**Nessus Analysis**

Hackers like to use vulnerabilities in a system to break through defenses in order to take over a machine. Vulnerabilities must be kept to a minimum if you want to stay safe. This is where Nessus comes in; a scanner that will detect known vulnerabilities in a device on a network. Nessus is meant to be used as a preliminary step, as it will show you what needs to be fixed and not as a total solution. It can quickly scan and rank issues that it finds while also teaching you why each issue is problematic. Once your assessments are done, it is up to you to either patch up the security of the device or block it from your network to increase your security. If more information is needed, the full version of Nessus offers over 80,000 plugins to further hone scans based on the OS, ports, DNS, databases, firewalls and more

I used Nessus to scan my local network for vulnerabilities on my devices. In order to “aim” Nessus, you need to know the IP address of the device you want it to look at. Nmap is a good way to find the IP addresses on your network. From there, I tested my Linux Mint computer and my Google TV box. Most of the results came out rather secure with the biggest vulnerability being the low risk UPNP protocol which is needed to be open for media streaming.

I then created a Metasploitable virtual machine on the network, to simulate a flawed device that can demonstrate vulnerabilities. Nessus ran for approximately 10 minutes and returned with a result of 150 items of interest. On the threat level of the results, 8% of the issues were critical, 3% were high, and 21% were medium. An example critical threat was classified as a backdoor, named rogue shell backdoor detection. It defined this issue as “a shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.” The commands Nessus used to try to find the flaw are shown in an output window, as well as showing the port and network protocol. Nessus also proposes a potential solution of examining the device to see if it has been compromised already, and reinstalling the system completely.

I recommend that Nessus should be used as a regular tool that tests devices on a network. It would also be a good policy to scan new devices when they are detected on the network. This way, an administrator will have to worry less about random backdoors and other issues that might exist. Nessus is only to be used as a starting point as while it recommends solutions, they may not be right for every situation. There may also be other information on the exploit that is newer that is not in Nessus’s database. Nessus is still a valuable resource to have in your toolbox to protect your network.

**Metasploitable Results**



