Keshia Horton

440 – Network Home Analysis

DIAGRAM

Diagram

Description automatically generated

DESCRIPTION

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **IP Address** | **OS** | **Open Ports** |
| Netgear R6300v2 | 192.168.1.1 | Linux | 53, 80, 5000, 8200, 20005 |
| LAPTOP-D55K6KSH | 192.168.1.8 | Windows | 135, 139, 445 |
| DESKTOP-5EM52PE | 192.168.1.5 | Windows | 135, 139, 445 |
| ROKU | 192.168.1.3 | Proprietary | - |
| Xbox One | 192.168.1.4 | Proprietary | - |

ANALYSIS

Netgear R6300v2 – This is my personal router. Port 53 is the DNS. There are vulnerabilities having this open to the public, but I ran a security check on it and it’s not open to the public. Port 80 is open and used for web traffic. Port 5000 is the Plug and Play port and is susceptible to trojan horse attacks. Port 8200 enables the transmission of datagram messages from a computer to a computer application. Port 20005 is a KCodes NetUSB Linux kernel driver. If someone gained access to my network internally, they could trigger a buffer overflow that would result in a DoS attack. Ports 5000, 8200, and 20005, however, are not open on the external network.

LAPTOP and DESKTOP – Ports 135, 139, 445 were all open but after testing they were not open to the public network. Port 135 is the Remote Procedural Call port. This port is used in client/server applications like Messenger Service. If this port was open to the public, a malformed web request to this port could create a DoS attack.

ROKU – No ports were able to be scanned. I did do some research to see what ports might be open. On a different Roku model, port 8080 was open. I tried telnetting in to this port but was not successful.

Xbox One – No ports were able to be scanned. After some research, port 53 is a port that is commonly open. I tried scanning this port, but it was not successful.

CONCLUSION

In conclusion, I was expected to have poor security and more open ports than there are. There weren’t any open ports to close or anything to patch. I will, however be more alert about my home security and stay consistent with checking the network, for updates, etc.

SCAN

Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-03 02:54 Pacific Standard Time

Nmap scan report for 192.168.1.3

Host is up (0.100s latency).

All 100 scanned ports on 192.168.1.3 are filtered

MAC Address: C8:3A:6B:DB:B9:FE (Roku)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 192.168.1.4

Host is up (0.19s latency).

All 100 scanned ports on 192.168.1.4 are filtered

MAC Address: 98:5F:D3:19:4E:18 (Microsoft)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 192.168.1.5

Host is up (0.053s latency).

Not shown: 97 filtered ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

MAC Address: 9C:B6:D0:F5:AE:97 (Rivet Networks)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: specialized|general purpose

Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (87%), FreeBSD 6.X|10.X (86%)

OS CPE: cpe:/o:microsoft:windows\_xp::sp2 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3

Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.8

Host is up (0.000031s latency).

Not shown: 97 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=7.70%E=4%D=12/3%OT=135%CT=7%CU=32017%PV=Y%DS=0%DC=L%G=Y%TM=5C050C

OS:45%P=i686-pc-windows-windows)SEQ(SP=108%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=

OS:S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4N

OS:W8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN

OS:(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=A

OS:S%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%

OS:W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)

OS:T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A

OS:=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D

OS:F=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=8

OS:0%CD=Z)

Network Distance: 0 hops

Service Info: Host: LAPTOP-D55K6KSH; OS: Windows; CPE: cpe:/o:microsoft:windows

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

Nmap done: 256 IP addresses (4 hosts up) scanned in 196.88 seconds

References

Ports database. (n.d.). Retrieved December 3, 2018, from https://www.speedguide.net/ports.phphttps://www.speedguide.net/ports.php