Name:___________________________

CS 600.443 Final Exam

This exam is closed book and closed notes. **You are required to do this completely on your own without any help from anybody else.** Feel free to write on the back of any page to continue an answer, and indicate (over) when doing so.

Part I. Multiple choice: circle one choice (2 points each)

1. Which of the following is typically not considered a firewall
   a. A multi homed router
   b. A packet filter
   c. A hub
   d. An application level gateway
2. Which of the following is a DDOS tool
   a. Trinoo
   b. Apache
   c. SSL
   d. IPsec
3. Which of the following is an example of Transport Layer security
   a. SSL/TLS
   b. WEP
   c. IPsec
   d. SSH
4. Which of the following is an example of Link layer security
   a. IPsec
   b. A cryptographic protocol for 802.11
   c. SSH
   d. RC4
5. Which of the following was not done by the Morris worm
   a. Use a dictionary to crack passwords
   b. Exploit a sendmail bug
   c. Copy itself to remote machines
   d. Email itself with a misleading subject line
6. Which statement about DES is false?
   a. The underlying cipher in DES was broken mathematically
   b. The keys are 56 bits in length, although the block size is 64 bits
   c. The key schedule is run in reverse for decrypting
   d. The full design criteria for the S/Box design is not public
7. Which of the following is true about AES
   a. The keys must be 128 bits long
   b. The NSA approved it because the developers were American
   c. It was designed by NIST
   d. It is a block cipher that can be used in CBC mode
8. Which of the following can be used to authenticate someone you've never communicated with, in the face of an active adversary?
   a. Diffie Hellman
   b. RSA
   c. HMAC
   d. None of the above

9. According to Randy Sabbet
    a. Now that the RSA patent expired, anybody can use it without a license
    b. A patent owner must continuously enforce the patent for it to stay valid
    c. You cannot patent something if a subset of it is patented by someone else
    d. All of the above

10. Which of the following was developed by the Honeynet researchers
    a. firewalls
    b. intrusion detection
    c. Sebek
    d. Application gateways

11. A honeypot is valuable because
    a. It can block previously unknown attacks
    b. No legitimate traffic should go there, so it identifies attackers' techniques
    c. It avoids buffer overflows
    d. It is designed by the attacker

Part II. True/Fale: circle T for True or F for False (2 points each)

T F 1. DRE voting machines are 100% secure
T F 2. The CalTech/MIT report introduced the concept of a frog
T F 3. In the Sensus system, the tallier and the validater must trust each other.
T F 4. Len Adelman, the 'A' in RSA was an early virus researcher.
T F 5. The Happy 99 virus deleted files on target computers.
T F 6. The MyDoom virus hit in the mid 90s and did not involve a denial of service attack.
T F 7. Passport is architecturally similar to Kerberos, but the authenticator is missing.
T F 8. Kerberos is based on Needham and Schroeder but uses timestamps instead of nonces.
T F 9. SSL protects against eavesdroppers on the network.
T F 10. IPsec often uses manual keys, but they can also be derived automatically using IKE
T F 11. VPNs can only be implemented in software.
T F 12. One of the privacy principles covered in class is "Notice and Disclosure".
T F 13. In the privacy lingo, "Access" means that you have access to a web site.
T F 14. Ad networks use cookies and referer headers to track user browsing patterns.

Part III. Short answer. (use the back if necessary) (4 points each)

1. Explain why you would not want to use a stream cipher on a noisy channel.

2. The original Kerberos protocol suffered from a dictionary attack. Describe the vulnerability and how you would exploit it.

3. How would you check to see if there was any spyware on your machine?

4. Describe the main difference in terms of security between 802.11 and Bluetooth.

5. Explain how an RFID blocker tag works.

6. In “distributed firewalls” an administrator ships out firewall rules to hosts over an authenticated channel, and each host enforces its own policy. Give 3 disadvantages of such a system over a centralized firewall.

7. The S-BGP proposal discussed in class uses public key signatures on attestations to validate routes. However, S-BGP has not been adopted, and some say that it is unrealistic. What is the problem? What technical reason is there for the lack of adoption of S-BGP?

8. Why should mixes send fixed sized blocks at fixed intervals?

9. Compare and contrast top down PKI versus the web of trust.

10. OPIE, also known as S/Key, uses hash chains to authenticate users. This means that no secrets need to be stored on the authentication server. Why is that?

11. In the Publius system, take m to be the number of hosts participating. Take k and n to be the number of shares of the key for a document in a k out of n secret splitting scheme. Two independent questions: What would happen if n > m? What are the security implications if k=n?

Part IV. Long answer. (20 points) use front and back of this sheet and the next, if necessary

Imagine that you control a jondo in a Crowd. Say, also that you are running the DNS server that services all the crowd members. Devise an attack that was not discussed in class or in the Crowds paper where you could tell if someone who was sending you requests was the originator of the request. Show the attack algorithm as well as the details, and explain why the attack is effective. Evaluate the seriousness of the attack, and discuss possible countermeasures.