EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **CFR-410**

Title : CyberSec First Responder (CFR) Exam

Version : DEMO

1.During a security investigation, a suspicious Linux laptop is found in the server room. The laptop is processing information and indicating network activity. The investigator is preparing to launch an investigation to determine what is happening with this laptop.
Which of the following is the MOST appropriate set of Linux commands that should be executed to conduct the investigation?
A. iperf, traceroute, whois, ls, chown, cat
B. iperf, wget, traceroute, dc3dd, ls, whois
C. lsof, chmod, nano, whois, chown, ls
D. lsof, ifconfig, who, ps, ls, tcpdump
Answer: B

2.Which of the following technologies would reduce the risk of a successful SQL injection attack?
A. Reverse proxy
B. Web application firewall
C. Stateful firewall
D. Web content filtering
Answer: B
Explanation:
Reference: http://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or- Mitigate-SQL-Injection-Attacks.htm

3.A Linux administrator is trying to determine the character count on many log files.
Which of the following command and flag combinations should the administrator use?
A. tr -d
B. uniq -c
C. wc -m
D. grep -c
Answer: C
Explanation:
Reference: https://cmdlinetips.com/2011/08/how-to-count-the-number-of-lines-words-and-characters-in-a-text- file-from-terminal/

4.Organizations considered “covered entities” are required to adhere to which compliance requirement?
A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
B. Payment Card Industry Data Security Standard (PCI DSS)
C. Sarbanes-Oxley Act (SOX)
D. International Organization for Standardization (ISO) 27001
Answer: A
Explanation:
Reference: https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html

5.An incident response team is concerned with verifying the integrity of security information and event management (SIEM) events after being written to disk.

Which of the following represents the BEST option for addressing this concern?

A. Time synchronization

B. Log hashing

C. Source validation

D. Field name consistency

Answer: A

Explanation:

Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf