CFR-410$^{Q\&As}$

CyberSec First Responder

Pass CertNexus CFR-410 Exam with 100% Guarantee

QUESTION 1

Which of the following characteristics of a web proxy strengthens cybersecurity? (Choose two.)

A. Increases browsing speed

B. Filters unwanted content

C. Limits direct connection to Internet

D. Caches frequently-visited websites

E. Decreases wide area network (WAN) traffic

Correct Answer: AD

QUESTION 2

A network administrator has determined that network performance has degraded due to excessive use of social media and Internet streaming services. Which of the following would be effective for limiting access to these types of services, without completely restricting access to a site?

A. Whitelisting

B. Web content filtering

C. Network segmentation

D. Blacklisting

Correct Answer: B

Reference: https://umbrella.cisco.com/solutions/web-content-filtering

QUESTION 3

An administrator believes that a system on VLAN 12 is Address Resolution Protocol (ARP) poisoning clients on the network. The administrator attaches a system to VLAN 12 and uses Wireshark to capture traffic. After reviewing the capture file, the administrator finds no evidence of ARP poisoning. Which of the following actions should the administrator take next?

A. Clear the ARP cache on their system.

B. Enable port mirroring on the switch.

C. Filter Wireshark to only show ARP traffic.

D. Configure the network adapter to promiscuous mode.

Correct Answer: D

Reference: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_arp_poisoning.htm

QUESTION 4

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 5

During a malware-driven distributed denial of service attack, a security researcher found excessive requests to a name server referring to the same domain name and host name encoded in hexadecimal. The malware author used which type of command and control?

A. Internet Relay Chat (IRC)

B. Dnscat2

C. Custom channel

D. File Transfer Protocol (FTP)

Correct Answer: D

Reference: https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html

QUESTION 6

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 7

After imaging a disk as part of an investigation, a forensics analyst wants to hash the image using a tool that supports piecewise hashing. Which of the following tools should the analyst use?

A. md5sum

B. sha256sum

C. md5deep

D. hashdeep

Correct Answer: A

QUESTION 8

An incident responder discovers that the CEO logged in from their New York City office and then logged in from a location in Beijing an hour later. The incident responder suspects that the CEO\\'s account has been compromised. Which of the following anomalies MOST likely contributed to the incident responder\\'s suspicion?

A. Geolocation

B. False positive

C. Geovelocity

D. Advanced persistent threat (APT) activity

Correct Answer: C

Reference: https://www.infosecurity-magazine.com/opinions/geo-velocity-adaptive/

QUESTION 9

When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?

A. Browser logs

B. HTTP logs

C. System logs

D. Proxy logs

Correct Answer: D

Reference: https://www.exabeam.com/siem-guide/events-and-logs/

QUESTION 10

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 11

An incident at a government agency has occurred and the following actions were taken:

-Users have regained access to email accounts

-Temporary VPN services have been removed

-Host-based intrusion prevention system (HIPS) and antivirus (AV) signatures have been updated

-

Temporary email servers have been decommissioned

Which of the following phases of the incident response process match the actions taken?

A.

Containment

B.

Post-incident

C.

Recovery

D. Identification

Correct Answer: A

QUESTION 12

An organization recently suffered a data breach involving a server that had Transmission Control Protocol (TCP) port 1433 inadvertently exposed to the Internet. Which of the following services was vulnerable?

A. Internet Message Access Protocol (IMAP)

B. Network Basic Input/Output System (NetBIOS)

C. Database

D. Network Time Protocol (NTP)

Correct Answer: C

Reference: http://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSSurveyPaper_20030516_Final.pdf (9)

QUESTION 13

An administrator investigating intermittent network communication problems has identified an excessive amount of traffic from an external-facing host to an unknown location on the Internet. Which of the following BEST describes what is occurring?

A. The network is experiencing a denial of service (DoS) attack.

B. A malicious user is exporting sensitive data.

C. Rogue hardware has been installed.

D. An administrator has misconfigured a web proxy.

Correct Answer: B

QUESTION 14

After successfully enumerating the target, the hacker determines that the victim is using a firewall. Which of the following techniques would allow the hacker to bypass the intrusion prevention system (IPS)?

A. Stealth scanning

B. Xmas scanning

C. FINS scanning

D. Port scanning

Correct Answer: C

Reference: https://nmap.org/book/firewall-subversion.html

QUESTION 15

A security professional discovers a new ransomware strain that disables antivirus on the endpoint during an infection. Which location would be the BEST place for the security professional to find technical information about this malware?

A. Threat intelligence feeds

B. Computer emergency response team (CERT) press releases

C. Vulnerability databases

D. Social network sites

Correct Answer: A

Reference: https://whatis.techtarget.com/definition/threat-intelligence-feed