Arkadiy Kantor

Nessus Scan Assignment

MIS 5211

The purpose of this exercise was to practice using Nessus scanner to check for Vulnerabilities. Nessus is the leading Vulnerability scanner. I decided to expose my whole network to the application. Recently having acquired several new and old Smart/IoT Devices. These devices can leave my home and personal property vulnerable so I thought it would be a good idea to take a shot at them considering the recent massive DDoS was using IoT devices.

First I did a Host scan of the 192.168.1.XXX subnet and found 15 devices. I cross-referenced this list to the DHCP table in my router so I knew what devices had what IP. Surprisingly the most vulnerabilities were found on Windows 10 desktop, thankfully none of them are critical but should probably be addressed. I was disappointed to find out that my “Enterprise grade” Ubiquiti Wireless AP had a critical bug and several other important warnings. My most alarming find was a potential critical Samba buffer overflow vulnerability that is on my wireless bridge. Its running a custom open source firmware which I have not kept up with patching.

This was a great exercise which game some great insight into what is happening on my home network. Since I have been automating so much of my house it will be even more critical to keep everything secure and up to date. I will work on patching up the flaws or eliminating the affected hardware/software in order to secure my network and house.