CS0-003$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

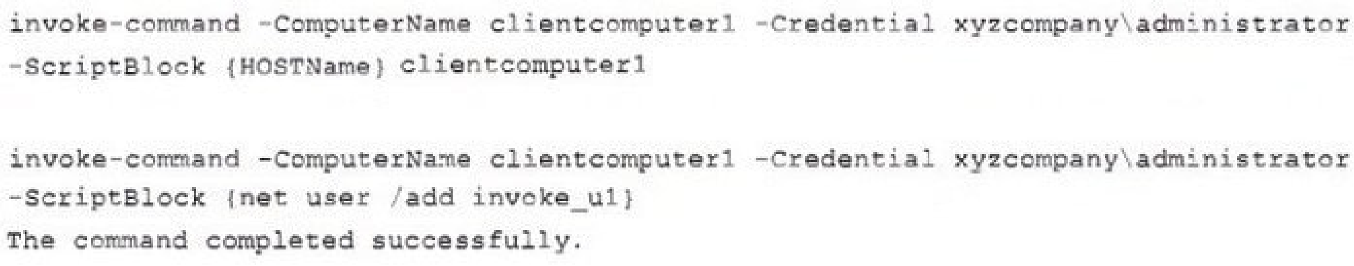
https://www.geekcert.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

The analyst reviews the following endpoint log entry: Which of the following has occurred?



```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator
-ScriptBlock {HOSTName} clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator
-ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

A. Registry change

B. Rename computer

C. New account introduced

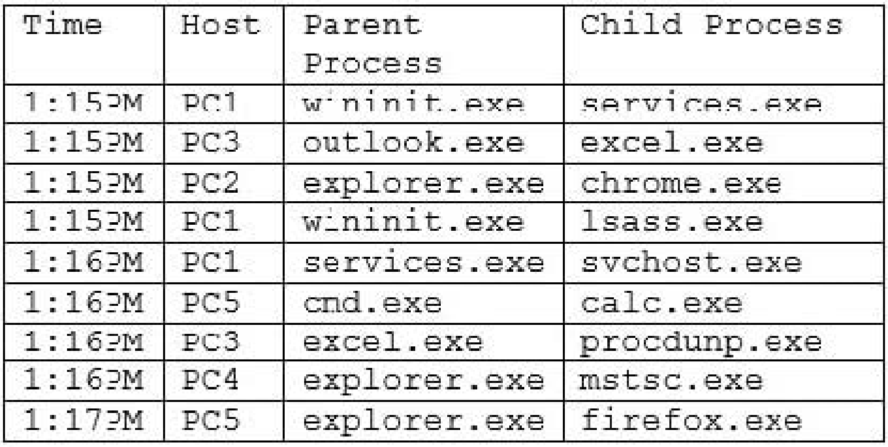
D. Privilege escalation

Correct Answer: C

The endpoint log entry shows that a new account named "admin" has been created on a Windows system with a local group membership of "Administrators". This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

QUESTION 2

An analyst is reviewing system logs while threat hunting:



Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdump.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

Which of the following hosts should be investigated first?

A. PC1 B. PC2

C. PC3

D. PC4

E. PC5

Correct Answer: C

QUESTION 3

An application must pass a vulnerability assessment to move to the next gate. Consequently, any security issues that are found must be remediated prior to the next gate. Which of the following best describes the method for end-to-end vulnerability assessment?

A. Security regression testing

B. Static analysis

C. Dynamic analysis

D. Stress testing

Correct Answer: C

QUESTION 4

An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:

CVSS: 3.1/AV:N/AC: L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R

Which of the following represents the exploit code maturity of this critical vulnerability?

A. E:U

B. S:C

C. RC:R

D. AV:N

E. AC:L

Correct Answer: A

The exploit code maturity of a vulnerability is indicated by the E metric in the CVSS temporal score. The value of U means that no exploit code is available or unknown1. The other options are not related to the exploit code maturity, but to other aspects of the vulnerability, such as attack vector, scope, availability, and complexity1.

QUESTION 5

A consumer credit card database was compromised, and multiple representatives are unable to review the appropriate customer information. Which of the following should the cybersecurity analyst do first?

A. Start the containment effort.

B. Confirm the incident.

C. Notify local law enforcement officials.

D. Inform the senior management team.

Correct Answer: B