CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

NEW QUESTION 1
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

Answer: A

NEW QUESTION 2
When tracing an attack to the point of origin, which of the following items is critical data to map layer 2 switching?

A. DNS cache
B. ARP cache
C. CAM table
D. NAT table

Answer: B

Explanation:
The host that owns the IP address sends an ARP reply message with its physical address. Each host machine maintains a table, called ARP cache, used to convert MAC addresses to IP addresses. Since ARP is a stateless protocol, every time a host gets an ARP reply from another host, even though it has not sent an ARP request for that reply, it accepts that ARP entry and updates its ARP cache. The process of updating a target host's ARP cache with a forged entry is referred to as poisoning.

NEW QUESTION 3
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 *

Answer: C

NEW QUESTION 4
Which of the following is an automated password cracking technique that uses a combination of uppercase and lowercase letters, 0-9 numbers, and special characters?

A. Dictionary attack
B. Password guessing
C. Brute force attack
D. Rainbow tables

Answer: C

NEW QUESTION 5
During the forensic analysis of a compromised computer image, the investigator found that critical files are missing, caches have been cleared, and the history and event log files are empty. According to this scenario, which of the following techniques is the suspect using?

A. System hardening techniques
B. System optimization techniques
C. Defragmentation techniques
D. Anti-forensic techniques

Answer: D

NEW QUESTION 6
Recently, a cybersecurity research lab discovered that there is a hacking group focused on hacking into the computers of financial executives in Company A to sell the exfiltrated information to Company B. Which of the following threat motives does this MOST likely represent?

A. Desire for power
B. Association/affiliation
C. Reputation/recognition
D. Desire for financial gain

Answer: D

NEW QUESTION 7
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

Answer: B

NEW QUESTION 8
Which of the following describes United States federal government cybersecurity policies and guidelines?

A. NIST
B. ANSI
C. NERC
D. GDPR

Answer: A

NEW QUESTION 9
After a security breach, a security consultant is hired to perform a vulnerability assessment for a company’s web application. Which of the following tools would the consultant use?

A. Nikto
B. Kismet
C. tcpdump
D. Hydra

Answer: A

NEW QUESTION 10
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

Answer: A

NEW QUESTION 10
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

Answer: D

NEW QUESTION 12
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

Answer: A

NEW QUESTION 16
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

Answer: AD

NEW QUESTION 18

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

Answer: A

NEW QUESTION 21
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.

Answer: C

NEW QUESTION 25
An organization recently suffered a breach due to a human resources administrator emailing employee names and Social Security numbers to a distribution list. Which of the following tools would help mitigate this risk from recurring?

A. Data loss prevention (DLP)
B. Firewall
C. Web proxy
D. File integrity monitoring

Answer: A

NEW QUESTION 28
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

Answer: A

NEW QUESTION 32
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

Answer: B

NEW QUESTION 37
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

NEW QUESTION 38
Which of the following are well-known methods that are used to protect evidence during the forensics process? (Choose three.)

A. Evidence bags
B. Lock box
C. Caution tape
D. Security envelope
E. Secure rooms
F. Faraday boxes

Answer: ACD

NEW QUESTION 42
......