Denial of service at home

Jacob Berger

4/21/20

Statement of Objective

This lab was intended to demonstrate how to perform a denial of service attack. It also provided a brief look at the results of the attack, as well as how to capture the results of said attack with tcpdump.

Procedure

The Kali VM was accessed and a TCP capture was started. The attack machine was accessed where LOIC was used to bombard an IP address with packets. The attack and capture were stopped after a short while and the results were saved to a .cap file. Another attack was performed using UDP, once with HTTP, and once more with HTTP without waiting for a reply. On the Windows Server machine, the access.log file was viewed and shown to contain the string from the attacks repeatedly.

Data Analysis

Flag 1 was contained in the configuration of the Kali machine, and was accessed by using ifconfig to show the network interface information.

Flags 2-5 were found in various subdirectories while looking for the log file.

Flag 6 was found in the log file itself, along with the string from the attacks.

Discussion of Results

The command which showed flag 1 is very useful for determining the current configuration of the network interfaces. I believe flags 2-5 were simply to make sure the log files were easy to find and I was in the correct directories. Flag 6 was useful because it revealed there was an identifiable result of our attacks, and where it could be found.

Conclusions

This lab shed light on how easy one of these attacks would be to perform in the real world. It's simple enough for anyone to perform an attack without really knowing what's going on behind the scenes.