MCQ's Question and Answers (the answers are highlighted in bold)

Q1. When the Federal Bureau of investigation was create ?.

A)1900 B)1980 C)19450 **D)1984**

Q2. What is The Full form of CART

A)Computer Analysis and Response Team B) Cathode Analog Ray Tube

C)Computer Accessories Repairing team D)None

Q3 When IOCE is Formed

A)1992 B)1980 C)19490 **D)1995**

Q4Full Form Of IOCE

A)International Organization on Computer Evidence B)Internet of Computer Education

C) Internet of Computer Evidence D)None

Q5When was the first FBI Regional Computer Forensic laboratory was Recognize ?.

A)1992 B)1980 C)19490 **D)2000**

Q6How Many Rules in Digital forensic

A)12 B)19 C)10 **D)6**

Q7 What is the Long form of DFI

A)Digital Forensic Investigation B)Digital Fraud Industry

C)Defining Form In D)None

Q8 How Many Phases in **RDMDFR**

A)12 B)19 C)10 **D)6**

Q9 Investigator should satisfy the following point:

A)Contribute to the society and human being B)Avoid harm to others

C)honest and trustworthy **D)All Of the Above**

Q10 Who proposed Road Map Model

A)G. Gunsh B)S. Ciardhuain C)J. Korn **D)G. Palmar**

Q11 Digital Evidence in the form of the:

A)Office File B)E-mail Messages C)Either A or B **D)Both A and B**

Q12 In Computer intrusions the attacker will be leave multiple traces of there presence in:

A)File System B)Registry C)System Logs **D)All of the Above**

Q13 What are the Form of Electronic Evidence:

A)Hard Drive B)E-mail C)Either A or B **D)Both A and B**

Q14 How Many Types of the Evidence

A)12 B)19 C)10 **D)6**

Q15 What is the full form of **BPO**

A)Business Process Outsourcing

Q16 The Digital evidence are used to established a credible link between……….

A)Attacker and victim and the crime scene B)Attacker And information

C)Either A or B D)Both A and B

Q17 The evidence and proof that can be obtained from the electronic source is called the…….

A)Digital Evidence B)Explainable evidence C)Either A or B D)Both A and B

Q18 Which of the following is not type of volatile evidence:

A)Routing Tables B) Main Memory C)Log Files **D) Cached Data**

Q19 Digital Evidence must follow the requirement of the

A)Ideal Evidence Rule B)Best Evidence Rule C)Exchange Rule **D)All of the mentioned**

Q20 White hat Hacker is known as the

A)Cracker **B)Ethical** C)Grey Hat D)Script Kiddies

Q21 What is an grey hat hacker

A)Black Hat Hacker B)White Hat Hacker **C)Combination of White and black hat hackers** D)None

Q22 A Hacker who identifies and exploits weakness in telephones instead of computers is known as:

A)Phreaker B)Hacktivist C)Ethical hacker D)Grey Hat hacker

Q23 Long Form of the VPN

A)Virtual Private Network B)Virtual Personal Network C)Both D)None

Q24 Who are use their skill to identify security problem with computer network

A)Black Hat Hacker **B)Ethical Hacker** C)Grey Hat hacker D)Script Kiddies

Q25 To crack the password you need cracking tool such as:

A)LC4 B)John The Ripper C)pwdump **D)All of the above**

Q26 NMAP known as:

A)Network Mapper B)NetCat C)SuperScan D)NetScan

Q27 What is the most valuable assets of an organization

A)Information

Q28 What is the full form of SMTP

A)Simple mail Transfer Protocol

Q29 What is the full form of DNS

A)Domain Name System B)Simple mail Transfer Protocol

C)Internet Message Access Protocol D) Network Mapper

Q30 What is the full form of IMAP

A)Internet Message Access Protocol B)Simple mail Transfer Protocol

C)Internet Message Access Protocol D)None

Q31 What is the full form of SNMP

A)Simple Network Management Protocol

Q32 Which of the following used for the Network Testing and port scanning

A)NetCat B)SuperScan C)NetScan **D)All of Above**

Q33 The whole email server may be targeted for a complete interruption of services with these failure like

A)Storage overload and bandwidth blocking

Q34 Which is the top most directory in the server file system

A)Root Directory

Q35 Which list is used in the authorization process

A)Access Control List

Q36 What is the latest version of UNIX

A)LINUX

Q37 Which OS is widely used in the world

A)Windows B)LINUX C)IOS D)NONE

Q38 Name of network analyzer which support windows and unix OS

A)Ethereal

Q39 You can grab banner by using

A)Telnet B)NetCat C)Either A or B **D)Both A and B**

Q40 An attacker can create an …………………………….. attack by sending hundreds or thousands of emails with very large attachment

A)Attachment Overloading Attack B)Connection Attack C)Auto Responder Attack

D)All of the Above

1. An Artificial Intelligence system developed by Terry A. Winograd to permit an interactive dialogue about a domain he called blocks-world.

a. SIMD

b. STUDENT

c. **SHRDLU**

d. BACON

2. What is Artificial intelligence?

a. Programming with your own intelligence

b. Putting your intelligence into Computer

c.**Making a Machine intelligent**

d.Playing a Game

3. **Who is the "father" of artificial intelligence?**

a.John McCarthy

b. **Fisher Ada**

c. Allen Newell

d.Alan Turning

4.**Which of the following is a proposed means of testing the intelligence of the machine?**

Turing TestTurning TestTuning Test

a.**Turing Test**

b.Turning Test

c.Tuning Test

d.None

5.Which of the following is not a component of a production system?

a.Control System

b.Associative Memory

c.Primary Memory

d.Secondary Memory

6. Zero sum game has player…

a. seven

b. Two

c.three player

d. **Multiplayer**

7.**Which one is used for compute the logical inference algorithm?**

a. Validity

b.Satisfiability

c. Logical equivalence

d.All of these

8.Single inference rule also called…

a. Resolution

b. Reference

c.Reference

d.None of these

9.Factoring means…

a.Removal of redundant literal

b.Removal of redundant variable

c.Addition of redundant variable

d.Addition of redundant literal

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. Cybertrails are advantageous because:
a. They are not connected to the physical world.
b. Nobody can be harmed by crime on the Internet.
c. They are easy to follow.
d. Offenders who are unaware of them leave behind more clues than they otherwise would have.

10. Private networks can be a richer source of evidence than the Internet because:
a. They retain data for longer periods of time.
b. Owners of private networks are more cooperative with law enforcement.
c. Private networks contain a higher concentration of digital evidence.
d. All of the above.

Question 1. Which of the following statements best describes a white-hat hacker?

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

Answer 1. Option A.

Question 2. A security audit performed on the internal network of an organization by the network administration is also known as ___________.

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

Answer 2. Option C..

Question 3. What is the first phase of hacking?

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

Answer 3. Option D.

Question 4. What type of ethical hack tests access to the physical infrastructure?

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

Answer 4. Option D

Question 5. The security, functionality, and ease of use triangle illustrates which concept?

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

Answer 5. Option B.

Question 6. Which type of hacker represents the highest risk to your network?

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

Answer 6. Option A.

Question 7. What are the three phases of a security evaluation plan? (Choose three answers.)

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

Answer 7. Options A, B, C.

Question 8. Hacking for a cause is called __________________.

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

Answer 8. Option B.

Question 9. Which federal law is most commonly used to prosecute hackers?

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

Answer 9. Option B.

Question 10. When a hacker attempts to attack a host via the Internet it is known as what type of attack?

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

Answer 10. Option A.

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

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

3. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are “they” referred to here?

a) Gray Hat Hackers

b) White Hat Hackers

c) Hactivists

d) Black Hat Hackers

Answer: d

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

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

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

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

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

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

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

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

Chapter 4 – Digital Evidences

1. 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

2. An attorney asking a digital investigator to find evidence supporting a particular line of Inquiry is an example of:

   a. Influencing the examiner
   b. Due diligence
   c. Quid pro quo
   d. Voir dire

3. 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

4. A scientific truth attempts to identify roles that are universally true. Legal judgment, on The other hand, has a standard of proof in criminal prosecutions of:

   a. Balance of probabilities
   b. Beyond a reasonable doubt
   c. Acquittal
   d. None of the above

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

   a. Relevance
   b. Authenticity
   c. Best evidence
   d. Nominally prejudicial

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

   a. Uninformed consen
   b. Forcible entry
   c. Obtained without authorization
   d. None of the above

7. In obtaining a warrant, an investigator must convince the judge on all of the following Points except:

a. Evidence of a crime is in existence
b. A crime has been committed
c. The owner or resident of the place to be searched is likely to have committed The crime
d. The evidence is likely to exist at the place to be searched

8. If, while searching a computer for evidence of a specific crime, evidence of a new, Unrelated crime is discovered, the best course of action is:

a. Abandon the original search, and pursue the new line of investigation
b. Continue with the original search but also pursue the new inquiry
c. Stop the search and obtain a warrant that addresses the new inquiry
d. Continue with the original search, ignoring the new information

9. 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

10. 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

Chapter 5 Basics of Ethical hacking

1. 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

2. 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

3. ___________ 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

4. Leaking your company data to the outside network without prior permission of senior authority is a crime.
   a) True
   b) False
   Answer: a

5. _____________ 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

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

7. 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

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

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

10. __________ 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

Chapter 5 Basics of Ethical hacking

1. 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

2. 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

3. ___________ 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

4. Leaking your company data to the outside network without prior permission of senior authority is a crime.
   a) True
   b) False
   Answer: a

5. _____________ 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

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

7. 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

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

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

10. __________ 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

Chapter 6 Types of hackers

Question 1. Which of the following statements best describes a white-hat hacker?

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

Answer. Option A.

Question 2. A security audit performed on the internal network of an organization by the network administration is also known as ___________.

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

Answer. Option C.

Question 3. What is the first phase of hacking?

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

Answer. Option D.

Question 4. What type of ethical hack tests access to the physical infrastructure?

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

Answer. Option D.

Question 5. The security, functionality, and ease of use triangle illustrates which concept?

A. As security increases, functionality and ease of use increase.

B. As security decreases, functionality and ease of use increase.

C. As security decreases, functionality and ease of use decrease.

D. Security does not affect functionality and ease of use.

Answer. Option B.

Question 6. Which type of hacker represents the highest risk to your network?

A. Disgruntled employees

B. Black-hat hackers

C. Grey-hat hackers

D. Script kiddies

Answer. Option A.

Question 7. What are the three phases of a security evaluation plan? (Choose three answers.)

A. Conduct Security Evaluation

B. Preparation

C. Conclusion

D. Final

E. Reconnaissance

F. Design Security

G. Vulnerability Assessment

Answer. Options A, B, C.

Question 8. Hacking for a cause is called __________________.

A. Active hacking

B. Hacktivism

C. Activism

D. Black-hat hacking

Answer. Option B.

Question 9. Which federal law is most commonly used to prosecute hackers?

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

Answer. Option B.

Question 10. When a hacker attempts to attack a host via the Internet it is known as what type of attack?

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

Answer. Option A.

Chapter-3 Basics of Digital Forensics

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.

Ans:D

2. IDIP stands for

A. Integrated Digital Investigation Process.

B. Integrated Data Investigator Process.

C. Integrated Digital Investigator Process.

D. Independent Digital Investigator Process.

Ans: A

3. Who proposed Road Map for Digital Forensic Research (RMDFR)

A. G.Gunsh.

B. S.Ciardhuain

C. J.Korn.

D. G.Palmar

Ans: D

4. Investigator should satisfy following points:

A. Contribute to society and human being.

B. Avoid harm to others.

C. Honest and trustworthy.

D. All of the above

Ans: D

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

Ans: A

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 copyright

B. Danger of macro viruses

C. Derivative works

D. computer-specific crime

Ans: B

7. There are three c's in computer forensics. Which is one of the three?

A. Control

B. Chance

C. Chains

D. Core

Ans: A

8. When Federal Bureau Investigation program was created?

A.1979

B.1984

C.1995

D.1989

Ans: B

9. When the field of PC forensics began?

A.1960's

B.1970's

C.1980's

D.1990's

Ans: C

10. _______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

Ans: D

10 MCQs from Each Chapter of Emerging Trend in Computer Science

Chapter 1 Artificial Intelligence

---

1. What is Artificial intelligence?

(A) Putting your intelligence into Computer

(B) Programming with your own intelligence

(C) Making a Machine intelligent

(D) Playing a Game

Ans: C

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

(A) PROLOG

(B) Java

(C) LISP

(D) Perl

Ans: D

3. What is state space?

(A) The whole problem

(B) Your Definition to a problem

(C) Problem you design

(Ď) Representing your problem with variable and parameter

Ans: D

4. A production rule consists of

(A) A set of Rule (B) A sequence of steps

(C) Both (a) and (b) (D) Arbitrary representation to problem

Ans: C

5. Which search method takes less memory?

(A) Depth-First Search (B) Breadth-First search

(C) Both (A) and (B) (D) Linear Search.

Ans: A

6.A heuristic is a way of trying

(A) To discover something or an idea embedded in a program

(B) To search and measure how far a node in a search tree seems to be from a goal

(C) To compare two nodes in a search tree to see if one is better than the other

(D) Only (a), (b) and (c).

Ans: D

7. A* algorithm is based on

(A) Breadth-First-Search

(B) Depth-First –Search

(C) Best-First-Search

(D) Hill climbing.

Ans: C

8. Which is the best way to go for Game playing problem?

(A) Linear approach

(B) Heuristic approach

(C) Random approach

(D) Optimal approach

Ans: B

9. How do you represent “All dogs have tails”.

(A) ∀x: dog(x)àhastail(x)

(B) ∀x: dog(x)àhastail(y)

(C) ∀x: dog(y)àhastail(x)

(D) ∀x: dog(x)àhasàtail(x)

Ans: A

10. Which is not a property of representation of knowledge?

(A) Representational Verification (B) Representational Adequacy

(C) Inferential Adequacy (D) Inferential Efficiency

Ans: A

Chapter-2 Internet of Things

----

1. Embedded systems are_____

A. General purpose

B. Special purpose

Ans: B

2. Embedded system is______

A. An electronic system

B. A pure mechanical system

C. An electro-mechanical system

D. (A) or (C)

Ans: D

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. None of these

Ans: D

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

Ans: C

5. The first recognized modern embedded system is

A. Apple computer

B. Apollo Guidance Computer (AGC)

C. Calculator

D. Radio navigation system

Ans: B

6. The first mass produced embedded system is

A. Minuteman-I

B. Minuteman-II

C. Autonetics D-17

D. Apollo Guidance Computer (AGC)

Ans: C

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

Ans: D

8. Which of the following is (are) example(s) of embedded system for data communication?

A. Network router

B. Digital camera

C. Music player

D. All of these

Ans: B

9. What are the essential tight constraint/s 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

Ans: D

10. A digital multi meter is an example of an embedded system for

A. Data communication

B. Monitoring

C. Control

D. All of these

Ans: B

Chapter-3 Basics of Digital Forensics

---

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.

Ans:D

2. IDIP stands for

(A) Integrated Digital Investigation Process.

(B) Integrated Data Investigator Process.

(C) Integrated Digital Investigator Process.

(D)Independent Digital Investigator Process.

Ans: A

3. Who proposed Road Map for Digital Forensic Research (RMDFR)

(A) G.Gunsh.

(B) S.Ciardhuain

(C) J.Korn.

(D) G.Palmar

Ans: D

4. Investigator should satisfy following points:

(A) Contribute to society and human being.

(B) Avoid harm to others.

(C) Honest and trustworthy.

(D) All of the above

Ans: D

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

Ans: A

6. More subtle because you are not aware that you are running these macros

(A) The purpose of copyright

(B) Danger of macro viruses

(C) Derivative works

(D) computer-specific crime

Ans: B

7. There are three c's in computer forensics. Which is one of the three?

(A) Control

(B) Chance

(C) Chains

(D) Core

Ans: A

8. When Federal Bureau Investigation program was created?

(A) 1979

(B) 1984

(C) 1995

(D) 1989

Ans: B

9. When the field of PC forensics began?

(A) 1960's

(B) 1970's

(C) 1980's

(D) 1990's

Ans: C

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, 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

Ans: B

Chapter 4- Digital Evidence

----

1. 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

Ans: C

2. 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, and embedded systems

Ans: D

3. 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

Ans: A

4. 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

Ans: C

5. 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

Ans: C

6. 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

Ans: B

7. 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 the above

Ans: D

8. 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

Ans: C

9. Cyber trails are advantageous because:

A. They are not connected to the physical world.

B. Nobody can be harmed by crime on the Internet.

C. They are easy to follow.

D. Offenders who are unaware of them leave behind more clues than they otherwise

would have.

Ans: D

10. Private networks can be a richer source of evidence than the Internet because:

A. They retain data for longer periods of time.

B. Owners of private networks are more cooperative with law enforcement.

C. Private networks contain a higher concentration of digital evidence.

D. All the above.

Ans: C

Chapter 5 Basics of Hacking (CO5)

----

1. Ethical Hacking is also known as _____

A. Black Hat Hacking.

B. White Hat Hacking.

C. Encryption.

D. None of these.

Ans. B

2. Tool(s) used by ethical hacker_____.

A. Scanner

B. Decoder

C. Proxy

D. All of these.

Ans. D

3. Vulnerability scanning in Ethical hacking finds_____.

A. Strengths.

B. Weakness.

C. A &B

D. None of these.

Ans. B

4. Ethical hacking will allow to____ all the massive security breaches.

A. Remove.

B. Measure.

C. Reject.

D. None of these.

Ans. B

5. Sequential step 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

Ans. A

6. ______ is the art of exploiting the human elements to gain access to the authorized user.

A. Social Engineering.

B. IT Engineering.

C. Ethical Hacking.

D. None of the above.

Ans. A

7. Which hacker refers to ethical hacker?

A. Black hat hacker.

B. White hat hacker.

C. Grey hat hacker.

D. None of the above.

Ans. B

8. The term cracker refers to_____

A. Black hat hacker.

B. White hat hacker.

C. Grey hat hacker.

D. None of the above.

Ans. A

9. Who described a dissertation on fundamentals of hacker's attitude?

A. G. Palma.

B. Raymond.

C. Either.

D. Jhon Browman.

Ans. B

10.Computer Hackers have been in existence for more than a____.

A. Decade.

B. Year.

C. Century

D. Era.

Ans. C

Chapter-6 Types of Hacking (CO6)

----

1. SNMP stands for_____

A. Simple Network Messaging Protocol

B. Simple Network Mailing Protocol

C. Simple Network Management Protocol

D. Simple Network Master Protocol

Ans: C

2. Which of the following tool is used for Network Testing and port Scanning______

A. NetCat

B. SuperScan

C. NetScan

D. All of above

Ans: D

3. Banner grabbing is used for

A. White Hat Hacking

B. Black Hat Hacking

C. Grey Hat Hacking

D. Script Kiddies

Ans: A

4. An attacker can create an________attack by sending hundreds or thousands of e-mails a with

very large attachments.

A. Connection Attack

B. Auto responder Attack

C. Attachment Overloading Attack

D. All the above

Ans: B

5. Which of the following tool is used for Windows for network queries from DNS lookups to

trace routes?

A. Sam Spade

B. SuperScan

C. NetScan

D. Netcat

Ans: A

6. Which tool is used for ping sweeps and port scanning?

A. Netcat

B. SamSpade

C. SuperScan

D. All the above

Ans: C

7. Which of the following tool is used for security checks as port scanning and firewall testing?

A. Netcat

B. Nmap

C. Data communication

D. Netscan

Ans: A

8. What is the most important activity in system cracking?

A. Information gathering

B. Cracking password

C. Escalating privileges

D. Covering tracks

Ans: B

9. Which Nmap scan is does not completely open a TCP connection?

A. SYN stealth scan

B. TCP scan

C. XMAS tree scan

D. ACK scan

Ans: A

10.Key loggers are form of

A. Spyware

B. Shoulder surfing

C. Trojan

D. Social engineering

Ans: A

MCQ EMERGING TRENDS

Chapter 1: - artificial inteligence

1) ***is a branch of science which deals with helping machine find solution to complex to problem in a more human like a fashion.***
   (a) Artificial intelligence
   (b) Internet of think
   (c) Embided system
   (d) Cyber security

2) ***Is a message that consist relavat meaning , implication , or input for decision and or action.***
   (a) Data
   (b) Information
   (c) Knowledge
   (d) Intelligence

3) ***The goal is for the software to use what is it is was learned in one area to solve problem in other area.***
   (a) Machine learning
   (b) Deep learning
   (c) Neural network
   (d) All of above

4) ***the consist of computer program that mimic the way the human brain process information.***
   (a) Machine learning
   (b) Deep learning
   (c) Neural learning
   (d) All of this
5) ***A heuristic is a rule of thumb-------***
   (a) Strategy
   (b) Trick
   (c) Simplification
   (d) All of above

6) ***The component of AI concept of------***
   (a) Logic
   (b) Congition

(c) Computation

(d) All of above

7) Is branch of science that deals with programming the system in such that they automatically learn with experience

(a) Machine learning

(b) Deep earning

(c) Neural learning

(d) All of above

8) The first AI programming language was called

(a) Basic

(b) IPL

(c) FORIRAN

(d) LISP

9) The characteristic of the computer system cable of thinking, reasoning and learning is know as

(a) Machine intelligence

(b) Human intelligence

(c) Artificial intelligence

(d) Virtual intelligence

10) There are how many dimensions of AI

(a) Four

(b) Two

(c) Three

(d) One

Chapter 2:- internet of things

1. _________ allows us to control electronic components
a) RETful API
b) RESTful API
c) HTTP
d) MQTT

*2**. MQTT stands for _____________***
a) MQ Telemetry Things
b) MQ Transport Telemetry
c) MQ Transport Things
*d**) MQ Telemetry Transport***

*3. **MQTT is better than HTTP for sending and receiving data.***
*a) **True***
b) False

*4**. MQTT is _________ protocol.***
a) Machine to Machine
b) Internet of Things
*c) **Machine to Machine and Internet of Things***
d) Machine things

5. Which protocol is lightweight?
a) MQTT
b) HTTP
c) CoAP

*6**. PubNub publishes and subscribes _________ in order to send and receive messages.***
a) Network
b) Account
c) Portal
*d**) Keys***

7. By clicking which key the PubNub will display public, subscribe, and secret keys.
a) Pane
*b**) Demo Keyset***
c) Portal
d) Network

8. The messageChannel class declares the _________ class attribute that defines the key string.

a) ***command_key***

b) command-key

c) commandkey

d) Key_command

9. ***_________ method saves the received arguments in three attributes.***

a) __Init

b) Init__

c) __Init__

*d) _init_*

10. _________ and _________ saves the publish and subscribe keys that we have generated with the PubNub Admin portal.

*a****) public_key and subscribe_key***

b) Public-key and subscribe-key

c) publickey and subscribekey

d) Key_public and key_subscribe

Chapter 3:- basic of digital forensic

1) ***The digital network divided radio frequency into time slots***

(a) TQMA

(b) COMA

(c) EDMA

(d) EDGE

2) When cases go to trial forensics examiner can play one of role

(a) 2

(b) 4

(c) 3

(d) 5

3) ***Forensics is the systematic trucking of incoming and outgoing ruffic on your network***

(a) Network

(b) Computer

(c) Criminal

(d) Server

4) Validate your tools and verify your evidence with to ensure its integrity

(a) Hashing algorithms

(b) Steganography

(c) Watermark

(d) Digital certificates

5) Is a written list of objection to certain testimony are exhibits

(a) Defendant

(b) Plaintiff

(c) Empanelling the jury

(d) Motion in limine

6) ***Regarding the trail the term means rejecting potential jurors****.*

(a) Voir dire

(b) Rebuttal

(c) Strikes

(d) Venireman

7) The evidences of proof that can be obtained from the electricity source is called the

(a) Digital evidence

(b) Demonstrative evidence

(c) Explainable evidence

(d) Substantial evidence

8) If a micro-phone is present during your testimony, placeit to eight to inches from you

(a) 3

(b) 5

(c) 4

(d) 6

9) Jurors typically average just over year of education and eight-grade reading level

(a) 11

(b) 9

(c) 10

(d) 12

10) The digital avoidance are use to stablish a credible link between

(a) Attacker and victim and crime scene

(b) Attacker and the crime scene

(c) Victim and crime scene

(d) Attacker and information.

Chapter 4:- digital evidence

1) 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 an a computer

2) Digital evidence , a hard drive is a example

(a) Open computer system

(b) Communication system

(c) Embedded system

(d) None of these

3) The term of digital evidence the internet is an example of

(a) Open computer system

(b) Communication system

(c) Embedded system

(d) None of these

4) Digital avoidance is a only useful in a counter of law

(a) True

(b) False

5) What are the three general categories of computer system that can contain digital evidence

(a) Desktop ,laptop ,server

(b) Personal computer

(c) Hardware, software

(d) Open computer system

6) In term of digital evidence , a smart card of use of example of

(a) Communication system

(b) Open system

(c) Embedded system

(d) None of above

7) ***All of forensic examination should be perform on a original digital evidence***

(a) True

(b) False

8) ***The term of digital evidence, the internet is an example of***

(a) Open computer system

(b) Communication system

(c) Embedded system

(d) None of these

9) ***Private network can be a richear sorce of digital evidence than they internet***

(a) They retain data for longer period of time

(b) Owener of private network more cooprative with law enforcement

(c) Private network contain higher concentration of digital evidence

(d) None of these

10) ***Digital evidence can be duplicate exactly without any change to be original data***

(a) True

(b) False

Chapter 5:- basic of hackings

*1). **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

2) ***. 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***

3). ___________ ***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

4) ***. Leaking your company data to the outside network without prior permission of senior authority is a crime.***
a) True
b) False

5). _____________ 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 .

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

7). ***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***

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

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

*10). __________ **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***

Chapter 6:- type of hacking

1) ***Which of the following statement based describe a white hat hackers***
(a) Security professional
(b) Former black hat
(c) Former grey hat
(d) Malicious hackers

2) ***SNMP stand for***
(a) simple network messeging protocol
(b) simple network mailing protocol
(c) simple network management protocol
(d) simple network master protocol

3) ***what is the first phase of hacking***
(a) attack
(b) maintaining access
(c) gaining access
(d) reconnaissance

4) ***banner grabbing is often use for***
(a) white hat hacking
(b) black hat hacking
(c) gray hat hacking
(d) script kiddies

5) ***an attack can create and attack by sending hundreds or thousand of e-mail with very large attachment***

(a) connection attack
(b) auto responder attack
(c) attachment overloading attack
(d) all of the above

6) ***what type of ethical hack test access to the physical infra structure***

(a) internal network
(b) remote network
(c) external network
(d) physical network

7) ***the security functinallity and ease of use triangle illustrated which concept***

(a) a security increase, functionality and ease of use increase
(b) a security decrease, functionality and ease of use increase
(c) a security increase, functionality and ease of use decrease
(d) security does not affect functionality and ease of use

8) ***which type of hackers represent the highest risk to your network***

(a) black hat hackers
(b) grey hat hackers
(c) disgruntled employees
(d) script kiddies

9) ***hackings for a causes is called***

(a) active hacking
(b) hacktivism
(c) activism
(d) black-hat-hackers

10) ***when a hackers attempt to attack a host via the internet is the know as what type of attack***

(a) remote attack
(b) local access
(c) internal attack
(d) physical access

Unit3. basics of digital forensics

1. 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, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation

    c. A 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

2. 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.

3. Which of the following is NOT focus of digital forensic analysis?

    a. Authenticity
    b. Comparison
    c. Proving
    d. Enhancement

4. Which of the following represents the step of scientific method?

    I- Develop hypothesis based on evidence

    II- Calculate hash value of evidence

    III- Test the hypothesis to look for additional evidence

    IV-make an imaging of the original evidence

    a. I and IV
    b. I and II
    c. II, III and IV
    d. All of above

5. What is the Primary Objectives of Digital Forensic for Business and Industry?

    a. Availability of service
    b. Prosecution
    c. Continuity of operation
    d. Security

6. Which of the following hold the highest value of evidence in the court?

a. Documentary
b. Demonstrative
c. Testimonial
d. Real

6. 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” ba

7. which is following father of computer forensics
a. M. Anderson
b. G. Gunsh
c. S. Ciardhuain
d. G. Palmar

8. Who proposed Road map model?
a. G. Gunsh
b. S. Ciardhuain
c. J. Korn
d. G. Palmar

9. IDIP stands for
a. Integrated Digital Investigation Process
b. Integrated Data Investigation Process
c. Integrated Digital Investigator Process
d. Independent Digital Investigation Process

10. When you give ____ testimony, you present this evidence and explain what it is and how it was obtained.

a. technical/scientific
b. expert
c. lay witness
d. deposition

Unit-4 Digital Evidences

1. 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

2. 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

3. 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

4. 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

5. 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

6. Digital evidence alone can be used to build a solid case.

   a. True
   b. False

7. 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

8. An argument for including computer forensic training computer security specialists is:

   a. It provides an additional credential.
   b. It provides them with the tools to conduct their own investigations.
   c. It teaches them when it is time to call in law enforcement.
   d. None of the above.

9. Digital evidence is only useful in a court of law.

a. True

b. False

10. 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

Unit-5 Basics of Hacking

1. ___________ 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

2. What is the first phase of hacking?

a. Attack

b. Maintaining access

c. Gaining access

d. Reconnaissance

e. Scanning

3. What is the one thing that old hackers were fond of or find interests in?

a) Breaking Other's system

b) Voracious thirst for knowledge

c) Cracking Phone calls

d) Learning new languages

4. A penetration tester must identify and keep in mind the ____________ & ____________ requirements of a firm while evaluating the security postures.

a) privacy and security

b) rules and regulations

c) hacking techniques

d) ethics to talk to seniors

5. What is the name of the first hacker's conference?

a) DEFCON

b) OSCON

c) DEVCON

d) SECCON

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

7. In which year the term hacking was coined?
a) 1965-67
b) 1955-60
c) 1970-80
d) 1980-82

8. From where the term 'hacker' first came to existence?

a) MIT
b) Stanford University
c) California
d) Bell's Lab

9. In which year, hacking became a practical crime and a matter of concern in the field of technology?

a) 1971
b) 1973
c) 1970
d) 1974

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

a. Local access
b. Remote attack
c. Internal attack
d. Physical access

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

a. DNSlookup
b. nslookup
c. whois
d. ipconfig

Unit-6 Types of Hacking

1. Why would a hacker use a proxy server?

   a. To create a stronger connection with the target.
   b. To create a ghost server on the network.
   c. To obtain a remote access connection.
   d. To hide malicious activity on the network.

2. A security audit performed on the internal network of an organization by the network administration is also known as ___________.
   a. Grey-box testing
   b. Black-box testing
   c. White-box testing
   d. Active testing E. Passive testing

3. Which are the four regional Internet registries?
   a. APNIC, PICNIC, NANIC, RIPE NCC
   b. APNIC, MOSTNIC, ARIN, RIPE NCC
   c. APNIC, PICNIC, NANIC, ARIN
   d. APNIC, LACNIC, ARIN, RIPE NCC

4. Attempting to gain access to a network using an employee's credentials is called the _____________ mode of ethical hacking.
   a. Local networking
   b. Social engineering
   c. Physical entry
   d. Remote networking

5. What tool can be used to perform SNMP enumeration?

   a. DNSlookup
   b. Whois
   c. Nslookup
   d. IP Network Browser

6. What is the purpose of a Denial of Service attack?
   a. Exploit a weakness in the TCP/IP stack
   b. To execute a Trojan on a system
   c. To overload a system so it is no longer operational
   d. To shutdown services by turning them off

7. What port does Telnet use?
   a. 22
   b. 80
   c. 20
   d. 23

8. Performing hacking activities with the intent on gaining visibility for an unfair situation is called ________.

   a. Cracking
   b. Analysis
   c. Hacktivism
   d. Exploitation

9. What protocol is the Active Directory database based on?

   a. LDAP
   b. TCP
   c. SQL
   d. HTTP

10 Which databases is queried by Whois?

   a. ICANN
   b. ARIN
   c. APNIC
   d. DNS

MCQ Chapter 01

1) Which is the first AI program?
   a) The Logical Brain
   b) AlphaSense
   c) The Jarvis
   d) The Logic Theorist

Ans: d) The Logical Theorist

2) Who is regarded as "The Father of AI?"
   a) Allan Turin
   b) John Mc Carthy
   c) J. C. Shaw
   d) Allen Newell

Ans: b) John Mc Carthy

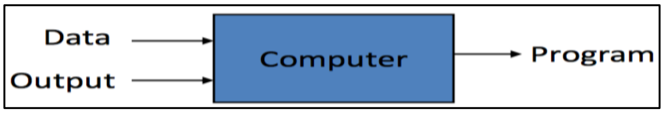
3) Which among this, is an AI created by IBM partner with Fluid PVT. Used specially for 'Data Analysis?'
   a) EVE AI
   b) Watson
   c) Siri
   d) Novel AI

Ans: b) Watson

4) What is PROLOG and LISP?
   a) Examples of super AI
   b) Languages of AI
   c) Concepts of AI
   d) Type of AI

Ans: b) Languages of AI

5) The given illustrative diagram is related to which topic?



a) Machine Learning
b) Neural Network Processing
c) Reasoning
d) Deep learning

Ans: a) Machine Learning

6) There are how many dimensions of AI?
a) Four
b) Three
c) Two
d) One

Ans: b) Three

7) The term “Strong” or “Super” AI comes under which ‘type’ of AI?
a) Type-1
b) Type-2
c) None of the above
d) All of the above

Ans: a) Type-1

8) These machines can use stored data for a limited time period only.
a) Reactive Machine
b) Self-Awareness
c) Limited machine
d) Theory of mind

Ans: c) Limited machine

9) “KBS” in AI stands for?
a) Knowledge Based Scenario
b) Knowledge Based System
c) Knowledge Based Segments
d) Knowing Best System

Ans: b) Knowledge Based System

10) There are how many ‘AI Approaches?’
    a) One
    b) Two
    c) Three
    d) Four

Ans: d) Four

MCQ Chapter 03

1. When was International Organization on Computer Evidence (IOCE) formed?
    a. 1980
    b. 1997
    c. 1995
    d. 1984

Ans: c. 1995

2. CART is referred as…
    a. Computer Art and Response Team
    b. Common Analysis and Response Team
    c. Computer Analysis and Reasoning Team
    d. Computer Analysis and Response Team

Ans: d. Computer Analysis and Response Team

3. How many Rules are there of Digital Forensics?
    a. 5
    b. 6
    c. 7
    d. 4

Ans: b. 6

4. Fill in the blanks.

   Digital Forensics is a series of steps to _________ and _________ electronic data through ________ method.

   a. Solve, analyses, Intelligent
   b. Uncover, analyses, scientific
   c. Uncover, analyses, electronic
   d. Solve, analyses, electronic

Ans: b. Uncover, analyses, scientific

5. There are how many models of digital forensics?
   a. 4
   b. 5
   c. 6
   d. 8

Ans: c. 6

6. Which of the following is not a model of digital forensics?
   a. RMDFR
   b. DFI
   c. IDIP
   d. UMDFPM

Ans: b. DFI

7. Who proposed EEDIP?
   a. Gunsh
   b. Korn
   c. Stepenson
   d. Palmer

Ans: c. Stepenson

8. There are hoe many phases in RMDFR model of digital forensics?
   a. Four
   b. Six
   c. Eight
   d. Ten

Ans: b. Six

9. When was pc forensics began?
    a. 1980
    b. 1984
    c. 1995
    d. 1997

Ans: a. 1980

10. Who is the father of Computer Forensics?
    a. Anderson
    b. Palmer
    c. Ciardhuain
    d. Korn

Ans: a. Anderson

MCQ Chapter 04

1. The digital evidence is used to establish the credible link between …
    a. System, evidence and victim
    b. Attacker, victim, and crime scene
    c. Attacker, victim and case file
    d. Attacker, system and victim

Ans: b. Attacker, victim and crime scene

2. An original copy of the document is considered as…
    a. Best evidence
    b. Original evidence
    c. Superior evidence
    d. True evidence

Ans: c. Superior evidence

3. Best Evidence Rule states that…
    a. It states that multiple copies of electronic files may be a part of the “original” or equivalent to the “original.”
    b. It states that copy of evidence may be considered as original evidence.
    c. It states that the multiple copies of evidence may be part of the “original” or equivalent to the “original.”
    d. It states that multiple copies of electronic files may be a part of the “original” or same as “original.”

Ans: a. It states that multiple copies of electronic files may be a part of the “original” or equivalent to the “original.”

4. According to Locard’s Exchange Principle, contact between two items will result in an _________.
    a. War
    b. Love
    c. Exchange
    d. Failure

Ans: c. Exchange

5. Which of the following is used to portray data more specifically and is helpful in determining the background of digital evidence?
    a. Data
    b. Metadata
    c. Cookies
    d. History

Ans: b. Metadata

6. Testimonial is the major type of Evidence.
    a. True
    b. False
    c. None
    d. N/A

Ans: a. True

7. When collecting evidence, you should always try to proceed from
    a. Least volatile to most volatile evidence
    b. Most volatile to least volatile evidence
    c. All evidence at same priority
    d. Least then medium then most volatile evidence

Ans: b. most volatile to least volatile evidence

8. You must have both ____ and ____ to validate your evidence.
    a. Proof and victim
    b. Power and skill
    c. Power and proof
    d. Proof and skill

Ans: b. power and skill

9. There are how many major types of evidence?
    a. Two
    b. Four
    c. Six
    d. Seven

Ans: c. six

10. Physical evidence is also called as.
    a. Illustrative evidence
    b. Explainable evidence
    c. Substantial evidence
    d. Real evidence

Ans: c. substantial evidence

MCQ Chapter 05

1. Select the most appropriate definition of Ethical hacking.
   a. Ethical hacking is the science of testing computer and network for security vulnerabilities and plugging the hole before the viruses get chance to exploit them.
   b. Ethical hacking is the art of hacking computer and network for security vulnerabilities and plugging the hole before the viruses get chance to exploit them.
   c. Ethical hacking is the science of testing computer and network for security vulnerabilities and plugging the hole before the unauthorized peoples get a chance to exploit them.
   d. Ethical hacking is the art of testing computer and network for security vulnerabilities and plugging the hole before the viruses get chance to handle them.

Ans: c. Ethical hacking is the science of testing computer and network for security vulnerabilities and plugging the hole before the unauthorized peoples get a chance to exploit them.

2. A hacker who gains access to system with a view to fix the identified weaknesses is known as
   a. White hat hackers
   b. Grey hath hackers
   c. Red hat hackers
   d. Hacktivist

Ans: a. white hat hackers

3. Complete the sentence below

   To catch a thief, think like a _______.

   a. Police
   b. Victim
   c. Thief
   d. Hacker

Ans: c. Thief

4. SATAN stands for_
   a. Security Advanced Tool for Analysis Networks
   b. Security Admin Tool for Analysis Networks
   c. Security Administrator Tool for Analysis Networks
   d. Security Administrator Tool for Analysing Network

Ans: c. Security Administrator for Analysis Networks

5. Which type of hackers are invited by the software vendors to find the security flaws in their system?
   a. White hat hackers
   b. Black hat hackers
   c. Grey hat hackers
   d. Blue hat hackers

Ans: d. Blue hat hackers

6. IRC stands for
   a. Internet Rules Chat
   b. Internet Relay Chat
   c. Internet Ready Chat
   d. Internet Readable chat

Ans: b. Internet Relay chat

7. A non-skilled person who gains access to computer system using already made tools are known as?
   a. Grey hat hackers
   b. Hacktivist
   c. Script kiddies
   d. Phreakers

Ans: c. Script kiddies

8. Identifying weakness in computer system or network to exploit its weaknesses to gain access is known as
   a. Cracking
   b. Cybersecurity
   c. Hacking
   d. Threatening

Ans: c. Hacking

9. Exploration of a phone network without authorization is known as
   a. Scripting
   b. Phreaking
   c. Phone hacking
   d. Call tracing

Ans: b. Phreaking

10. Social engineering the ____ of exploiting the human elements to gain access to unauthorized resources.
    a. Art
    b. Science
    c. Hacking
    d. Skill

Ans: a. Art

MCQ Chapter 06

1. Which of the following is not a network testing and port scanning tool?
    a. Nmap
    b. SuperScan
    c. John the ripper
    d. NetCat

Ans: c. John the Rippers

2. Select the most appropriate option for the below two statements.

    I. A Dos attack can take down your internet connection
    II. A Dos attack can take down your entire system

    a. Both I and II are true
    b. I is true II is false
    c. I is false II is True
    d. Both I and II are false

Ans: a. Both I and II are true

3. SNMP stands for
    a. Simple Network Message Protocol
    b. Simple New Message Protocol
    c. Simple Network Management Protocol
    d. Simple Network Managing Protocol

Ans: c. Simple Network Management Protocol

4. Which protocol does hackers use to make their system seems as your system or another allowed host on your network?
   a. SNMP protocol
   b. TCP protocol
   c. ARP protocol
   d. ICMP protocol

Ans: c. ARP protocol

5. Letter bomb is also known as
   a. Official bomb
   b. Hacking bomb
   c. Mail bomb
   d. E-mail bomb

Ans: d. Email Bomb

6. Which attack allows the attacker to execute the scripts on the victim's browser?
   a. SSL attack
   b. Cookie attack
   c. Banner grabbing
   d. XSS attack

Ans: d. XSS attack

7. ACL stands for.
   a. Application Control Language
   b. Application Control list
   c. Access control List
   d. Access Command List

Ans: c. Access Control List

8. As an ethical hacker, you should scan all ________ UDP and TCP port on each network host that's found by your scanner.
   a. 65535
   b. 65353
   c. 65333
   d. 65555

Ans: a. 65535

9. Which of the following are the foundation of all the technical security issues in your information systems?
    a. Network Infrastructure vulnerabilities
    b. Information vulnerabilities
    c. System Infrastructure vulnerabilities
    d. Network Information vulnerabilities

Ans: a. Network infrastructure vulnerabilities

10. Which attack is an HTTP attack which allows attackers to access restricted directories and execute commands outside the web servers root directory?
    a. XSS attack
    b. Path Traversal attack
    c. MITM attack
    d. SQL Injection attack

Ans: b. Path traversal Attack

1What allows digital devices to interconnect and transmit data?

a. a sensor

b.a global positioning sensor

c.a smart phone

d.a network

2. Which command is used to test network connectivity and provide a response to each packet received by the remote host?

a.test

b.tracer

c.ping

d.connect

3. What type of device could allow a refrigerator to place a replacement order for an item contained within it?

a.digital network

b.generator

c.smart phone

d.sensor

4. True or False?

Once connected to the home gateway, smart devices can be controlled from a smartphone, tablet, or PC.

a.true

b.false

5. What information is conveyed by the SSID that is configured on an IoT device?

a.the registration server

b.he default gateway

c.the wireless network

d.the home gateway

6. What is comprised of millions of smart devices and sensors connected to the internet?

a.the fog

b.the internet of things

c.the data center

d.the cloud

7. Which tool allows a user to simulate real networks?

a.artificial intelligence

b.Packet Tracer

c.internet

d.PAN

8. True or False?

The Internet of Things will connect inanimate objects to the network with intelligent sensors.

a.true

b.false

9. Which type of network is used to connect a company located in one area of a city to another location in a city far away?

a.LAN

b.PAN

c.MAN

d.WAN

10. Which type of computing is located at the edge of a business or corporate network and that allows data from sensors to be preprocessed?

a.internet

b.fog

c.wireless

d.WAN

1. Artificial Intelligence system developed by Terry A. Winograd to permit an interactive dialogue about a domain he called blocks-world.

- ➢ SIMD
- ➢ STUDENT
- ➢ SHRDLU
- ➢ BACON

And:- SHRDLU

2. What is Artificial intelligence?

- ➢ Programming with your own intelligence
- ➢ Putting your intelligence into Computer
- ➢ Making a Machine intelligent
- ➢ Playing a Game

And:- Making a Machine intelligent

3. DARPA, the agency that has funded a great deal of American Artificial Intelligence research, is part of the Department of

- Education
- Defense
- Energy
- Justice

And:- Defense.

4. Who is the “father” of artificial intelligence?

- John McCarthy
- Fisher Ada
- Allen Newell
- Alan Turning

And:- Fisher Ada .

5. KEE is a product of

- IntelliCorpn
- Teknowledge
- Texas Instruments
- Tech knowledge

Ans:- IntelliCorpn .

6. Default reasoning is another type of

- Analogical reasoning
- Bitonic reasoning
- Non-monotonic reasoning
- Monotonic reas

Ans:- Non-monotonic reasoning.

7. Weak AI is

- a set of computer programs that produce output that would be considered to reflect intelligence if it were generated by humans.
- the study of mental faculties through the use of mental models implemented on a computer.
- the embodiment of human intellectual capabilities within a computer.
- All of the above

Ans:- Weak AI is the study of mental faculties through the use of mental models implemented on a computer.

8. If a robot can alter its own trajectory in response to external conditions, it is considered to be:

- mobile
- open loop
- intelligent
- non-servo

Ans:- intelligent .

9. One of the leading American robotics centers is the Robotics Institute located at

RAND

MIT

CMU

SRI

And:- CMU

10. What is the name of the computer program that contains the distilled knowledge of an expert?

- Management information System
- Expert system
- Data base management system
- Artificial intelligence

Ans:- expert system.

11. In LISP, the function evaluates both <variable> and <object> is -

- setq
- add
- set
- eva

Ans:- setq

12. What is Artificial intelligence?

- Making a Machine intelligent
- Putting your intelligence into Computer
- Programming with your own intelligence
- putting more memory into Computer

Ans:- Making a Machine intelligent.

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

- PROLOG
- LISP
- Perl
- Java script

And:- Perl

14. Which is not a property of representation of knowledge?

- Inferential Adequacy
- Representational Adequacy
- Representational Verification
- Inferential Efficiency

Ans:- Representational Verification .

15. A Hybrid Bayesian network contains

- Both discrete and continuous variables
- Only Discontinuous variable
- Both Discrete and Discontinuous variable
- Continous variable only.

And:- Both discrete and continuous variables

3. Basics of Digital Forensic

1. When cases go to trial, you as a forensics examiner can play one of ____ roles.

a. 2 c. 4

b. 3 d.5

Ans:- 2

2. When you give ____ testimony, you present this evidence and explain what it is and how it was obtained.

a. technical/scientific. c. lay witness

b. expert d. deposition

And:- technical/scientific.

3. Validate your tools and verify your evidence with ____ to ensure its integrity

a. hashing algorithms c. steganography

b. watermarks d. digital certificates

And:- hashing algorithms

4. For forensics specialists, keeping the ____ updated and complete is crucial to supporting your role as an expert and showing that you're constantly enhancing your skills through training, teaching, and experience.

a. testimony c. examination plan

b. CV d. deposition

Ans:- CV

5. If your CV is more than ____ months old, you probably need to update it to reflect new cases and additional training.

a. 2 c. 4

b. 3 d. 5

Ans:- 3

6. __ is a written list of objections to certain testimony or exhibits.

a. Defendant c. Plaintiff

b. Empanelling the jury d. Motion in limine

Ans:- Motion in limine

7. Regarding a trial, the term ____ means rejecting potential jurors.

a. voir dire c. strikes

b. rebuttal d. venireman

Ans:- strikes

8. ____ from both plaintiff and defense is an optional phase of the trial. Generally, it's allowed to cover an issue raised during cross-examination

a. Rebuttal c. Closing arguments

b. Plaintiff d. Opening statements

Ans:- Rebuttal

9. If a microphone is present during your testimony, place it ____ to eight inches from you.

a. 3 c. 5

b. 4 d. 6

Ans:- 6

10. Jurors typically average just over ____ years of education and an eighth-grade reading level. a. 9 c. 11

b. 10 d. 12

Ans:- 12

4. Digital Evidences

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. Cybertrails are advantageous because:

a. They are not connected to the physical world.

b. Nobody can be harmed by crime on the Internet.

c. They are easy to follow.

d. Offenders who are unaware of them leave behind more clues than they otherwise would have.

10. Private networks can be a richer source of evidence than the Internet because:

a. They retain data for longer periods of time.

b. Owners of private networks are more cooperative with law enforcement.

c. Private networks contain a higher concentration of digital Evidences

d. None of the above.

5. Basic of Hacking

1. What is the attack called “evil twin”?

- ➢ **Rogue access point**
- ➢ ARP poisoning
- ➢ Session hijacking
- ➢ MAC spoofing

2. What are the forms of password cracking techniques?

- ➢ AttackSyllable
- ➢ AttackBrute Forcing
- ➢ AttacksHybrid
- ➢ **All of the above**

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

- Avoiding detection
- Testing security controls
- **Resolving security vulnerabilities**
- Determining return on investment for security measures

4. What is the first phase of hacking?

- Maintaining access
- Gaining access
- Reconnaissance
- Scanning

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

- Black-hat hackers
- Grey-hat hackers
- Script kiddies
- **Disgruntled employees**

6. Hacking for a cause is called ....

- **Hacktivism**
- Black-hat hacking
- Active hacking
- Activism

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

- Local access
- **Remote attack**
- Internal attack
- Physical access

8. Which are the four regional Internet registries?

- APNIC, MOSTNIC, ARIN, RIPE NCC
- APNIC, PICNIC, NANIC, ARIN
- APNIC, PICNIC, NANIC, RIPE NCC
- **APNIC, LACNIC, ARIN, RIPE NCC**

9. What port number does HTTPS use?

- 53
- **443**
- 80
- 21

10. Banner grabbing is an example of what?

- Footprinting
- Active operating system fingerprinting
- **Passive operating system fingerprinting**
- Application analysis

6. Types of Hacking

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

A. Security professional

B. Former black hat

C. Former grey hat

D. Malicious hacker

2. A security audit performed on the internal network of an organization by the network administration is also known as ___________.

A. Grey-box testing

B. Black-box testing

C. White-box testing

D. Active testing

E. Passive testing

3. What is the first phase of hacking?

A. Attack

B. Maintaining access

C. Gaining access

D. Reconnaissance

E. Scanning

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

A. Internal network

B. Remote network

C. External network

D. Physical access

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

A. As security increases, functionality and ease of use increase.

B. As security decreases, functionality and ease of use increase.

C. As security decreases, functionality and ease of use decrease.

D. Security does not affect functionality and ease of use.

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

A. Disgruntled employees

B. Black-hat hackers

C. Grey-hat hackers

D. Script kiddies

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

A. Conduct Security Evaluation

B. Preparation

C. Conclusion

D. Final

E. Reconnaissance

F. Design Security

G. Vulnerability Assessment

Answer :- A, B, C.

8. Hacking for a cause is called ___________________.

A. Active hacking

B. Hacktivism

C. Activism

D. Black-hat hacking

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

A. Title 12

B. Title 18

C. Title 20

D. Title 2

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

A. Remote attack

B. Physical access

C. Local access

D. Internal attack

MCQ'S

CHAPTER 3: Basics of Digital Forensics

1. IOCE is …………………..?
    a. Organization on computer evidence
    b. Organization on communication evidence
    c. Organization on country education
    d. Organization on crime evidence

    Ans : a)Organization on computer evidence

2. Digital forensic applied both ……………. ?
    a. Analysis and response action
    b. Computer crime and civil action
    c. Criminal and civil action
    d. Regional and forensic action

    Ans : c) criminal and civil action

3. How many rules are there in Digital Forensics :
    a. 5
    b. 2
    c. 7
    d. 6

   Ans : d) 6

4. Compliance with the law and …………
    a. Professional norms.
    b. Collection
    c. Prevention
    d. Examination

   Ans : a) Professional norms

5. What is the full form of ADFM
    a. Abstract defining forensic model
    b. Abstract digital forensic model
    c. Abstract digital forensic media
    d. Analysis digital forensic model

   Ans : b) Abstract digital forensic model

6. The whole process is trigged by ………….
    a. Investigator
    b. Society
    c. Digital forensic
    d. Criminal activity

   Ans : d) Criminal activity

7. Digital forensic 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

   Ans: b) Preservation of computer data

8. IDIP stand for
    a. Integrated digital investigation process
    b. Integrated data investigation process
    c. Integrated digital investigator process
    d. None of the above

   Ans : a) Integrated digital investigation process

9. Who proposed Road map model ?
    a. G.Gunsh
    b. S.Ciardhuain
    c. J.Korn
    d. G.Palmar

Ans : d) G.Palmar

10. Field of PC forensics began in which year ?
    a. 1975
    b. 1944
    c. 1971
    d. 1980

Ans : d) 1980

MCQ'S

CHAPTER 4: Digital Evidences

1. Which of the following is not a digital device ?
    a. Computer
    b. Phone
    c. Guitar
    d. Internet

Ans : c) Guitar

2. Rule of evidence is called as …………
    a. Digital Evidence
    b. Law of Evidence
    c. Hidden Evidence
    d. Electronic Evidence

Ans : b) Law Of Evidence

3. BPO stand for ………….
    a. Business profile outsourcing
    b. Business profile outcome
    c. Business process outsourcing
    d. Business process outcome

Ans : c) Businesses process outsourcing

4. The digital evidence are used to establish a credible link between……
   a. Attacker and victim and the crime scene
   b. Attacker and the crime scene
   c. Victim and the crime scene
   d. Attacker and information

Ans : a) Attacker and victim and the crime scene

5. Which of the following is not a type of volatile evidence?

   a. Routing Table
   b. Main memory
   c. Log files
   d. Cached Data

Ans : c) Log files

5. Will volatile evidences last forever
   a. No
   b. Not Sure
   c. Yes
   d. None of the above

Ans : a) No

6. Investigation means :
   a. Collection of information
   b. A procedure to find the Digital Evidence
   c. Searching over internet
   d. Hacking computer systems

Ans : b) A procedure to find the Digital Evidence

7. The evidence or proof that can be obtained from the electronic source is called the ………
   a. Digital evidence
   b. Demonstrative evidence
   c. Explainable evidence
   d. Substantial evidence

Ans : a) Digital evidence

8. Which one is not a 103 rule of evidence
   a. Maintaining a claim of error
   b. Aim of an offer of proof
   c. Plain error taken
   d. Destroying data

Ans : d) Destroying data

9. Digital evidence must follow the requirements of the ……..
   a. Ideal evidence
   b. Best evidence
   c. Exchange evidence
   d. All of the mentioned

   Ans : b) Best evidence

MCQ'S

CHAPTER 5: Basics of Hacking

1. What is hacking ?
   a. Identifying weakness in computer system or networks
   b. Refers to act of locating vulnerabilities
   c. A security to your personal data
   d. Protocols of corrupting data

   Ans : a) Identifying weakness in computer system or networks

2. Ethical Hacking is known as ……….
   a. White Hat hacking
   b. Black Hat hacking
   c. Encrypting
   d. None of these

   Ans : a) white Hat hacking

3. How many steps are there the legality of ethical hacking ?
   a. 5
   b. 2
   c. 7
   d. 6

   Ans : a) 5

4. Tools used by ethical hackers……….
   a. Scanner
   b. Decoder
   c. Proxy
   d. All of these

   Ans : a) scanner

5. Hackers are also called as
    a. Good Guys
    b. Bad Guys
    c. Both of the above
    d. None of the above

   Ans : b) Bad Guys

6. Vulnerability scanning in Ethical hacking finds……….
    a. Strengths
    b. Weakness
    c. A&B
    d. None of these

   Ans : b) weakness

7. What is the required education to be an ethical hacker ?
    a. Diploma holder
    b. 10+2 passed
    c. Bachelor's degree in the related field
    d. Nothing needed

   Ans : c) Bachelor's degree in related field

8. Ethical hacking will allow to ………all the massive security breaches.
    a. Reject
    b. Measure
    c. Remove
    d. None of these

   Ans : d) None of these

9. Security tools that are widely used are :
    a. Nmap
    b. WebInspect
    c. Network Strumbler
    d. All of the above

   Ans : d) All of the above

10. TCP stand for………
    a. Transmission Control Protocol
    b. Transfer Control Protocol
    c. Travel Control Protocol
    d. Tracking Control Protocol

    Ans : a) Transmission Control Protocol

MCQ'S

CHAPTER 6: Types of Hacking

1. SNMP stand for…………
    a. Simple network messaging protocol
    b. Simple network Mailing protocol
    c. Simple network management protocol
    d. Simple network Master protocol

   Ans : c) Simple network management protocol

2. What is the full form of NIV Foundation?
    a. Network Infrastructure Violation
    b. Network Issue Vulnerabilities
    c. Network Infrastructure Vulnerabilities
    d. Network Information Vulnerabilities

   Ans : c) Network Infrastructure Vulnerabilities

3. Banner grabbing is often used for…….
    a. White hat hacking
    b. Black hat hacking
    c. Gray hat hacking
    d. Script kiddies

   Ans : a) white hat hacking

4. What is the full form of UDP
    a. Union Development Program
    b. User Data Program
    c. User Datagram Protocol
    d. Unified Datagram Provider

   Ans : c) User Datagram Protocol

5. IMAP stand for…………
    a. Internet message access protocol
    b. Internet mailing access protocol
    c. Information access protocol
    d. None of these

   Ans : a) Internet message access protocol

6. What is full form of MAC
    a. Model Access Communication
    b. Media Access Control
    c. Multimedia Access Control
    d. Modern Access Control

   Ans : b) Media Access Control

7. Which IEEE standards specify the technologies for wireless LANs 802.11
    a. IEEE 802.11
    b. IEEE 802.10
    c. IEEE 279.6
    d. IEEE 275.4

   Ans : a) 802.11

8. An attackers can create an …....attack by sending hundreds or thousand of e-mail with very large attachment.
    a. Connection Attack
    b. Auto responder Attack
    c. Attachment overloading Attack
    d. All of the above

   Ans : c) Attachment overloading attack

9. Port no.(6346,6347) Gnutella service having which protocols …..
    a. TCP
    b. UDP
    c. TCP, UDP
    d. NONE

   Ans : c) TCP,UDP

10. What is the full form of DMZ
    a. Demilitarized Zone
    b. Demonetized Zone
    c. Demand Zone
    d. Demoralized Zone

    Ans : a) Demilitarized Zone

MCQ'S

CHAPTER 1: Artificial Intelligence

1) Which is the first AI program?
   a) The Logical Brain
   b) AlphaSense
   c) The Jarvis
   d) The Logic Theorist

   Ans: d) The Logical Theorist

2) Who is regarded as "The Father of AI?"
   a) Allan Turin
   b) John Mc Carthy
   c) J. C. Shaw
   d) Allen Newell

   Ans: b) John Mc Carthy

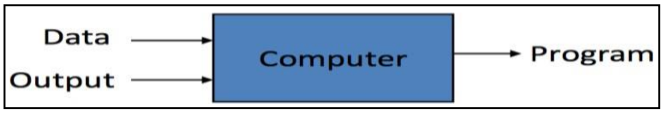
3) Which among this, is an AI created by IBM partner with Fluid PVT. Used specially for 'Data Analysis?'
   a) EVE AI
   b) Watson
   c) Siri
   d) Novel AI Ans: b)

   Watson

4) What is PROLOG and LISP?
   a) Examples of super AI
   b) Languages of AI
   c) Concepts of AI
   d) Type of AI

   Ans: b) Languages of AI

5) The given illustrative diagram is related to which topic?
   a) Machine Learning
   b) Neural Network Processing
   c) Reasoning
   d) Deep learning



   Ans: a) Machine Learning

6) There are how many dimensions of AI?

a) Four

b) Three

c) Two

d) One

Ans: b) Three

7) The term “Strong” or “Super” AI comes under which ‘type’ of AI?

a) Type-1

b) Type-2

c) None of the above

d) All of the above

Ans: a) Type-1

8) These machines can use stored data for a limited time period only.

a) Reactive Machine

b) Self-Awareness

c) Limited machine

d) Theory of mind Ans: c)

Limited machine

9) “KBS” in AI stands for?

a) Knowledge Based Scenario

b) Knowledge Based System

c) Knowledge Based Segments

d) Knowing Best System

Ans: b) Knowledge Based System

10) There are how many ‘AI Approaches?’

a) One

b) Two

c) Three

d) Four

Ans: d) Four

CHAPTER 2: Internet of Things

1) Raspbian is:

a) Assembler

b) Language

c) Compiler

d) OS

Ans:- d. OS

2) Which one out of these is not LPWAN technologies:

a) SigFox

b) WiFi

c) NB-oT

d) LoRa

Ans:- b. WiFi

3) 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 the above

Ans:- c. Neural

networks

4) ________________is a branch of Science which deals with the helping machine find solutions to complex problems in a more human like fashion

a. Artificial Intelligence

b. Internet Od Things

c. Embedded system

d. cyber Security

Ans:- a. Artificial Intelligence

5) What does LTE stands for:-
a) Long Terms Errors

b) Long Term Evolution

c) Lengthy terminal Estimation

d) Long term Estimates

Ans:- b. Long Term Evolution

6) Which transport layer protocols is used by DHCP:-

a. RSVP

b.TCP

c. DCCP

d. UDP

Ans:- d. UDP

7) Which one out of these is not a data link layer technology:-

a) Bluetooth

b) UART

c) WiFi

d) HTTP

Ans:- d. HTTP

8) IoT stands for:-

a) Internet of Technology

b) Intranet of Things

c) Internet of Things

d) Information of Things

Ans:- c. Internet of

Things

9) WSN stands for:-

a) Wide Sensor Network
b) Wireless Sensor Network

c) Wired Sensor Network

d) None of these

Ans:- b. Wireless Sensor Network

10) Which is not the feature of IoT:-

a. Connectivity

b. Self-configuring

c. Endpoint Management

d. Artificial Intelligence

Ans:- b. Self-configuring

CHAPTER 3: Basics of Digital Forensics

11. Which of the following sciences pay vital role in criminal justice systems ?

a. Digital Forensics
b. Forensic Science
c. PC Forensics
d. INTERPOL Forensic

Ans : b) Forensic Science

12. The full form of DFI is :

e. Digital Forensic Investigation
f. Digitalized Forensic Investigation
g. Digital Foreign Investment
h. Direct Forensic Investigation

Ans : a) Digital Forensic Science

13. How many rules are there in Digital Forensics :

a. 5
b. 2
c. 7
d. 6

Ans : d) 6

14. Which of the following is not involved in DFI’s road map :

a. Identification
b. Collection
c. Prevention
d. Examination

Ans : c) Prevention

15. What is the full form of EEDIP

a. End to End Digital Investigation Program
b. End to End Digital Investigation Process
c. End to End Digital Forensic Investigation
d. End to End Digital Forensic Investment

Ans : b) End to End Digital Investigation Process

16. Ethical Issues in Digital Forensic means :
    a. Set of moral principals that regulate the use of computers
    b. Related to ethical hacking
    c. Honesty towards investigation
    d. Compliance with law

Ans : a) Set of moral principals that regulate the use of computers

17. What do primary investigator consider from the original source :
    a. Summarize and hold the data
    b. Whether to analyze more data or to extract more data
    c. Examine the data and store it
    d. Compress the data

Ans : b) Whether to analyze more data or to extract more data

18. Who proposed the UML Modelling of Digital Forensic Process Model
    a. Kohn, Eloff and Oliver
    b. Response Team
    c. Only (a)
    d. None of the above

Ans : a) Kohn, Eloff and Oliver

19. From what should the digital data must be protected ?
    a. Copied
    b. Deleted
    c. Modified
    d. Destroyed

Ans : c) Modified

20. Field of PC forensics began in which year ?
    a. 1975
    b. 1944
    c. 1971
    d. 1980

Ans : d) 1980

MCQ’S

CHAPTER 4: Digital Evidences

10. Which of the following is not a digital device ?
    a. Computer
    b. Phone
    c. Guitar
    d. Internet

Ans : c) Guitar

11. Digital evidences are also called as :
    a. Digital proof
    b. Evidence
    c. Hidden Truth
    d. Electronic Evidence

Ans : d) Electronic Evidence

12. Which of the following is not the form of digital evidence:
    a. Text messages
    b. Emails
    c. Pictures
    d. Paper

Ans : d) Paper

13. According to Edmond Locard, there will be interchange if :
    a. Two items interchange with each other
    b. Two items make contact
    c. No interaction needed
    d. No devices needed

Ans : b) Two items make contact

14. What is digital evidence according to Cohen ?
    a. Baggage of proofs
    b. Collection of evidences
    c. Bag of bits
    d. Backpack of Bytes

Ans : c) Bag of bits

15. Will volatile evidences last forever
    a. No
    b. Not Sure
    c. Yes
    d. None of the above

Ans : a) No

16. Investigation means :
    a. Collection of information
    b. A procedure to find the Digital Evidence
    c. Searching over internet
    d. Hacking computer systems

Ans : b) A procedure to find the Digital Evidence

17. To whom is the IP addresses were traced ?
    a. Internet Service Provider
    b. Cyber Crime Office
    c. Only (a)
    d. None of the above

Ans : a) Internet Service Provider

18. Which one is not a 103 rule of evidence
    a. Maintaining a claim of error
    b. Aim of an offer of proof
    c. Plain error taken
    d. Destroying data

Ans : d) Destroying data

19. Which one of the following locates data on network devices :
    a. ARP Cache
    b. Kernel Statistics
    c. Routing Table
    d. Memory

Ans : c) Routing Table

MCQ'S

CHAPTER 5: Basics of Hacking

11. What is hacking ?
    a. Identifying weakness in computer system or networks
    b. Refers to act of locating vulnerabilities
    c. A security to your personal data
    d. Protocols of corrupting data

    Ans : a) Identifying weakness in computer system or networks

12. Malicious users are also called as :
    a. External attackers
    b. Trusted users
    c. hacker
    d. Internal attackers

    Ans : d) Internal attackers

13. How many steps are there the legality of ethical hacking ?
    a. 5
    b. 2
    c. 7
    d. 6

    Ans : a) 5

14. What is PayPal ?
    a. Pay through Pal
    b. NetBanking
    c. Payment Gateway
    d. Information app

    Ans : c) Payment Gateway

15. Hackers are also called as
    a. Good Guys
    b. Bad Guys
    c. Both of the above
    d. None of the above

    Ans : b) Bad Guys

16. Ethical hackers are
    a. Trained hackers
    b. Related to ethical hacking
    c. Bad guys
    d. Good guys

Ans : a) Trained hackers

17. What is the required education to be an ethical hacker ?
    a. Diploma holder
    b. 10+2 passed
    c. Bachelor's degree in the related field
    d. Nothing needed

Ans : c) Bachelor's degree in related field

18. Which is not an Ethical Hacking related career
    a. Back-End Developer
    b. Software Tester
    c. Software Developer
    d. Computer Networking Specialist

Ans : a) Software Tester

19. Security tools that are widely used are :
    a. Nmap
    b. WebInspect
    c. Network Strumbler
    d. All of the above

Ans : d) All of the above

20. What is the full form of TCP :
    a. Transmission Control Protocol
    b. Transfer Control Protocol
    c. Travel Control Protocol
    d. Tracking Control Protocol

Ans : a) Transmission Control Protocol

MCQ'S

CHAPTER 6: Types of Hacking

11. Network Testing and port scanning tools are :
    a. Sam Spade
    b. SuperScan
    c. NetScan
    d. All of the above

    Ans : d) All of the above

12. What is the full form of NIV Foundation?
    a. Network Infrastructure Violation
    b. Network Issue Vulnerabilities
    c. Network Infrastructure Vulnerabilities
    d. Network Information Vulnerabilities

    Ans : c) Network Infrastructure Vulnerabilities

13. Number of Successful NetBIOS queries :
    a. 5
    b. 13
    c. 12
    d. 17

    Ans : b) 13

14. What is the full form of UDP
    a. Union Development Program
    b. User Data Program
    c. User Datagram Protocol
    d. Unified Datagram Provider

    Ans : c) User Datagram Protocol

15. What is Banner Grabbing ?
    a. Act of capturing the information by banners
    b. Grabbing Information
    c. Information Sharing
    d. Sharing Information

    Ans : a) Act of capturing the information by banners

16. What is full form of MAC
    a. Model Access Communication
    b. Media Access Control
    c. Multimedia Access Control
    d. Modern Access Control

Ans : b) Media Access Control

17. Which IEEE standards specify the technologies for wireless LANs 802.11
    a. IEEE 802.11
    b. IEEE 802.10
    c. IEEE 279.6
    d. IEEE 275.4

Ans : a) 802.11

18. LINUX is an
    a. Application
    b. Software
    c. Toolkit
    d. Operating System

Ans : d) Operating System

19. Which of the following is an Email attack :
    a. Hacking
    b. Decrypting
    c. Bomb
    d. Banner

Ans : d) Banner

20. What is the full form of DMZ
    a. Demilitarized Zone
    b. Demonetized Zone
    c. Demand Zone
    d. Demoralized Zone

Ans : a) Demilitarized Zone

MCQ’s Question and Answers (the answers are highlighted in bold)

Q1. When the Federal Bureau of investigation was create ?.

A)1900 B)1980 C)19450 **D)1984**

Q2. What is The Full form of CART

A)Computer Analysis and Response Team B) Cathode Analog Ray Tube

C)Computer Accessories Repairing team D)None

Q3 When IOCE is Formed

A)1992 B)1980 C)19490 **D)1995**

Q4Full Form Of IOCE

A)International Organization on Computer Evidence B)Internet of Computer Education

C) Internet of Computer Evidence D)None

Q5When was the first FBI Regional Computer Forensic laboratory was Recognize ?.

A)1992 B)1980 C)19490 **D)2000**

Q6How Many Rules in Digital forensic

A)12 B)19 C)10 **D)6**

Q7 What is the Long form of DFI

A)Digital Forensic Investigation B)Digital Fraud Industry

C)Defining Form In D)None

Q8 How Many Phases in **RDMDFR**

A)12 B)19 C)10 **D)6**

Q9 Investigator should satisfy the following point:

A)Contribute to the society and human being B)Avoid harm to others

C)honest and trustworthy **D)All Of the Above**

Q10 Who proposed Road Map Model

A)G. Gunsh B)S. Ciardhuain C)J. Korn **D)G. Palmar**

Q11 Digital Evidence in the form of the:

A)Office File B)E-mail Messages C)Either A or B **D)Both A and B**

Q12 In Computer intrusions the attacker will be leave multiple traces of there presence in:

A)File System B)Registry C)System Logs **D)All of the Above**

Q13 What are the Form of Electronic Evidence:

A)Hard Drive B)E-mail C)Either A or B **D)Both A and B**

Q14 How Many Types of the Evidence

A)12 B)19 C)10 **D)6**

Q15 What is the full form of **BPO**

A)Business Process Outsourcing

Q16 The Digital evidence are used to established a credible link between……….

A)Attacker and victim and the crime scene B)Attacker And information

C)Either A or B D)Both A and B

Q17 The evidence and proof that can be obtained from the electronic source is called the…….

A)Digital Evidence B)Explainable evidence C)Either A or B D)Both A and B

Q18 Which of the following is not type of volatile evidence:

A)Routing Tables B) Main Memory C)Log Files **D) Cached Data**

Q19 Digital Evidence must follow the requirement of the

A)Ideal Evidence Rule B)Best Evidence Rule C)Exchange Rule **D)All of the mentioned**

Q20 White hat Hacker is known as the

A)Cracker **B)Ethical** C)Grey Hat D)Script Kiddies

Q21 What is an grey hat hacker

A)Black Hat Hacker B)White Hat Hacker **C)Combination of White and black hat hackers** D)None

Q22 A Hacker who identifies and exploits weakness in telephones instead of computers is known as:

A)Phreaker B)Hacktivist C)Ethical hacker D)Grey Hat hacker

Q23 Long Form of the VPN

A)Virtual Private Network B)Virtual Personal Network C)Both D)None

Q24 Who are use their skill to identify security problem with computer network

A)Black Hat Hacker **B)Ethical Hacker** C)Grey Hat hacker D)Script Kiddies

Q25 To crack the password you need cracking tool such as:

A)LC4 B)John The Ripper C)pwdump **D)All of the above**

Q26 NMAP known as:

A)Network Mapper B)NetCat C)SuperScan D)NetScan

Q27 What is the most valuable assets of an organization

A)Information

Q28 What is the full form of SMTP

A)Simple mail Transfer Protocol

Q29 What is the full form of DNS

A)Domain Name System B)Simple mail Transfer Protocol

C)Internet Message Access Protocol D) Network Mapper

Q30 What is the full form of IMAP

A)Internet Message Access Protocol B)Simple mail Transfer Protocol

C)Internet Message Access Protocol D)None

Q31 What is the full form of SNMP

A)Simple Network Management Protocol

Q32 Which of the following used for the Network Testing and port scanning

A)NetCat B)SuperScan C)NetScan **D)All of Above**

Q33 The whole email server may be targeted for a complete interruption of services with these failure like

A)Storage overload and bandwidth blocking

Q34 Which is the top most directory in the server file system

A)Root Directory

Q35 Which list is used in the authorization process

A)Access Control List

Q36 What is the latest version of UNIX

A)LINUX

Q37 Which OS is widely used in the world

A)Windows B)LINUX C)IOS D)NONE

Q38 Name of network analyzer which support windows and unix OS

A)Ethereal

Q39 You can grab banner by using

A)Telnet B)NetCat C)Either A or B **D)Both A and B**

Q40 An attacker can create an …………………………….. attack by sending hundreds or thousands of emails with very large attachment

A)Attachment Overloading Attack B)Connection Attack C)Auto Responder Attack

D)All of the Above

1. What is the first phase of hacking?

A. Attack

B. Maintaining access

C. Gaining access

D. Reconnaissance

E. Scanning

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

A. Internal network

B. Remote network

C. External network

D. Physical access

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

A. Disgruntled employees

B. Black-hat hackers

C. Grey-hat hackers

D. Script kiddies

4. Hacking for a cause is called ___________________.

A. Active hacking

B. Hacktivism

C. Activism

D. Black-hat hacking

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

A. Remote attack

B. Physical access

C. Local access

D. Internal attack

6. Which are the four regional Internet registries?

A. APNIC, PICNIC, NANIC, RIPE NCC

B. APNIC, MOSTNIC, ARIN, RIPE NCC

C. APNIC, PICNIC, NANIC, ARIN

D. APNIC, LACNIC, ARIN, RIPE NCC

7.How does traceroute work?

A. It uses an ICMP destination-unreachable message to elicit the name of a router.

B. It sends a specially crafted IP packet to a router to locate the number of hops from the sender to the destination network.

C. It uses a protocol that will be rejected by the gateway to determine the location.

D. It uses the TTL value in an ICMP message to determine the number of hops from the sender to the router.

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

A. Host names and IP addresses

B. Whois information

C. DNS server locations

D. Name server types and operating systems

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

A. Impersonation

B. Third-person authorization

C. Help desk

D. Valid user

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

A. It increases security.

B. It makes security harder to enforce.

C. It removes the employee’s responsibility to make judgments.

D. It decreases security.

Chapter No 3 : Basics Of Digital Forensic

1. 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, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation**

C. A 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

2. Does database forensic include in Digital Forensic application

A. **True**

B. False

3. Which of the following is NOT focus of digital forensic analysis?

A. Authenticity

B. Comparison

C. **Proving**

D. Enhancement

4. Which of the following represents the step of scientific methodI- Develop hypothesis based on evidenceII- Calculate hash value of evidenceIII- Test the hypothesis to look for additional evidence IV-make an imaging of the original evidence

A. All above

B. I and III

C. II and IV

D. II, III and IV

5. What is the Primary Objectives of Digital Forensic for Business and Industry

A. **Availability of service**

B. Continuity of operation

C. Prosecution

D. Security

6. Which of the following hold the highest value of evidence in the court?

A. Documentary

B. Demonstrative

C. Testimonial

D. **Real**

7. 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" ba

8. ____ is a written list of objections to certain testimony or exhibits.

a.Defendant

b.Empanelling the jury

c.Plaintiff

d.Motion in limine

9. Attorneys can now submit documents electronically in many courts; the standard format in federal courts is ____.

a. Microsoft Word (DOC)

b. Portable Document Format (PDF)

c. Encapsulated Postscript (EPS)

d. Postscript (PS)

10. A(n) ____is a document that lets you know what questions to expect when you are testifying.

a.written report

b.affidavit

c.examination plan

d.subpoena

Chapter No 4 : Digital Evidences

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. Cybertrails are advantageous because:

a. They are not connected to the physical world.

b. Nobody can be harmed by crime on the Internet.

c. They are easy to follow.

d. Offenders who are unaware of them leave behind more clues than they otherwise would have.

10. Private networks can be a richer source of evidence than the Internet because:

a. They retain data for longer periods of time.

b. Owners of private networks are more cooperative with law enforcement.

c. Private networks contain a higher concentration of digital evidence.

d. All of the above.

Chapter No 5 : Basics of hacking

1. 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

2. 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

3. ___________ 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

4. Leaking your company data to the outside network without prior permission of senior authority is a crime.
a) True
b) False

5. _____________ 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

6. The legal risks of ethical hacking include lawsuits due to __________ of personal data.

a) stealing

b) disclosure

c) deleting

d) hacking

7. 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

8. An ethical hacker must ensure that proprietary information of the firm does not get leaked.

a) True

b) False

9. After performing ____________ the ethical hacker should never disclose client information to other parties.

a) hacking

b) cracking

c) penetration testing

d) exploiting

10. __________ 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

1.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

2. 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

4**. 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

5. 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

7. 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

8. 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

9. Cybertrails are advantageous because:

a. They are not connected to the physical world.

b. Nobody can be harmed by crime on the Internet.

c. They are easy to follow.

d. Offenders who are unaware of them leave behind more clues than they otherwise would have.

MULTIPLE CHOICE QUESTIONS

Chapter 1- Artificial Intelligence

1. A ____ is a rule of thumb, strategy, trick, simplification, or any other kind of device which drastically limits search for solutions in large problem spaces.

A. Heuristic
B. Critical

C. Value based
D. Analytical

Ans: A

2. ______ do not guarantee optimal/any solutions
A. Heuristic
B. Critical
C. Value based
D. Analytical

Ans: A

3. Cognitive science related with _____
A. Act like human

B. ELIZA

C. Think like human
D. None of above

Ans: C

4. _____ Model should reflect how results were obtained. A. Design model

B. Logic model

C. Computational model
D. None of above

Ans: C

5. Communication between man and machine is related with ______

A. LISP B.
ELIZA

C. All of above D.
None of above

Ans: B

6. ELIZA created by _____
A. John McCarthy

B. Steve Russell

C. Alain Colmerauer

D. Joseph Weizenbaum

Ans: D

7. The concept derived from ________ level are propositional logic, tautology, predicate calculus, model, temporal logic.

A. Cognition level
B. Logic level

C. Functional level
D. All of above

Ans: B

8. PROLOG is an AI programming language which solves problems with a form of symbolic logic known as ______.

A. Propositional logic
B. Tautology

C. Predicate calculus
D. Temporal logic

Ans: C

9. 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 above

Ans: B

10. PROLOG, LISP, NLP are the language of ____

B. Machine Learning
C. Internet of Things
D. Deep Learning

Ans: A

11. ______ is used for AI because it supports the implementation of software that computes with symbols very well.

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

Ans: A

Chapter-2 Internet of Things

1. MQTT stands for _____________

A. MQ Telemetry Things

B. MQ Transport Telemetry

C. MQ Transport Things

D. MQ Telemetry Transport

Ans: D

2. MQTT is better than HTTP for sending and receiving data.
A. True

B. False

Ans: A

3. MQTT is _________ protocol.
A. Machine to Machine

B. Internet of Things

C. Machine to Machine and Internet of
Things D. Machine Things

Ans: C

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

Ans: A

5. 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

Ans: B

6. XMPP is used for streaming which type of elements?

A. XPL

B. XML

C. XHL

D. MPL

Ans: B

7. XMPP creates _________ identity.

A. Device

B. Email

C. Message

D. Data

Ans: A

8. XMPP uses ________ architecture.

A. Decentralized client-server

B. Centralized client-server

C. Message

D. Public/subscriber

Ans: A

9. What does HTTP do?

A. Enables network resources and reduces perception of latency
B. Reduces perception of latency and allows multiple concurrency exchange
C. Allows multiple concurrent exchange and enables network resources

D. Enables network resources and reduces perception of latency and Allows multiple concurrent exchange.

Ans: D

10. HTTP expands?
A. Hyper Text Transfer Protocol

B. Hyper Terminal Transfer Protocol
C. Hyper Text Terminal Protocol
D. Hyper Terminal Text Protocol

Ans: A

Chapter-3 Basics of Digital Forensics

1. Which of 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 above

E. None of above

Ans: D

2. Which of following is not general ethical norm for Investigator? A. To contribute to society and human being.

B. Uphold any relevant Evidence.
C. To be honest and trustworthy.
D. To honor confidentially.

Ans: B

3. Which of 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.

Ans: D

4. 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.

Ans: A

5. Which term refers for modifying a computer in a way which was not originally intended to view Information?

A. Metadata

B. Live analysis
C. Hacking

D. Bit Copy

Ans: C

6. 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.Robotis

C.ComputerForenss
D.Animation

Ans: C

7. What are the important parts of the mobile device which used in Digital forensic?
A. SIM
B. RAM

C. ROM.
D.EMMC chip
Ans: D

Using what, data hiding in encrypted images be carried out in digital forensics?

A. Acquisition.

B.Steganogrhy. C.
Liveanalysis

D. Hashing.

And: B

Which of this is not a computer crime?

C. Sabotage.
D. Identification of data

Ans. D

Which file is used to store the user entered password?

A. .exe
B. .txt
C. .iso
D. .asm

Ans: D

Chapter-4 DIGITAL EVIDENCE

1. A Valid Definition of Digital Evidence is
  a. Data Stored or transmitted using a computer
  b. Information of Probative value
  c. **Digital dada of probative Value**
  d. Any digital evidence on computer

2. In term of Digital evidence, a hard drive is example.of
  a. Open Computer System
  b. Communication System
  c. Embedded Computer System
  d. None of the Above

3. In term of Digital evidence, a mobile telephone is an example.of
  a. Open Computer System
  b. Communication System
  c. **Embedded Computer System**
  d. None of the Above

4. In term of Digital evidence, the internet is an example of
  a. Open computer System
  b. **Communication System**
  c. Embedded Computer System
  d. None of the above

5. Digital Evidence is only useful in court of law
  a. True
  b. **False**

6. Video Surveillance can be form of Digital evidence
  a. **True**
  b. False

7. Computer 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**

8. 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

9. Private networks can be a richer source of evidence than the Internet because:
   a. They retain data for longer periods of time.
   b. Owners of private networks are more cooperative with law enforcement.
   c. Private networks contain a higher concentration of digital evidence.
   d. All of the above

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

Chapter-5 Basics of Hacking

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

   A. Security professional

   B. Former black hat

   C. Former grey hat

   D. Malicious hacker

2. **What is the first phase of hacking?**

   A. Attack

   B. Maintaining access

   C. Gaining access

   D. Reconnaissance

   E. Scanning

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

A. Internal network

B. Remote network

C. External network

D. Physical access

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

A. Disgruntled employees

B. Black-hat hackers

C. Grey-hat hackers

D. Script kiddies

5. **Hacking for a cause is called ___________________**

A. Active hacking

B. Hacktivism

C. Activism

D. Black-hat hacking

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

A. Title 12

B. Title 18

C. Title 20

D. Title 2

8. port number does FTP use?

A. 21

B. 25

C. 23

D. 80

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

a. **Avoiding Detection**
b. Determining return on investment (ROI) for security measure
c. Resolving security vulnerabilities
d. Testing Security Controls

10. Leaking your company data to the outside network without prior permission of senior authority is a crime.

a) True
b) False

Chapter-6 Types Of Hacking

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

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

3. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are "they" referred to here?

a) Gray Hat Hackers
b) White Hat Hackers
c) Hactivists
d) Black Hat Hackers

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

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

6. 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

7. 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

8. _________ 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

9. 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

10. __________ 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