Ethical Hacking
Choose the correct answer:

1. This is the difference between black hat hackers and white hat hackers in terms of purpose.
    A. White hats hack to find vulnerabilities, while black hats hack for personal gain
    B. White hats hack for personal gain, while black hats hack to find vulnerabilities
    C. There are no difference of purpose between white hats and black hats.
    D. Black hats hack to protect asset, while white hats hack to destroy asset.

2. This is the difference between black hat hackers and white hat hackers in terms of legality.
    A. White hats are legal, while black hats are illegal
    B. White hats are illegal, while black hats are legal
    C. White hats and black hats are both legal
    D. White hats and black hats are both illegal

3. This is the difference between black hat hackers and white hat hackers in terms of the tools used in hacking.
    A. White hats use licensed programs, while black hats used pirated programs
    B. White hats used legal programs, while black hats used illegal programs
    C. White hats and black hats use the same tools
    D. White hats authorize the tools used, while black hats exploit the tools used

4. This is the best asset of any ethical hackers today.
    A. Network skills
    B. Scripting knowledge
    C. Use of Tools
    D. Trust

5. This is the profession in which the hackers are employed to check the organizations vulnerabilities by testing its current security via controlled hacking attacks.
    A. Malicious Hacking
    B. Ethical Hacking
    C. Legal Hacking
    D. Proprietary Hacking

6. This is the phase of ethical hacking methodology where the hacker will collect information from the target.
    A. Scanning
    B. Gaining Access
    C. Reconnaissance
    D. Maintaining Access

7. This is the phase of ethical hacking methodology where the hacker will test all active networks identified to see where the hacker can exploit any security vulnerability.
    A. Reconnaissance
    B. Scanning
    C. Gaining Access
    D. Maintaining Access

8. This is the phase of ethical hacking methodology where the hacker will not inject malicious scripts to violate the security triad.
    A. Reconnaissance
    B. Scanning
    C. Gaining Access
    D. Maintaining Access

9. This is the phase of ethical hacking methodology where the hacker will preserve its access to the target system for future use.
    A. Reconnaissance
    B. Scanning
    C. Gaining Access
    D. Maintaining Access

10. This is the OS primarily designed for hacking purposes.
    A. Windows
    B. Mac
    C. Linux Mint
    D. Kali Linux

11. This is the operating system primarily used for hacking purposes.
    a. Kali Linux
    b. Linux Mint
    c. Arch Linux
    d. Pop! OS

12. This is the open source firewall and router that is used for the demo of this course.
    A. pfSense
    B. Sophos Firewall
    C. SonicWall
    D. Cisco Secure

13. This is one of the web servers specifically designed to be vulnerable for learning ethical hacking.
    A. PHPMyadmin
    B. Xampp
    C. Metaspoloitable
    D. Metasploit

14. This is the protocol that contains all the MAC address of the connected devices and their assigned IP address.
    A. Address Partner Protocol
    B. Address Resolution Protocol
    C. Address Definition Protocol
    D. Address Change Protocol

15. This is the unique ID that the routers use to identify the devices connected to it.
    A. IP Address
    B. MAC Address
    C. TCP Address
    D. UTP Address

16. This is the unique ID that routers assign to devices in order to determine their location within the network
    A. IP Address
    B. Mac Address
    C. TCP Address
    D. UTP Address

17. This is a hacking technique that fakes the ARP table so that the attacker can receive any data coming from the victim device
    A. ARP faking
    B. ARP Masking
    C. ARP Spoofing
    D. ARP Dominating

18. This is the tool that can be used to show the ARP table of a network
    A. Netarp
    B. Netserver
    C. Netsystem
    D. Netdiscover

19. This is a tool that can be used to analyze the packets travelling in the network
    A. ARP Table
    B. Netdiscover
    C. Wireshark
    D. ARP Spoofing

20. This is the "landing area" of data coming to a device.
    A. ID
    B. Port
    C. Network
    D. Traffic

21. This is the readable text that humans understand in a computer screen.
    A. Encryption
    B. Plaintext
    C. Ciphertext
    D. Decryption

22. This is a short set of characters that is used to understand ciphertext.
    A. Encryption
    B. Decryption
    C. Key
    D. Keyspace

23. This is the logic gate where there result is false if the two values are the same
    E. XOR
    F. AND
    G. OR
    H. NOT

24. This is the key that is used by users in order to encrypt their message to the recipient.
    I. Open Key
    J. Close Key
    K. Public Key
    L. Private Key

25. This is the key that is used by the recipient of the message to decrypt the message he or she received.
    M. Open Key
    N. Close Key
    O. Public Key
    P. Private Key

26. This is the type of malicious software that hackers used to lock the owners to access the system and asks for money to release the system the hackers held.
    Q. Trojan
    R. Virus
    S. Adware
    T. Ransomware

27. This is how you hack without touching a computer.
    U. Ethical Hacking
    V. Black Hat Hacking
    W. White Hat Hacking
    X. Social Engineering
28. ANSWER: D

29. This is the protocol used to transport email.
    Y. TCP
    Z. SMTP
    AA. UDP
    BB. IP

30. This is the standard port number for email.
    CC. 25
    DD. 50
    EE. 75
    FF. 100

31. This are repositories that contains list of vulnerabilities of known systems.
    GG. Vulnerability List
    HH. Vulnerability Databases
    II. Vulnerability Scanners
    JJ. Vulnerability Webpages