300-215Q&As

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

Pass Cisco 300-215 Exam with 100% Guarantee

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

https://www.geekcert.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

A. process injection

B. privilege escalation

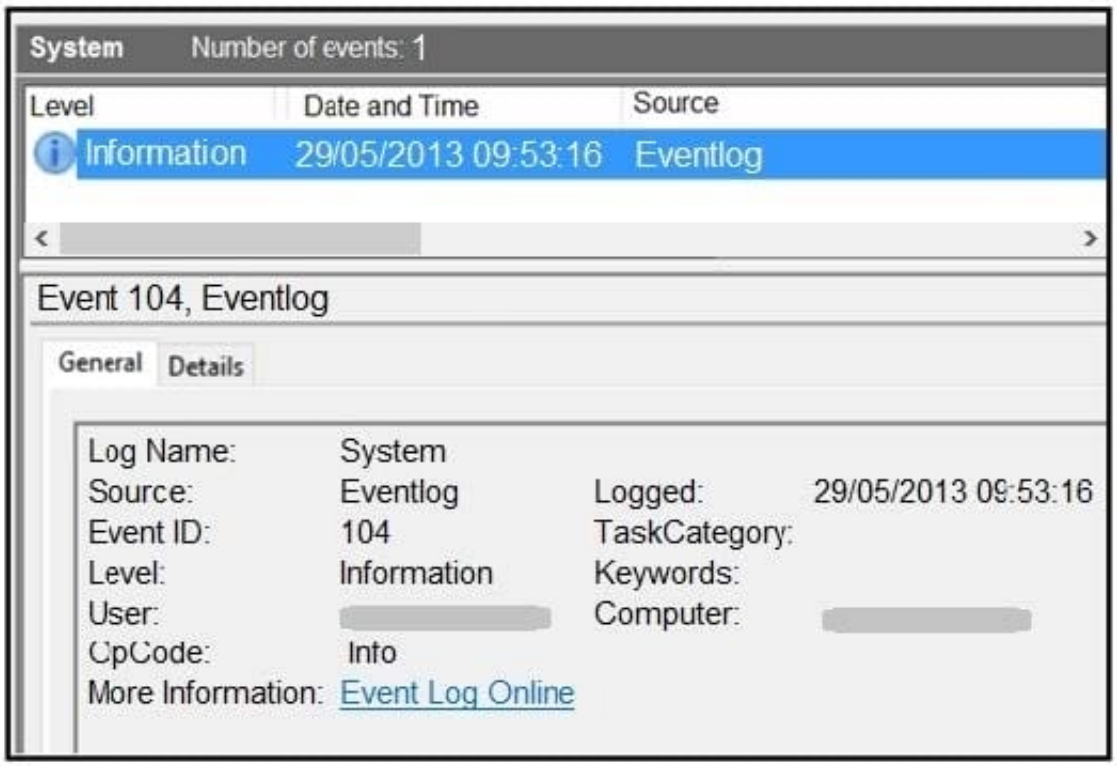
C. GPO modification

D. token manipulation

Correct Answer: A

Reference: https://attack.mitre.org/techniques/T1055/

QUESTION 2



Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

A. data obfuscation

B. reconnaissance attack

C. brute-force attack

D. log tampering

Correct Answer: B

QUESTION 3

```
indicator:Observable id= "example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
<cybox:Object id= "example:Object-3a7aa9db-d082-447c-a422-293b78e24238">
<cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
<EmailMessageObj:Header>
<EmailMessageObj:From category= "e-mail">
<AddressObj:Address_Value condition= "Contains">@state.gov</AddressObj:Address Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= "FileObj:FileObjectType">
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi type= 'cyboxVocabs:HashNameVocab- 1.0">MD5</cyboxCommon:Type>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelatiobshipVocab-
1.0">Contains</cybox:Relationship>
 </cybox:Related_Object>|
 </cybox:Related_Objects>
 </cybox:Object>
 </indicator:Observable>
```

Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

A. Update the AV to block any file with hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

B. Block all emails sent from an @state.gov address.

C. Block all emails with pdf attachments.

D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

E. Block all emails with subject containing "cf2b3ad32a8a4cfb05e9dfc45875bd70".

Correct Answer: AB

QUESTION 4

Which tool is used for reverse engineering malware?

A. Ghidra

B. SNORT

C. Wireshark

D. NMAP

Correct Answer: A

Reference: https://www.nsa.gov/resources/everyone/ghidra/#:~:text=Ghidra%20is%20a%20software%20reverse,in%20their%20networks%20and%20systems.

QUESTION 5

A security team is discussing lessons learned and suggesting process changes after a security breach incident. During the incident, members of the security team failed to report the abnormal system activity due to a high project workload. Additionally, when the incident was identified, the response took six hours due to management being unavailable to provide the approvals needed. Which two steps will prevent these issues from occurring in the future? (Choose two.)

A. Introduce a priority rating for incident response workloads.

B. Provide phishing awareness training for the fill security team.

C. Conduct a risk audit of the incident response workflow.

D. Create an executive team delegation plan.

E. Automate security alert timeframes with escalation triggers.

Correct Answer: AE