1. **Report Header**

   Utilizing nmap and telnet to access open ports and closing ports to improve security
   Austin Hall
   4/17/20

2. **Statement of Objective**

   One objective of this experiment was to investigate the way vulnerable ports can be closed to improve the security of a pfScan firewall. Another purpose of conducting the experiment was to explore the way nmap and telnet can be used to scan/ connect to these ports.

3. **Procedure**

   To conduct this experiment, I needed two virtual machines. The primary machine I used was a Linux system, while the target machine was a windows system with several opened ports. I first used nmap and it's GUI equivalent, zenmap, to scan a range of ports (7-19) to find ones that are open. During the next stage of the experiment, I went through the list and used telnet to connect to many of these open ports using "telnet 192.168.12.11 <port number>". Once connected to the remote machine, in most instances, I simply typed the escape key and then quit the connection. But in a couple of connections, I either retrieved a file from an ftp server and read the text file, or queried what an http get requested header would return from port 80. In the final stage, I closed unnecessary ports and services. To do this, I opened the Microsoft Management Console. Then for each port that needed to be closed, I would search for the service name in this console and in the "startup type" dropdown list, select disabled. Each time after closing a port, I would verify it was closed using nmap and specifying the desired port.

4. **Data Analysis**

   During this experiment, I gathered my data by connecting to a remote machine with the use of telnet after scanning for open ports with nmap. The first three flags were 999818, 944555, and 934303, and I captured them by using nmap to scan open ports. The three flags were listed under the "services" section of the nmap scan on ports 1030, 1031, and 1032 of the remote machine. I found the next flag by connecting to port 17 of the remote machine using telnet. The flag was displayed on the screen after connecting and had the value 233344. The objective in gathering this information was to expose the vulnerability of port 17. The next flag was a little more difficult to find. I had to connect to the FTP server using the login name "ftp" and password "password". After listing the files available to view, then using the get command, I was able to transfer the hi.txt file to my own machine. The objective of this capture was to exploit the FTP server's files. After getting the files, I exited the machine using the bye command, and at which point was presented the fifth flag with the value 775661. The final flag was found within the text file obtained from the FTP server. After opening the file, the contents were "hello world" with the value of flag 6, which was 667222.

5. Discussion of Results

The first three flags captured were easy to find, they were simply listed with the nmap port scan command. The data they held didn't tell me much, but their real word data equivalent would be the services provided by a particular open port, and showed me how to look at these ports for pertinent information. The data of the next flag didn't have any practical significance either, but a real world equivalent might. The flag was found by exploiting an open port and gaining access to a remote machine using telnet, which in a real system may provide me with a useful "quote of the day." The next flag found in the FTP server, again, contained no useful information, but the method in gathering that information had some real value. In the real world, it will be very useful to be able to connect to an FTP server and query it for information. The final flag also didn't contain information that was useful, but knowing how to open a file that was obtained remotely will be a necessary tool. After capturing each of these flags, the ports that they were found using, and several other vulnerable ports, were closed on the remote machine to improve the security. After closing each port, I tested whether they were properly secured or not using the nmap scanner.

6. Conclusion

Although the captured flags don't reflect one of the objectives of this experiment, the objective of securing the vulnerable ports to improve security was achieved. Each port that I was able to exploit and gather data from was subsequently closed, thus improving on previous vulnerabilities. The second objective, to explore the use of nmap and telnet in scanning and connecting to open ports, was achieved as well. Each flag captured in this experiment was done so using one of these two tools, and often in conjunction with one another. The implication of this experiment is that there are some ports that may be vulnerable, and because of this vulnerability, they can be exploited, allowing access to a system. Because of this, unnecessary or unused ports should be closed to improve the security of a network.