Home Lab: Packet Capture & Traffic Investigation / Johnathan Campbell

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

1. Objective

Finding exposed services, assessing security threats, simulating attacker reconnaissance against a Windows 10 host, and using system hardening techniques to reduce attack surface were the objectives of this lab.

2. Lab Environment

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

An external attacker conducting reconnaissance against the Windows 10 host was mimicked by the Ubuntu machine.

3. Reconnaissance Activity

Command Executed:

sudo nmap -sS -sV -T4 192.168.1.3

```
jzlc@SOC101-Ubuntu:~$ sudo nmap -sS -sV -T4 192.168.1.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-22 01:13 CST
Nmap scan report for 192.168.1.3
Host is up (0.0034s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
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 11.64 seconds
jzlc@SOC101-Ubuntu:~$
```

Scan Results Identified:

- 80/tcp open – Microsoft IIS httpd 10.0
- 139/tcp open – netbios-ssn
- 445/tcp open – microsoft-ds

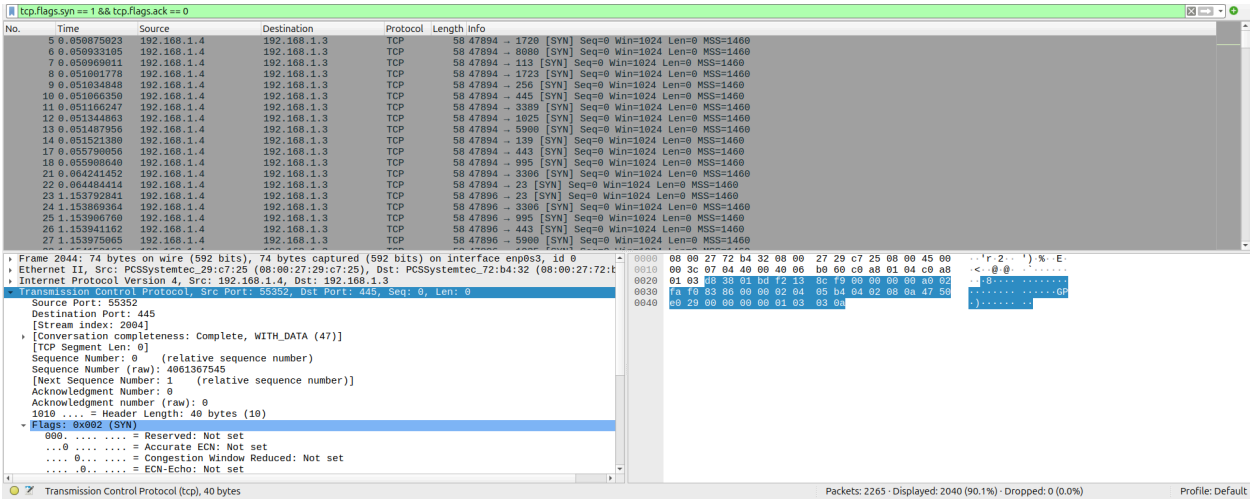
These findings validated that the target host's web and SMB services were accessible.

4. Packet-Level Analysis

4.1 SYN Scan Detection

Wireshark filtering:

tcp.flags.syn == 1 && tcp.flags.ack == 0



Observed Behavior:

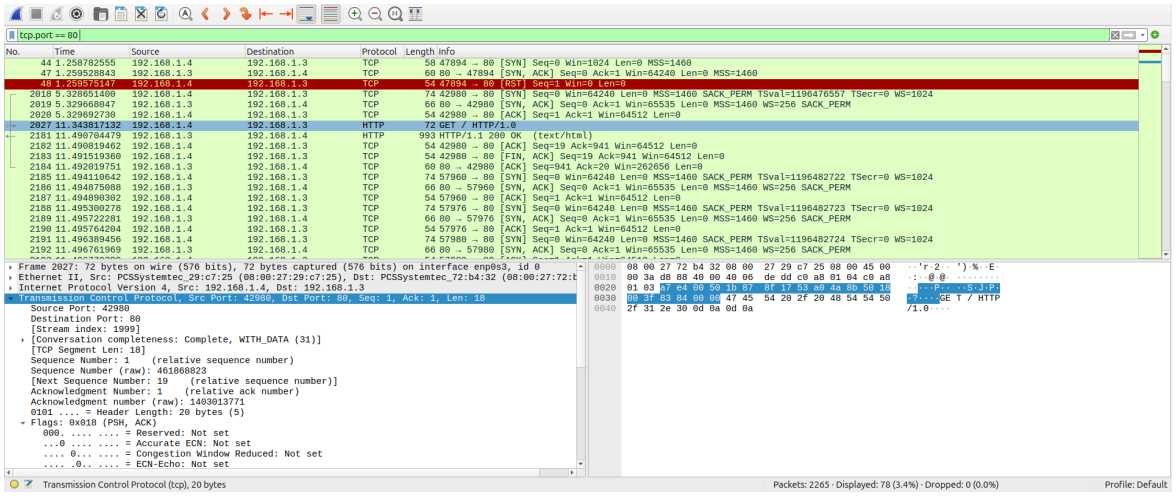
- SYN packets coming from the Ubuntu host in large quantities
- Targeting sequential destination ports
- Quick packet timing
- TCP handshakes that are incomplete (SYN --- RST)

This pattern is consistent with Nmap SYN reconnaissance scanning.

4.2 HTTP Service Interaction (Port 80)

Wireshark filtering:

tcp.port == 80



Observed Behavior:

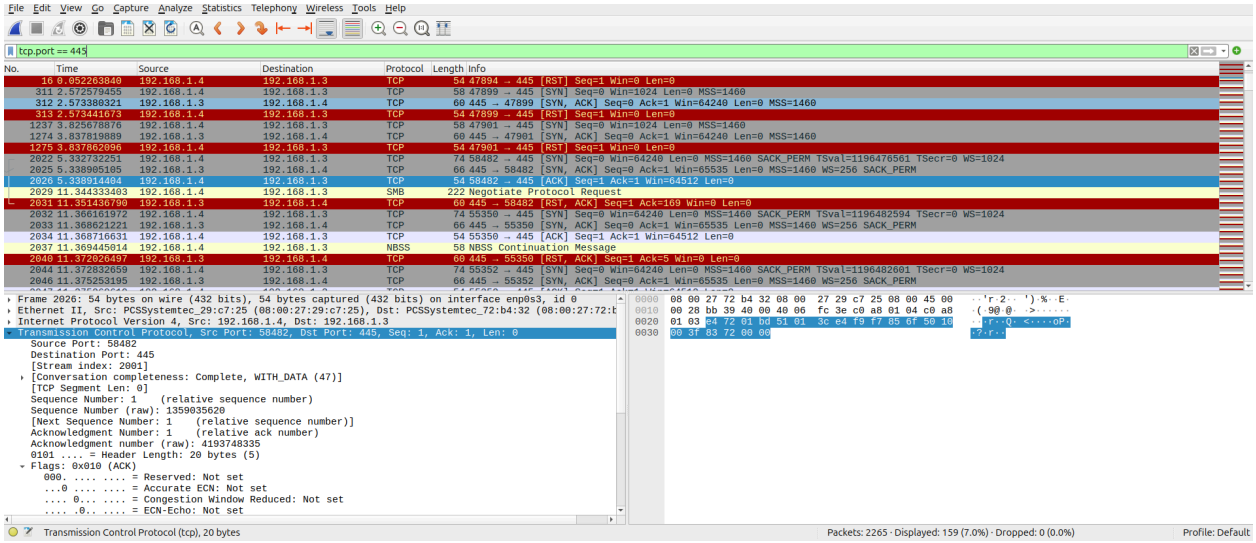
- Full TCP three-way handshake
- HTTP GET request observed
- Server response from Microsoft IIS

This verified successful session establishment and active web service exposure.

4.3 SMB Negotiation (Port 445)

Wireshark filtering:

tcp.port == 445



Observed Behavior:

- SMB negotiation protocol packets
- NBSS session setup attempts
- TCP handshake completion

This demonstrated that SMB file-sharing services could be reached and were reacting to attempts at enumeration.

5. Indicators of Reconnaissance

The following indicators were identified:

- Rapid SYN packet bursts targeting multiple ports
- Repeated connection attempts across common Windows service ports
- Incomplete TCP handshakes indicative of stealth scanning
- Service version detection behavior

These behaviors align with early-stage attacker reconnaissance.

6. Security Risk Assessment

Port 80 (HTTP)

- Web application exposure
- Potential attack vectors: misconfiguration, outdated services, exploitation

Port 445 (SMB)

- Lateral movement risk
- Credential harvesting potential
- Ransomware propagation vector

Port 139 (NetBIOS)

- Legacy protocol exposure
- System enumeration and information disclosure risk

7. Conclusion

This lab demonstrated the ability to:

- Capture live reconnaissance traffic
- Identify SYN scan behavior
- Analyze full TCP handshakes
- Observe SMB negotiation attempts
- Correlate Nmap scan results with packet-level evidence

The exercise reinforced practical understanding of how reconnaissance activity appears at the network layer and how exposed services increase system attack surface.