

**END TERM EXAMINATION
EIGHTH SEMESTER 2015-16
HUL-2401 – Cyber Security**

Time allowed: 3 Hrs.**Max. Marks: 100****General Instructions :**

1. All questions are compulsory
2. Each question carry one mark
3. There is no negative marking

1. In computer security, means that computer system assets can be modified only by authorized parties.

- A) Confidentiality B) Integrity C) Availability D) Authenticity

2. In computer security, means that the information in a computer system only be accessible for reading by authorized parties.

- A) Confidentiality B) Integrity C) Availability D) Authenticity

3. Which of the following is independent malicious program that need not any host program?

- A) Trap doors B) Trojan Horse C) Virus D) Worm

4. The Is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by unlikely sequence of events?

- A) Logic Bomb B) Virus C) Trojan Horse D) Trap doors

5. The is code embedded in some legitimate program that is set to "explode" when certain conditions are met.

- A) Logic Bomb B) Trap doors C) Virus D) Trojan Horse

6. Which of the following malicious program do not replicate automatically?

- A) Trojan Horse B) Virus C) Worm D) Zombie

7. programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.

- A) Zombie B) Trojan Horses C) Worm D) Logic Bomb

8. A is a program that can infect other programs by modifying them, the modification includes a copy of the virus program, which can go on to infect other programs.

- A) Worm B) Zombie C) Virus D) Trap doors

9. Which of the following does NOT use a 'Cryptographically Technique' to protect data?

- A) the use of digital signatures B) data encryption C) the use of stored encrypted password files D) using asymmetric keys at 'sender' and 'receiver' nodes

10. Which of the following crimes is done using a computer as the instrument ?

- A) Computer Manipulation B) Money Laundering C) Data Alteration D) Theft of services

11. are software programs installed on a computer system which usually are located between OS and keyboard hardware to record every key stroke.

- A) Keystroke B) PC key logger C) Software Key Logger D) Anonymizer

12. They used readymade software or application to hack a computer.

- A) Hacker B) Cracker C) Script kiddies D) Phreakers

13. In which year Information Technology Act was implemented in India.

- A)2013 B)2000 C)2015 D)2003
14. _____ mail is also known as junk mail
- A)Spoof B)Spam C)Fake D)Fraud
15. _____ is a science of changing information into unintelligible form.
- A) Cryptography B) Steganography C) Password diving D) None of them
16. _____ is a fraud involving another person's identity for an illegal purpose.
- A) Password Sniffing B) Internet Time Theft C) Identity Theft D) Salami
17. _____ involves altering raw data just before it is processed by computer.
- A) Data Diddling B) Forgery Attack C) Salami Attack D) None of them
18. Which of the following is purpose of Hacking:
- A) Greed B) Revenge C)) Passion D) All of them
19. Which of the following terms best describes data that is to be encrypted?
- A) Text B) Cipher Text C) Plain text D) Cryptography
20. First Cybercrime was recorded in _____
- A) 1820 B) 1880 C) 1940 D) 2004
21. 'Cyber' is a prefix derived from:
- A) cybernoc B) cybercell C) cybermatic D) cybernetic
22. First virus was installed on _____ computer in 1982.
- A) Apple B) Microsoft C) Google D) IBM
23. Any information being subject to human action or not, that can be extracted from a computer.
- A) Digital Evidence B) Analog Evidence C) Physical Evidence D) Logical Evidence
24. _____ Uses Computer Forensics.
- A) Corporations B) Insurance Companies C) Criminal Prosecutors D) All of them
25. Which of the following is the reason for Computer Forensic:
- A) Forgery B) Virus C) Fraud D) All of them
26. Computer/Cyber Crime is a _____ Technique.
- A) Social B) Corporate C) Socio-Technical D) General
27. Recovering Deleted, Encrypted and Damaged data is known as:
- A) Cyber Security B) Computer Forensic C) Physical Security D) None of them
28. Hashing algorithm protects which of the following characteristic of the Cryptographic.
- A) Availability B) Integrity C) Confidentiality D) Authenticity
29. Transposition stream cipher uses which of the following technology:
- A) Replace the character B) Rearrange the letters C) Substitute the character D) None of them
30. Keyword searching service provided by:
- A) Computer Crime B) Cyber security C) Cyber criminals D) Computer forensics
31. In Block Cipher plain content can be divided into which of the following block:
- A) 16 Bytes B) 26 Bytes C) 6 Bytes D) All of them
32. Asymmetric Encryption algorithm protects

A) Confidentiality B) Integrity C) Availability D) All of them

33. _____ is a kind of malware whose presence is typically hidden from the user.

A) Spyware B) Logic Bomb C) Key Logger D) Anonymizer

34. When someone takes control of your website consider as

A) Salami B) Web Jacking C) Spoofing D) Data Diddling

35. _____ mail is one that originate from one source but actually has been sent from another source.

A) Spam B) Fake C) Spoof D) Fraud

36. Computer program that lies dormant and triggered on a event on a particular day is:

A) Virus B) Worm C) Logic Bomb D) Trojan Horse

37. CGA stand for

A) Cryptographically granted Access B) Cryptographically generated address C) Cryptographically granted Address D) None of them

38. Which of the following describes crime that is not reported to the police and that remains unknown to officials?

A) Dark figure of crime B) Light figure of crime C) Cyber stalking D) Crime typology

39. Which of the following describes unlawful activity undertaken and supported by organized criminal groups operating across national boundaries?

A) Malware B) Transnational organized crime C) Computer crime D) Corporate crime

40. Which of the following describes malicious computer programs such as viruses, worms, and Trojan horses?

A) Arson B) Software Piracy C) Malware D) Larceny

41. Which of the following is unsolicited commercial bulk email whose primary purpose is the commercial advertisement or promotion of a commercial product or service?

A) Cyber terrorism B) Terrorism C) Spam D) Malware

42. is to protect data and passwords.

A) Encryption B) Authentication C) Authorization D) Non-repudiation

43. SSID stands for _____

A) Service Set ID B) Service Set Identifier C) System Service Identifier D) None of the above

44. The idea behind this attack is to deduct a small amount of money which would go completely unnoticed in a first sight.

A) Salami B) Data Diddling C) Web Jacking D) Spoofing

45. WEP stands for

A) Wireless Equivalent Privacy B) Wired Equivalent Protocol C) Wireless Equivalent Protocol D) None of them

46. Which of the following is used to send secure messages from one location to another using a public network such as the Internet?

A) Physical Public Network B) Virtual Public Network C) Physical Private Network D) Virtual Private Network

47. Which of the following is/are methods of providing secure communication between two entities through the use of mathematical coding?
- A) Private key encryption B) Public key encryption C) Digital Signature encryption D) All of the above
48. Which term best describes the type of attack that makes it seem like two computers are communicating with each other, when actually they are sending and receiving data with a computer between them?
- A) Spoofing B) Man in Middle C) Middle Man D) None of them
49. A software defect is considered as
- A) Risk B) Threat C) Vulnerability D) Asset
50. In this technique attacker often launches an attack on wireless network by creating a new network with strong signal strength.
- A) Sniffing B) Man in the Middle C) DoS D) Spoofing
51. What has become more important because of the increased use of computers, the internet and WWW.
- A) Natural Disasters B) Data integrity and data security C) Hardware Malfunctions D) Malicious deletions
52. What can a firewall protect against?
- A) Viruses B) fire C) connecting to and from the "outside" world D) unauthenticated interactive logins from the "outside" world
53. Which of the following methods can effectively be used to prevent logical breach of security?
- A) Operating system and other system software design B) Distributed systems design C) Network design D) computer architectural design
54. _____ is the criminal practice of using social engineering over telephone system.
- A) Smishing B) Vishing C) Phishing D) Mishing
55. _____ is an art of detecting messages that are hidden in images, audio/video files.
- A) Steganography B) Cryptanalysis C) Cryptography D) Steganalysis
56. An attempt to make a computer resource unavailable to its intended users is called
- A) Botnet process B) DoS attack C) Virus attack D) worms attack
57. _____ is the criminal practice of using social engineering using SMS service
- A) Smishing B) Vishing C) Mishing D) Phishing
58. _____ is a technique of changing an assigned Media Access Control address of a network Interface card to a different one
- A) MAC Filtering B) MAC Spoofing C) IP Filtering D) IP Spoofing
59. The attacker usually installs the sniffers on the wireless network and conduct activities such as:
- A) Collecting MAC address B) Detection of SSID C) Collecting frame to crack WEP D) All of them
60. This must be used to protect from a SQL injection attack
- A) Modify error report B) Input Validation C) Isolate servers D) All of them
61. In this attack a query is sent to the database to check if a user has valid name and password.
- Brute Force attack B) SQL injection attack C) Password Guessing D) Dictionary attack
62. In this technique hundreds or thousands of zombie computers are used to flood a device with requests.
- A) Buffer Overflow B) DDoS C) Man in Middle D) DoS
63. This type of attack involves inquiring the network to discover host(s) to confirm information
- A) Active reconnaissance B) Active attack C) Rattling the doorknobs D) All of them
64. Purpose of a proxy server is _____.
- A) Keep System behind curtain B) Speed up access to a resource C) Both A and B D) None of them
65. This type of attack involves all possible permutation-combinations of letters, numbers and special characters to crack the password.
- A) Brute force attack B) Dictionary attack C) Hybrid attack D) Rainbow table attack
66. The program files as well as boot sector is infected with activation of this type of virus attack.

- A) Program virus B) Multipartite virus C) Boot sector virus D) Stealth virus
67. Which of the following accurately reflects the purpose of steganography?
- A) Steganography B) Steganography hides C) Steganography exposes D) Steganography
scrambles a message so the existence of the data. hidden data encrypts cleartext data
that it cannot be viewed
68. _____ scanning is to understand the existing weakness in the system.
- A) Port B) Vulnerability C) Network D) System
69. Program that is designed to take advantage of vulnerability in an application or an operating system to enter an application is known as
- A) Zombie B) Worm C) Trojan Horse D) Virus
70. In this technique attacker insert a new node between two existing nodes.
- A) Spoofing B) Sniffing C) Man in the Middle D) DoS
71. Which of the following attack is likely to result in Identity theft?
- A) Phishing attack B) Denial of Service attack C) Worm attack D) Virus infection
72. Virus is a computer _____.
- A) File B) Database C) Program D) Network
73. A software update to fix a security flaw or other problem is known as
- A) Repair B) Patch C) Exploit D) Hot Fix
74. _____ type of cookies could not be retained after the browser is closed
- A) Persistent cookies B) Session cookies C) Stored cookies D) None of them
75. A program advertised as performing one activity but actually doing something else, or performing both the advertised and malicious activities.
- A) Virus B) Zombie C) Trojan Horse D) Worm
76. Public Key Cryptography is Synonymous with
- A) Symmetric Key B) Private key C) Asymmetric key D) None of the above
Cryptography Cryptography Cryptography
77. Threats are categorized as:
- A) Passive or active B) Traffic C) Masquerade D) Others
78. This technology is used to measure and analyze human body characteristics for authentication purpose.
- A) Footprinting B) JBOD C) Biometric D) Anthropomorphism
79. In a SQL injection attack this command is used to retrieve data from a web page/web site.
- A) Get B) Post C) Select D) Retrieve
80. What is the difference between Data Integrity and Data Security?
- A) Limiting physical access B) Encryption; Audit trails C) Consistent, accurate D) Distributing work to
to computer systems; and reliable data; preserve integrity;
assigning passwords to protection of data from installing system
users. unauthorized access. passwords
81. In this phishing attack Phishers identify the victim in advance:
- A) Dragnet B) Lobsterpot C) Rod and reel D) Gilt net
82. How are viruses spread?
- A) Through Firewalls B) Downloading infected C) Garbled information D) Install anti-virus
programs and files from
internet.
83. If someone steal the source code of a game and sold it, is considered as violation of _____.
- A) Patent B) Trademark C) Trademark D) Copyright
84. Main purpose of a sniffer in a wireless network is to
- A) Detect SSID B) Collect MAC C) Collect frame to crack D) All of them
WEP
85. Gaining unauthorized access to a computer system would fall under which category of computer crime?
- A) Hacking B) Destruction of data & C) Theft of Services D) Data Theft

Software

86. _____ technique involves copying information of a debit/ credit card to create a duplicate card.
A) Traiangulation B) Traditional C) Modren D) None of them
87. Wireless network can be secured by
A) MAC address filtering B) Disbaling Mac filtering C) Disabling SSID D) All of them
88. This process involves blocking the access of a specific IP address.
A) IP Blocking B) IP Clocking C) Industry Espionage D) None of them
89. _____ can be used as IP address Multiplexer to enable to connect to number of computers on the internet
A) FTP Server B) Proxy Server C) Web Server D) None of these
90. Which among given is a Bluetooth hacking tool:
A) Bluejacking B) Car-Whispering C) Bluebugging D) All of them
91. What is the maximum header size of an IP packet?
A) 32 Bytes B) 30 Bytes C) 64 Bytes D) 62 Bytes
92. _____ attack is a computer threat which attempts to exploit computer application vulnerability that is unknown to anybody in the world.
A) Data Diddling B) Vulnerability C) Zero day D) None of the above
93. Dumpster diving is an example of
A) Phishing B) Fraud C) Social Engineering D) Cyber Stalking
94. A software update to fix a security flaw or other problem is known as
A) Repair B) Hot Fix C) Patch D) Exploit
95. Counterfeit websites are used by _____ to extract personal information.
A) Foistware B) Phreakers C) Heedless guests D) Stalkers
96. _____ is used by attackers to find the open port in a network
A) Vulnerability Scanner B) Port Scanner C) Network Scanner D) All of them
97. People who send multiple mails from zombie computers are known as
A) Spoofer B) Spies Kiddies C) Spammer D) Stalker
98. Which among these is used to track missing laptop(s).
A) Motion Sensor B) Labels C) Alarms D) All of them
99. In the realm of 'cyber attack', DDOS stands for
A) Distributed Destruction of System B) Damaging Downtime of System C) Digital Data Output Spoit D) None of them
100. When a service provider uses public cloud resources to create a private cloud is known as:
A) Public cloud B) Global cloud C) Private cloud D) Virtual cloud

End Term Exam

Semester-VIII

Roll No:

[Total No. of Pages:04]

Date:

Time: 180 minutes

Department:

Title of the Course: Cyber Security

Max. Marks: 100

Course Code: HUL 2401

Q1 Sam send a message Tim and Joe using same encryption key, at the receiving side Tim and Joe decrypt the message with the key used by Sam to encrypt the message is an example of _____.

- (a) Symmetric encryption (b) Hashing
(c) Asymmetric encryption (d) None of the above

Q2 _____ is a person who is ethically opposed to the abuse of computer systems.

- (a) White hat hacker (b) Red hat hacker
(c) Green hat hacker (d) Black hat hacker

Q3 Which among these is a feature of Hashing

- (a) Confidentiality (b) Availability
(c) Authenticity (d) None of these

Q4 _____ the first phase to commit a crime and is treated as passive attack

- (a) Scanning (b) Scrutinizing
(c) Reconnaissance (d) None of them

Q5 Which statement about virus attack is true

- A. Boot sector virus infects the storage media
B. Program virus is a hybrid virus
C. Stealth virus mask itself so detection is not easy
D. Multipartite virus target .exe files
(a) Both A and B (b) Both A and C
(c) Both A and D (d) None of them

Q6 In the right setting a thief will steal your information by sampling watching what you type.

- (a) Snagging (b) Spying
(c) Social Engineering (d) Shoulder surfing

Q7 _____ is the criminal practice of using social engineering over telephone.

- (a) Phishing (b) Mishing
(c) Vishing (d) Smishing

Q8 _____ attack is a computer threat which attempts to exploit computer application vulnerability that are unknown to anybody in the world.

- (a) Zerod day (b) Vulnerability
(c) Data Diddling (d) Salami

Q9 Which among given is a Bluetooth hacking tool?

- (a) Bluejacking (b) Blue bugging
(c) Car Whispering (d) All of them

Q10 In asymmetric cryptographic algorithm when Tom wants to send a message to Alisha he will decrypt it with

- (a) His Public Key (b) Public key of Alisha
(c) His Private Key (d) Private key of Alisha

Q11 Another name of Public Key Cryptography

- (a) Symmetric Key Cryptography
(b) Private key Cryptography
(c) Asymmetric key Cryptography
(d) None of the above

Q12 _____ are software programs installed on a computer system which usually are located between OS and keyboard hardware to record every key stroke

- (a) Key Stroker (b) Key Logger
(c) Software Key logger (d) Anonymizers

Q13 A destructive employee of a company installed a script in the server to take revenge from his employer and this is going to be executed after one week of the installation date is an example of:

- (a) Worm (b) Logic Bomb
(c) Virus (d) Trojan Horse

Q14 "Do no evil" is the motto of

- (a) Microsoft (b) Google
(c) Yahoo (d) Intel

Q15 Which term best describes the type of attack that makes it possible to deny the service of a server using multiple computers from different geographical locations?

- (a) Buffer Over flow (b) DoS
(c) Man in Middle (d) None of these

Q16 Which term best describes the type of attack that makes it seem like two computers are communicating with each other, when actually they are sending and receiving data with a computer between them?

- (a) Spoofing (b) Middle Man
(c) Bucket Brigade (d) Replay

Q17 A _____ is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks.

- (a) Worm (b) Zombie
(c) Virus (d) Trap doors

Q18 This type of attack involves gathering information about individual about his/her knowledge, for example which the IN and OUT time of an employee.

- (a) Passive attack (b) Active attack
(c) Forgery attack (d) None of these

Q19 Difference between Data Integrity and Data Security is

(a) Limiting physical access to computer systems; assigning passwords to users.

(b) Consistent, accurate and reliable data; protection of data from unauthorized access.

(c) Encryption; Audit trails

(d) Distributing work to preserve integrity; installing system passwords

Q20 In a computer security, _____ means that computer system assets can be modified only by authorized parties

- (a) Confidentiality (b) Integrity
(c) Availability (d) Authenticity

Q21 It is a type of program do not replicate automatically?

- (a) Worm (b) Zombie
(c) Trojan Horse (d) Logic Bomb

Q22 Which of the following is independent malicious program that need not any host program?

- (a) Trap doors (b) Trojan Horse
(c) Virus (d) Worm

Q23 _____ also known as a "trading name that a business trader use under commercial purposes.

- (a) Trade Secret (b) Trade Name
(c) Patent (d) Copy Right

Q24 Doodle me Diddle fraud held in 1996 in India was a _____ type of cyber crime

- (a) Salami (b) Credit Card
- (c) Data Diddling (d) None of them

Q25 The purpose of a DoS attack is/are:

- (a) Flood a network with traffic, thereby preventing legitimate network traffic
- (b) Disrupt connection between two systems
- (c) Prevent a particular individual to access the service(s).
- (d) All of them

Q26 Which of the following is issued online for use over the Internet and is stored in an electronic device such as a chip card or computer memory?

- (a) Hard Cash (b) Business Card
- (c) E-Cash (d) E-Card

Q27 Gaining unauthorized access to a computer system would fall under which category of computer crime?

- (a) Hacking
- (b) Theft of Service
- (c) Destruction of data & Software
- (d) Data Theft

Q28 One day while working on your system you receive an email from an organization asking that you verify your account information within 12 hours, or your account will be closed, the best thing to do is

- (a) Reply to the email asking them why this information is required.
- (b) Reply to the email with the information asked for
- (c) report the email to the actual organization and then delete the email.
- (d) None of these

Q29 A _____ is a document that grant the holder exclusive right on an invention for fixed number of years.

- (a) Copy Right (b) Patent
- (c) Trade Mark (d) Trade Secret

Q30 Which of these companies is not a leader in Cloud Computing?

- (a) Google (b) Amazon
- (c) Microsoft (d) Blackboard

Q31 _____ is the simple process of intercepting wireless data that is broadcasted on unsecured network.

- (a) Spoofing (b) Sniffing
- (c) Spamming (d) None of them

Q32 Which of the following is a cyber crime?

- (a) Hacking (b) Worm Attack
- (c) Virus Attack (d) None of these

Q33 This attack involves altering raw data just before final processing and then changing it back after the processing is completed:

- (a) Data Tampering (b) Data Diddling
- (c) Salami Attack (d) None of these

Q34 _____ is a type of virus which effect/ infects the storage media on which OS is stored.

- (a) Boot Sector Virus (b) Program Virus
- (c) Multipartite Virus (d) Stealth Virus

Q35 Network administrator must do _____ to protect a wireless network.

- (a) MAC address filtering (b) Disabling SSID
- (c) Disabling Mac filtering (d) All of them

Q36 It is a technique breaking into phone or other communication systems.

- (a) Hacking (b) Cracking
- (c) Phreaking (d) War dialling

Q37 _____ is a tool installed on your computer to detect the presence of a key logger

- (a) Keylogger (b) Anti Keylogger
- (c) Software Keylogger (d) Hardware Keylogger

Q38 _____ is a generic term which refers to all the legal and regulate aspects of Internet and the World Wide Web

- (a) Cyber Law (b) Cyber Dyne
- (c) Cyber Cafe (d) Electronic Law

Q39 What is the difference between Data Integrity and Data Security?

- (a) Limiting physical access to computer systems; assigning passwords to users
- (b) Consistent, accurate and reliable data; protection of data from unauthorized access.
- (c) Encryption; Audit trails
- (d) Distributing work to preserve integrity; installing system passwords

Q40 Attacker uses this server to connect with a network which is block through the firewall of the organization.

- (a) Web Server (b) FTP Server
- (c) Proxy Server (d) None of these

Q41 We can categorize threats as:

- (a) Passive attack (b) Active attack
- (c) Both a and b (d) None of them

Q42 Symbol of a reputed firm is

- (a) Patent (b) Copyright
- (c) Trademark (d) All of the above

Q43 _____ are the symbols used by businesses to identify their goods and services.

- (a) Trade Mark (b) Trade Secret
- (c) Designs (d) None of them

Q44 _____ is a preparation towards preattack.

- (a) Passive attack (b) Active attack
- (c) Reconnaissance (d) None of them

Q45 Whenever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputaion concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person is said:

- (a) Cyber Stalking (b) Phishing
- (c) Social Engineering (d) Cyberdefamation

Q46 _____ cipher replaces one character with another character to create cipher text.

- (a) Substitution (b) Transposition
- (c) either (a) or (b) (d) neither (a) or (b)

Q47 Information Technology Act ITA was amended in _____ year in India

- (a) 2000 (b) 2004
- (c) 2008 (d) 2012

Q48 A cookie that was not created by the Web site that attempts to access it is called a

- (a) First-party cookie (b) Second-party cookie
- (c) Third-party cookie (d) Fourth-party cookie

Q49 A hacker who claims to be motivated by improving security by uncovering vulnerabilities is called.

- (a) Black hat attacker (b) White hat attacker
- (c) Cowboy attacker (d) Resource attacker

Q50 This mechanism is used to protect private networks from outside attack is

- (a) Firewall (b) Antivirus
- (c) Digital signature (d) Formatting

Q51 _____ can be used as IP address Multiplexer to enable to connect to number of computers on the internet.

- (a) Web Server (b) FTP Server
- (c) Proxy Server (d) None of these

Q52 Which term best describes the type of password attack that uses a large pregenerated data set of hashes from nearly every possible password?

- (a) Brute Force Attack (b) Dictionary Attack
- (c) Rainbow Table Attack (d) Host File Attack

Q53 Hackers often gain entry to a network by pretending to be at a legitimate computer shows an example of_____.

- (a) Spoofing (b) Forging
- (c) IP Spoofing (d) ID Theft

Q54 Multiple ping packets are send through ping command which results into more traffic than the victim can handle, in this type of denial of service attack

- (a) Flood attack (b) Ping of death attack
- (c) SYN attack (d) Smurf attack

Q55 It is a way of generating significant computer network traffic on a victim network.

- (a) Flood attack (b) Ping of death attack
- (c) Teardrop attack (d) Smurf attack

Q56 When the control of a web site is taken by an attacker is considered as

- (a) Data Diddling (b) Salami
- (c) Web theft (d) Web Jacking

Q57 This is installed between coputer and Keyboard to generate the log of keys pressed by user.

- (a) PC Key logger (b) Software key logger
- (c) Hardware key logger (d) None of them

Q58 This process involves changing contents of a website depending upon a user's IP address and geographical location

- (a) IP Base Clocking (b) IP Base Blocking
- (c) Industry Espionage (d) None of them

Q59 Which among given is/are challenge(s) for any organization

- (a) Employee wasted time on internet
- (b) Controlling Access to Web Application
- (c) Bandwidth Wastage
- (d) All of them

Q60 This techniques is used on a wireless network to scan the network passively.

- (a) Scanning (b) Spoofing
- (c) Sniffing (d) All of them

Q61 This in built feature of web browsers to warn about malicious sites by:

- (a) Anti-phishing filters in IE and Firefox
- (b) Web of Trust
- (c) Clearing history of browser
- (d) Addlock Plus

Q62 _____ is a social media computing allows people to connect and share information.

- (a) Facebook (b) My Space
- (c) Linkedin (d) Twitter

Q63 _____ is not a cloud sphere.

- (a) Joint Sphere (b) User Sphere
- (c) Recipient Sphere (d) Client Sphere

Q64 Secret key cryptography is synoymous with

- (a) Symmetric Key Cryptography
- (b) Asymmetric key cryptography
- (c) Private key cryptography
- (d) Quantum Cryptography

Q65 To encypt a message from Aman to Alka using public key cryptography, the following is needed:

- (a) Aman's private key (b) Aman's public key
- (c) Alka's private key (d) Alka's public key

Q66 Which of the following protocols is used in accessing web mail?

- (a) SMTP (b) HTTP
- (c) POP3 (d) IMAP

Q67 The phrase _____ describes viruses, worms, trojan horse attack applets, and attack scripts

- (a) Malware (b) Spam
- (c) Phishing (d) Virus

Q68 A counter- measure to eavesdropping on the communication link is the use of

- (a) A cryptography checksum (b) Encryption

- (c) A login name and password (d) A fake identity

Q69 Poorly designed social networking sites are especially vulnerable to

- (a) Buffer overflow attack (b) SQL injection attack
- (c) Non- Persistent cross-site scripting attacks
- (d) Persistent cross-site scripting attacks

Q70 A SQL injection attack may be used to

- (a) Change number of coloumns in a table
- (b) Read a row in a table
- (c) Change coloumn name in a table
- (d) None of them

Q71 The most effective remedy for SQL injection attacks is

- (a) To filter HTML form input at the client side
- (b) To employ stored procedures on the database server
- (c) To employ prepared SQL statements on the web server
- (d) To perform input validation on the server via regular

expression

Q72 Tasks performed by firewall include

- (a) Access Control (b) Packet Integrity Checking
- (c) IP address spoofing (d) All

Q73 The role of a payment gateway is

- (a) A proxy to the merchant
- (b) A proxy to the bankcard network
- (c) A financial service provider
- (d) A government regulator

Q74 The motivation of an ethical hacker is

- (a) Financial gain
- (b) The thrill of hacking
- (c) To desire to identify vulnerabilities so they can be patched before they are publicaly exposed
- (d) A religious/political/ideological cause

Q75 Which of the follwoing is/are necessary feature(s) of a DDoS attack

- (a) Use of a TCP SYN packets
- (b) Use of a spoofed IP address
- (c) Use of multiple attackers georgraphically dispressed
- (d) Use of malformed IP packets

Q76 An attack originating and/or attempted within the security perimeter of an organization is _____ type of attack.

- (a) Active (b) Inside
- (c) Passive (d) Outside

Q77 The attacker usually installs the sniffers on the wireless network and conduct activity such as:

- (a) Detection of SSID (b) Collecting MAC address
- (c) Collecting fram to creack WEP (d) All

Q78 A Digital certificate is used to bind

- (a) A person's public key to his private key
- (b) A person's public key to his identity
- (c) A person's private key to his identity
- (d) A person's signature to his private key

Q79 Which of the following attacks is/are likely to result in identity theft?

- (a) Phishing attack (b) Denial of Service attack
- (c) Virus Infection (d) All

Q80 In which of the following does someone use an application to capture and manipulate packets as they are passing through your network?

- (a) DoS (b) Backdoor
- (c) Man in Middle (d) Spoofing

Q81 _____ is a "technique to influence" people to obtain the information or perform some action.

- (a) Social Engineering (b) Phishing
- (c) Cyber stalking (d) None

Q82 Intellectual Property Rights (IPR) protect the use of information and ideas that are of.

- (a) Ethical value (b) Moral Value
- (c) Social value (d) Commercial value

Q83 A hacker that changes or forges information in an electronic resource, is engaging in _____.

- (a) Sniffing (b) Denial of Service
(c) Terrorism (d) Data Diddling
- Q84 It involves harassing or threatening behavior that an individual will conduct repeatedly for following a person, visiting a person's home and/or business place
(a) Phishing (b) Social Engineering
(c) Cyber Stalking (d) None
- Q85 Security risks from social engineering is/are
(a) Malware distribution (b) Cyber bullying
(c) Privacy concern (d) All
- Q86 Threats are categorized as:
(a) Passive or active (b) Traffic
(c) Masquerade (d) Others
- Q87 How are viruses spread?
(a) Through Firewalls (b) Downloading infected programs and files from internet.
(c) Garbled information. (d) Install anti-virus.
- Q88 DDoS stand for
(a) Distributed Denial of Service attack
(b) Digital Data Output Spoit
(c) Damaging Downtime of System
(d) Distributed Destruction of System
- Q89 _____ is not a kind of cyber attack.
(a) Cber Stalking (b) Micro sites
(c) Firewall attack (d) E-Mail
- Q90 The latest WLAN standard is:
(a) 802.11g (b) 802.11n
(c) 802.12g (d) 802.12n
- Q91 The following is used when the source code for a piece of software is unavailable
(a) Blackbox testing (b) Whitebox testing
(c) Regrssion testing (d) Unit testing
- Q92 Which of the following is/are true of various forms of malware:
(a) A worm attaches itself to a file or program
(b) A Trojan is stand-alone program
(c) A virus does not necessarily replicate
(d) All of the above
- Q93 _____ cryptography technique is used for ATM cards
(a) Symmetric (b) Assymetric
(c) Hashing (d) None
- Q94 _____ cipher takes one character and replaces it with another.
(a) Stream (b) Single
(c) Substitution (d) Hash
- Q95 The purpose of digital signatue is/are
(a) Verify Sender (b) Prove Integrity of message
(c) Prevent sender from disowing the message
(d) All
- Q96 _____ is the science of transforming information into a secure form so that unauthorized users cannot access it.
(a) Steganography (b) Cryptography
(c) Neither a nor b (d) Both a and b
- Q97 A victim unknowingly downloads a Trojan horse virus is a _____ type of crime.
(a) Type 1 Cyber crime (b) Type 2 Cyber crime
(c) Type 3 Cyber crime (d) Type 4 Cyber crime
- Q98 Survival mantra for netizens is are:
(a) Keep genuine software
(b) keep browsers updated with security patches
(c) Keep an effective Antivirus and updates
(d) All of them
- Q99 _____ is a technique of changing an assigned Media Access Control address of a network Interface card to a different one
(a) IP Spoofing (b) IP Filtering
(c) MAC Spoofing (d) MAC Filtering

- Q100 Which among following(s) can be patented.
(a) Process (b) Machine
(c) Composition of matter (d) All of the above

Roll No.....

Total No. of Pages: 04

END TERM EXAMINATION
FIFTH SEMESTER DECEMBER 2015
CAL3313 – CYBER SECURITY

Time allowed: 3 Hrs.

Max. Marks: 100

General Instructions :

1. All questions are compulsory
2. Each question carry one mark
3. There is no negative marking

Q1 _____ are used in denial of service attacks, typically against targeted websites.

- (a) Worm (b) Zombie
(c) Virus (d) Trojan Horse

Q2 _____ is a form of virus explicitly designed to hide itself from detection by antivirus.

- (a) Stealth Virus (b) Polymorphic Virus
(c) Parasitic Virus (d) Macro Virus

Q3 A _____ is a program that secretly takes over another Internet-attached computer and then uses the computer to launch attacks.

- (a) Worm (b) Zombie
(c) Virus (d) Trap doors

Q4 In computer security, _____ means that computer system assets can be modified by the authorized parties.

- (a) Confidentiality (b) Integrity
(c) Availability (d) Authenticity

Q5 Which of the following malicious program does not replicate automatically?

- (a) Trojan (b) Virus
(c) Worm (d) none of these

Q6 A _____ is a program that can infect other programs by modifying them, the modification includes a copy of the virus program, which can go on to infect other programs.

- (a) Worm (b) Virus
(c) Zombie (d) Trap doors

Q7 IPSec is designed to provide the security at the

- (a) Transport layer (b) Network Layer
(c) Application Layer (d) Session Layer

Q8 An attempt to make a computer resource unavailable to its intended users is called

- (a) DoS attack (b) Virus attack
(c) Botnet process (d) worms attack

Q9 Pretty good privacy (PGP) is used in

- (a) Browser Security (b) Email Security
(c) FTP Security (d) None of these

Q10 When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called

- (a) DNS Lookup (b) DNS Hijacking
(c) DNS Spoofing (d) None of these

Q11 WPA2 is used for security in

- (a) ethernet (b) Bluetooth
(c) wifi (d) None of these

Q12 What characteristic make Internet so attractive?

- (a) the 'secure' surroundings within which it is implemented
(b) the ability to provide an open, easy-to-use network
(c) it eliminates the need for firewalls
(d) You don't require a fast computer to use the internet

Q13 Which of the following methods can effectively be used to prevent logical breach of security?

- (a) Operating system and other system software
(b) computer architectural design

(c) Distributed systems design

(d) Network design

Q14 What can a firewall protect against?

- (a) viruses
(b) unauthenticated interactive logins from the "outside" world
(c) fire (d) connecting to and from the "outside" world

Q15 The type of threats on the security of a computer system or network arei) Interruption ii) Interception iii) modification iv) creation v) abrication

- (a) i, ii, iii and iv only
(b) ii, iii, iv and v only
(c) i, ii, iii and v only
(d) All of the above

Q16 What has become more important because of the increased use of computers, the internet and WWW.

- (a) Natural Disasters (b) Hardware Malfunctions
(c) Data integrity and data security (d) Malicious deletions

Q17 Which of the following describes someone who gains illegal access to a computer system?

- (a) Hacker (b) Identity theft
(c) Intruder (d) Cyber-terrorist

Q18 Which of the following are the ethical issues facing the use of technology in business today?

- (a) E-mail Privacy (b) Software piracy
(c) Intellectual property (d) All of the above

Q19 Which of the following is used to send secure messages from one location to another using a public network such as the Internet?

- (a) Physical Public Network (b) Virtual Public Network
(c) Physical Private Network (d) Virtual Private Network

Q20 Which of the following is/are methods of providing secure communication between two entities through the use of mathematical coding?

- (a) Digital Signature encryption (b) Public key encryption
(c) Private key encryption (d) All of the above

Q21 What is the maximum header size of an IP packet?

- (a) 32 bytes (b) 64 bytes
(c) 30 bytes (d) 62 bytes

Q22 Which of the following is/are Protocols of Application?

- (a) FTP (b) DNS
(c) Telnet (d) All of the above

Q23 I want to request secure web pages using https://. What port will I need to open on my firewall to allow these SSL-encrypted packets to flow?

- (a) 161 (b) 53
(c) 6000 (d) 443

Q24 IT Act in India was amended in

- (a) 2000 (b) 2004
(c) 2008 (d) 2010

DO NOT WRITE ANYTHING ON QUESTION PAPER EXCEPT ROLL NO.

- Q25 Intellectual property rights and _____ are two of the most important developing areas of law.
(a) Cyber Law (b) copyright infringement
(c) patent law (d) trademark infringement
- Q26 Commercial use domain names will normally use the following suffix in their website address.
(a) .net (b) .gov
(c) .com (d) .org
- Q27 If Social engineering is used to crack the password, it comes under the category of
(a) Online Attack (b) Offline attack
(c) Non-electronic (d) None of these
- Q28 SQL injection attack involves _____ command to retrieve information from a web page/web site.
(a) GET (b) POST
(c) SELECT (d) DELETE
- Q29 In this type of password cracking technique attacker substitutes numbers and symbols to get the password.
(a) Dictionary Attack (b) Hybrid attack
(c) Bruce force attack (d) Rainbow attack
- Q30 The latest standard of WLAN is
(a) 802.11g (b) 802.11n
(c) 802.12g (d) 802.12n
- Q31 In this technique attacker often launches an attack on wireless network by creating a new network with strong signal strength.
(a) Sniffing (b) Spoofing
(c) Man in the middle (d) Dos
- Q32 SSID stand for _____.
(a) System Service Identifier (b) Service Set ID
(c) Service Set Identifier (d) None of the above
- Q33 WEP stand for
(a) Wireless Equivalent Protocol
(b) Wired Equivalent Protocol
(c) Wireless Equivalent Privacy
(d) Wired Equivalent Privacy
- Q34 _____ cookies remains in the system until intentionally removed by user
(a) System (b) Session
(c) Persistent (d) Transient
- Q35 _____ cookies is not retained after the browser is closed
(a) Persistent Cookies (b) Stored Cookies
(c) Transient Cookies (d) None of them
- Q36 This social media tool allows people to connect and share information.
(a) Facebook (b) LinkedIn
(c) MySpace (d) Twitter
- Q37 Which among given is not a kind of cloud sphere?
(a) JointSphere (b) UserSphere
(c) ClinetSphere (d) Recipient Sphere
- Q38 Anti-phishing tools cannot detect such kinds of phishing sites
(a) Website Forgery (b) Phone Phishing
(c) Mail Phishing (d) Flash Phishing
- Q39 The SSID of Wireless Access Point can be upto _____ characters.
(a) 16 (b) 20
(c) 24 (d) 32
- Q40 Purpose of a proxy server is _____.
(a) Keep System behind curtain
(b) Speed up access to the resource
(c) Both A & B
(d) None of these
- Q41 In this technique hundreds or thousands of zombie computers are used to flood a device with requests.
(a) Dos (b) DDoS
(c) Man in the middle (d) Buffer Overflow
- Q42 This must be used to protect from a SQL injection attack
(a) Input validation (b) Modify error report
(c) Isolate servers (d) All of them
- Q43 _____ not involves in securing a wireless network
(a) Disable remote login
(b) Disable WPA/WEP encryption
(c) Disable SSID broadcast
(d) Enable MAC address filtering
- Q44 _____ is a kind of malware whose presence is typically hidden from the user.
(a) Spyware (b) Logic Bomb
(c) Key Logger (d) Anonymizer
- Q45 Which among these is not a threat from social Media?
(a) Malware Distribution (b) Stalking
(c) Privacy Concern (d) All of them
- Q46 _____ is an art of detecting messages that are hidden in images, audio/video files.
(a) Steganalysis (b) Steganography
(c) Cryptography (d) Cryptanalysis
- Q47 This process involves changing contents of a website depending upon a user's IP address and geographical location.
(a) IP base blocking (b) IP base clocking
(c) Industry Espionage (d) None of these
- Q48 A _____ mail is one that originate from one source but actually has been sent from another source
(a) Spam (b) Spoof
(c) Fake (d) Fraud
- Q49 An accountant of a company change the data base while the computation of the salary of the employee and when salary is generated he change back the data to its original form, this shows the example of a
(a) Salami attack (b) Forgery attack
(c) Social Engineering attack (d) None of these
- Q50 _____ scanning is to understand the existing weakness in the system
(a) Port (b) Network
(c) Vulnerability (d) System
- Q51 When someone take control of your website consider as
(a) Salami (b) Data Didding
(c) Web Jacking (d) Spoofing
- Q52 Which term best describes the type of attack that makes it seem like two computers are communicating with each other, when actually they are sending and receiving data with a computer between them?
(a) Spoofing (b) Middle Man
(c) Man in the middle attack (d) Replay
- Q53 Dumpster diving is an example of
(a) Social Engineering (b) Phishing
(c) Fraud (d) Cyber Staking
- Q54 Which among given is a Bluetooth hacking tool
(a) Bluejacking (b) Bluebugging
(c) Car-whispering (d) All of them
- Q55 CGA stands for
(a) Cryptographically generated address
(b) Cryptographically granted Access
(c) Cryptographically granted Address
(d) None is correct
- Q56 Counterfeit websites are used by _____ to extract personal information.
(a) Foistware (b) Heedless guests
(c) Phreakers (d) All of them

DO NOT WRITE ANYTHING ON QUESTION PAPER EXCEPT ROLL NO.

- Q57 _____ is a tool which extract the data from the phone of a person even his/her mobile phone is switched off
(a) Bluejack (b) Bluesnaffer
(c) Bluediving (d) Bluebugger
- Q58 Hashing algorithm can protect the _____ of information.
(a) Confidentiality (b) Integrity
(c) Availability (d) Authencity
- Q59 In which year IT act implemented in India
(a)1998 (b) 2000
(c) 2004 (d) 2008
- Q60 Asymmetric Encryption algorithm protects
(a) Confidentiality (b) Integrity
(c) Availability (d) All of them
- Q61 This type of virus when executed infects program files along with boot record.
(a) Boot Sector virus (b) Program virus
(c) Multipartite virus (d) Stealth virus
- Q62 The attacker usually installs the sniffers on the wireless network and conduct activities such as:
(a) Detection of SSID (b) Collecting MAC address
(c) collecting frame to crack WEP (d) All of them
- Q63 A small hardware device or a program that monitors each keystroke a user types on the computer's keyboard is known as:
(a) Proxy Server (b) Anonymizer
(c) Key Logger (d) Key Capture
- Q64 IPSec is designed to provide security at
(a) Transport layer (b) Network layer
(c) Application layer (d) Session layer
- Q65 WPA2 is used for security in
(a) ethernet (b) bluetooth
(c) wi-fi (d) None of these
- Q66 PGP encrypts data by using a block cipher called
(a) international data encryption algorithm
(b) private data encryption algorithm
(c) intrenet data encryption algorithm
(d) none mentioned
- Q67 In wireless ad-hoc network
(a) access point is not required (b) access point is must
(c) nodes are not required (d) access point is hidden
- Q68 A piece of icon or image on a web page associated with another webpage is called
(a) url (b) hyperlink
(c) plugin (d) None
- Q69 A web cookie is a small piece of data
(a) sent from a website and stored in user's web browser while a user is browsing a website
(b) sent from user and stored in the server while a user is browsing a website
(c) sent from root server to all servers
(d) sent from client to server
- Q70 Which of the following is not the funtion of network layer?
(a) routing (b) inter networking
(c) congestion control (d) error checking
- Q71 In cryptography, what is cipher?
(a) algorithm for performing encryption and decryption
(b) encrypted message
(c) both a and b (d) None of the above
- Q72 The header length of IPv6 datagram is
(a) 10 bytes (b) 25 bytes
(c) 30 bytes (d) 40 bytes
- Q73 IPv6 does not use _____ type of address
(a) Broadcast (b) Multicast
(c) Unicast (d) None of the above
- Q74 Cryptographic hash function takes an arbitrary block of data and returns
(a) fized size bit string (b) variable size bit string
(c) bit string (d) None of these
- Q75 Which one of the following is a cryptographic protocol used to secure HTTP connection?
(a) stream control transmission protocol (SCTP)
(b) transport layer security (TSL)
(c) explicit congestion notification (ECN)
(d) resource reservation protocol
- Q76 What is the number one concern about cloud computing?
(a) Too expensive (b) Security concerns
(c) Too many platforms (d) Accessibility
- Q77 Which is not a major cloud computing platform?
(a) Google 101 (b) IBM Deep blue
(c) MS Azure (d) Amazon EC 2
- Q78 "Cloud" in cloud computing, represents what?
(a) Wireless (b) harddrives
(c) People (d) Internet
- Q79 _____ is the feature of cloud computing that allows the service to change in size or volume in order to meet a user's needs.
(a) Scalability (b) Virtualization
(c) Security (d) Cost-savings
- Q80 The attackers a network of compromised devices known as
(a) Internet (b) Botnet
(c) Telnet (d) D-net
- Q81 The DoS attack is which the attacker establishes a large number of half-open or fully open TCP connections at the target host
(a) Vulnerability attack (b) Bandwidth Flooding
(c) Connection Flooding (d) All of the above
- Q82 Sniffers can be deployed in
(a) Wired environment (b) Wi-fi
(c) Ethernet LAN (d) All of the above
- Q83 A botnet is
(a) a computer virus that replicates and spreads itself from computer to computer via e-mail and other Internet traffic.
(b) software that gives you administrator rights to a computer or network.
(c) an exact copy or snapshot of the contents of an electronic medium.
(d) a collection of computers that have been infected with blocks of code that can run automatically by themselves.
- Q84 Which of the following refers to the forging of the return address on an e-mail so that the e-mail message appears to come from someone other than the actual sender?
(a) Spoofing (b) Redacting
(c) Spamming (d) Pharming
- Q85 SQL injection is an attack in which _____ code is inserted into strings that are later passed to an instance of SQL Server.
(a) malicious (b) reduntant
(c) clean (d) Non-reduntant
- Q86 Point out the correct statement
(a) Parameterized data cannot be manipulated by a skilled and determined attacker
(b) Procedure that constructs SQL statements should be reviewed for injection vulnerabilities
(c) The primary form of SQL injection consists of indirect insertion of code
(d) None of the above is correct

- Q87 _____ is time based SQL injection attack.
(a) Quick detection (b) Initial Exploitation
(c) Blind SQL injection (d) Inline comments
- Q88 Paid advertising based on a per-click model is called
(a) Sponsored search engine advertising
(b) Feedback (c) Source advertising
(d) Search Engine Optimization
- Q89 Mobile marketing to-date is most successful among
(a) American consumers (b) Younger consumers
(c) Spanish consumers (d) None of the consumers
- Q90 Which of the following is IEEE fiber cable standard?
(a) 100BASE-FX (b) 100BASE-CX
(c) 10GBASE-LR (d) 10BASE-FL
- Q91 What typically happens when a buffer is overflowed?
(a) The memory space that comes after the buffer holds the extra data as well as keeping the data that it contained before
(b) Whatever is in the memory space that comes after the buffer is overwritten
(c) The memory chip in the computer gets too big and explodes
(d) Electrons fall out of the memory chip and start a fire.
- Q92 A DNS Client is called
(a) DNS Updator (b) DNS resolver
(c) DNS handler (d) None of the above
- Q93 Network layer firewall works as a
(a) frame filter (b) packet filter
(c) both a and b (d) None of the above
- Q94 _____ has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet, resulting in direct and concomitant losses.
(a) Digital crime (b) Cyber crime
(c) Computer related crime (d) None of the above
- Q95 Which of the following crimes is done using a computer as the instrument?
(a) Computer Manipulation (b) Money laundering
(c) Data alteration (d) Theft of services
- Q96 Which of the following techniques is most effective in preventing computer crime?
(a) Backups (b) Digital forensic analysis
(c) Using a firewall (d) None of the above
- Q97 What is a Hacktivist?
(a) Politically motivated hacker
(b) Denial of service attacker
(c) A proponent of Napster
(d) A person engaging in an intentional act involving a computer in which the person may have gained at the victim expense.
- Q98 What is purpose of cryptanalysis software?
(a) Breaking encryption
(b) Taking advantage of security hole
(c) Impairing or destroying function in a computer
(d) Delivering attack software
- Q99 Which of the following is not a similarity between real-world stalking and cyber stalking?
(a) Most victims are women (b) Most stalkers are men
(c) The stalker and victim are near to each other
(d) Stalkers are generally motivated by the desire to control the victim
- Q100 What percentage of kids have been bullied while online?
(a) 42% (b) 11%
(c) 67% (d) 2%

**END TERM EXAMINATION
FIFTH SEMESTER 2015-16
CAL3313 – CYBER SECURITY**

Time : 03 Hrs.

Max. Marks : 100

General Instructions :

1. All questions are compulsory
2. Each question carry one mark
3. There is no negative marking

- 1) Anti-phishing tools cannot detect such kinds of phishing sites.
(i) Website forgery (ii) Phone phishing
(iii) Mail phishing (iv) Flash phishing
- 2) In this type of attack attacker establishes a connection between a victim and the server to which victim is connected to extract the information.
(i) Man in the middle attack (ii) Bucket-brigade attack
(iii) Janus attack (iv) All of them
- 3) This type of attack involves all possible permutation-combinations of letters, numbers and special characters to crack the password.
(i) Dictionary attack (ii) Hybrid attack
(iii) Brute force attack (iv) Rainbow table attack
- 4) All the program files as well as boot sector is infected with activation of this type of virus attack
(i) Boot sector virus (ii) Multipartite virus
(iii) Stealth virus (iv) Program virus
- 5) Purpose of a proxy server is _____.
(i) Keep System behind curtain (ii) Speed up access to a resource
(iii) Both A and B (iv) None of them
- 6) This type of attack involves inquiring the network to discover host(s) to confirm information
(i) Active attack (ii) Rattling the doorknobs
(iii) Active reconnaissance (iv) All of them
- 7) Hashing algorithm can protect the _____ of information.
(i) Confidentiality (ii) Integrity
(iii) Availability (iv) Authenticity
- 8) This ensures that the information is correct and no unauthorized person or malicious software has altered that data.
(i) Confidentiality (ii) Integrity
(iii) Availability (iv) Authenticity
- 9) Asymmetric Encryption algorithm protects
(i) Confidentiality (ii) Integrity
(iii) Availability (iv) All of them
- 10) In which year Information Technology Act was implemented in India
(i) 1998 (ii) 2000
(iii) 2004 (iv) 2008
- 11) In this technique hundreds or thousands of zombie computers are used to flood a device with requests.
(i) DoS (ii) DDoS
(iii) Man in Middle (iv) Buffer Overflow
- 12) _____ attack occurs when a process attempts to store data in random access memory (RAM) beyond the boundaries of a fixed-length storage buffer.
(i) DoS (ii) DDoS
(iii) Man in Middle (iv) Buffer Overflow

- 13) In this type of attack attacker halt the wireless access point, so that victim cannot get access of it.
- (i) Man in middle attack
 - (ii) DoS attack
 - (iii) DDoS attack
 - (iv) Wireless attack.
- 14) In this attack a query is sent to the database to check if a user has valid name and password.
- (i) Password Guessing
 - (ii) SQL injection attack
 - (iii) Dictionary attack
 - (iv) Brute Force attack
- 15) This must be used to protect from a SQL injection attack
- (i) Input Validation
 - (ii) Modify error report
 - (iii) Isolate servers
 - (iv) All of them
- 16) _____ is used by attackers to find the open port in a network
- (i) Vulnerability Scanner
 - (ii) Network Scanner
 - (iii) Port Scanner
 - (iv) All of them
- 17) Counterfeit websites are used by _____ to extract personal information.
- (i) Foist ware
 - (ii) Heedless guests
 - (iii) Phreakers
 - (iv) Stalkers
- 18) When a service provider uses public cloud resources to create a private cloud is known as:
- (i) Public cloud
 - (ii) Private cloud
 - (iii) Global cloud
 - (iv) Virtual cloud
- 19) This GUI based utility is used to find Bluetooth enabled devices
- (i) Bluetooth Jacking
 - (ii) Bluetooth scanner
 - (iii) BlueBugger
 - (iv) BlueSniff
- 20) _____ is a tool which extract the data from the phone of a person even his/her mobile phone is switched off
- (i) Bluejack
 - (ii) Bluesnarfer
 - (iii) Bluediving
 - (iv) Bluebugger
- 21) The attacker usually installs the sniffers on the wireless network and conduct activities such as:
- (i) Detection of SSID
 - (ii) Collecting MAC address
 - (iii) Collecting frame to crack WEP
 - (iv) All of them
- 22) _____ not involves in securing a wireless network
- (i) Disable remote login
 - (ii) Disable WPA/WEP encryption
 - (iii) Disable SSID Broadcast
 - (iv) Enable Mac address filtering
- 23) _____ is a kind of malware whose presence is typically hidden from the user.
- (i) Spyware
 - (ii) Logic Bomb
 - (iii) Key Logger
 - (iv) Anonymizer
- 24) Which among given is not a kind of cloud sphere?
- (i) Joint Sphere
 - (ii) User Sphere
 - (iii) Clinet Sphere
 - (iv) Recipient Sphere
- 25) _____ is a professional networking tool used to connect with community of top executives.
- (i) Facebook
 - (ii) LinkedIn
 - (iii) MySpace
 - (iv) Twitter
- 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer?
- (i) Man in Middle
 - (ii) Buffer Over Flow
 - (iii) DoS
 - (iv) DDoS
- 27) CGA stands for
- (i) Cryptographically generated address
 - (ii) Cryptographically granted Access
 - (iii) Cryptographically granted Address
 - (iv) None of them
- 28) _____ involves gathering information about individual about a target without his/her knowledge
- (i) Passive Attack
 - (ii) Active Attack
 - (iii) Forgery Attack
 - (iv) Cyberstalking
- 29) A _____ mail is also known as junk mail

- (i) Spoof (ii) Spam
(iii) Fake (iv) Fraud
- 30) People who send multiple mails from zombie computers are known as
(i) Spoofer (ii) Spies Kiddies
(iii) Spammer (iv) Stalker
- 31) This social media tool allows people to connect and share information.
(i) Facebook (ii) LinkedIn
(iii) MySpace (iv) Twitter
- 32) Which among these is not a threat from social Media?
(i) Malware Distribution (ii) Stalking
(iii) Privacy Concern (iv) All of them
- 33) We can use these built-in and add-on features in web browsers to warn about malicious sites by:
(i) Anti-phishing filters in IE and Firefox (ii) Web of Trust
(iii) Clearing history of browser (iv) Addlock Plus
- 34) _____ is a technique of changing an assigned Media Access Control address of a network Interface card to a different one
(i) IP Spoofing (ii) MAC Spoofing
(iii) IP Filtering (iv) MAC Filtering
- 35) It refers to a scenario wherein an attacker on host A inserts A between all communications between host X and Y.
(i) Middle man (ii) Denial of Service
(iii) Distributed Denial of Service (iv) Bucket-brigade attack
- 36) _____ is the criminal practice of using social engineering using SMS service
(i) Phishing (ii) Vishing
(iii) Mishing (iv) Smishing
- 37) Which among given is a Bluetooth hacking tool
(i) Bluejacking (ii) Bluebugging
(iii) Car-Whispering (iv) All of them
- 38) _____ can be used as IP address Multiplexer to enable to connect to number of computers on the internet
(i) Web Server (ii) FTP Server
(iii) Proxy Sever (iv) None of the above
- 39) _____ are software programs installed on a computer system which usually are located between OS and keyboard hardware to record every key stroke.
(i) Keystroker (ii) PC Keylogger
(iii) Software Keylogger (iv) Anonymizer
- 40) A computer program that lies dormant and triggered on a event on a particular day is
(i) Virus (ii) Logic Bomb
(iii) Worm (iv) Trojan Horse
- 41) _____ are used in denial of service attacks, typically against targeted websites.
(i) Worm (ii) Zombie
(iii) Virus (iv) Trojan Horse
- 42) _____ is a form of virus explicitly designed to hide itself from detection by antivirus.
(i) Stealth Virus (ii) Polymorphic Virus
(iii) Parasitic Virus (iv) Macro Virus
- 43) A _____ is a program that secretly takes over another Internet-attached computer and then uses the computer to launch attacks.
(i) Worm (ii) Zombie
(iii) Virus (iv) Trap doors
- 44) In computer security, _____ means that computer system assets can be modified by the authorized parties.

- (i) Confidentiality (ii) Integrity
(iii) Availability (iv) Authenticity

45) Which of the following malicious program does not replicate automatically?
(i) Trojan (ii) Virus
(iii) Worm (iv) none of these

46) A is a program that can infect other programs by modifying them, the modification includes a copy of the virus program, which can go on to infect other programs.
(i) Worm (ii) Virus
(iii) Zombie (iv) Trap doors

47) IPSec is designed to provide the security at the
(i) Transport layer (ii) Network Layer
(iii) Application Layer (iv) Session Layer

48) An attempt to make a computer resource unavailable to its intended users is called
(i) DoS attack (ii) Virus attack
(iii) Botnet process (iv) worms attack

49) Pretty good privacy (PGP) is used in
(i) Browser Security (ii) Email Security
(iii) FTP Security (iv) None of these

50) When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called
(i) DNS Lookup (ii) DNS Hijacking
(iii) DNS Spoofing (iv) None of these

51) It is an eavesdropping on a wireless network to scan the network passively.
(i) Sniffing (ii) Spoofing
(iii) Scanning (iv) Blocking

52) WEP stand for
(i) Wireless equivalence Protocol (ii) Wired equivalence Protocol
(iii) Wireless equivalence Privacy (iv) Wired equivalence Privacy

53) They are ultimate mobile users who spends little time in the office, however they required regular access to data while on move
(i) Tethered Workers (ii) Road Warrior
(iii) Nomad (iv) Roaming Users

54) _____ is an art of detecting messages that are hidden in images, audio/video files.
(i) Steganalysis (ii) Steganography
(iii) Cryptography (iv) Cryptanalysis

55) In this type of DoS attack there is/are not any chance of the recovery of the server.
(i) DDoS (ii) HDoS
(iii) PDoS (iv) SDoS

56) Which term best describes the type of password attack that uses a large pregenerated data set of hashes from nearly every possible password?
(i) Brute Force Attack (ii) Dictionary Attack
(iii) Rainbow Table Attack (iv) Host File Attack

57) This refers to harass an individual or group of individuals or organization
(i) Social Engineering (ii) Phishing
(iii) Fraud (iv) Cyber Stalking

58) Dumpster diving is an example of
(i) Social Engineering (ii) Phishing
(iii) Fraud (iv) Cyber Stalking

59) _____ attack is a computer threat which attempts to exploit computer application vulnerability that are unknown to anybody in the world.
(i) Zero day (ii) Vulnerability

- (iii) Data Diddling (iv) None of the above
- 60) _____ is the criminal practice of using social engineering over telephone system
- (i) Phishing (ii) Vishing
(iii) Mishing (iv) Smishing
- 61) WPA2 is used for security in
- (i) ethernet (ii) Bluetooth
(iii) wifi (iv) None of these
- 62) What characteristic make Internet so attractive?
- (i) the 'secure' surroundings within which it is implemented
(ii) the ability to provide an open, easy-to-use network
(iii) it eliminates the need for firewalls
(iv) You don't require a fast computer to use the internet
- 63) Which of the following methods can effectively be used to prevent logical breach of security?
- (i) Operating system and other system software (ii) computer architectural design
(iii) Distributed systems design (iv) Network design
- 64) What can a firewall protect against?
- (i) viruses
(ii) unauthenticated interactive logins from the "outside" world
(iii) fire
(iv) connecting to and from the "outside" world
- 65) The type of threats on the security of a computer system or network are
- i) Interruption ii)Interception iii) modification iv) creation v) abrication
- (i) i, ii, iii and iv only
(ii) ii, iii, iv and v only
(iii) i, ii, iii and v only
(iv)All of the above
- 66) What has become more important because of the increased use of computers, the internet and WWW.
- (i) Natural Disasters (ii)Hardware Malfunctions
(iii) Data integrity and data security (iv)Malicious deletions
- 67) _____ server is a computer on a network which acts as an intermediary for connections with other computers on that network
- (i) Web (ii) FTP
(iii) Mail (iv) Proxy
- 68) _____ is a type of deception designed to steal your personal information, credit card details, passwords, account data or other information
- (i) Phishing (ii) Social Engineering
(iii) Spamming (iv) Hacking
- 69) The SSID of Wireless Access Point can be upto _____ characters.
- (i) 16 (ii) 20
(iii) 24 (iv) 32
- 70) SQL injection attack involves _____ command to retrieve information from a web page/web site.
- (i) GET (ii) POST
(iii) SELECT (iv) DELETE
- 71) In this technique attacker often launches an attack on wireless network by creating a new network with strong signal strength.
- (i) Sniffing (ii) Spoofing
(iii) Man in the Middle (iv) DoS
- 72) A software update to fix a security flaw or other problem is known as
- (i) Repair (ii) Patch
(iii) Hot Fix (iv) Exploit
- 73) A program that hides its true intent and then reveal itself when activated is known

- (i) Trojan Horse (ii) Virus
(iii) Worm (iv) Zombie
- 74) A software defect is considered as
(i) Asset (ii) Threat
(iii) Vulnerability (iv) Risk
- 75) Which term best describes the type of attack that makes it seem like two computers are communicating with each other, when actually they are sending and receiving data with a computer between them?
(i) Spoofing (ii) Middle Man
(iii) Man in Middle (iv) Replay
- 76) _____ scanning is to understand the status of open/block stuff on a web page
(i) Port (ii) Network
(iii) Vulnerability (iv) System
- 77) Which of the following describes someone who gains illegal access to a computer system?
(i) Hacker (ii) Identity theft
(iii) Intruder (iv) Cyber-terrorist
- 78) Which of the following are the ethical issues facing the use of technology in business today?
(i) E-mail Privacy (ii) Software piracy
(iii) Intellectual property (iv) All of the above
- 79) Which of the following is used to send secure messages from one location to another using a public network such as the Internet?
(i) Physical Public Network (ii) Virtual Public Network
(iii) Physical Private Network (iv) Virtual Private Network
- 80) Which of the following is/are methods of providing secure communication between two entities through the use of _____ mathematical coding?
(i) Digital Signature encryption (ii) Public key encryption
(iii) Private key encryption (iv) All of the above
- 81) What is the maximum header size of an IP packet?
(i) 32 bytes (ii) 64 bytes
(iii) 30 bytes (iv) 62 bytes
- 82) Which of the following is/are Protocols of Application?
(i) FTP (ii) DNS
(iii) Telnet (iv) All of the above
- 83) I want to request secure web pages using https://. What port will I need to open on my firewall to allow these SSL-encrypted packets to flow?
(i) 161 (ii) 53
(iii) 6000 (iv) 443
- 84) IP address consists of _____ bits.
(i) 32 (ii) 128
(iii) 64 (iv) 256
- 85) Intellectual property rights and _____ are two of the most important developing areas of law.
(i) Cyber Law (ii) copyright infringement
(iii) patent law (iv) trademark infringement
- 86) Commercial use domain names will normally use the following suffix in their website address.
(i) .net (ii) .gov
(iii) .com (iv) .org
- 87) It is a technique breaking into phone or other communication systems.
(i) Hacking (ii) Cracking
(iii) Phreaking (iv) War dialler
- 88) This process involves changing contents of a website depending upon a user's IP address and geographical location.

- (i) IP base blocking (ii) IP base clocking
(iii) Industry Espionage (iv) None of them
- 89) Which term best describes the type of password attack that uses a large pre-generated data set of hashes from nearly every possible password?
(i) Brute Force Attack (ii) Dictionary Attack
(iii) Rainbow Table Attack (iv) Host File Attack
- 90) What is the maximum header size of an IP packet?
(i) 32 bytes (ii) 64 bytes
(iii) 30 bytes (iv) 62 bytes
- 91) _____ Cookies are also known as Stored cookies.
(i) Session (ii) Persistent
(iii) Transient (iv) Web based
- 92) _____ involves altering raw data just before it is processed by computer.
(i) Forgery attack (ii) Data Diddling attack
(iii) Salami attack (iv) None of the above
- 93) _____ scanning is to understand the existing weakness in the system
(i) Port (ii) Network
(iii) Vulnerability (iv) System
- 94) It is a technique breaking into phone or other communication systems.
(i) Hacking (ii) Cracking
(iii) Phreaking (iv) War dialler
- 95) The idea behind this attack is to deduct a small amount of money which would go completely unnoticed in a first sight.
(i) Salami (ii) Data Diddling
(iii) Web Jacking (iv) Spoofing
- 96) When someone take control of your website consider as
(i) Salami (ii) Data Diddling
(iii) Web Jacking (iv) Spoofing
- 97) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer?
(i) Man in Middle (ii) Buffer Over Flow
(iii) DoS (iv) DDoS
- 98) This type of phishing method involves the use of spammed mails bearing falsified corporate identification.
(i) Dragnet (ii) Rod and reel
(iii) Lobsterpot (iv) Gilnet
- 99) In this type of phishing attack browser of a victim is targeted to redirect him/her to a fake web site.
(i) Dragnet (ii) Rod and reel
(iii) Lobsterpot (iv) Gilnet
- 100) SSID stand for _____.
(i) System Service Identifier (ii) Service Set ID
(iii) Service Set Identifier (iv) None of the above

End Term Exam

Semester.....

Roll No:

[Total No. of Pages:04]

Date:

Time: 90 minutes

Department:

Title of the Course: Cyber Security

Max. Marks: 100

Course Code: HUL 2401

Q1 Which of the following uses two keys to encrypt a message?

- (a) Symmetric encryption Algorithms
- (b) Hashing Algorithm
- (c) Asymmetric encryption Algorithm
- (d) None of the above

Q2 In this phishing attack Phishers identify the victim in advance:

- (a) Dragnet
- (b) Lobsterpot
- (c) Rod and reel
- (d) Gilnet

Q3 Which among these is a feature of Hashing

- (a) Confidentiality
- (b) Availability
- (c) Authenticity
- (d) None of these

Q4 In this type of DoS attack there is/are not any chance of the recovery of the server

- (a) HdoS
- (b) DDoS
- (c) SdoS
- (d) PDoS

Q5 Which statement about virus attack is true

- A. Boot sector virus infects the storage media
- B. Program virus is a hybrid virus
- C. Stealth virus mask itself so detection is not easy
- D. Multipartite virus target .exe files
- (a) Both A and B
- (b) Both A and C
- (c) Both A and D
- (d) None of them

Q6 An attempt to make a computer resource unavailable to its intended users is called.

- (a) Virus attack
- (b) Worm attack
- (c) Botnet Process
- (d) Denial of Service

Q7 _____ is the criminal practice of using social engineering over telephone.

- (a) Phishing
- (b) Mishing
- (c) Vishing
- (d) Smishing

Q8 _____ attack is a computer threat which attempts to exploit computer application vulnerability that are unknown to anybody in the world.

- (a) Zerod day
- (b) Vulnerability
- (c) Data Diddling
- (d) Salami

Q9 Which among given is a Bluetooth hacking tool?

- (a) Bluejacking
- (b) Blue bugging
- (c) Car Whispering
- (d) All of them

Q10 In asymmetric cryptographic algorithm when Tom wants to send a message to Alisha he will decrypt it with

- (a) His Public Key
- (b) Public key of Alisha
- (c) His Private Key
- (d) Private key of Alisha

Q11 Another name of Public Key Cryptography

- (a) Symmetric Key Cryptography
- (b) Private key Cryptography
- (c) Asymmetric key Cryptography
- (d) None of the above

Q12 _____ are software programs installed on a computer system which usually are located between OS and keyboard hardware to record every key stroke

- (a) Key Stroker
- (b) Key Logger
- (c) Software Key logger
- (d) Anonymizers

Q13 This computer program lies dormant and triggered on a event on a particular day is:

- (a) Worm
- (b) Logic Bomb
- (c) Virus
- (d) Trojan Horse

Q14 "Do no evil" is the motto of

- (a) Microsoft
- (b) Google
- (c) Yahoo
- (d) Intel

Q15 Which term best describes the type of attack that makes it possible to deny the service of a server using multiple computers from different geographical locations?

- (a) Buffer Over flow
- (b) DoS
- (c) Man in Middle
- (d) None of these

Q16 Which term best describes the type of attack that makes it seem like two computers are communicating with each other, when actually they are sending and receiving data with a computer between them?

- (a) Spoofing
- (b) Middle Man
- (c) Bucket Brigade
- (d) Replay

Q17 A _____ is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks.

- (a) Worm
- (b) Zombie
- (c) Virus
- (d) Trap doors

Q18 This type of attack involves gathering information about individual about his/her knowledge, for example which the IN and OUT time of an employee.

- (a) Passive attack
- (b) Active attack
- (c) Forgery attack
- (d) None of these

Q19 Difference between Data Integrity and Data Security is

- (a) Limiting physical access to computer systems; assigning passwords to users.
- (b) Consistent, accurate and reliable data; protection of data from unauthorized access.
- (c) Encryption; Audit trails
- (d) Distributing work to preserve integrity; installing system passwords

Q20 In a computer security, _____ means that computer system assets can be modified only by authorized parties

- (a) Confidentiality
- (b) Integrity
- (c) Availability
- (d) Authenticity

Q21 It is a type of program do not replicate automatically?

- (a) Worm
- (b) Zombie
- (c) Trojan Horse
- (d) Logic Bomb

Q22 Which of the following is independent malicious program that need not any host program?

- (a) Trap doors
- (b) Trojan Horse
- (c) Virus
- (d) Worm

Q23 _____ also known as a "trading name that a business trader use under commercial purposes.

- (a) Trade Secret
- (b) Trade Name
- (c) Patent
- (d) Copy Right

Q24 Doodle me Diddle fraud held in 1996 in India was a _____ type of cyber crime

- (a) Salami (b) Credit Card
- (c) Data Diddling (d) None of them

Q25 The purpose of a DoS attack is/are:

- (a) Flood a network with traffic, thereby preventing legitimate network traffic
- (b) Disrupt connection between two systems
- (c) Prevent a particular individual to access the service(s).
- (d) All of them

Q26 Which of the following is issued online for use over the Internet and is stored in an electronic device such as a chip card or computer memory?

- (a) Hard Cash (b) Business Card
- (c) E-Cash (d) E-Card

Q27 Gaining unauthorized access to a computer system would fall under which category of computer crime?

- (a) Hacking
- (b) Theft of Service
- (c) Destruction of data & Software
- (d) Data Theft

Q28 One day while working on your system you receive an email from an organization asking that you verify your account information within 12 hours, or your account will be closed, the best thing to do is

- (a) Reply to the email asking them why this information is required.
- (b) Reply to the email with the information asked for
- (c) report the email to the actual organization and then delete the email.
- (d) None of these

Q29 A _____ is a document that grant the holder exclusive right on an invention for fixed number of years.

- (a) Copy Right (b) Patent
- (c) Trade Mark (d) Trade Secret

Q30 Which of these companies is not a leader in Cloud Computing?

- (a) Google (b) Amazon
- (c) Microsoft (d) Blackboard

Q31 _____ is the simple process of intercepting wireless data that is broadcasted on unsecured network.

- (a) Spoofing (b) Sniffing
- (c) Spamming (d) None of them

Q32 Which of the following is a cyber crime?

- (a) Hacking (b) Worm Attack
- (c) Virus Attack (d) None of these

Q33 This attack involves altering raw data just before final processing and then changing it back after the processing is completed:

- (a) Data Tampering (b) Data Diddling
- (c) Salami Attack (d) None of these

Q34 _____ is a type of virus which effect/ infects the storage media on which OS is stored.

- (a) Boot Sector Virus (b) Program Virus
- (c) Multipartite Virus (d) Stealth Virus

Q35 Network administrator must do _____ to protect a wireless network.

- (a) MAC address filtering (b) Disabling SSID
- (c) Disabling Mac filtering (d) All of them

Q36 It is a technique breaking into phone or other communication systems.

- (a) Hacking (b) Cracking
- (c) Phreaking (d) War dialling

Q37 _____ is a tool installed on your computer to detect the presence of a key logger

- (a) Keylogger (b) Anti Keylogger
- (c) Software Keylogger (d) Hardware Keylogger

Q38 _____ is a generic term which refers to all the legal and regulate aspects of Internet and the World Wide Web

- (a) Cyber Law (b) Cyber Dyne
- (c) Cyber Cafe (d) Electronic Law

Q39 _____ is the art and science of detecting messages that are hidden in images, audio/video files using steganography

- (a) Cryptography (b) Steganography
- (c) Cryptanalysis (d) Steganalysis

Q40 Attacker uses this server to connect with a network which is block through the firewall of the organization.

- (a) Web Server (b) FTP Server
- (c) Proxy Server (d) None of these

Q41 We can categorize threats as:

- (a) Passive attack (b) Active attack
- (c) Both a and b (d) None of them

Q42 Which among these is purpose of hacking

- (a) Greed (b) Revenge
- (c) Desire to access forbidden information (d) All

Q43 _____ are the symbols used by businesses to identify their goods and services.

- (a) Trade Mark (b) Trade Secret
- (c) Designs (d) None of them

Q44 _____ is a preparation towards preattack.

- (a) Passive attack (b) Active attack
- (c) Reconnaissance (d) None of them

Q45 Whenever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputaion concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person is said:

- (a) Cyber Stalking (b) Phishing
- (c) Social Engineering (d) Cyberdefamation

Q46 _____ cipher replaces one character with another character to create cipher text.

- (a) Substitution (b) Transposition
- (c) either (a) or (b) (d) neither (a) or (b)

Q47 Information Technology Act ITA was amended in _____ year in India

- (a) 2000 (b) 2004
- (c) 2008 (d) 2012

Q48 A cookie that was not created by the Web site that attempts to access it is called a

- (a) First-party cookie (b) Second-party cookie
- (c) Third-party cookie (d) Fourth-party cookie

Q49 A hacker who claims to be motivated by improving security by uncovering vulnerabilities is called.

- (a) Black hat attacker (b) White hat attacker
- (c) Cowboy attacker (d) Resource attacker

Q50 This mechanism is used to protect private networks from outside attack is

- (a) Firewall (b) Antivirus
- (c) Digital signature (d) Formatting

Q51 _____ can be used as IP address Multiplexer to enable to connect to number of computers on the internet.

- (a) Web Server (b) FTP Server
- (c) Proxy Server (d) None of these

Q52 Which term best describes the type of password attack that uses a large pregenerated data set of hashes from nearly every possible password?

- (a) Brute Force Attack (b) Dictionary Attack
- (c) Rainbow Table Attack (d) Host File Attack

Q53 This technology is used to determine and analyze human body uniqueness for authentication purpose.

- (a) Footprinting (b) Biometric
- (c) JBOD (d) Anthropomorphism

- Q54 Multiple ping packets are sent through ping command which results into more traffic than the victim can handle, in this type of denial of service attack
- Flood attack
 - Ping of death attack
 - SYN attack
 - Smurf attack
- Q55 It is a way of generating significant computer network traffic on a victim network.
- Flood attack
 - Ping of death attack
 - Teardrop attack
 - Smurf attack
- Q56 When the control of a web site is taken by an attacker is considered as
- Data Diddling
 - Salami
 - Web theft
 - Web Jacking
- Q57 This is installed between computer and Keyboard to generate the log of keys pressed by user.
- PC Key logger
 - Software key logger
 - Hardware key logger
 - None of them
- Q58 This process involves changing contents of a website depending upon a user's IP address and geographical location
- IP Base Clocking
 - IP Base Blocking
 - Industry Espionage
 - None of them
- Q59 Which among given is/are challenge(s) for any organization
- Employee wasted time on internet
 - Controlling Access to Web Application
 - Bandwidth Wastage
 - All of them
- Q60 This technique is used on a wireless network to scan the network passively.
- Scanning
 - Spoofing
 - Sniffing
 - All of them
- Q61 This is built feature of web browsers to warn about malicious sites by:
- Anti-phishing filters in IE and Firefox
 - Web of Trust
 - Clearing history of browser
 - Addlock Plus
- Q62 _____ is a social media computing allows people to connect and share information.
- Facebook
 - My Space
 - Linkedin
 - Twitter
- Q63 _____ is not a cloud sphere.
- Joint Sphere
 - User Sphere
 - Recipient Sphere
 - Client Sphere
- Q64 Secret key cryptography is synonymous with
- Symmetric Key Cryptography
 - Asymmetric key cryptography
 - Private key cryptography
 - Quantum Cryptography
- Q65 To encrypt a message from Aman to Alka using public key cryptography, the following is needed:
- Aman's private key
 - Aman's public key
 - Alka's private key
 - Alka's public key
- Q66 Which of the following protocols is used in accessing web mail?
- SMTP
 - HTTP
 - POP3
 - IMAP
- Q67 The buffer overflow attack is caused by
- A vulnerability in the design of a networking protocol
 - A Vulnerability in the implementation of a networking protocol
 - A vulnerability in human behaviour
 - A vulnerability in software
- Q68 A counter-measure to eavesdropping on the communication link is the use of
- A cryptography checksum
 - Encryption
 - A login name and password
 - A fake identity
- Q69 Poorly designed social networking sites are especially vulnerable to
- Buffer overflow attack
 - SQL injection attack
 - Non-Persistent cross-site scripting attacks
 - Persistent cross-site scripting attacks
- Q70 A SQL injection attack may be used to
- Change number of columns in a table
 - Read a row in a table
 - Change column name in a table
 - None of them
- Q71 The most effective remedy for SQL injection attacks is
- To filter HTML form input at the client side
 - To employ stored procedures on the database server
 - To employ prepared SQL statements on the web server
 - To perform input validation on the server via regular expression
- Q72 Tasks performed by firewall include
- Access Control
 - Packet Integrity Checking
 - IP address spoofing
 - All
- Q73 The role of a payment gateway is
- A proxy to the merchant
 - A proxy to the bankcard network
 - A financial service provider
 - A government regulator
- Q74 The motivation of an ethical hacker is
- Financial gain
 - The thrill of hacking
 - To desire to identify vulnerabilities so they can be patched before they are publicly exposed
 - A religious/political/ideological cause
- Q75 Which of the following is/are necessary feature(s) of a DDoS attack
- Use of a TCP SYN packets
 - Use of a spoofed IP address
 - Use of multiple attackers geographically dispersed
 - Use of malformed IP packets
- Q76 An attack originating and/or attempted within the security perimeter of an organization is _____ type of attack.
- Active
 - Inside
 - Passive
 - Outside
- Q77 The attacker usually installs the sniffers on the wireless network and conduct activity such as:
- Detection of SSID
 - Collecting MAC address
 - Collecting frame to crack WEP
 - All
- Q78 A Digital certificate is used to bind
- A person's public key to his private key
 - A person's public key to his identity
 - A person's private key to his identity
 - A person's signature to his private key
- Q79 Which of the following attacks is/are likely to result in identity theft?
- Phishing attack
 - Denial of Service attack
 - Virus Infection
 - All
- Q80 In which of the following does someone use an application to capture and manipulate packets as they are passing through your network?
- DoS
 - Backdoor
 - Man in Middle
 - Spoofing
- Q81 _____ is a "technique to influence" people to obtain the information or perform some action.
- Social Engineering
 - Phishing
 - Cyber stalking
 - None
- Q82 In this technique user tries to get the user disclose valuable personal data- such as credit card numbers, password, account data and other information by convincing the user to provide it under false pretenses.
- Phishing
 - Data Diddling
 - Salami
 - DoS

Q83 In this netizens to the website designed and developed by him, by altering the browser address bar through java script commands.

- (a) Flash Phishing
- (b) Web Forgery
- (c) Phone Phishing
- (d) Social Phishing

Q84 It involves harassing or threatening behavior that an individual will conduct repeatedly for following a person, visiting a person's home and/or business place

- (a) Phishing
- (b) Social Engineering
- (c) Cyber Stalking
- (d) None

Q85 Security risks from social engineering is/are

- (a) Malware distribution
- (b) Cyber bullying
- (c) Privacy concern
- (d) All

Q86 Threats are categorized as:

- (a) Passive or active
- (b) Traffic
- (c) Masquerade
- (d) Others

Q87 How are viruses spread?

- (a) Through Firewalls
- (b) Downloading infected programs and files from internet.
- (c) Garbled information.
- (d) Install anti-virus.

Q88 DDoS stand for

- (a) Distributed Denial of Service attack
- (b) Digital Data Output Spoit
- (c) Damaging Downtime of System
- (d) Distributed Destruction of System

Q89 _____ is not a kind of cyber attack.

- (a) Cber Stalking
- (b) Micro sites
- (c) Firewall attack
- (d) E-Mail

Q90 The latest WLAN standard is:

- (a) 802.11g
- (b) 802.11n
- (c) 802.12g
- (d) 802.12n

Q91 The following is used when the source code for a piece of software is unavailable

- (a) Blackbox testing
- (b) Whitebox testing
- (c) Regrsson testing
- (d) Unit testing

Q92 Which of the following is/are true of various forms of malware:

- (a) A worm attaches itself to a file or program
- (b) A Trojan is stand-alone program
- (c) A virus does not necessarily replicate
- (d) All of the above

Q93 _____ cryptography technique is used for ATM cards

- (a) Symmetric
- (b) Assymetric
- (c) Hashing
- (d) None

Q94 _____ cipher takes one character and replaces it with another.

- (a) Stream
- (b) Single
- (c) Substitution
- (d) Hash

Q95 The purpose of digital signatue is/are

- (a) Verify Sender
- (b) Prove Integrity of message
- (c) Prevent sender from disowing the message
- (d) All

Q96 _____ is the science of transforming information into a secure form so that unauthorized users cannot access it.

- (a) Steganography
- (b) Cryptography
- (c) Neither a nor b
- (d) Both a and b

Q97 A victim unknowingly downloads a Trojan horse virus is a _____ type of crime.

- (a) Type 1 Cyber crime
- (b) Type 2 Cyber crime
- (c) Type 3 Cyber crime
- (d) Type 4 Cyber crime

Q98 Survival mantra for netizens is are:

- (a) Keep genuine software
- (b) keep browsers updated with security patches
- (c) Keep an effective Antivirus and updates
- (d) All of them

Q99 _____ is a technique of changing an assigned Media Access Control address of a network Interface card to a different one

- (a) IP Spoofing
- (b) IP Filtering

(c) MAC Spoofing

(d) MAC Filtering

Q100 This is used by attacker to automatically dials a phone number looking for a computer on the other end.

- (a) Dialler
- (b) Auto dialler
- (c) Self dialler
- (d) War dialler

End Term Exam

Semester - VII

Roll No:

[Total No. of Pages:04]

Date:

Time: 90 minutes

Department:

Title of the Course: Cyber Security

Max. Marks: 100

Course Code: HUL 2401

- Q1 D DoS stand for
(a) Dual Disk Operating System
(b) Denial of Services
(c) Distributed Denial of Services
(d) None of these
- Q2 Which among these is a mail protocol
(a) SMTP (b) IMAP
(c) POP (d) All of them
- Q3 Which among these is a feature of Hashing
(a) Transposition (b) Availability
(c) either (a) or (b) (d) Neither (a) nor (b)
- Q4 Which of the following accurately reflects the purpose of steganography?
(a) Steganography scrambles a message so that it cannot be viewed
(b) Steganography hides the existence of the data.
(c) Steganography exposes hidden data.
(d) Steganography encrypts cleartext data.
- Q5 We don't want our packets to get lost in transit. Which OSI layer is responsible for ordered delivery of packets?
(a) Network (b) DataLink
(c) Transport (d) Physical
- Q6 Which term best describes the type of attack that makes it seem like two computers are communicating with each other, when actually they are sending and receiving data with a computer between them
(a) Phishing (b) Social Engineering
(c) Fraud (d) Cyber Stalking
- Q7 _____ is the criminal practice of using social engineering over telephone.
(a) Phishing (b) Mishing
(c) Vishing (d) Smishing
- Q8 _____ attack is a computer threat which attempts to exploit computer application vulnerability that are unknown to anybody in the world.
(a) Zero day (b) Vulnerability
(c) Data Diddling (d) Salami
- Q9 Which among given is a Bluetooth hacking tool?
(a) Bluejacking (b) Blue bugging
(c) Car Whispering (d) All of them
- Q10 In asymmetric cryptographic algorithm when Tom wants to send a message to Alisha he will decrypt it with
(a) His Public Key (b) Public key of Alisha
(c) His Private Key (d) Private key of Alisha
- Q11 This type of attack involves gathering information about individual about his/her knowledge, for example which the IN and OUT time of an employee.
(a) Passive attack (b) Active attack
(c) Forgery attack (d) None of these
- Q12 _____ are software programs installed on a computer system which usually are located between OS and keyboard hardware to record every key stroke
(a) Key Stroker (b) Key Logger
(c) Software Key logger (d) Anonymizers
- Q13 Which of the following is not a method to preserve the security and Integrity of Information?
(a) An Antivirus Software (b) Firewall
(c) Phishing (d) Disk Encryption
- Q14 To perform an attack in this technique attacker insert a new node 'X' between two existing nodes.
(a) Spoofing (b) Sniffing
(c) Man in Middle (d) DoS
- Q15 Which term best describes the type of attack that makes it possible to deny the service of a server using multiple computers from different geographical locations?
(a) Buffer Over flow (b) DoS
(c) Man in Middle (d) None of these
- Q16 A program advertised as performing one activity but actually doing something else, or performing both the advertised and malicious activities
(a) Trojan Horse (b) Virus
(c) Worm (d) Logic Bomb
- Q17 A _____ is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks.
(a) Trap door (b) Trojan Horse
(c) Worm (d) Logic Bomb
- Q18 Another name of Public Key Cryptography
(a) Symmetric Key Cryptography
(b) Private key Cryptography
(c) Asymmetric key Cryptography
(d) None of the above
- Q19 Difference between Data Integrity and Data Security is
(a) Limiting physical access to computer systems; assigning passwords to users.
(b) Consistent, accurate and reliable data; protection of data from unauthorized access.
(c) Encryption; Audit trails
(d) Distributing work to preserve integrity; installing system passwords
- Q20 The _____ is code embedded in some legitimate program that is set to "explode" when certain conditions are met
(a) Confidentiality (b) Integrity
(c) Availability (d) Authenticity
- Q21 It is a type of program do not replicate automatically?
(a) Worm (b) Zombie
(c) Trojan Horse (d) Logic Bomb
- Q22 Which of the following is independent malicious program that need not any host program?
(a) Trap doors (b) Trojan Horse
(c) Virus (d) Worm
- Q23 A _____ creates copies during replication that are functionally equivalent but have distinctly different bit patterns.
(a) Boot Sector Virus (b) Polymorphic Virus
(c) Parasitic Virus (d) Micro Virus

Q24 Doodle me Diddle fraud held in 1996 in India was a _____ type of cyber crime

- (a) Salami (b) Credit Card
- (c) Data Diddling (d) None of them

Q25 The purpose of a DoS attack is/are:

- (a) Flood a network with traffic, thereby preventing legitimate network traffic
- (b) Disrupt connection between two systems
- (c) Prevent a particular individual to access the service(s).
- (d) All of them

Q26 Which of the following is issued online for use over the Internet and is stored in an electronic device such as a chip card or computer memory?

- (a) Hard Cash (b) Business Card
- (c) E-Cash (d) E-Card

Q27 Gaining unauthorized access to a computer system would fall under which category of computer crime?

- (a) Hacking
- (b) Theft of Service
- (c) Destruction of data & Software
- (d) Data Theft

Q28 On day while working on your system you receive an email from an organization asking that you verify your account information within 12 hours, or your account will be closed, the best thing to do is

- (a) Reply to the email asking them why this information is required.
- (b) Reply to the email with the information asked for
- (c) report the email to the actual organization and then delete the email.
- (d) None of these

Q29 A _____ is a document that grant the holder exclusive right on an invention for fixed number of years.

- (a) Copy Right (b) Patent
- (c) Trade Mark (d) Trade Secret

Q30 An attempt to make a computer resource unavailable to its intended users is called

- (a) Denial of Service attack (b) Virus attack
- (c) Worm attack (d) Botnet Process

Q31 _____ is the simple process of intercepting wireless data that is broadcasted on unsecured network.

- (a) Spoofing (b) Sniffing
- (c) Spamming (d) None of them

Q32 Which of the following is a cyber crime?

- (a) Hacking (b) Worm Attack
- (c) Virus Attack (d) None of these

Q33 This attack involves altering raw data just before final processing and then changing it back after the processing is completed:

- (a) Data Tampering (b) Data Diddling
- (c) Salami Attack (d) None of these

Q34 _____ is a type of virus which effect/ infects the storage media on which OS is stored.

- (a) Boot Sector Virus (b) Program Virus
- (c) Multipartite Virus (d) Stealth Virus

Q35 Network administrator must do _____ to protect a wireless network.

- (a) MAC address filtering (b) Disabling SSID
- (c) Disabling Mac filtering (d) All of them

Q36 It is a technique breaking into phone or other communication systems.

- (a) Hacking (b) Cracking
- (c) Phreaking (d) War dialling

Q37 Ethical responsibilities of IT professionals include

- (a) Limiting risks (b) Minimizing cost
- (c) Maximizing profit (d) Minimizing testing

Q38 _____ is a generic term which refers to all the legal and regulate aspects of Internet and the World Wide Web

- (a) Cyber Law (b) Cyber Dyne
- (c) Cyber Cafe (d) Electroni Law

Q39 The art or science which detects messages that are hidden in images, audio/video files is known as

- (a) Cryptography (b) Steganography
- (c) Cryptanalysis (d) Steganalysis

Q40 Name the type of server used by attackers to connect with a network which is block through the firewall of the organization/ institution.

- (a) Web Server (b) FTP Server
- (c) Proxy Server (d) None of these

Q41 Threats can be categorize as:

- (a) Passive attack (b) Active attack
- (c) Both a and b (d) None of them

Q42 For a hacker the purpose of hacking is/are:

- (a) Greed (b) Revenge
- (c) Desire to access forbidden information (d) All

Q43 _____ are the symbols used by businesses to identify their goods and services.

- (a) Trade Mark (b) Trade Secret
- (c) Designs (d) None of them

Q44 _____ is a preparation towards preattack.

- (a) Passive attack (b) Active attack
- (c) Reconnaissance (d) None of them

Q45 Whenever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputaion concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person is said:

- (a) Cyber Stalking (b) Phishing
- (c) Social Engineering (d) Cyberdefamation

Q46 _____ cipher replaces one character with another character to create cipher text.

- (a) Substitution (b) Transposition
- (c) either (a) or (b) (d) neither (a) or (b)

Q47 In India Information Technology Act ITA was amended in _____ year.

- (a) 2000 (b) 2004
- (c) 2008 (d) 2012

Q48 A cookie that was not created by the Web site that attempts to access it is called a

- (a) First-party cookie (b) Second-party cookie
- (c) Third-party cookie (d) Fourth-party cookie

Q49 A hacker who claims to be motivated by improving security by uncovering vulnerabilities is called.

- (a) Black hat attacker (b) White hat attacker
- (c) Cowboy attacker (d) Resource attacker

Q50 This mechanism is used to protect private networks from outside attack is

- (a) Firewall (b) Antivirus
- (c) Digital signature (d) Formatting

Q51 _____ can be used as IP address Multiplexer to enable to connect to number of computers on the internet.

- (a) Web Server (b) FTP Server
- (c) Proxy Server (d) None of these

Q52 Which term best describes the type of password attack that uses a large pregenerated data set of hashes from nearly every possible password?

- (a) Brute Force Attack (b) Dictionary Attack
- (c) Rainbow Table Attack (d) Host File Attack

Q53 This technology is used to determine and analyze human body uniqueness for authentication purpose.

- (a) Footprinting (b) Biometric
- (c) JBOD (d) Anthropomorphism

- Q54 In this type of DoS attack attacker sends numbers of ping packets through ping command which result into more traffic than the victim can handle.
- (a) Flood attack (b) Ping of death attack
(c) SYN attack (d) Smurf attack
- Q55 It is a way of generating significant computer network traffic on a victim network.
- (a) Flood attack (b) Ping of death attack
(c) Teardrop attack (d) Smurf attack
- Q56 When the control of a web site is taken by an attacker is considered as
- (a) Data Diddling (b) Salami
(c) Web theft (d) Web Jacking
- Q57 This is installed between coputer and Keyboard to generate the log of keys pressed by user.
- (a) PC Key logger (b) Software key logger
(c) Hardware key logger (d) None of them
- Q58 Consider the following representation and fill appropriate keyword in the blank space concerning 'Trojan Horse'
Unlike Viruses ,they are -----programs
- (a) stand-alone (b) variable
(c) harmless (d) destructive
- Q59 Which among given is/are challenge(s) for any organization
- (a) Employee wasted time on internet
(b) Controlling Access to Web Application
(c) Bandwidth Wastage
(d) All of them
- Q60 In wireless network to scan the network passively which technique(s) is used.
- (a) Scanning (b) Spoofing
(c) Sniffing (d) All of them
- Q61 This is built feature of web browsers to warn about malicious sites by:
- (a) Anti-phishing filters in IE and Firefox
(b) Web of Trust
(c) Clearing history of browser
(d) Addlock Plus
- Q62 _____ is a social media computing allows people to connect and share information.
- (a) Facebook (b) My Space
(c) Linkedin (d) Twitter
- Q63 _____ is not a cloud sphere.
- (a) Joint Sphere (b) User Sphere
(c) Recipient Sphere (d) Client Sphere
- Q64 Secret key cryptography is synoymous with
- (a) Symmetric Key Cryptography
(b) Asymmetric key cryptography
(c) Private key cryptography
(d) Quantum Cryptography
- Q65 To encrypt a message from Aman to Alka using public key cryptography, the following is needed:
- (a) Aman's private key (b) Aman's public key
(c) Alka's private key (d) Alka's public key
- Q66 Which of the following protocols is used in accessing web mail?
- (a) SMTP (b) HTTP
(c) POP3 (d) IMAP
- Q67 The buffer overflow attack is caused by
- (a) A vulnerability in the design of a networking protocol
(b) A Vulnerability in the implementation of a networking protocol
(c) A vulnerability in human behaviour
(d) A vulnerability in software
- Q68 Which statement is/are true regarding 'Virus'
- (a) Some Viruses are helpful also
(b) It infects files through floppy,storage media,internet etc.
(c) both (a) and (b) are incorrect
(d) both (a) and (b) are correct
- Q69 Poorly designed social networking sites are especially vulnerable to
- (a) Buffer overflow attack (b) SQL injection attack
(c) Non- Persistent cross-site scripting attacks
(d) Persistent cross-site scripting attacks
- Q70 A SQL injection attack may be used to
- (a) Change number of coloumns in a table
(b) Read a row in a table
(c) Change coloumn name in a table
(d) None of them
- Q71 The most effective remedy for SQL injection attacks is
- (a) To filter HTML form input at the client side
(b) To employ stored procedures on the database server
(c) To employ prepared SQL statements on the web server
(d) To perform input validation on the server via regular expression
- Q72 Tasks performed by firewall include
- (a) Access Control (b) Packet Integrity Checking
(c) IP address spoofing (d) All
- Q73 The role of a payment gateway is
- (a) A proxy to the merchant
(b) A proxy to the bankcard network
(c) A financial service provider
(d) A government regulator
- Q74 Which is the most interesting facgtor that motivates a hacker
- (a) Financial gain
(b) The thrill of hacking
(c) To desire to identify vulnerabilities so they can be patched before they are publicaly exposed
(d) A religious/political/ideological cause
- Q75 SMURF is
- (a) DDoS
(b) Trapdoor
(c) antivirus
(d) None of these
- Q76 An attack originating and/or attempted within the security perimeter of an organization is _____ type of attack.
- (a) Active (b) Inside
(c) Passive (d) Outside
- Q77 The attacker usually installs the sniffers on the wireless network and conduct activity such as:
- (a) Detection of SSID (b) Collecting MAC address
(c) Collecting frame to crack WEP (d) All of them
- Q78 A Digital certificate is used to bind
- (a) A person's public key to his private key
(b) A person's public key to his identity
(c) A person's private key to his identity
(d) A person's signature to his private key
- Q79 Which of the following attacks is/are likely to result in identity theft?
- (a) Phishing attack (b) Denial of Service attack
(c) Virus Infection (d) All
- Q80 In which of the following does someone use an application to capture and manipulate packets as they are passing through your network?
- (a) DoS (b) Backdoor
(c) Man in Middle (d) Spoofing
- Q81 _____ is a "technique to influence" people to obtain the information or perform some action.
- (a) Social Engineering (b) Phishing
(c) Cyber stalking (d) None
- Q82 In this technique user tries to get the user disclose valuable personal data- such as credit card numbers, password, account data and other information by convicting the user to provide it under false pretenses.
- (a) Phishing (b) Data Diddling
(c) Salami (d) DoS
- Q83 Dumpster diving is an example of

- (a) Social Engineering (b) Phishing (a) Dialler (b) Auto dialler
(c) Fraud (d) Cyber Stalking (c) Self dialler (d) War dialler
- Q84 It involves harassing or threatening behavior that an individual will conduct repeatedly for following a person, visiting a person's home and/or business place
(a) Phishing (b) Social Engineering
(c) Cyber Stalking (d) None
- Q85 Security risks from social engineering is/are
(a) Malware distribution (b) Cyber bullying
(c) Privacy concern (d) All
- Q86 Threats are categorized as:
(a) Passive or active (b) Traffic
(c) Masquerade (d) Others
- Q87 How are viruses spread?
(a) Through Firewalls (b) Downloading infected programs and files from internet.
(c) Garbled information. (d) Install anti-virus.
- Q88 A challenge relating to Cyber-crimes is the collection of _____
(a) Electronic Evidence
(b) Paper Evidence
(c) Mechanical Evidence
(d) Hardware Evidence.
- Q89 _____ is not a kind of cyber attack.
(a) Cber Stalking (b) Micro sites
(c) Firewall attack (d) E-Mail
- Q90 The latest WLAN standard is:
(a) 802.11g (b) 802.11n
(c) 802.12g (d) 802.12n
- Q91 The following is used when the source code for a piece of software is unavailable
(a) Blackbox testing (b) Whitebox testing
(c) Regrssion testing (d) Unit testing
- Q92 Which of the following is/are true of various forms of malware:
(a) A worm attaches itself to a file or program
(b) A Trojan is stand-alone program
(c) A virus does not necessarily replicate
(d) All of the above
- Q93 _____ cryptography technique is used for ATM cards
(a) Symmetric (b) Assymetric
(c) Hashing (d) None
- Q94 _____ cipher takes one character and replaces it with another.
(a) Stream (b) Single
(c) Substitution (d) Hash
- Q95 The purpose of digital signatue is/are
(a) Verify Sender (b) Prove Integrity of message
(c) Prevent sender from disowing the message
(d) All
- Q96 _____ is the science of transforming information into a secure form so that unauthorized users cannot access it.
(a) Steganography (b) Cryptography
(c) Neither a nor b (d) Both a and b
- Q97 A victim unknowingly downloads a Trojan horse virus is a _____ type of crime.
(a) Type 1 Cyber crime (b) Type 2 Cyber crime
(c) Type 3 Cyber crime (d) Type 4 Cyber crime
- Q98 Survival mantra for netizens is are:
(a) Keep genuine software
(b) keep browsers updated with security patches
(c) Keep an effective Antivirus and updates
(d) All of them
- Q99 This process involves changing contents of a website depending upon a user's IP address and geographical location
(a) IP Base Clocking (b) IP Base Blocking
(c) Industry Espionage (d) None of them
- Q100 This is a program that automatically dials a phone number looking for a computer on the other end.