Brent Easley

MIS-5211

Intro to Ethical Hacking

**Nessus Vulnerability Scan Report**

Performing a vulnerability scan is fundamental for any organization. Vulnerability scans are an important process that every network administrator should perform regularly. Vulnerability scans can find unnecessary services running on some devices, web services that contain known vulnerabilities, dangerous applications, such as peer to peer applications, and third party applications that can be exploited. A tool like Nessus can help with finding potential network security vulnerabilities. In this vulnerability scan report, I used the Nessus Scanning tool on the wireless network at my home. I used the Nessus scanner on the following devices: my Comcast cable modem, my work laptop and a laptop I borrowed for testing. My work laptop has Windows 10 installed on it and the laptop I borrowed for testing has Windows 10 installed on the hard drive. I used my work computer as the host device to perform the scans over my wireless network. The Nessus scan came back with the following report: My work computer had 4 medium level vulnerabilities, 94 info reports, my home cable modem had 1 medium vulnerability, 1 low security vulnerability, and 5 information reports and the laptop I borrowed had 13 information reports and no vulnerabilities.

 The 5 vulnerabilities reported on my work laptop were SSL Certificate could not be trusted, SMB Signing Disabled, SSL Certificate Cannot be Trusted and SSL Self Self-Signed Certificate. From the diagnosis of the scan from Nessus, it seemed to recognize that VMware was installed on my laptop and that was the cause of the vulnerabilities. The possible vulnerabilities could be subjected to man-in-the middle attacks if the remote host was a public host in production. There were two vulnerabilities on the Comcast cable modem in my house. The two vulnerabilities were DHCP Server Detection which gave me a low warning and DNS Server Cache Snooping Remote Information Disclosure which displayed a medium warning. The resolution for the DHCP Server Detection was to apply filtering and the resolution for the DNS Server Cache Snooping Remote Information Disclosure was to contact the vendor of the DNS software for a fix. The last device that was scanned by Nessus was a laptop that I borrowed for testing and this device did not report back any vulnerabilities and gave 7 information reports.

 The first step of protecting your devices on your network are patch management and antivirus protection. Once those steps have been taken, hackers still might be able to exploit your network, so that is why running a vulnerability scan you might be able to find multiple security issues with the software on your devices and the hardware that is connected to your network. A reliable vulnerability scan assessment should be the next move in protecting the hosts on your network. A vulnerability scan assessment should be performed on any network, whether it be at your home, or if you are in charge of the network at your place of employment. Networks are changing every day and it is important to protect your personal and confidential information. A vulnerability scan assessment should be scheduled to run frequently and to alert the network administrator every time there is a change to the network. This will be essential in keeping the network secure at all times and sensitive information out of the wrong hands.