T.Y.B.Sc.C.S.
Sem VI
Ethical Hacking

Sample Questions

1. What is C stands for in CIA triad ?
    A. Confidentiality
    B. Common
    C. candidate
    D. calibre

2. What is I stands for in CIA triad ?
    A. Intension
    B. Important
    C. Illegal
    D. Integrity

3. What is PIN Stands for ?
    A. Personal identification name
    B. Personal internal number
    C. Personal identification number
    D. Protection identification number

4. -----is to access information and other computing services begins with administrative policies and procedures
    A. Authentication
    B. Verification
    C. Authorization
    D. Validation

5. -------_replicates and executes itself, usually doing damage to your computer in th process
    A. Worm
    B. Virus
    C. Trojan Horse
    D. Rabbit

6. -------is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information
    A. Spyware Threat
    B. Backtracking
    C. Cookies
    D. PIN

7. An_-------_ is any attempt or tries to expose, alter, disable, destroy , steal or gain unauthorised access to or make unauthorized use of an asset
    A. Asset
    B. Attack
    C. Alter
    D. Attempt

8. -------_ attack attempts to alter system resources or affect their operation
    A. Normal
    B. Passive
    C. Active
    D. Big

9. ------- path by attacker get an access to an information system to perform malicious activities
    A. Attack Vectors
    B. Threat
    C. Attack
    D. Plan

10. _------- designed to take complete program of a system
    A. Virus
    B. Worm
    C. Rootkits
    D. Trojan

11. ------- is the action of recording the keys struck on a keyboard
    A. key count
    B. backtracking
    C. keystroke logging
    D. phishing

12. -------is a cyber-attack in which the penetrator seeks to machine or network resource unavailable
    A. Denial of Service
    B. Denial of Request
    C. Denial of Response
    D. Denial of Server

13. A brute force attack is a -------_ method
    A. Rapid
    B. Fast
    C. Slow
    D. Trial-and-Error

14. ------- is cyber attack where a malicious actor inserts him/herself into a conversation between two parties
    A. Man-in-the-middle
    B. Eavesdropping
    C. Phishing
    D. DOS

15. The_------- attack consists of the exploitation of the web session control mechanism
    A. DOS
    B. Backtracking
    C. Session Hijacking
    D. shoulder surfing

16. In which attack the hacker hides the actual UI where victim is supposed to click ?
    A. Clickjacking
    B. Hijacking
    C. Session Hijacking
    D. Man-in-the-middle

17. DNS Spoofing also known as _____
    A. DNS Clearance
    B. Spoofing
    C. Sniffing
    D. DNS Cache poisoning

18. ------- are programs to execute a series of operation automatically
    A. robots
    B. machine
    C. helper
    D. bots

19. --------is the process of identifying negative and positive risks that impact an objective
    A. Risk Management
    B. Risk assessment
    C. Risk Control
    D. Risk Removal

20. The Rabbit virus makes multiple copies of itself on a single computer
    A. Trojan
    B. Worm
    C. Rabbit
    D. Malware

21. A_------- is the secure and confidential information to an untrusrted environment
    A. data release
    B. false data
    C. attack
    D. data breach

22. The attack surface of a software environment is the total of the different points called as _____ -------
    A. Malware
    B. Data
    C. Attack vector
    D. Threat

23. The WannaCry ransomware attack had exploited vulnerability in Windows OS called ____
    A. Eternal
    B. EternalBluBlue
    C. BabyCry
    D. EternalBlue

24. What is mean By a claim of identity?
    A. Verification
    B. Threat
    C. Security
    D. Authentication

25. -------_ is the property that information is not made disclosed or available to unauthorized people.
    A. Threat
    B. Confidentiality
    C. Integrity
    D. Availability

26. The success of any risk management of any organization or industry is depending on the management of -------data
    A. Risk
    B. Authorization
    C. Integrity
    D. Security

27. _-------_ is a sneaky program that tracks and reports your computing activity without consent.
    A. Spyware
    B. Trojan
    C. Ransomware
    D. Malware

28. _-------_ flaws give attackers the capability to inject client side scripts into the applications
    A. Cross Site Scripting
    B. HTML
    C. XML
    D. RSS

29. Cross Site Request Forgery also known as -------_ session riding or sea surf is an attack vector that tricks a web browser into executing an unwanted action in an application to which a user is logged in
    A. CSRF
    B. XSS
    C. XSRF
    D. CSS

30. -------headers are control information passed from which to web servers on http requests ,and from servers to web clients on http responses.
    A. HTML
    B. HTTP
    C. CSRF
    D. XSRF

31. _------- Keyloggers are computer programs designed to work on the target computer's software.
    A. Hardware based
    B. Software based
    C. Component
    D. Unit

32. A_-------__ is a trial-and-error method used to obtain information such as a user password or personal Identification number
    A. Brute force attack
    B. Click jacking
    C. Jack click
    D. Waterhole attack

33. ------- is a hacking technique using which a hacker replicates the most-accessed sites and traps the victim by sending that spoofed link.
    A. Sniffing
    B. Eavesdropping
    C. Brute force
    D. Phishing

34. A _------- overflow conditions exists when a program attempts to put more data in a buffer that it can hold or when a program attempts to put data in a memory area past a buffer.
    A. Buffer
    B. DNS
    C. ARP
    D. Identity theft

35. DNS cache poisoning , also known as -------_ spoofing , is type of attack that exploits vulnerabilities in the domain name System(DNS) to divert Internet traffic away from legitimate servers and towards fake ones
    A. DNS Poisoning
    B. ARP Poisoning
    C. Buffer overflow
    D. Identity theft

36. The information can be used to obtain credit, merchandise and services in the name of the victim, or to provide the thief with false _____
    A. Data
    B. Credentials
    C. information
    D. File

37. _------- delivers substantial benefits to end users
    A. BOTNETs
    B. Option B
    C. None of these
    D. Internet of things

38. The need of _-------_ is to create security awareness at all levels in a business
    A. Non Ethical hacking
    B. Security
    C. Ethics
    D. Ethical hacking

39. Vulnerabilities in the system can be identified before they get exploited by _____.
    A. Black Hat hackers
    B. Grey Hat hackers
    C. green hat hackers
    D. white hat hackers

40. ------- is an organisations adherence to loss, regulation, Guidelines and specification relevant to its business
    A. Non Regulatory Compliance
    B. Refusal
    C. Regulatory Compliance
    D. Repulsion

41. _------- is not needed to perform Black Box Testing
    A. Theoretical Knowledge
    B. Technical Knowledge
    C. Programming Knowledge
    D. Designing

42. ------- is based on trail and error method.
    A. Black Box Testing
    B. White Box Testing
    C. Grey Box Testing
    D. Green Box Testing

43. Vulnerability also provides the organisation with the necessary knowledge, awareness and risk background to understand the _------- to its environment and react appropriately.
    A. Threats
    B. Warning
    C. Triviality
    D. Insignificance

44. ------- is the process to identify security vulnerabilities in an application by evaluating the system or network with various malicious techniques.
    A. Non penetration testing
    B. Unit Testing
    C. Penetration testing
    D. Component Testing

45. A _-------_ is a potential or adverse event that may be malicious
    A. Risk
    B. threat
    C. virus
    C. worm

46. _------- is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or to mitigate the effects of, threats to the system.
    A. Data Modelling
    B. System Modelling
    C. Threat Modelling
    D. Risk Modelling

47. ------- kind of testing simulates an attack from a malicious hackers.
    A. Risk Assessment
    B. Security Auditing
    C. Penetration testing
    D. Vulnerability Scanning

48. _------- is type of testing in which the pen tester has little or knowledge of the target.
    A. Grey Box Testing
    B. Black Box Testing
    C. White Box Testing
    D. Green Box Testing

49. _------- is a form of testing in which the information given to the tester is complete
    A. Black Box Testing
    B. Red Box Testing
    C. Green Box testing
    D. White Box Testing

50. External Pen test is designed to test out the ability of an _-------_ to the internal network of a computer system
    A. Local
    B. Intruder
    C. Native
    D. Remote

51. The goal of external pen test is to _-------_ specific services and the desired information that can be found
    A. block
    B. lock
    C. access
    D. Deny

52. An attack from the _-------_ has the potential to do far greater damage.
    A. outside
    B. inside
    C. between
    D. External

53. _-------_ means no usernames and passwords are used in the scanning or testing
    A. Authenticated
    B. Integrity
    C. Unauthenticated
    D. Atomicity

54. __------- means the scanning or testing is able to use usernames and passwords to simulate a user being on that system or website
    A. Unauthenticated
    B. Authorised
    C. Integrity
    D. Authenticated

55. _------- testing requires expert professionals to run the tests.
    A. Automated Testing
    B. Manual Testing
    C. Pen Testing
    D. Unit Testing

56. _------- test tools provide clear reports with less experienced professional
    A. Manual testing
    B. Both a and B
    C. None of the above
    D. Automated Testing

57. .In -------_ results vary from test to test.
    A. Automated Testing
    B. Both a and B
    C. None of the above
    D. Manual Testing

58. -------_ should be remembered by user
    A. Automated Clean up
    B. User Clean up
    C. Memory Cleaning up
    D. Component clean up

59. ------- is time consuming process
    A. Automated Testing
    B. Manual Testing
    C. White box testing
    D. Black box testing

60. -------_ can be useful when trying to understand why your authenticated scan fails, or why not many targets are being found as you expected.
    A. Proxies
    B. Qualys
    C. WebInspect
    D. nessus

61. ------- is used for researching security vulnerabilities and developing code that allows a network administrator to break into his own network to identify security risks and document which vulnerabilities need to be addressed first.
    A. WebInspect
    B. Nessus
    C. Metasploit
    D. Proxies

62. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether ------ access or other malicious activity is possible and identify which flaws pose a threat to the application.
    A. Unauthorized
    B. Authorized
    C. Authenticated
    D. Unauthenticated

63. _------- is a web application security scanning tools offered by HP
    A. Qualys
    B. Proxies
    C. MetaSploit
    D. WebInspect

64. A _------- is a program or automated script which browses the world wide web
    A. Web designer
    B. Web editor
    C. Web Tester
    D. Web crawler

65. A _-------__ test attempts to actively exploit weakness in an environment
    A. Vulnerability Scanning
    B. Both a and B
    C. Penetration
    D. None of the above

66. _------- is a set of procedure for identifying live host, port and services, discovering OS and architecture of target system, Identifying vulnerabilities and threats in the network
    A. Loading
    B. Testing
    C. Editing
    D. Scanning

67. -------_sniffing is a utility which is being used since release of Ethernet.
    A. data
    B. system
    C. packet
    D. Circuit

68. Packet sniffing allows individuals to -------_ data as it is transmitted over a network
    A. Rupture
    B. Leaving
    C. All of the above
    D. Capture

69. A _------- assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications.
    A. Vulnerability
    B. Non Vulnerability
    C. Risky
    D. Non Risky
70. Linux is -------_ operating system
    A. Open source
    B. Secure
    C. Free
    D. Closed source

71. msfgui stands for
    A. metasplit famework GUI
    B. metasploit framework GUI
    C. metaspoil framework GUI
    D. Metaspoil UI

72. The process of gathering information about your target is called
    A. Enumeration
    B. Information gathering
    C. Hacking
    D. none of these

73. -------sniffing is a utility which is being used since the released of Ethernet
    A. Scanning
    B. Packet sniffing
    C. Server
    D. Information

74. ------- escalation requires the attackers to grant himself higher privileges
    A. Horizontal Privileges
    B. North
    C. South privileges
    D. Vertical privileges

75. Password cracking refers to various measure used to discover
    A. Computer password
    B. Phone password
    C. Antivirus
    D. Virus

76. the purpose of password cracking might be to help user to recover a____
    A. Forgotten password
    B. Forgotten username
    C. Forgotten details
    D. Personal detail

77. Internet is -------_ switch network
    A. Mac
    B. Packet
    C. IP
    D. Free

78. Hackers use-------to perform activities that are malicious and illegal
    A. Internet
    B. Router
    C. IP Spoofing
    D. IP address

79. SMTP relay is a mail server through which we can send _____
    A. Inbound emails
    B. Outbound emails
    C. Internal
    D. none of these

80. Disable IP directed broadcast on your ____
    A. Pc
    B. Router
    C. Mail
    D. Mobile

81. In VoIP Signaling, confidential data needs to be protected from ?
    A. Malicious attack
    B. Server attack
    C. Eavesdropping attacks
    D. Threats

82. Brute force attacks is used by criminal to crack
    A. Structured data
    B. Encrypted data
    C. Unstructured data
    D. Plain text

83. Even the extra space in TCP and IP header can be used for -------information
    A. Showing
    B. Hiding
    C. Execute
    D. none of these

84. The application log contain events that are logged by
    A. User
    B. Client
    C. Program
    D. Hacker

85. Log files name and location information is stored in
    A. Memory
    B. Registry
    C. Diary
    D. Array

.

86. TOR is an _-------_ network
    A. Public
    B. Anonymous
    C. Private
    D. Open source

87. ------- scanning is used to create a profile of the target organization
    A. Port
    B. Network
    C. Vulnerability
    D. Threat

88. Valid telephone number can result in
    A. 401error
    B. 404error
    C. 101error
    D. 100error

89. What is the first phase of hacking
    A. Reconnaissance
    B. Scanning
    C. Maintaining access
    D. Gaining access

90. Hacking for a cause is called_------__
    A. Hacktivism
    B. Black-hat hacking
    C. Active hacking
    D. Activism

91. A packet with all flags set which type of scan
    A. Full Open
    B. TCP connect
    C. Syn scan
    D. XMAS
    XMAS

92. Which tool can be used to perform a DNS zone transfer on windows
    A. DNSlookup
    B. ipconfig
    C. whois
    D. nslookup

93. What is maximum length of an SSID
    A. Sixteen characters
    B. Thirty-two characters
    C. 22 character
    D. 09 character

94. Which wireless mode connect machine directly to one another without use of an access point
    A. Point to point
    B. Infrastructure
    C. Ad hoc
    D. BSS

95. Performing a shoulder surfing in order to check other's password is _------- ethical practice.
    A. A bad
    B. Not so good
    C. A good
    D. Very good social engineering practice

96. -------_ has now evolved to be one of the most popular automated tools for unethical hacking.
    A. Automated apps
    B. Database software
    C. Worms
    D. Malware

97. ------- is the technique used in business organizations and firms to protect IT assets.
    A. Unethical hacking
    B. fixing bugs
    C. Ethical hacking
    D. Internal data-breach

98. The legal risks of ethical hacking include lawsuits due to _-------_of personal data.
    A. Stealing
    B. Disclosure
    C. Deleting
    D. Hacking

99. After performing------- the ethical hacker should never disclose client information to other parties.
    A. Hacking
    B. Cracking
    C. Penetration testing
    D. Exposure

100. What is the preferred communications method used with systems on a bot-net?
    A. TFTP
    B. emails
    C. none of these
    D. IRC