1.What method does the hacker gain information from the system?

1. Surf internet
2. Active Method
3. Update OS patches
4. Scan OS with antivirus

2. What is nslookup?

1. querying the domain name system (DNS) to get information about domain name
2. use for scanning ipv6

3. Does Neo trace provide good information about registration details for the owner of each computer and the network of each node IP?

1. no
2. yes

4. What does VisualRoute integrate with other tools?

1. Whireshark
2. AngryIP
3. Traceroute, ping and whois

5. Can NMAP scan UDP packets on a host?

1. Yes
2. no

6. Is this a SQL Injection statement “select \* from users where userID=105 or 1=1”?

1. no
2. yes

7 What is injected into cross-site scripting?

1. Virus,
2. malicious script and codes
3. SQL statements,
4. malware

8. How to display DHCP filter type in wireshark ?

1. .option.type
2. bootp.option.type == 53

9. How does worm harm a computer?

1. consuming bandwidth
2. corrupt computer files,
3. always restart computer

10 . What software tool can be used for ddos execution?

1. cain and Abel
2. L0phtCrack
3. colasoft packagebuilder
4. Java SDK

11. What packet is advisable to send for Dos stimulation ?

1. TCP
2. udp
3. arp

12. What is the weakest encryption below?

1. md5
2. s h a
3. d e s

13. What is a dictionary attack?

1. In cryptography, a brute force attack or exhaustive key search is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in encryption system that will otherwise make his task easier
2. An attempt to gain illicit access to a computer system by using a very large set of words to generate potential password

14. What activities can a webcopier be used?

1. Just copy html files
2. Phishing activities to perform an attacks
3. Exploit javascript codes

15. What is the most important task for an ethical hacker?

1. get trained for cyber-law and prepare reports for security audits
2. join ethical hacking groups
3. Attend seminars about cyber-law
4. Create incident forms and prepare reports for security audits

16. Which of the following is Android malware?

1. PDF control
2. Geinimi
3. Pokergames
4. mobileworld

17. Does geinimi obfuscated code?

1. Yes
2. no

18. Do you need to insert your own code for Android malware creation?

1. Yes
2. No

19. What is the name of the database that stores password in Android?

1. Webview.db
2. mysqldb.sql

20. What are the commands to decompile the APK file

1. select \* from password
2. adb pull / app in (or app private)hello.apk
3. jar.hello.apk

21. Can you monitor wireshark, fiddler & burp suite to monitor traffic on Android?

1. Yes
2. no

22. Is this the definition of a computer virus “Computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user”?

1. Yes
2. no

23. How does computer virus spread from one computer to another?

1. while typing Word documents
2. when it's host is taken to the uninfected computer, for instance by a user sending it over a network or the internet
3. sending files to print over the printer

24. Can a macro program be infected by a virus?

1. yes
2. no

25. How does the source code virus work ?

1. by adding Trojan code to it
2. by creating a website

26. What is malware?

1. is a software designed to infiltrate or damage a computer system without the owners informed consent
2. a software shows advertisements on your computer

27. What is spyware ?

1. is a denial service software
2. install secretly on a personal computer to intercept or take partial control over the users interaction with computer, without the user’s informed consent

28. What is rootkit ?

1. is a computer virus which consists of a program designed to take fundamental control of a computer system, without authorisation by the systems owner
2. display the Windows password

29. What is the approach to detect viruses?

1. the active approach
2. the heuristic approach
3. the software lifecycle approach

30. What is a MAC address?

1. media access control a unique id assigned to wireless adaptor and routers
2. it isn't an IP address

31. What is 802.11?

1. it is a wireless card
2. it is the Wireless communication standard by IEEE

32. WiFi has how many modes?

1. 7
2. 3
3. 6
4. 1

33. Is ARP a protocol?

1. Yes
2. no

34.How to view the probe frame?

1. a.ping -all
2. airmonng start wlan2

airrodumping mon0

35.What are the values of WEP key?

1. WEP uses 1024 bit
2. WEP uses 64,128 and 256 bit (very rare)
3. WEP uses 2048 bit

36. What is the flaw of WEP?

1. RC4 is a stream cipher and the same key should not be used twice.
2. uses DES encryption

37. Does WEP use open method authentication?

1. No
2. yes

38. What if the WPA packet was tampered with ?

1. WPS will stop using the current keys and rekey.
2. shift back to WEP keys

39. Why is WPA difficult to crack?

1. Need to dictionary attack
2. Need to perform Brute force on the handshake

40. Why is WPA2 recommended?

1. we have to choose strong password in order to achieve good security
2. not detectable by Wireshark

41. What is the weakness of the WPA2?

1. wireshark can display the keys
2. it is possible to crack WPA2 with very high chances of success but it depends on the length and complexity of the password
3. uses 3 pair key system

42. What are wireless active attacks?

1. sniffing the air for packets without sending any data to the AP or clients
2. breaking the key while sending data to while sending data to the AP or clients

43. What are wireless passive attacks?

1. sniffing the air for packets without sending any data to the AP or clients
2. breaking the key while sending data to while sending data to the AP or clients

44. Is ARP an attacking method?

1. no
2. yes

45. Is Aircrack-ng a tool to crack wireless security?

1. yes
2. no

46. Is Kismet a wireless tool for security?

1. Yes
2. no

47. Is the UDP packet causing weakness to the wireless network?

1. yes
2. no

48. What is TKIP?

1. Temporal Key Integrity Protocol
2. Tempo Key Int Phases

49. Why is the Share key less secure?

1. share key is less secure because it can be easily crack by dictionary attack
2. share key is less secure because it allow attacker to get IVs using the challenge through response mechanism

50. Which of the following is the way to avoid the virus?

1. always remember to scan any removable hardware using anti-virus software before accessing it
2. uninstall the anti-virus
3. use common passwords