CECS 378 Assignment 4 - Denial of Service

20 points

Assignment Description. Answer the following questions from the Chapter 7 reading from your textbook. Be through and complete with your answers. You *may* work on these questions with a partner (no more than two working together), but **both** students must submit the document individually on Beachboard Dropbox along with both of your names on each submission.

1. Define a denial-of-service (DoS) attack. How does it differ from a distributed denial-of-service (DDoS) attack?

2. What is the primary defense against many DoS attacks, and where is it implemented?

3. What architecture does a DDoS attack typically use?

4. What do the terms slashdotted and flash crowd refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack?

5. What steps should be taken when a DoS attack is detected?

6. 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?

7. In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5-Mbps link? How many per second if the attacker uses a 2-Mbps link? Or a10-Mbps link?

8. Consider a distributed variant of the attack we explore in the above problem. Assume the attacker has compromised a number of broadband-connected residential PCs to use as zombie systems. Also assume each such system has an average uplink capacity of 128 kbps. What is the maximum number of 500-byte ICMP echo request (ping) packets a single zombie PC can send per second? How many such zombie systems would the attacker need to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a10-Mbps link? Given reports of botnets composed of many thousands of zombie systems, what can you conclude about their controller's ability to launch DDoS attacks on multiple such organizations simultaneously? Or on a major organization with multiple, much larger network links than we have considered in these problems?

9. Assume a future where security countermeasures against DoS attacks are much more widely implemented than at present. In this future network, antispoofing 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?

10. In order to implement a DNS amplification attack, the attacker must trigger the creation of a sufficiently large volume of DNS response packets from the intermediary to exceed the capacity of the link to the target organization. Consider an attack where the DNS response packets are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker trigger to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a 10-Mbps link? If the DNS request packet to the intermediary is 60 bytes in size, how much bandwidth does the attacker consume to send the necessary rate of DNS request packets for each of these three cases?

Deliverables. Submit the answers to the questions on **Beachboard Dropbox** by the indicated due date and time. Acceptable file submission formats are: .txt, .rtf, .odt, .doc, .docx, or .pdf.