[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 11 Exam Answers

1. How does using HTTPS complicate network security monitoring?

- HTTPS cannot protect visitors to a company-provided web site.
- HTTPS can be used to infiltrate DNS queries.
- Web browser traffic is directed to infected servers.
- **HTTPS adds complexity to captured packets.**

2. Which protocol is used to send e-mail messages between two servers that are in different e-mail domains?

- POP3
- **SMTP**
- HTTP
- IMAP4

3. What are two ways that ICMP can be a security threat to a company? (Choose two.)

- **by collecting information about a network**
- by corrupting network IP data packets
- **by providing a conduit for DoS attacks**
- by corrupting data between email servers and email recipients
- by the infiltration of web pages

4. Which function is provided by the Sguil application?

- **It makes Snort-generated alerts readable and searchable.**
- It detects potential network intrusions.
- It reports conversations between hosts on the network.
- It prevents malware from attacking a host.

5. Which two options are network security monitoring approaches that use advanced analytic techniques to analyze network telemetry data? (Choose two.)

- NetFlow
- Snorby
- **NBAD**
- **NBA**
- IPFIX
- Sguil

6. A system administrator has recommended to the CIO a move of some applications from a Windows server to a Linux server. The proposed server will use ext4 partitions and serve as a web server, file server, and print server. The CIO is considering the recommendation, but has some questions regarding security.

a. Which two methods does Linux use to log data in order to identify a security event? (Choose two.)

- **Apache access logs**
- Event Viewer

- NetFlow
- SPAN
- **syslog**

b. What is a daemon?

- a background process that runs without the need for user interaction
- **a record to keep track of important events**
- a type of security attack
- an application that monitors and analyzes suspicious activity

c. Because the company uses discretionary access control (DAC) for user file management, what feature would need to be supported on the server?

- access based on security clearance held
- principle of least privilege
- role-based access control
- **user-based data access control**

d. What are two benefits of using an ext4 partition instead of ext3? (Choose two.)

- compatibility with CDFS
- compatibility with NTFS
- decreased load time
- **improved performance**
- an increase in the number of supported devices
- **increase in the size of supported files**

7. How can IMAP be a security threat to a company?

- It can be used to encode stolen data and send to a threat actor.
- **An email can be used to bring malware to a host.**
- Encrypted data is decrypted.
- Someone inadvertently clicks on a hidden iFrame.

8. A system administrator runs a file scan utility on a Windows PC and notices a file lsass.exe in the Program Files directory. What should the administrator do?

- Open the Task Manager, right-click on the lsass process and choose End Task.
- Uninstall the lsass application because it is a legacy application and no longer required by Windows.
- Move it to Program Files (x86) because it is a 32bit application.
- **Delete the file because it is probably malware.**

9. How does a web proxy device provide data loss prevention (DLP) for an enterprise?

- by checking the reputation of external web servers
- by functioning as a firewall
- by inspecting incoming traffic for potential exploits
- **by scanning and logging outgoing traffic**

10. A system analyst is reviewing syslog messages and notices that the PRI value of a message is 26. What is the severity value of the message?

- 1
- **2**
- 3
- 6

11. Which statement describes session data in security logs?

- **It is a record of a conversation between network hosts.**

- It can be used to describe or predict network behavior.
- It reports detailed network activities between network hosts.
- It shows the result of network sessions.

12. In a Cisco AVC system, in which module is NetFlow deployed?

- Management and Reporting
- **Metrics Collection**
- Control
- Application Recognition

13. What port number would be used if a threat actor was using NTP to direct DDoS attacks?

- 443
- 25
- 69
- **123**

14. Which information can be provided by the Cisco NetFlow utility?

- IDS and IPS capabilities
- security and user account restrictions
- **peak usage times and traffic routing**
- source and destination UDP port mapping

15. What is Tor?

- a type of Instant Messaging (IM) software used on the darknet
- a way to share processors between network devices across the Internet
- a rule created in order to match a signature of a known exploit
- **a software platform and network of P2P hosts that function as Internet routers**

16. Which statement describes statistical data in network security monitoring processes?

- It shows the results of network activities between network hosts.
- It contains conversations between network hosts.
- **It is created through an analysis of other forms of network data.**
- It lists each alert message along with statistical information.

17. Refer to the exhibit. A network administrator is reviewing an Apache access log message. What is the status of the access request by the client?

- The request was unsuccessful because of server errors.
- **The request was fulfilled successfully.**
- The request was redirected to another web server.
- The request was unsuccessful because of client errors.

18. How might corporate IT professionals deal with DNS-based cyber threats?

- **Monitor DNS proxy server logs and look for unusual DNS queries.**
- Use IPS/IDS devices to scan internal corporate traffic.
- Limit the number of simultaneously opened browsers or browser tabs.
- Limit the number of DNS queries permitted within the organization.

19. Refer to the exhibit. A junior network engineer is handed a print-out of the network information shown. Which protocol or service originated the information shown in the graphic?

- NetFlow
- TACACS+
- RADIUS
- **Syslog**

20. Which technology is used in Cisco Next-Generation IPS devices to consolidate multiple security layers into a single platform?

- WinGate
- **FirePOWER**
- Apache Traffic Server
- Squid

21. Refer to the exhibit. How is the traffic from the client web browser being altered when connected to the destination website of www.cisco.com?

- Traffic is sent in plain-text by the user machine and is encrypted by the TOR node in France and decrypted by the TOR node in Germany.
- Traffic is encrypted by the user machine and sent directly to the cisco.com server to be decrypted.
- Traffic is encrypted by the user machine, and the TOR network only routes the traffic through France, Canada, Germany, and delivers it to cisco.com.
- **Traffic is encrypted by the user machine, and the TOR network encrypts next-hop information on a hop-by-hop basis.**

22. Which Windows log contains information about installations of software, including Windows updates?

- **setup logs**
- application logs
- system logs
- security logs

23. Which Windows log records events related to login attempts and operations related to file or object access?

- setup logs
- **security logs**
- application logs
- system logs

24. What does it indicate if the timestamp in the HEADER section of a syslog message is preceded by a period or asterisk symbol?

- The timestamp represents the round trip duration value.
- The syslog message indicates the time an email is received.
- **There is a problem associated with NTP.**
- The syslog message should be treated with high priority.

25. Which two application layer protocols manage the exchange of messages between a client with a web browser and a remote web server? (Choose two.)

- **HTTPS**
- DHCP
- HTML
- DNS
- **HTTP**

26. Which protocol is a name resolution protocol often used by malware to communicate with command-and-control (CnC) servers?

- IMAP
- HTTPS
- **DNS**

- ICMP