Network Administration Project

Table of contents

Introduction 1

Methodology 1

Network Device Information 1

Machine Designation: Windows 2

1. nmap Scan 2

2. Process of Discovery 2

2.a. Port 135 – msrpc(Microsoft WindowsRPC) 2

2.b. Port 139 – netbios-ssn Microsoft Windows netbios-ssn 2

2.c Port 447 –microsoft-ds? 2

2.d. Port 3389 –ms-wbt-server Microsoft Terminal Services 3

2.e. Port 5357 – Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) 3

Machine Designation: Winserver 3

3. nmap Scan 3

4. Process of Discovery 4

4.a. Port 80(Microsoft IIS httpd): 4

4.b. Port 135 – msrpc(Microsoft WindowsRPC) 4

4.c Port 139 – netbios-ssn(Microsoft Windows netbios-ssn): 4

4.d. Port 445 –microsoft-ds: 4

4.e. Port 3389 –microsoft-ds: 4

4.f. Port 5357 – Microsoft HTTPAPI httpd 4

Machine Designation: Linux 5

5. nmapScan 5

6. Process of Discovery 5

6.a. Port 80 – syn ack Apache httpd 5

6.b. Port 3306 – MySQL 5

6.c. Port 3389 – Microsoft Terminal service 5

Machine Designation: Kali Linux 6

7. nmap Scan 6

8. Process of Discovery 6

Machine Designation: VPC 7

9. Nmap Scan 7

10. Process of Discovery 7

Wireshark Capture 7

Topography 8

Conclusion 9

references 9

# Introduction:

This report aims to provide an analysis of the network and documentation of devices.

**Tools used**: Zenmap and Wireshark.

I employed Zenmap for device identification on the network and Wireshark to capture and analyze the network traffic. The data gathered includes detailed information about each device from Zenmap scans, along with the packet level details.

# Methodology:

This report involves a systematic approach to gather, verify and document information about the devices within the network. The following steps outline the methodology used for this project.

* Turned on all the devices and tools.
* Identified all the devices using Zenmap scans and captured network packets using Wireshark to know the communication patterns.
* Physically accessed devices to double check the information obtained from Zenmap and Wireshark.
* Developed a topology diagram showing the network layout.

# Network Device information:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Machine Designation** | **Device Host Name** | **IP Address** | **MAC Address** | **Operating System, version** | **ARP Ping scan elapsed time** |
| Windows 1 | Desktop-WI N10PRO | 172.16.14. 50 | 50:01:00:02: 00:01 | MS Window 10.0.17763.107 | 0.26s |
| Winserver | WIN-SERVER-2022 | 172.16.14. 53 | 50:01:00:01: 00:01 | Microsoft Windows 2022 and 10.0.20348**.** | 0.20s |
| Linux | User-pc | 172.16.14. 52 | 50:01:00:05: 00:01 | Ubuntu Version 20.04.6 LTS | 0.19s |
| Kali Linux | Kali | 172.16.14. 51 | 50:01:00:07: 00:01 | KALI GNU/LINUX VERSION 6.1.0-Kali9-amd 64 | 0.19s |
| VPC | NA | 172.16.14. 101 | 00:50:79: 66:68:03 | NA | 0.17s |

**Machine Designation: Windows**

**1.Nmap Scans:**

A screenshot of a computer program

Description automatically generated

A table with text on it

Description automatically generated

**FIG:** The above two screenshots represent the scans with their open ports

**2.Process of Discovery:**

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device’s IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

**2.a Port 135 – msrpc(Microsoft WindowsRPC)**:

OSI Layer-4  
Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software. If you have remote users who VPN into your network, you might need to open this port on the firewall to allow access to the Exchange server.

**2.b Port 139 – netbios-ssn(Microsoft Windows netbios-ssn)**:

OSI layer 4

NetBIOS is a protocol used for file and print sharing under all current versions of Windows. While this is not a problem, the way that the protocol is implemented can be. There are a few vulnerabilities associated with leaving this port open.

**2.c Port 445 –microsoft-ds**:

OSI layer 7

TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. The SMB (Server Message Block) protocol is used for file sharing in Windows NT/2K/XP and later. In Windows NT it ran on top of NetBT (NetBIOS over TCP/IP, ports 137, 139 and 138/udp). In Windows 2K/XP and later, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra NetBT layer, for this they use TCP port 445.

**2.d Port 3389 –microsoft-ds**:

OSI layer 7

This port is vulnerable to Denial-of-Service attack against Windows NT Terminal Server. A remote attacker can quickly cause a server to reach full memory utilization by creating a large number of normal TCP connections to port 3389. Individual connections will timeout, but a low bandwidth  
continuous attack will maintain a terminal server at maximum memory utilization and prevent new connections from a legitimate source from taking place. Legitimate new connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection.

**2.e Port 5357:**

OSI layer 7

Used by Microsoft Network Discovery should be filtered for public networks. Disabling Network Discovery for any public network profile should close the port unless it's being used by another potentially malicious service.

To disable Network Discovery for a public profile, navigate to:

- Control Panel\Network and Internet\Network and Sharing Center\Advanced sharing settings

- disable Network Discovery for any public network

**Machine designation**: **Winserver**

3.Nmap Scans:

A computer screen shot of text

Description automatically generated

A screenshot of a computer program

Description automatically generated

**FIG:** The above two screenshots represent the Zenmap scans with their open ports

**4. Process of Discovery:**

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device’s IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

**4.a Port 80(Microsoft IIS httpd):**

OSI Layer-7

Hyper Text Transfer Protocol (HTTP) - port used for web traffic. Some broadband routers run a web server on port 80 or 8080 for remote management. WAN Administration can (and should, in most cases) be disabled using the Web Admin interface. Any Desk remote desktop software uses TCP ports 80, 443, 6568, 7070 (direct line connection)

**4.b Port 135 – msrpc(Microsoft WindowsRPC)**:

OSI Layer-4  
Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software. If you have remote users who VPN into your network, you might need to open this port on the firewall to allow access to the Exchange server.

**4.c Port 139 – netbios-ssn(Microsoft Windows netbios-ssn)**:

OSI layer 4

NetBIOS is a protocol used for file and print sharing under all current versions of Windows. While this is not a problem, the way that the protocol is implemented can be. There are a few vulnerabilities associated with leaving this port open.

**4.d Port 445 –microsoft-ds**:

OSI layer 7

TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. The SMB (Server Message Block) protocol is used for file sharing in Windows NT/2K/XP and later. In Windows NT it ran on top of NetBT (NetBIOS over TCP/IP, ports 137, 139 and 138/udp). In Windows 2K/XP and later, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra NetBT layer, for this they use TCP port 445.

**4.e Port 3389 –microsoft-ds**:

OSI layer 7

This port is vulnerable to Denial-of-Service attack against Windows NT Terminal Server. A remote attacker can quickly cause a server to reach full memory utilization by creating a large number of normal TCP connections to port 3389.

Individual connections will timeout, but a low bandwidth continuous attack will maintain a terminal server at maximum memory utilization and prevent new connections from a legitimate source from taking place. Legitimate new connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection.

**4.f Port 5357:**

OSI layer 7

Used by Microsoft Network Discovery should be filtered for public networks. Disabling Network Discovery for any public network profile should close the port unless it's being used by another potentially malicious service.

To disable Network Discovery for a public profile, navigate to:

- Control Panel\Network and Internet\Network and Sharing Center\Advanced sharing settings

- disable Network Discovery for any public network.

**Machine designation**: **Linux**

**5. Nmap Scan:**

A screenshot of a document

Description automatically generated

**FIG:** The above screenshot represents the Zenmap scans with their open ports

**6. Process of Discovery:**

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device’s IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

**6.a. Port 80 –(syn-ack Apache httpd):**

OSI Layer-7

Hyper Text Transfer Protocol (HTTP) - port used for web traffic. Some broadband routers run a web server on port 80 or 8080 for remote management. WAN Administration can (and should, in most cases) be disabled using the Web Admin interface. Any Desk remote desktop software uses TCP ports 80, 443, 6568, 7070 (direct line connection).

**6.b. Port 3306-MySQL)**:

OSI Layer-7

MySQL database server connections. MySQL 5.5.8, when running on Windows, allows remote attackers to cause a denial of service via a crafted packet to TCP port 3306.

**6.c. Port 3389 –(microsoft Terminal Service)**:

OSI Layer-7

This port is vulnerable to Denial-of-Service attack against Windows NT Terminal Server. A remote attacker can quickly cause a server to reach full memory utilization by creating a large number of normal TCP connections to port 3389.

Individual connections will timeout, but a low bandwidth continuous attack will maintain a terminal server at maximum memory utilization and prevent new connections from a legitimate source from taking place. Legitimate new connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection.

**Machine designation**: **Kalilinux**

**7. Nmap Scan:**

A screenshot of a computer

Description automatically generated

**FIG:** The above screenshot represents the Zenmap scans with their open ports

**8. Process of Discovery:**

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device’s IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

Unable to detect the operating system in Zenmap scans. But below attaching the screenshot of system information when checked externally.

A screenshot of a computer

Description automatically generated

**Machine designation**: **VPC**

**9. Nmap Scan:**

A document with text and numbers

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Fig: Zenmap scan on VPC.**

**10. Process of Discovery:**

For the VPC, I acquired a manual IP address in the terminal using the command “ip dhcp”. Subsequently, I conducted the Zenmap scan using that IP address. To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device’s IP address. In addition to the Zenmap scan, I initiated the packet capture in Wireshark by clicking on the start button. After collecting the required information, I stopped Wireshark from capturing packets.

**Wireshark Captures:**

I initiated packet capture by launching the Wireshark application, selecting the desired network interface. Utilized tools like Zenmap for network scanning and examined the results within Wireshark. Applied filters to pinpoint specific packets based on the port numbers. Analyzed the captured packets to assess network activity and gather information.

A screenshot of a computer

Description automatically generated

The above provided screenshot represents a sequence of packet captures.

# 10. Topography:

A screenshot of a computer

Description automatically generated

**Topology Representation collected from Zenmap.**

In our network topology, we have implemented VLANs to enhance our overall network performance and security. It allows us to logically segment our network into distinct domains, each with its own VLAN ID and associated network devices.

# Conclusion:

# In conclusion, strengthening network security involves the implementation of VLANs as they serve to isolate various types of traffic, providing a mechanism to restrict unauthorized access effectively.

# References:

Port 80, Details. n.d.SpeedGuide. <https://www.speedguide.net/port.php?port=80>

Port 139, Details. n.d.SpeedGuide. <https://www.speedguide.net/port.php?port=139>

Port 135, Details. n.d.SpeedGuide. <https://www.speedguide.net/port.php?port=135>

Port 445, Details. n.d.SpeedGuide. <https://www.speedguide.net/port.php?port=445>

Port 3389, Details. n.d.SpeedGuide. <https://www.speedguide.net/port.php?port=3389>

Port 3306, Details. n.d.SpeedGuide. <https://www.speedguide.net/port.php?port=3389>

Port 5357, Details. n.d.SpeedGuide. <https://www.speedguide.net/port.php?port=5357>

**Zenmap** version 7.94, developed by Nmap Software LLC. <https://nmap.org/zenmap/)>

**Wireshark** Version 4.2.2(v4.2.2-0-g404592842786), developed by Gerald Combs and contributors. <https://www.wireshark.org/>

Linux command cheat sheet <https://phoenixnap.com/kb/linux-commands-cheat-sheet>