Certified CyberSAFE Professional

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(s): A C

---

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(s): 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(s): 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(s): 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(s): B

---

6. 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(s): B

---

7. A system administrator identifies unusual network traffic from outside the local network.
Which of the following is the BEST method for mitigating the threat?

A. Malware scanning

B. Port blocking

C. Packet capturing

D. Content filtering

Answer(s): C

---

8. 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(s): B

---

9. 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

Answer(s): C

---

10. 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(s): A D

---

11. A cybersecurity expert assigned to be the IT manager of a middle-sized company discovers that there is little endpoint security implementation on the company's systems.
Which of the following could be included in an endpoint security solution? (Choose two.)

- [ ] A. Web proxy
- [ ] B. Network monitoring system
- [ ] C. Data loss prevention (DLP)
- [ ] D. Anti-malware
- [ ] E. Network Address Translation (NAT)

Answer(s): A B

---

12. 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(s): B

---

13. 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(s): D

---

14. 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(s): A

---

15. 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(s): C

---

16. 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(s): D

---

17. A web server is under a denial of service (DoS) attack. The administrator reviews logs and creates an access control list (ACL) to stop the attack.
Which of the following technologies could perform these steps automatically in the future?

A. Intrusion prevention system (IPS)

B. Intrusion detection system (IDS)

C. Blacklisting

D. Whitelisting

Answer(s): B

---

18. 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(s): A

---

19. 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(s): C

---

20. 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(s): B
