Final CSC668 NAME (QUESTIONS CARRY 3 POINTS, ESSAY AND CALC QS CARRY 10 POINTS)

True/False:

___ 1. Educational institutions were some of the first adopters of WLANs because of their dramatic advantages in teaching and learning.

___ 2. Security attacks are isolated against organizations.

___ 3. Promiscuous mode will not work on a WLAN.

___ 4. IEEE 802.11 WLANs have more collisions than wired Ethernet networks.

___ 5. A secure WLAN should use WEP for its encryption, although WPA may be required in older legacy equipment.

Multiple Choice

___ 6. In WEP, the ___ is a 24-bit value that changes each time a packet is encrypted.
   a. initialization vector (IV)
   b. pseudo-random number generator (PRNG)
   c. integrity check value (ICV)
   d. RC4

___ 7. ___ traffic is traffic destined for only one address.
   a. Severalcast
   b. Multicast
   c. Unicast
   d. Broadcast

___ 8. A more proactive approach than intrusion detection is a(n) ___.
   a. RF fingerprinting
   b. trilateration system
   c. RSSI system
   d. intrusion prevention system (IPS)

___ 9. ___ is the process of tracking the assets.
   a. Asset management
   b. Risk identification
   c. Threat management
   d. Vulnerability identification

___ 10. A(n) ___ policy should clearly address how passwords are managed.
   a. password management
   b. VPN
   c. acceptable use
   d. WLAN use

Completion

11. _____ uses the existing data WLAN to make and receive telephone calls.

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

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

14. Certificates are issued by a trusted third party called a(n) _____.

15. An SNMP _____ acknowledges the message with an SNMP response.

Matching

   a. Phishing
   b. Dumpster diving
   c. Handheld PC
   d. Mini PCI
   e. Chipset
   f. Omni-directional antenna
   g. Wireless Zero Configuration (WZC)
   h. IPSec
   i. SNMP management station

___ 16. designed to provide the familiar applications from a desktop computer in a mobile format.

a. Block cipher
b. Pre-authentication
c. WPA
d. WPA2
e. DHCP
f. Personal security model
g. AES-CCMP
h. Enterprise security model
i. RADIUS

___ 17. intended for settings in which an authentication server is unavailable.

a. Password
b. Digital certificates
c. Registration authority (RA)
d. Kerberos
e. PAP
f. MS-CHAP
g. Nonce
h. Group master key (GMK)
i. EAP

___ 18. authentication system developed by the Massachusetts Institute of Technology (MIT).

a. CFS
b. Secure FTP (SFTP)
c. SSH
d. HTTPS
e. PPTP
f. IPsec tunnel mode
g. Endpoint
h. VPN Client
i. Layer 4-7 device

___ 19. UNIX-based command interface and protocol for securely accessing a remote computer.

a. Data
b. Security policy
c. Security policy cycle
d. Attack tree
e. Risk assessment
f. Exposure Factor (EF)
g. Annualized Rate of Occurrence (ARO)
h. Code of ethics
i. Acceptable use policy (AUP)

___ 20. a valuable tool used in threat modeling.

Short Answer

21. What is the difference between active and passive monitoring?

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

23. Could you estimate the amount of time it would take to crack a DES encryption by testing all possibilities? If you have a 1GHZ processor, could you estimate the amount of time it would take to crack a DES encryption by testing all 2^56 possibilities?

24. (a) Alice needs to send a long message to Bob. Assume that all they know about each other is the

other party's public key, denoted as PKA for Alice and PKB for Bob. Draw a diagram (a conceptual framework from your thoughts) to show how Alice should generate the message to be transmitted if they want to provide source authentication, non-repudiation, and confidentiality of message content. (You will lose 2 points for each mechanism you miss or add unnecessarily.) (5 points)

(b) Suppose Alice needs to send many long messages to Bob during a short period of time. Assume that all they know about each other is the other party's public key, denoted as PKA for Alice and PKB for Bob. What should they do to be more efficient than repeating the scenario in (a)? Describe your solution concisely, and then draw diagrams (conceptual framework of your thoughts) to illustrate your protocol(s). (You will lose 2 points for each mechanism you miss or add unnecessarily.) (5 p)