Tidying Up Ports

Jacob Berger

4/18/20

Statement of Objective

The goal of this lab was to familiarize

Procedure

A virtual machine running Kali was accessed and Zenmap was started. An “intense scan” was done on a single host where the OS and all open ports were displayed. On the Ports/Hosts tab, more information was available such as a longer description of the service and the version. Back in the terminal window, we next tried to connect to each of the open ports starting with the lowest number. The first two were able to connect, the third connection was closed by the host with a flag, and the next was just a wall of ASCII characters. The next port accessed was the FTP service, where files were listed and transferred with “ls” and “get”. The next port was accessed using telnet, where again a username and password were required as with FTP. Port 80 was accessed and some HTTP information was printed out. Ports 7-19 were specifically scanned again. On the target machine, the “Simple TCP/IP” service was stopped and disabled, which resulted in a second scan of ports 7-19 all being closed. This did not affect the FTP service. The service was stopped and disabled resulting in subsequent nmap scans showing the port is now closed. This process was repeated for the remaining open ports.

Data Analysis

Flags 1-3 were easily found by running a simple nmap scan from the terminal. They revealed the name, status, and description of the ports.

Flag 4 was accessed with the telnet service. This was just using the Quote of the Day service.

Flag 5 was found in the closing message after exiting the FTP service. A username and password were required to access the FTP server.

Flag 6 was hidden in the contents of the file we downloaded from the target system. This shows that an FTP connection can be used to easily transfer files from one host to another.

Discussion of Results

The flags in this lab were all fairly simple to obtain. The first three found with a nmap scan revealed basic information about the state of the target’s ports. Doing a more intense scan with Zenmap showed much more information about these ports. This is valuable for determining the version of each service. The next two flags were found by exploring more open ports that may not be too useful anymore, such as the QOTD service. This shows that there are most likely open ports on the average user’s machine that don’t need to be open, as they aren’t being utilized.

Conclusions

This lab was a wakeup call for me, as I had no idea there were so many open ports on my own machine at home. If I was unaware of this throughout prior classes, I’m sure there are more vulnerable systems

everywhere. Nmap/Zenmap are powerful tools that can provide much more information about a system than the user most likely wants to divulge or even is aware of. I can also see the telnet and FTP services as large vulnerabilities for the average user.