Nessus/ShieldsUp Assignment

Jim Kinter

CIDM6340

1. What did you do – I started by asking for permission to scan my employer’s network. Unfortunately I was summarily denied and told that any use of network surveillance/interrogation is considered a cyber crime and would result in termination. Since I don’t have access to another network, I chose to analyze my personal network. I started the vulnerability investigation/assessment of my local network by running the Common Ports scan using ShieldsUp. Because ShieldsUp only scans a single address, the software scanned the WAN side of my router. In the spring of 2024 I took CIDM 6310 and we did a similar exercise to this using ShieldsUp. At the time the software found a litany of security vulnerabilities. Following that exercise, I really took the matter seriously and undertook a process of remediating the vulnerabilities and patching all of the devices on the network. That exercise seems to have resulted in a better security posture for myself and my family. The experience of running the scans was straight forward and resulted in a clean bill of health. Next, I downloaded and installed Nessus. I entered the license key that was emailed to me and let the installer compile the plugins. After the installation completed I let the software scan the network. The discovery scan identified 32 devices. Because the Nessus student/education license only allows me to scan 16 devices, I randomly selected devices on the network, making sure to choose my PC, the Orbi router and the Orbi Satellite, and then 14 other devices. I used the information from the NMAP exercise to inform this selection; however , since that NMAP exercise was over a week ago I couldn’t have absolute certainty that the IP Addresses identified by NMAP were what I thought they were in the Nessus selection list. I let the Nessus scan run for the 16 identified hosts and then I reviewed the results.
2. What are the results – As you can see below, both of the ShieldsUp scans yielded a healthy report with no public exposures. Because the free version of the ShieldsUp services can only interrogate my network from outside, the failure to identify vulnerabilities is both a blessing and a curse. A blessing because this means that, at least for the things that ShieldsUp scanned for, my network is safe. A curse because it’s only looking at things from the outside and that doesn’t mean that there are no vulnerabilities, just that my Orbi router’s configuration is preventing bad actors from seeing/scanning/finding the hosts that are on the LAN side of the router. The free version of the ShieldsUp tool doesn’t seem to allow me to scan the LAN side of the network so I have to trust Nessus to identify what vulnerabilities exist behind the router. When I ran the Nessus Scan everything came back clear with a few minor exceptions. Two of the low risk findings were false positives in that they were raised about the existence of a DHCP service on the router, but the router actually is the DHCP server on the network. The other low risk vulnerability has to do with ICMP Timestamp Request but this vulnerability is associated with Windows devices and none of the devices Nessus identified are windows devices. The Nessus tool allows the user to specify the 16 IP addresses to scan and then uses a library of 185,101 vulnerabilities across 56 dimensions to identify and score any matched conditions.

A close-up of a computer security system

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. What did you learn – My biggest learning from this exercise is that the time and effort spent at the end of last semester to minimize the attack surface of the network and implement practices to ensure that all devices on the network are running patched OS and the most up to date firmware has been time well spent. Taking a defense in depth approach, regularly assessing network devices, monitoring changes in network behaviors or hosts, using tools like NMAP, ShieldsUp, Wireshark, and Nessus , and reviewing event logs are great steps to protect my family; however, I also can’t uses this finding to get complacent or convince myself that the things that you’ve taught me are enough. Risk mitigation is a never-ending process of inspection, adaptation, and investment.