By InterviewMocks.com

Ethical Hacking MCQ Quiz & Test

Q1. What is the ethics behind training how to hack a system?

A. To hack a system without the permission
B. To corrupt software or service using malware
C. To think like hackers and know how to defend such attacks
D. To hack a network that is vulnerable

Q2. Performing a shoulder surfing in order to check other's password is.......ethical practice:

A. very good social engineering practice
B. good
C. not so good
D. bad

Q3. ....has now evolved to be one of the most popular automated tools for unethical hacking:

A. Malware
B. Automated apps
C. Worms
D. Database software

Q4. Leaking your company data to the outside network without prior permission of senior authority is a crime:

A. True
B. False

Q5. ....is the technique used in business organizations and firms to protect IT assets:

A. Unethical hacking
B. Ethical hacking
C. Internal data-breach
D. Fixing bugs

Q6. The legal risks of ethical hacking include lawsuits due to .... of personal data:

    A. deleting
    B. stealing
    C. hacking
    D. disclosure

Q7. Before performing any penetration test, through legal procedure, which key points listed below is not mandatory?

    A. Know the nature of the organization
    B. Type of broadband company used by the firm
    C. Characteristics of work done in the firm
    D. System and network

Q8. An ethical hacker must ensure that proprietary information of the firm does not get leaked:

    A. false
    B. true

Q9. After performing .... the ethical hacker should never disclose client information to other parties.

    A. cracking
    B. penetration testing
    C. hacking
    D. exploiting

Q10. ....is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.

    A. Ethics in cyber-security
    B. Ethics in black hat hacking
    C. Social ethics
    D. Corporate ethics

Q11. ....helps to classify arguments and situations, better understand a cyber-crime and helps to determine appropriate actions.

A. Social ethics
B. Corporate behaviour
C. Cyber-ethics
D. Cyber-bullying

Q12. A penetration tester must identify and keep in mind the .... & .... requirements of a firm while evaluating the security postures.

A. hacking techniques
B. rules and regulations
C. ethics to talk to seniors
D. privacy and security

Q13. What is the preferred communications method used with systems on a bot-net?

A. TFTP
B. ICMP
C. IRC
D. E-mail

Q14. Which wireless standard can operate at speeds of 100+ Mbps and uses the 2.4GHz to 5GHz range?

A. 802.11g
B. 802.11n
C. 802.11a
D. 802.11b

Q15. What are the forms of password cracking techniques?

A. AttacksHybrid
B. AttackBrute Forcing
C. AttackSyllable
D. All of the above

Q16. What is the attack called 'evil twin'?

A. Rogue access point
B. ARP poisoning
C. Session hijacking
D. MAC spoofing

Q17. Which wireless mode connects machines directly to one another, without the use of an access point?

    A. Ad hoc
    B. BSS
    C. Point to point
    D. Infrastructure

Q18. CDMA stands for:

    A. Code data multiple access
    B. Code data management authority
    C. Code division multiple access
    D. None

Q19. What is the maximum length of an SSID?

    A. Sixteen characters
    B. Sixty-four characters
    C. Thirty-two characters
    D. Eight characters

Q20. Which of the following is a passive wireless discovery tool?

    A. Kismet
    B. Netsniff
    C. Aircrack
    D. NetStumbler

Q21. Which of the following is true regarding WEP cracking?

    A. Initialization vectors are small, get reused frequently, but are encrypted during transmission
    B. Initialization vectors are large, get reused frequently, but are encrypted during transmission
    C. Initialization vectors are small, get reused frequently, and are sent in cleartext
    D. Initialization vectors are large, get reused frequently, and are sent in cleartext

Q22. Which of the following statements best describes a white-hat hacker?

A. Malicious hacker
B. Former black hat
C. Security professional
D. Former grey hat

Q23. A security audit performed on the internal network of an organization by the network administration is also known as:

A. White-box testing
B. Grey-box testing
C. Black-box testing
D. Active testing

Q24. What is the first phase of hacking?

A. Reconnaissance
B. Scanning
C. Maintaining access
D. Gaining access

Q25. What type of ethical hack tests access to the physical infrastructure?

A. Internal network
B. Remote network
C. External network
D. Physical access

Q26. The security, functionality, and ease of use triangle illustrates which concept?

A. As security decreases, functionality and ease of use increase.
B. As security decreases, functionality and ease of use decrease.
C. Security does not affect functionality and ease of use.
D. As security increases, functionality and ease of use increase.

Q27. Which type of hacker represents the highest risk to your network?

A. Black-hat hackers
B. Script kiddies
C. Disgruntled employees
D. Grey-hat hackers

Q28. Which federal law is most commonly used to prosecute hackers?

A. Title 20
B. Title 18
C. Title 2
D. Title 12

Q29. When a hacker attempts to attack a host via the Internet it is known as what type of attack?

A. Local access
B. Physical access
C. Internal attack
D. Remote attack

Q30. Which are the four regional Internet registries?

A. APNIC, PICNIC, NANIC, ARIN
B. APNIC, PICNIC, NANIC, RIPE NCC
C. APNIC, LACNIC, ARIN, RIPE NCC
D. APNIC, MOSTNIC, ARIN, RIPE NCC

Please Visit interviewmocks.com to download more pdfs