resource\\_exhaustion](https://www.owasp.org/index.php/Resource_exhaustion)

#### NEW QUESTION 267

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

Antivirus

Anti-malware Anti-spyware Log monitoring

Full-disk encryption

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

Bluetooth disabled FireWire disabled WiFi adapter disabled

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

A. Group policy to limit web access

B. Restrict VPN access for all mobile users

- C. Remove full-disk encryption
- D. Remove administrative access to local users
- E. Restrict/disable TELNET access to network resources
- F. Perform vulnerability scanning on a daily basis
- G. Restrict/disable USB access

**Answer:** DG

**Explanation:**

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

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

Incorrect Answers:

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

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

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

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

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

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

**NEW QUESTION 272**

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

- A. Background checks
- B. Job rotation
- C. Least privilege
- D. Employee termination procedures

**Answer:** B

**Explanation:**

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

Incorrect Answers:

A: To verify that a potential employee has a clean background and that any negative history is exposed prior to employment, a background check is used.

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

D: The employee termination procedures will not identify the employees involved in these activities and reduce the risk of this activity occurring in the future.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 243, 245, 246

**NEW QUESTION 276**

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

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

**Answer:** D

**Explanation:**

The scene has to be secured first to prevent contamination. Once a forensic copy has been created, an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.

Incorrect Answers:

A: To prevent contamination, the scene should be secured first. B: The scene should be secured before taking inventory.

C: Implementing a chain of custody can only occur once evidence has been accessed. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254

**NEW QUESTION 279**

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

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

**Answer:** C

**Explanation:**

Integer overflow errors can occur when a program fails to account for the fact that an arithmetic operation can result in a quantity either greater than a data type's maximum value or less than its minimum value.

Incorrect Answers:

A: Race conditions are a form of attack that normally targets timing, and sometimes called asynchronous attacks. The objective is to exploit the delay between the time of check (TOC) and the time of use (TOU).

B: Click-jacking is when attackers deceive Web users into disclosing confidential information or taking control of their computer while clicking on seemingly harmless web pages.

D: Use after free errors happen when a program carries on making use of a pointer after it has been freed.

E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.

References: <https://www.owasp.org/index.php/IntegerHYPERLINK>

"[https://www.owasp.org/index.php/Integer\\_overflow](https://www.owasp.org/index.php/Integer_overflow)"\_overfHYPERLINK "[https://www.owasp.org/index.php/Integer\\_overflow](https://www.owasp.org/index.php/Integer_overflow)"low

[https://www.owasp.org/index.php/Using\\_freed\\_memory](https://www.owasp.org/index.php/Using_freed_memory)

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 151, 153, 163

**NEW QUESTION 283**

.....

## Relate Links

**100% Pass Your CAS-003 Exam with ExamBible Prep Materials**

<https://www.exambible.com/CAS-003-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>