Vendor: CertNexus

Exam Code:CFR-410

Exam Name: CyberSec First Responder (CFR)

Version: Demo

QUESTION 1

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. Logic bomb

Correct Answer: A

QUESTION 2

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

Correct Answer: B

Reference: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/11/Exercising-BC-Plans-for-Natural-Disasters-A-Quick-Guide-for-MNOs.pdf

---

QUESTION 3

An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/screen) in numerical order?

A. cat | tac

B. more

C. sort –n

D. less

Correct Answer: C

Reference: https://kb.iu.edu/d/afjb

QUESTION 4

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

Correct Answer: A

QUESTION 5

Detailed step-by-step instructions to follow during a security incident are considered:

A. Policies

B. Guidelines

C. Procedures

D. Standards

Correct Answer: C

QUESTION 6

Organizations considered "covered entities" are required to adhere to which compliance requirement?

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

B. Payment Card Industry Data Security Standard (PCI DSS)

C. Sarbanes-Oxley Act (SOX)

D. International Organization for Standardization (ISO) 27001

Correct Answer: A

Reference: https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html

QUESTION 7

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

Correct Answer: B

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.

Reference: https://www.researchgate.net/publication/221056734_Securing_Layer_2_in_Local_Area_Networks

---

QUESTION 8

Tcpdump is a tool that can be used to detect which of the following indicators of compromise?

A. Unusual network traffic

B. Unknown open ports

C. Poor network performance

D. Unknown use of protocols

Correct Answer: A

Reference: https://books.google.com.pk/books?id=b7swDwAAQBAJandpg=PA122andlpg=PA122anddq=Tcpdump+is+a+tool+that+can+be+used+to+detect+which+of+the+following+indicators+of +compromiseandsource=blandots=RxkWHHpNC4andsig=ACfU3U2L48OSw8R8HdLy2ytAuYsRDi9Hmgandhl=enandsa=Xandved=2ahUKEwi44PjnybbpAhVNzIUKHSloCJgQ6AEwAHoECBMQAQ#v=onepageandq=Tcpdump%20is%20a%20tool%20that% 20can%20be%20used%20to%20detect%20which%20of%20the%20following%20indicators%20of%20compromiseandf=false

---

QUESTION 9

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 10

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

Correct Answer: A

QUESTION 11

A Windows system administrator has received notification from a security analyst regarding new malware that executes under the process name of "armageddon.exe" along with a request to audit all department workstations for its presence. In the absence of GUI-based tools, what command could the administrator execute to complete this task?

A. ps -ef | grep armageddon

B. top | grep armageddon

C. wmic process list brief | find "armageddon.exe"

D. wmic startup list full | find "armageddon.exe"

Correct Answer: C

Reference: https://www.andreafortuna.org/2017/08/09/windows-command-line-cheatsheet-part-2-wmic/

QUESTION 12

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