[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 7 Exam Answers

1. What are two monitoring tools that capture network traffic and forward it to network monitoring devices? (Choose two.)

- **SPAN**
- **network tap**
- SNMP
- SIEM
- Wireshark

2. Which technology is an open source SIEM system?

- Wireshark
- StealWatch
- Splunk
- **ELK**

3. What network attack seeks to create a DoS for clients by preventing them from being able to obtain a DHCP lease?

- IP address spoofing
- **DHCP starvation**
- CAM table attack
- DHCP spoofing

4. Which protocol would be the target of a cushioning attack?

- DHCP
- **HTTP**
- ARP
- DNS

5. Which network monitoring capability is provided by using SPAN?

- **Network analysts are able to access network device log files and to monitor network behavior.**
- Statistics on packets flowing through Cisco routers and multilayer switches can be captured.
- Traffic exiting and entering a switch is copied to a network monitoring device.
- Real-time reporting and long-term analysis of security events are enabled.

6. Which type of DNS attack involves the cybercriminal compromising a parent domain and creating multiple subdomains to be used during the attacks?

- **shadowing**
- amplification and reflection
- tunneling
- cache poisoning

7. Refer to the exhibit. What protocol would be used by the syslog server service to create this type of output for security purposes?

- NTP
- AAA
- ICMP
- **SNMP**

9. What is the result of a passive ARP poisoning attack?

- **Confidential information is stolen.**
- Network clients experience a denial of service
- Data is modified in transit or malicious data is inserted in transit.
- Multiple subdomains are created.

10. Which term is used for bulk advertising emails flooded to as many end users as possible?

- **spam**
- adware
- brute force
- phishing

11. Which capability is provided by the aggregation function in SIEM?

- **reducing the volume of event data by consolidating duplicate event records**
- searching logs and event records of multiple sources for more complete forensic analysis
- presenting correlated and aggregated event data in real-time monitoring
- increasing speed of detection and reaction to security threats by examining logs from many systems and applications

12. Which protocol is attacked when a cybercriminal provides an invalid gateway in order to create a man-in-the-middle attack?

- HTTP or HTTPS
- ICMP
- DNS
- **DHCP**

13. Which network monitoring tool can provide a complete audit trail of basic information of all IP flows on a Cisco router and forward the data to a device?

- SPAN
- Wireshark
- **NetFlow**
- SIEM

14. What are two methods used by cybercriminals to mask DNS attacks? (Choose two.)

- **domain generation algorithms**
- shadowing
- **fast flux**
- reflection
- tunneling

15. Which protocol is exploited by cybercriminals who create malicious iFrames?

- **HTTP**
- ARP
- DNS
- DHCP

16. Which SIEM function is associated with speeding up detection of security threats by examining logs and events from different systems?

- forensic analysis

- retention
- **correlation**
- aggregation

17. In which TCP attack is the cybercriminal attempting to overwhelm a target host with half-open TCP connections?

- reset attack
- session hijacking attack
- port scan attack
- **SYN flood attack**

18. In which type of attack is falsified information used to redirect users to malicious Internet sites?

- ARP cache poisoning
- DNS amplification and reflection
- **DNS cache poisoning**
- domain generation

19. Refer to the exhibit. A junior network administrator is inspecting the traffic flow of a particular server in order to make security recommendations to the departmental supervisor. Which recommendation should be made?

- **A more secure protocol should be used.**
- The total length (TL) field indicates an unsecure Layer 4 protocol is being used.
- The person accessing the server should never access it from a device using a private IP address.
- The person accessing the server should use the private IP address of the server.

20. Which network monitoring tool saves captured packets in a PCAP file?

- **Wireshark**
- SIEM
- SNMP
- NetFlow

22. Which cyber attack involves a coordinated attack from a botnet of zombie computers?

- ICMP redirect
- MITM
- **DDoS**
- address spoofing

23. How is optional network layer information carried by IPv6 packets?

- inside an options field that is part of the IPv6 packet header
- inside the Flow Label field
- inside the payload carried by the IPv6 packet
- **inside an extension header attached to the main IPv6 packet header**

24. What type of attack targets an SQL database using the input field of a user?

- Cross-site scripting
- **SQL injection**
- buffer overflow
- XML injection

25. What network monitoring technology enables a switch to copy and forward traffic sent and received on multiple interfaces out another interface toward a network analysis device?

- **port mirroring**

- NetFlow
- SNMP
- network tap