NALLAMUTHU GOUNDER MAHALINGAM COLLEGE (AUTONOMOUS)

Re-accredited by NAAC & ISO 9001: 2015 Certified

Affiliated to Bharathiar University, Coimbatore

POLLACHI - 642 001

PART IV - SKILL BASED ELECTIVE – II: Cyber security & Ethical Hacking

1. ARPANET stands for _____.

(a) Advanced Real Projects Air Network

(b) Advanced Research Preparation Agency Network

(c) Advanced Recruitment Process Agency Network

(d) Advanced Research Projects Agency Network

Ans: (d) Advanced Research Projects Agency Network

2. Web Site is a collection of _____.

(a) Audio and video files

(b) Pictures

(c) Web pages

(d) All of the above

Ans: (d) All of the above

3. DNS is an acronym for _____.

(a) Domain Name Security

(b) Domain Number System

(c) Document Name System

(d) Domain Name System

Ans: (d) Domain Name System

4. _____protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
   (a) FTP
   (b) TCP/IP
   (c) HTTP
   (d) SMTP
   Ans: (c) HTTP

5. _____ is an applications which is used at low price to a level where capabilities of video conference and instant messages over the we(b)
   (a) ISD
   (b) Skype, Gtalk
   (c) Yahoo
   (d) AOL
   Ans: (b) Skype, Gtalk

6. Internet protocols include _____.
   (a) Ethernet
   (b) ARCnet
   (c) MAC
   (d) TCP/IP
   Ans: (d) TCP/IP

7. The centralized authority known as _____, which is responsible for assigning a unique number known as IP(Internet Protocol) address.
   (a) Internet Protocol (IP)
   (b) Internet Assigned Numbers Authority (IANA)
   (c) Uniform Resource Locator (URL)
   (d) Regional Internet Registries (RIRs)
   Ans: (b) Internet Assigned Numbers Authority (IANA)

8. _____ is the example of rootname servers of the DNS of the Internet.
   (a) VeriSign Global Registry Services
   (b) DNS top-level domains (TLD)
   (c) Internet Service Provider (ISP)
   (d) Number Resource Organization (NRO)
   Ans: (a) VeriSign Global Registry Services

9. _____, as the name suggests, in a network of network and it is a collection of several small, medium and large networks.
   (a) Internet
   (b) HTTP protocol
   (c) Internet Service Provider (ISP)
   (d) Personal Digital Assistants (PDAs)
   Ans: (a) Internet

10. _____is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc.
   (a) Internet
   (b) Cyber Crime
   (c) Internet Service Provider (ISP)
   (d) IT architecture
   Ans: (b) Cyber Crime

11. In 1981s, National Science Foundation (NFS) developed _____ and was connected to ARPANET using TCP/IP protocol suite.
   (a) Computer Science Network (CSNET)
   (b) NFSNET
   (c) National Research and Education Network (NREN)
   (d) Internet Assigned Numbers Authority (IANA)
   Ans: (a) Computer Science Network (CSNET)

12. An IP address consists of two parts, which are _____.

    (a) Internet

    (b) Network and Host

    (c) IP addresses

    (d) Two Regional Internet Registries

    Ans: (b) Network and Host

13. Cyber-crime can be categorized into _____ types.

    (a) 4

    (b) 3

    (c) 2

    (d) 6

    Ans: (c) 2

14. NAP is an acronym for _____.

    (a) Network Assign Points

    (b) Network Access Points

    (c) Not a Problem

    (d) Node Access Point

    Ans: (b) Network Access Points

15. System in a computer which translates an IP address into an easier name is called _____ .

    (a) Packet-Switching Domain System

    (b) Domain Name System

    (c) Domain

    (d) Domain Numbering System

    Ans: (b) Domain Name System

16. In 1980s, from causing the physical damaging to computers to making a computer malfunction using a malicious code called _____.
    (a) cyber crime
    (b) web browser
    (c) Domain
    (d) virus
    Ans: (d) virus

17. The web pages are access using a application software called a _____.
    (a) Web pages
    (b) Internet
    (c) Web browser
    (d) Websites
    Ans: (c) Web browser

18. _____ is a malicious code that is installed in the host machine by pretending to be useful software.
    (a) Worms
    (b) Virus
    (c) Trojan horse
    (d) Browser hijacking software
    Ans: (c) Trojan horse

19. The term _____ is used to describe an attack to the network or the computer system by some person with authorized system access.
    (a) Insider attack
    (b) External Attack
    (c) Intrusion
    (d) IP address
    Ans: (a) Insider attack

20. The insider attack can be prevented by planning and installing an Internal _____ in the organization.
    (a) External Attack
    (b) Intrusion Detection Systems
    (c) Intrusion
    (d) IT architecture
    Ans: (b) Intrusion Detection Systems

21. When the attacker is either hired by an insider or an external entity to the organization, it is known as _____.
    (a) External Attack
    (b) Insider Attack
    (c) Cyber Crimes
    (d) IT architecture
    Ans: (b) Intrusion Detection Systems

22. Malware stands for _____ and it is designed to gain access or installed into the computer without the consent of the user.
    (a) Malicious Software
    (b) Host Machine
    (c) Cyber Crimes
    (d) Remote Servers
    Ans: (a) Malicious Software

23. _____ is a special type of malware which is used to financially support by the organizations whose products are advertised.
    (a) Malicious Software
    (b) Adware
    (c) Spyware
    (d) Freeware
    Ans: (b) Adware

24. The term _____, describes a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine.
    (a) Malicious Software
    (b) Adware
    (c) Spyware
    (d) Freeware
    Ans: (c) Spyware

25. _____are a class of virus which can replicate themselves.
    (a) Worms
    (b) Adware
    (c) Spyware
    (d) Virus
    Ans: (a) Worms

26. Which of the following is not a type of cyber-crime?
    (a) Data theft
    (b) Unauthorized account access
    (c) Email spoofing and spamming
    (d) Installing antivirus for protection
    Ans: (d) Installing antivirus for protection

27. Which type of malware replicates itself in order to spread to other computers?
    (a) Virus
    (b) Trojens
    (c) Adware
    (d) Spyware
    Ans: (b) Trojens

28. botnet is an acronym for _____.

(a) Robot-Network

(b) Bottle Network

(c) Robotics Netwrok

(d) Road Network

Ans: (d) Domain Name System

29. The term _____, defines an act of stalking, harassing or threatening someone using Internet/computer as a medium.

(a) Cyber Stalking

(b) Cyber Crimes

(c) Scareware

(d) Malicious

Ans: (a) Cyber Stalking

30. If a telephone is used as a medium for identity theft, it is known as _____.

(a) Cyber Stalking

(b) Vishing

(c) Scareware

(d) Malicious

Ans: (b) Vishing

31. _____ defines a practice of modifying computer hardware and software to accomplish a goal outside the creator's original purpose.

(a) Cyber Stalking

(b) Vishing

(c) Computer Hacking

(d) Malicious

Ans: (c) Computer Hacking

32. The hackers can be categorized into _____ types.

(a) 4

(b) 3

(c) 2

(d) 6

Ans: (a) 4

33. A white hat hacker also referred to as _____.

(a) spamming

(b) Ethical hackers

(c) Black hat hackers

(d) Anonymity hackers

Ans: (b) Ethical hackers

34. The term _____ refers the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations to protect the system from outside hackers.

(a) White hat hackers

(b) Crackers

(c) Black hat hackers

(d) Anonymity hackers

Ans: (a) White hat hackers

35. A Black Hat hacker also referred to as _____.

(a) Crackers

(b) Ethical hackers

(c) White hat hackers

(d) Anonymity hackers

Ans: (a) Crackers

36. _____ type of hack, which is to hack the system for social, political or economically motivated intentions.
    (a) Black Hat hackers
    (b) Ethical hackers
    (c) White hat hackers
    (d) Anonymity hackers
    Ans: (a) Black Hat hackers

37. Sending of unsolicited and commercial bulk message over the internet is known as _____.
    (a) Black Hat hackers
    (b) Grey Hat hackers
    (c) Spamming
    (d) Blue hat hackers
    Ans: (c) Spamming

38. An email can be classified as spam, if it meets following criteria:
    (A) Mass mailing (B) Anonymity C. Unsolicited
    (a) A & B
    (b) A & C
    (c) A Only
    (d) A, B & C
    Ans: (d) A, B & C

39. _____is an activity which involves injecting a malicious client side script into a trusted website.
    (a) Cross Site Scripting
    (b) Mailbox
    (c) Spams
    (d) Remote Servers
    Ans: (a) Cross Site Scripting

40. If the browser executes _____ the malicious script, the malicious script gets access to the cookies and sensitive information to gain financial benefit or physical access to a system for personal interest.
    (a) Cross Site Scripting (XSS)
    (b) Online Auction Fraud
    (c) Cyber Squatting
    (d) Logic Bombs
    Ans: (a) Cross Site Scripting (XSS)

41. The examples of web jacking are.
    A. Indian hackers hacked website of Pakistani railways and flashed Indian flag in the Home page for several hours
    (B) Online Auction Fraud
    C. An attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner.
    (a) A Only
    (b) A & B
    (c) C Only
    (d) A, B & C
    Ans: (a) A Only

42. Identify the techniques for two-factor authentication _____.
    (a) Biometric data
    (b) One Time Password (OTP)
    (c) SMS
    (d) Registration Process
    Ans: (a) Biometric data

43. _____ defines a process of identifying an individual and ensuring that the individual is the same who he/she claims to be.
    (a) Biometric data
    (b) One Time Password (OTP)
    (c) Authentication
    (d) Registration Process
    Ans: (c) Authentication

44. VPN Stands for _____.
    (a) Virtual Private Node
    (b) Virtual Public Network
    (c) Virtual Private Network
    (d) Visual Public Network
    Ans: (c) Virtual Private Network

45. _____ is a technique to convert the data in unreadable form before transmitting it over the internet.
    (a) Encryption
    (b) Key distribution
    (c) Decryption
    (d) Digital Signatures
    Ans: (a) Encryption

46. If the same key is used to lock and unlock the data, it is known as _____encryption.
    (a) Encryption
    (b) Symmetric Key
    (c) Decryption
    (d) Public Key
    Ans: (b) Symmetric Key

47. What are the two main types of encryption?

(a) Encryption and Public Key

(b) Symmetric and Asymmetric Encryption

(c) Encryption and Decryption

(d) Public and Private Key

Ans: (b) Symmetric and Asymmetric Encryption

48. _____defines a process of certifying the content of a document.

(a) Authentication

(b) Validation

(c) Re-encrypted

(d) Signature

Ans: (b) Validation

49. Which device is example for hardware firewall?

(a) Routers

(b) Software

(c) Server

(d) Client

Ans: (a) Routers

50. _____is a branch of science which deals with tools and techniques for investigation of digital data to find evidences against a crime which can be produced in the court of law.

(a) Cyber Attack

(b) Cyber Forensic

(c) Cyber Crime

(d) Report

Ans: (b) Cyber Forensic

51. NCCC stands for _____.
    (a) National Cyber Coordination Centre
    (b) National Cyber Crime Centre
    (c) National Crime and Criminal Centre
    (d) National Critical Criminal Centre
    Ans: (a) National Cyber Coordination Centre

52. As a part of the Digital India programme, the Government is setting up a _____Center that will detect malicious programmes and remove such harmful software from their devices.
    (a) National Cyber Coordination Centre
    (b) Botnet Cleaning Center
    (c) India Information Sharing and Analysis Centre
    (d) Data Security Council of India
    Ans: (b) Botnet Cleaning Center

53. NCRB is an acronym for _____.
    (a) National Crime Records Bureau
    (b) National Crime Report Bureau
    (c) National Cyber Report Bureau
    (d) Network Crime Records Bureau
    Ans: (a) National Crime Records Bureau

54. _____ is a Web-based, open source password manager built to store login information securely.
    (a) Security
    (b) Clipperz
    (c) Personal Manager
    (d) Locker
    Ans: (b) Clipperz

55. _____ is a type of free anti-virus software and its common features which for online security.

(a) Security

(b) Threatfire Lite

(c) Personal Manager

(d) Gmail account

Ans: (b) Threatfire Lite

56. What are the two main Firewall in “Windows 7” that work together?

(a) Windows Firewall and Windows Media Player

(b) Windows Firewall Lite and Windows Firewall with Security

(c) Windows Firewall and Windows Firewall with Advanced Security (WFAS)

(d) Windows 7 and Firewall

Ans: (c) Windows Firewall and Windows Firewall with Advanced Security (WFAS)

57. When the user first connect to some network, user prompted to select a network location such a feature is known as _____.

(a) Network Location Awareness (NLA)

(b) Firewall Rules

(c) Control Panel

(d) Active Directory domain

Ans: (a) Network Location Awareness (NLA)

58. Operating Systems includes _____.

(a) Google

(b) Linux

(c) Gmail Account

(d) Windows Firewall

Ans: (b) Linux

59. When the browser opens a secured connection, _____ can be seen in the URL instead of http.

(a) https

(b) TCP/IP

(c) URL

(d) secure

Ans: (a) https

60. _____ is a computer maintenance tool that can scan and delete browser cache and cookies.

(a) Browser

(b) Ccleaner

(c) URL

(d) Opera

Ans: (b) Ccleaner

61. WLAN is an acronym for _____.

(a) Wireless LAN

(b) Wired LAN

(c) Wire LAN

(d) With LAN

Ans: (a) Wireless LAN

62. In cyber law terminology ‘DoS’ stands for _____

(a) Denial of Secure

(b) Denied of Service

(c) Denial of Service

(d) Document of Service

Ans: (c) Denial of Service

63. Wi-Fi can provide more secure ways to communicate with people, by using VoIP

(a) VoIP

(b) VPN

(c) AP

(d) FOSS

Ans: (a) VoIP

64. The most popular commercial VoIP application, _____, is available for all smartphone platforms and works well if wireless connectivity is reliable.
    (a) Skype
    (b) SMS
    (c) Open Source
    (d) SIM
    Ans: (a) Skype

65. _____ is a Free and Open-Source Software application that encrypts voice communication data sent between two devices that run this application.
    (a) Skype
    (b) RedPhone
    (c) VoIP
    (d) SIM
    Ans: (b) RedPhone

66. What software is used to protect computers against viruses?
    (a) Antivirus
    (b) Disk defragmenter
    (c) Disk cleanup
    (d) Backup wizard
    Ans: (a) Antivirus

67. Which of the following is known as Malicious software?
    (a) maliciousware
    (b) illegalware
    (c) badware
    (d) malware
    Ans: (d) malware

68. An example of an IP address is _____.
    (a) 11110110.01011010.10011100.1111100
    (b) 11111111
    (c) 00000000

(d) 10101100

Ans: (a) 11110110.01011010.10011100.1111100

69. An example of an URL is _____.

(a) abcd101a

(b) http:\\www.uou.ac.in.

(c) www.abc

(d) 10101100

Ans: (b) http:\\www.uou.ac.in.

70. VIRUS stands for _____.

(a) Very Intelligent Result Until Source

(b) Vital Information Resource Under Slege

(c) Viral Important Record User Searched

(d) Very Interchanged Resource Under Search

Ans: (b) Vital Information Resource Under Slege

71. Which of the following is not an antivirus software?

(a) AVG

(b) Avast

(c) BitDefender

(d) Code Red

Ans: (d) Code Red

72. Which of the following is/are threats for electronic payment systems?

(a) Computer virus

(b) Trojan horse

(c) Computer worms

(d) All of the above

Ans: (d) All of the above

73. Firewalls are used to protect against _____.

(a) Virus attacks

(b) Fire attacks

(c) Unauthorised access

(d) Data Driven attacks

Ans: (c) Unauthorised access

74. _____ are used in denial of service attacks, typically against targeted web sites.

(a) Trojan horse

(b) Zombie

(c) Worm

(d) Virus

Ans: (b) Zombie

75. Social engineering is _____.

(a) A website created for people who share common interests

(b) Scams distributed through email such as phishing, pharming and impersonation

(c) A targeted attack on a personal computer

(d) None of the above

Ans: (b) Scams distributed through email such as phishing, pharming and impersonation

76. Another form of phishing is Smishing _____.

(a) Cyber Terrorism

(b) Smishing

(c) Vandalism

(d) None of the above

Ans: (b) Smishing

77. Unsolicited commercial E-mail is knows as _____.

(a) Spam

(b) Malware

(c) Virus

(d) Spyware

Ans: (a) Spam

78. _____ Refers to email that appears to have been originated from one source when it wasactually sent from another source.

(a) Email bombing

(b) Email spoofing

(c) Email spamming

(d) None of these

Ans: (b) Email spoofing

79. _____ refers to sending email to thousands and thousands of users-similar to a chainletter.

(a) Email bombing

(b) Email spoofing

(c) Email spamming

(d) None of these

Ans: (c) Email spamming

80. Vishing is mean for _____.

(a) SMS phishing

(b) Voice phishing

(c) Phishing

(d) All the above

Ans: (b) Voice phishing

81. What type of symmetric key algorithm using a streaming cipher to encrypt information?

(a) RC4

(b) Blowfish

(c) SHA

(d) MD5

Ans: **(a)** RC4

82. To hide information inside a picture, what technology is used?

(a) Rootkits

(b) Bitmapping

(c) Steganography

(d) Image Rendering

Ans: (c) Steganography

83. What is the purpose of a Denial of Service attack?

(a) Exploit a weakness in the TCP/IP stack

(b) To execute a Trojan on a system

(c) To overload a system so it is no longer operational

(d) To shutdown services by turning them off

Ans: (c) To overload a system so it is no longer operational

84. The first phase of hacking an IT system is compromise of which foundation of security?

(a) Availability

(b) Confidentiality

(c) Integrity

(d) Authentication

Ans: (b) Confidentiality

85. Phishing is a form of _____.

(a) Spamming

(b) Identify Theft

(c) Impersonation

(d) Scanning

Ans: (c) Impersonation

86. keyloggers are a form of _____.

(a) Spyware

(b) Shoulder surfing

(c) Trojan

(d) Social engineering

Ans: (a) Spyware

87. Firewalls are to protect against

(a) Virus Attacks

(b) Fire Attacks

(c) Data Driven Attacks

(d) Unauthorized Attacks

Ans: (d) Unauthorized Attacks

88._____ is a code injecting method used for attacking the database of a system / website.

(a) HTML injection

(b) SQL Injection

(c) Malicious code injection

(d) XML Injection

Ans: (b) SQL Injection

89. There are _____ types of cryptographic techniques used in general.

(a) 2

(b) 3

(c) 4

(d) 5

Ans : (b) 3

90. Which 2 protocols are used in the Transport layer of the TCP/IP model?

(a) UDP and HTTP

(b) TCP and UDP

(c) HTTP and TCP

(d) ICMP and HTTP

Ans : (b) TCP and UDP

91. Which of the protocol is not used in the network layer of the TCP/IP model?

(a) ICMP

(b) IP

(c) IGMP

(d) HTTP

Ans: (d) HTTP

92. _____ protocol attack is done in the data-link layer.

(a) HTTP

(b) TCP/IP

(c) DNS

(d) POP

Ans : (c) DNS

93. Which of the following is not an example of a block cipher?

(a) DES

(b) IDEA

(c) Caesar cipher

(d) Twofish

Ans: (c) Caesar cipher

94. DES stands for _____

(a) Data Encryption Security

(b) Data Encrypted Standard

(c) Device Encryption Standard

(d) Data Encryption Standard

Ans: (d) Data Encryption Standard

95. _____ refers to phishing performed over smart-phone by calling.

(a) Algo-based phishing

(b) Email-based phishing

(c) Domain Phishing

(d) Vishing

Ans: (d) Vishing

96. Which of the following is not an example or type of phishing?

(a) Tracking

(b) Vishing

(c) Smishing

(d) Pharming

Ans: (a) Tracking

97. A cryptosystem is also termed as _____

(a) secure system

(b) cipher system

(c) cipher-text

(d) secure algorithm

Ans: (b) cipher system

98. _____ takes the plain text and the key as input for creating cipher-text.

(a) Decryption Algorithm

(b) Hashing Algorithm

(c) Tuning Algorithm

(d) Encryption Algorithm

Ans: (a) Decryption Algorithm

99. Encryption-decryption in cryptosystem is done in _____ ways.

(a) 4

(b) 3

(c) 5

(d) 2

Ans: (d) 2

100. _____ attack is the exploitation of the web-session & its mechanism that is usually managed with a session token.

(a) Session Hacking

(b) Session Hijacking

(c) Session Cracking

(d) Session Compromising

Ans: (b) Session Hijacking

101. There are _____ types of session hijacking.

(a) 2

(b) 3

(c) 4

(d) 5

Ans: (a) 2

102. _____ framework made cracking of vulnerabilities easy like point and click.

(a) .Net

(b) Metasploit

(c) Zeus

(d) Ettercap

Ans: (b) Metasploit

103. Nmap is abbreviated as Network Mapper.

(a) True

(b) False

Ans: (a) True

104. _____ is a popular tool used for discovering networks as well as in security auditing.

(a) Ettercap

(b) Metasploit

(c) Nmap

(d) Burp Suit

Ans: (c) Nmap

105. Which of this Nmap do not check?
(a) services different hosts are offering
(b) on what OS they are running
(c) what kind of firewall is in use
(d) what type of antivirus is in use
Ans: (d) what type of antivirus is in use

106. Which of the following deals with network intrusion detection and real-time traffic analysis?
(a) John the Ripper
(b) L0phtCrack
(c) Snort
(d) Nessus
Ans: (c) Snort

107. Wireshark is a _____ tool.
(a) Network protocol analysis
(b) Network connection security
(c) Connection analysis
(d) Defending malicious packet-filtering
Ans: (a) Network protocol analysis

108. Which of the below-mentioned tool is used for Wi-Fi hacking?
(a) Wireshark
(b) Nessus
(c) Aircrack-ng
(d) Snort
Ans: (c) Aircrack-ng

109. Aircrack-ng is used for _____
(a) Firewall bypassing
(b) Wi-Fi attacks

(c) Packet filtering

(d) System password cracking

Ans: (b) Wi-Fi attacks

110. _____ is a popular IP address and port scanner.

(a) Cain and Abel

(b) Snort

(c) Angry IP Scanner

(d) Ettercap

Ans: (c) Angry IP Scanner

111. _____ is a popular tool used for network analysis in multiprotocol diverse network.

(a) Snort

(b) SuperScan

(c) Burp Suit

(d) EtterPeak

Ans: (d) EtterPeak

112. _____ scans TCP ports and resolves different hostnames.

(a) SuperScan

(b) Snort

(c) Ettercap

(d) QualysGuard

Ans: (a) SuperScan

113. _____ is a web application assessment security tool.

(a) LC4

(b) WebInspect

(c) Ettercap

(d) QualysGuard

Ans: (b) WebInspect

114. Which of the following attack-based checks WebInspect cannot do?

(a) cross-site scripting

(b) directory traversal

(c) parameter injection

(d) injecting shell code

Ans: (d) injecting shell code

115. _____ is a password recovery and auditing tool.

(a) LC3

(b) LC4

(c) Network Stumbler

(d) Maltego

Ans: (b) LC4

116. L0phtCrack is formerly known as LC3.

(a) True

(b) False

Ans: (b) False

117. _____ is a code injecting method used for attacking the database of a system / website.

(a) HTML injection

(b) SQL Injection

(c) Malicious code injection

(d) XML Injection

Ans: (b) SQL Injection

118. This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

(a) SQL injection

(b) HTML Injection

(c) Cross Site Scripting (XSS)

(d) Cross Site Request Forgery (XSRF)

Ans: (c) Cross Site Scripting (XSS)

119. An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

(a) Cyber-crime

(b) Cyber Attack

(c) System hijacking

(d) Digital crime

Ans: (b) Cyber Attack

120. _____ are the special type of programs used for recording and tracking user's keystroke.

(a) Keylogger

(b) Trojans

(c) Virus

(d) Worms

Ans: (a) Keylogger

121. Stuxnet is a _____

(a) Worm

(b) Virus

(c) Trojan

(d) Antivirus

Ans: (a) Worm

122. The first computer virus is --------

(a) I Love You

(b) Blaster

(c) Sasser

(d) Creeper

Ans: (d) Creeper

123. MCAfee is an example of

(a) Photo Editing Software

(b) Quick Heal

(c) Virus

(d) Antivirus

Ans: (d) Antivirus

124. Which of the following is known as Malicious software?

(a) illegalware

(b) badware

(c) malware

(d) maliciousware

Ans: (c) malware

125. To protect a computer from virus, you should install -------- in your computer.

(a) backup wizard

(b) disk cleanup

(c) antivirus

(d) disk defragmenter

Ans: (c) antivirus

126. VIRUS stands for

(a) Very Intelligent Result Until Source

(b) Very Interchanged Resource Under Search

(c) Vital Information Resource Under Slege

(d) Viral Important Record User Searched

Ans: (c) Vital Information Resource Under Slege

127. Which of the following is not an antivirus software?

(a) AVG

(b) Avast

(c) Code Red

(d) MCAfee

Ans: (c) Code Red

128. What is short for malicious software (is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems)?

(a) Malware

(b) Moleculewar

(c) Malisoft

(d) Malairasoft

Ans: (a) Malware

129. Which of the following is/are threats for electronic payment systems?

(a) Computer worms

(b) Computer virus

(c) Trojan horse

(d) All of the above

Ans: (d) All of the above

130. Which of the following virus overtake computer system, when it boots and destroy information?

(a) System infectors

(b) Trojan

(c) Boot infectors

(d) Stealth virus

Ans: (d) Stealth virus

131. Key logger is a

(a) Firmware

(b) Antivirus

(c) Spyware

(d) All of the above

Ans: (c) Spyware

132. To protect yourself from computer hacker, you should turn on a

(a) Script

(b) Firewall

(c) VLC

(d) Antivirus

Ans: (b) Firewall

133. Firewalls are used to protect against --------

(a) data driven attacks

(b) fire attacks

(c) virus attacks

(d) unauthorised access

Ans: (d) unauthorised access

134. Which of the following would most likely not be a symptom of a virus?

(a) The web browser opens to an unusual home page

(b) Odd message or images are displayed on the screen

(c) Existing program files and icons disappear

(d) The CD–ROM stops functioning

Ans: (d) The CD–ROM stops functioning

135. Code red is a(n) ----------

(a) Word Processing Software

(b) Antivirus

(c) Virus

(d) Photo Editing Software

Ans: (c) Virus

136. -------- software are programs that are installed onto your computer and can scan and remove known viruses which you may have contracted.

(a) Firmmware

(b) Adware

(c) Keylogger

(d) Antivirus

Ans: (d) Antivirus

137. Which of the following describes programs that can run independently travel from system to system and disrupt computer communication?
(a) Viruses
(b) Trojans
(c) Droppers
(d) Worm
Ans: (d) Worm

138. A -------- is a computer program that can replicate itself and spread from one computer to another.
(a) Antivurs
(b) PenDrive
(c) Mouse
(d) Computer Virus
Ans: (d) Computer Virus

139. Authentication is
(a) modification
(b) insertion
(c) hard to assure identity of user on a remote system
(d) none of the above
Ans: (c) hard to assure identity of user on a remote system

140. -------- are attempts by individuals to obtain confidential information from you to falsifying their identity.
(a) Computer viruses
(b) Phishing scams
(c) Phishing trips
(d) Spyware scams
Ans: (b) Phishing scams

141. A virus that migrates freely within a large population of unauthorized email user is called a -------
(a) flame war

(b) worm
(c) macro
(d) plagiarism
Ans: (c) macro

142. -------- are often delivered to a PC through an email attachment and are often designed to do harm.
(a) Spam
(b) Email
(c) Portals
(d) Virus
Ans: (d) Virus

143. The altering of data so that it is not usable unless the changes are undone is
(a) ergonomics
(b) compression
(c) biometrics
(d) encryption
Ans: (d) encryption

144. When a logic bomb is activated by a time related event, it is known as -------
(a) virus
(b) trojan horse
(c) time related bomb sequence
(d) time bomb
Ans: (d) time bomb

145. A ------- is a computer program that can invade computer and perform a variety of functions ranging from annoying (e.g. popping up messages as a joke) to dangerous (e.g. deleting files or destroying your hard disk).
(a) Ms Word
(b) Ms Access
(c) Antivirus
(d) Computer Virus

Ans: (d) Computer Virus

146. Cybersecurity is primarily about?
(a) people
(b) processes
(c) technologies
(d) All of the above
Ans: (d) All of the above

147. Cybersecurity encompass the full range of?
(a) vulnerability reduction
(b) incident response
(c) recovery policies
(d) All of the above
Ans: (d) All of the above

148. Cybersecurity is the protection of?
(a) Internet connected systems
(b) Non-Internet connected systems
(c) Both A and B
(d) None of the above
Ans: (a) Internet connected systems

149. Cybersecurity also be referred to as?
(a) incident security
(b) information technology security
(c) internet security
(d) threat security
Ans: (b) information technology security

150. What is true about cybersecurity?
(a) cybersecurity as the set of principles and practices designed to protect our computing resources

(b) cybersecurity as the set of principles and practices designed to protect our online information against threats

(c) cybersecurity is a critical function and needed insurance of many businesses.

(d) All of the above

Ans: (d) All of the above

151. In which year, the first computer worm (virus) created?

(a) 1969

(b) 1970

(c) 1971

(d) 1972

Ans: (b) 1970