1) ………………….. is a branch of information technology known as information security?
   a) Computer security
   b) Cyber security
   c) IT security
   d) All of these

2) It takes advantages of basic hardware and software security characteristics
   a) System design
   b) Data access control
   c) System access control
   d) None of the above

3) Verification of a login name and password is known as
   a) Configuration
   b) Accessibility
   c) Authentication
   d) Logging in
   e) Other than those given as options

4) If you are allowing a person on the network based on the credentials to maintain the security of your network, then this act refers to the process of
   a) Authentication   b) Automation
   c) Firewall   d) Encryption
   e) None of these

5) The scrambling of code is known as
   a) Encryption   b) Firewalling
   c) Scrambling   d) deception

6) The main reason to encrypt a file is to
   a) Reduce its size
   b) Secure it for transmission
   c) Prepare it for backup
   d) Include it in the start – up sequence

7) Cracked software are another source of
   a) E – mail attack   b) Virus attack
   c) Trojan horse   d) All of these

8) A malware is a
   a) Program   b) Hardware
   c) Person   d) None of these

9) Software's such as viruses, worms and trojan horses that have a malicious content, is known as
   a) Malicious software (malware)
   b) Adware
   c) Scareware
   d) Spyware
   e) Firewall

10) Viruses, trojan horses and worms are
   a) Able to harm computer system
   b) Unable to detect if present on computer
   c) User – friendly applications
   d) Harmless applications resident on computer
   e) None of these

11) It is a self – replicating program that infects computer and spreads by inserting copies of itself into other executable code or documents
   a) Keylogger   b) Worm
   b) Virus   d) Cracker

12) A computer virus is
   a) Deliberately created
   b) Created accidently
   c) Produced as a result of some program error
   d) All of the above

13) …………… are often delivered to a PC through a mail attachment and are often designed to do harm

a) Portals
b) Spam
c) Viruses
d) Other than those given as options
e) E – mail messages

14) Which of the following refers to dangerous programs that can be 'caught' of opening E – mail attachments and downloading software from the Internet?
a) Utility   b) Virus
c) Honey Pot   d) Spam
e) App

15) A program designed to destroy data on your computer which can travel to 'infect' other computers is called a
a) Disease   b) Torpedo
c) Hurricane   d) Virus
e) Infector

16) If your computer rebooting itself, then it is likely that
a) It has a virus
b) It dies not have enough memory
c) There is no printer
d) There has been a power surge
e) It needs a CD – ROMS

17) Computer virus is
a) A hardware
b) Windows tool
c) A computer programs
d) A system software
e) None of the above

18) Which among the following is related to the internet and mail?
a) Boot – up
b) Magnetic Tapes
c) Application software

d) Virus

19) The first PC virus was developed in
a) 1980   b) 1984
c) 1986   d) 1988

20) Which was the first PC boot sector virus?
a) Creeper   b) Payload
c) Bomb   d) Brain

21) The first computer virus is
a) Creeper   b) PARAM
c) The famous   d) HARLIE

22) The .... of a threat measures its potential impact on a system
a) Vulnerabilities
b) Counter measures
c) Degree of harm
d) Susceptibility
e) None of these

23) Which of the following is the type of software that has self – replicating software that causes damage to files and systems?
a) Viruses   b) Trojan horses
c) Bots   d) Worms

24) Like a virus, it is also a self – replicating program. The difference between a virus and it is that it does not create copies of it self on one system it propagates through computer networks
a) Key logger   b) Worm
c) Cracker   d) None of these

25) A worm
a) Can automatically move in network
b) Can only transferred with human intervention
c) Worms are harmless

d) None of the above

26) Worm is a program that infects computer and spreads by inserting copies of itself into other executable code or documents
a) Self – attached
b) Self – replicating
c) Non – self – replicating
d) Hacking

27) A computer virus normally attaches itself to another computer program known as
a) Host program
b) Target program
c) Backdoor program
d) Bluetooth
e) Trojan horse

28) These are program designed as to seem to being or be doing one thing, but actually being or doing another
a) Trojan horse   b) Key loggers
c) Worms   d) Crackers

29) Viruses that fool a user into downloading and / or executing them by pretending to be useful applications are also sometimes called
a) Trojan horses   b) Key loggers
c) Worms   d) Crackers

30) A .... is a small program embedded inside of a GIF image
a) Web bug   b) Cookie
c) Spyware application   d) Spam

31) Hackers often gain entry to a network be pretending to be a legitimate computer
a) Spoofing   b) Forging
c) IP spoofing   d) All of these

32) Attempt to gain unauthorized access to a user's system or information by pretending to be the user
a) Spoofing   b) Hacker
c) Cracker   d) Phishing
e) None of these

33) Which of the following enables to determine how often a user visited a website?
a) Hacker   b) Spammer
c) Phish   d) Identity theft
e) Cookie

34) A person who uses his or her expertise to gain access to other people computers to get information illegally or do damage is a
Or
A person who uses his expertise for software
a) Spammer   b) Hacker
c) Instant messenger   d) All of these
e) None of these

35) Hackers
a) Have the same motive
b) Is another name of users
c) Many legally break into computer as long as they do not do any damage
d) Break into other people's computer

36) What is a person called who uses a computer to cause harm to people or destroy critical systems?
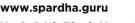a) Cyber Terrorist
b) Black – Hat – Hacker
c) Cyber cracker
d) Hacktivist
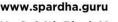e) Other than those given as options

37) .... are attempts by individuals to obtain confidential information from you by falsifying their identity?
   a) Phishing
   b) Computer viruses
   c) Spyware scams
   d) Viruses
   e) Phishing scams

38) Which of the following is a criminal activity attempting to acquire sensitive information such as passwords, credit cards, debits by masquerading as a trustworthy person or business in an electronic communication?
   a) Spoofing
   b) Phishing
   c) Stalking
   d) Hacking
   e) None of these

39) All of the following are examples of real – security and privacy risks except
   a) Hackers
   b) Spam
   c) Viruses
   d) Identify theft
   e) None of these

40) Junk E – mail is also called
   a) Spam
   b) Spoof
   c) Sniffer script
   d) Spool
   e) None of these

41) .... Is a type of electronic spam where unsolicited message is sent by E – mail
   a) Trash mail
   b) Cram mail
   c) Draft mail
   d) Spam mail

42) Adware is something
   a) Which is added to your computers
   b) By adding this performance of your computer increases
   c) Software that gets different advertisement
   d) None of the above

43) It is a toolkit for hiding the fact that a computer's security has been compromised, is a general description of a set of programs which work to subvert control of an operating system from its legitimate (in accordance with established rules) operators
   a) Rootkit
   b) Keylogger
   b) Worm
   d) Cracker

44) An anti – virus is a (n)
   a) Program code
   b) Computer
   c) Company name
   d) Application software

45) Anti – virus software is an example of
   a) Business software
   b) An operating system
   c) A security
   d) An office suite

46) A digital signature is a (n)
   a) Scanned signature
   b) Signature in binary form
   c) Encrypting information
   d) Handwritten signature
   e) None of the above

47) To protect yourself from computer kicker instructions, you should install a
   a) Firewall
   b) Mailer
   c) Macro
   d) Script
   e) None of these

48) Which of the following is a key function of firewall?
   a) Monitoring
   b) Deleting
   c) Copying
   d) Moving
   e) None of these

49) Mechanism to protect network from outside attack is
   a) Firewall
   b) Anti – virus
   c) Digital signature
   d) Formatting

50) A firewall operated by
   a) The pre – purchase phase
   b) Isolating intranet extranet
   c) Screening packets to / from the network and provide controllable filtering of network traffic
   d) All of the above
   e) None of the above

51) Coded entries which are used to gain access to a computer system are called
   a) Entry codes
   b) Passwords
   c) Security commands
   d) Codewords

52) Password enables users to
   a) Get into the system quickly
   b) Make efficient use of time
   c) Retain confidentiality of files
   d) Simplify file structure

53) Which of the following is the combination of numbers, alphabets along with username used to get access to user account?
   a) Password
   b) Username

   c) Title name
   d) Host – ID

54) .... refers to privileges that allow a user to read, write or execute a file
   a) Authentication
   b) File access permission
   c) Password
   d) Firewall

55) The unauthorized real – time interception of a private communication such as a phone call, instant message is known as
   a) Replay
   b) Eavesdropping
   c) Patches
   d) Payloads

56) Vendor created program modifications are called
   a) Patches
   b) Anti – virus
   c) Hales
   d) Fixes
   e) Overlaps

57) Which of the following is a computer's memory, but unlike a virus, it does not replicate itself?
   a) Trojan horse
   b) Logic Bomb
   c) Cracker
   d) Firewall
   e) None of these

58) They are also called slag code and does b=not replicate itself
   a) Time
   b) Anti – virus
   c) Logic Bomb
   d) All of these

59) It hides the true network addresses and used to intercept all messages entering and leaving the network
   a) Logic Bomb
   b) Firewall
   c) Patches
   d) Proxy server

60) The legal right to use software based on specific restrictions is granted via a
   a) Software privacy policy
   b) Software license

c) Software password manager
d) Software log
e) None of the above

61) ……………….. Refers to the unauthorized copying and distribution of software

Or

Illegal copying and distribution of software is
a) Hacking
b) Software piracy
c) Software literacy
d) Cracking
e) Copyright