Port Scanning Report

Introduction

This report outlines the methodology and findings from a port scanning activity conducted as part of a cybersecurity internship project. The primary objective was to identify open ports on a target system, understand the services running on these ports, assess potential security risks, and recommend mitigation strategies.

Tools Utilized

- **Port Scanning Tool**: Nmap
- **Operating System**: Windows 10

Methodology

1. Scanning All TCP Ports

To perform a comprehensive scan of all 65,535 TCP ports on the target system, the following Nmap command was executed:

```
nmap -p- 192.168.xxx.x
```

Explanation of the command:

- `nmap`: Invokes the Nmap tool.
- `-p-`: Instructs Nmap to scan all 65,535 TCP ports.
- `192.168.135.1`: Specifies the target IP address.
- This command provides a complete overview of all open TCP ports on the target system.

2. Service and Version Detection

After identifying open ports, a more detailed scan was conducted to determine the services running on these ports and their versions:

```
nmap -sV -p 135,902,912 192.168.135.1
```

Explanation of the command:

- `-sV`: Enables service and version detection.
- `-p 135,902,912`: Specifies the ports to scan.
- `192.168.135.1`: Specifies the target IP address.
- This scan provides detailed information about the services running on the specified ports.

Scan Results

The scans revealed the following open ports and associated services:

Port	Protocol	Service	Description
135	TCP	MSRPC	Microsoft Remote Procedure Call Endpoint Mapper. Learn more
902	TCP	ISS RealSecure / VMware	Used by VMware vSphere for ESXi host management and ISS RealSecure Sensor. Learn more
912	TCP	APEX Mesh / VMware Authentication Daemon	APEX relay-relay service; also associated with VMware Authentication Daemon. Learn more

🔍 Analysis & Security Implications

Port 135 – MSRPC

- **Purpose**: Facilitates communication between applications across a network using Microsoft's Remote Procedure Call (RPC) protocol.
- **Security Considerations**:
  - **Vulnerabilities**: Known to be exploited in attacks like Blaster Worm and WannaCry.
  - **Exposure Risks**: Can be used by attackers to execute remote commands or escalate privileges.
- **Recommendations**:
  - Restrict access to port 135 using firewalls.
  - Disable RPC services if not required.
  - Regularly update Windows systems to patch known vulnerabilities.

Port 902 – ISS RealSecure / VMware

- **Purpose**: Used by VMware vSphere for ESXi host management and by ISS RealSecure Sensor.
- **Security Considerations**:
  - **Unauthorized Access**: Open port can allow unauthorized access to VMware services.
  - **Brute-force Attacks**: Potential for attackers to attempt credential guessing.
- **Recommendations**:
  - Restrict access to trusted IP addresses.
  - Implement strong authentication mechanisms.
  - Regularly update VMware products to patch known vulnerabilities.Wikipedia

Port 912 – APEX Mesh / VMware Authentication Daemon

- **Purpose**: APEX relay-relay service; also associated with VMware Authentication Daemon.
- **Security Considerations**:
  - **Denial of Service (DoS)**: Vulnerabilities can be exploited to crash services.
  - **Unauthorized Access**: Potential for attackers to gain unauthorized access or execute commands.

- **Recommendations**:
    - Restrict access to port 912 using firewalls.
    - Disable the service if not required.
    - Regularly update associated software to patch known vulnerabilities.

☑ Recommendations Summary

- **MSRPC (Port 135)**:
    - Restrict access using firewalls.
    - Disable RPC services if not needed.
    - Keep Windows systems updated.
- **ISS RealSecure / VMware (Port 902)**:
    - Limit access to trusted IPs.
    - Use strong authentication.
    - Update VMware products regularly.
- **APEX Mesh / VMware Authentication Daemon (Port 912)**:
    - Restrict access using firewalls.
    - Disable service if unnecessary.
    - Keep associated software updated.