Midterm **CSC686** **Date:**

(50 questions, each question 2 points) score 100

True/False
Indicate whether the statement is true or false.

____ 1. Security attacks are isolated against organizations.

____ 2. WEP relies on a secret key shared between a wireless client device and the access point.

____ 3. Deploying dynamic WEP is a very expensive solution that involves a lot of effort.

____ 4. Promiscuous mode will not work on a WLAN.

____ 5. An incorrect configuration of wireless hardware or software can often result in easy access to a system.

____ 6. DoS attacks are rare against wired network servers.

____7. . Pre-authentication allows for faster roaming between access points.

____ 8. WPA2 uses the Advanced Encryption Standard (AES) for data encryption but does not support IEEE 802.1x authentication or PSK technology.

____ 9. It is recommended that AES encryption and decryption be performed in hardware because of the computationally intensive nature of AES.

____ 10. An advantage to backhaul wireless mesh networks is that they can be quickly deployed in an emergency.

Multiple Choice
Identify the choice that best completes the statement or answers the question.

____ 11. A ____ site provides office space but the customer must provide and install all the equipment needed to continue operations.
a. cold
b. hot
c. warm
d. red

____ 12. ____ is software (or sometimes hardware) that allows to view the contents of wireless packets.
a. Spyware
b. Malware
c. Wireless packet sniffer
d. Adware

____ 13. The IEEE ____ standard specifies a maximum rated speed of 54 Mbps and also supports 48, 36, 24, 18, 12, 9, and 6 Mbps transmissions using the UNII band.
a. 802.11
b. 802.11a
c. 802.11b
d. 802.11z

____ 14. The APs can be positioned so that the cells overlap to facilitate movement between cells, known as ____.
a. SSID broadcast
b. handoff
c. roaming
d. scanning

____ 15. In a ____ attack, an attacker attempts to create every possible key combination by using a program to systematically change one character at a time.
a. social engineering
b. brute force
c. dictionary
d. birthday

____ 16. ____ relies on tricking and deceiving someone to access a system.
a. Social engineering
b. Wardriving
c. Warchalking
d. Wireless site mapping

____ 17. At regular intervals (normally every 100 ms) the wireless access point sends a beacon frame to announce its presence and to provide the necessary information for devices that want to join the network. This process is known as ____.
a. phishing
b. beaconing
c. pharming
d. mapping

____ 28. Wireless networks were identified by drawing on sidewalks or walls around the area of the network known as ____.
a. warchalking
b. phishing
c. pharming
d. dumpster diving

____ 19. The first two versions of SNMP, SNMPv1 and SNMPv2, used ____ that acted like a password to allow or deny access to the information that was collected.
a. community strings
b. management information base (MIB)
c. packet sniffers
d. flash memories

____ 20. ____ is a service that allows devices on a network to discover other devices and determine how to work with them.

a. IPSec
b. SNMP
c. UPnP
d. PnP

Completion

Complete each statement.

21. The term _____ is frequently used to describe the tasks of guarding information that is in a digital format.

22. A wireless device is set to look for beacon frames from the AP. This is known as _____.

23. _____ involves phishers setting up their own search engines to direct traffic to illegitimate sites.

24. The smallest mobile computing device is a(n) _____.

25. The GPS receiver can deduce its own location based on a mathematical principle called _____.

26. _____ are devices that combine access point, router, and network address translation features.

27. The Anti-Spyware Coalition defines _____ as technologies that are implemented in ways that impair a user's control over the use of system resources.

28. AES performs three steps on every block (128 bits) of cleartext. Within the second step, multiple iterations (called _____) are performed depending on the key size.

29. WPA authentication can be accomplished by using either IEEE 802.1x or _____ technology.

30. The 802.11 MAC layer _____ mode is based upon polling and serves as a centralized scheduling mechanism.

Matching

Match each item with an statement below:

a. Security
b. Distributed attacks
c. Firewalls
d. IEEE
e. IEEE 802.11u
f. The FCC
g. Unregulated bands
h. IEEE 802.11n
i. AreTec

____ 31. greatest disadvantage to wireless LANs.

____ 32. standards for how WLANs connect to external networks such as the Internet or cellular networks.

____ 33. the world's largest technical professional society with members around the globe.

____ 34. bands of the radio spectrum that are available nationwide to all users, without requiring a license.

____ 35. organization that promotes standardization in wireless technologies.

Match each item with an statement below:

a. Access control
b. Access restrictions
c. Cipher
d. RC4
e. SSID
f. Keystream attack
g. AirSnort
h. WEP2
i. Shoulder surfing

____ 36. an encryption algorithm.

____ 37. tool to perform WEP attacks.

____ 38. looking over someone's shoulder.

____ 39. adds two new security enhancements to WEP.

____ 40. method of restricting access to resources.

Short Answer

41. What is a MAC address?

42. What are the minimum criteria for creating good passwords?

43. What are the security problems related to adware?

44. Briefly describe the history of AES.

45. What are the main characteristics of the Temporal Key Integrity Protocol (TKIP)?

46. What are the two basic functions of an access point?

47. What are some of the advantages of a wireless router?

48. What are the three basic types of filtering?

49. What are the primary differences between LDAP and DAP?

50. What are the advantages and disadvantages of distributed sites with centralized authentication and security deployment?