Vendor: CompTIA

Exam Code: CS0-002

Exam Name: CompTIA CSA+ Certification Exam

Version: DEMO

QUESTION 1
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
Jun 25 10:40:34 localhost pkexec[19962]: comptia: Executing command [USEReroot] [TTY=unknown] [CWD=/home/comptia] [CONMAND=/usr/libexec/gsd-backlight-helper --set-
brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; CONMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?

A. The comptia user knows the sudo password.
B. The comptia user executed the sudo su command.
C. The comptia user knows the root password.
D. The comptia user added himself or herself to the /etc/sudoers file.

Answer: C
Explanation:
The user is not in the sudoers file, you use your own password for that. the user used the su command to switch user accounts, when no user is specified, the su command defaults to the root account. the user is now logged into the root account, you need to know the root password to log into the root account.

QUESTION 2
A security analyst is revising a company's MFA policy to prohibit the use of short message service (SMS) tokens. The Chief Information Officer has questioned this decision and asked for justification. Which of the following should the analyst provide as justification for the new policy?

A. SMS relies on untrusted, third-party carrier networks.
B. SMS tokens are limited to eight numerical characters.
C. SMS is not supported on all handheld devices in use.
D. SMS is a cleartext protocol and does not support encryption.

Answer: D
Explanation:
Short Message Service (SMS) is a text messaging service component of most telephone, World Wide Web, and mobile telephony systems. Multimedia Messaging Service (MMS) handles messages that include graphics or videos. Both technologies present security challenges. Because messages are sent in clear text, both are susceptible to spoofing and spamming.

QUESTION 3
A product security analyst has been assigned to evaluate and validate a new product's security capabilities. Part of the evaluation involves reviewing design changes at specific intervals for security deficiencies, recommending changes, and checking for changes at the next checkpoint. Which of the following BEST describes the activity being conducted?

A. User acceptance testing
B. Stress testing
C. Code review
D. Security regression testing

Answer: D
Explanation:
Security Regression Testing Regression testing focuses on testing to ensure that changes that have been made do not create new issues. From a security perspective, this often comes into play when patches are installed or when new updates are applied to a system or application. Security regression testing is performed to ensure that no new vulnerabilities, misconfigurations, or other issues have been introduced.

QUESTION 4
Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from nonauthorized access.
B. Build the chain-of-custody document, noting the media model, serial number, size, vendor, date, and time of acquisition.
C. Perform a disk sanitization using the command #dd if=/dev/zero of=/dev/sdc bs=1M over the media that will receive a copy of the collected data.
D. Execute the command #dd if-/dev/sda of=/dev/sdc bs=512 to clone the evidence data to external media to prevent any further change.

Answer: B
Explanation:
Chain of custody should be done before taking a copy of data, because this defines what tools were used to obtain the data/who handled the copying. This is a crucial step for submitting data to court because this can help (along with hashing obv) prove the integrity of data.

QUESTION 5
An analyst is responding to an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the field. Malware was loaded on the device via the installation of a third-party software package. The analyst has baselined the device. Which of the following should the analyst do to BEST mitigate future attacks?

A. Implement MDM
B. Update the maiware catalog
C. Patch the mobile device's OS
D. Block third-party applications

Answer: A
Explanation:
MDM solution to manage the configuration of those devices, automatically installing patches, requiring the use of encryption, and providing remote wiping functionality. MDM solutions may also restrict the applications that can be run on a mobile device to those that appear on an approved list.

QUESTION 6
Which of the following is an advantage of SOAR over SIEM?

A. SOAR is much less expensive.
B. SOAR reduces the amount of human intervention required.

C. SOAR can aggregate data from many sources.
D. SOAR uses more robust encryption protocols.

Answer: B
Explanation:
When comparing SOAR vs. SIEM, SIEM will only provide the alert. After that, it's up to the administrator to determine the path of an investigation (so, this means in my opinion more human intervation). A SOAR that automates investigation path workflows can significantly cut down on the amount of time required to handle alerts.

QUESTION 7
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. CASB
B. VPC
C. Federation
D. VPN

Answer: D
Explanation:
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.

QUESTION 8
A Chief Executive Officer (CEO) is concerned the company will be exposed lo data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

Answer: D
Explanation:
Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner.

QUESTION 9
After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

A. Make a backup of the server and update the JBoss server that is running on it.
B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

Answer: C
Explanation:
The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy.

QUESTION 10
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

A. SCADA
B. CAN bus
C. Modbus
D. IoT

Answer: B
Explanation:
The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.

QUESTION 11
A cybersecurity analyst needs to harden a server that is currently being used as a web server. The server needs to be accessible when entering www.company.com into the browser. Additionally, web pages require frequent updates, which are performed by a remote contractor. Given the following output:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT       STATE    SERVICE
22/tcp     open     ssh
23/tcp     open     telnet
53/tcp     open     domain
80/tcp     open     http
443/tcp    open     https
```

Which of the following should the cybersecurity analyst recommend to harden the server? (Choose two.)

A. Uninstall the DNS service
B. Perform a vulnerability scan
C. Change the server's IP to a private IP address
D. Disable the Telnet service
E. Block port 80 with the host-based firewall
F. Change the SSH port to a non-standard port

Answer: DE
Explanation:
A host based firewall would allow you to block http since you have https which is more secure. I think Blocking DNS wouldn't allow someone to type www.company.com, they would have to type the IP address of the web server. And making the web server private IP would only make it accessible in the internal network.

QUESTION 12
Which of the following is MOST important when developing a threat hunting program?

A. Understanding penetration testing techniques
B. Understanding how to build correlation rules within a SIEM
C. Understanding security software technologies
D. Understanding assets and categories of assets

Answer: C
Explanation:
When creating a threat hunting program it is important to start by developing standardized processes to guide threat hunting efforts. Security teams should outline when and how hunting takes place (whether at scheduled intervals, in response to specific triggering actions, or continuously with the help of automated tools), what techniques are to be used, and which people and TOOLS will be responsible for performing specific threat hunting tasks.

QUESTION 13
A company's application development has been outsourced to a third-party development team. Based on the SLA, the development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

A. Input validation
B. Security regression testing
C. Application fuzzing
D. User acceptance testing
E. Stress testing

Answer: C
Explanation:
Threat actors use fuzzing to find zero-day exploits - this is known as a fuzzing attack. Security professionals, on the other hand, leverage fuzzing techniques to assess the security and stability of applications.
https://brightsec.com/blog/fuzzing/

QUESTION 14
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Date/time	Destination	Protocol	Host	Info
2020-08-20	92.168.4.52	HTTP	utoftor.com	POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:

```
Post /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$s.0.k..4.4.RQA.6.... HTTP/1.1 200 OK
Server: nginx/1.6.2
```

Which of the following describes what has occurred?

A. The host attempted to download an application from utoftor.com.
B. The host downloaded an application from utoftor.com.
C. The host attempted to make a secure connection to utoftor.com.
D. The host rejected the connection from utoftor.com.

Answer: B
Explanation:
"Connection: close" mean when used in the response message? Bookmark this question. Show activity on this post. When the client uses the Connection: close header in the request message, this means that it wants the server to close the connection after sending the response message. 200 OK is the most common HTTP status code. It generally means that the HTTP request succeeded.

QUESTION 15
Which of the following types of controls defines placing an ACL on a file folder?

A. Technical control
B. Confidentiality control
C. Managerial control
D. Operational control

Answer: A
Explanation:
Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption.

QUESTION 16
A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix.

Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?

A. Web-application vulnerability scan
B. Static analysis
C. Packet inspection
D. Penetration test

Answer: B
Explanation:
What is static analysis?
Static analysis is a method of analyzing code for defects, bugs, or security issues prior to pushing to production.
https://cloudacademy.com/blog/what-is-static-analysis-within-ci-cd-pipelines/

QUESTION 17
A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions.
Which of the following roles would be BEST suited to determine the breach notification requirements?

A. Legal counsel
B. Chief Security Officer
C. Human resources
D. Law enforcement

Answer: A
Explanation:
Legal counsel responsible for ensuring that the team's actions comply with legal, policy, and regulatory requirements and can advise team leaders on compliance issues and communication with regulatory bodies.

QUESTION 18
A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives.
Which of the following would be BEST for the analyst to configure to achieve this objective?

A. A TXT record on the name server for SPF
B. DNSSEC keys to secure replication
C. Domain Keys identified Man
D. A sandbox to check incoming mad

Answer: C
Explanation:
In a nutshell, SPF allows email senders to define which IP addresses are allowed to send mail for a particular domain. DKIM on the other hand, provides an encryption key and digital signature that verifies that an email message was not forged or altered.

QUESTION 19
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?

A. Remote code execution
B. Buffer overflow
C. Unauthenticated commands
D. Certificate spoofing

Answer: C
Explanation:
The Modbus protocol lacks security and heavily relies on command input (i.e. diagnostic commands).
https://www.radiflow.com/blog/hack-the-modbus/

QUESTION 20
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version.
When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

A. Infrastructure
B. Capabilities
C. Adversary
D. Victims

Answer: A
Explanation:
Infrastructure: The infrastructure refers to the physical or logical communication structures used by an adversary to supply a capability, such as IP or e-mail addresses, domain names, etc.

QUESTION 21
Which of the following describes the main difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

A. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
C. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are
D. Unsupervised algorithms produce more false positives. Than supervised algorithms.

Answer: B
Explanation:
Supervised learning models can be time-consuming to train, and the labels for input and output variables require expertise. Meanwhile, unsupervised learning methods can have wildly inaccurate results unless you have human intervention to validate the output variables.

QUESTION 22
A company is experiencing a malware attack within its network. A security engineer notices many of the impacted assets are connecting outbound to a number of remote destinations and exfiltrating data. The security engineer also see that deployed, up-to-date antivirus signatures are ineffective.
Which of the following is the BEST approach to prevent any impact to the company from similar attacks in the future?

A. IDS signatures
B. Data loss prevention
C. Port security
D. Sinkholing

Answer: B
Explanation:
Preventing data exfiltration is possible with security solutions that ensure data loss and leakage prevention. For example, firewalls can block unauthorized access to resources and systems storing sensitive information. On the other hand, a security information and event management system (SIEM) can secure data in motion, in use, and at rest, secure endpoints, and identify suspicious data transfers.

QUESTION 23
As part of an intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several domains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for intelligence gathering?

A. Update the whitelist.
B. Develop a malware signature.
C. Sinkhole the domains
D. Update the Blacklist

Answer: C
Explanation:
A sinkhole is a server designed to capture malicious traffic and prevent control of infected computers by the criminals who infected them.
https://www.wired.com/story/what-is-sinkholing/

QUESTION 24
A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to 90 offline. Which of the following solutions would work BEST prevent to this from happening again?

A. Change management
B. Application whitelisting
C. Asset management
D. Privilege management

Answer: A
Explanation:
Change Management
o The process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts
o Each individual component should have a separate document or database record that describes its initial state and subsequent changes
▪ Configuration information
▪ Patches installed
▪ Backup records
▪ Incident reports/issues

o Change management ensures all changes are planned and controlled to minimize risk of a service disruption

QUESTION 25
A security analyst identified one server that was compromised and used as a data mining machine, and a clone of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

A. System timeline reconstruction
B. System registry extraction
C. Data carving
D. Volatile memory analysts

Answer: D
Explanation:
Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

QUESTION 26
An organization is focused on restructuring its data governance programs and an analyst has been Tasked with surveying sensitive data within the organization.
Which of the following is the MOST accurate method for the security analyst to complete this assignment?

A. Perform an enterprise-wide discovery scan.
B. Consult with an internal data custodian.
C. Review enterprise-wide asset Inventory.
D. Create a survey and distribute it to data owners.

Answer: D
Explanation:
A Data Owner is the person accountable for the classification, protection, use, and quality of one or more data sets within an organization. This responsibility involves activities including, but not limited to, ensuring that: The organization's Data Glossary is comprehensive and agreed upon by all stakeholders.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**