

SHREE UTTAR GUJARAT BBA COLLEGE

TYBBA (SEM-5)

Subject: Cyber Security

1. What is Cyber Security?
 - a) Cyber Security provides security against malware
 - b) Cyber Security provides security against cyber-terrorists
 - c) Cyber Security protects a system from cyber attacks
 - d) **All of the mentioned**
2. What does cyber security protect?
 - a) **Cyber security protects criminals**
 - b) Cyber security protects internet-connected systems
 - c) Cyber security protects hackers
 - d) None of the mentioned
3. Who is the father of computer security?
 - a) **August Kerckhoffs**
 - b) Bob Thomas
 - c) Robert
 - d) Charles
4. Which of the following act violates cyber security?
 - a) Exploit
 - b) **Attack**
 - c) Threat
 - d) Vulnerability
5. Governments hired some highly skilled hackers for providing cyber security for the country or state. These types of hackers are termed as _____
 - a) **Nation / State sponsored hackers**
 - b) CIA triad
 - c) Special Hackers
 - d) Government Hackers
6. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?
 - a) **Cyber attack**
 - b) Computer security
 - c) Cryptography
 - d) Digital hacking

7. Which of the following is a type of cyber security?
- a) Cloud Security
 - b) Network Security
 - c) Application Security
 - d) All of the above
8. What are the features of cyber security?
- a) Compliance
 - b) Defense against internal threats
 - c) Threat Prevention
 - d) All of the above
9. In which year has hacking become a practical crime and a matter of concern in the field of cyber technology?
- a) 1991
 - b) 1983
 - c) 1970
 - d) 1964
10. Which of the following actions compromise cyber security?
- a) Vulnerability
 - b) Attack
 - c) Threat
 - d) Exploit
11. Which of the following is not a type of peer-to-peer cyber-crime?
- a) MiTM
 - b) Injecting Trojans to a target victim
 - c) Credit card details leak in the deep web
 - d) Phishing
12. Which of the following is a component of cyber security?
- a) Internet Of Things
 - b) AI
 - c) Database
 - d) Attacks
13. Which of the following is a type of cyber attack?
- a) Phishing
 - b) SQL Injections
 - c) Password Attack
 - d) All of the above
14. Which of the following is not an advantage of cyber security?
- a) Makes the system slower
 - b) Minimizes computer freezing and crashes

- c) Gives privacy to users
 - d) Protects system against viruses
15. "Cyberspace" was coined by _____
- a) Richard Stallman
 - b) William Gibson
 - c) Andrew Tannenbaum
 - d) Scott Fahlman
16. Which of the following is not a step followed by cyber-criminals in data breaching?
- a) Exfiltration
 - b) Research and info-gathering
 - c) Attack the system
 - d) Fixing the bugs
17. Which of the following online service's privacy cannot be protected using Tor?
- a) Browsing data
 - b) Instant messaging
 - c) Login using ID
 - d) Relay chats
18. Which of the following term refers to a group of hackers who are both white and black hat?
- a) Yellow Hat hackers
 - b) Grey Hat hackers
 - c) Red Hat Hackers
 - d) White-Black Hat Hackers
19. Which of the following is not an email-related hacking tool?
- a) Mail Password
 - b) Email Finder Pro
 - c) Mail PassView
 - d) Sendinc
20. Which of the following DDoS in mobile systems wait for the owner to trigger the cyber attack?
- a) botnets
 - b) programs
 - c) virus
 - d) worms
21. Which of the following is the least strong security encryption standard?
- a) WPA3
 - b) WPA2

- c) WPA
 - d) **WEP**
22. Which of the following is the hacking approach where cyber-criminals design fake websites or pages for tricking or gaining additional traffic?
- a) **Pharming**
 - b) Website-Duplication
 - c) Mimicking
 - d) Spamming
23. A cyber-criminal or penetration tester uses the additional data that stores certain special instructions in the memory for activities to break the system in which of the following attack?
- a) Clickjacking
 - b) **Buffer-overflow**
 - c) Phishing
 - d) MiTM
24. Which of the following do Cyber attackers commonly target for fetching IP address of a target or victim user?
- a) ip tracker
 - b) emails
 - c) **websites**
 - d) web pages
25. Which of the following is defined as an attempt to harm, damage or cause threat to a system or network?
- a) Digital crime
 - b) Threats
 - c) System hijacking
 - d) **Cyber Attack**
26. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are “they” referred to here?
- a) White Hat Hackers
 - b) **Black Hat Hackers**
 - c) Hactivists
 - d) Gray Hat Hackers
27. IT security in any firm or organization is maintained and handled by
-
- a) Software Security Specialist
 - b) CEO of the organization
 - c) Security Auditor
 - d) **IT Security Engineer**

28. Where did the term “hacker” originate?

- a) MIT
- b) New York University
- c) Harvard University
- d) Bell’s Lab

29. Which of the following is the best source for developing Recovery Time Objectives (RTO)?

- a) Industry averages
- b) Tape restore statistics
- c) Business impact analysis
- d) Previous recovery test results

30. In providing risk reporting to management, the most appropriate vehicle for the initial reporting of a major security incident would be to include it in a:

- a) Quarterly report
- b) Special report
- c) Monthly report
- d) Weekly report

31. To protect the computer system against the hacker and different kind of viruses, one must always keep _____ on in the computer system.

- a) Antivirus
- b) Firewall
- c) Vlc player
- d) Script

32. Which of the following is not a step followed by cyber-criminals in data breaching?

- a) Exfiltration
- b) Research and info-gathering
- c) Attack the system

d) Fixing the bugs

33. What’s the quickest way to stop a suspected app, device, or OS from spying on you?

A. Google user reports of that device’s spying activity and what those people did to stop it.

B. Log out of the suspected device or account and go about your day.

C. Visit Consumer Affairs or the Federal Trade Commission website for tips.

34. Which of the following DDoS in mobile systems wait for the owner to trigger the cyber attack?

a) botnets

b) programs

c) virus

d) worms

35. Which of the following is a Stuxnet?

a) Trojan

b) Antivirus

c) Worm

d) Virus

36. The Altering of data so that it is not usable unless the changes are undone is

A. Biometrics

B. Encryption

C. Ergonomics

D. Compression

37. Which of the following can diminish the chance of data leakage?

a) Steganography

b) Chorography

c) Cryptography

d) Authentication

38. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

- a. Malware
- b. Spyware**
- c. Adware
- d. All of the above

39. _____ is a type of software designed to help the user's computer detect viruses and avoid them.

- a. Malware
- b. Adware
- c. Antivirus**
- d. Both B and C

40. Data theft includes:

- a. unauthorized attempts to bypass the security mechanisms of an information system or network.
- b. use of information and communication technologies to support hostile behaviour
- c. a form of fraud or cheating of another persons' identity
- d. without the permission of the person who is in charge of the computer, to download, copy or extract any data, computer data base or information from computer**

41. Hacking means:

- a. unauthorized attempts to bypass the security mechanisms of an information system or network.**
- b. use of information and communication technologies to support deliberate, repeated and hostile behaviour
- c. a form of fraud or cheating of another persons' identity in which someone pretends to be someone else by assuming that person's identity.
- d. without the permission of the owner to download computer data.

42. Authentication is _____

A. To assure identity of user on a remote system

B. Insertion

C. Modification

D. Integration

43. Identify the type of security that protects information from illegal access or theft thereby preserving the user privacy.

a) Information Security

b) Cyber Security

c) Network Security

d) Application Security

44. Which of the following denotes the deliberate exploitation of computer systems and its resources connected through Internet?

a) Cyber crime

b) Cyber warfare

c) Hacking

d) Cyber attack

45. Figure out the action of pretending to be a licensed venture and sending fake e-mails to users.

a) Phishing

b) Spamming

c) Baiting

d) All the above

46. Give examples for Ransomware.

a) Wannacry

b) CoinMiner

- c) Smoke Leader
- d) Emotet

47. Which of the following is correct?

- a) **Risk=threat x vulnerability**
- b) Threat=risk x vulnerability
- c) Vulnerability=risk +threat
- d) Risk=threat – vulnerability

48. Which of the following is not a cybercrime?

- a) Denial of Service
- b) Man in the Middle
- c) Malware
- d) AES**

49. There are _____ major ways of stealing email information.

- a) 2
- b) 3**
- c) 4
- d) 5

50. Which of them is not a major way of stealing email information?

- a) Stealing cookies
- b) Reverse Engineering**
- c) Password Phishing
- d) Social Engineering

51. _____ is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise.

- a) Email security**
- b) Email hacking
- c) Email protection
- d) Email safeguarding

52. If a website uses a cookie, or a browser contains the cookie, then every time you visit that website, the browser transfers the cookie to that website.

a) True

b) False

53. The stored cookie which contains all your personal data about that website can be stolen away by _____ using _____ or trojans.

a) attackers, malware

b) hackers, antivirus

c) penetration testers, malware

d) penetration testers, virus

54. Which of the following is a non-technical type of intrusion or attack technique?

a) Reverse Engineering

b) Malware Analysis

c) Social Engineering

d) Malware Writing

55. Email users who use IE as their _____ are vulnerable to Reaper Exploit.

a) Web engine

b) Rendering engine

c) Game engine

d) HTML engine

56. _____ needs to be turned off in order to prevent from this attack.

a) Email scripting

b) Email attachments

c) Email services

d) Third party email programs

57. Which of the following will not help in preserving email security?

a) Create a strong password

b) Connect your email to a phone number

c) Use two-factor authentication for password verification and login

d) Click on unknown links and sites

58. _____ is targeted bulk email marketing software.

a) Email Spider Toolkit

b) Email Spider Easy

c) Email Crawler Easy

d) Email Spider Toolkit

59. A _____ tries to formulate a web resource occupied or busy its users by flooding the URL of the victim with unlimited requests than the server can handle.

- a) Phishing attack
- b) DoS attack**
- c) Website attack
- d) MiTM attack

60. During a DoS attack, the regular traffic on the target _____ will be either dawdling down or entirely interrupted.

- a) network
- b) system
- c) website**
- d) router

61. The intent of a _____ is to overkill the targeted server's bandwidth and other resources of the target website.

- a) Phishing attack
- b) DoS attack**
- c) Website attack
- d) MiTM attack

62. A DoS attack coming from a large number of IP addresses, making it hard to manually filter or crash the traffic from such sources is known as a _____

- a) GoS attack
- b) PDoS attack
- c) DoS attack
- d) DDoS attack**

63. DDoS stands for _____

- a) Direct Distribution of Server
- b) Distributed Denial of Service**
- c) Direct Distribution of Service
- d) Distributed Denial of Server

64. Application layer DoS attack is also known as _____

- a) Layer4 DoS attack
- b) Layer5 DoS attack
- c) Layer6 DoS attack
- d) Layer7 DoS attack**

65. Authentication is _____ .

A. To assure identity of user on a remote system

B. Insertion

C. Modification

D. Integration

66. Licence to a Certifying Authority to issue electronic signature certificate will be valid for a period of :

(a) 5 yrs

(b) 10 yrs

(c) 2 yrs

(d) 7 yrs

67. Which of the following is considered as the unsolicited commercial email.

a) Virus

b) Malware

c) Spam

d) All of the above

68. _____ is a type of software designed to help the user's computer detect viruses and avoid them.

a. Malware

b. Adware

c. Antivirus

d. Both B and C

69. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_____:

a. Antivirus

b. Firewall

c. Cookies

d. Malware

70. Which of the following refers to the violation of the principle if a computer is no more accessible?

- a. Access control
- b. Confidentiality
- c. Availability
- d. All of the above