Home Lab: Network Reconnaissance & Port Scan Detection / Johnathan Campbell

Environment: VirtualBox (Windows 10 + Ubuntu)
Date: January 2026
Tools Used: Nmap, Windows Defender Firewall

1. Objective

This lab's goals were to identify exposed services, evaluate security risks, simulate attacker reconnaissance activity against a Windows 10 host, and apply system hardening techniques to minimize attack surface.

2. Lab Environment

Component	Description
Attacker Machine	Ubuntu Linux VM
Target Machine	Windows 10 VM
Network	VirtualBox internal network
Scanning Tool	Nmap

An attacker conducting network reconnaissance against the Windows 10 host was simulated using the Ubuntu virtual machine.

3. Initial Configuration

In order to replicate a realistic enterprise setup, the Windows 10 system was configured with file sharing and network discovery enabled. To expose SMB services, Windows Defender Firewall inbound rules for file and printer sharing were temporarily activated.

4. Reconnaissance Phase

Command Executed:

sudo nmap -sS -sV -T4 192.168.1.3

Scan Results:

```
jzlc@SOC101-Ubuntu:~/Desktop$ sudo nmap -sS -sV -T4 192.168.1.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-20 13:36 CST
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:72:B4:32 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.41 seconds
jzlc@SOC101-Ubuntu:~/Desktop$ sudo nmap -sS -sV -T4 192.168.1.3
```

Analysis:

- NetBIOS port 139 was open.
- SMB port 445 was open.
- Microsoft file sharing services were found through service detection.
- The host confirmed exposure by responding to the SYN scan.

5. Security Risk Assessment

Port 445 (SMB):

- frequently used for lateral movement.
- Ransomware campaigns often target this group.
- can reveal authentication methods and file shares.

Port 139 (NetBIOS):

- Legacy protocol used for network name resolution.
- Can enable system enumeration and credential harvesting.

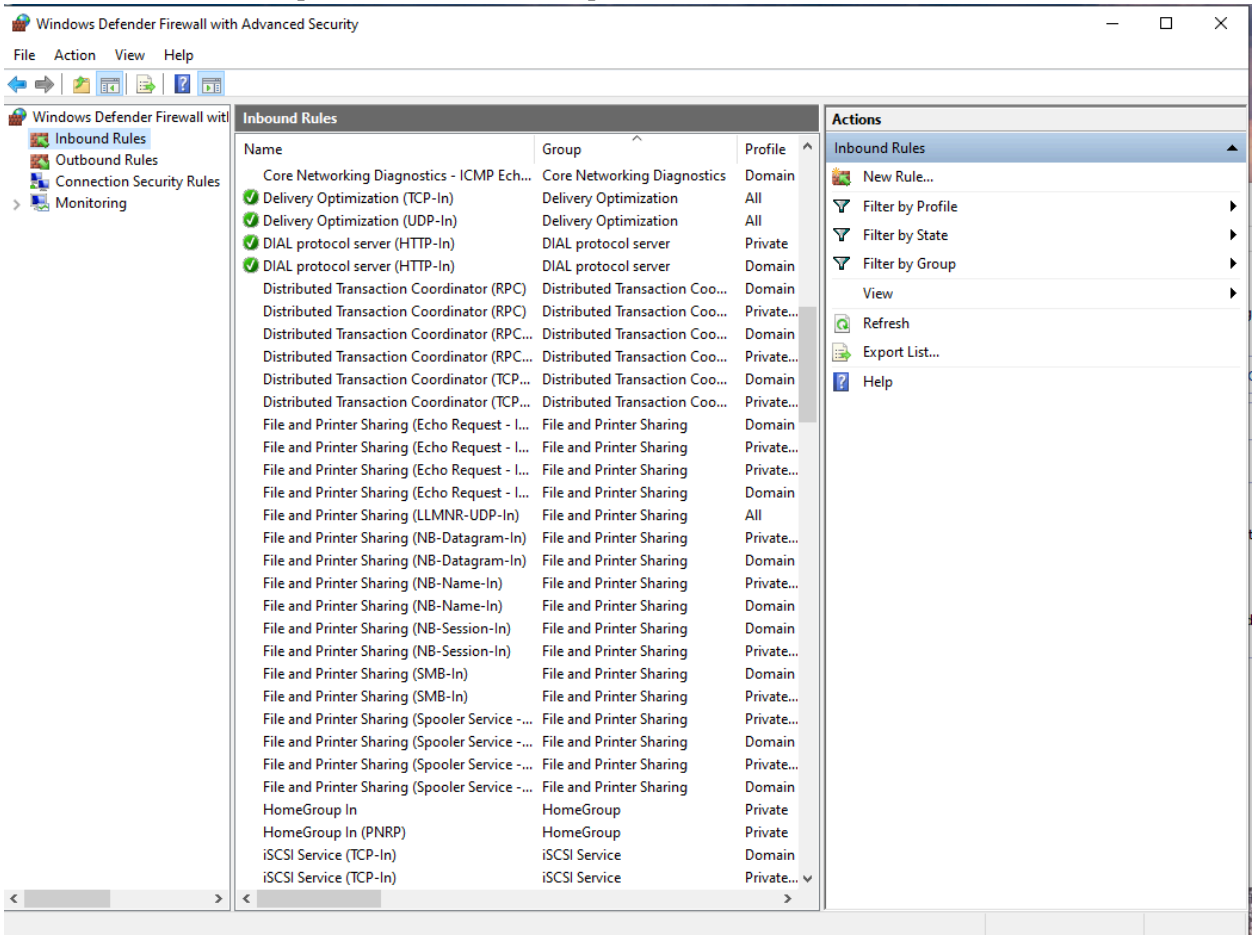
Risk Level:

Depending on the authentication setup and network segmentation, moderate to high.

6. Remediation Actions

The following defensive measures were implemented:

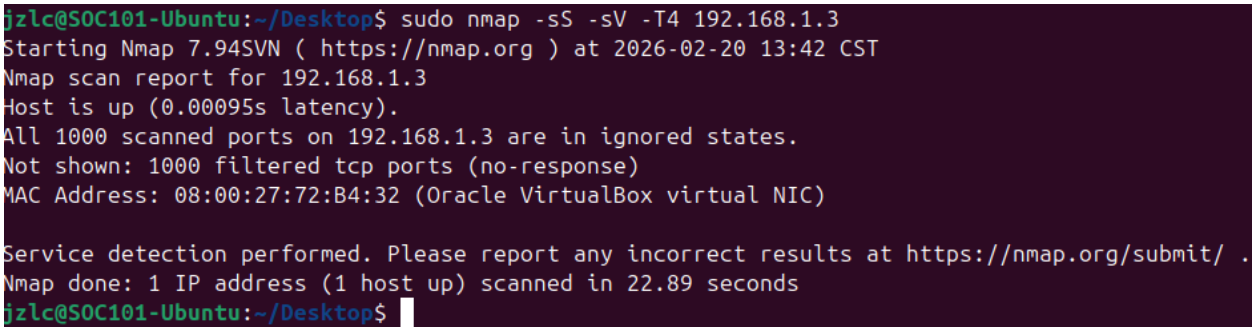
1. "File and Printer Sharing" inbound firewall rules have been disabled.
2. In the advanced sharing settings, network discovery and file sharing were disabled.
3. confirmed the implementation of firewall policies.



7. Validation Phase

Re-Scan Command:

sudo nmap -sS -sV -T4 192.168.1.3



Analysis:

- Previously open SMB and NetBIOS services were no longer externally accessible.
- Attack surface was successfully reduced.
- Firewall properly filtered inbound scan attempts.

8. Conclusion

This lab successfully demonstrated:

- Attacker-style reconnaissance using Nmap
- Identification of exposed Windows services
- Security risk evaluation of SMB exposure
- System hardening through firewall configuration
- Validation of remediation via re-scanning

The exercise reinforced the importance of minimizing unnecessary service exposure to reduce attack surface and prevent lateral movement opportunities within enterprise environments.