Executive Summary

This exercise is to get a warm feeling of the Nessus tools and how to utilize its great capabilities on scanning vulnerabilities and other basic network issues within a private or public network.

Nessus is a powerful remote security scanning tool, which scans a computer or network, and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to your network.

In this test, we scanned 192.168.1.1/24, which Nessus detected 9 hosts, and 53 vulnerabilities. Once the results were available, the summary of medium, low, and info were not as alarming as I thought they were going to be, however the medium level vulnerabilities described SSL Certificates cannot be trusted, SMB signing disabled and SSL Self-Signed Certificates as some of the medium vulnerabilities to fix within my host computer.

Nessus scan provides the results, and brakes down descriptions and solutions to each vulnerability found. This makes it easy to understand and to remediate issues. With the scan detail, users can identify the name and status of each potential issue and how to resolve it, all in one page.

My opinion on Nessus is that it is a powerful tool and it can be used for good purposes, since it really provides the user the ultimate experience, besides the fact that network vulnerabilities are discovered and a simple analysis on how to fix them is also part of the tool.

I really enjoyed working this exercise because now I am more familiar with my own vulnerabilities and I can find out how to fix them soon.