What did you do?

I have a decent understanding of networking and cyber security from training for my MOS as a Signal Officer. I typically understand the topic at hand in these realms and how the players interact. I don’t have the knowledge of how to actually complete the actions necessary, which you’ll see below in some comic reliefs actions taken. Aside from the instructions provided on the Nmap.org website, I used several other tools to research answers. Techies have the issue of already understanding everything they’re talking about and need to work on making the content relatable to introduce aspiring Techies. I read several articles and how to guides on NMAP, command prompt commands, and network architecture. More fruitful was calling Non-Commissioned Officers I’ve worked with in the past. They love helping (or is it me needing help?) and describing their day in and day out job.

1. Visited nmap.org
2. Clicked on “Get Nmap 7.94 here”
3. Clicked Windows option
4. Downloaded nmap-7.94-setup.exe
5. Ran the setup.exe to install and setup the software
6. Agreed to license agreement
7. Designated components below to install excluding Npcap 1.75 and Check online for newest Ncap
   * Nmap Core Files
   * Register Nmap Path
   * Network Performance Improvements
   * Zenmap (GUI Frontend)
   * Ndiff (Scan comparison tool)
   * Ncat (Modern Netcat reincarnation)
   * Nping (Packet generator)
8. Chose to support 802.11
9. Chose file location C:/Program Files (x86)/Nmap
10. Setup completed successfully
11. Created shortcuts in Start menu Folder and Desktop Icon
12. Opened Zenmap GUI
13. Verified I have administrative rights on my PC through file explorer C: > Users
14. Opened Command Prompt
15. Changed directory to “\Program Files (x86)\Nmap”
16. Ran command “nmap -sVC -O -T4 scanme.nmap.org”
17. Ran “ipconfig” to find PC’s IP 192.168.1.15
18. Using Zenmap GUI typed IPv4 into Target field and scanned
19. Printed Zenmap GUI to pdf “Nmap Scan GUI”
20. Attempted to print command prompt output by inputting “dir>print.txt”
21. Attempted to print command prompt output by inputting “Nmap scan.txt
22. Attempted to print command prompt output by inputting “nmap sVC -O -T4 scanme.nmap.org > Nmapscan.txt”
23. Gave up on printing from command prompt
24. Copy pasted into textfile
25. Printed to pdf “Nmap Scan CMD”
26. Opened cmd prompt next morning
27. Ran a trace route “tracert 8.8.8.8”
28. Found home Wi-Fi Router IPv4 192.168.1.1
29. Using Zenmap GUI typed IPv4 into Target field and scanned
30. Printed Zenmap GUI to pdf “Nmap Scan GUI-Router”
31. Using Zenmap GUI typed next IPv4 from trace route 173.219.255.52 into Target field and scanned
32. Printed Zenmap GUI to pdf “Nmap Scan GUI-Provider Router
33. Used Snipping Tool to capture Provider Router Topology
34. Printed to pdf “Nmap Topology-Provider Router”
35. Using Zenmap GUI typed full IPv4 range 192.168.15.1-255 into Target field and scanned
36. Printed to pdf “Nmap Scan GUI-Home Network
37. Used Snipping Tool to capture Home Network Topology
38. Printed to pdf “Nmap Topology-Home Network
39. Using Zenmap GUI typed IPv4 of Neighborhood Service provider router with subnet mask 173.219.255.0/24 and scanned
40. Printed Zenmap GUI to pdf “Nmap Scan GUI-Neighborhood
41. Used Snipping Tool to capture Neighborhood and Home Network Topology
42. Printed to pdf “Nmap Topology-Neighborhood

In analyzing the data I found the NMAP Scan data compilation is as follows:

* NMAP Scan Report for X.X.X.X
* Host status (up/down) with latency
* Not Shown # closed TCP ports
* Port status
  + Port #
  + Protocol used
  + State (open/filtered)
  + Service (Port name)
  + Version (description/version in use)
* OS or Aggressive OS guesses (% breakdown on likelihood of OS if unsure)
* Common Platform Enumeration (CPE) – standardized naming convention
* OS Details
* Uptime guess (how long device has been connected to network)
* Network distance (# of hops from host to destination)
* TCP Sequence prediction: Difficulty?
* IP ID Sequence Generation Incremental (subnet used)
* Service Info: OS; CPE
* Traceroute
  + # Hops
  + Round trip time
  + Address (Device type and IP)

In all honesty, when the NMAP results came back it looked like the matrix at first. My first batch of data analysis was all over the board in picking out details that made sense here and there. I slept on the issue and had a realization in the morning. Computers/networks/commands are all logical. They go from point A to point B. I need to digest the information in the same manner, line by line. I’m accustomed to reading orders and training documents quickly to pull out the pertinent information. Doesn’t seem to be the case for this data set, at least with my level of hands on at this time. Using this step by step process provided the standard data set above with details of devices below.

What are the results?

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.1 | Docsis-Gateway (Home Router) | 990 Closed TCP Ports | |
| 53 – DNS – Open  80 – HTTP – Open  443 – HTTPS – Open  8000 – HTTP ALT – Open  49152 – Certificate Mgmt – Open  49153 – Certificate Mgmt – Open  49154 – Certificate Mgmt – Open | 22 – SSH – Filtered  23 – TELNET – Filtered  9000 – CSLISTENER – Filtered | Protocol 6: TCP Used for 10 ports | Running Linux 3.X I 4.X |
| Uptime 37.529 days  0.0035s latency | 1 Hop, RTT 3.52ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=263 | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.15 | DESKTOP-3SHPIF1 (PC) | 997 Closed TCP Ports | |
| 135 – MSRPC – Open  139 – NETBIOS-SSN – Open  445 – MICROSOFT-DS – Open |  | Protocol 6: TCP Used for 3 ports | Running Microsoft 10 1607 (98%) |
| Uptime 3.293 days  0.00055s latency | 0 Hops | TCP Sequence Prediction: Difficulty=255 | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.129 | Galaxy-Tab-A7-Lite (Cell Phone) | 1000 Closed TCP Ports | |
|  |  | Protocol 6: TCP Used for 0 ports | Running Unknown OS |
| Uptime Unknown  0.038s latency | 1 Hop, RTT 38.46ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=Unknown | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.187 | BRWC61999450D8 (Printer) | 995 Closed TCP Ports | |
| 80 – HTTP – Open  443 – HTTPS – Open  515 – LPD - Open  631 – IPP - Open  9100 – PDL - Open |  | Protocol 6: TCP Used for 5 ports | Running Unknown OS |
| Uptime 5.861 days  0.0069s latency | 1 Hop, RTT 6.90ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=259 | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.210 | RokuPremiere (Roku) | 998 Closed TCP Ports | |
| 7000 – RTSP – Open  9080 – GLRPC - Open |  | Protocol 6: TCP Used for 2 ports | Running Google Android 5.X |
| Uptime 13.477 days  0.0073s latency | 1 Hop, RTT 7.28ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=260 | |

|  |  |  |  |
| --- | --- | --- | --- |
| *173.219.255.0/24* | *84 Commercial Routers/Switches/Firewalls* | | *996 Closed TCP Ports* |
| *\*Traceroute via:*  *Protocol 1: ICMP,*  *199 – SNMP – Protocol 6: TCP\** | *25 – SMTP – Filtered*  *135 – MSRPC – Filtered*  *139 – NETBIOS-SSN – Filtered*  *445 – MICROSOFT-DS – Filtered* | *Protocol 6: TCP Used for 4 ports* | *Running Guesses:*  *Cisco Embedded*  *D-Link Embedded*  *D-Link NetDefend Firewall* |
| *Uptime Unknown*  *Variable latency* | *3-18 Hops, RTT Variable*  *33434 – Traceroute* | | *TCP Sequence Prediction: Difficulty=Unknown* |

Areas identified that are subject to a cybersecurity attack:

* Internet Control Message Protocol (ICMP)
* Transmission Control Protocol (TCP)
* Port 33434 Traceroute (for mapping)
* Open Ports:
  + Port 53 Domain Name System (DNS)
  + Port 80 Hypertext Transfer Protocol (HTTP)
  + Port 443 Hypertext Transfer Protocol Secure (HTTPS)
  + Port 515 Line Printer Daemon (LPD) Print Service
  + Port 631 Internet Printing Protocol (IPP)
  + Port 7000 (RTSP) Streaming Video Content
  + Port 9080 (GLRPC) Groove Collaboration Software (Audio?)
  + Port 9100 Page Description Language (PDL) Data Steam
  + Port 49152-49154 Certificate Management over Cryptographic Message Syntax (CMS)
* Filtered Ports:
  + Port 25 Simple Mail Transfer Protocol (SMTP)
  + Port 135 Microsoft End Point Mapper (MSRPC)
  + Port 139 NetBIOS Session Service (NETBIOS-SSN)
  + Port 445 Microsoft Directory Services (MICROSOFT-DS) Active Directory
* OS
  + Windows 10 1607
  + Google Android 5.X
  + Linux 3.X I 4.X
* Applications/Software
* VPN
* PKI/Security Certificate
  + CA/RA
* Users
  + Accessed website content/security/UI fields/http headers/cookies/downloads
  + Passwords
  + Email
  + Social Media
  + Peer to Peer Sharing
* Physical Devices
  + PC
  + Cell Phone
  + Printer
  + Roku
  + Home Router
    - WPA/WPA2/WPA3
  + Ethernet
  + USB charging
  + External hard drive
* Network Architecture
  + Routers/Switches/Firewalls
  + Wi-Fi
  + Bluetooth
  + Cloud storage
* Physical Security
  + Data Collection – Trash
  + Intruders
* Trusted consumer databases
* Previous connections to networks
  + Public Wi-Fi – Hotel/Library/Restaurant
  + Vehicles
  + Airplane

AKA everything not bolted down! Networking mapping identifies what parts of a system need to be tested for vulnerabilities. As NIST 1271 outlines the Cybersecurity Framework – “Identify, Protect, Detect, Respond, Recover.” Any of the multitude of varieties listed is a potential entry point on my home network’s attack surface. The moment a device is connected to another, vulnerability exists. The modern era’s capability to have information at our fingertips grants immense strength and weakness simultaneously. My compiled attack surface includes protocols, ports, operating systems, applications, software, security certificates, physical access, wireless point access, Bluetooth connections, previous network access, trusted consumer databases, internet provider, physical security, cloud storage and applications, Bluetooth devices, Wi-Fi, internet of things, etc. The amount of attack vectors a nefarious actor can utilize multiplies exponentially on each of these surfaces. The problem with the battle of cybersecurity is wrapped up nicely by Napoleon Hill. “Whatever the mind can conceive and believe, the mind can achieve regardless of how many times you may have failed in the past or how lofty your aims and hopes may be.” The benefit (or challenge) therein is the reputable actors have the same capacity to combat attacks.

What did you learn?

This exercise proved to induce a crawl-walk-run approach with my novice command prompt skills. As a Signal Officer, I have always had the birds-eye-view of the network and haven’t been a “button pusher.” It’s been insightful to address an in-depth look into the network structure. The topology tab on Zenmap was more intuitive for visual information digestion of the network architecture as a whole. I have become accustomed to monitoring tactical networks during field exercises using SNMP displayed in a Network Operation Center. NMAP provided a better grasp of network design to set the foundation for hardening security as well as opening up capabilities. As scary as analyzing the attack surface becomes when you realize it’s just about everything, I see the need to weigh the risk. Does the benefit of what a protocol/port/application/etc provides outweigh the risk? I can see ways of analyzing the risk-benefit and presenting them to commanders/CEOs for a decision.

I recognize that NMAP can be used to verify security measures like port closures and firewall programming. Also, newly uncovered/published vulnerabilities (patch Tuesday) can be specifically targeted with NMAP to test for exposure. Ports 1-1000 were scanned automatically, but I was able to find several webpages that showed comprehensive lists for every type of scan imaginable. A shortcoming I noticed is NMAP gives you a snapshot of your network, but not an analysis tool to compare previous and current iterations. There may be an additional resource that does comparative analysis on historic/current NMAPs, but with the free content I have it’s up to the network manager playing one of these things is not like the other. NMAP is not an IDS/IPS/IDPS, but it will ferret out devices that aren’t expected to be on the network. I was surprised to find NMAP can discover what OS is being used and device vendor names. Although it also makes sense because the analysis provides the MAC, which have prefixes that are vendor specific just like all Visa credit cards begin with a “4.”

I knew the were a lot of ports, but I had no idea there were over 65,000. I would have ballparked it at a few thousand.

* 0-1023 Well Known Ports
* 1024-49151 Registered Ports
* 49152-65535 Dynamic and Private Ports

As expected, firewalls blocked NMAP, I couldn’t see into other home networks nor their devices. Thank goodness! The risk areas exposed by the attack surface were staggering, and that was only with two known protocols and a handful of ports. I understand what systems were identified to review for security vulnerabilities in the coming weeks. Applications and operating system protection best practices available are to ensure timely updates and patches…and reduce the amount used (exposure).

I did not know that using TCP to scan port 80 would have a provided URL. On my home router, port 80 had a redirect to 443 and https://account.suddenlink.net/router-portal.html. Going to this URL in a browser redirected again to https://www.optimum.net. It was interesting to see port 443 conduct an asymmetric encryption three-way handshake SSL-Cert, PKI (RSA 2048 bits), SHA-1 hash, session key.

Ultimately I see the utility of NMAP for vulnerability detection, penetration testing, host/port discovery, the ability to remotely check OS and software version, and obtain hardware information. It’s a superb tool.