Free Questions for GCED by certscare

Shared by Taylor on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which command is the Best choice for creating a forensic backup of a Linux system?

Options:

A- Run form a bootable CD: tar cvzf image.tgz /

B- Run from compromised operating system: tar cvzf image.tgz /

C- Run from compromised operating system: dd if=/ dev/hda1 of=/mnt/backup/hda1.img

D- Run from a bootable CD: dd if=/dev/hda1 of=/mnt/backup/hda1.img

Answer:

D

Explanation:

Using dd from a bootable CD is the only forensically sound method of creating an image. Using tar does not capture slack space on the disk. Running any command from a compromised operating system will raise integrity issues.

Question 2

Question Type: MultipleChoice

Which of the following is considered a preventative control in operational security?

Options:

A- Smoke Sensors

B- Fire Suppressant

C- Voltage Regulators

D- Vibration Alarms

Answer:

B

Explanation:

A fire suppressant device is a preventive control. Smoke sensors, vibration alarms, and voltage regulators are part of detection controls.

Question 3

Question Type: MultipleChoice

An analyst wants to see a grouping of images that may be contained in a pcap file. Which tool natively meets this need?

Options:

A- Scapy

B- NetworkMiner

C- TCPReplay

D- Wireshark

Answer:

A

Question 4

Question Type: MultipleChoice

What does the following WMIC command accomplish?

process where name='malicious.exe' delete

Options:

A- Removes the 'malicious.exe' process form the Start menu and Run registry key

B- Stops current process handles associated with the process named 'malicious.exe'

C- Removes the executable 'malicious.exe' from the file system

D- Stops the 'malicious.exe' process from running and being restarted at the next reboot

Answer:

B

Question 5

Question Type: MultipleChoice

An incident response team investigated a database breach, and determined it was likely the result of an internal user who had a default password in place. The password was changed. A week later, they discover another loss of database records. The database admin provides logs that indicate the attack came from the front-end web interface. Where did the incident response team fail?

Options:

A- They did not eradicate tools left behind by the attacker

B- They did not properly identify the source of the breach

C- They did not lock the account after changing the password

D- They did not patch the database server after the event

Answer:

D

Question 6

Question Type: **MultipleChoice**

Which Windows CLI tool can identify the command-line options being passed to a program at startup?

Options:

A- netstat

B- attrib

C- WMIC

D- Tasklist

Answer:

C

Question 7

Question Type: **MultipleChoice**

The matrix in the screen shot below would be created during which process?

Threat	Severity	Likelihood
External hacker attacks public website	5	7
Employee leaks/loses sensitive information	7	5
Malware infects corporate desktops and laptops	4	8

Options:

A- Risk Assessment

B- System Hardening

C- Data Classification

D- Vulnerability Scanning

Answer:

A

Question 8

Question Type: MultipleChoice

Following a Digital Forensics investigation, which of the following should be included in the final forensics report?

Options:

A- An executive summary that includes a list of all forensic procedures performed.

B- A summary of the verified facts of the incident and the analyst's unverified opinions.

C- A summary of the incident and recommended disciplinary actions to apply internally.

D- An executive summary that includes high level descriptions of the overall findings.

Answer:

D

Explanation:

A professional forensic report should include an executive summary, including a description of the incident and the overall findings.

The written report needs to be factually accurate and free from speculation or bias, meaning that an analyst's unverified or unsubstantiated opinions should not be included in the report. Beyond the executive summary, the detailed report should include a

description of the data preserved, a detailed explanation of the procedures performed, and a summary of the facts. Disciplinary action, if needed, would be addressed through other channels and not included in the forensic analyst's report.

Question 9

Question Type: MultipleChoice

Which type of attack could be used to obtain IOS router configuration files without a valid user password?

Options:

A- ARP cache poisoning

B- CDP sniffing

C- SNMP man in the middle

D- TFTP brute force

Answer:

D

Explanation:

TFTP is a protocol to transfer files and commonly used with routers for configuration files, IOS images, and more. It requires no authentication. To download a file you need only know (or guess) its name. CDP, SNMP and ARP are not used for accessing or transferring IOS configuration files.