Module 5: True or False questions

1. T/F Authentication is the verification of the identity of (user or machine).
2. T/F Authentication is the verification of the identity of user but not of a machine.
3. T/F Authentication tools are passwords, access cards, and biometrics.
4. T/F Authentication tools are passwords, access cards, but not biometrics.
5. T/F An example of a physical device to authenticate users is the eToken.
6. T/F An example of a physical device to authenticate users is the smart card.
7. T/F An example of a physical device to authenticate users is an eToken but not a smart card.
8. T/F In eTokens data is physically protected on the device itself.
9. T/F Successful client-side authentication with the password invokes the eToken to generate a stored or generated passcode, which is sent to the server-side for authentication.
10. T/F Among the issues with eTokens are that they can be stolen.
11. T/F Among the issues with eTokens are replay attacks.
12. T/F Biometrics used as tool for authentication are two groups: physical and behavioral.
13. T/F There are physical biometrics used for authentication but not behavioral.
14. T/F Behavioral biometrics include signatures, voices, keystrokes, gaits.
15. T/F Behavioral biometrics include signatures, voices, palm print, keystrokes, gaits.
16. T/F Among the legal concerns about biometric attributes are that their storage can be used for illegal/unethical purposes.
17. T/F The two-factor authentication requires providing two out of three components: something you are, something you have, something you know.
18. T/F Three objectives of information security are confidentiality, integrity and availability.
19. T/F Three objectives of information security are conformity, integrity and authentication.
20. T/F Threats to confidentiality could be intercepted data transfers but not physical loss of data.
21. T/F Threats to confidentiality could be an unauthorized access to physical records but not privileged access of confidential information by employees.
22. T/F Encryption solutions to protect confidentiality include PGP, S/MIME, PKI, and OpenVPN.
23. T/F Encryption solutions to protect confidentiality include PGP, S/MIME, RVF, and OpenVPN.
24. T/F Symmetric private/secret/single key cryptography uses one key.
25. T/F Public Key Cryptography includes a public key and a private key.
26. T/F Public Key Cryptography is asymmetric since parties are not equal.
27. T/F Public Key Cryptography is symmetric since parties are equal.
28. T/F Three approaches to attacking RSA Security are brute force key search, mathematical attacks, timing attacks.
29. T/F Three approaches to attacking RSA Security are brute force key search, mathematical attacks, cognitive attacks.
30. T/F Distributed Denial of Service Attack is the use of hundreds of thousands Botnets to overwhelm service and make it unavailable.
31. T/F Known ways of Denial of Service attacks are TCP-SYN flood and Ping of death.
32. T/F IOT is an easy target to exploit and launch DDoS attacks.
33. T/F Mirai DDoS attack in 2016 brought down several ISPs on the U.S. East Coast.
34. T/F Browser attacks are the most common types of attacks.
35. T/F The browser attacks trick Internet users into downloading malware.

36. T/F Zeus is a Trojan horse for stealing banking information/keystroke logging and form grabbing.
37. T/F CryptoJacking is the use of the victim's computer to mine cryptocurrencies using javascript.
38. T/F Port-scanning is when hostile searchers over the Internet look for open ports.
39. T/F DNS cache poisoning is when corrupt DNS cache is corrupted and returned with an incorrect IP address.
40. T/F IP spoofing is creating a false source IP address to hide the identity of the sender.
41. T/F GPS spoofing is to broadcast incorrect GPS signals.
42. T/F A phishing attack is when the attacker disguises as a trustworthy entity to gain the users' password, username, credit card information or banking information.
43. T/F Three phishing techniques are spear phishing, clone phishing, and whaling.
44. T/F CryptoJacking is the use of attacker's own computer to mine cryptocurrencies using javascript.
45. T/F Browsers attacks mean creating a false source IP address to hide the identity of the sender.
46. T/F Four phishing techniques are spear phishing, clone phishing, crypto-phishing and whaling.
47. T/F Buffer overflow is common in program when data exceeds the boundary of the buffer.
48. T/F Intrusion Detection Systems (IDS) are software framework monitors for malicious activities/policy violations.
49. T/F Two detection method groups of Intrusion Detection Systems (IDS) are signature based detection tools and anomaly based.
50. T/F Three detection method groups of Intrusion Detection Systems (IDS) are signature based detection tools, symmetrical detection tools, and anomaly based.
51. T/F Signature based detection tools are looking for (static) signatures of specific patterns.
52. T/F Anomaly based detection tools are detecting unknown attacks – traffics deviating from the normal ones.
53. T/F Signature based detection tools are detecting unknown attacks – traffics deviating from the normal ones.
54. T/F Anomaly based detection tools are looking for (static) signatures of specific patterns.
55. T/F A firewall is a border between two networks and all communications must pass through the bottleneck of the firewall.
56. T/F A firewall is a border between two networks and some suspicious communications must pass through the bottleneck of the firewall.
57. T/F Firewall uses protection methods like Packet Filtering, Network Address Translation (NAT), Proxy Services.
58. T/F Firewall uses protection methods like Packet Filtering, Network Address Translation (NAT), Data Analysis Filter (DAF) and Proxy Services.
59. T/F Network Address Translation (NAT) translates the addresses of internal hosts so as to hide them from the outside world.
60. T/F Network Address Translation (NAT) rejects TCP/IP packets from unauthorized hosts and/or connection attempts by unauthorized hosts