1). Which of the following typically keeps tabs on every onlineactivity the victim engages in, compiles all the data in the background, and sends it to a third party?

a)Adware b) Malware c) Spyware d) All of the above

2). Which of the following statements best describes how theprinciple would be broken if a computer was no longer accessible?

a) Confidentiality b) Access control c) Availability d) All ofthe above

3). The most important step in system hacking is:

a) Cracking passwords b) Covering tracks c) Information gathering d) None ofthe above

4. Computer forensics also known as?

A. digital forensic science B. computer crime

C. computer forensic science D. computer forensics investigations

5). Which of the following is a common type of social engineeringattack?

a).Brute force attack b) Distributed Denial of Service(DDoS) attack

c). Phishing attack d)SQL injection attack

6. Which of these is NOT involved in the CIA Triad?

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

7. Which of the following malware types does not clone orreplicate itself through infection?

a. Viruses b)Worms c)Trojans d) Rootkits

8).Which of the following is not a cybercrime?

a) Denial of Service b) Man in the Middle c) Malware3 d) AES

9).Which of the following is a type of cyber attack?

a) Phishing b) SQL Injections c) Password Attack d) All of the above

10).What is the name of the IT law that India is having in theIndian legislature?

a).India’s Technology (IT) Act, 2000 b).India’s Digital Information Technology (DIT) Act, 2000

c). India’s Information Technology (IT) Act, 2000 d).The Technology Act, 2008

11. What is the punishment in India for stealing computer documents, assets or any software’s source code from anyorganization, individual, or from any other means?

a). 6 months of imprisonment and a fine of Rs. 50,000 b). 1 year of imprisonment and a fine of Rs. 100,000

c).2 years of imprisonment and a fine of Rs. 250,000

d).3 years of imprisonment and a fine of Rs. 500,000

12. What is the updated version of the IT Act, 2000?

a) IT Act, 2007 b) Advanced IT Act, 2007 c) IT Act, 2008 d) Advanced IT Act, 2008

13. Compromising a user's session for exploiting the user's dataand do malicious activities or misuse user's credentials is called ___

a) Session Hijacking b) Session Fixation c) Cookie stuffing d) Session Spying

14. Which of them is not a wireless attack?

a) Eavesdropping b) MAC Spoofing c) Wireless Hijacking d) Phishing

15. These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actionsover a digital medium.

a) Malwareb) Remote Access Trojan c) Keyloggers d) Spyware

16. 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

17. Which of the following malware types does not clone orreplicate itself through infection?

a. Viruses b)Worms c)Trojans d) Rootkits

18. Amendment to IT Act 2000 came into effect on__.

a) 2008 Oct. b) 2009 July 3 c) 2008 June 1 d) 2009 Oct. 27

19. Which are the Sections of IT Act that deal with credit card fraud ?

a) 66, 66 C, 66 D b) 42, 67, 67 A, 67 B c) 43, 66, 66 C, 66 B d) None

20. These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actionsover a digital medium.

a) Malware b) Remote Access Trojans c) Keyloggers d) Spyware

21. the full form of Malware is ________________

22. _____is a code injecting method used for attackingthe database of a system / website.

23.An attempt to harm, damage or cause threat to a system ornetwork is broadly termed as _

24. ______is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish Every appeal to Cyber Appellate Tribunal shall be filed within a period of_.

25.Governments hired some highly skilled hackers for providingcyber security for the country or state. These types of hackersare termed as __

26.They are nefarious hackers, and their main motive is to gain

27.financial profit by doing cyber-crimes. Who are “they”referred to here?

28.Cyber-laws are incorporated for punishing all criminalsonly._____True/False

29.In which year India’s IT Act came into existence__

30.Under which section of IT Act, stealing any digital asset or information is written a cyber-crime.

31. State whether True or False: Data encryption isused to ensure confidentiality.____True /False

32. __________kind of malware does not replicate or clone itself through infection?

33.They are malicious hackers whose primary goal is to commitCybercrimes to make money. Who are "they" in this context? __________

34. Cyber-crimes can be categorized into   types

35. Safeguarding the data from unauthorized modification by unknown users is known as____________

36._____Section deals with cyber terrorism ?

37.The term computer is defined under Section_____of the I.T. Act

38.Tampering with Computer Source Documents is _ offence

39._____is a weakness that can be exploited by attackers.

40.Risk and vulnerabilities are the same things______True/False

1. Explain the different phases involved in planning the cybercrime?
2. Describe the Indian Information Technology Act 2000?
3. Describe the Digital forensics process?
4. Explain the different cyber security safe guards?
5. List the cybercrimes in India during 2007?
6. What is malware? explain different types of malwares?
7. Classify cybercrimes. Describe various cybercrimes against Society?
8. Describe the Cyber forensics and Digital Evidence?
9. Explain about Worms and Trojan Horses?
10. Who are cyber criminals ?explain different categories of cyber Criminals
11. Describe the need for cyber security?
12. Mention the challenges to Indian Law and Cybercrime?
13. Explain E-Mail spoofing with an example?
14. Discuss how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs?
15. Explain the need for computer forensics?

16. Illustrate password sniffing with an example?

17. Explain global perspective on cyber crime?

18. Define Attack and Explain it in detail along with an example?

19. What are main objectives of national cyber security policy 2013?