

#1. What is the purpose of a Certificate Authority (CA) in the context of network security?

- To issue and verify...
- To conduct DDoS attacks
- To monitor network traffic
- To develop software applications
- To perform vulnerability scans

#2. What is a common technique used to protect against SQL injection attacks?

- Input validation
- Social engineering
- Firewall configuration
- Data encryption
- Biometric authentication

#3. What is the main purpose of a Proxy Server in network security?

- To act as an intermediary...
- To physically secure servers

To conduct DDoS attacks

To gather information

To bypass firewalls

#4. Which encryption protocol is commonly used to secure web traffic?

HTTPS

FTP

SMTP

Telnet

SNMP

#5. In ethical hacking, what is the purpose of a Man-in-the-Middle (MitM) attack?

To intercept and alter...

To steal sensitive information

To exploit software vulnerabilities

To establish a secure connection

To gather information

#6. What is the main purpose of a Intrusion Detection System (IDS) in network

security?

- To monitor network traffic...
- To host websites anonymously
- To conduct DDoS attacks
- To gather information
- To bypass firewalls

#7. Which type of encryption uses a single key for both encryption and decryption?

- Symmetric encryption
- Asymmetric encryption
- Public key encryption
- Hashing
- Digital signatures

#8. What is the main goal of a social engineering attack in ethical hacking?

- To manipulate individuals...
- To steal sensitive information
- To exploit software vulnerabilities

To establish a secure connection

To gather information

#9. What is the purpose of a honeynet in network security?

To lure and monitor potential...

To store sensitive data securely

To provide training for ethical...

To block network traffic

To generate strong encryption keys

#10. What is the primary objective of a Red Team in ethical hacking?

To simulate real-world...

To document system configurations

To develop new software applications

To perform penetration tests

To create secure passwords

#11. What is the purpose of a firewall in network security?

To monitor and filter...

- To physically secure servers
- To encrypt data in transit
- To store sensitive information
- To generate encryption keys

#12. Which of the following is an example of social engineering attack?

- Phishing
- DDoS attack
- SQL injection
- Cross-site scripting
- Firewall configuration

#13. What is the difference between a vulnerability and an exploit in ethical hacking?

- A vulnerability is a...
- An exploit is a type of...
- A vulnerability is an...
- An exploit is a security...
- A vulnerability leads to...

#14. What is the purpose of a virtual private network (VPN) in ethical hacking?

- To establish a secure...
- To host websites anonymously
- To conduct DDoS attacks
- To gather information
- To bypass firewalls

#15. In ethical hacking, what is the term “payload” typically associated with?

- Malicious code
- Secure encryption
- Network configuration
- Server hardware
- Data backup strategies

#16. What is the main goal of a DDoS (Distributed Denial of Service) attack?

- To overwhelm a target...
- To steal sensitive information
- To exploit software vulnerabilities



To establish a secure...



To gather information

#17. What is a common method of protecting sensitive information during transmission over a network?



Encryption



Social engineering



SQL injection



Firewall configuration



Biometric authentication

#18. What does the term “phreaking” refer to in the context of hacking?



Manipulating and exploiting...



Hacking telephone systems



Gaining unauthorized access...



Exploiting software vulnerabilities



Cracking passwords

#19. What is the purpose of a DNS (Domain Name System) in network communication?

Resolving human-readable...

Encrypting data in transit

Blocking malicious websites

Conducting vulnerability scans

Storing sensitive information

#20. What is the primary goal of conducting a security assessment in ethical hacking?

To evaluate the security...

To launch cyberattacks

To identify vulnerabilities...

To develop new software applications

To perform penetration tests

Next

Results



