CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

NEW QUESTION 1
Various logs are collected for a data leakage case to make a forensic analysis. Which of the following are MOST important for log integrity? (Choose two.)

A. Hash value
B. Time stamp
C. Log type
D. Modified date/time
E. Log path

Answer: AB

NEW QUESTION 2
Which of the following is the GREATEST risk of having security information and event management (SIEM) collect computer names with older log entries?

A. There may be duplicate computer names on the network.
B. The computer name may not be admissible evidence in court.
C. Domain Name System (DNS) records may have changed since the log was created.
D. There may be field name duplication when combining log files.

Answer: D

NEW QUESTION 3
A security analyst is required to collect detailed network traffic on a virtual machine. Which of the following tools could the analyst use?

A. nbtstat
B. WinDump
C. fport
D. netstat

Answer: D

NEW QUESTION 4
A common formula used to calculate risk is:+ Threats + Vulnerabilities = Risk. Which of the following represents the missing factor in this formula?

A. Exploits
B. Security
C. Asset
D. Probability

Answer: C

NEW QUESTION 5
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

NEW QUESTION 6
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.

Answer: D

NEW QUESTION 7
It was recently discovered that many of an organization's servers were running unauthorized cryptocurrency mining software. Which of the following assets were being targeted in this attack? (Choose two.)

A. Power resources
B. Network resources
C. Disk resources
D. Computing resources
E. Financial resources

Answer:

AB

NEW QUESTION 8
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 9
A security operations center (SOC) analyst observed an unusually high number of login failures on a particular database server. The analyst wants to gather supporting evidence before escalating the observation to management. Which of the following expressions will provide login failure data for 11/24/2015?

A. grep 20151124 security_log | grep –c "login failure"
B. grep 20150124 security_log | grep "login_failure"
C. grep 20151124 security_log | grep "login"
D. grep 20151124 security_log | grep –c "login"

Answer: C

NEW QUESTION 10
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 10
A first responder notices a file with a large amount of clipboard information stored in it. Which part of the MITRE ATT&CK matrix has the responder discovered?

A. Collection
B. Discovery
C. Lateral movement
D. Exfiltration

Answer: D

NEW QUESTION 14
A government organization responsible for critical infrastructure is being attacked and files on the server been deleted. Which of the following are the most immediate communications that should be made regarding the incident? (Choose two.)

A. Notifying law enforcement
B. Notifying the media
C. Notifying a national compute emergency response team (CERT) or cybersecurity incident response team (CSIRT)
D. Notifying the relevant vendor
E. Notifying a mitigation expert

Answer: CE

NEW QUESTION 18
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 22

A suspicious script was found on a sensitive research system. Subsequent analysis determined that proprietary data would have been deleted from both the local server and backup media immediately following a specific administrator’s removal from an employee list that is refreshed each evening. Which of the following BEST describes this scenario?

A. Backdoor
B. Rootkit
C. Time bomb
D. Login bomb

Answer: A

NEW QUESTION 27
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 31
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.

Answer: D

NEW QUESTION 34
Which of the following attacks involves sending a large amount of spoofed User Datagram Protocol (UDP) traffic to a router’s broadcast address within a network?

A. Land attack
B. Fraggle attack
C. Smurf attack
D. Teardrop attack

Answer: C

NEW QUESTION 38
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

Answer: B

NEW QUESTION 41
A security engineer is setting up security information and event management (SIEM). Which of the following log sources should the engineer include that will contain indicators of a possible web server compromise? (Choose two.)

A. NetFlow logs
B. Web server logs
C. Domain controller logs
D. Proxy logs
E. FTP logs

Answer: BC

NEW QUESTION 45
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

Answer: B

NEW QUESTION 47
A Linux system administrator found suspicious activity on host IP 192.168.10.121. This host is also establishing a connection to IP 88.143.12.123. Which of the following commands should the administrator use to capture only the traffic between the two hosts?

A. # tcpdump -i eth0 host 88.143.12.123
B. # tcpdump -i eth0 dst 88.143.12.123
C. # tcpdump -i eth0 host 192.168.10.121
D. # tcpdump -i eth0 src 88.143.12.123

Answer: B

NEW QUESTION 51
A company help desk is flooded with calls regarding systems experiencing slow performance and certain Internet sites taking a long time to load or not loading at all. The security operations center (SOC) analysts who receive these calls take the following actions:
-Running antivirus scans on the affected user machines
-Checking department membership of affected users
-Checking the host-based intrusion prevention system (HIPS) console for affected user machine alerts
-Checking network monitoring tools for anomalous activities
Which of the following phases of the incident response process match the actions taken?

A. Identification
B. Preparation
C. Recovery
D. Containment

Answer: A

NEW QUESTION 53
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 57
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

NEW QUESTION 59
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 61
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

Answer: A

NEW QUESTION 63
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)

Answer: D

NEW QUESTION 66
Which of the following types of attackers would be MOST likely to use multiple zero-day exploits executed against high-value, well-defended targets for the purposes of espionage and sabotage?

A. Cybercriminals
B. Hacktivists
C. State-sponsored hackers
D. Cyberterrorist

Answer: C

NEW QUESTION 69
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 70
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 73
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 78
As part of an organization’s regular maintenance activities, a security engineer visits the Internet Storm Center advisory page to obtain the latest list of blacklisted host/network addresses. The security engineer does this to perform which of the following activities?

A. Update the latest proxy access list
B. Monitor the organization’s network for suspicious traffic
C. Monitor the organization’s sensitive databases
D. Update access control list (ACL) rules for network devices

Answer: D

NEW QUESTION 81
Which of the following is the FIRST step taken to maintain the chain of custody in a forensic investigation?

A. Security and evaluating the electronic crime scene.
B. Transporting the evidence to the forensics lab
C. Packaging the electronic device
D. Conducting preliminary interviews

Answer: C

NEW QUESTION 84
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

Answer: D

NEW QUESTION 87
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

Answer: AE

NEW QUESTION 92
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 95
Which of the following, when exposed together, constitutes PII? (Choose two.)

A. Full name
B. Birth date
C. Account balance
D. Marital status
E. Employment status

Answer: AC

NEW QUESTION 99
Which of the following data sources could provide indication of a system compromise involving the exfiltration of data to an unauthorized destination?

A. IPS logs
B. DNS logs
C. SQL logs
D. SSL logs

Answer: A

NEW QUESTION 104
Which of the following does the command nmap –open 10.10.10.3 do?

A. Execute a scan on a single host, returning only open ports.
B. Execute a scan on a subnet, returning detailed information on open ports.
C. Execute a scan on a subnet, returning all hosts with open ports.
D. Execute a scan on a single host, returning open services.

Answer: D

NEW QUESTION 106
While performing routing maintenance on a Windows Server, a technician notices several unapproved Windows Updates and that remote access software has been installed. The technician suspects that a malicious actor has gained access to the system. Which of the following steps in the attack process does this activity indicate?

A. Expanding access
B. Covering tracks
C. Scanning
D. Persistence

Answer: A

NEW QUESTION 107
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 110
An incident responder was asked to analyze malicious traffic. Which of the following tools would be BEST for this?

A. Hex editor
B. tcpdump
C. Wireshark
D. Snort

Answer: C

NEW QUESTION 115
When performing an investigation, a security analyst needs to extract information from text files in a Windows operating system. Which of the following commands should the security analyst use?

A. findstr
B. grep
C. awk
D. sigverif

Answer: C

NEW QUESTION 117
Which of the following is a method of reconnaissance in which a ping is sent to a target with the expectation of receiving a response?

A. Active scanning
B. Passive scanning
C. Network enumeration
D. Application enumeration

Answer: C

NEW QUESTION 121
During which phase of a vulnerability assessment would a security consultant need to document a requirement to retain a legacy device that is no longer supported and cannot be taken offline?

A. Conducting post-assessment tasks
B. Determining scope
C. Identifying critical assets
D. Performing a vulnerability scan

Answer: C

NEW QUESTION 122
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 127
According to Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, an organization must retain logs for what length of time?

A. 3 months
B. 6 months
C. 1 year
D. 5 years

Answer: C

NEW QUESTION 128
......