



TAREA 07

**CONFIGURACIÓN DE
DISPOSITIVOS Y
SISTEMAS
INFORMÁTICOS II**

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

Desde hace unos días no paramos de recibir incidentes de seguridad en el SOC. Tenemos 2 incidentes nuevos que resolver. Uno relacionado con una denegación de servicio distribuido y otro relacionado con un ataque a la web de la compañía.

Nos han enviado la información recopilada en el análisis del incidente de DDoS (Denegación de Servicio Distribuida). Tenemos que ordenar la información para buscar desde qué [ISPs](#) viene el ataque para informar a nuestro SOC, y pueda tomar las acciones oportunas con los ISP de país sobre las IPs detectadas, y pueda cortar el ataque desde el origen (fichero - [datos conexiones](#)).

Con esta información, además podremos aplicar las contramedidas necesarias y disminuir el impacto del ataque.

Para realizar el ataque puede utilizar comandos de Linux con una máquina Linux o instalando [Cygwin](#) en una máquina Windows: cat, grep, head, tail, sort, cut, awk, netcat o automatizarlo con python.

El ataque se ha producido por UDP y los campos relativos a los logs recibidos tienen el siguiente formato:

Columna	Descripción
1	Fecha
2	Hora
3	Duración
4	Protocolo
5	IP:puerto origen
6	->
7	IP:puerto destino
8	Nº paquetes transmitidos
9	Nº bytes transmitidos
10	Número de flujo

Necesitamos:

- Tener un listado de IPs únicas
- Su geolocalización con un servicio de [whois](#)

Relativo al ataque web, debemos identificar ([fichero logs.zip](#)):

- Las herramientas ofensivas utilizadas por los atacantes
- Las páginas web sobre las que han realizado el ataque
- Usuarios utilizados en cada uno de los servicios atacados
- Ficheros descargados

Para estas tareas se proporcionarán ficheros de registros (logs) de los que es necesario extraer la información al que se ha hecho referencia anteriormente

Incidente de denegación de servicio distribuido

Nos han enviado la información recopilada en el análisis del incidente de DDoS (Denegación de Servicio Distribuida). Tenemos que ordenar la información para buscar desde qué [ISPs](#) viene el ataque para informar a nuestro SOC, y pueda tomar las acciones oportunas con los ISP de país sobre las IPs detectadas, y pueda cortar el ataque desde el origen (fichero - [datos conexiones](#)).

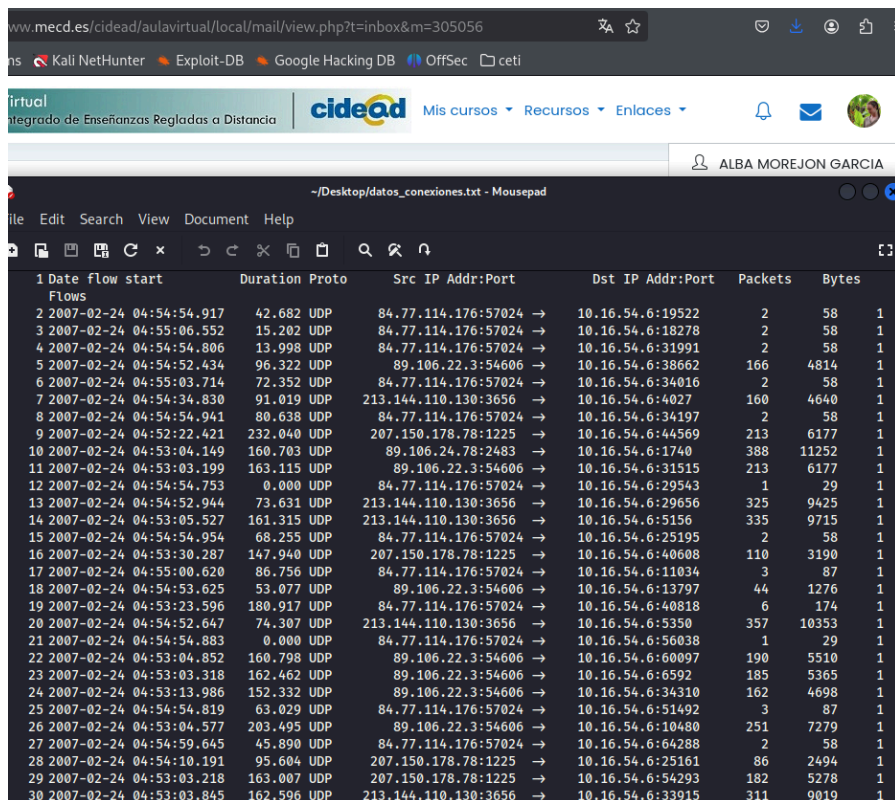
Con esta información, además podremos aplicar las contramedidas necesarias y disminuir el impacto del ataque.

Para realizar el ataque puede utilizar comandos de Linux con una máquina Linux o instalando [Cygwin](#) en una máquina Windows: cat, grep, head, tail, sort, cut, awk, netcat o automatizarlo con python.

Necesitamos:

- Tener un listado de IPs únicas
- Su geolocalización con un servicio de [whois](#)

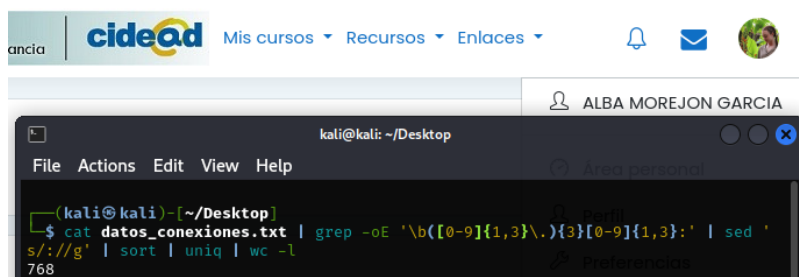
Empezamos copiando la información de datos_conexiones a un fichero .txt con el mismo nombre para poder analizarlo mejor.



1	Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes
2	2007-02-24 04:54:54.917	42.682	UDP	84.77.114.176:57024 →	10.16.54.6:19522	2	58 1
3	2007-02-24 04:55:06.552	15.202	UDP	84.77.114.176:57024 →	10.16.54.6:18278	2	58 1
4	2007-02-24 04:54:54.806	13.998	UDP	84.77.114.176:57024 →	10.16.54.6:31991	2	58 1
5	2007-02-24 04:54:52.434	96.322	UDP	89.106.22.3:54606 →	10.16.54.6:38662	166	4814 1
6	2007-02-24 04:55:03.714	72.352	UDP	84.77.114.176:57024 →	10.16.54.6:34016	2	58 1
7	2007-02-24 04:54:34.830	91.019	UDP	213.144.110.130:3656 →	10.16.54.6:4027	160	4640 1
8	2007-02-24 04:54:54.941	80.638	UDP	84.77.114.176:57024 →	10.16.54.6:34197	2	58 1
9	2007-02-24 04:52:22.421	232.040	UDP	207.150.178.78:1225 →	10.16.54.6:44569	213	6177 1
10	2007-02-24 04:53:04.149	160.703	UDP	89.106.24.78:2483 →	10.16.54.6:1740	388	11252 1
11	2007-02-24 04:53:03.199	163.115	UDP	89.106.22.3:54606 →	10.16.54.6:31515	213	6177 1
12	2007-02-24 04:54:54.753	0.000	UDP	84.77.114.176:57024 →	10.16.54.6:29543	1	29 1
13	2007-02-24 04:54:52.944	73.631	UDP	213.144.110.130:3656 →	10.16.54.6:29656	325	9425 1
14	2007-02-24 04:53:05.527	161.315	UDP	213.144.110.130:3656 →	10.16.54.6:5156	335	9715 1
15	2007-02-24 04:54:54.954	68.255	UDP	84.77.114.176:57024 →	10.16.54.6:25195	2	58 1
16	2007-02-24 04:53:30.287	147.940	UDP	207.150.178.78:1225 →	10.16.54.6:40608	110	3190 1
17	2007-02-24 04:55:00.620	86.756	UDP	84.77.114.176:57024 →	10.16.54.6:11034	3	87 1
18	2007-02-24 04:54:53.625	53.077	UDP	89.106.22.3:54606 →	10.16.54.6:13797	44	1276 1
19	2007-02-24 04:53:23.596	180.917	UDP	84.77.114.176:57024 →	10.16.54.6:40818	6	174 1
20	2007-02-24 04:54:52.647	74.307	UDP	213.144.110.130:3656 →	10.16.54.6:5350	357	10353 1
21	2007-02-24 04:54:54.883	0.000	UDP	84.77.114.176:57024 →	10.16.54.6:56038	1	29 1
22	2007-02-24 04:53:04.852	160.798	UDP	89.106.22.3:54606 →	10.16.54.6:60097	190	5510 1
23	2007-02-24 04:53:03.318	162.462	UDP	89.106.22.3:54606 →	10.16.54.6:6592	185	5365 1
24	2007-02-24 04:53:13.986	152.332	UDP	89.106.22.3:54606 →	10.16.54.6:34310	162	4698 1
25	2007-02-24 04:54:54.819	63.029	UDP	84.77.114.176:57024 →	10.16.54.6:51492	3	87 1
26	2007-02-24 04:53:04.577	203.495	UDP	89.106.22.3:54606 →	10.16.54.6:10480	251	7279 1
27	2007-02-24 04:54:59.645	45.890	UDP	84.77.114.176:57024 →	10.16.54.6:64288	2	58 1
28	2007-02-24 04:54:10.191	95.604	UDP	207.150.178.78:1225 →	10.16.54.6:25161	86	2494 1
29	2007-02-24 04:53:03.218	163.007	UDP	207.150.178.78:1225 →	10.16.54.6:54293	182	5278 1
30	2007-02-24 04:53:03.845	162.596	UDP	213.144.110.130:3656 →	10.16.54.6:33915	311	9019 1

A continuación vamos a mostrar (`wc -l`) cuántos registros hay en el archivo datos_conexion.txt, buscando por ips (`grep -oE 'b([0-9]{1,3}\.){3}[0-9]{1,3}:'`) únicas (`uniq`).

`"cat datos_conexiones.txt | grep -oE 'b([0-9]{1,3}\.){3}[0-9]{1,3}:' | sed 's://g' | sort | uniq | wc -l"`

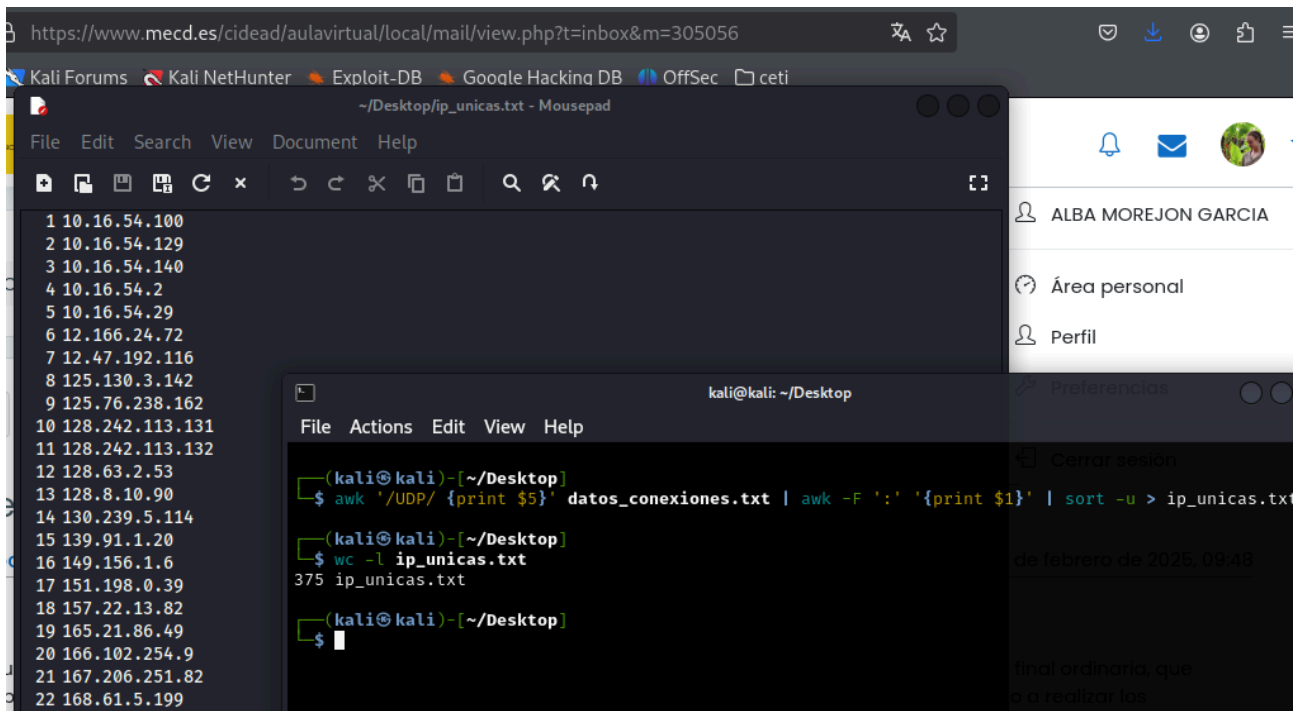


```
kali@kali: ~/Desktop
File Actions Edit View Help
$ cat datos_conexiones.txt | grep -oE 'b([0-9]{1,3}\.){3}[0-9]{1,3}:' | sed 's://g' | sort | uniq | wc -l
768
```

A continuación, filtramos las líneas que contengan el protocolo UDP (`awk '/UDP/ {print $5}'`), mostramos sólo la columna que muestra las ips (`awk -F ':' '{print $1}'`), las ordenamos de menor a mayor y eliminamos los duplicados (`sort -u`) para que solo salga una vez cada ip.

Y mostramos el número de registros (`wc -l`) que tiene el archivo con el filtrado que acabamos de hacer.

`"awk '/UDP/ {print $5}' datos_conexiones.txt | awk -F ':' '{print $1}' | sort -u > ip_unicas.txt"`



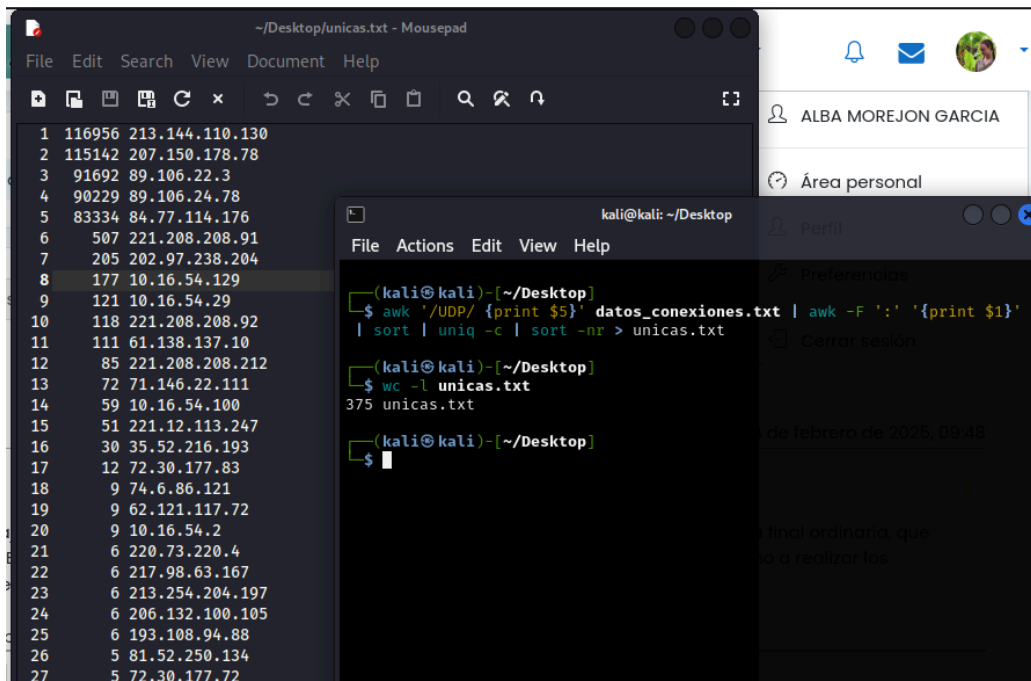
```
(kali@kali)-[~/Desktop]
$ awk '/UDP/ {print $5}' datos_conexiones.txt | awk -F ':' '{print $1}' | sort -u > ip_unicas.txt

(kali@kali)-[~/Desktop]
$ wc -l ip_unicas.txt
375 ip_unicas.txt

(kali@kali)-[~/Desktop]
$
```

Ahora podemos ordenar las ips del anterior documento por el número de veces que aparecen en el fichero de las conexiones (`sort -nr`) para saber desde que ips se ha intentado hacer más número de conexiones.

`"awk '/UDP/ {print $5}' datos_conexiones.txt | awk -F ':' '{print $1}' | sort -u | uniq -c | sort -nr > unicas.txt"`



```
(kali@kali)-[~/Desktop]
$ awk '/UDP/ {print $5}' datos_conexiones.txt | awk -F ':' '{print $1}' | sort -u | uniq -c | sort -nr > unicas.txt

(kali@kali)-[~/Desktop]
$ wc -l unicas.txt
375 unicas.txt

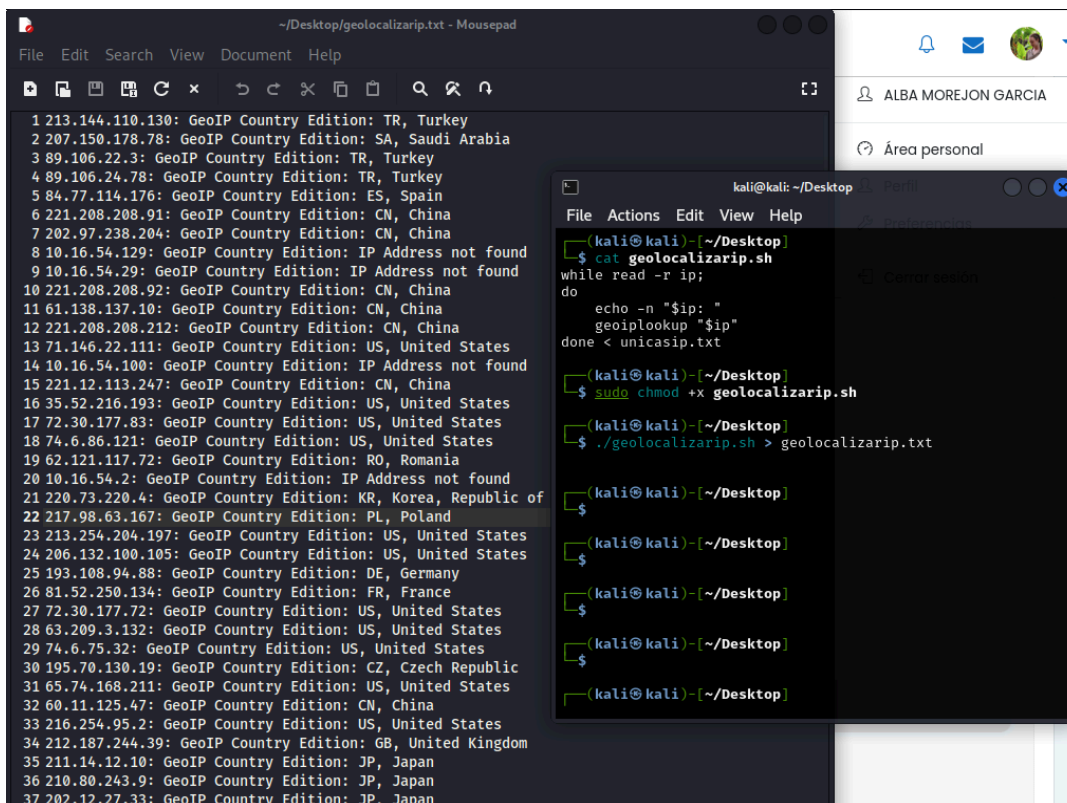
(kali@kali)-[~/Desktop]
$
```

Con un script vamos a mostrar a qué país pertenece cada ip, para poder localizar de qué proveedor de servicios de internet proviene el ataque y poder tomar las acciones oportunas.

Hemos elegido el documento que tiene las ips ordenadas por número de conexión. Desde los países que más conexiones se han hecho son: Turquía, China y Estados Unidos. Algunas ips no han podido ser localizadas porque pertenecen al rango 10.16.0.0/24 que coincide con la red interna.

El script utilizado, localiza las ips con el comando “geolookup”:

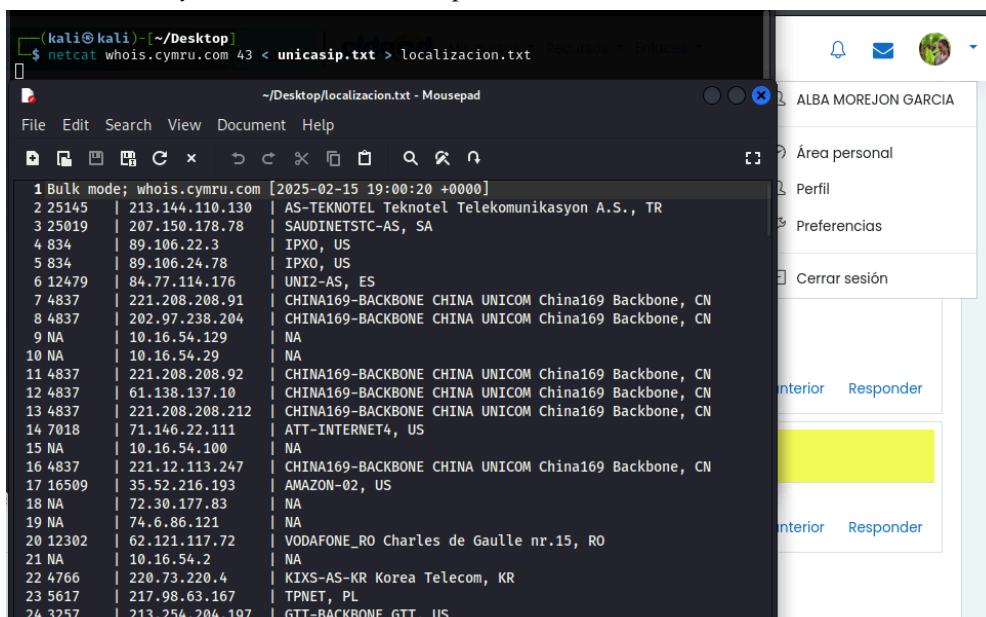
```
while read -r ip;
do
    echo -n "$ip: "
    geoipllookup "$ip"
done < unicasip.txt
```



```
~/Desktop/geolocalizarip.txt - Mousepad
File Edit Search View Document Help
1 213.144.110.130: GeoIP Country Edition: TR, Turkey
2 207.150.178.78: GeoIP Country Edition: SA, Saudi Arabia
3 89.106.22.3: GeoIP Country Edition: TR, Turkey
4 89.106.24.78: GeoIP Country Edition: TR, Turkey
5 84.77.114.176: GeoIP Country Edition: ES, Spain
6 221.208.208.91: GeoIP Country Edition: CN, China
7 202.97.238.204: GeoIP Country Edition: CN, China
8 10.16.54.129: GeoIP Country Edition: IP Address not found
9 10.16.54.29: GeoIP Country Edition: IP Address not found
10 221.208.208.92: GeoIP Country Edition: CN, China
11 61.138.137.10: GeoIP Country Edition: CN, China
12 221.208.208.212: GeoIP Country Edition: CN, China
13 71.146.22.111: GeoIP Country Edition: US, United States
14 10.16.54.100: GeoIP Country Edition: IP Address not found
15 221.12.113.247: GeoIP Country Edition: CN, China
16 35.52.216.193: GeoIP Country Edition: US, United States
17 72.30.177.83: GeoIP Country Edition: US, United States
18 74.6.86.121: GeoIP Country Edition: US, United States
19 62.121.117.72: GeoIP Country Edition: RO, Romania
20 10.16.54.2: GeoIP Country Edition: IP Address not found
21 220.73.220.4: GeoIP Country Edition: KR, Korea, Republic of
22 217.98.63.167: GeoIP Country Edition: PL, Poland
23 213.254.204.197: GeoIP Country Edition: US, United States
24 206.132.100.105: GeoIP Country Edition: US, United States
25 193.108.94.88: GeoIP Country Edition: DE, Germany
26 81.52.250.134: GeoIP Country Edition: FR, France
27 72.30.177.72: GeoIP Country Edition: US, United States
28 63.209.3.132: GeoIP Country Edition: US, United States
29 74.6.75.32: GeoIP Country Edition: US, United States
30 195.70.130.19: GeoIP Country Edition: CZ, Czech Republic
31 65.74.168.211: GeoIP Country Edition: US, United States
32 60.11.125.47: GeoIP Country Edition: CN, China
33 216.254.95.2: GeoIP Country Edition: US, United States
34 212.187.244.39: GeoIP Country Edition: GB, United Kingdom
35 211.14.12.10: GeoIP Country Edition: JP, Japan
36 210.80.243.9: GeoIP Country Edition: JP, Japan
37 202.12.27.33: GeoIP Country Edition: JP, Japan
```

También hicimos la prueba con el siguiente comando para verificar la procedencia de las ips:

“netcat whois.cymru.com 43 < unicasip.txt > localizacion.txt”



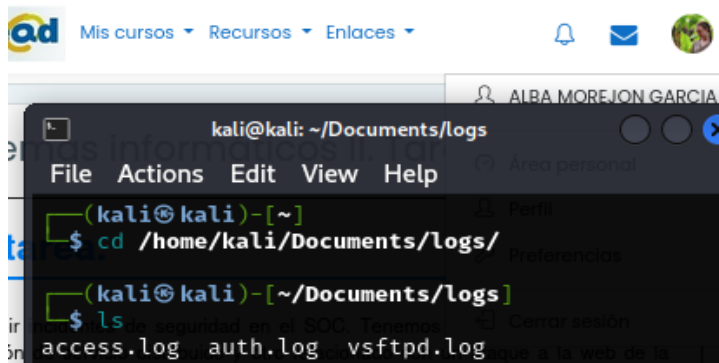
```
(kali@kali)-[~/Desktop]
$ netcat whois.cymru.com 43 < unicasip.txt > localizacion.txt
~/Desktop/localizacion.txt - Mousepad
File Edit Search View Document Help
1 Bulk mode; whois.cymru.com [2025-02-15 19:00:20 +0000]
2 25145 | 213.144.110.130 | AS-TEKNETEL Teknetel Telekomunikasyon A.S., TR
3 25019 | 207.150.178.78 | SAUDINETSTC-AS, SA
4 834 | 89.106.22.3 | IPXO, US
5 834 | 89.106.24.78 | IPXO, US
6 12479 | 84.77.114.176 | UNI2-AS, ES
7 4837 | 221.208.208.91 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
8 4837 | 202.97.238.204 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
9 NA | 10.16.54.129 | NA
10 NA | 10.16.54.29 | NA
11 4837 | 221.208.208.92 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
12 4837 | 61.138.137.10 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
13 4837 | 221.208.208.212 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
14 7018 | 71.146.22.111 | ATT-INTERNET4, US
15 NA | 10.16.54.100 | NA
16 4837 | 221.12.113.247 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
17 16509 | 35.52.216.193 | AMAZON-02, US
18 NA | 72.30.177.83 | NA
19 NA | 74.6.86.121 | NA
20 12302 | 62.121.117.72 | VODAFONE_RO Charles de Gaulle nr.15, RO
21 NA | 10.16.54.2 | NA
22 4766 | 220.73.220.4 | KIXS-AS-KR Korea Telecom, KR
23 5617 | 217.98.63.167 | TPNET, PL
24 3257 | 213.254.204.197 | GTT-BACKBONE GTT, US
```

Incidente de ataque a la web de la compañía

Relativo al ataque web, debemos identificar ([fichero logs.zip](#)):

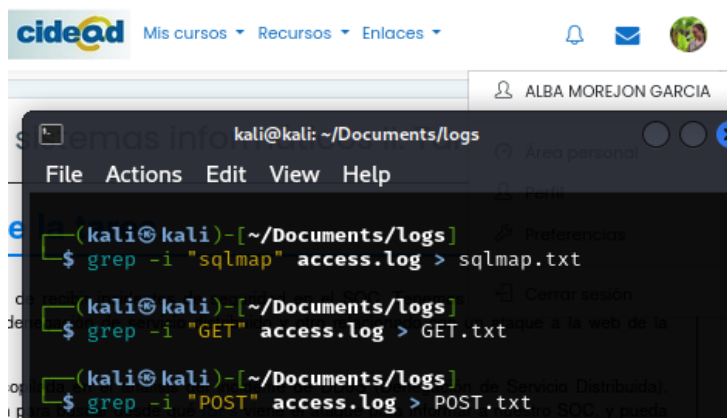
- Las herramientas ofensivas utilizadas por los atacantes
- Las páginas web sobre las que han realizado el ataque
- Usuarios utilizados en cada uno de los servicios atacados
- Ficheros descargados

Descargamos en una carpeta, el archivo comprimido facilitado en el enunciado que contiene los archivos logs.

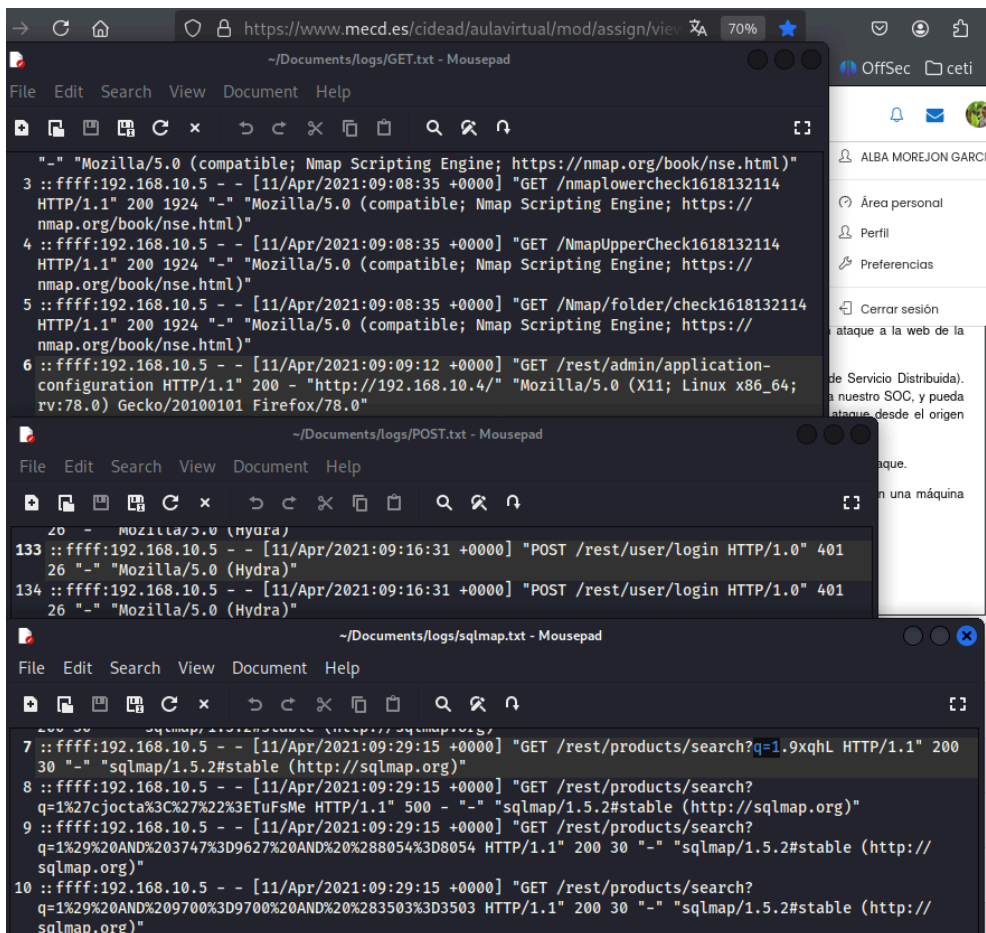


Vamos a empezar a analizar el primer fichero, el **access.log**.

Hacemos un primer filtrado, buscando los registros que contengan palabras clave como: sqlmap, get, post... entre otras.



Y mostramos una parte de los ficheros extraídos con cada palabra clave.



Analizamos cada fichero.

Analizamos un ejemplo de los registros:

```

::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /.git/HEAD HTTP/1.1" 200 1924 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

```

- ::ffff:192.168.10.5 Dirección ip del cliente que realizó la solicitud
- No tendríamos la identidad del cliente
- No tendríamos el usuario que ha sido autenticado
- [11/Apr/2021:09:08:35 +0000] fecha y hora en el que se realizó la solicitud
- "GET /.git/HEAD HTTP/1.1" el método HTTP (GET), la ruta solicitada y la versión del protocolo
- 200 el código de respuesta fue exitoso (HTTP:200)
- 1924 el tamaño en bytes que ocupa la respuesta
- "-" URL desde la que se realiza la solicitud
- "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" la cadena user-agent identifica el navegador o la herramienta que hizo la solicitud (En este caso, motor de script Nmap)

GET.txt

Herramientas ofensivas utilizadas:

- Nmap: identificado en el user-agent:

"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

- Sqlmap: identificado por:

"sqlmap/1.5.2#stable (http://sqlmap.org)"

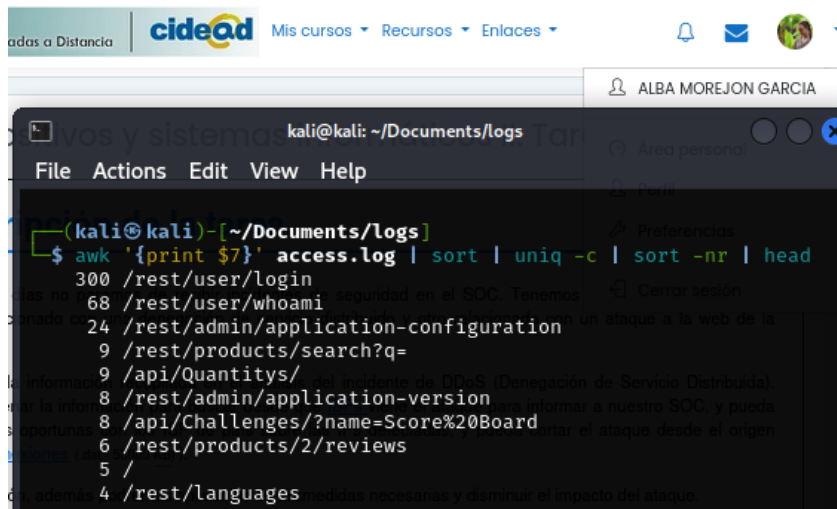
- Feroxbuster: identificado por el user-agent:

"feroxbuster/2.2.1"

Páginas webs atacadas:

A continuación, con siguiente el comando, vemos la columna del fichero de accesos en la que se muestra la ruta de solicitud HTTP, ordenada alfabéticamente por número de apariciones, ordenada de forma descendente mostrando las primeras líneas:

`“awk '{print $7}' access.log | sort | uniq -c | sort -nr | head”`



```
(kali@kali)-[~/Documents/logs]
$ awk '{print $7}' access.log | sort | uniq -c | sort -nr | head
300 /rest/user/login
68 /rest/user/whoami
24 /rest/admin/application-configuration
9 /rest/products/search?q=
9 /api/Quantitys/
8 /rest/admin/application-version
8 /api/Challenges/?name=Score%20Board
6 /rest/products/2/reviews
5 /
4 /rest/languages
```

En este fichero, no se han encontrado usuarios, pero el intento de inicio de sesión en `“/rest/user/login”` indica que se ha estado probando credenciales.

No se observan ficheros descargados pero hay intentos de acceso a archivos como el siguiente registro:
`::ffff:192.168.10.5 - - [11/Apr/2021:09:34:40 +0000] "GET /ftp/www-data.bak HTTP/1.1" 403 300 "-"`
`"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"`

POST.txt

Herramientas ofensivas utilizadas:

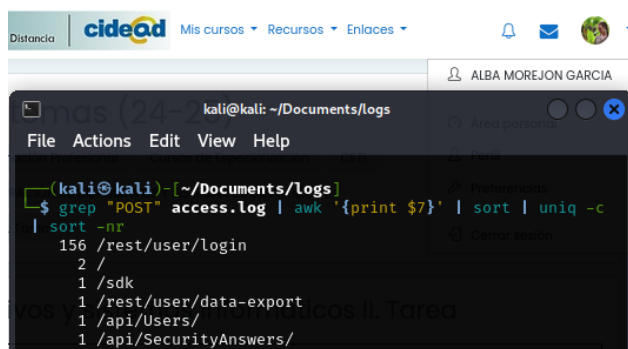
- Nmap: identificado en el user-agent:

`"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"`

- Hydra: identificado por:

`"Mozilla/5.0 (Hydra)"`

Con el mismo comando de antes, vemos las páginas webs que han sido intentadas de atacar:



```
(kali@kali)-[~/Documents/logs]
$ grep "POST" access.log | awk '{print $7}' | sort | uniq -c | sort -nr
156 /rest/user/login
2 /
1 /sdk
1 /rest/user/data-export
1 /api/Users/
1 /api/SecurityAnswers/
```

No se han encontrado usuarios específicos, pero el intento de inicio de sesión en `“/rest/user/login”` indica que se ha estado probando credenciales repetidamente.

No se observan ficheros descargados.

SQLMAP.txt

Herramientas ofensivas utilizadas:

- Sqlmap: identificado por:

"sqlmap/1.5.2#stable (http://sqlmap.org)"

Páginas webs atacadas:

/rest/products/search, son solicitudes GET con diferentes parámetros de búsqueda muchas intentan inyectar código SQL. Algunos ejemplos de parámetros inyectados:

- q=1
- q=1&QKqc=7074 AND 1-1 UNION ALL SELECT 1, NULL, '<script>alert("XSS")</script>', table_name FROM
- information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../etc/passwd') #
- q=1.9xqhL
- q=1%29%20AND%203747% 3D9627%20AND%20%288054%3D8054
- q=1%20AND%206384%3D1910
- q=1%20AND%206826%3D9654--%20qX0s

Resumen de la información obtenida hasta ahora del fichero access.log

Herramientas ofensivas identificadas

- Sqlmap: Utilizado para realizar inyecciones SQL.
- Nmap: Utilizado para escanear puertos y servicios.
- Hydra: Utilizado para ataques de fuerza bruta.
- Feroxbuster. Utilizado para descubrir rutas y archivos en el servidor.

Páginas web atacadas

- /rest/products/search
- /rest/user/login
- /api/Users/
- /api/SecurityAnswers/
- /api/Quantitys/
- /api/Challenges/?name=Score%20Board
- /rest/products/[varios IDs]/reviews
- /rest/saveLoginlp
- /rest/deluxe-membership
- /rest/continue-code
- /rest/image-captcha
- /assets/public/images/uploads/
- /api/Feedbacks/
- /api/SecurityQuestions/
- /api/Addresss
- /ftp
- /admin
- /backup
- /promotion
- /login
- /administartion

Usuarios utilizados

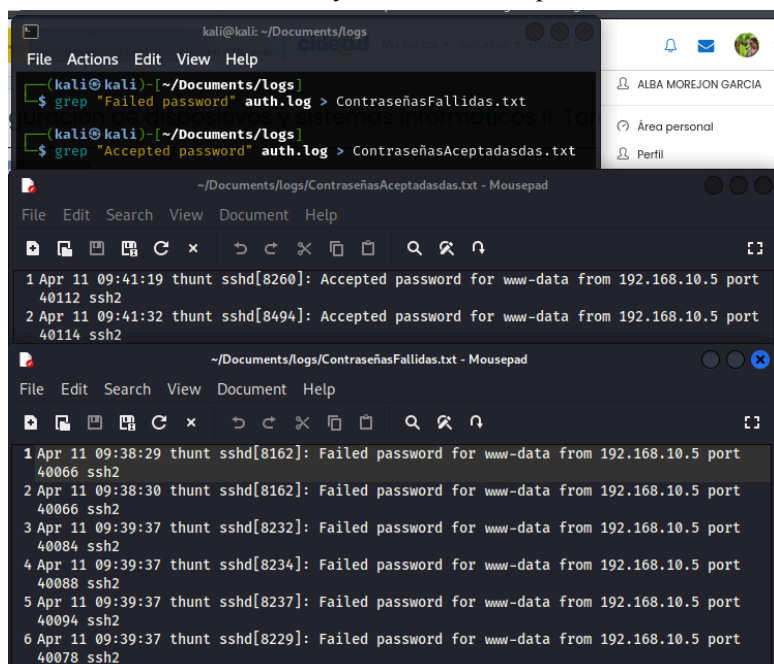
- No se identifican usuarios específicos, pero hay múltiples intentos de inicio de sesión en /rest/user/ login.

Ficheros descargados

- No se observan descargas de archivos en las muestras específicas, pero hay intentos de acceso a archivos de respaldo en /ftp/www-data.baky/ftp/coupons_2013.md.bak.

Seguimos analizando el fichero auth.log.

Vamos a analizar los intentos de autenticación en el sistema, hemos registrado en diferentes documentos los intentos fallidos y los intentos aceptados con el comando “*grep*” *Failed password*” *auth.log*”



```
kali@kali: ~/Documents/logs
File Actions Edit View Help
$ grep "Failed password" auth.log > ContraseñasFallidas.txt
$ grep "Accepted password" auth.log > ContraseñasAceptadasdas.txt

~/Documents/logs/ContraseñasAceptadasdas.txt - Mousepad
File Edit Search View Document Help
1 Apr 11 09:41:19 thunt sshd[8260]: Accepted password for www-data from 192.168.10.5 port 40112 ssh2
2 Apr 11 09:41:32 thunt sshd[8494]: Accepted password for www-data from 192.168.10.5 port 40114 ssh2

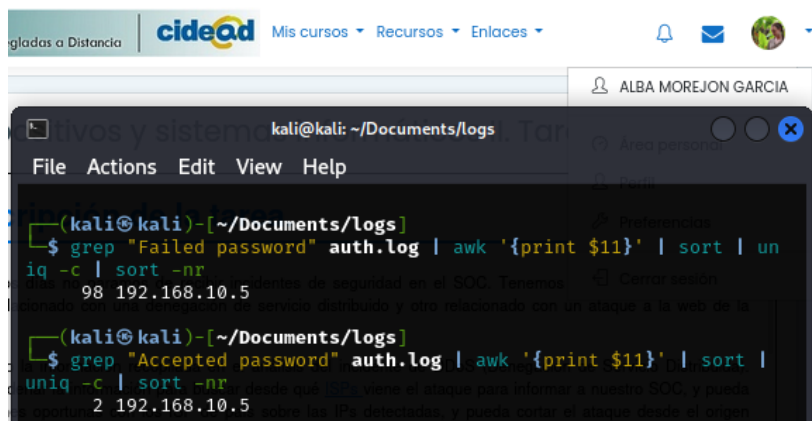
~/Documents/logs/ContraseñasFallidas.txt - Mousepad
File Edit Search View Document Help
1 Apr 11 09:38:29 thunt sshd[8162]: Failed password for www-data from 192.168.10.5 port 40066 ssh2
2 Apr 11 09:38:30 thunt sshd[8162]: Failed password for www-data from 192.168.10.5 port 40066 ssh2
3 Apr 11 09:39:37 thunt sshd[8232]: Failed password for www-data from 192.168.10.5 port 40084 ssh2
4 Apr 11 09:39:37 thunt sshd[8234]: Failed password for www-data from 192.168.10.5 port 40088 ssh2
5 Apr 11 09:39:37 thunt sshd[8237]: Failed password for www-data from 192.168.10.5 port 40094 ssh2
6 Apr 11 09:39:37 thunt sshd[8229]: Failed password for www-data from 192.168.10.5 port 40078 ssh2
```

Analizamos un ejemplo de los registros:

Apr 11 09:39:37 thunt sshd[8230]: Failed password for www-data from 192.168.10.5 port 40080 ssh2

- *Apr 11 09:39:37* fecha y hora en el que se realizó la solicitud
- *thunt* el nombre del host donde ocurrió el evento
- *sshd [xxxx]* nombre e ID del proceso (PID)
- *Failed password for www-data from 192.168.10.5 port 40080 ssh2* mensaje de registro
 - *Failed password* resultado del intento de autenticación
 - *ww-data* cuenta de usuario
 - *192.168.10.5* dirección desde la cual se realizó el intento de autenticación
 - *port 40080* puerto desde el que se realizó la conexión
 - *ssh2* protocolo utilizado

Vemos la lista de direcciones ip desde las cuales se han realizado los intentos, junto con el número de veces ordenadas de mayor a menor. Comando: “*grep*” *Failed password*” *auth.log* | *awk* ‘{print \$11}’ | *sort* | *uniq -c* | *sort -nr*”



```
gladas a Distancia cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA
kali@kali: ~/Documents/logs
File Actions Edit View Help
$ grep "Failed password" auth.log | awk '{print $11}' | sort | uniq -c | sort -nr
98 192.168.10.5
$ grep "Accepted password" auth.log | awk '{print $11}' | sort | uniq -c | sort -nr
2 192.168.10.5
```

Vemos en los intentos de conexión que ha sido únicamente la cuenta de usuario *www-data* y todas los intentos se han realizado desde la ip *192.168.10.5*. Y solo han sido aceptados 2 de ellos.

Por último analizamos el fichero vsftpd.log.

Con el comando `"grep "OK DOWNLOAD" vsftpd.log"` encontramos registros de descargas que han sido exitosas.

Con el comando `"grep "OK UPLOAD" vsftpd.log"` se ven los ficheros que se han subido.

Con el comando `"grep "OK UPLOAD" vsftpd.log"` vemos los intentos de inicio de sesión.

Con el comando `"grep "FAIL" vsftpd.log"` encontramos registros de errores.

```
gladas a Distancia | cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

kali@kali: ~/Documents/logs
File Actions Edit View Help

(kali@kali)-[~/Documents/logs]
$ grep "OK DOWNLOAD" vsftpd.log
Sun Apr 11 09:35:45 2021 [pid 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/www-data.bak", 2602 bytes, 544.81Kbyte/sec
Sun Apr 11 09:36:08 2021 [pid 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/coupons_2013.md.bak", 131 bytes, 3.01Kbyte/sec

(kali@kali)-[~/Documents/logs]
$ grep "OK UPLOAD" vsftpd.log

(kali@kali)-[~/Documents/logs]
$ grep "LOGIN" vsftpd.log
Sun Apr 11 08:13:40 2021 [pid 6334] [anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
Sun Apr 11 08:15:14 2021 [pid 6477] [anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
Sun Apr 11 08:15:33 2021 [pid 6482] [anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
Sun Apr 11 08:15:58 2021 [pid 6526] [ftp] OK LOGIN: Client "::ffff:127.0.0.1", anon password "?"
Sun Apr 11 08:18:07 2021 [pid 6627] [ftp] OK LOGIN: Client "::ffff:127.0.0.1", anon password "ls"
Sun Apr 11 08:29:34 2021 [pid 6846] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 08:29:34 2021 [pid 6840] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 08:29:35 2021 [pid 6837] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 09:08:34 2021 [pid 8020] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 09:08:34 2021 [pid 8014] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 09:08:35 2021 [pid 8013] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 09:35:37 2021 [pid 8152] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "?"
```

```
gladas a Distancia | cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

kali@kali: ~/Documents/logs
File Actions Edit View Help

(kali@kali)-[~/Documents/logs]
$ grep "FAIL" vsftpd.log
Sun Apr 11 08:13:40 2021 [pid 6334] [anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
Sun Apr 11 08:15:14 2021 [pid 6477] [anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
Sun Apr 11 08:15:33 2021 [pid 6482] [anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
```

Resumen de los hallazgos del fichero vsftpd.log

Descargas exitosas

- Fecha y hora: 11 de abril de 2021
- Dirección IP del cliente::ffff:192.168.10.5
- Archivos descargados:
 - /www-data.bak (2602 bytes)
 - /coupons_2013.md.bak (131 bytes)

Subidas exitosas: no se encontraron registros de subidas exitosas en el archivo vsftpd.log.

Intentos de inicio de sesión

- Fallidos:
 - Usuario: anonymous
 - Dirección IP del cliente::ffff:127.0.0.1
 - Fechas y horas:
 - 11 de abril de 2021, 08:13:40
 - 11 de abril de 2021, 08:15:14
 - 11 de abril de 2021, 08:15:33
- Exitosos:
 - Usuario: ftp
 - Dirección IP del cliente::ffff:127.0.0.1y::ffff:192.168.10.5 • Fechas y horas.
 - 11 de abril de 2021, 08:15:58 (127.0.0.1)
 - 11 de abril de 2021, 08:18:07 (127.0.0.1)
 - 11 de abril de 2021, 08:29:34 (192.168.10.5)
 - 11 de abril de 2021, 08:29:35 (192.168.10.5)
 - 11 de abril de 2021, 09:08:34 (192.168.10.5)
 - 11 de abril de 2021, 09:08:35 (192.168.10.5)
 - 11 de abril de 2021, 09:35:37 (192.168.10.5)

En conclusión, el análisis del archivo vsftpd.log muestra que el atacante logró descargar dos archivos (/www-data.bak y /coupons_2013.md.bak) desde la dirección IP::ffff:192.168.10.5. También hubo múltiples intentos de inicio de sesión, desde las direcciones IP::ffff:127.0.0.1 y ::ffff:192.168.10.5.

El análisis de los archivos access.log, auth.log y vsftpd.log revela que los atacantes utilizaron herramientas como sqlmap para inyecciones SQL, Nmap para escanear puertos y servicios, Hydra para ataques de fuerza bruta y feroxbuster para descubrir rutas y archivos en el servidor. Las páginas web atacadas incluyen /rest/user/login con 300 accesos, indicando múltiples intentos de inicio de sesión, / est/user/whoami con 68 accesos para identificar al usuario autenticado, y otras rutas como /api/Quantitys/, /rest/admin/application-version, y /api/Challenges/? name=Score%20Board. Los usuarios utilizados en los servicios atacados incluyen www-data, con múltiples intentos de inicio de sesión fallidos y dos exitosos desde la IP 192.168.10.5, y ftp, con varios intentos de inicio de sesión exitosos desde las IPs 127.0.0.1 y 192.168.10.5. Los archivos descargados incluyen / www-data.bak y /coupons_2013.md.bak, ambos desde la IP 192.168.10.5.

Se recomienda revisar los accesos y actividades de los usuarios www-data y ftp, cambiar las contraseñas comprometidas e implementar autenticación multifactor (MFA) y considerar bloquear la IP 192.168.10.5 para prevenir futuros ataques.