1. Report Header

Performing a Denial of Service Attack Using Various Packet Protocols
Austin Hall
4/21/20

2. Statement of Objective

The primary objective of this experiment was to educate students about performing a Denial of Service attack using three different protocols. The lab experiment was undertaken with the purpose of exploring how a DoS attack is executed, plotting the data generated, and comparing the value among the different protocols.

3. Data Capture/ Analysis

To conduct this experiment, I needed three virtual machines and a pfSense firewall. The primary machine I used was a linux sniffer that captured the packets passing over the network. Then I also used a Windows system as the attack machine, a pfSense firewall, and a Windows server. To begin the experiment, I booted up the linux machine and then saved the current IP configuration to a file. This is also where I found the first flag. It was in another text file that was similar to the one I just created, which I opened with cat ip2.txt. It contained the output of another ifconfig command and there was a data field called sample flag and it had the value of 999818. The next flag was captured in a very similar way, the only difference being a file called ip3.txt instead of ip2.txt and the value was 123457. The data contained in these files wasn't itself pertinent, but the real world equivalent could be useful because it was placed in an area of text that contains important information and is an abstraction of what could be useful data. After creating the file with the ifconfig output, I used ifconfig eth0 0.0.0.0 up to configure the system to not have an IP address. After that, I began to do a TCPdump sniff on the eth0 interface and wrote this data to a file called TCPcapture.cap, using the command tcpdump -i eth0 -nntttt -s 0 -w TCPcapture.cap. While this capture is running, it will record the number of incoming packets on the network. Once this capture began, I moved over to the Windows attack machine, booted it up, and started the program called Low Orbit Ion Cannon, which is an open source network stress testing and denial of service attack application. For the target address, I used 203.0.113.100, which is the address of the pfSense. For the method I used TCP and began the attack. I let it run for 30 second before ending it, and then ended the packet capture running on the Linux machine. I then opened this capture file to view the contents and check the number of packets received by the can from the attack, which was around 30,000,000 packets. I then moved onto doing a UDP and an HTTP attack, following the exact same procedure as with TCP, except under the method selection, I selected the appropriate protocol. After attacking in the three different ways and capturing the results, I booted up the other Windows server and navigated to the C drive on its local disk. I navigated to and then opened the xampp folder where I found the third flag in a text file named flag3. The value of this flag 774556, which again, doesn't mean anything, but it was found in a place that in the real world could have important data like logs and other system information. Then from within the xampp folder, I navigated to the apache folder where I found the fourth flag with the value 345678. The flag has no real value other than being a place holder for something that could have possible value in the real world. From within the apache folder, I found the fifth flag in the logs folder, and using the same method as before, discovered the value to be 818772. The sixth flag was a little more difficult to find because it was in file within the logs folder named access.log. This file had several mb of text data and to find the flag, I had to use the find function and searched for the string “flag6” within the document. I found the value to be 445616. The real world application of this value is the ability to search for a specific value within a large collection of data, and that data being the access logs.

4. Conclusion

Although the captured flags don't reflect one of the objectives of this experiment, the objective of using the Low Orbit Ion Cannon to conduct different DoS attacks on a network was achieved. I used this application to attack the network and was able to plot the number of packets received by the target system, which was a surprisingly large number and satisfied another objective of the experiment. Comparing the result of each DoS attack was achieved as well and it was interesting to see that HTTP sent the most packets. Each flag captured in this experiment had its real world implication, being for the most part, an example of how to find system logs to analyze the traffic on a network and showcasing the high volume that a DoS attack produces. The implication of this experiment is that a network can only handle so much traffic coming in at a time, and if too much happens at once, the system will not be able to function properly. Because of this, precautions should be taken to minimize the damage that an attack of this kind can produce.