Nmap Assignment

Port 23 is the port I selected as being the most vulnerable as it is used for telnet. Telnet transmits all data in cleartext and has absolutely no encryption any data sent via this port would be extremely easy to intercept and/or manipulate. I just recently put a new hard drive and am running a fresh windows install thanks to this assignment I realized telnet was still on it no longer is.

In lieu of a screen shot I have added the complete log of the nmap scan due to it being a virtual machine I felt that enough information was not given:

# Nmap 7.60 scan initiated Sat Oct 14 22:02:15 2017 as: nmap -sV -T4 -O -F -oN nmapscan.txt --version-light 10.0.0.1

Nmap scan report for 10.0.0.1

Host is up (0.021s latency).

Not shown: 94 closed ports

PORT STATE SERVICE VERSION

22/tcp filtered ssh

23/tcp filtered telnet

53/tcp open domain dnsmasq 2.76

80/tcp open http lighttpd

443/tcp open ssl/http lighttpd

49152/tcp open upnp Portable SDK for UPnP devices 1.6.22 (Linux 3.12.14; UPnP 1.0)

MAC Address: 00:50:F1:80:00:00 (Intel)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4

OS details: Linux 3.2 - 4.8

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel:3.12.14

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Sat Oct 14 22:02:35 2017 -- 1 IP address (1 host up) scanned in 21.05 seconds