TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **CFR-310**

Title : CyberSec First Responder

Version : DEMO

1.A network security analyst has noticed a flood of Simple Mail Transfer Protocol (SMTP) traffic to internal clients. SMTP traffic should only be allowed to email servers.
Which of the following commands would stop this attack? (Choose two.)
A. iptables -A INPUT -p tcp –dport 25 -d x.x.x.x -j ACCEPT
B. iptables -A INPUT -p tcp –sport 25 -d x.x.x.x -j ACCEPT
C. iptables -A INPUT -p tcp –dport 25 -j DROP
D. iptables -A INPUT -p tcp –destination-port 21 -j DROP
E. iptables -A FORWARD -p tcp –dport 6881:6889 -j DROP
Answer: AC

2.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.> /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.
Answer: B

3.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

4.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

5.Which of the following is a cybersecurity solution for insider threats to strengthen information protection?

A. Web proxy

B. Data loss prevention (DLP)

C. Anti-malware

D. Intrusion detection system (IDS)

Answer: B

Explanation:

Reference: https://www.techrepublic.com/article/how-to-protect-your-organization-against-insider-threats/