Vulnerability Scanning Report

**Overview:**

Network vulnerability scans are used to detect weaknesses in networks. In the era of Network of Things any piece of hardware connected to your infrastructure could be a vulnerability. In addition to pc’s and printers we now have mobile phones, tablets, televisions, VOIP phones, refrigerators, alarm systems to name a few that could act as a gateway for a potential attack on a network. Threats can range from the loss of network connectivity to financial and personal data exfiltration. That is why it is important for organizations’ IT teams to perform vulnerability scans on their networks hardware (Servers, routers, switches, appliances) before introducing them into the production environment.

**Summary:**

My vulnerability scan was done using Nessus vulnerability Scanner. I used Nessus vulnerability scan advance network scan feature on my home network which consist of a wireless router, Apple TV, Vizio Smart TV, iPad Air, iPhone, Windows 10 laptop, MacBook Pro, MacBook Air and VM Linux box(metasploitable). All my personal devices are kept up to date with the necessary Windows and IOS updates. In addition to that I also create local profiles that are password protected and have virus protection software installed. My VM is a metasploitable with vulnerabilities imbedded in it. Before running the scan, I was pretty sure that my home network was well secured and protected. As a result of my scan I was able to confirm that my home network was indeed secure from critical outside risks.

My initial scan was wide and covered the IP range of 192.168.1.1 – 192.168.1.100



The scan represented above yielded no red flags; I did have 6 mediums and 1 low vulnerability but nothing to be alarmed about. Those vulnerable were all found on the network router and were primarily SSL certificate related. I plan to search for a firmware update to see if those vulnerabilities could be remediated. Nessus also revealed that the devices on my network had a lot of open ports but that was to be expected. I then ran Nessus vulnerability scan against a Metasploitable virtual machine which yielded some very interesting results. There were warnings in the critical, medium and low risk categories.

 

**Warning #1:**



The scan revealed the VNC Server component has a weak password which could easily be exploited. The fix is to simply change the password to a stronger more secure one. I recommend using a passphrase.

**Warning #2:**



The current Unix operating system is no longer supported. Once an OS is no longer supported, hackers target those Operating Systems for future vulnerabilities because they are aware that everyone would not immediately go out and update their OS and many people simply forget over time. The fix is to update to the latest supported OS.

**Warning #3:**



File transfer protocol is configured to allow anonymous logins. Allowing any remote user to authenticate without having to provide username and password. The fix is to disable this setting.

**Warning #4:**



The File Transfer Protocol(FTP) is currently configured to send usernames and Password in clear text, so anyone with a sniffer can easily steal user names and password. Which over time someone could collect a substantial amount of data. The fix is to switch to secure file transfer protocol(SFTP)

**Conclusion:**

IT security is more relevant today than it has ever been. The concept of set it up and forget doesn’t fly any longer. By default, many servers and hardware appliances come with a great deal of open ports. If those ports aren’t needed, then they should be closed before going into production. It is better to be more restrictive then to find out later something could have been avoided. Securing and maintaining a company’s infrastructure should be one of the top priorities of any CEO in this technology driven age. Tools such as Nessus vulnerability Scanner can be used along with other techniques to keep a vigilant eye on your network.