

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

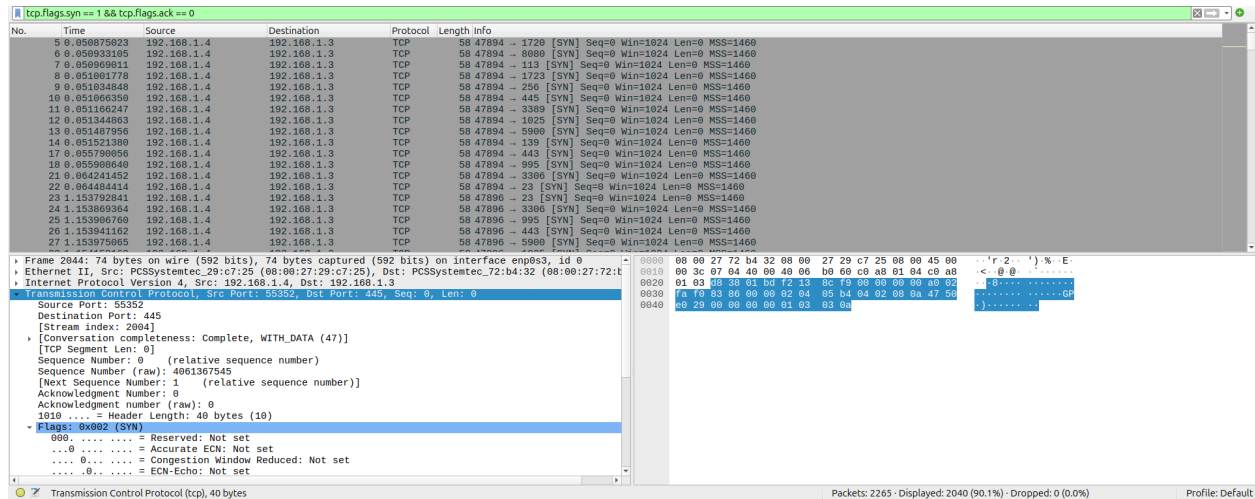
These findings validated that the target host's web and SMB services were accessible.

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`

The image shows a Wireshark packet capture on interface em0/3, filtered for 'tcp.port == 80'. The capture shows a successful TCP three-way handshake and an HTTP GET request. The first three packets are the handshake: a SYN from 192.168.1.4 to 192.168.1.3, an ACK from 192.168.1.3 to 192.168.1.4, and a SYN-ACK from 192.168.1.3 to 192.168.1.4. The fourth packet is an HTTP GET request from 192.168.1.4 to 192.168.1.3. The packet details pane shows the TCP segment length as 18 bytes, and the HTTP request line as 'GET / HTTP/1.1'. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
44	1.250782555	192.168.1.4	192.168.1.3	TCP	60	47894 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47	1.250928843	192.168.1.3	192.168.1.4	TCP	60	80 → 47894 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
48	1.250975147	192.168.1.4	192.168.1.3	TCP	54	47894 → 80 [ACK] Seq=1 Win=0 Len=0
2010	5.329053494	192.168.1.3	192.168.1.4	TCP	74	82000 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM TSval=1196470557 TSecr=0 WS=1024
2019	5.329668847	192.168.1.3	192.168.1.4	TCP	60	80 → 42980 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2020	5.329692736	192.168.1.4	192.168.1.3	TCP	54	42980 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0
2027	11.349867132	192.168.1.4	192.168.1.3	HTTP	72	GET / HTTP/1.1

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

The image shows a Wireshark packet capture on interface em0/3, filtered for 'tcp.port == 445'. The capture shows SMB negotiation protocol packets. The first three packets are the handshake: a SYN from 192.168.1.4 to 192.168.1.3, an ACK from 192.168.1.3 to 192.168.1.4, and a SYN-ACK from 192.168.1.3 to 192.168.1.4. The fourth packet is an SMB Negotiate Protocol Request from 192.168.1.4 to 192.168.1.3. The packet details pane shows the TCP segment length as 0 bytes, and the SMB Negotiate Protocol Request details. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.052203840	192.168.1.4	192.168.1.3	TCP	54	47894 → 445 [RST] Seq=1 Win=0 Len=0
312	2.573389321	192.168.1.3	192.168.1.4	TCP	60	445 → 47899 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
313	2.573441673	192.168.1.4	192.168.1.3	TCP	54	47899 → 445 [RST] Seq=1 Win=0 Len=0
1237	3.825678876	192.168.1.4	192.168.1.3	TCP	54	47901 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1274	3.837618689	192.168.1.3	192.168.1.4	TCP	60	445 → 47901 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1276	3.837662096	192.168.1.4	192.168.1.3	TCP	54	47901 → 445 [RST] Seq=1 Win=0 Len=0
2022	5.332732251	192.168.1.4	192.168.1.3	TCP	74	58482 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1196470561 TSecr=0 WS=1024
2025	5.338903495	192.168.1.3	192.168.1.4	TCP	60	445 → 58482 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2026	5.338914484	192.168.1.4	192.168.1.3	TCP	54	58482 → 445 [ACK] Seq=1 Ack=1 Win=64512 Len=0
2029	11.344333483	192.168.1.4	192.168.1.3	SMB	222	Negotiate Protocol Request

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.