Research Report 1 NMAP

1. What did you do?

I began by installing the NMAP software from “nmap.org”. After installing the software I began to run scans. I then did research on how to scan a full network not just one device. I then ran a full Intense scan on my network. The IPs included in the scan are 10.0.0.0-10.0.0.255. The command was this, nmap -T4 -A -v 10.0.0.0-255. I then looked through the results. I then looked into all the other scan options and ran a few of them.

1. What are the results?

components and protocols

The NMAP scan found 16 hosts online and 19 different services. This is the list of hosts and services:

A number of numbers on a white background

Description automatically generated A screenshot of a computer

Description automatically generated

It found 4 different host types:

|  |  |
| --- | --- |
|  | A router. |
|  | A wireless access point. |
|  | A firewall. |
|  | A host with some ports filtered. |

It did have a few errors. My router is on 10.0.0.1 and it only called it a host with 3-6 open ports. My wireless AP is on 10.0.0.41 and it called it a router. I have a Philips Hue hub on 10.0.0.46 and it called it a wireless AP. It did correctly find our mobile phones at 10.0.0.198 and 10.0.0.137. Our printer is on 10.0.0.40. There is a Ubuntu Server on 10.0.0.10. It found a few smart home devices 10.0.0.56 a Chromecast, 10.0.0.111 a rumba, 10.0.0.132 a google home.

I see three main attack surfaces open ports/services, wireless, and open physical ports on unmanaged switches. The physical ports are an attach vector sense someone could just plug in a device and be into the network from there. The wireless is a similar issue as open ports. Our wireless is of course password protected but between over broadcasting signal and someone repeating the signal to extend it, someone could still attack the network without ever going inside. Once someone is on the network all the other devices are very easy to get to and attack. Someone could also scan the packets and log what is being done and sent over the network.

The open ports and services is probably the largest vulnerability of any network. The more services being used just increase the number of attack vectors. For a residential home I have more than the average home since I have a Ubuntu Server. It alone accounts for 7 different ports/services. A screenshot of a computer program

Description automatically generated

A few of these ports have been forwarded through the firewall so incoming traffic could reach it from the internet or WAN. Most of the ports that do this are forwarded from non-standard ports. An example of this is the SSH or port 22. The Router is not listening to port 22 it is listening to another port that then forwards to 22.

1. What did you learn?

With this being my personal network takeaways and what I’ve learned from this research report is a bit limited. Learning about NMAP as tool has been and will continue to be very useful professionally. I’ve already used it to help trace out what devices are on a network and what switches they go through, so we could find the path a network cable took. Having a new tool is always nice.

I also was not aware of just how many different services are used on a network. I knew of the common ones like ssh, http/https, and vnc. Finding 19 different services did shock me even with having a server. The server only used 7 services while the windows desktops used the majority of the ones found. It is always shocking how much you can see just being on a network. It shows just how vulnerable a workstation can be.

References

Surfing the Network Topology | Nmap Network Scanning. (n.d.). Nmap.org. <https://nmap.org/book/zenmap-topology.html>

What is Network Mapping or Nmap. (n.d.). Www.tutorialspoint.com. Retrieved July 18, 2023, from https://www.tutorialspoint.com/what-is-network-mapping-or-nmap

Peter L Dordal (2022). An Introduction to Computer Networks https://wtclass.wtamu.edu/bbcswebdav/pid-2646370-dt-content-rid-51652144\_1/xid-51652144\_1

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch01\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650746\_1/xid-51650746\_1

Jennex, M. (2023). Why Computers Are Vulnerable r3 [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650747\_1/xid-51650747\_1

Jennex, M. (2023). CIDM6341 Introduction [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650748\_1/xid-51650748\_1

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch12\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646267-dt-content-rid-51650758\_1/xid-51650758\_1