San Diego State University
CS574 Computer Security
Homework Assignment #5
Due Date: May 9 2021 11:59 PM

● Please type the solutions using a word processor such as MS Word, Latex, or write by hand neatly and upload the scanned copy of it.
● I, _____ (sign your name here), guarantee that this homework is my independent work and I have never copied any part from other resources. Also, I acknowledge and agree with the plagiarism penalty specified in the course syllabus.
● Turn in your assignment through the blackboard before the deadline. Penalty will be applied to late submission.

1. (20 points) 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. 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. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? 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?

2. (30 points) Client puzzles is one effective method that is proposed against DDoS. Specifically, after the client sends a connection request, the server will generate a fresh pair of k and x such that $\mathrm{HMAC}_{\mathrm{k}}(x)$ ends with n bits of 0. Afterward, this random challenge k and the difficulty parameter n will be sent to the client. Now, the client has to provide the server with a solution x' such that $\mathrm{HMAC}_{\mathrm{k}}(x')$ also ends in n zero bits. (Let's assume that the server and the client agree on the hash function in HMAC. It doesn't matter whether $x = x'$.)

   a) The output of HMAC is uniformly random. Given n, what is the probability that the client can find at least one solution after trying N times? Pick an n by yourself and draw the probability-N graph to explain the tendency.

   b) How does n affect the security?

   c) How many HMAC calculation does the server need to do in this protocol (not including the pair generation)?

   d) Do you think k needs to be random for each client's request? Why?

3. (20 points) Describe how a DNS poisoning attack works and ways to mitigate it. List a case where a DNS poisoning took place. Which network was poisoned, who were the victims, and how did hackers exploit the poisoned system? Could this exploit have been stopped? How? Whose responsibility is it to stop these kinds of attacks? (You may refer online sources but the information should be in your words)

4. (30 points) When a DoS attack is detected

a) What steps should be taken?

b) What measures are needed to trace the source of various types of packets used in a DoS attack? Are some types of packets easier to trace back to their source than others?

c) Assume a future where security countermeasures against DoS attacks are much more widely implemented than at present. In this future network, anti-spoofing and directed broadcast filters are widely deployed. Also, the security of PCs and workstations is much greater, making the creation of botnets difficult. Do the administrators of server systems still have to be concerned about, and take further countermeasures against, DoS attacks? If so, what types of attacks can still occur, and what measures can be taken to reduce their impact?