Vulnerability Scanning and Reporting Project

Date: 5/09/2024

Author: Yonase Kidane

Introduction

The objective of this project was to identify potential security vulnerabilities on my system using Nmap, a popular network scanning tool. The focus was on detecting open ports that could expose the system to external threats. After identifying these vulnerabilities, necessary measures were taken to secure the system, and the results were documented.

Tools Used

- **Vulnerability Scanner:** Nmap
- **Operating System:** Windows 10

Scan Results

Initial Scan Findings

The initial Nmap scan revealed several open ports that could potentially expose the system to security risks:

- **Port 25 (SMTP):** Filtered
- **Port 135 (MSRPC):** Open
- **Port 139 (NetBIOS):** Open
- **Port 445 (SMB):** Open
- **Port 2869 (ICS/LAN):** Open
- **Port 5357 (WSDAPI):** Open

These ports were associated with various services, including Microsoft networking services, file sharing, and device communication.

Actions Taken

To secure the system, the following actions were taken:

1. **Disabled Services:**
    - **UPnP Device Host:** Disabled to block ports 2869 and 5357.
    - **Function Discovery Resource Publication:** Disabled to block ports related to device discovery.
    - **Server Service:** Disabled to block SMB file sharing on port 445.
2. **Firewall Configuration:**
    - **Port 25 (SMTP):** Ensured that the firewall was configured to filter this port, preventing any unauthorized email services.

Final Scan Results

After taking the necessary actions, a second Nmap scan was conducted to verify the changes. The results were as follows:

- **Port 25 (SMTP):** Filtered (blocked by firewall)
- **Port 445 (SMB):** Closed
- **Port 2869 (ICS/LAN):** Closed
- **Port 5357 (WSDAPI):** Closed

These results confirmed that the previously open ports had been successfully secured.

Detailed Analysis

Port 25 (SMTP):

- **Status:** Filtered
- **Action Taken:** Firewall configured to block this port, preventing any SMTP services from running.
- **Justification:** As no local email server is in use, this port was unnecessary and posed a potential security risk.

Port 445 (SMB):

- **Status:** Closed
- **Action Taken:** Disabled the Server service to block this port, preventing file sharing.

- **Justification:** File sharing services are not used on this machine, so the port was closed to reduce attack vectors.

Port 2869 (ICS/LAN):

- **Status:** Closed
- **Action Taken:** Disabled the UPnP Device Host service.
- **Justification:** UPnP services are not needed, and disabling this service enhances security by closing the associated ports.

Port 5357 (WSDAPI):

- **Status:** Closed
- **Action Taken:** Disabled the Function Discovery Resource Publication service.
- **Justification:** Network device discovery services were not necessary, so disabling this service helped secure the system.

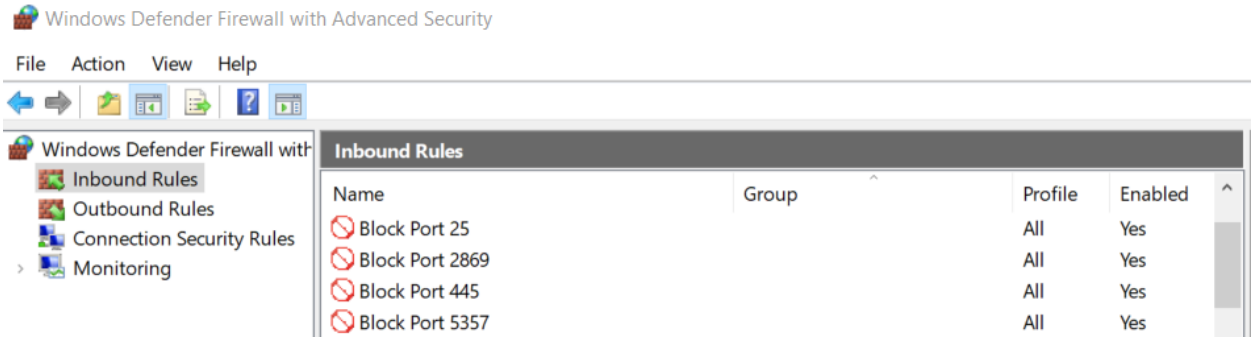
Conclusion

By identifying and securing open ports, the system's attack surface was significantly reduced. The final Nmap scan confirmed that all critical ports are either filtered or closed, and no additional vulnerabilities were found. It is recommended to continue regular vulnerability scans and monitor the system to maintain security.

Screenshots

```
C:\Users\yk>nmap --script vuln 192.168.1.107
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-04 21:58 AUS Eastern Standard Time
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.107
Host is up (0.0018s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
587/tcp  filtered submission
2869/tcp open     icslap
5357/tcp open     wsdapi
6666/tcp filtered irc
6667/tcp filtered irc
6668/tcp filtered irc
6669/tcp filtered irc

Host script results:
```

```
C:\WINDOWS\system32>nmap -p 25,445,2869,5357 192.168.1.107
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-05 22:04 AUS Eastern Standard Time
Nmap scan report for 192.168.1.107
Host is up (0.0010s latency).

PORT     STATE    SERVICE
25/tcp   filtered smtp
445/tcp  closed   microsoft-ds
2869/tcp closed   icslap
5357/tcp closed   wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds

C:\WINDOWS\system32>
```



Recommendations

- **Ongoing Monitoring:** Regularly scan the system for vulnerabilities.
- **Security Updates:** Ensure that the system and software are kept up to date with security patches.
- **Review Configurations:** Periodically review firewall and service configurations to ensure that no unnecessary ports are left open.