Dear John Henderson,

I hope you are doing well. I wanted to provide you with a detailed summary of the network investigation project I recently completed. Here’s a breakdown of the key findings:

1. Examination of Endpoints and IP Addresses:

* Utilized arp-Scan and nmap to identify devices on the network.
* Confirmed IP addresses of the discovered devices.

1. Open Ports on devices:

* Conducted nmap scans to identify open ports on specific devices.
* Recorded the open ports for each device.

1. Testing open port from Kali:

* Ran comprehensive nmap scans to identify open ports across all machines in the network.

1. Nmap scan for OS and Services Detection:

* Noted the detected OS and services for each device.

1. Network Traffic Analysis and ARP/MAC Capture:

* Captured network traffic using Wireshark during port testing.

Attached to this email are screenshots depicting each step of the process, including terminal commands, nmap scan outputs and Wireshark captures and table with all the collected data posted. I’ve also included a table of lists of the data for all devices discovered on the network.

Thank you for your time and consideration. Please let me know if you need and further information or insights.

Best regards,

Sabah diiriye

Network:172.16.14.0/24

Linux

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Open Port | Services | MAC | OS |
| 172.16.14.52 | 80,3389,9200 | http, ms-wbt-server xrdp, ssl/rtsp | 50:01:00:05:00:00 | Ubuntu 4.15-5.6 |

Winserver

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Open Port | Services | MAC | OS |
| 172.16.14.53 | 80,135,139,445,3389 | Http, msrpc, netbios-ssn, Microsoft-ads, ms-wbt-server | 50:01:00:01:15:00 | Microsoft Windows 10586-14393 |

Window 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Open Port | Services | MAC | OS |
| 172.16.14.54 | 135,139,445,3389,5357 | Ms-wbt-server,http,netbios-ssn,Microsoft -ds | 50:01:00:03:00:00 | Microsoft window 10 1507-1607 |

Kali

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Open Port | Services | MAC | OS |
| 172.16.14.51 | closed | N/A | N/A | N/A |

Window 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Open Port | Services | MAC | OS |
| 172.16.14.50 | 135,139,445,3389,5357 | Msrcp, netbios-ss, Microsoft-ad,Ms-wbt-server,wsdapi | 50:01:00:02:00:00 | Microsoft Window 10 1507-1607 |

Nmap scan 172……52

A computer screen shot of a program

Description automatically generated

Nmap scan 172……53

A computer screen shot of a program

Description automatically generated

Nmap scan 172……54

A computer screen shot of a program

Description automatically generated

Nmap scan 172……51

A computer screen with white text

Description automatically generated

Nmap scan 172……50

A screenshot of a computer program

Description automatically generated

Nmap scan entire map part1

A screenshot of a computer program

Description automatically generated

Nmap scan entire map part2

A screenshot of a computer

Description automatically generated

Capture network traffic Wireshark 172….50

A screenshot of a computer

Description automatically generated

Capture network traffic..Wireshark..172……51

A screenshot of a computer program

Description automatically generated

Capture network traffic… Wireshark….172…..52

A screenshot of a computer

Description automatically generated

Capture network traffic….Wireshark …172…..53

A screenshot of a computer

Description automatically generated

Capture network traffic… Wireshark….172……54

A screenshot of a computer

Description automatically generated

House, N. (2023, August 24). Nmap Cheat Sheet 2023: All the Commands, Flags & Switches. *StationX*. <https://www.stationx.net/nmap-cheat-sheet/>