

KillTest

高品質 より良いサービス



練習問題

<https://www.killtest.jp>

1年間無料アップデート

Exam : 300-215

Title : Conducting Forensic
Analysis and Incident
Response Using Cisco
CyberOps Technologies
(CBRFIR)

Version : DEMO

1. An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process.

Which two actions should the engineer take? (Choose two.)

- A. Restore to a system recovery point.
- B. Replace the faulty CPU.
- C. Disconnect from the network.
- D. Format the workstation drives.
- E. Take an image of the workstation.

Answer: C, E

Explanation:

When suspicious activity is detected on a workstation, immediate steps need to be taken to preserve evidence and prevent further compromise:

Disconnecting the system from the network (C) is crucial to stop potential exfiltration of data or ongoing communications with a command-and-control server. This isolation prevents further spread or damage while preserving the state of the compromised system for further investigation.

Taking an image of the workstation (E) is part of the forensics acquisition process. It involves creating a bit-by-bit copy of the system's disk, which preserves all evidence in its current state. This allows for thorough forensic analysis without affecting the original evidence.

These steps align with the best practices outlined in the incident response and forensics processes (as described in the CyberOps Technologies (CBRFIR) 300-215 study guide). Specifically, in the Identification and Containment phases of the incident response cycle, it's emphasized that isolating the system and preserving evidence through imaging are critical to ensuring both containment of the threat and successful forensic investigation.

2. DRAG DROP

A security-team engineer must obtain the timestamps and detailed messages for failed-login events from a previously compromised Windows Server 2016 system. The engineer must construct a PowerShell script and export the events to a TXT file for analysis. The script must extract only events from the 72 hours immediately preceding its execution.

Drag and drop the code snippets onto the blanks to construct the script. Not all options are used.

```
$startTime = (Get-Date).  
Get-WinEvent -FilterHashtable @{LogName='  '; Id=4625;  
StartTime=$startTime} | Select-Object TimeCreated, Message |  
Format-Table -AutoSize | Out-File -  .\LogonFail.txt
```

Answer:

```
$startTime = (Get-Date).  
Get-WinEvent -FilterHashtable @{LogName='  '; Id=4625;  
StartTime=$startTime} | Select-Object TimeCreated, Message |  
Format-Table -AutoSize | Out-File -  .\LogonFail.txt
```

Explanation:

(Get-Date). Add Hours (-72) calculates the precise starting timestamp 72 hours before the script runs. Get-Win Event then applies a server-side filter to the Windows Security log for event ID 4625, which represents a failed account logon, and restricts results through StartTime=\$startTime. Select-Object Time Created, Message retains the two fields required by the scenario. Finally, Out-File - FilePath .\LogonFail.txt writes the formatted results to the specified text file; FilePath is the valid parameter, whereas Output is not. System is the wrong event log, and the other time expressions are not valid replacements for the required method call. This construction aligns with CBRFIR objective 2.5 on building PowerShell scripts to parse and search logs. Microsoft documents both Get-WinEvent - FilterHashtable and Out-File -FilePath.

3.Which issue is associated with gathering evidence from virtualized environments provided by major cloud vendors?

- A. increased data transparency provided by cloud vendors
- B. difficulty ensuring the integrity of data due to multitenancy
- C. reduced complexity in isolating and securing evidence
- D. simplified chain of custody due to virtualization

Answer: B

4. What describes the first step in performing a forensic analysis of infrastructure network devices?

- A. immediately disconnecting the device from the network
- B. initiating an immediate full system scan
- C. resetting the device to factory settings and analyzing the difference
- D. producing an accurate, forensic-grade duplicate of the device's data

Answer: D

Explanation:

The first and most important step in forensic analysis is to preserve the integrity of the data. According to best practices outlined in the Cisco CyberOps Associate guide and NIST 800-86, forensic investigators must first produce a forensically sound, bit-by-bit copy of the system's data (i.e., imaging). This enables analysis to occur without altering the original evidence, which is essential for legal admissibility and maintaining the chain of custody.

5. Refer to the exhibit.

5b53797374656d2e57696e646f77732e4d657373616765426f785d3a3a53686f7728225468697320697320612062656e69676e20736372697074212229

- A. hex encoding
- B. metamorphic encoding
- C. ASCII85 encoding
- D. Base64 encoding

Answer: D

Explanation:

The string shown is long, alphanumeric, and includes both uppercase and lowercase letters with numbers—characteristics of Base64 encoding. This format is widely used to obfuscate payloads in malicious scripts, particularly in phishing or malware campaigns. Base64 encoding is also supported by Python and other platforms for data transformation.