Samantha Leahy

Research Report 2: NMAP

What did you do?

I first downloaded nmap 7.94 from the website provided of nmap.org. After downloading, I opened the command prompt window and dragged the folder that I wanted to use (which included the download of nmap) into the window. It took me a few tries to finally be able to execute nmap in the window, due to not fully understanding which exact folder or spot in the path I needed to be at for the application to run correctly. After successfully executing nmap, to map my home network, I then ran two separate commands. The first one was nmap -sVC -O -T4 scanme.nmap.org which was included in the instructions on how to run nmap. The second command I ran was nmap -v -A snanme.nmap.org, which I found in the options summary after first executing nmap under 'EXAMPLES'. I analyzed which ports were open/closed and what each port was servicing. I also analyzed how many ports were listed as not shown and closed. Another characteristic I analyzed was the TCP sequence prediction. I was able to put together an attack surface by looking at these results and deciding where possible weak spots could be.

What are the results?

After running the two commands listed in the above paragraph, I noticed that the output information was similar, but the command nmap -sVC -O -T4 scanme.nmap.org did not include traceroute information like the other did. After doing some research, I found that traceroute is used to "provide a map of how data on the internet travels form your computer to its destination" (information found at this link). The traceroute results provided the hop number, round trip time, and IP address. The nmap results showed that 996 ports were closed and not shown while 3 ports were open and 1 was filtered.

The protocol I found that was utilized in the mapping process was TCP, ensuring a standard is met to allow messages to be exchanged. The components used to piece together an attack surface presented by the network were the number of open ports and the TCP sequence prediction from the mapping results. The number of open ports presented was 3 which can lead to a vulnerability when it comes to the attack surface. The TCP sequence prediction did not present a vulnerability for the attack surface, but a benefit as the results presented difficult. The physical aspect of my home network's attack surface includes 3 mobile devices, 4 laptops, and a Bluetooth speaker. An attacker can access these components physically which makes this aspect vulnerable. We have internet security in place for the laptop devices which lessens the vulnerability of that physical aspect.

What did you learn?

The mapping process was new to me and helped me put together a possible attack surface for my home network. I had not thought about the vulnerabilities of my home network until fitting these pieces together. This helps me understand more why this can be done for an organization and how helpful it would be to know the vulnerabilities to reduce the chances of attackers gaining access to valuable information. I work from home with customer information that needs to stay protected, so the more I know about an attack surface, the more secure I feel about the systems that play a part in my home network. For future use, if I were to move or create my own company, I would have a better understanding of where to start on piecing together an attack surface.