CFR-410 Q&As

CyberSec First Responder (CFR)

Pass CertNexus CFR-410 Exam with 100% Guarantee

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

https://www.leads4pass.com/cfr-410.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An automatic vulnerability scan has been performed. Which is the next step of the vulnerability assessment process?

A. Hardening the infrastructure

B. Documenting exceptions

C. Assessing identified exposures

D. Generating reports

Correct Answer: D

Reference: https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/

QUESTION 2

An incident handler is assigned to initiate an incident response for a complex network that has been affected by malware. Which of the following actions should be taken FIRST?

A. Make an incident response plan.

B. Prepare incident response tools.

C. Isolate devices from the network.

D. Capture network traffic for analysis.

Correct Answer: D

QUESTION 3

Nmap is a tool most commonly used to:

A. Map a route for war-driving

B. Determine who is logged onto a host

C. Perform network and port scanning

D. Scan web applications

Correct Answer: C

Reference: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html

QUESTION 4

Which of the following could be useful to an organization that wants to test its incident response procedures without risking any system downtime?

A. Blue team exercise

B. Business continuity exercise

C. Tabletop exercise

D. Red team exercise

Correct Answer: B

Reference: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/11/Exercising-BC-Plans-for-Natural-Disasters-A-Quick-Guide-for-MNOs.pdf

QUESTION 5

A system administrator identifies unusual network traffic from outside the local network. Which of the following is the BEST method for mitigating the threat?

A. Malware scanning

B. Port blocking

C. Packet capturing

D. Content filtering

Correct Answer: C

QUESTION 6

A security administrator notices a process running on their local workstation called SvrsScEsdKexzCv.exe. The unknown process is MOST likely:

A. Malware

B. A port scanner

C. A system process

D. An application process

Correct Answer: A

QUESTION 7

A security administrator is investigating a compromised host. Which of the following commands could the investigator use to display executing processes in real time?

A. ps

B. top

C. nice

D. pstree

Correct Answer: B

Reference: https://www.cyberciti.biz/faq/show-all-running-processes-in-linux/

QUESTION 8

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

Correct Answer: B

QUESTION 9

Which of the following are part of the hardening phase of the vulnerability assessment process? (Choose two.)

A. Installing patches

B. Updating configurations

C. Documenting exceptions

D. Conducting audits

E. Generating reports

Correct Answer: AB

QUESTION 10

Which of the following security best practices should a web developer reference when developing a new web-based application?

A. Control Objectives for Information and Related Technology (COBIT)

B. Risk Management Framework (RMF)

C. World Wide Web Consortium (W3C)

D. Open Web Application Security Project (OWASP)

Correct Answer: D

QUESTION 11

An unauthorized network scan may be detected by parsing network sniffer data for:

A. IP traffic from a single IP address to multiple IP addresses.

B. IP traffic from a single IP address to a single IP address.

C. IP traffic from multiple IP addresses to a single IP address.

D. IP traffic from multiple IP addresses to other networks.

Correct Answer: C

QUESTION 12

An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/screen) in numerical order?

A. cat | tac

B. more

C. sort –n

D. less

Correct Answer: C

Reference: https://kb.iu.edu/d/afjb

QUESTION 13

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

Correct Answer: C

Reference: https://cmdlinetips.com/2011/08/how-to-count-the-number-of-lines-words-and-characters-in-a-text-file-from-terminal/

QUESTION 14

While planning a vulnerability assessment on a computer network, which of the following is essential? (Choose two.)

A. Identifying exposures

B. Identifying critical assets

C. Establishing scope

D. Running scanning tools

E. Installing antivirus software

Correct Answer: AC

QUESTION 15

Which of the following would MOST likely make a Windows workstation on a corporate network vulnerable to remote exploitation?

A. Disabling Windows Updates

B. Disabling Windows Firewall

C. Enabling Remote Registry

D. Enabling Remote Desktop

Correct Answer: D