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.passapply.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A threat actor attempts to avoid detection by turning data into a code that shifts numbers to the right four times. Which anti-forensics technique is being used?

A. encryption

B. tunneling

C. obfuscation

D. poisoning

Correct Answer: C

Reference: https://www.vadesecure.com/en/malware-analysis-understanding-code-obfuscation-techniques/#:~:text=Obfuscation%20of%20character%20strings%20is,data%20when%20the%20code%20executes.

QUESTION 2

```
[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]

[Classification: Web Application Attack] [Priority: 1]

04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80

TCP TTL:63 TOS:0x0 ID:20054 IpLen: 20 DgmLen:342 DF

***AP*** Seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32

[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```

Refer to the exhibit. According to the SNORT alert, what is the attacker performing?

A. brute-force attack against the web application user accounts

B. XSS attack against the target webserver

C. brute-force attack against directories and files on the target webserver

D. SQL injection attack against the target webserver

Correct Answer: C

QUESTION 3

An "unknown error code" is appearing on an ESXi host during authentication. An engineer checks the authentication

logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

A. /var/log/syslog.log

B. /var/log/vmksummary.log

C. var/log/shell.log

D. var/log/general/log

Correct Answer: A

Reference: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.monitoring.doc/GUID-832A2618-6B11-4A28-9672-93296DA931D0.html

QUESTION 4

A security team receives reports of multiple files causing suspicious activity on users\\' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

A. Inspect registry entries

B. Inspect processes.

C. Inspect file hash.

D. Inspect file type.

E. Inspect PE header.

Correct Answer: BC

Reference: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a

QUESTION 5

An organization uses a Windows 7 workstation for access tracking in one of their physical data centers on which a guard documents entrance/exit activities of all personnel. A server shut down unexpectedly in this data center, and a security specialist is analyzing the case. Initial checks show that the previous two days of entrance/exit logs are missing, and the guard is confident that the logs were entered on the workstation. Where should the security specialist look next to continue investigating this case?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList

C. HKEY_CURRENT_USER\Software\Classes\Winlog

D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser

Correct Answer: A

Reference: https://www.sciencedirect.com/topics/computer-science/window-event-log