ZEAL EDUCATION SOCIETY'S

ZEAL POLYTECHNIC,PUNE

NARHE | PUNE -41 | INDIA

DEPARTMENT OF COMPUTER ENGINEERING

Question Bank for Multiple Choice Questions

Program: Diploma in Computer Engineering	**Program Code:- CO**
Scheme:- I	**Semester:- SIXTH**
Course:- Emerging Trends in Computer & IT	**Course Code:- 22618**
Unit 01 – Artificial Intelligence	**Marks:-06**

1.1 Introduction of AI
Concept
Scope of AI
Components of AI
Types of AI
Application of AI
1.2 Concept of machine learning and deep learning.

1. Which of these schools was not among the early leaders in AI research?
A. Dartmouth University
B. Harvard University
C. Massachusetts Institute of Technology
D. Stanford University
E. None of the above

2. DARPA, the agency that has funded a great deal of American AI research, is part of the Department of:
A. Defense
B. Energy
C. Education
D. Justice
E. None of the above

3. The conference that launched the AI revolution in 1956 was held at:
A. Dartmouth
B. Harvard
C. New York
D. Stanford
E. None of the above

4. What is the term used for describing the judgmental or commonsense part of the problem solving?
A. Heuristic
B. Critical
C. Value-based
D. Analytical
E. None of the above

5. What of the following is considered to be a pivotal event in the history of AI.

A. 1949, Donald O, The organization of Behavior.
B. 1950, Computing Machinery and Intelligence.
C. 1956, Dartmouth University Conference Organized by John McCarthy.
D. 1961, Computer and Computer Sense.
E. None of the above

6. A certain Professor at the Stanford University coined the word 'artificial intelligence' in1956 at a conference held at Dartmouth College. Can you name the Professor?

A. David Levy
B. John McCarthy
C. Joseph Weizenbaum
D. Hans Berliner
E. None of the above

7. The field that investigates the mechanics of human intelligence is:

A. History
B. cognitive science
C. psychology
D. sociology
E. None of the above

8. A.M. Turing developed a technique for determining whether a computer could or could not demonstrate the artificial Intelligence, Presently, this technique is called

A. Turing Test
B. Algorithm
C. Boolean Algebra
D. Logarithm
E. None of the above

9. The first AI programming language was called:

A. BASIC
B. FORTRAN
C. IPL
D. LISP
E. None of the above

10. What is Artificial intelligence?

A. Putting your intelligence into Computer
B. Programming with your own intelligence
C. Making a Machine intelligent
D. Putting more memory into Computer

11. Who is a father of AI?

A. Alain Colmerauer
B. John McCarthy
C. Nicklaus Wirth
D. Seymour Papert

12. Artificial Intelligence has its expansion in the following application.

A. Planning and Scheduling
B. Game Playing
C. Robotics
D. All of the above

13. The characteristics of the computer system capable of thinking, reasoning and learning isknown is

A. machine intelligence
B. human intelligence
C. artificial intelligence
D. virtual intelligence

14. The first AI programming language was called:

A. BASIC
B. FORTRAN
C. IPL
D. LISP

15. The first widely used commercial form of Artificial Intelligence (AI) is being used in many popular products like microwave ovens, automobiles and plug in circuit boards for desktop PCs.What is name of AI?

A. Boolean logic
B. Human logic
C. Fuzzy logic
D. Functional logic

16. What is the term used for describing the judgmental or commonsense part of the problem solving?

A. Heuristic
B. Critical
C. Value-based
D. Analytical

17. _____is a branch of computer science which deals with helping machines finds solutions to complex problems in a more human-like fashions

A. Artificial Intelligence
B. Internet of Things
C. Embedded System
D. Cyber Security

18. In_____the goal is for the software to use what it has learned in one area to solve problems in otherareas.

A. Machine Learning
B. Deep Learning
C. Neural Networks
D. None of these

19. Computer programs that mimic the way the human brain processes information is called as

A. Machine Learning
B. Deep Learning
C. Neural Networks
D. None of these

20. A_____is a rule of thumb, strategy, trick, simplification, or any other kind of device which drastically limits the search for solutions in large problem spaces.

A. Heuristic
B. Critical
C. Value based
D. Analytical

21. _____do not guarantee optimal/any solutions

A. Heuristic
B. Critical
C. Value based
D. Analytical

22. Cognitive science related with _____

A. Act like human
B. ELIZA
C. Think like human
D. None of the above

23. _____Model should reflect how results were obtained.

A. Design model
B. Logic model
C. Computational model
D. None of the above

24. Communication between man and machine is related with _____

A. LISP
B. ELIZA
C. All of the above
D. None of the above

25. ELIZA created by _____

A. John McCarthy
B. Steve Russell
C. Alain Colmerauer
D. Joseph Weizenbaum

26. The concept derived from_____level is propositional logic, tautology, predicate calculus, model, temporal logic.

A. Cognition level
B. Logic level
C. Functional level
D. All of the above

27. PROLOG is an AI programming language which solves problems with a form of symboliclogic known as_____.

A. Propositional logic
B. Tautology
C. Predicate calculus
D. Temporal logic

28. The_____level contains constituents at the third level which are knowledge-based system, heuristic search, automatic theorem proving, multi-agent system.

A. Cognition level
B. Gross level
C. Functional level
D. All of the above

29. PROLOG, LISP, NLP are the language of _____

A. Artificial Intelligence
B. Machine Learning
C. Internet of Things
D. Deep Learning

30. _____is used for AI because it supports the implementation of software that computes with symbolsvery well.

A. LISP
B. ELIZA
C. PROLOG
D. NLP

31. Symbols, symbolic expressions, and computing with those is at the core of _____

A. LISP
B. ELIZA
C. PROLOG
D. NLP

32. _____that deals with the interaction between computers and humans using the natural language

A. LISP
B. ELIZA
C. PROLOG
D. NLP

33. The core components are constituents of AI are derived from

A. Concept of logic
B. Cognition
C. Computation
D. All of the above

34. Aristotle's theory of syllogism and Descartes and Kant's critic of pure reasoning made knowledge on_____.

A. Logic
B. Computation logic
C. Cognition logic
D. All of the above

35. Charles Babbage and Boole who demonstrate the power of _____

A. Logic
B. Computation logic
C. Cognition logic
D. All of the above

36. In 1960s,_____pushed the logical formalism to integrate reasoning with knowledge.

A. Marvin Minsky
B. Alain Colmerauer
C. John McCarthy
D. None of above

37. Sensing organs as input, mechanical movement organs as output and central nervous system (CNS) inthe brain as control and computing devices is known as_____of human being

A. Information Control Paradigm
B. Information Processing Paradigm
C. Information Processing Control
D. None of the above

38. _____model was developed and incorporated in machines which mimicked the functionalities of human origin.

A. Functional model
B. Neural model
C. Computational model
D. None of the above

39. Chomsky's linguistic computational theory generated a model for syntactic analysis through_____

A. Regular Grammar
B. Regular Expression
C. Regular Word
D. None of these

40. Human to Machine is_____and Machine to Machine is_____.

A. Process, Process
B. Process, Program
C. Program, Hardware
D. Program, Program

41. Weak AI is also known as _____

A. Narrow AI
B. General AI
C. Neural AI
D. None of the above

42. _____AI is able to perform a dedicated task.

A. Narrow AI
B. General AI
C. Neural AI
D. None of the above

43. Narrow AI is performed multiple tasks at a time.

A. True
B. False

44. Weak AI is_____

A. The embodiment of human intellectual capabilities within a computer.
B. A set of computer programs that produce output that would be considered to reflect intelligence if it were generated by humans.

C. The study of mental faculties through the use of mental models implemented on a computer
D. All of the above
E. None of the above

45. Strong AI is_____
A. The embodiment of human intellectual capabilities within a computer.
B. A set of computer programs that produce output that would be considered to reflect intelligence if it were generated by humans.
C. The study of mental faculties through the use of mental models implemented on a computer
D. All of the above
E. None of the above

46. Artificial intelligence is_____
A. The embodiment of human intellectual capabilities within a computer.
B. A set of computer programs that produce output that would be considered to reflect intelligence if it were generated by humans.
C. The study of mental faculties through the use of mental models implemented on a computer
D. All of the above
E. None of the above

47. Apple Siri is a good example of_____AI.
A. Narrow AI B. General AI
C. Neural AI D. None of the above

48. IBM Watson supercomputer comes under_____AI.
A. Narrow AI B. General AI
C. Neural AI D. None of above

49. _____AI is a type of intelligence which could perform any intellectual task with efficiencylike human.
A. Narrow AI **B. General AI**
C. Super AI D. None of the above

50. The idea behind_____AI to make such a system which could be smarter and think likea human by its own.
A. Narrow AI **B. General AI**
C. Super AI D. None of the above

51. The worldwide researchers are now focusing on developing machines with_____AI.
A. Narrow AI **B. General AI**
C. Super AI D. None of the above

52. Playing chess, purchasing suggestions on e-commerce site, self-driving cars, speech recognition and image recognition are the example of__.
A. Narrow AI B. General AI
C. Super AI D. None of above

53. A machine can perform any task better than a human with cognitive properties is known as _____ AI.

A. Narrow AI
B. General AI
C. Super AI
D. None of the above

54. Ability to think, puzzle, make judgments, plan, learn, communication by its own is known as AI.

A. Narrow AI
B. General AI
C. Super AI
D. None of the above

55. _____AI is a hypothetical concept of AI.

A. Narrow AI
B. General AI
C. Super AI
D. None of the above

56. Which AI system not store memories or past experiences for future actions.

A. Reactive machine
B. Limited memory
C. Theory of mind
D. None of the above

57. Which machines only focus on current scenarios and react on it as per as possible best action.

A. Reactive machine
B. Limited memory
C. Theory of mind
D. None of the above

58. IBM's deep blue system is an example of_____.

A. Reactive machine
B. Limited memory
C. Theory of mind
D. None of the above

59. Google Alpha Go is an example of_____.

A. Reactive machine
B. Limited memory
C. Theory of mind
D. None of the above

60. Which can stores past experiences or some data for short period time.

A. Reactive machine
B. Limited memory
C. Theory of mind
D. None of above

61. The self-driving car is an example of_____.

A. Reactive machine
B. Limited memory
C. Theory of mind
D. None of the above

Ans: B [Car stores recent speed of nearby cars, the distance of others car, speed limit, other information to navigate the road]

62. Which AI should understand human emotions, people, and beliefs and be able to interact socially likehumans.

A. Reactive machine
B. Limited memory
C. Theory of mind
D. None of the above

63. Which machines will be smarter than human mind?

A. Reactive machine
B. Limited memory
C. Theory of mind
D. Self-Awareness

64. _____machines will have their own consciousness and sentiments

A. Reactive machine
B. Theory of mind
C. Self-Awareness
D. Both B & C

65. Which is not the commonly used programming language for AI?

A. PROLOG
B. LISP
C. Perl
D. Java script

66. What is Machine learning?

A. The autonomous acquisition of knowledge through the use of computer programs
B. The autonomous acquisition of knowledge through the use of manual programs
C. The selective acquisition of knowledge through the use of computer programs
D. The selective acquisition of knowledge through the use of manual programs

67_____is a branch of science that deals with programming the systems in such a waythat they automatically learn and improve with experience

A. Machine Learning
B. Deep Learning
C. Neural Networks
D. None of these

68. Classifying email as spam, labeling webpages based on their content, voice recognition arethe example of_____.

A. **Supervised learning**
B. Unsupervised learning
C. Machine learning
D. Deep learning

69. K-means, self-organizing maps, hierarchical clustering are the examples of_____.

A. Supervised learning
B. Unsupervised learning
C. Machine learning
D. Deep learning

70. Deep learning is a subfield of machine learning where concerned algorithms are inspired bythe structured and function of the brain called_____.

A. Machine learning
B. Artificial neural networks
C. Deep learning
D. Robotics

71. Machine learning is invented by_____.

A. John McCarthy
B. Nicklaus Wirth
C. Joseph Weizenbaum
D. Arthur Samuel

Prepared By Mr. Vijay B. Mohite	**Verified By** Module Coordinator	**Re-Verified By** Dept. Academic Coordinator	**Approved By** Prof. S.B. Tamboli HoD (Comp. Engg.)

Question Bank for Multiple Choice Questions

Program: Diploma in Computer Engineering	**Program Code:- CO**
Scheme:- I	**Semester:- SIXTH**
Course:- Emerging Trends in Computer & IT	**Course Code:- 22618**

Unit 02 – Internet of Things	**Marks:- 18**
2.1 Embedded Systems: Embedded system concepts, Purpose of embedded systems Architecture of embedded systems, Embedded processors-PIC, ARM, AVR, ASIC **2.2 IoT: Definition and characteristics of IoT** Physical design of IoT, Things of IoT, IoT Protocols, Logical design of IoT, IoT functional blocks, IoT Communication models, IoT Communication APIs, IoT Enabling Technologies, IoT levels and deployment templates, IoT Issues and Challenges, Applications IoT Devices and its features: Arduino, Uno, Raspberry Pi, Nodeμ, Case study on IoT Applications using various Sensors and actuators	

1. Embedded systems are_____
A. General-purpose
B. Special purpose

2. Embedded system is_____
A.An electronic system
B. A pure mechanical system
C. An electro-mechanical system
D. (A) or (C)

3. Which of the following is not true about embedded systems?
A. Built around specialized hardware
B. Always contain an operating system
C. Execution behavior may be deterministic
D. All of these
E. None of these

4. Which of the following is not an example of a "small-scale embedded system"?
A. Electronic Barbie doll
B. Simple calculator
C. Cell phone
D. Electronic toy car

5. The first recognized modern embedded system is
A. Apple computer
B. Apollo Guidance Computer (AGC)
C. Calculator
D. Radio navigation system

6. The first mass-produced embedded system is
A. Minuteman-I
B. Minuteman-II
C. Autonetics D-17
D. Apollo Guidance Computer (AGC)

7. Which of the following is an (are) an intended purpose(s) of embedded systems?
A. Data collection
B. Data processing
C. Data communication
D. All of these
E. None of these

8. Which of the following is (are) example(s) of an embedded system for data communication?
A. Network router
B. Digital camera
C. Music player
D.All of these
E. None of these

9. What are the essential tight constraints related to the design metrics of an embedded system?
A. Ability to fit on a single chip
B. Low power consumption
C. Fast data processing for real-time operations
D.All of the above

10. A digital multimeter is an example of an embedded system for
A. Data communication
B. Monitoring
C. Control
D. All of these
E. None of these

11. Which of the following is an (are) example(s) of an embedded system for signal processing?
A. Apple iPod (media player device)
B. SanDisk USB mass storage device
C. Both (A) and (B)
D. None of these

12. The instruction set of RISC processor is
A. Simple and lesser in number
B. Complex and lesser in number
C. Simple and larger in number
D. Complex and larger in number

13. Which of the following is true about CISC processors?
A. The instruction set is non-orthogonal
B. The number of general-purpose registers is limited
C. Instructions are like macros in c language
D. Variable-length instructions
E. All of these
F. None of these

14. Main processor chip in computers is_____
A. ASIC
B. ASSP
C. CPU
D. CPLD

15. Processors used in many microcontroller products need to be_____
A. high power
B. low power
C. low interrupt response
D. low code density

16. In microcontrollers, UART is acronym of_____
A. Universal Applied Receiver/Transmitter
B. Universal Asynchronous Rectified Transmitter
C. Universal Asynchronous Receiver/Transmitter
D. United Asynchronous Receiver/Transmitter

17. Which architecture is followed by general-purpose microprocessors?
A. Harvard architecture
B. Von Neumann architecture
C. None of the mentioned
D. All of the mentioned

18. Which architecture involves both the volatile and non-volatile memory?
A. Harvard architecture
B. Von Neumann architecture
C. None of the mentioned
D. All of the mentioned

19. Which architecture provides separate buses for program and data memory?
A. Harvard architecture
B. Von Neumann architecture
C. None of the mentioned
D. All of the mentioned

20. Harvard architecture allows:
A. Separate program and data memory
B. Pipe-ling
C. Complex architecture
D. All of the mentioned

21. Which of the following processor architecture supports easier instruction pipelining?
A. Harvard
B. Von Neumann
C. Both of them
D. None of these

22. Which of the following is an example of a wireless communication interface?
A. RS-232C
B. Wi-Fi
C. Bluetooth
D. EEE1394
E. Both (B) and (C)

23. ARM stands for _____
A. Advanced RISC Machine
B. Advanced RISC Methodology
C. Advanced Reduced Machine
D. Advanced Reduced Methodology

24. What is the processor used by ARM7?
A. 8-bit CISC
B. 8-bit RISC
C. 32-bit CISC
D. 32-bit RISC

25. The main importance of ARM microprocessors is providing operation with _____
A. Low cost and low power consumption
B. Higher degree of multi-tasking
C. Lower error or glitches
D. Efficient memory management

26. ARM processors where basically designed for _____
A. Mainframe systems
B. Distributed systems
C. Mobile systems
D. Supercomputers

27. ASIC chip is
A. Simple in design.
B. Manufacturing time is less.
C. It is faster
D. Both A&C.
28. ASIC stands for
A. Application-System Integrated Circuits
B. Application-Specific Integrated Circuits
C. Application-System Internal Circuits
D. Application-Specific Internal Circuits

29. In microcontrollers, I2C stands for
A. Inter-Integrated Clock
B. Initial-Integrated Clock
C. Intel-Integrated Circuit
D. Inter-Integrated Circuit

30. _____is the smallest microcontrollers which can be programmed to perform a large range of tasks.
A. PIC microcontrollers
B. ARM microcontrollers
C. AVR microcontrollers
D. ASIC microcontrollers

31. _____was developed in the year 1996 by ATMEL Corporation
A. PIC
B. AVR
C. ARM
D. ASIC

32. AVR stands for_____.
A. Advanced Virtual RISC
B. Alf-EgilBogen and VegardWollan RISC
C. Both A & B
D. None of the above

33. AVR microcontroller executes most of the instruction in_____.
A. Single execution cycle.
B. Double execution cycle.
C. Both A& B
D. None of the above.

34. The term "the Internet of things" was coined by
A. Edward L. Schneider
B. Kevin Ashton
C. John H.
D. Charles Anthony

35. The huge numbers of devices connected to the Internet of Things have to communicate automatically, not via humans, what is this called?
A. Bot to Bot(B2B)
B. Machine to Machine(M2M)
C. InterCloud
D. Skynet

36. What does "Things" in IoT refer to?
A. General device
B. Information
C. IoT devices
D. Object

37. Interconnection of Internet and computing devices embedded in everyday objects, enabling them to send and receive data is called_____
A. Internet of Things
B. Network Interconnection
C. Object Determination
D. None of these

38. _____is a computing concept that describes the idea of everyday physical objects being connected to the internet.
A. IoT (Internet of Things)
B. MQTT
C. COAP
D. SPI

39_____devices may support a number of interoperable communication protocols and communicate with other devices and also with infrastructure.
A. Artificial Intelligence
B. Machine Learning
C. Internet of Things
D. None of the above

40. Which one is not an element of IoT?
A. Process
B. People
C. Security
D. Things

41. IIOT stands for
A. Information Internet of Things
B. Industrial Internet of Things
C. Innovative Internet of Things
D. None of the above

42. Name of the IoT device which is first recognized?
A. Smart Watch
B. ATM
C. Radio
D. Video Game

43. _____is used by IoT
A. Radio information technology
B. Satellite
C. Cable
D. Broadband

44. _____consists of communication protocols for electronic devices, typically a mobile device and a standard device.
A. RFID
B. MQTT
C. NFC
D. None of the above

45. _____refers to establish a proper connection between all the things of IoT.
A. Connectivity
B. Analyzing
C. Sensing
D. Active Engagement

46. IOT devices which have unique identities and can perform_____.
A. Remote sensing
B. Actuating
C. Monitoring capabilities
D. All of the above

47. The sensed data communicated_____.
A. Cloud-based servers/storage.
B. I/O interfaces.
C. Internet connectivity.
D. None of the above

48. IoT devices are various types, for instance_____.
A. Wearable sensors
B. Smartwatches.
C. LED lights
D. All of the above

49. _____is a collection of wired Ethernet standard for the link layer.
A. IEEE 802.3
B. IEEE 802.11
C. IEEE 802.16
D. IEEE 802.15.4

50._____is a collection of WLAN communication standards.
A. IEEE 802.3
B. IEEE 802.11
C. IEEE 802.16
D. IEEE 802.15.4

51. ____is a collection of wireless broadband standards (WiMax).
A. IEEE 802.3
B. IEEE 802.11
C. IEEE 802.16
D. IEEE 802.15.4

52____is a collection of standards for LR-WPANs.
A. IEEE 802.3
B. IEEE 802.11
C. IEEE 802.16
D. IEEE 802.15.4

53. LR-WPANs standards from the basis of specifications for high-level communication protocol such as____.
A. Zigbee
B. Allsean
C. Tyrell
D. Microsoft's Azure

54. _____includes GSM and CDMA.
A. 2G
B. 3G
C. 4G
D. None of the above

55. _____include UMTS and CDMA2000.
A. 2G
B. 3G
C. 4G
D. None of the above

56_____include LTE.
A. 2G
B. 3G
C. 4G
D. None of the above

57._____layer protocols determine how the data is physically sent over the network's physical layer or medium.
A. Application layer
B. Transport layer
C. Network layer
D. Link-layer

58_____layer is responsible for sending of IP datagrams from the source network to the destination network.
A. Application layer
B. Transport layer
C. Network layer
D. Link-layer

59. ___layer performs the host addressing and packet routing.
A. Application layer
B. Transport layer
C. Network layer
D. Link-layer

60. _____protocols provide end to end message transfer capability independent of the underlying network.
A. Network layer
B. Transport layer
C. Application layer
D. Link-layer

61. The____protocols define how the applications interface with the lower-layer protocol to send the data over the network.
A. Application layer
B. Transport layer
C. Network layer
D. Link-layer

62. 6LOWPAN stands for
A. 6 LOW Personal Area Network
B. IPv6 LOW Personal Area Network
C. IPv6 over Low power wireless personal area network
D. None of the above

63. 802.3 is the standard for 10BASE5 Ethernet that uses_____cable as shared medium.
A. Twisted pair cable
B. Coaxial cable
C. Fiber optic cable
D. None of the above

64. IEEE 802.11 standards provide data rates _____
A. 10 Gbit/s.
B. 1 Gbit/s
C. 1 Mb/s to up to 6.75 Gb/s
D. 250 Kb/s

65. _____of the following is a protocol related to IoT
A. Zigbee
B. 6LoWPAN
C. CoAP
D. All of the above

66. _____is useful for time-sensitive application that have very small data units to exchange and do not want the overhead of connection setup.
A. TCP
B. UDP
C. Transport layer
D. None of the above.

67. _____protocol uses Universal Resource Identifiers (URIs) to identify HTTP resources.
A. HTTP
B. COAP
C. WebSocket
D. MQTT

68. The 10/100Mbit Ethernet support enables the board to connect to _____
A. LAN
B. MAN
C. WAN
D. WLAN

69. Which one out of these is not a data link layer technology?
A. Bluetooth
B. UART
C. Wi-Fi
D. HTTP

70. What is the size of the IPv6 Address?
A. 32 bits
B. 64 bits
C. 128 bits
D. 256 bits

71. MQTT stands for _____
A. MQ Telemetry Things
B. MQ Transport Telemetry
C. MQ Transport Things
D. MQ Telemetry Transport

72. MQTT is better than HTTP for sending and receiving data.
A. True
B. False

73. MQTT is_____protocol.
A. Machine to Machine
B. Internet of Things
C. Machine to Machine and Internet of Things
D. Machine Things

74. Which protocol is lightweight?
A. MQTT
B. HTTP
C. CoAP
D. SPI

75. MQTT is:
A. Based on client-server architecture
B. Based on publish-subscribe architecture
C. Based on both of the above
D. Based on none of the above

76**. XMPP is used for streaming which type of elements?**
A. XPL
B. XML
C. XHL
D. MPL

77. XMPP creates_____identity.
A. Device
B. Email
C. Message
D. Data

78. XMPP uses_____architecture.
A. Decentralized client-server
B. Centralized client-server
C. Message
D. Public/subscriber

79. What does HTTP do?
A. Enables network resources and reduces the perception of latency
B. Reduces perception of latency and allows multiple concurrency exchange
C. Allows multiple concurrent exchanges and enables network resources
D. Enables network resources and reduces the perception of latency and Allows multiple concurrent exchange.

80. HTTP expands?
A. HyperText Transfer Protocol
B. Hyper Terminal Transfer Protocol
C. HyperText Terminal Protocol
D. Hyper Terminal Text Protocol

81. CoAP is specialized in _____
A. Internet applications
B. Device applications
C. Wireless applications
D. Wired applications

82. Which protocol is used to link all the devices in the IoT?
A. TCP/IP
B. Network
C. UDP
D. HTTP

83. Data in network layer is transferred in the form of _____
A. Layers
B. Packets
C. Bytes
D. Bits

84. Services provided by the application layer?
A. Webchat
B. Error control
C. Connection services
D. Congestion control

85. TCP and UDP are called?
A. Application protocols
B. Session protocols
C. Transport protocols
D. Network protocols

86. The security-based connection is provided by which layer?
A. Application layer
B. Transport layer
C. Session layer
D. Network layer

87. Using which layer in transport layer data integrity can be assured?
A. Checksum
B. Repetition codes
C. Cyclic redundancy checks
D. Error correction codes

88. The transport layer receives data in the form of?
A. Packets
B. Byte streams
C. Bits stream
D. both packet and Byte stream

89. The network layer is considered as the_____?
A. Backbone
B. packets
C. Bytes
D. bits

90. The network layer consists of which hardware devices?
A. Router
B. Bridges
C. Switches
D. All of the above

91. Network layer protocol exits in_____?
A. Host
B. Switches
C. Packets
D. Bridges

92. Which protocol has a quality of service?
A. XMPP
B. HTTP
C. CoAP
D. MQTT

93. _____is a data-centric middleware standard for device-to-device and machine-to-machine communication.
A. Data Distribution Service (DDS)
B. Advanced Message Queuing Protocol (AMQP)
C. Extensible Messaging and Presence Protocol (XMPP)
D. Message Queue Telemetry Transport (MQTT)

94. _____is a bi-directional, fully duplex communication model that uses a persistent connection between client and server.
A. Request-Response
B. Publish-Subscriber
C. Push-Pull
D. Exclusive Pair

95. ___is a stateful communication model and the server is aware of all open connections.
A. Request-Response
B. Publish-Subscriber
C. Push-Pull
D. Exclusive Pair

96. Which is not an IoT communication model.
A. Request-Response
B. Publish-Subscribe
C. Push-Producer
D. Exclusive Pair

97. In Node MCU, MCU stands for_____.
A. Micro Control Unit
B. MicroController Unit
C. Macro Control Unit
D. Macro Controller Unit

98. REST is acronym for_____
A. Representational State Transfer
B. Represent State Transfer
C. Representational State Transmit
D. Representational Store Transfer

99. WSN stands for
A. Wide Sensor Network
B. Wireless Sensor Network
C. Wired Sensor Network
D. None of these

100. The benefit of cloud computing services
A. Fast
B. Anywhere access
C. Higher utilization
D. All of the above

101. PaaS stands for_____
A. Platform as a Service
B. Platform as a Survey
C. People as a Service
D. Platform as a Survey

102. _____as a Service is a cloud computing infrastructure that creates a development environment upon which applications may be build.
A. Infrastructure
B. Service
C. Platform
D. All of the mentioned

103. _____is a cloud computing service model in which hardware is virtualized in the cloud.
A. IaaS
B. CaaS
C. PaaS
D. None of the mentioned

104. Which of the following is the fundamental unit of the virtualized client in an IaaS deployment?
a) work unit
b) workspace
c) workload
d) all of the mentioned

105. _____offering provides the tools and development environment to deploy applications on another vendor's application.
A. PaaS
B. IaaS
C. CaaS
D. All of the mentioned

106._____is the most refined and restrictive service model.
A. IaaS
B. CaaS
C. PaaS
D. All of the mentioned

107. _____is suitable for IoT applications to have low latency or high throughput requirements.
A. REST
B. Publish-Subscriber
C. Push-Pull
D. WebSocket

108. ____is one of the most popular wireless technologies used by WSNs.
A. Zigbee
B. AllSean
C. Tyrell
D. Z-Wave

109. Zigbeespecification are based on_____.
A. 802.3
B. 802.11
C. 802.16
D. 802.15.4

110. ____is a transformative computing paradigm that involves delivering applications and services over the internet.
A. WSN
B. Cloud Computing
C. Big Data
D. None of the above

111. The process of collecting, organizing and collecting large sets of data called as
A. WSN
B. Cloud Computing
C. Big Data
D. None of the above

112. Does Raspberry Pi need external hardware?
A. True
B. False

113. Does RPi have internal memory?
A. True
B. False

114. What do we use to connect TV to RPi?
A. Male HDMI
B. Female HDMI
C. Male HDMI and Adapter
D. Female HDMI and Adapter

115. How power supply is done to RPi?
A. USB connection
B. Internal battery
C. Charger
D. Adapter

116. What is the Ethernet/LAN cable used in RPi?
A.Cat5
B.Cat5e
C. cat6
D .RJ45

117. Which instruction set architecture is used in Raspberry Pi?
A. X86
B. MSP
C. AVR
D. ARM

118. Does micro SD card present in all modules?
A. True
B. False

119. Which characteristics involve the facility the thing to respond in an intelligent way to a particular situation?
A. Intelligence
B. Connectivity
C. Dynamic Nature
D. Enormous Scale

120. _____empowers IoT by bringing together everyday objects.
A. Intelligence
B. Connectivity
C. Dynamic Nature
D. Enormous Scale

121. The collection of data is achieved with_____changes.
A. Intelligence
B. Connectivity
C. Dynamic Nature
D. Enormous Scale

122. The number of devices that need to be managed and that communicate with each other will be much larger.
A. Intelligence
B. Connectivity
C. Dynamic Nature
D. Enormous Scale

123. _____inIoT as one of the key characteristics, devices have different hardware platforms and networks.
A. Sensors
B. Heterogeneity
C. Security
D. Connectivity

124. Devices that transforms electrical signals into physical movements
A. Sensors
B. Actuators
C. Switches
D. Display
125. Stepper motors are_____
A. AC motors
B. DC motors
C. Electromagnets
D. None of the above

126. DC motors convert electrical into____energy.
A. Mechanical
B. Wind
C. Electric
D. None

127. Linear actuators are used in_____
A. Machine tools
B. Industrial machinery
C.both A and B
D.None

128. Solenoid is a specially designed _____
A. Actuator
B. Machine
C. Electromagnet
D. none of above

129. Stepper motors are_____
A. AC motors
B. DC motors
C. Electromagnets
D. None of the above

130. Accelerometer sensors are used in_____
A. Smartphones
B. Aircrafts
C. Both
D. None of the above

131. Image sensors are found in_____
A. Cameras
B. Night-vision equipment
C. Sonars
D. All of the above

132. Gas sensors are used to detect_____gases.
A. Toxic
B. Natural
C. Oxygen
D. Hydrogen

133. Properties of Arduino are:
A. Inexpensive
B. Independent
C. Simple
D. both A and C

134. Properties of IoT devices.
A. Sense
B. Send and receive data
C. Both A and B
D. None of the above

135. IoT devices are ____
A. Standard
B. Non-standard
C. Both
D. None

136. What is the microcontroller used in Arduino UNO?
A. ATmega328p
B. ATmega2560
C. ATmega32114
D. AT91SAM3x8E

137. ___is an open-source electronic platform based on easy to used hardware and software.
A. Arduino
B. Uno
C. Raspberry Pi
D. Node

138_____is used latching, locking, triggering.
A. Solenoid
B. Relay
C. Linear Actuator
D. Servo motors

139.____detect the presence or absence of nearby objects without any physical contact.
A. Smoke Sensor
B. Pressure Sensor
C. IR Sensor
D. Proximity Sensor

140____sensors include thermocouples, thermistors, resistor temperature detectors (RTDs) and integrated circuits (ICs).
A. Smoke Sensor
B. Temperature Sensor
C. IR Sensor
D. Proximity Sensor

141. The measurement of humidity is
A. RH
B. PH
C. IC
D. None of the above

142 ____sensor is used for automatic door controls, automatic parking system, automated sinks, automated toilet flushers, hand dryers.
A. Smoke Sensor
B. Temperature Sensor
C. IR Sensor
D. Motion Sensor

143 ____sensor measure heat emitted by objects.
A. Smoke Sensor
B. Temperature Sensor
C. IR Sensor
D. Proximity Sensor

Prepared By Mr. Vijay B. Mohite	**Verified By** Module Coordinator	**Re-Verified By** Dept. Academic Coordinator	**Approved By** Prof. S.B. Tamboli HoD (Comp. Engg.)

Question Bank for Multiple Choice Questions

Program: Diploma in Computer Engineering	**Program Code:- CO**
Scheme:- I	**Semester:- SIXTH**
Course:- Emerging Trends in Computer & IT	**Course Code:- 22618**

Unit 03 – Basics of Digital Forensic	**Marks:- 08**

3.1 Digital forensics
Introduction to digital forensic, History of forensic, Rules of digital forensic, Definition of digital forensic, Digital forensics investigation and its goal
3.2 Models of Digital Forensic Investigation
Road map for Digital Forensic Research (**RMDFR**) Investigative Model
Abstract Digital Forensics Model (ADFM)
Integrated Digital Investigation Process (IDIP)
End to End digital investigation process (EEDIP)
An extended model for cybercrime investigation
UML modeling of digital forensic process model (UMDFPM)
3.3 Ethical issues in digital forensic
General ethical norms for investigators, Unethical norms for investigation

1. Digital forensics is all of them except:
A. Extraction of computer data.
B. Preservation of computer data.
C. Interpretation of computer data.
D. Manipulation of computer data.

2. IDIP stands for
A. **Integrated Digital Investigation Process.**
B. Integrated Data Investigator Process.
C. Integrated Digital Investigator Process.
D. Independent Digital Investigator Process.

3. Who proposed Road Map for Digital Forensic Research (RMDFR)
A. G.Gunsh.
B. S.Ciardhuain
C. J.Korn.
D. G.Palmar

4. The investigator should satisfy the following points:
A. Contribute to society and human beings.
B. Avoid harm to others.
C. Honest and trustworthy.
D. All of the above

5. In the past, the method for expressing an opinion has been to frame a_____question based on available factual evidence.
A. **Hypothetical**
B. Nested
C. Challenging
D. Contradictory

6. More subtle because you are not aware that you are running these macros (the document opens and the application automatically runs); spread via email
A. The purpose of the copyright
B. The danger of macro viruses
C. Derivative works
D. computer-specific crime

7. There are three c's in computer forensics. Which is one of the three?
A. **Control**
B. Chance
C. Chains
D. Core

8. When Federal Bureau Investigation program was created?
A.1979
B.1984
C.1995
D.1989

9. When the field of PC forensics began?
A.1960's
B.1970's
C.1980's
D.1990's

10. What is Digital Forensic?
A. Process of using scientific knowledge in analysis and presentation of evidence in court
B. The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, the chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation
C. process where we develop and test hypotheses that answer questions about digital events
D. Use of science or technology in the investigation and establishment of the facts or evidence in a court of law

11. Digital Forensics entails .
A. Accessing the system's directories viewing mode and navigating through the various systems files and folders
B. Undeleting and recovering lost files
C. Identifying and solving computer crimes
D. The identification, preservation, recovery, restoration, and presentation of digital evidence from systems and devices

12. Which of the following is FALSE?
A. The digital forensic investigator must maintain absolute objectivity
B. It is the investigator's job to determine someone's guilt or innocence.
C. It is the investigator's responsibility to accurately report the relevant facts of a case.
D. The investigator must maintain strict confidentiality, discussing the results of an investigation on only a "need to know"

13. What is the most significant legal issue in computer forensics?
A. Preserving Evidence
B. Seizing Evidence
C. Admissibility of Evidence
D. Discovery of Evidence

14. _____phase includes putting the pieces of a digital puzzle together and developing investigative hypotheses
A. Preservation phase
B. Survey phase
C. Documentation phase
D. Reconstruction phase
E. Presentation phase

15. In_____phase investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location
A. Preservation phase
B. Survey phase
C. Documentation phase
D. Reconstruction phase
E. Presentation phase

16. In_____phase investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location
A. Preservation phase
B. Survey phase
C. Documentation phase
D. Reconstruction phase
E. Presentation phase

17. Computer forensics do not involve_____activity.
A. Preservation of computer data.
B. Extraction of computer data.
C. Manipulation of computer data.
D. Interpretation of computer data.

18. A set of instruction compiled into a program that perform a particular task is known as:
A. Hardware.
B.CPU
C. Motherboard
D. Software

19. Which of following is not a rule of digital forensics?
A. An examination should be performed on the original data
B. A copy is made onto forensically sterile media. New media should always be used if available.
C. The copy of the evidence must be an exact, bit-by-bit copy
D. The examination must be conducted in such a way as to prevent any modification of the evidence.

20. To collect and analyze the digital evidence that was obtained from the physical investigation phase, is the goal of which phase?
A. Physical crime investigation
B. Digital crime investigation.
C. Review phase.
D. Deployment phase.

21. To provide a mechanism to an incident to be detected and confirmed is purpose of which phase?
A. Physical crime investigation
B. Digital crime investigation.
C. Review phase.
D. Deployment phase.

22. Which phase entails a review of the whole investigation and identifies an area of improvement?
A. Physical crime investigation
B. Digital crime investigation.
C. Review phase.
D. Deployment phase

23. _____is known as father of computer forensic.
A. G. Palmar
B. J. Korn
C. Michael Anderson
D. S.Ciardhuain.

24. _____is well established science where various contribution have been made
A. Forensic
B. Crime
C. Cyber Crime
D. Evidence

25. Who proposed End to End Digital Investigation Process (EEDIP)?
A. G. Palmar
B. Stephenson
C. Michael Anderson
D. S.Ciardhuain

26. Which model of Investigation proposed by Carrier and Safford?
A. Extended Model of Cybercrime Investigation (EMCI)
B. Integrated Digital Investigation Process(IDIP)
C. Road Map for Digital Forensic Research (RMDFR)
D. Abstract Digital Forensic Model (ADFM)

27. Which of the following is not a property of computer evidence?
A. Authentic and Accurate.
B. Complete and Convincing.
C. Duplicated and Preserved.
D. Conform and Human Readable.

28. _____can makes or breaks investigation.
A. Crime
B. Security
C: Digital Forensic
D: Evidence

29. _____is software that blocks unauthorized users from connecting to your computer.
A. Firewall
B. Quick launch
C. OneLogin
D. Centrify

30. Which of the following are general Ethical norms for Investigator?
A. To contribute to society and human beings.
B. To avoid harm to others.
C. To be honest and trustworthy.
D. All of the above
E. None of the above

31. Which of the following are Unethical norms for Investigator?
A. Uphold any relevant evidence.
B. Declare any confidential matters or knowledge.
C. Distort or falsify education, training, credentials.
D. All of the above
E. None of the above

32. Which of the following is not a general ethical norm for Investigator?
A. To contribute to society and human beings.
B. Uphold any relevant Evidence.
C. To be honest and trustworthy.
D. To honor confidentially.

33. Which of the following is a not unethical norm for Digital Forensics Investigation?
A. Uphold any relevant evidence.
B. Declare any confidential matters or knowledge.
C. Distort or falsify education, training, credentials.
D. To respect the privacy of others.

34. What is called as the process of creation a duplicate of digital media for purpose of examining it?
A. Acquisition.
B. Steganography.
C. Live analysis
D. Hashing.

35. Which term refers to modifying a computer in a way which was not originally intended to view Information?
A. Metadata
B. Live analysis
C. Hacking
D. Bit Copy

36. The ability to recover and read deleted or damaged files from a criminal's computer is an example of a law enforcement specialty called?
A. Robotics
B. Simulation
C. Computer Forensics
D. Animation

37. What are the important parts of the mobile device which used in Digital forensic?
A. SIM
B. RAM
C. ROM.
D.EMMC chip

38. Using what, data hiding in encrypted images be carried out in digital forensics?
A. Acquisition.
B. Steganography.
C. Live analysis
D. Hashing.

39. Which of this is not a computer crime?
A. e-mail harassment
B. Falsification of data.
C. Sabotage.
D. Identification of data

40. Which file is used to store the user entered password?
A. .exe
B. .txt
C. .iso
D. .sam

41. _____is the process of recording as much data as possible to create reports and analysis on user input.
A. Data mining
B. Data carving
C. Metadata
D. Data Spoofing.

42. _____searches through raw data on a hard drive without using a file system.
A. Data mining
B. Data carving
C. Metadata
D. Data Spoofing.

43. What is the first step to Handle Retrieving Data from an Encrypted Hard Drive?
A. Formatting disk
B. Storing data
C. Finding configuration files.
D. Deleting Files

Prepared By Mr. Vijay B. Mohite	**Verified By** Module Coordinator	**Re-Verified By** Dept. Academic Coordinator	**Approved By** Prof. S.B. Tamboli HoD (Comp. Engg.)

Question Bank for Multiple Choice Questions

Program: Diploma in Computer Engineering	**Program Code:- CO**
Scheme:- I	**Semester:- SIXTH**
Course:- Emerging Trends in Computer & IT	**Course Code:- 22618**
Unit 04 – Digital Evidences	**Marks:- 10**

4.1 Digital Evidences Definition of Digital Evidence, Best Evidence Rule, Original Evidence
4.2 Rules of Digital Evidence
4.3 Characteristics of Digital Evidence Locard's Exchange Principle Digital Stream of bits
4.4 Types of evidence Illustrative, Electronics, Documented, Explainable, Substantial, Testimonial
4.5 Challenges in evidence handling-Authentication of evidence, Chain of custody, Evidence validation
4.6 Volatile evidence

1. The digital evidence are used to establish a credible link between____
a. Attacker and victim and the crime scene
b. Attacker and crime scene
c. victim and the crime scene
d. Attacker and Information

2. Digital evidences must follow the requirements of the _____
a. Ideal Evidences rule
b. Best Evidences rule
c. Exchange rule
d. All of the mentioned

3. From the two given statements 1 & 2, select the correct option from a-d
1) Original media can be used to carry out digital investigation process
2) By default, every part of the victim's computer is considered unreliable.
a. a and b both are true
b. a is true and b is false
c. a and b both are false
d. a is false and b is true

4. The evidences of proof that can be obtained from the electronic source is called the
a. Digital Evidence
b. Demonstrative Evidence
c. Explainable Evidence
d. Substantial Evidence

5. Which of the following is not a type of volatile evidence?
a. Routing Table
b. Main Memory
c. Log files
d. Cached Data

6. A valid definition of digital evidence is:
a. Data stored or transmitted using a computer
b. Information of probative value
c. Digital data of probative value
d. Any digital evidence on a computer

7. What are the three general categories of computer systems that can contain digital evidence?
a. Desktop, laptop, server
b. Personal computer, Internet, mobile telephone
c. Hardware, software, networks
d. Open computer systems, communication systems, embedded systems

8. In terms of digital evidence, a hard drive is an example of:
a. Open computer systems
b. Communication systems
c. Embedded computer systems
d. None of the above

9. In terms of digital evidence, a mobile telephone is an example of:
a. Open computer systems
b. Communication systems
c. Embedded computer systems
d. None of the above

10. In terms of digital evidence, a Smart Card is an example of:
a. Open computer systems
b. Communication systems
c. **Embedded computer systems**
d. None of the above

11. In terms of digital evidence, the Internet is an example of:
a. Open computer systems
b. Communication systems
c. Embedded computer systems
d. None of the above

12. Computers can be involved in which of the following types of crime?
a. Homicide and sexual assault
b. Computer intrusions and intellectual property theft
c. Civil disputes
d. All of the above

13. A logon record tells us that, at a specific time
a. An unknown person logged into the system using the account
b. The owner of a specific account logged into the system
c. The account was used to log into the system
d. None of the above

14. The criminological principle which states that, when anyone, or anything, enters a crime scene he/she takes something of the scene with him/her, and leaves something of himself/herself behind, is:
a. **Locard's Exchange Principle**
b. Differential Association Theory
c. Beccaria's Social Contract
d. None of the above

15. Personal computers and networks are often a valuable source of evidence. Those involved with------should be comfortable with this technology
a. Criminal investigation
b. Prosecution
c. Defense work
d. **All of the above**

16. Digital evidence is only useful in a court of law.
a.True
b. False

17. Video surveillance can be a form of digital evidence.
a.**True**
b. False

18. All forensic examinations should be performed on the original digital evidence.
a.True
b. False

19. Digital evidence can be duplicated exactly without any changes to the original data.
a.**True**
b. False

20. Computers were involved in the investigations into both World Trade Center attacks.
a.**True**
b. False

21. Computer professionals who take inappropriate actions when they encounter child pornography on their employer's systems can lose their jobs or break the law.
a.**True**
b. False

22. Digital evidence is always circumstantial.
a.True
b. False

23. Digital evidence alone can be used to build a solid case.
a.True
b. False

24. Automobiles have computers that record data such as vehicle speed, brake status, and throttle position when an accident occurs.
a.**True**
b. False

25. Computers can be used by terrorists to detonate bombs.
a.**True**
b.False

26. The aim of a forensic examination is to prove with certainty what occurred.
a.True
b. False

27. Even digital investigations that do not result in legal action can benefit from principles of forensic science.
a.**True**
b. False

28. Forensic science is the application of science to investigation and prosecution of crime or to the just resolution of conflict.
a.**True**
b. False

29. When a file is deleted from a hard drive, it can often be recovered.
a.**True**
b. False

30. Preservation of digital evidence can involve which of the following?
a. Collecting computer hardware
b. Making a forensic image of storage media
c. Copying the files that are needed from storage media
d. All of the above

31. Examination of digital evidence includes (but is not limited to) which of the following activities?
a. Seizure, preservation, and documentation
b. **Recovery, harvesting, and reduction**
c. Experimentation, fusion, and correlation
d. Arrest, interviewing, and trial

32. Analysis of digital evidence includes which of the following activities?
a.Seizure, preservation, and documentation
b.**Experimentation, fusion, and correlation**
c. Recovery, harvesting, and reduction
d. Arrest, interviewing, and trial

33. Evidence can be related to its source in which of the following ways?
a. Top, middle, bottom
b. IP address, MD5 value, filename, date-time stamps
c. Production, segment, alteration, location
d. Parent, uncle, orphan

34. Different types of analysis include which of the following?
a.**Relational (e.g., link analysis) and temporal (e.g., timeline analysis)**
b.Cryptography
c. Metadata hashing
d.Digital photography

35. When a website is under investigation, before obtaining authorization to seize the systems it is necessary to:
a. **Determine where the web servers are located**
b. Inform personnel at the web server location that you'll be coming to seize the systems
c. Conduct a reconnaissance probe of the target website
d.None of the above

36. Which of the following is NOT an information gathering process?
a. Scanning the system remotely
b. Studying security audit reports
c. Attempting to bypass logon security
d. Examining e-mail headers

37. Unlike law enforcement, system administrators are permitted to_____on their network when it is necessary to protect the network and the data it contains.
a.Open unread e-mails.
b. Monitor network traffic.
c. Modify system logs.
d. Divulge user personal information.

38. Although it was not designed with evidence collection in mind,_____can still be useful for examining network traffic.
a.EnCase
b. FTK
c. Wireshark
d. CHKDSK

39. Issues to be aware of when connecting to a computer over a network and collecting information include:
a.Creating and following a set of standard operating procedures
b.Keeping a log of actions taken during the collection process
c. Documenting which server actually contains the data that's being collected
d.**All of the above**

40. When a computer contains digital evidence, it is always advisable to turn it off immediately.
a.True
b. False

41. A forensic image of a hard disk drive preserves the partition table.
a.**True**
b. False

42. All forensic tools acquire digital evidence from storage media in the same way.
a.True
b. False

43. It is not necessary to sanitize/wipe a hard drive purchased directly from a manufacturer.
a.True
b. False

44. Chain of custody enables anyone to determine where a piece of evidence has been, who handled it when, and what was done to it since it was seized.
a.**True**
b. False

45. No two files can have the same MD5 value.
a.True
b. False

46. After the MD5 value of a piece of digital evidence has been calculated, any change in that piece of evidence can be detected.
a.**True**
b. False

47. When drawing up an affidavit for a warrant, it is important to specifically mention all desired digital evidence.
a.**True**
b. False

48. When seeking authorization to search a network and digital evidence that may exist in more than one jurisdiction it is not necessary to obtain a search warrant for each location.
a.True
b. False

49. Digital investigators should remember that evidence can reside in unexpected places, such as network routers.
a.**True**
b. False

50. Active monitoring is time consuming, invasive, and costly and should only be used as a last resort.
a.**True**
b. False

51. A digital evidence class characteristic is similar to tool mark analysis in the physical world.
a.**True**
b. False

52. TCP/IP network traffic never contains useful class characteristics.

a.True

b. False

53. It is not possible to recover deleted system or network log files.

a.True

b. False

54. Having a member of the search team trained to handle digital evidence:

a. Can reduce the number of people who handle the evidence

b. Can serve to streamline the presentation of the case

c. Can reduce the opportunity for opposing counsel to impugn the integrity of the evidence

d. All of the above

55. A digital investigator pursuing a line of investigation in a case because that line of investigation proved successful in two previous cases is an example of:

a. Logical reasoning

b. Common sense

c. Preconceived theory

d. Investigator's intuition

56. Regarding the admissibility of evidence, which of the following is not a consideration:

a. Relevance

b. Authenticity

c. Best evidence

d. **Nominally prejudicial**

57. According to the text, the most common mistake that prevents evidence seized from being admitted is:

a.Uninformed consent

b. Forcible entry

c. Obtained without authorization

d. None of the above

58. The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as:

a. Chain of custody

b. Field notes

c. Interim report

d. None of the above

59. When assessing the reliability of digital evidence, the investigator is concerned with whether the computer that generated the evidence was functioning normally, and:

a. Whether chain of custody was maintained

b. Whether there are indications that the actual digital evidence was tampered with

c. Whether the evidence was properly secured in transit

d. Whether the evidence media was compatible with forensic machines

60. The fact that with modern technology, a photocopy of a document has become acceptable in place of the original is known as:

a. Best evidence rule

b. Due diligence

c. ***Quid pro quo***

d. ***Voir dire***

61. Evidence contained in a document provided to prove that statements made in court are true is referred to as:
a. Inadmissible evidence
b. Illegally obtained evidence
c. Hearsay evidence
d. Direct evidence

62. Business records are considered to be an exception to:
a. Direct evidence
b. Inadmissible evidence
c. Illegally obtained evidence
d. Hearsay evidence

63. Direct evidence establishes a:
a. Fact
b. Assumption
c. Error
d. Line of inquiry

64. There is no need for any specialized training in the collection of digital evidence.
a. True
b. False

65. It is the duty of a digital investigator to ignore influences from any source.
a. True
b. False

66. The application of preconceived theories to a particular case is a good method of reducing caseload.
a.True **b. False**

67. In the United States, the prosecution must prove guilt beyond a reasonable doubt.
a. True
b. False

68. Chain of custody is the process of documenting who has handled evidence, where and when, as it travels from the crime scene to the courts.
a. True
b. False

69. Typically, a photocopy of a document is considered hearsay evidence and is not admissible in court.
a. True
b. False

70. Direct evidence establishes a fact.
a.**True**
b. False

71. Coerced testimony is the most common mistake that prevents evidence seized from being admitted.
a.True
b. False

72. Determining whether digital evidence has been tampered with is a major concern of the digital examiner.
a.**True**
b. False

73. Exceeding the scope of a warrant is not likely to affect the admissibility of the evidence collected.
a.True
b. False

74. Digital evidence cannot be direct evidence because of its separation from the events it represents.
a.True
b. False

75. When creating an expert report, digital investigators should support assertions in their reports with multiple independent sources of evidence.
a.**True**
b. False

76. Voir dire is the process of becoming accepted as an expert by the court.
a.**True**
b. False

77. During testimony, when a lawyer appears not to be tech savvy, it is a good practice to guess what the attorney is trying to ask.
a.True
b. False

78. A proper response to a question that you do not know the answer to is, "I don't know."
a.**True**
b. False

79. The term "computer contaminant" refers to:
a.Excessive dust found inside the computer case
b.Viruses, worms, and other malware
c. Spam e-mails
d. Nigerian scam e-mails

80. In those states with legislation addressing computer forgery, contraband in the form of "forgery devices" may include:
a.Computers
b. Computer equipment
c. Specialized computer software
d. All of the above

81. Hacking is an example of:
a. Computer-assisted crime
b. Computer-related crime
c. Computer-integrity crime
d. Computer malfeasance crime

82. Forgery is an example of:
a. **Computer assisted crime**
b. Computer-related crime
c. Computer-integrity crime
d. Computer malfeasance crime

83. Jurisdiction claims may be based on:
a.Location of the perpetrator's computer
b.Location of the victim's computer
c.Location of intermediary computers
d. **All of the above**

84. The goal of an investigation is to:
a.Convict the suspect
b.**Discover the truth**
c.Find incriminating evidence
d.All of the above

85. An investigation can be hindered by the following:
a. Preconceived theories
b. b. Improperly handled evidence
c. Offender concealment behavior
d. **All of the above**

86. Forensic examination involves which of the following:
a.Assessment, experimentation, fusion, correlation, and validation
b.Seizure and preservation
c. **Recovery, harvesting, filtering, organization, and search**
d. All of the above

87. Forensic analysis involves the following:
a. **Assessment, experimentation, fusion, correlation, and validation**
b. Seizure and preservation
c. Recovery, harvesting, filtering, organization, and search
d.All of the above

88. The first step in applying the scientific method to a digital investigation is to:
a. Form a theory on what may have occurred
b. Experiment or test the available evidence to confirm or refute your prediction
c. **Make one or more observations based on events that occurred**
d. Form a conclusion based on the results of your findings

89. Which of the following should the digital investigator consider when arranging for the transportation of evidence?
a.Should the evidence be physically in the possession of the investigator at all times?
b.Will the evidence copies be shared with other experts at other locations?
c. Will there be environmental factors associated with the digital media?
d.**All of the above**

90. Generating a plan of action and obtaining supporting resources and materials falls under which step in the digital investigation?
a. Preparation
b. Survey/identification
c. Preservation
d. Examination and analysis

91. Forensic examination and forensic analysis are separate processes.
a.**True**
b. False

92. When a network is involved in a crime, investigators must seize and preserve all systems on the network.
a.True
b. False

93. When seizing a computer, it is always acceptable to lose the contents of RAM.
a.True
b. False

94. Case management is a critical part of digital investigations.
a.**True**
b. False

95. Forensic examination is the process of extracting, viewing, and analyzing information from the evidence collected.
a.**True**
b. False

96. The crime scene preservation process includes all but which of the following:
a.Protecting against unauthorized alterations
b.Acquiring digital evidence
c.**Confirming system date and time**
d.Controlling access to the crime scene

97. The challenge to controlling access to a digital crime scene is that:
a.**Information may be stored on Internet servers in different locations.**
b.The computer may be shared.
c.The computer case may be locked.
d.None of the above.

98. When presenting evidence on an organizational network, the digital investigator may require the assistance of:
a.**System administrators**
b.The CEO of the organization
c.The CSO (Chief Security Officer)
d.Additional forensic investigators

99. The proper collection of evidence at a crime scene is crucial in terms of admissibility in court.
a.**True**
b. False

100. The investigation and study of victim characteristics is known as:
a.Criminal profiling
b.Behavioral imprints
c.**Victimology**
d.Crime scene analysis

101. One reason digital investigators write threshold assessments more often than full reports is because:
a.They will be included in a final report, and so, distribute the time for final report preparation over the entire period of the investigation.
b.They keep their supervisor aware of their productivity.
c.**They take less time to prepare and may be sufficient to close out an investigation.**
d.They serve as field notes for the investigator.

102. One reason not to put too much trust into those who run the company's computers is that:
a.There has always been an antagonism between system administrators and law enforcement.
b.They are typically too busy to take the time to answer your questions.
c.They are usually not authorized to answer questions.
d.**They may be the offenders.**

103. Although crime scenes are typically photographed, it is a good idea to create diagrams of the crime scene because:

a. Diagramming is a common crime scene technician's skill; however, it requires continual practice.

b. **The process of creating a diagram can result in a digital investigator noticing an important item of evidence that would otherwise have been missed.**

c. The quality of photographs taken at the crime scene is not known until the film is developed.

d. **None of the above**

104. When processing the digital crime scene in a violent crime investigation it is important to have __to ensure that all digital evidence and findings can hold up under close scrutiny.

a. A good supply of electrostatic bags for holding sensitive electronic components

b. More than one reliable camera for photographing the crime scene

c. **Standard operating procedures for processing a digital crime scene**

d. A good supply of nitrile gloves

Prepared By Mr. Vijay B. Mohite	**Verified By** Module Coordinator	**Re-Verified By** Dept. Academic Coordinator	**Approved By** Prof. S.B. Tamboli HoD (Comp. Engg.)

Question Bank for Multiple Choice Questions

Program: Diploma in Computer Engineering	**Program Code:- CO**
Scheme:- I	**Semester:- SIXTH**
Course:- Emerging Trends in Computer & IT	**Course Code:- 22618**
Unit 05 – Basics of Hacking	**Marks:- 12**

5.1 Ethical Hacking- How Hackers Beget Ethical Hackers, Defining hacker, Malicious users
5.2 Understanding the need to hack your own systems
5.3 Understanding the dangers your systems face- Nontechnical attacks, Network-infrastructure attacks, Operating-system attacks, Application and other specialized attacks
5.4 Obeying the Ethical hacking Principles- Working ethically, Respecting privacy, Not crashing your systems
5.5 The Ethical hacking Process- Formulating your plan, Selecting tools, Executing the plan, Evaluating results, Moving on
5.6 Cracking the Hacker Mind-set- What You"re Up Against?, Who breaks in to computer systems? Why they do it? Planning and Performing Attacks Maintaining Anonymity

1. Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as _____
a) Black Hat hackers
b) White Hat Hackers
c) Grey Hat Hackers
d) Red Hat Hackers
Answer: b
Explanation: White Hat Hackers are cyber security analysts and consultants who have the intent to help firms and Governments in the identification of loopholes as well as help to perform penetration tests for securing a system.

2. Which is the legal form of hacking based on which jobs are provided in IT industries and firms?
a) Cracking
b) Non ethical Hacking
c) Ethical hacking
d) Hactivism
Answer: c
Explanation: Ethical Hacking is an ethical form of hacking done by white-hat hackers for performing penetration tests and identifying potential threats in any organizations and firms.

3. They are nefarious hackers, and their main motive is to gain financial profit by doing cybercrimes. Who are "they" referred to here?
a) Gray Hat Hackers
b) White Hat Hackers
c) Hactivists
d) Black Hat Hackers
Answer: d
Explanation: Black Hat hackers also termed as „crackers" and are a major type of cyber criminals who take unauthorized access in user"s account or system and steal sensitive data or inject malware into the system for their profit or to harm the organization.

4. _____are the combination of both white as well as black hat hackers.
a) Grey Hat hackers
b) Green Hat hackers
c) Blue Hat Hackers
d) Red Hat Hackers
Answer: a
Explanation: Grey Hat Hackers have a blending character of both ethical as well as un-ethical hacker. They hack other"s systems for fun but do not harm the system, exploits bugs and vulnerabilities in network without the knowledge of the admin or the owner.

5. The amateur or newbie in the field of hacking who don't have many skills about coding and in-depth working of security and hacking tools are called _____
a) Sponsored Hackers
b) Hactivists
c) Script Kiddies
d) Whistle Blowers
Answer: c
Explanation: Script Kiddies are new to hacking and at the same time do not have many interests in developing coding skills or find bugs of their own in systems; rather they prefer downloading of available tools (developed by elite hackers) and use them to break any system or network. They just try to gain attention of their friend circles.

6. Suicide Hackers are those _____
a) who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity
b) individuals with no knowledge of codes but an expert in using hacking tools
c) who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints
d) who are employed in an organization to do malicious activities on other firms
Answer: a
Explanation: Suicide hackers are those who break into any network or system with or without knowing the consequences of the cybercrime and its penalty. There are some suicide hackers who intentionally do crimes and get caught to bring their names in the headlines.

7. Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____
a) State sponsored hackers
b) Blue Hat Hackers
c) Cyber Terrorists
d) Red Hat Hackers
Answer: c
Explanation: Cyber Terrorists are very expert programmers and cyber criminals who hide themselves while doing malicious activities over the internet and they are smart enough to hide themselves or their tracks of action. They are hired for gaining unauthorized access to nation"s data centres or break into the network of intelligence agencies.

8. One who disclose information to public of a company, organization, firm, government and private agency and he/she is the member or employee of that organization; such individuals are termed as _____

a) Sponsored hackers
b) Crackers
c) Hactivist
d) Whistleblowers

Answer: d

Explanation: Whistleblowers are those individuals who is a member or an employee of any specific organization and is responsible for disclosing private information of those organizations, firms, either government or private.

9. These types of hackers are the most skilled hackers in the hackers' community. Who are "they" referred to?

a) White hat Hackers
b) Elite Hackers
c) Licensed Penetration Testers
d) Red Hat Hackers

Answer: b

Explanation: The tag "Elite hackers" are considered amongst the most reputed hackers who possess most of the hacking and security skills. They are treated with utmost respect in the hackers" community. Zero day vulnerabilities, serious hacking tools and newly introduced bugs are found and developed by them.

10. _____are those individuals who maintain and handles IT security in any firm or organization.

a) IT Security Engineer
b) Cyber Security Interns
c) Software Security Specialist
d) Security Auditor

Answer: a

Explanation: This is an intermediary level of position of an individual in an organization or firm who builds and preserves different systems and its associated security tools of the firm of organization to which he/she belongs.

11. Role of security auditor is to _____

a) secure the network
b) probe for safety and security of organization"s security components and systems
c) detects and prevents cyber-attacks and threats to organization
d) does penetration testing on different web applications

Answer: b

Explanation: Security auditors are those who conduct auditing of various computer and network systems on an organization or company and reports the safety and security issues as well as helps in suggesting improvements or enhancements in any particular system that is threat prone.

12. _____are senior level corporate employees who have the role and responsibilities of creating and designing secured network or security structures.

a) Ethical Hackers
b) Chief Technical Officer
c) IT Security Engineers
d) Security Architect

Answer: d

Explanation: Security architect are those senior grade employees of an organization who are in charge of building, designing, implementing and testing of secured network topologies, protocols as well as secured computers in an organization.

13. _____security consultants uses database security monitoring & scanning tools to maintain security to different data residing in the database / servers / cloud.

a) Database
b) Network
c) System
d) Hardware

Answer: a

Explanation: Database Security consultants are specific individuals hired in order to monitor and scan the database systems and keep them secured from unwanted threats and attacks by giving access to restricted users, blocking unwanted files, multi-factor access control etc.

14. Governments hired some highly skilled hackers. These types of hackers are termed as _____

a) Special Hackers
b) Government Hackers
c) Cyber Intelligence Agents
d) Nation / State sponsored hackers

Answer: d

Explanation: Nation / State sponsored hackers are specific individuals who are employed or hired by the government of that nation or state and protect the nation from cyber terrorists and other groups or individuals and to reveal their plans, communications and actions.

15. Someone (from outside) who tests security issues for bugs before launching a system or application, and who is not a part of that organization or company are _____

a) Black Hat hacker
b) External penetration tester
c) Blue Hat hacker
d) White Hat Hacker

Answer: c

Explanation: Blue Hat Hackers are outsiders yet security testers who are temporarily hired for performing outsourced security test for bugs and vulnerabilities in any system before launching it to the market or making the application live.

16. The full form of Malware is _____

a) Malfunctioned Software
b) Multipurpose Software
c) Malicious Software
d) Malfunctioning of Security

Answer: c

Explanation: Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

17. Who deploy Malwares to a system or network?

a) Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
b) Criminal organizations, White hat hackers, malware developers, cyber-terrorists
c) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
d) Criminal organizations, gray hat hackers, Malware developers, Penetration testers

Answer: a

Explanation: Criminal-minded organizations, groups and individuals cyber-terrorist groups, Black hat hackers, malware developers etc are those who can deploy malwares to any target system or network in order to deface that system.

18. _____is a code injecting method used for attacking the database of a system / website.
a) HTML injection
b) SQL Injection
c) Malicious code injection
d) XML Injection
Answer: b
Explanation: SQLi (Structured Query Language Injection) is a popular attack where SQL code is targeted or injected; for breaking the web application having SQL vulnerabilities. This allows the attacker to run malicious code and take access to the database of that server.

19. XSS is abbreviated as _____
a) Extreme Secure Scripting
b) Cross Site Security
c) X Site Scripting
d) Cross Site Scripting
Answer: d
Explanation: Cross Site Scripting is another popular web application attack type that can hamper the reputation of any site.

20. This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?
a) SQL injection
b) HTML Injection
c) Cross Site Scripting (XSS)
d) Cross Site Request Forgery (XSRF)
Answer: c
Explanation: XSS attack can be infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage (usually a blogging page). This can hamper the reputation of a site and the attacker may place any private data or personal credentials.

21. When there is an excessive amount of data flow, which the system cannot handle,_____attack takes place.
a) Database crash attack
b) DoS (Denial of Service) attack
c) Data overflow Attack
d) Buffer Overflow attack
Answer: d
Explanation: The Buffer overflow attack takes place when an excessive amount of data occurs in the buffer, which it cannot handle and lead to data being over-flow into its adjoined storage. This attack can cause a system or application crash and can lead to malicious entry-point.

22. Compromising a user's session for exploiting the user's data and do malicious activities or misuse user's credentials is called _____
a) Session Hijacking
b) Session Fixation
c) Cookie stuffing
d) Session Spying
Answer: a
Explanation: Using session hijacking, which is popularly known as cookie hijacking is an exploitation method for compromising the user"s session for gaining unauthorized access to user"s information.

23. Which of this is an example of physical hacking?
a) Remote Unauthorised access
b) Inserting malware loaded USB to a system
c) SQL Injection on SQL vulnerable site
d) DDoS (Distributed Denial of Service) attack
Answer: b
Explanation: If a suspicious gain access to server room or into any confidential area with a malicious pen-drive loaded with malware which will get triggered automatically once inserted to USB port of any employee"s PC; such attacks come under physical hacking, because that person in gaining unauthorized physical access to any room or organization first, then managed to get an employee"s PC also, all done physically – hence breaching physical security.

24. Which of them is not a wireless attack?
a) Eavesdropping
b) MAC Spoofing
c) Wireless Hijacking
d) Phishing
Answer: d
Explanation: Wireless attacks are malicious attacks done in wireless systems, networks or devices. Attacks on Wi-Fi network is one common example that general people know. Other such sub-types of wireless attacks are wireless authentication attack, Encryption cracking etc.

25. An attempt to harm, damage or cause threat to a system or network is broadly termed as _____
a) Cyber-crime
b) Cyber Attack
c) System hijacking
d) Digital crime
Answer: b
Explanation: Cyber attack is an umbrella term used to classify different computer & network attacks or activities such as extortion, identity theft, email hacking, digital spying, stealing hardware, mobile hacking and physical security breaching.

26. Which method of hacking will record all your keystrokes?
a) Keyhijacking
b) Keyjacking
c) Keylogging
d) Keyboard monitoring
Answer: c
Explanation: Keylogging is the method or procedure of recording all the key strokes/keyboard button pressed by the user of that system.

27. _____are the special type of programs used for recording and tracking user's keystroke.
a) Keylogger
b) Trojans
c) Virus
d) Worms
Answer: a
Explanation: Keyloggers are surveillance programs developed for both security purpose as well as done for hacking passwords and other personal credentials and information. This type of programs actually saves the keystrokes done using a keyboard and then sends the recorded keystroke file to the creator of such programs.

28. Stuxnet is a _____
a) Worm
b) Virus
c) Trojan
d) Antivirus
Answer: a
Explanation: Stuxnet is a popular and powerful worm that came into existence in mid 2010, which was very powerful as it was accountable for the cause of huge damage to Iran"s Nuclear program. It mainly targets the PLCs (Programmable Logic Controllers) in a system.

29. According to the CIA Triad, which of the below-mentioned element is not considered in the triad?
a) Confidentiality
b) Integrity
c) Authenticity
d) Availability
Answer: c
Explanation: According to the CIA triad the three components that a security need is the Confidentiality, Integrity, Availability (as in short read as CIA) .

30. _____is the latest technology that faces an extra challenge because of CIA paradigm.
a) Big data
b) Database systems
c) Cloud storages
d) Smart dust
Answer: a
Explanation: Big data has additional challenges that it has to face because of the tremendous volume of data that needs protection as well as other key elements of the CIA triad, which makes the entire process costly and time-consuming.

31. One common way to maintain data availability is _____
a) Data clustering
b) Data backup
c) Data recovery
d) Data Altering
Answer: b
Explanation: For preventing data from data-loss, or damage data backup can be done and stored in a different geographical location so that it can sustain its data from natural disasters & unpredictable events.

32. _____is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
a) Network Security
b) Database Security
c) Information Security
d) Physical Security
Answer: c
Explanation: Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information for alteration, destruction, deletion or disclosure by unauthorised users.

33. From the options below, which of them is not a vulnerability to information security?
a) flood
b) without deleting data, disposal of storage media
c) unchanged default password
d) latest patches and updates not done
Answer: a
Explanation: Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

34. __platforms are used for safety and protection of information in the cloud.
a) Cloud workload protection platforms
b) Cloud security protocols
c) AWS
d) One Drive
Answer: a
Explanation: Nowadays data centres support workloads from different geographic locations across the globe through physical systems, virtual machines, servers, and clouds. Their security can be managed using Cloud workload protection platforms which manage policies regarding security of information irrespective of its location.

35. _____technology is used for analyzing and monitoring traffic in network and information flow.
a) Cloud access security brokers (CASBs)
b) Managed detection and response (MDR)
c) Network Security Firewall
d) Network traffic analysis (NTA)
Answer: d
Explanation: Network traffic analysis (NTA) is an approach of information security for supervising the traffic in any network, a flow of data over the network as well as malicious threats that are trying to breach the network. This technological solution also helps in triage the events detected by Network Traffic Analysing tools.

36. Compromising confidential information comes under _____
a) Bug
b) Threat
c) Vulnerability
d) Attack
Answer: b
Explanation: Threats are anything that may cause damage or harm to a computer system, individual or any information. Compromising of confidential information means extracting out sensitive data from a system by illegal manner.

37. Lack of access control policy is a _____
a) Bug
b) Threat
c) Vulnerability
d) Attack
Answer: c
Explanation: Access control policies are incorporated to a security system for restricting of unauthorised access to any logical or physical system. Every security compliance program must need this as a fundamental component. Those systems which lack this feature is vulnerable.

38. Possible threat to any information cannot be _____
a) reduced
b) transferred
c) protected
d) ignored
Answer: d
Explanation: When there lies a threat to any system, safeguards can be implemented, outsourced, distributed or transferred to some other system, protected using security tools and techniques but cannot be ignored.

39. How many basic processes or steps are there in ethical hacking?
a) 4
b) 5
c) 6
d) 7
Answer: c
Explanation: According to the standard ethical hacking standards, the entire process of hacking can be divided into 6 steps or phases. These are: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Tracks clearing, reporting.

40. _____is the information gathering phase in ethical hacking from the target user.
a) Reconnaissance
b) Scanning
c) Gaining access
d) Maintaining access
Answer: a
Explanation: Reconnaissance is the phase where the ethical hacker tries to gather different kinds of information about the target user or the victim"s system.

41. Which of the following is not a reconnaissance tool or technique for information gathering?
a) Hping
b) NMAP
c) Google Dorks
d) Nexpose
Answer: d
Explanation: Hping, NMAP & Google Dorks are tools and techniques for reconnaissance. Nexpose is a tool for scanning the network for vulnerabilities.

42. There are_____subtypes of reconnaissance.
a) 2
b) 3
c) 4
d) 5
Answer: a
Explanation: Reconnaissance can be done in two different ways. 1st, Active Reconnaissance which involves interacting with the target user or system directly in order to gain information; 2nd, Passive Reconnaissance, where information gathering from target user is done indirectly without interacting with the target user or system.

43. Which of the following is an example of active reconnaissance?
a) Searching public records
b) Telephone calls as a help desk or fake customer care person
c) Looking for the target"s details in the database
d) Searching the target"s details in paper files
Answer: b
Explanation: As active reconnaissance is all about interacting with target victim directly, hence telephonic calls as a legitimate customer care person or help desk person, the attacker can get more information about the target user.

44. Which of the following is an example of passive reconnaissance?
a) Telephonic calls to target victim
b) Attacker as a fake person for Help Desk support
c) Talk to the target user in person
d) Search about target records in online people database
Answer: d
Explanation: Passive reconnaissance is all about acquiring of information about the target indirectly, hence searching any information about the target on online people database is an example of passive reconnaissance.

45. Which of them does not comes under scanning methodologies?
a) Vulnerability scanning
b) Sweeping
c) Port Scanning
d) Google Dorks
Answer: d
Explanation: Google dork is used for reconnaissance, which uses special search queries for narrowing down the search results. The rest three scanning methodologies are used for scanning ports (logical), and network vulnerabilities.

46. Which of them is not a scanning tool?
a) NMAP
b) Nexpose
c) Maltego
d) Nessus
Answer: c
Explanation: NMAP is used for both reconnaissance and scanning purposes. Nepose and Nessus are fully scanning tool. Maltego is an example of a reconnaissance tool used for acquiring information about target user.

47. Which of the following comes after scanning phase in ethical hacking?
a) Scanning
b) Maintaining access
c) Reconnaissance
d) Gaining access
Answer: d
Explanation: Gaining access is the next step after scanning. Once the scanning tools are used to look for flaws in a system, it is the next phase where the ethical hackers or penetration testers have to technically gain access to a network or system.

48. In_____phase the hacker exploits the network or system vulnerabilities.
a) Scanning
b) Maintaining access
c) Reconnaissance
d) Gaining access
Answer: d
Explanation: Penetration testers after scanning the system or network tries to exploit the flaw of the system or network in “gaining access” phase.

49. A_____can gain access illegally to a system if the system is not properly tested in scanning and gaining access phase.
a) security officer
b) malicious hacker
c) security auditor
d) network analyst
Answer: b
Explanation: Malicious hackers can gain illegal access at OS level, application level or network level if the penetration testers or ethical hackers lack in testing and reporting the vulnerabilities in a system.

50. Which of the following hacking tools and techniques hackers’ do not use for maintaining access in a system?
a) Rootkits
b) Backdoors
c) Trojans
d) Wireshark
Answer: d
Explanation: Wireshark is not a tool for maintaining access because it is used for analysing network protocols at a microscopic level (very minutely). It is an interactive tool for data traffic analysing on any computer.

51. In_____phase, the hackers try to hide their footprints.
a) Scanning
b) Tracks clearing
c) Reconnaissance
d) Gaining access
Answer: b
Explanation: Tracks clearing or covering tracks is the name of the phase where the hackers delete logs of their existence & other activity records they do during the hacking process. This step is actually an unethical one.

52. Which of them is not a track clearing technique?
a) Altering log files
b) Tunnelling
c) Port Scanning
d) Footprint removing
Answer: c
Explanation: Port scanning is a method used in the scanning phase. Altering or changing log files, tunnelling for hiding your identity and removing footprints from different sites are examples of clearing tracks.

53. _____is the last phase of ethical hacking process.
a) Scanning
b) Tracks clearing
c) Reconnaissance
d) Reporting
Answer: d

54. Ethical Hacking is also known as

a) Black Hat hacking
b) White Hat hacking
c) Encrypting
d) None of these

55. Tool(s) used by ethical hackers____

a) Scanner
b) Decoder
c) Proxy
d) All of these

56. Vulnerability scanning in Ethical hacking finds

a) Strengths
b) **Weakness**
c) a & b
d) None of these

57. Ethical hacking will allow to_____all the massive security breaches.

a) Remove
b) measure
c) Reject
d) None of these

58. Sequential steps hackers use are ,__,__,__

A) Maintaining Access
B) Reconnaissance
C) Scanning
D) Gaining Access

a) B, C, D, A
b) B, A C, D
c) A, B, C, D
d) D, C, B, A

59. _____phase in ethical hacking is known as the pre-attack phase.

a) Reconnaissance
b) Scanning
c) Gaining access
d) Maintaining access

Answer: b

Explanation: In the scanning phase, the hacker actively scans for the vulnerabilities or specific information in the network which can be exploited.

Prepared By Mr. Vijay B. Mohite	**Verified By** Module Coordinator	**Re-Verified By** Dept. Academic Coordinator	**Approved By** Prof. S.B. Tamboli HoD (Comp. Engg.)

Question Bank for Multiple Choice Questions

Program: Diploma in Computer Engineering	**Program Code:- CO**
Scheme:- I	**Semester:- SIXTH**
Course:- Emerging Trends in Computer & IT	**Course Code:- 22618**

Unit 06 – Types of Hacking	**Marks:- 16**

6.1 Network Hacking
Network Infrastructure, Network Infrastructure Vulnerabilities, Scanning-Ports, Ping sweeping, Scanning SNMP, Grabbing Banners, Analysing Network Data and Network Analyzer, MAC-daddy attack
Wireless LANs: Implications of Wireless Network Vulnerabilities, Wireless Network Attacks
6.2 Operating System Hacking
Introduction of Windows and Linux Vulnerabilities
6.3 Applications Hacking
Messaging Systems- Vulnerabilities, E-Mail Attacks- E-Mail Bombs, Banners, Best practices for minimizing e-mail security risks
Web Applications: Web Vulnerabilities, Directories Traversal and Countermeasures,
Database system- Database Vulnerabilities, Best practices for minimizing database security risks

1. SNMP stands for
a) Simple Network Messaging Protocol
b) Simple Network Mailing Protocol
c) Simple Network Management Protocol
d) Simple Network Master Protocol

2. Which of the following tool is used forNetwork Testing and port scanning?
a) NetCat
b) SuperScan
c) NetScan
d) **All of Above**

3. Banner grabbing is often used for
a) White Hat Hacking
b) Black Hat Hacking
c) Gray Hat Hacking
d) Script Kiddies

4. An attacker can create an_____attack by sending hundreds or thousands of e-mails with very large attachments.
a) Connection Attack
b) Auto responder Attack
c) Attachment Overloading Attack
c) All of the above

5. An email bomb is also known as
a) Post bomb
b) Internet bomb
c) Letter bomb
d) All of the above

6. _____is any action that might compromise cyber-security.
a) Threat
b) Vulnerability
c) Exploit
d) Attack
Answer: a
Explanation: Threat can be termed as a possible danger that may lead to breach the cyber security and may cause possible harm to the system or the network.

7. Existence of weakness in a system or network is called _____
a) Threat
b) Vulnerability
c) Exploit
d) Attack
Answer: b
Explanation: Vulnerability is the term used to define weakness in any network or system that can get exploited by an attacker. Exploiting the weakness can lead to the unexpected & undesirable event in cyber security.

8. _____is an act of hacking by the means of which a political or social message is conveyed.
a) Hacktivism
b) Whistle-blowing
c) Surveillance
d) Pseudonymization
Answer: a
Explanation: Hacktivism is an act of defacing a website, or any network or system. Systems and networks are compromised with a political or social agenda.

9. _____is the method of developing or creating a structurally similar yet unauthentic and illegitimate data of any firm or company.
a) Data copying
b) Data masking
c) Data breaching
d) Data duplicating
Answer: b
Explanation: Data masking is the method used for developing or creating a structurally similar version of data of any organization that is not authentic. These types of unauthentic data are purposefully created for protecting the actual data.

10. Data masking is also known as _____
a) Data obfuscation
b) Data copying
c) Data breaching
d) Data duplicating
Answer: a
Explanation: Data obfuscation is the alternate term used for data masking, that is used for developing or creating a structurally similar version of data of any organization that is not authentic. These types of unauthentic data are purposefully created for protecting the actual data

11. Backdoors are also known as _____
a) Trap doors
b) Front doors
c) Cover doors
d) Back entry
Answer: a
Explanation: Trap-doors are hidden entry points in any already hacked system that is set to bypass security measures.

12. Adware are pre-chosen_____developed to display ads.
a) banner
b) software
c) malware
d) shareware
Answer: b
Explanation: Adware is software that is displayed on system or web pages for showing pre-chosen ads.

13. _____is an attack technique occurs when excess data gets written to a memory block.
a) Over buffering
b) Buffering
c) Buffer overflow
d) Memory full
Answer: c
Explanation: Buffer overflow is a flaw that occurs in memory when excessive data is written which makes the buffer allocated to seize.

14. _____is an attempt to steal, spy, damage or destroy computer systems, networks or their associated information.
a) Cyber-security
b) Cyber-attack
c) Digital hacking
d) Computer security
Answer: b
Explanation: Cyber-attack can be defined as an attempt to steal, spy, damage or destroy different components of cyberspace such as computer systems, associated peripherals, network systems, and information.

15. _____is a device which secretly collects data from credit / debit cards.
a) Card Skimmer
b) Data Stealer
c) Card Copier
d) Card cloner
Answer: a
Explanation: Card skimmer is hardware that is installed and setup in ATMs secretly so that when any user will swipe or insert their card in the ATM, the skimmer will fetch all information from the magnetic strip.

16. _____is the way or technique through which majority of the malware gets installed in our system.
a) Drive-by click
b) Drive-by redirection
c) Drive-by download
d) Drive-by injecting USB devices
Answer: c

Explanation: An accidental yet dangerous action that takes place in the cyberspace which helps attackers place their malware into the victim's system. This technique is called Drive-by download.

17. _____is the hacking approach where cyber-criminals design fake websites or pages for tricking or gaining additional traffic.

a) Cyber-replication
b) Mimicking
c) Website-Duplication
d) Pharming

Answer: a

Explanation: The technique and approach through which cyber-crooks develop fake web pages and sites to trick people for gaining personal details such as login ID and password as well as personal information, is known as pharming.

18. RAM-Scraping is a special kind of malware that looks (scrape) for sensitive data in the hard drive.

a) True
b) False

Answer: a

Explanation: It is a special kind of malware that looks for sensitive data that you've stored in your hard drive. RAM-scraping is one of those kinds.

19. When you book online tickets by swiping your card, the details of the card gets stored in _____

a) database system
b) point-of-sale system
c) servers
d) hard drives

Answer: b

Explanation: The point-of-sale system is a system where the retailer or company stores financial records and card details of the e-commerce system or online business transactions.

20. _____are deadly exploits where the vulnerability is known and found by cyber-criminals but not known and fixed by the owner of that application or company.

a) Unknown attacks
b) Secret attacks
c) Elite exploits
d) Zero-day exploits

Answer: d

Explanation: Zero-day exploits are used to attack a system as soon as cyber-criminals came to know about the weakness or the day the weaknesses are discovered in a system. Hackers exploit these types of vulnerabilities before the creator releases the patch or fix the issue.

21. Zero-day exploits are also called _____

a) zero-day attacks
b) hidden attacks
c) un-patched attacks
d) un-fixed exploits

Answer: a

Explanation: Zero-day exploits are also called zero-day attacks where the vulnerability is known and found by cyber-criminals or ethical hackers but not known and fixed by the creator/owner of that application or company.

22. There are_____major types of ports in computers.
a) 1
b) 2
c) 3
d) 4
Answer: b
Explanation: There are 2 major types of ports in computer systems. These are physical ports and logical ports.

23. PS2 and DVI are examples of Logical ports.
a) True
b) False
Answer: b
Explanation: PS2 and DVI are examples of physical ports. Physical ports can be touched and seen with our naked eyes.

24. Physical ports are usually referred to as _____
a) jacks
b) cables
c) interfaces
d) hardware plugs
Answer: c
Explanation: Physical ports are connections that connect two systems for their interactions. LAN, PS2 and DVI are examples of physical ports.

25. _____are logical numbers assigned for logical connections.
a) Logical ports
b) Physical ports
c) Networking cables
d) IP address
Answer: a
Explanation: Logical ports are end-point to a logical connection. The numbers are pre-assigned by IANA (Internet Assigned Numbers Authority) which ranges from 0 – 65536.

26. Logical ports are also known as _____
a) numbered ports
b) virtual numbering
c) virtual ports
d) network protocol ports
Answer: c
Explanation: Logical ports are also known as virtual ports which are part of TCP/IP networking. The numbers of ports are pre-assigned by IANA (Internet Assigned Numbers Authority) which ranges from 0 – 65536.

27. Which of the following is the port number for FTP data?
a) 20
b) 21
c) 22
d) 23
Answer: a
Explanation: Port number 20 is the logical port number for FTP data service. FTP protocol is a standard protocol used for transmitting and receiving files from client to server through a network.

28. Which of the following is the port number for SMTP data?
a) 20
b) 21
c) 25
d) 23
Answer: c

29. Which of the following is the port number for FTP control?
a) 20
b) 21
c) 22
d) 23
Answer: b

Explanation: Port number 21 is the logical port number for FTP control service. FTP protocol is a standard protocol used for transmitting and receiving files from client to server through a network.
30. Which of the following is the port number for SSH (Secure Shell)?
a) 20
b) 21
c) 22
d) 23
Answer: c
Explanation: Port number 22 is the logical port number for Secure Shell service. SSH gives users (specifically system administrators), a way to securely access computers on unsecured network connectivity.

31. Which of the following is the port number for Telnet?
a) 20
b) 21
c) 22
d) 23
Answer: d
Explanation: Port number 23 is the logical port number for Telnet. Telnet is used for bi-directional communication over the internet in text-oriented format. It also gives virtual terminal connectivity.

32. Which of the following are the port numbers for IPSec service?
a) 50, 51
b) 49, 50
c) 51, 52
d) 23, 24
Answer: a
Explanation: Port numbers 50 and 51 are the logical port numbers for IPSec service. IPSec is a standard protocols suite used among 2 communication points that help in providing data authentication, confidentiality, and integrity.

33. Which of the following are the port numbers for DHCP?
a) 66, 67
b) 67, 68
c) 65, 66
d) 68, 69
Answer: c
Explanation: Port numbers 67 and 68 are the logical port numbers for Dynamic Host Configuration Protocol (DHCP) service. It helps in providing Internet Protocol (IP) host automatically along with related configuration information like subnet mask and default gateway.

34. Which of the following is the port number for TFTP service?
a) 69
b) 70
c) 71
d) 72
Answer: a
Explanation: Port number 69 is the logical port number for Trivial File Transfer Protocol (TFTP) service. It is an internet software utility protocol used for transferring files.
35. Port 80 handles unencrypted web traffic.
a) True
b) False
Answer: a
Explanation: Ports are assigned to different services for identification of which port is sending traffic over the network. Port 80 is used by the popular HTTP (Hyper Text Transfer Protocol) that handles unencrypted web traffic.

36. Why it is important to know which service is using which port number?
a) For database security
b) For reporting data security to the auditor
c) For understanding which data is going through secured traffic and which is not
d) For checking unused data traffic
Answer: c
Explanation: If a security analyst or ethical hacker knows which port is open and through which port data is going, he/she will be able to know which data is going in encrypted form and which one is not. Also, it helps in securing a system by closing the logical ports so that hackers cannot gain access through them.

37. Which of the following is the port number for HTTP?
a) 79
b) 80
c) 81
d) 82
Answer: b
Explanation: Port number 80 is the logical port number for the popular Hyper-Text Transfer Protocol (HTTP) service. This protocol defines how messages are formatted and transmitted over unencrypted traffic.

38. Which of the following is the port number for POP3?
a) 110
b) 111
c) 112
d) 113
Answer: a
Explanation: Port number 110 is the logical port number for Post Office Protocol-3 service. This protocol periodically checks our mail-box for synchronizing our latest emails with that of the server.

39. Which of the following is the port number for SNMP?
a) 160
b) 161
c) 162
d) 163
Answer: b
Explanation: Port number 161 is the logical port number for Simple Network Management Protocol (SNMP) service. It's an application layer protocol that helps in managing and monitoring our network devices.

40. Firewalls can be of_____kinds.
a) 1
b) 2
c) 3
d) 4
Answer: c
Explanation: Firewalls are of three kinds – one is the hardware firewalls, another is software firewalls and the other is a combination of both hardware and software.

41. An ethical hacker must need to have the skills of understanding the problem, networking knowledge and to know how the technology works.
a) True
b) False
Answer: a
Explanation: An ethical hacker must need to have the skills of understanding the problem, networking knowledge and to know how the technology works. Password guessing and securing, network traffic sniffing, exploring for vulnerabilities are some other skills.

42. _____enables a hacker to open a piece of program or application and re-build it with further features & capabilities.
a) Social engineering
b) Reverse engineering
c) Planting malware
d) Injecting code
Answer: b
Explanation: Reverse engineering is the technique used to enable a hacker to open a piece of program or application (usually in a low-level language such as Assembly language) and re-build it with further features & capabilities.

43. Which of the following do not comes under the intangible skills of hackers?
a) Creative thinking
b) Problem-solving capability
c) Persistence
d) Smart attacking potential
Answer: d
Explanation: Every hacker must possess some intangible skill-set such as creative thinking to process out a new way of penetrating a system, problem-solving skills as to cease down any active attack and persistence, try in different ways without losing hope.

44. Why programming language is important for ethical hackers and security professionals?
a) Only to write malware
b) For solving problems and building tool and programs
c) To teach programming
d) To develop programs to harm others
Answer: b
Explanation: A programming language is important for hackers and security professionals to understand so that they can understand the working behaviour of any virus, ransomware, or other malware, or write their own defense code to solve a problem. Nowadays, security tools and malware are developed by security professionals with high skills and knowledge.

45. Understanding of_____is also important for gaining access to a system through networks.
a) OS
b) email-servers
c) networking
d) hardware
Answer: c
Explanation: A proper understanding of networking is very important for hackers who are trying to gain access to a system through networks. How TCP/IP works, how topologies are formed and what protocols are used for what purposes are some mandatory stuff a hacker or security professional must understand.

46. For hacking a database or accessing and manipulating data which of the following language the hacker must know?
a) SQL
b) HTML
c) Tcl
d) F#
Answer: a
Explanation: For hacking a database or accessing and manipulating data, a hacker must need to have the knowledge of SQL (Structured Query Language). From a hacker's perspective, if you've accessed any database for short period of time and want to change some specific data, you must need to write a proper SQL query to search for or implement your hack faster.

47. Information Gathering about the system or the person or about organization or network is not important.
a) True
b) False
Answer: b
Explanation: Information Gathering about the system or the person or about organization or network is not important so that as a hacker one can get to know well about the target system or victim.

48. _____is an ethical hacking technique used for determining what operating system (OS) is running on a remote computer.
a) Footprinting
b) Cyber-printing
c) OS fingerprinting
d) OS penetration testing
Answer: c
Explanation: OS fingerprinting is an ethical hacking technique used for determining what operating system (OS) is running on a remote computer.

49. How many types of fingerprinting are there in ethical hacking?
a) 5
b) 4
c) 3
d) 2
Answer: d
Explanation: There are two types of fingerprinting in ethical hacking. These are active fingerprinting and passive fingerprinting. Active fingerprinting is gained if you send especially skilled packets to a target machine whereas passive fingerprinting is dependent on sniffer traces from the remote computer.

50. _____is a common tool used for doing OS fingerprinting.
a) Hping
b) Wireshark
c) Nmap
d) Nessus
Answer: c
Explanation: Nmap is a common tool that is used for performing OS fingerprinting. Before targeting any system for the attack, it is necessary to know what OS the website is hosting, which can be found out using some simple command of this tool.

51. To secure your system from such type of attack, you have to hide your system behind any VPN or proxy server.
a) True
b) False
Answer: a
Explanation: It is recommended to hide your system from such fingerprinting attack, performed by hackers, with a secure proxy server by using VPN tools. This technique will completely preserve your identity and hence your system.
52. A_____is a network scanning practice through which hackers can use to conclude to a point which IP address from a list of IP addresses is mapping to live hosts.
a) ping-based hacking
b) ping sweep
c) ping-range
d) pinging
Answer: b
Explanation: A ping sweep is a network scanning practice through which hackers can use to conclude to a point which IP address from a list of IP addresses is mapping to live hosts.

53. Ping sweep is also known as _____
a) ICMP sweep
b) SNMP sweep
c) SGNP sweep
d) SICMP sweep
Answer: a
Explanation: A ping sweep which is also known as ICMP sweep is a network scanning practice through which hackers can use to conclude to a point which IP address from a list of IP addresses is mapping to live hosts.

54. The_____command is used on Linux for getting the DNS and host-related information.
a) dnslookup
b) lookup
c) nslookup
d) infolookup
Answer: c
Explanation: The 'nslookup' command is used on Linux for getting the DNS and host-related information. DNS enumeration is the method used to locate all the DNS-servers and their associated records.

55. The configuration of DNS needs to be done in a secure way.
a) True
b) False
Answer: a
Explanation: Configuration of DNS needs to be done in a secure way, otherwise it is possible that cyber-criminals and hackers may take away lots of sensitive information from the organization.

56. _____are piece of programs or scripts that allow hackers to take control over any system.
a) Exploits
b) Antivirus
c) Firewall by-passers
d) Worms
Answer: a
Explanation: Exploits are the piece of programs or scripts that allow hackers to take control over any system. Vulnerability scanners such as Nexpose and Nessus are used for finding such vulnerabilities.

57. The process of finding vulnerabilities and exploiting them using exploitable scripts or programs are known as _____
a) infiltrating
b) exploitation
c) cracking
d) hacking
Answer: b
Explanation: The process of finding vulnerabilities and exploiting them using exploitable scripts or programs are known as exploitation. Vulnerability scanners such as Nexpose and Nessus are used for finding such vulnerabilities and then they are exploited using such programs and scripts.

58. Which of them is not a powerful vulnerability detecting tool?
a) Nessus
b) Nexpose
c) Metasploit
d) Nmap
Answer: d
Explanation: Some of the most widely used tools for detecting vulnerabilities in a system are Nessus, Nexpose, Metasploit and OpenVAS. Hackers use these tools for detecting vulnerabilities and then write exploits to exploit the systems.

59. _____is the specific search engine for exploits where anyone can find all the exploits associated to vulnerability.
a) Google
b) Bing
c) Exploit-db
d) Exploit-engine
Answer: c
Explanation: Since based on vulnerabilities, we can find exploits, Exploit-db is the specific search engine for exploits where anyone can find all the exploits associated with vulnerability. You can find this from https://www.exploit-db.com.

60. Which of the following is not a type of cyber crime?
a) Data theft
b) Forgery
c) Damage to data and systems
d) Installing antivirus for protection
Answer: d
Explanation: Cyber crimes are one of the most threatening terms that is an evolving phase. It is said that major percentage of the World War III will be based on cyber-attacks by cyber armies of different countries.

61. Cyber-laws are incorporated for punishing all criminals only.
a) True
b) False
Answer: b
Explanation: Cyber-laws were incorporated in our law book not only to punish cyber criminals but to reduce cyber crimes and tie the hands of citizens from doing illicit digital acts that harm or damage other's digital property or identity.

62. Cyber-crime can be categorized into_____types.
a) 4
b) 3
c) 2
d) 6
Answer: c
Explanation: Cyber crime can be categorized into 2 types. These are peer-to-peer attack and computer as weapon. In peer-to-peer attack, attackers target the victim users; and in computer as weapon attack technique, computers are used by attackers for a mass attack such as illegal and banned photo leak, IPR violation, pornography, cyber terrorism etc.

63. Which of the following is not a type of peer-to-peer cyber-crime?
a) Phishing
b) Injecting Trojans to a target victim
c) MiTM
d) Credit card details leak in deep web
Answer: d
Explanation: Phishing, injecting Trojans and worms to individuals comes under peer-to-peer cyber crime. Whereas, leakage of credit card data of a large number of people in deep web comes under computer as weapon cyber-crime.
64. Which of the following is not an example of a computer as weapon cyber-crime?
a) Credit card fraudulent
b) Spying someone using keylogger
c) IPR Violation
d) Pornography
Answer: b
Explanation: DDoS (Distributed Denial of Service), IPR violation, pornography are mass attacks done using a computer. Spying someone using keylogger is an example of peer-to-peer attack.

65. Which of the following is not done by cyber criminals?
a) Unauthorized account access
b) Mass attack using Trojans as botnets
c) Email spoofing and spamming
d) Report vulnerability in any system
Answer: d
Explanation: Cyber-criminals are involved in activities like accessing online accounts in unauthorized manner; use Trojans to attack large systems, sending spoofed emails. But cyber-criminals do not report any bug is found in a system, rather they exploit the bug for their profit.

66. What is the name of the IT law that India is having in the Indian legislature?
a) India's Technology (IT) Act, 2000
b) India's Digital Information Technology (DIT) Act, 2000
c) India's Information Technology (IT) Act, 2000
d) The Technology Act, 2008
Answer: c
Explanation: The Indian legislature thought of adding a chapter that is dedicated to cyber law. This finally brought India's Information Technology (IT) Act, 2000 which deals with the different cyber-crimes and their associated laws.

67. In which year India's IT Act came into existence?
a) 2000
b) 2001
c) 2002
d) 2003
Answer: a
Explanation: On 17th Oct 2000, the Indian legislature thought of adding a chapter that is dedicated to cyber law, for which India's Information Technology (IT) Act, 2000 came into existence.

68. What is the full form of ITA-2000?
a) Information Tech Act -2000
b) Indian Technology Act -2000
c) International Technology Act -2000
d) Information Technology Act -2000
Answer: d
Explanation: Information Technology Act -2000 (ITA-2000), came into existence on 17th Oct 2000, that is dedicated to cyber-crime and e-commerce law in India.

69. The Information Technology Act -2000 bill was passed by K. R. Narayanan.
a) True
b) False
Answer: b
Explanation: The bill was passed & signed by Dr. K. R. Narayanan on 9th May, in the year 2000. The bill got finalised by head officials along with the Minister of Information Technology, Pramod Mahajan.

70. Under which section of IT Act, stealing any digital asset or information is written a cyber-crime.
a) 65
b) 65-D
c) 67
d) 70
Answer: a
Explanation: When a cyber-criminal steals any computer documents, assets or any software's source code from any organization, individual, or from any other means then the cyber crime falls under section 65 of IT Act, 2000.

71. What is the punishment in India for stealing computer documents, assets or any software's source code from any organization, individual, or from any other means?
a) 6 months of imprisonment and a fine of Rs. 50,000
b) 1 year of imprisonment and a fine of Rs. 100,000
c) 2 years of imprisonment and a fine of Rs. 250,000
d) 3 years of imprisonment and a fine of Rs. 500,000
Answer: d
Explanation: The punishment in India for stealing computer documents, assets or any software's source code from any organization, individual, or from any other means is 3 years of imprisonment and a fine of Rs. 500,000.

72. What is the updated version of the IT Act, 2000?
a) IT Act, 2007
b) Advanced IT Act, 2007
c) IT Act, 2008
d) Advanced IT Act, 2008
Answer: c
Explanation: In the year 2008, the IT Act, 2000 was updated and came up with a much broader and precise law on different computer-related crimes and cyber offenses.

73. In which year the Indian IT Act, 2000 got updated?
a) 2006
b) 2008
c) 2010
d) 2012
Answer: b
Explanation: In the year 2008, the IT Act, 2000 was updated and came up with a much broader and precise law on different computer-related crimes and cyber offenses.

74. What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds?
a) Cracking or illegally hack into any system
b) Putting antivirus into the victim
c) Stealing data
d) Stealing hardware components
Answer: a
Explanation: Under section 66 of IT Act, 2000 which later came up with a much broader and precise law says that cracking or illegally hacking into any victim's computer is a crime. It covers a wide range of cyber-crimes under this section of the IT Act.

75. What is the ethics behind training how to hack a system?
a) To think like hackers and know how to defend such attacks
b) To hack a system without the permission
c) To hack a network that is vulnerable
d) To corrupt software or service using malware
Answer: a
Explanation: It is important for ethical hackers and security professional to know how the cyber-criminals think and proceed to target any system or network. This is why ethical hackers and penetration testers are trained with proper ethics to simulate such a scenario as how the real cyber-attack takes place.

76. Performing a shoulder surfing in order to check other's password is_____ethical practice.
a) a good
b) not so good
c) very good social engineering practice
d) a bad
Answer: d
Explanation: Overlooking or peeping into someone's system when he/she is entering his/her password is a bad practice and is against the ethics of conduct for every individual. Shoulder surfing is a social engineering attack approach used by some cyber-criminals to know your password and gain access to your system later.

77. _____has now evolved to be one of the most popular automated tools for unethical hacking.
a) Automated apps
b) Database software
c) Malware
d) Worms
Answer: c
Explanation: Malware is one of the biggest culprits that harm companies because they are programmed to do the malicious task automatically and help hackers do illicit activities with sophistication.

78. Leaking your company data to the outside network without prior permission of senior authority is a crime.
a) True
b) False
Answer: a
Explanation: Without prior permission of the senior authority or any senior member, if you're leaking or taking our your company's data outside (and which is confidential), then it's against the code of corporate ethics.

79. _____is the technique used in business organizations and firms to protect IT assets.
a) Ethical hacking
b) Unethical hacking
c) Fixing bugs
d) Internal data-breach
Answer: a
Explanation: Ethical hacking is that used by business organizations and firms for exploiting vulnerabilities to secure the firm. Ethical hackers help in increasing the capabilities of any organization or firm in protecting their IT and information assets.

80. The legal risks of ethical hacking include lawsuits due to_____of personal data.
a) stealing
b) disclosure
c) deleting
d) hacking
Answer: b
Explanation: The legal risks of ethical hacking contains lawsuits due to disclosure of personal data during the penetration testing phase. Such disclosure of confidential data may lead to a legal fight between the ethical hacker and the organization.

81. Before performing any penetration test, through legal procedure, which key points listed below is not mandatory?
a) Know the nature of the organization
b) Characteristics of work done in the firm
c) System and network
d) Type of broadband company used by the firm
Answer: d
Explanation: Before performing any penetration test, through the legal procedure the key points that the penetration tester must keep in mind are –
i) Know the nature of the organization ii) what type of work the organization do and
iii) the system and networks used in various departments and their confidential data that are sent and received over the network.

82. An ethical hacker must ensure that proprietary information of the firm does not get leaked.
a) True
b) False
Answer: a
Explanation: Yes, it is very important for an ethical hacker to make sure that while doing penetration tests, the confidential data and proprietary information are preserved properly and not get leaked to the external network.

83. After performing_____the ethical hacker should never disclose client information to other parties.
a) hacking
b) cracking
c) penetration testing
d) exploiting
Answer: c
Explanation: It is against the laws and ethics of ethical hackers that after doing penetration tests, the ethical hacker should never disclose client information to other parties. The protection of client data is in the hands of the ethical hacker who performed the tests.

84. _____is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.
a) Social ethics
b) Ethics in cyber-security
c) Corporate ethics
d) Ethics in black hat hacking
Answer: d
Explanation: Ethics in cyber-security is the branch of cyber security that deals with morality and provides different theories and principles' regarding the view-points about what is right and what need not to be done.

Prepared By Mr. Vijay B. Mohite	**Verified By** Module Coordinator	**Re-Verified By** Dept. Academic Coordinator	**Approved By** Prof. S.B. Tamboli HoD (Comp. Engg.)