[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 12 Exam Answers

1. How is the hash value of files useful in network security investigations?

- **It helps identify malware signatures.**
- It is used to decode files.
- It is used as a key for encryption.
- It verifies confidentiality of files.

2. Which tool is a Security Onion integrated host-based intrusion detection system?

- **OSSEC**
- Sguil
- ELSA
- Snort

3. Which type of evidence supports an assertion based on previously obtained evidence?

- direct evidence
- **corroborating evidence**
- best evidence
- indirect evidence

4. Which tool is developed by Cisco and provides an interactive dashboard that allows investigation of the threat landscape?

- Wireshark
- **Talos**
- Sguil
- Snort

5. Which term is used to describe the process of converting log entries into a common format?

- standardization
- **normalization**
- classification
- systemization

6. According to NIST, which step in the digital forensics process involves extracting relevant information from data?

- collection
- examination
- **analysis**
- reporting

7. A law office uses a Linux host as the firewall device for the network. The IT administrator is adding a rule to the firewall iptables to block internal hosts from connecting to a remote device that has the IP address 209.165.202.133. Which command should the administrator use?

- iptables -I FORWARD -p tcp -d 209.165.202.133 –dport 7777 -j DROP
- **iptables -I INPUT -p tcp -d 209.165.202.133 –dport 7777 -j DROP**

- iptables -I PASS -p tcp -d 209.165.202.133 –dport 7777 -j DROP
- iptables -I OUTPUT -p tcp -d 209.165.202.133 –dport 7777 -j DROP

8. What procedure should be avoided in a digital forensics investigation?

- Secure physical access to the computer under investigation.
- **Reboot the affected system upon arrival.**
- Make a copy of the hard drive.
- Recover deleted files.

9. Which statement describes a feature of timestamps in Linux?

- Human readable timestamps measure the number of seconds that have passed since January 1, 1970.
- All devices generate human readable and Unix Epoch timestamps.
- **It is easier to work with Unix Epoch timestamps for addition and subtraction operations.**
- Unix Epoch timestamps are easier for humans to interpret.

10. Which tool is included with Security Onion that is used by Snort to automatically download new rules?

- Sguil
- Wireshark
- ELSA
- **PulledPork**

11. Which tool would an analyst use to start a workflow investigation?

- ELSA
- Bro
- **Sguil**
- Snort

12. What is indicated by a Snort signature ID that is below 3464?

- **The SID was created by Sourcefire and distributed under a GPL agreement.**
- This is a custom signature developed by the organization to address locally observed rules.
- The SID was created by members of EmergingThreats.
- The SID was created by the Snort community and is maintained in Community Rules.

13. How does an application program interact with the operating system?

- accessing BIOS or UEFI
- **making API calls**
- sending files
- using processes

14. A threat actor has successfully breached the network firewall without being detected by the IDS system. What condition describes the lack of alert?

- true negative
- true positive
- false positive
- **false negative**

17. Use the following scenario to answer the questions. A company has just had a cybersecurity incident. The threat actor or actors appeared to have a goal of network disruption and appeared to use a common security hack tool that overwhelmed a particular server with a large amount of traffic, which rendered the server inoperable.

a. How would a certified cybersecurity analyst classify this type of threat actor?

- **amateur**

- hacktivist
- state-sponsored
- terrorist

b. The security team at this company has removed the compromised server and preserved it with the security hack still embedded. What type of evidence is this?

- **best**
- classified
- corroborating
- indirect

c. Which type of attack was achieved?

- access
- **DoS**
- DDoS
- social engineering

d. What would be the threat attribution in this case?

- evaluating the server alert data
- obtaining the most volatile evidence
- **determining who is responsible for the attack**
- reporting the incident to the proper authorities

e. What are three common tools used to carry out this type of attack? (Choose three.)

- ping sweep
- **TCP SYN flood**
- **buffer overflow**
- IP, MAC, and DHCP spoofing
- **smurf attack**
- man-in-the-middle

18. Refer to the exhibit. A network security specialist issues the command *tcpdump* to capture events. What is the function provided by the ampersand symbol used in the command?

- **It instructs the tcpdump to capture data that starts with the symbol.**
- It tells the Linux shell to execute the tcpdump process in the background.
- It tells the Linux shell to display the captured data on the console.
- It tells the Linux shell to execute the tcpdump process indefinitely.

19. Refer to the exhibit. A cybersecurity analyst is using Sguil to verify security alerts. How is the current view sorted?

- by sensor number
- by source IP
- **by frequency**
- by date/time

20. Which three procedures in Sguil are provided to security analysts to address alerts? (Choose three.)

- **Expire false positives.**
- Pivot to other information sources and tools.
- Construct queries using Query Builder.
- **Escalate an uncertain alert.**
- Correlate similar alerts into a single line.
- **Categorize true positives.**

21. Which two strings will be matched by the regular expression? (Choose two.)
Level[^12]

- **Level4**
- **Level3**
- Level2
- Level1
- Level12

22. Which statement describes the status after the Security Onion VM is started?

- SGUIL becomes enabled via the sudo sguil -e terminal command.
- Awk becomes enabled via the sudo awk terminal command.
- Pullpork is used by ELSA as an open source search engine.
- **Snort is enabled by default.**

23. What are the three core functions provided by the Security Onion? (Choose three.)

- business continuity planning
- **full packet capture**
- **alert analysis**
- **intrusion detection**
- security device management
- threat containment

24. Refer to the exhibit. A network security analyst is using the Follow TCP Stream feature in Wireshark to rebuild the TCP transaction. However, the transaction data seems indecipherable. What is the explanation for this?

- The transaction data is encoded with Base64.
- **The transaction data is a binary file.**
- The data shown is line noise.
- The transaction data is corrupted.

25. What is the tool that has alert records linked directly to the search functionality of the Enterprise Log Search and Archive (ELSA)?

- **Sguil**
- Wireshark
- CapME
- Snort

26. Refer to the exhibit. A network security analyst is examining captured data using Wireshark. The captured frames indicate that a host is downloading malware from a server. Which source port is used by the host to request the download?

- 66
- 1514
- 6666
- **48598**

27. Which two types of unreadable network traffic could be eliminated from data collected by NSM? (Choose two.)

- routing updates traffic
- STP traffic
- **SSL traffic**
- **IPsec traffic**
- broadcast traffic