Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

CS0-003 MCQs
CS0-003 TestPrep
CS0-003 Study Guide
CS0-003 Practice Test
CS0-003 Exam Questions

PASS

killexams.com

CompTIA

CS0-003

CompTIA Cybersecurity Analyst (CySA+)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/CS0-003

Question: 62

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network.

Which of the following should the CSIRT conduct next?

A. Take a snapshot of the compromised server and verify its integrity
B. Restore the affected server to remove any malware
C. Contact the appropriate government agency to investigate
D. Research the malware strain to perform attribution

Answer: A

Explanation:

The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the serverâs data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

Question: 63

During an incident, an analyst needs to acquire evidence for later investigation.

Which of the following must be collected first in a computer system, related to its volatility level?

A. Disk contents
B. Backup data
C. Temporary files
D. Running processes

Answer: D

Explanation:

The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when

the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

Question: 64

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region.

Which of the following shell script functions could help achieve the goal?

A. function w() { a=$(ping -c 1 $1 | awk-F â/â âEND{print $1}â) && echo â$1 | $aâ }
B. function x() { b=traceroute -m 40 $1 | awk âEND{print $1}â) && echo â$1 | $bâ }
C. function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F â.in-addrâ â{print $1}â).origin.asn.cymru.com TXT +short }
D. function z() { c=$(geoiplookup$1) && echo â$1 | $câ }

Answer: C

Explanation:

The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F â.in-addrâ â{print $1}â).origin.asn.cymru.com TXT +short }

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

Question: 65

A security analyst is writing a shell script to identify IP addresses from the same country.

Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(ping -c 1 $1 | awk -F â/â âEND{print $1}â) && echo â$1 | $infoâ }
B. function x() { info=$(geoiplookup $1) && echo â$1 | $infoâ }
C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo â$1 | $infoâ }
D. function z() { info=$(traceroute -m 40 $1 | awk âEND{print $1}â) && echo â$1 | $infoâ }

Answer: B

Explanation:

The function that would help the analyst identify IP addresses from the same country is:

function x() { info=$(geoiplookup $1) && echo â$1 | $infoâ }

This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

Question: 66

A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

A. Ask the web development team to update the page contents
B. Add the IP address allow listing for control panel access
C. Purchase an appropriate certificate from a trusted root CA
D. Perform proper sanitization on all fields

Answer: D

Explanation:

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

Question: 67

A user reports a malware alert to the help desk. A technician verities the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes.

Which of the following should the security analyst do next?

A. Document the procedures and walk through the incident training guide.
B. Reverse engineer the malware to determine its purpose and risk to the organization.

C. Sanitize the workstation and verify countermeasures are restored.
D. Isolate the workstation and issue a new computer to the user.

Answer: C

Explanation:

Sanitizing the workstation and verifying countermeasures are restored are part of the eradication and recovery processes that the security analyst should perform next. Eradication is the process of removing malware or other threats from the affected systems, while recovery is the process of restoring normal operations and functionality to the affected systems. Sanitizing the workstation can involve deleting or wiping any malicious files or programs, while verifying countermeasures are restored can involve checking and updating any security controls or settings that may have been compromised.

Reference: https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

Question: 68

A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence.

Which of the following types of media are most volatile and should be preserved? (Select two).

A. Memory cache
B. Registry file
C. SSD storage
D. Temporary filesystems
E. Packet decoding
F. Swap volume

Answer: A,D

Explanation:

Memory cache and swap volume are types of media that are most volatile and should be preserved during a digital forensics investigation. Volatile media are those that store data temporarily and lose their contents when the power is turned off or interrupted. Memory cache is a small and fast memory that stores frequently used data or instructions for faster access by the processor. Swap volume is a part of the hard disk that is used as an extension of the memory when the memory is full or low.

Reference: https://www.techopedia.com/definition/10339/memory-dump

Question: 69

A development team recently released a new version of a public-facing website for testing prior to

production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility.

Which of the following activities best describes the process the development team is initiating?

A. Static analysis
B. Stress testing
C. Code review
D. User acceptance testing

Answer: D

Explanation:

User acceptance testing is a process of verifying that a software application meets the requirements and expectations of the end users before it is released to production. User acceptance testing can help to validate the functionality, usability, performance and compatibility of the software application with real-world scenarios and feedback. User acceptance testing can involve various teams, such as developers, testers, customers and stakeholders.

Reference: https://www.techopedia.com/definition/3887/user-acceptance-testing-uat

Question: 70

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is compatia.org. The testing is successful, and the security technician is prepared to fully implement the solution.

Which of the following actions should the technician take to accomplish this task?

A. Add TXT @ "v=spfl mx include:_spf.comptia. org -all" to the DNS record.
B. Add : XT @ "v=spfl mx include:_spÂ£.comptia.org -all" to the email server.
C. Add TXT @ "v=spfl mx include:_spÂ£.comptia.org +all" to the domain controller.
D. AddTXT @ "v=apfl mx lnclude:_spf .comptia.org +a 11" to the web server.

Answer: A

Explanation:

Adding TXT @ âv=spfl mx include: _spf.comptia. org -allâ to the DNS record can help to prevent outside entities from spoofing the companyâs email domain, which is comptia.org. This is an example of a Sender Policy Framework (SPF) record, which is a type of DNS record that specifies which mail servers are authorized to send email on behalf of a domain. SPF records can help to prevent spoofing by allowing the recipient mail servers to check the validity of the senderâs domain against the SPF record. The â-allâ at the end of the SPF record indicates that any mail server that is not listed in the SPF record is not authorized to send email for comptia.org.

Reference: https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/

Question: 71

A security analyst who works in the SOC receives a new requirement to monitor for indicators of

compromise.

Which of the following is the first action the analyst should take in this situation?

A. Develop a dashboard to track the indicators of compromise.

B. Develop a query to search for the indicators of compromise.
C. Develop a new signature to alert on the indicators of compromise.
D. Develop a new signature to block the indicators of compromise.

Answer: B

Explanation:

Developing a query to search for the indicators of compromise is the first action the analyst should take in this situation. Indicators of compromise (IOCs) are pieces of information that suggest a system or network has been compromised by an attacker. IOCs can include IP addresses, domain names, file hashes, URLs, or other artifacts that are associated with malicious activity. Developing a query to search for IOCs can help to identify any potential incidents or threats in the environment and initiate further investigation or response.

Explanation:

Reference: https://www.crowdstrike.com/cybersecurity-101/incident-response/indicators-of-compromise/

Question: 72

During an investigation, an analyst discovers the following rule in an executive's email client:

```
IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com>
SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>
```

The executive is not aware of this rule.

Which of the following should the analyst do first to evaluate the potential impact of this security incident?

A. Check the server logs to evaluate which emails were sent to <someaddress@domain,com>.
B. Use the SIEM to correlate logging events from the email server and the domain server.
C. Remove the rule from the email client and change the password.
D. Recommend that the management team implement SPF and DKI

Answer: A

Explanation:

Checking the server logs to evaluate which emails were sent to <someaddress@domain,com> is the first action the analyst should do to evaluate the potential impact of this security incident. Server logs are records of events or activities that occur on a server, such as email transactions, web requests, or authentication attempts. Checking the server logs can help to determine how many emails were sent to <someaddress@domain,com>, when they were sent, who sent them, and what they contained. This can help to assess the scope and severity of the incident and plan further actions.

Reference: https://www.techopedia.com/definition/1308/server-log

Question: 73

A security analyst is investigating a compromised Linux server.

The analyst issues the ps command and receives the following output:

```
1286    ?    Ss    0:00   /usr/sbin/cupsd -f
1287    ?    Ss    0:00   /usr/sbin/httpd
1297    ?    Ssl   0:00   /usr/bin/libvirtd
1301    ?    Ss    0:00   ./usr/sbin/sshd -D
1308    ?    Ss    0:00   /usr/sbin/atd -f
```

Which of the following commands should the administrator run next to further analyze the compromised system?

A. gbd /proc/1301
B. rpm -V openssh-server
C. /bin/Is -1 /proc/1301/exe
D. kill -9 1301

Answer: A

Explanation:

/bin/ls -1 /proc/1301/exe is the command that will show the absolute path to the executed binary file associated with the process ID 1301, which is ./usr/sbin/sshd. This information can help the security analyst determine if the binary is an official version and has not been modified, which could be an indicator of a compromise. /proc/1301/exe is a special symbolic link that points to the executable file that was used to start the process 1301.

Reference: https://unix.stackexchange.com/questions/197854/how-does-the-proc-pid-exe-symlink-differ-from-ordinary-symlinks

Question: 74

The following output is from a tcpdump al the edge of the corporate network:

```
12:47:22.179345 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 10.5.1.1 > 198.134.5.201: IP6 (hlim 63, next-header
TCP (6) payload length: 32) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788: Flags [S], cksum 0x58cf (correct), seq 1155375165, win 8192,
options [mss 1412,nop,wscale 2,nop,nop,sackOK], length 0

12:47:22.251065 PPPoE  [ses 0x8122] IP (tos 0x6, ttl 59, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 198.134.5.201 > 10.5.1.1: IP6 (hlim 127, next-
header TCP (6) payload length: 32) 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788 > 2001:67c:2158:a019::ace.53104: Flags [S.], cksum 0xd361 (correct), seq 2642471061,
ack 1155375166, win 8192, options [mss 1220,nop,wscale 6,nop,nop,sackOK], length 0
```

Which of the following best describes the potential security concern?

A. Payload lengths may be used to overflow buffers enabling code execution.
B. Encapsulated traffic may evade security monitoring and defenses
C. This traffic exhibits a reconnaissance technique to create network footprints.
D. The content of the traffic payload may permit VLAN hopping.

Answer: B

Explanation:

Encapsulated traffic may evade security monitoring and defenses by hiding or obfuscating the actual content or source

of the traffic. Encapsulation is a technique that wraps data packets with additional headers or protocols to enable communication across different network types or layers.

Encapsulation can be used for legitimate purposes, such as tunneling, VPNs, or NAT, but it can also be used by attackers to bypass security controls or detection mechanisms that are not able to inspect or analyze the encapsulated traffic.

Reference: https://www.techopedia.com/definition/10339/memory-dump

Question: 75

A company's threat team has been reviewing recent security incidents and looking for a common theme. The team discovered the incidents were caused by incorrect configurations on the impacted systems. The issues were reported to support teams, but no action was taken.

Which of the following is the next step the company should take to ensure any future issues are remediated?

A. Require support teams to develop a corrective control that ensures security failures are addressed once they are identified.
B. Require support teams to develop a preventive control that ensures new systems are built with the required security configurations.
C. Require support teams to develop a detective control that ensures they continuously assess systems for configuration errors.
D. Require support teams to develop a managerial control that ensures systems have a documented configuration baseline.

Answer: A

Explanation:

Requiring support teams to develop a corrective control that ensures security failures are addressed once they are identified is the best step to prevent future issues from being remediated. Corrective controls are actions or mechanisms that are implemented after a security incident or failure has occurred to fix or restore the normal state of the system or network. Corrective controls can include patching, updating, repairing, restoring, or reconfiguring systems or components that were affected by the incident or failure.

Reference: https://www.techopedia.com/definition/10339/memory-dump

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.