CFR-310 Q&As

CyberSec First Responder

Pass CertNexus CFR-310 Exam with 100% Guarantee

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

https://www.leads4pass.com/cfr-310.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security analyst has discovered that an application has failed to run. Which of the following is the tool MOST likely used by the analyst for the initial discovery?

A. syslog

B. MSConfig

C. Event Viewer

D. Process Monitor

Correct Answer: C

QUESTION 2

Which of the following is susceptible to a cache poisoning attack?

A. Domain Name System (DNS)

B. Secure Shell (SSH)

C. Hypertext Transfer Protocol Secure (HTTPS)

D. Hypertext Transfer Protocol (HTTP)

Correct Answer: A

Reference: https://www.sciencedirect.com/topics/computer-science/cache-poisoning-attack

QUESTION 3

The Key Reinstallation Attack (KRACK) vulnerability is specific to which types of devices? (Choose two.)

A. Wireless router

B. Switch

C. Firewall

D. Access point

E. Hub

Correct Answer: AE

Reference: https://www.kaspersky.com/blog/krackattack/19798/

QUESTION 4

If a hacker is attempting to alter or delete system audit logs, in which of the following attack phases is the hacker involved?

A. Covering tracks

B. Expanding access

C. Gaining persistence

D. Performing reconnaissance

Correct Answer: A

Reference: https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/coveringtracks/log-tampering-101/#gref

QUESTION 5

A secretary receives an email from a friend with a picture of a kitten in it. The secretary forwards it to the ~COMPANYWIDE mailing list and, shortly thereafter, users across the company receive the following message:

“You seem tense. Take a deep breath and relax!”

The incident response team is activated and opens the picture in a virtual machine to test it. After a short analysis, the following code is found in C:

\Temp\chill.exe:Powershell.exe –Command “do {(for /L %i in (2,1,254) do shutdown /r /m Error! Hyperlink reference not valid.andgt; /f /t / 0 (/c “You seem tense. Take a deep breath and relax!”);Start-Sleep –s 900) } while(1)”

Which of the following BEST represents what the attacker was trying to accomplish?

A. Taunt the user and then trigger a shutdown every 15 minutes.

B. Taunt the user and then trigger a reboot every 15 minutes.

C. Taunt the user and then trigger a shutdown every 900 minutes.

D. Taunt the user and then trigger a reboot every 900 minutes.

Correct Answer: B

QUESTION 6

While reviewing some audit logs, an analyst has identified consistent modifications to the sshd_config file for an organization\\'s server. The analyst would like to investigate and compare contents of the current file with archived versions of files that are saved weekly. Which of the following tools will be MOST effective during the investigation?

A. cat * | cut –d ‘,’ –f 2,5,7

B. more * | grep

C. diff

D. sort *

Correct Answer: C

Reference: https://www.tldp.org/LDP/abs/html/filearchiv.html

QUESTION 7

Malicious code designed to execute in concurrence with a particular event is BEST defined as which of the following?

A. Logic bomb

B. Rootkit

C. Trojan

D. Backdoor

Correct Answer: A

Reference: https://searchsecurity.techtarget.com/definition/Malware-Glossary

QUESTION 8

During an incident, the following actions have been taken:

-Executing the malware in a sandbox environment

-Reverse engineering the malware

-Conducting a behavior analysis

Based on the steps presented, which of the following incident handling processes has been taken?

A. Containment

B. Eradication

C. Recovery

D. Identification

Correct Answer: A

The "Containment, eradication and recovery" phase is the period in which incident response team tries to contain the incident and, if necessary, recover from it (restore any affected resources, data and/or processes).

Reference: https://blog.rapid7.com/2017/01/11/introduction-to-incident-response-life-cycle-of-nist-sp-80061/

QUESTION 9

Which of the following are common areas of vulnerabilities in a network switch? (Choose two.)

A. Default port state

B. Default credentials

C. Default protocols

D. Default encryption

E. Default IP address

Correct Answer: AB

QUESTION 10

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-networkmapper.html

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

Which of the following enables security personnel to have the BEST security incident recovery practices?

A. Crisis communication plan

B. Disaster recovery plan

C. Occupant emergency plan

D. Incident response plan

Correct Answer: B

QUESTION 13

During which of the following attack phases might a request sent to port 1433 over a whole company network be seen within a log?

A. Reconnaissance

B. Scanning

C. Gaining access

D. Persistence

Correct Answer: B

Reference: https://blog.stealthbits.com/finding-microsoft-sql-server-targets-sql-attacks/

QUESTION 14

Which common source of vulnerability should be addressed to BEST mitigate against URL redirection attacks?

A. Application

B. Users

C. Network infrastructure

D. Configuration files

Correct Answer: A

Reference: https://blog.qualys.com/securitylabs/2016/01/07/open-redirection-a-simple-vulnerabilitythreatens-your-web-applications

QUESTION 15

After a hacker obtained a shell on a Linux box, the hacker then sends the exfiltrated data via Domain Name System (DNS). This is an example of which type of data exfiltration?

A. Covert channels

B. File sharing services

C. Steganography

D. Rogue service

Correct Answer: A