



Vendor: CompTIA

Exam Code: CS0-004

Exam Name: CompTIA Cybersecurity Analyst (CySA+)
Certification Exam

Version: DEMO

QUESTION 1

An analyst executes the top command on a Linux system for an unresponsive application and observes the following output:

PID	USER	%CPU	%MEM	COMMAND
6651	xrdp	6.3	0.2	xrdp
7316	comptia	0.3	0.1	top
7583	root	91.2	96	python
6680	comptia	0.7	0.1	kworker

Which of the following is the most likely cause of this issue?

- A. Service disruption
- B. Unauthorized software
- C. Resource exhaustion
- D. Filesystem changes

Answer: C

Explanation:

The python process is consuming 91.2% CPU and 96% memory, exhausting system resources and causing the application to become unresponsive.

QUESTION 2

Which of the following is the most difficult for threat actors to change according to the Pyramid of Pain model?

- A. Tactics, techniques, and procedures
- B. Tools
- C. Domain names
- D. Internet Protocol addresses

Answer: A

Explanation:

TTPs reflect an attacker's established behavior and operational methods, making them much harder to change than tools, domains, or IP addresses.

QUESTION 3

An analyst is assigned to a new cybersecurity improvement project. The analyst wants to better understand the workflow processes and the skill set of the cybersecurity engineers on this task force. The analyst sets up a recurring, weekly conference call. Which of the following best describes the purpose for the conference call?

- A. To conduct incident response training
- B. To create vendor information sessions
- C. To manage and facilitate team coordination
- D. To respond to customer requirements

Answer: C

Explanation:

A recurring team call supports information sharing, workflow alignment, role awareness, and coordination among the cybersecurity engineers.

QUESTION 4

A security analyst uses a full pcap solution to extract all traffic from the last two days associated with the 10.213.4.27 file server. This file server is under investigation due to concerns about potential data exfiltration using Domain Name System (DNS) traffic. Which of the following commands should the analyst use to extract any potentially leaked data from the suspicious.pcap file?

- A. strings suspicious.pcap | grep 10.213.4.27
- B. zeek -r suspicious.pcap ; grep 10.213.4.27 file.log
- C. snort -r suspicious.pcap ; grep eve.log 10.213.4.27
- D. tcpdump -r suspicious.pcap port 53 and host 10.213.4.27

Answer: D

Explanation:

This command reads the packet capture and filters traffic involving the file server on DNS port 53, allowing the analyst to inspect potential DNS-based data exfiltration.

QUESTION 5

An analyst is configuring a security information and event management system to capture fileless malware execution events. Which of the following log files requires additional configuration to accomplish this task?

- A. Microsoft-Windows-Crypto-DPAPI/Operational
- B. Microsoft-Windows-PowerShell/Operational
- C. Microsoft-Windows-UserPnp/DeviceInstall
- D. Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Answer: B

Explanation:

Fileless malware commonly executes through PowerShell. Enhanced PowerShell logging, such as script block and module logging, must be specifically enabled to capture detailed execution activity for the SIEM.

QUESTION 6

A binary file that might contain malicious code is hosted on an isolated machine. An analyst wants to quickly detect the malicious code. Which of the following should the analyst use?

- A. strings
- B. VirusTotal
- C. WHOIS
- D. Yet Another Recursive Acronym (YARA)

Answer: D

Explanation:

YARA scans files locally for patterns and signatures associated with known malware. It is appropriate for an isolated system, whereas VirusTotal requires uploading or querying the file online.

QUESTION 7

A security analyst analyzes the output of a web application access log for a company based in the United States. Given the following output:

datetime	username	status	src_address	region
07-12-2025 09:01:00Z	tlindy	failed	63.102.4.78	US
07-12-2025 09:02:00Z	tlindy	success	63.102.4.78	US
07-12-2025 09:03:00Z	jschott	failed	185.23.154.24	RU
07-12-2025 09:07:00Z	ssanford	success	63.102.4.71	US
07-12-2025 09:08:00Z	mschultz	success	63.102.4.74	US
07-12-2025 09:08:00Z	jschott	failed	185.23.154.22	RU
07-12-2025 09:10:00Z	wlangey	success	63.102.4.79	US
07-12-2025 09:14:00Z	pking	failed	185.23.127.21	RU
07-12-2025 09:15:00Z	tlindy	success	185.87.14.12	RU
07-12-2025 09:13:00Z	jschott	failed	185.28.154.54	RU
07-12-2025 09:18:00Z	oohare	success	63.102.4.70	US
07-12-2025 09:18:00Z	jschott	failed	185.23.127.21	RU
07-12-2025 09:19:00Z	mschultz	success	63.102.4.74	US
07-12-2025 09:20:00Z	qjones	success	63.102.4.71	US
07-12-2025 09:23:00Z	jschott	success	63.102.4.78	US
07-12-2025 09:23:00Z	dman	failed	185.23.127.21	RU
07-12-2025 09:25:00Z	tlindy	success	63.102.4.71	US
07-12-2025 09:28:00Z	jschott	failed	185.143.137.221	RU
07-12-2025 09:31:00Z	mschultz	success	63.102.4.74	US

Which of the following users should be investigated first?

- A. jschott
- B. dman
- C. mschultz
- D. tlindy

Answer: D

Explanation:

tlindy has a successful login from a Russian IP address between successful U.S.-based logins, indicating a potentially compromised account or impossible-travel activity. The other Russian login attempts shown were unsuccessful.

QUESTION 8

An analyst reviews the following system logs from a recent breach attempt:

Time	User	Command	IP
12:51:11	Berry	whoami	10.10.12.13
12:51:12	Berry	netstat -tulpn	10.10.12.13
12:51:13	Berry	sudo su	10.10.12.13
12:51:14	Berry	./linpeas.sh	10.10.12.13
12:51:15	Berry	su Larry	10.10.12.13
12:51:16	Larry	sudo nano	10.10.12.13
12:51:19	Larry	reset; sh1>&0 2>&0	10.10.12.13
12:51:25	root	whoami	10.10.12.13

Which of the following techniques did the attacker attempt to use?

- A. Exfiltration
- B. Remote code execution
- C. Privilege escalation
- D. Spoofing

Answer: C

Explanation:

The attacker used sudo, su, and linpeas.sh to move from lower-privileged accounts to the root account, demonstrating privilege escalation.

QUESTION 9

The vulnerability management team must scan the cloud environment to establish security baselines. Which of the following assessment tools should the team use to perform this task?

- A. Metasploit
- B. Prowler
- C. Maltego
- D. Caldera

Answer: B

Explanation:

Prowler assesses cloud environments against security benchmarks and best practices, helping establish and validate cloud security baselines.

QUESTION 10

A security analyst reruns infrastructure as code (IaC) to tear down and rebuild a new environment after a ransomware attack. Which of the following describes this phase?

- A. Analysis
- B. Post-incident
- C. Detection
- D. Containment
- E. Recovery

Answer: E

Explanation:

Rebuilding the environment from trusted IaC configurations restores systems and services to

normal operation after the ransomware attack.

QUESTION 11

A security analyst isolates a Windows 11 workstation from the network after known malware is detected. The list of security information and event management (SIEM) events during the malware installation and timeline does not identify a specific user who was logged in. The security analyst uses the local administrative account to log in and would like a list of logins to the machine. Which of the following PowerShell commands should the analyst use?

- A. Eventvwr.exe -LogType "Security" EventID "*" | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation
- B. Get-WinEvent -FilterHashTable @{ Logname="Security" ED=4624; } | Sort-Object TimeCreated -Descending | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation
- C. Get-WinEvent -FilterHashTable @{ Logname="System" ED=9754; } | Sort-Object TimeCreated -Descending | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation
- D. Get-WinEvent -FilterHashTable @{ Logname="Application" ED=7124; } | Sort-Object TimeCreated -Descending | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation

Answer: B

Explanation:

Windows event ID 4624 records successful logons in the Security event log, allowing the analyst to identify users who logged in and export the results for analysis. The intended PowerShell filter key is ID=4624.

QUESTION 12

An analyst prepares an after action report following an incident in which multiple systems were compromised over several days. The analyst provides raw event logs from each compromised system in the report and determines that a patient-zero system cannot be found. Which of the following should the analyst do to determine the patient-zero system?

- A. Establish an accurate timeline of events.
- B. Enable monitoring on the compromised systems.
- C. Isolate the compromised systems before remediation.
- D. Improve the content for incident updates during shift handoff.
- E. Perform a reverse composition analysis on malware packages.

Answer: A

Explanation:

Correlating the logs chronologically identifies which system showed the earliest evidence of compromise, helping determine patient zero.

QUESTION 13

Which of the following actions should an incident response analyst take during the recovery phase of the incident response process?

- A. Verify that malicious activity has occurred.
- B. Reimage the disk.
- C. Take the system offline.

D. Write the final report.

Answer: B

Explanation:

Reimaging restores the affected system to a trusted, operational state. Verification occurs during detection and analysis, taking the system offline is containment, and the final report is completed after the incident.

QUESTION 14

Which of the following is the most important component to include in the preparation phase of an incident response plan?

- A. Roles and responsibilities
- B. After action reports
- C. Data integrity validation
- D. Chain of custody

Answer: A

Explanation:

During preparation, the organization must clearly define who performs each incident response function so actions, escalation, and communication occur efficiently.

QUESTION 15

An analyst receives an alert that a user clicked on a malicious link. The analyst verifies that the link is malicious and was intended to capture credentials. The analyst verifies that the user visited the website, but no evidence indicates that the credentials were used. The analyst recommends that the user take remedial training and closes the case. Which of the following steps in the incident response process did the analyst neglect?

- A. Analysis
- B. Containment
- C. Recovery
- D. Post-incident

Answer: B

Explanation:

The analyst validated the incident but failed to contain the threat, such as blocking the malicious URL/domain and taking precautionary action on the user's credentials before closing the case.

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