**Homework 04 (totally 124 pts)**

1. (8pts) Consider the Kerberos interaction discussed in this chapter.
   1. Why is the ticket to Bob encrypted with KB?
   2. Why is “Alice” included in the (encrypted) ticket to Bob?
   3. In the REPLY message, why is the ticket to Bob encrypted with the key SA?
   4. Why is the ticket to Bob sent to Alice (who must then forward it to Bob) instead of being sent directly to Bob?
2. (8pts) Consider the Kerberized login discussed in this chapter.
   1. What is a TGT and what is its purpose?
   2. Why is the TGT sent to Alice instead of being stored on the KDC?
   3. Why is the TGT encrypted with KKDC?
   4. Why is the TGT encrypted with KA when it is sent from the KDC to Alice’s computer?
3. (8pts) Describe (enumerate) the insecurity of GSM and then modify the GSM security protocol (Figure 10.25) so that it can provide mutual authentication.
4. (6 pts) Explain how TCP SYN flooding attacks work? (with a figure)

5. (6 pts) Describe how reflection attacks and DNS amplification DoS attacks work （you may read this article to get a deeper understanding of reflection DDoS attacks： https://www.akamai.com/us/en/about/news/press/2015-press/akamai-warns-of-3-new-reflection-ddos-attack-vectors.jsp

6. (8pts) Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection requests. Consider a server system with a table for 256 connection requests. This system will *retry* sending the SYN-ACK packet five times when it fails to receive an ACK packet in response, at 30-second intervals, before purging the request from its table (pay special attention when you compute the time a connect request stays in the table). Assume that no additional countermeasures are used against this attack and that the attacker has filled this table with an initial flood of connection requests.

1. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? (4 pts)
2. Assuming that the TCP SYN packet is 40 bytes in size (ignoring framing overhead), how much bandwidth does the attacker consume to continue this attack? (4 pts)

7. (6 pts) Describe (with some details) three methods for DoS attack prevention or mitigation or defense.

8. (9 pts) This problem deals with storing passwords in a file.

1. Why is it a good idea to hash passwords that are stored in a file?
2. What is a salt and why should a salt be used whenever passwords are hashed?
3. What are the criteria for a good password hashing function?

9. (8 pts)Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary is able to attempt passwords at a rate of one per second.

1. Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?
2. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

10. (10pts) Because of the known risks of the UNIX password system, the SunOS-4.0 documentation recommends that the password file be removed and replaced with a publicly readable file called /etc/publickey. An entry in the file for user A consists of a user’s identifier , the user’s public key , and the corresponding private key . This private key is encrypted using DES with a key derived from the user’s login password . When A logs in, the system decrypts E(PRa, Pa) to obtain PRa.



1. The system then verifies that was correctly supplied. How?



1. How can an opponent attack this system?
2. (8 pts) Problem 7.26.
3. (9pts) Problem 7.38 (a)(b)(c) only .
4. textbook 11.6.a (6pts)
5. 11.15 (8pts)
6. 11.16 (8 pts)