



300-215^{Q&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

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





QUESTION 1

An engineer is analyzing a ticket for an unexpected server shutdown and discovers that the web-server ran out of useable memory and crashed.

Which data is needed for further investigation?

- A. /var/log/access.log
- B. /var/log/messages.log
- C. /var/log/httpd/messages.log
- D. /var/log/httpd/access.log

Correct Answer: B

QUESTION 2

Which tool conducts memory analysis?

- A. MemDump
- B. Sysinternals Autoruns
- C. Volatility
- D. Memoryze

Correct Answer: C

Reference: <https://resources.infosecinstitute.com/topic/memory-forensics-and-analysis-using-volatility/>

QUESTION 3

What is the transmogrify anti-forensics technique?

- A. hiding a section of a malicious file in unused areas of a file
- B. sending malicious files over a public network by encapsulation
- C. concealing malicious files in ordinary or unsuspecting places
- D. changing the file header of a malicious file to another file type

Correct Answer: D

Reference: <https://www.csoononline.com/article/2122329/the-rise-of-anti-forensics.html#:~:text=Transmogrify%20is%20similarly%20wise%20to,a%20file%20from%2C%20say%2C%20>



QUESTION 4

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

QUESTION 5

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>

[Latest 300-215 Dumps](#)

[300-215 PDF Dumps](#)

[300-215 Study Guide](#)