[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 6 Exam Answers

1. **What type of malware has the primary objective of spreading across the network?**
- virus
- **worm**
- Trojan horse
- botnet

2. **Why would a rootkit be used by a hacker?**
- **to gain access to a device without being detected**
- to do reconnaissance
- to reverse engineer binary files
- to try to guess a password

3. **Which type of hacker is motivated to protest against political and social issues?**
- cybercriminal
- script kiddie
- vulnerability broker
- **hacktivist**

4. **What is a characteristic of a Trojan horse as it relates to network security?**
- Extreme quantities of data are sent to a particular network device interface.
- An electronic dictionary is used to obtain a password to be used to infiltrate a key network device.
- Too much information is destined for a particular memory block, causing additional memory areas to be affected.
- **Malware is contained in a seemingly legitimate executable program.**

5. **What is a botnet?**
- a group of web servers that provide load balancing and fault tolerance
- an online video game intended for multiple players
- a network that allows users to bring their own technology
- **a network of infected computers that are controlled as a group**

6. **Which type of Trojan horse security breach uses the computer of the victim as the source device to launch other attacks?**
- DoS
- FTP
- data-sending
- **proxy**

7. **What is the primary goal of a DoS attack?**
- **to prevent the target server from being able to handle additional requests**
- to scan the data on the target server
- to facilitate access to external networks
- to obtain all addresses in the address book within the server

8. What is a main purpose of launching an access attack on network systems?

- to prevent other users from accessing the system
- to scan for accessible networks
- to gather information about the network
- **to retrieve data**

9. What causes a buffer overflow?

- launching a security countermeasure to mitigate a Trojan horse
- **attempting to write more data to a memory location than that location can hold**
- sending repeated connections such as Telnet to a particular device, thus denying other data sources
- sending too much information to two or more interfaces of the same device, thereby causing dropped packets
- downloading and installing too many software updates at one time

10. A company pays a significant sum of money to hackers in order to regain control of an email and data server. Which type of security attack was used by the hackers?

- DoS
- spyware
- Trojan horse
- **ransomware**

11. What is the term used to describe an email that is targeting a specific person employed at a financial institution?

- spam
- spyware
- vishing
- target phishing
- **spear phishing**

12. Which access attack method involves a software program that attempts to discover a system password by the use of an electronic dictionary?

- packet sniffer attack
- denial of service attack
- buffer overflow attack
- **brute-force attack**
- port redirection attack
- IP spoofing attack

13. In what way are zombies used in security attacks?

- **They are infected machines that carry out a DDoS attack.**
- They are maliciously formed code segments used to replace legitimate applications.
- They target specific individuals to gain corporate or personal information.
- They probe a group of machines for open ports to learn which services are running

14. What are two evasion methods used by hackers? (Choose two.)

- scanning
- **encryption**
- access attack
- phishing
- **resource exhaustion**

15. What are two purposes of launching a reconnaissance attack on a network? (Choose two.)

- to retrieve and modify data
- **to scan for accessibility**
- to escalate access privileges
- to prevent other users from accessing the system
- **to gather information about the network and devices**

16. What are three techniques used in social engineering attacks? (Choose three.)

- **vishing**
- **phishing**
- **pretexting**
- buffer overflow
- man-in-the-middle
- sending junk email

17. An attacker is using a laptop as a rogue access point to capture all network traffic from a targeted user. Which type of attack is this?

- port redirection
- trust exploitation
- buffer overflow
- **man in the middle**

18. A user is curious about how someone might know a computer has been infected with malware. What are two common malware behaviors? (Choose two.)

- The computer emits a hissing sound every time the pencil sharpener is used.
- **The computer freezes and requires reboots.**
- No sound emits when an audio CD is played.
- **The computer gets increasingly slower to respond.**
- The computer beeps once during the boot process.

19. Which type of security attack would attempt a buffer overflow?

- ransomware
- reconnaissance
- **DoS**
- scareware

21. What is a significant characteristic of virus malware?

- Virus malware is only distributed over the Internet.
- Once installed on a host system, a virus will automatically propagate itself to other systems.
- **A virus is triggered by an event on the host system.**
- A virus can execute independently of the host system

22. A senior citizen receives a warning on the computer that states that the operating system registry is corrupt and to click a particular link to repair it. Which type of malware is being used to try to create the perception of a computer threat to the user?

- DoS
- **scareware**
- phishing
- adware

24. What is the motivation of a white hat attacker?

- fine tuning network devices to improve their performance and efficiency
- taking advantage of any vulnerability for illegal personal gain
- studying operating systems of various platforms to develop a new system

- **discovering weaknesses of networks and systems to improve the security level of these systems**

25. What is a ping sweep?

- **a network scanning technique that indicates the live hosts in a range of IP addresses.**
- a query and response protocol that identifies information about a domain, including the addresses that are assigned to that domain.
- a software application that enables the capture of all network packets that are sent across a LAN.
- a scanning technique that examines a range of TCP or UDP port numbers on a host to detect listening services

26. What is the term used when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source?

- Trojan
- vishing
- **phishing**
- backdoor

27. What are the three major components of a worm attack? (Choose three.)

- **an enabling vulnerability**
- a propagation mechanism
- **a payload**
- **a probing mechanism**
- a penetration mechanism
- an infecting vulnerability

28. Which security threat installs on a computer without the knowledge of the user and then monitors computer activity?

- **spyware**
- viruses
- worms
- adware