1. ______________________is the science of testing computers and network for security vulnerabilities and plugging the holes found before the unauthorized people get a chance to exploit them.

Ans: ethical hacking

2. ____________is identifying weakness in computer systems and/or computer networks and coming up with countermeasures that protect the weaknesses.

Ans: ethical hacking

3. Ethical hacking is also known as

penetration testing,
Intrusion testing,
Red teaming.

4. ____________is the art of exploiting the human elements to gain access to unauthorized resources.

Ans: Social engineering

5. __________is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes.

Ans: Social engineering

6. A __________is a person who finds and exploits the weakness in computer systems and/or networks to gain access.

Ans: Hacker

7. What is the attack called "evil twin"?

○ Rogue access point

● ARP poisoning

○ Session hijacking

○ MAC spoofing

8. What are the forms of password cracking techniques?

○ AttackSyllable

○ AttackBrute Forcing

○ AttacksHybrid

○ All of the above

9. what is the primary goal of an Ethical Hacker ?

○ Avoiding detection

○ Testing security controls

○ **Resolving security vulnerabilities**

○ Determining return on investment for security measures

10. What is the first phase of hacking?

○ Maintaining access

○ Gaining access

○ **Reconnaissance**

○ Scanning

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

○ Black-hat hackers

○ Grey-hat hackers

○ Script kiddies

○ **Disgruntled employees**

12. Hacking for a cause is called ....

○ **Hacktivism**

○ Black-hat hacking

○ . Active hacking

○ Activism

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

○ Local access

○ **Remote attack**

○ Internal attack

○ Physical access

14. What port number does HTTPS use?

○ 53

○ **443**

○ 80

○ 21

15. Banner grabbing is an example of what?

○ Footprinting

○ Active operating system fingerprinting

○ **Passive operating system fingerprinting**

○ Application analysis

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

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

17. **A security audit performed on the internal network of an organization by the network administration is also known as __________.**

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

18. What is the first phase of hacking?

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

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

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

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

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

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

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

22. What are the three phases of a security evaluation plan? (Choose three answers.)

- **A. Conduct Security Evaluation**
- **B. Preparation**
- **C. Conclusion**
- D. Final
- E. Reconnaissance
- F. Design Security

23. Hacking for a cause is called ___________________.

- A. Active hacking
- **B. Hacktivism**
- C. Activism
- D. Black-hat hacking

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

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

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

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

26. Which are the four regional Internet registries?

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

Explanation: The four Internet registries are ARIN (American Registry of Internet Numbers), RIPE NCC (Europe, the Middle East, and parts of Central Asia), LACNIC (Latin American and Caribbean Internet Addresses Registry), and APNIC (Asia Pacific Network Information Centre).

27. Which of the following is a tool for performing footprinting undetected?

- **A. Whois search**
- B. Traceroute
- C. Ping sweep
- D. Host scanning

28. Which of the following tools are used for footprinting? (Choose 3 answers.)

- **A. Whois**
- **B. Sam Spade**
- C. NMAP
- D. SuperScan
- **E. Nslookup**

29. What is the next step to be performed after footprinting?

- **A. Scanning**
- B. Enumeration
- C. System hacking
- D. Active information gathering

30. Which are good sources of information about a company or its employees? (Choose all that apply.)

- A. Newsgroups
- B. Job postings
- C. Company website
- D. Press releases

Answer Options A, B, C, D.
Explanation: Newsgroups, job postings, company websites, and press releases are all good sources for information gathering.

31. How does traceroute work?

A. It uses an ICMP destination-unreachable message to elicit the name of a router.
B. It sends a specially crafted IP packet to a router to locate the number of hops from the sender to the destination network.
C. It uses a protocol that will be rejected by the gateway to determine the location.
D. It uses the TTL value in an ICMP message to determine the number of hops from the sender to the router.

32. What is footprinting?

A. Measuring the shoe size of an ethical hacker
B. Accumulation of data by gathering information on a target
C. Scanning a target network to detect operating system types
D. Mapping the physical layout of a target's network

33. Nslookup can be used to gather information regarding which of the following?

- **A. Host names and IP addresses**
- B. Whois information
- C. DNS server locations
- D. Name server types and operating systems

34. Which of the following is a type of social engineering?

- **A. Shoulder surfing**
- B. User identification
- C. System monitoring
- D. Face-to-face communication

35. Which is an example of social engineering?

- A. A user who holds open the front door of an office for a potential hacker
- **B. Calling a help desk and convincing them to reset a password for a user account**
- C. Installing a hardware keylogger on a victim's system to capture passwords
- D. Accessing a database with a cracked password

36. What is the best way to prevent a social-engineering attack?

- A. Installing a firewall to prevent port scans
- B. Configuring an IDS to detect intrusion attempts
- C. Increasing the number of help-desk personnel
- **D. Employee training and education**

37. Which of the following is the best example of reverse social engineering?

- **A. A hacker pretends to be a person of authority in order to get a user to give them information.**
- B. A help-desk employee pretends to be a person of authority.
- C. A hacker tries to get a user to change their password.
- D. A user changes their password.

38. Using pop-up windows to get a user to give out information is which type of social engineering attack?

- A. Human-based
- **B. Computer-based**
- C. Nontechnical
- D. Coercive

39. What is it called when a hacker pretends to be a valid user on the system?

- **A. Impersonation**
- B. Third-person authorization
- C. Help desk
- D. Valid user

40. What is the best reason to implement a security policy?

- A. It increases security.
- B. It makes security harder to enforce.
- **C. It removes the employee’s responsibility to make judgments.**
- D. It decreases security.

41. Faking a website for the purpose of getting a user’s password and username is which type of social engineering attack?

- A. Human-based
- **B. Computer-based**
- C. Web-based
- D. User-based

42. Dumpster diving can be considered which type of social engineering attack?

- **A. Human-based**
- B. Computer-based
- C. Physical access
- D. Paper-based

43. What port number does FTP use?

- **A. 21**
- B. 25
- C. 23
- D. 80

44. What port number does HTTPS use?

- **A. 443**
- B. 80
- C. 53
- D. 21

45. What is war dialing used for?

- A. Testing firewall security
- **B. Testing remote access system security**
- C. Configuring a proxy filtering gateway
- D. Configuring a firewall

46. Banner grabbing is an example of what?

- **A. Passive operating system fingerprinting**
- B. Active operating system fingerprinting
- C. Footprinting
- D. Application analysis

47. What are the three types of scanning?

- **A. Port, network, and vulnerability**
- B. Port, network, and services

- C. Grey, black, and white hat
- D. Server, client, and network

48. What is the main problem with using only ICMP queries for scanning?

- A. The port is not always available.
- B. The protocol is unreliable.
- **C. Systems may not respond because of a firewall.**
- D. Systems may not have the service running.

49. What does the TCP RST command do?

- A. Starts a TCP connection
- B. Restores the connection to a previous state
- C. Finishes a TCP connections
- **D. Resets the TCP connection**

50. What is the proper sequence of a TCP connection?

- **A. SYN-SYN ACK-ACK**
- B. SYN-ACK-FIN
- C. SYN-SYNACK-ACK
- D. SYN-PSH-ACK

51. A packet with all flags set is which type of scan?

- A. Full Open
- B. Syn scan
- **C. XMAS**
- D. TCP connect

52. What is the proper command to perform and NMAP SYN scan every 5 minutes?

- A. nmap -ss – paranoid
- **B. nmap -Ss -paranoid**
- C. nmap -Ss -fast
- D. namp -Ss -sneaky

53. In order to prevent a hacker from using SMB session hijacking, which TCP and UDP ports would you block at the firewall?

- A. 167 and 137
- B. 80 and 23
- **C. 139 and 445**
- D. 1277 and 1270

54. Why would an attacker want to perform a scan on port 137?

- A. To locate the FTP service on the target host
- B. To check for file and print sharing on Windows systems
- C. To discover proxy servers on a network
- **D. To discover a target system with the NetBIOS null session vulnerability**

55. SNMP is a protocol used to manage network infrastructure devices. What is the SNMP read/write community name used for?

- A. Viewing the configuration information
- **B. Changing the configuration information**
- C. Monitoring the device for errors
- D. Controlling the SNMP management station

56. Why would the network security team be concerned about ports 135–139 being open on a system?

- **A. SMB is enabled, and the system is susceptible to null sessions.**
- B. SMB is not enabled, and the system is susceptible to null sessions.
- C. Windows RPC is enabled, and the system is susceptible to Windows DCOM remote sessions.
- D. Windows RPC is not enabled, and the system is susceptible to Windows DCOM remote sessions.

57. Which step comes after enumerating users in the CEH hacking cycle?

- **A. Crack password**
- B. Escalate privileges
- C. Scanning
- D. Covering tracks

58. What is enumeration?

- A. Identifying active systems on the network
- B. Cracking passwords
- **C. Identifying users and machine names**
- D. Identifying routers and firewalls

59. What is a command-line tool used to look up a username from a SID?

- A. UsertoSID
- B. Userenum
- **C. SID2User**
- D. Getacct

60. Which tool can be used to perform a DNS zone transfer on Windows?

- **A. nslookup**
- B. DNSlookup
- C. whois
- D. ipconfig

61. What is a null session?

- A. Connecting to a system with the administrator username and password
- B. Connecting to a system with the admin username and password
- C. Connecting to a system with a random username and password
- **D. Connecting to a system with no username and password**

62. What is a countermeasure for SNMP enumeration?

- **A. Remove the SNMP agent from the device.**
- B. Shut down ports 135 and 139 at the firewall.
- C. Shut down ports 80 and 443 at the firewall.
- D. Enable SNMP read-only security on the agent device.

63 What is the ethics behind training how to hack a system?
a) To think like hackers and know how to defend such attacks
b) To hack a system without the permission
c) To hack a network that is vulnerable
d) To corrupt software or service using malware
64. Performing a shoulder surfing in order to check other's password is ____________ ethical practice.
a) a good
b) not so good
c) very good social engineering practice
d) a bad
65. ___________ has now evolved to be one of the most popular automated tools for unethical hacking.
a) Automated apps
b) Database software
c) Malware
d) Worms
66. Leaking your company data to the outside network without prior permission of senior authority is a crime.
a) True
b) False
View Answer

67. _____________ is the technique used in business organizations and firms to protect IT assets.
a) Ethical hacking
b) Unethical hacking
c) Fixing bugs
d) Internal data-breach
View Answer

68. The legal risks of ethical hacking include lawsuits due to __________ of personal data.
a) stealing
b) disclosure
c) deleting
d) hacking

69. Before performing any penetration test, through legal procedure, which key points listed below is not mandatory?
a) Know the nature of the organization
b) Characteristics of work done in the firm
c) System and network
d) Type of broadband company used by the firm

70. An ethical hacker must ensure that proprietary information of the firm does not get leaked.
a) True
b) False

71.. After performing ____________ the ethical hacker should never disclose client information to other parties.
a) hacking
b) cracking
c) penetration testing
d) exploiting

72. __________ 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) Social ethics
b) Ethics in cyber-security
c) Corporate ethics
d) Ethics in black hat hacking

73. ________ helps to classify arguments and situations, better understand a cyber-crime and helps to determine appropriate actions.
a) Cyber-ethics
b) Social ethics
c) Cyber-bullying
d) Corporate behaviour

74. A penetration tester must identify and keep in mind the ___________ & ___________ requirements of a firm while evaluating the security postures.
a) privacy and security
b) rules and regulations
c) hacking techniques
d) ethics to talk to seniors

75. **someone who maliciously breaks into systems for personal gain. Technically , these criminals are ______________. _________break into systems with malicious intent.**

Ans: crackers(criminal hackers). Crackers

76. ______________involves comparing a company's security policies to what's actually taking place.

Ans : Security auditing

77.**Ethical Hacker(White hat):** A hacker who gains access to systems with a view to fix identified weaknesses. They may also perform penetration testing and vulnerability assessments.

78. **Cracker(Black hat):** A hacker who gains aunautorized access to computer system for personal gain.

79. **Gray Hat:** A hacker who is in between ethical and black hat hakcers. He/She breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

80.**Script Kiddies:** A non-skilled person who gains access to computer systems using already made tools.

81. **Hacktivist:** A hacker who use hacking to send social,religious,and political etc messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

82. **Phreaker:** A hacker who identifies and exploits weaknesses in telephone instead of computers.

83. Penetration testing stages

1. Planning and reconnaissance
2. Scanning
3. Gaining access
4. Maintain access
5. Analysis and WAF configuration

84. Nontechnical attacks

Hackers break into buildings, computer rooms or other areas containing critical information or property.

85. Network infrastructure attacks

1. **Connecting into a network through a rogue modem attached to a computer behind a firewall.**
2. **Exploiting weakness in network transport mechanisms such as TCP/IP and NetBIOS.**
3. **Flooding a network with too many requests, creating a Denial of Service(DoS) for legitimate requests.**
4. **Installing a network analyzer on a network and capturing every packet that travels across it.**
5. **Piggybacking into a network through an insecure wireless configuration.**

86..Operating system attack

1. **Exploiting specific protocol implementations**
2. **Attacking built-in authentication systems**
3. **Breaking file system security**
4. **Cracking passwords and encryption mechanism.**

87. List out some of the common tools used by Ethical hackers?

- Meta Sploit
- Wire Shark
- NMAP(Network Mapper)
- John The Ripper
- Maltego
- EtherPeek
- WebInspect
- LC4
- Network Stumbler
- ToneLoc
- Internet Scanner
- Ethereal
- Nessus
- Nikto
- Kismet
- THC-Scan
- SATAN(Security Adminstrator Tool for Analysing Network)

88. What are the types of ethical hackers?

The types of ethical hackers are

- Grey Box hackers or Cyberwarrior
- Black Box penetration Testers
- White Box penetration Testers
- Certified Ethical hacker

89. What are the types of computer based social engineering attacks? Explain what is Phishing?

Computer based social engineering attacks are

- Phishing
- Baiting
- On-line scams

Phishing technique involves sending false e-mails, chats or website to impersonate real system with aim of stealing information from original website.

90. Explain what is Network Sniffing?

A network sniffer monitors data flowing over computer network links. By allowing you to capture and view the packet level data on your network, sniffer tool can help you to locate network problems. Sniffers can be used for both stealing information off a network and also for legitimate network management.

91. Explain what is Burp Suite, what are the tools it consist of?

Burp suite is an integrated platform used for attacking web applications. It consists of all the Burp tools required for attacking an application. Burp Suite tool has same approach for attacking web applications like framework for handling HTTP request, upstream proxies, alerting, logging and so on.

The tools that Burp Suite has

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Decoder
- Comparer
- Sequencer

92. Mention what are the types of password cracking techniques?

The types of password cracking technique includes

- AttackBrute Forcing
- AttacksHybrid
- AttackSyllable
- AttackRule

93. Explain what are the types of hacking stages?

The types of hacking stages are

- Gaining AccessEscalating
- PrivilegesExecuting
- ApplicationsHiding
- FilesCovering Tracks

94. What is SQL injection and its types?

If the application doesn't sanitize the user input then the SQL injection happens. Thus a malicious hacker would inject SQL question to gain unauthorized access and execute administration operations on the database. SQL injections may be classified as follows:

- Error-based SQL injection
- Blind SQL injection
- Time-based SQL injection

95. What's a denial of service (DOS) attack and what are the common forms?

DOS attacks involve flooding servers, systems or networks with traffic to cause over-consumption of victim resources. This makes it troublesome or not possible for legitimate users to access or use targeted sites.

Common DOS attacks include:

- Buffer overflow attacks
- ICMP flood
- SYN flood
- Teardrop attack
- Smurf attack

96. Which programming language is used for hacking?

It's best, actually, to master all 5 of Python, C/C++, Java, Perl, and LISP. Besides being the foremost vital hacking languages, they represent totally different approaches to programming, and each of it can educate you in valuable ways.

97. What is meant by spoofing attack?

A spoofing attack is when a malicious party impersonates another device or user on a network so as to launch attacks against network hosts, steal data, unfold malware or bypass access controls. Different Spoofing attacks are deployed by malicious parties to achieve this.

98. What are the different types of spoofing?

- ARP Spoofing Attack.
- DNS Spoofing Attack.
- IP Spoofing Attack.