Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Bastionado de redes y sistemas

UD07. Configuración de dispositivos y sistemas informáticos II.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

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 (.dat - 53000 KB)).

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:

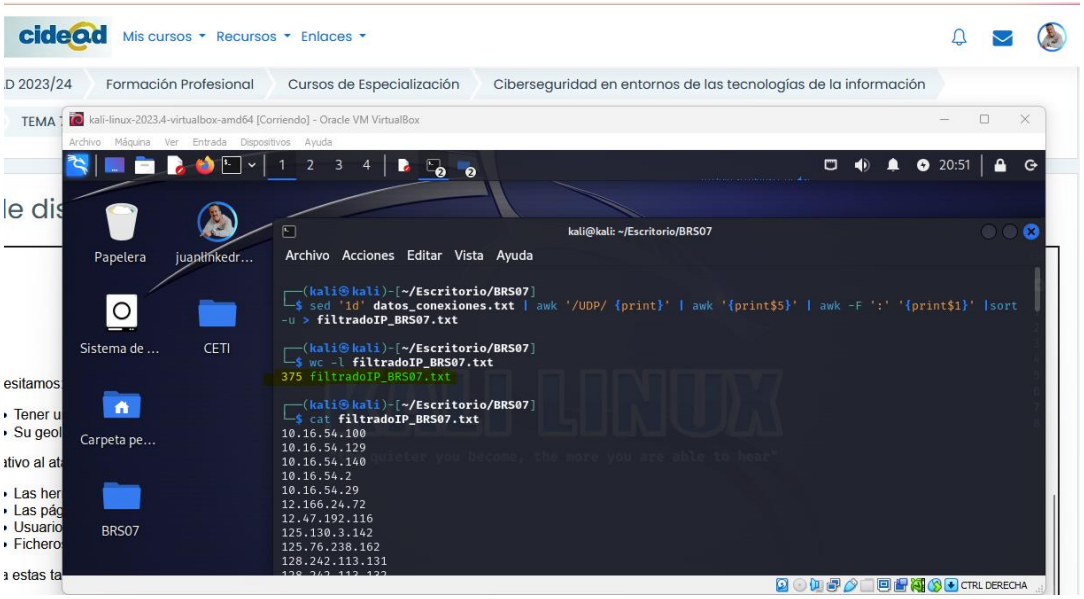
Columna	Descripción
1	Fecha
2	Hora
3	Duración
4	Protocolo
5	IP:puerto origen
6	->
7	IP:puerto destino
8	Nº paquetes transmitidos
9	Nº bytes transmitidos
10	Número de flujo

Héctor Fernández Bardal. *Tabla datos ejercicio* (CC0)

Necesitamos:

✓ Tener un listado de IPs únicas

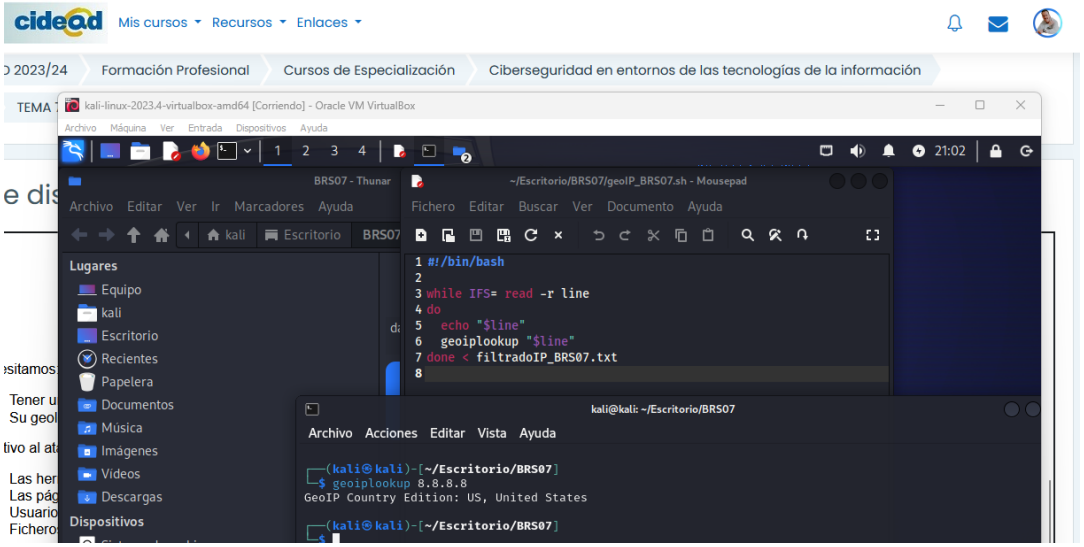
Concatenamos comandos para, por un lado, limpiar las cabeceras y luego procesar las líneas que contengan el texto **UDP**. Como **awk** toma por defecto el espacio como separador, filtramos por el elemento 5, seleccionamos como separador **':'** y tomamos el primer elemento. Filtramos y ordenamos para quedarnos con las IP únicas (375 como veremos tras ejecutar) y lo guardamos en un archivo.



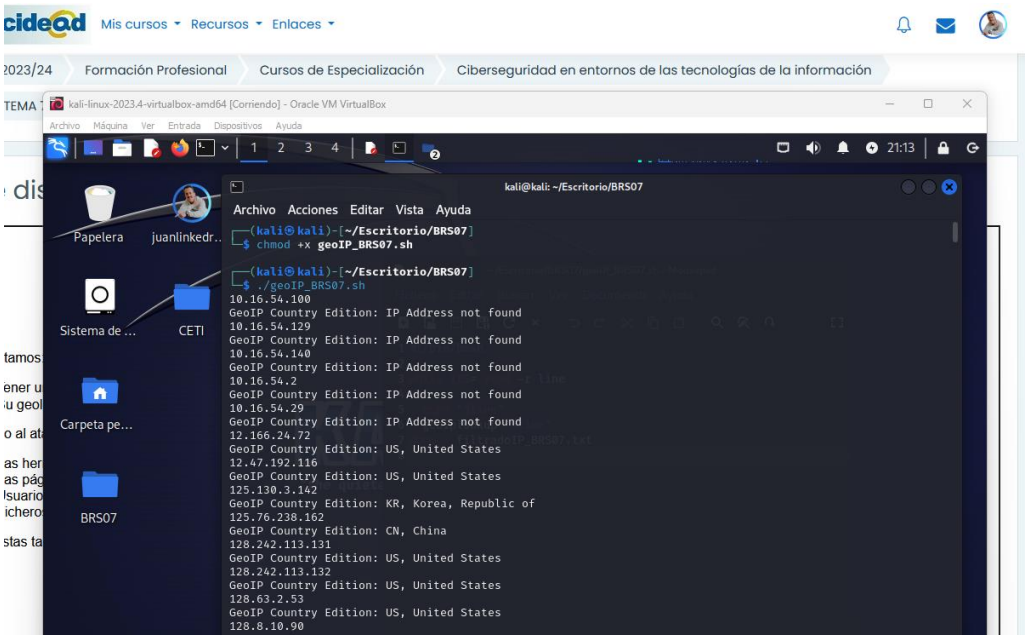
✓ Su geolocalización con un servicio de whois

Aprovecho la instalación previa del servicio whois gratuito, **GeoIP** de **MaxMind.**

Creo un script para que recorra cada línea y ejecutando el comando **geoiplookup**, nos indique el país.



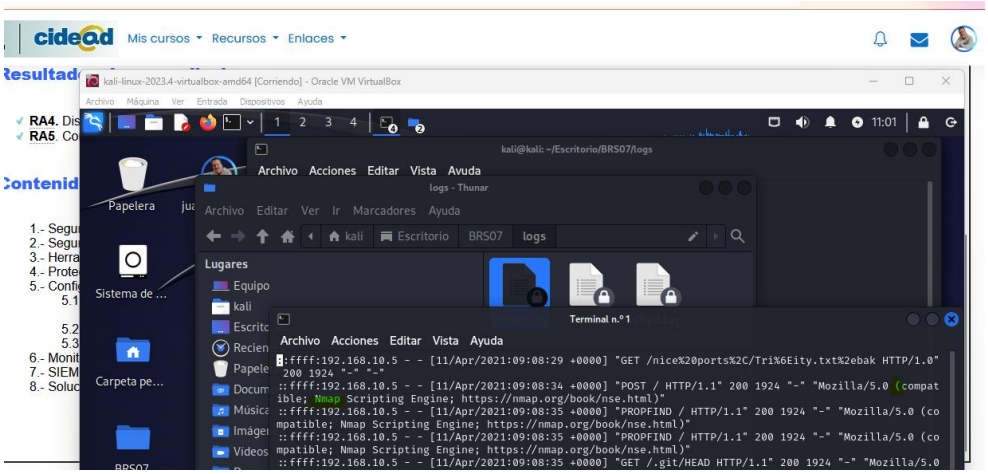
Ejecutamos el script para que muestre los datos.



Relativo al ataque web, debemos identificar (fichero logs.zip (zip - 6,41 KB)):

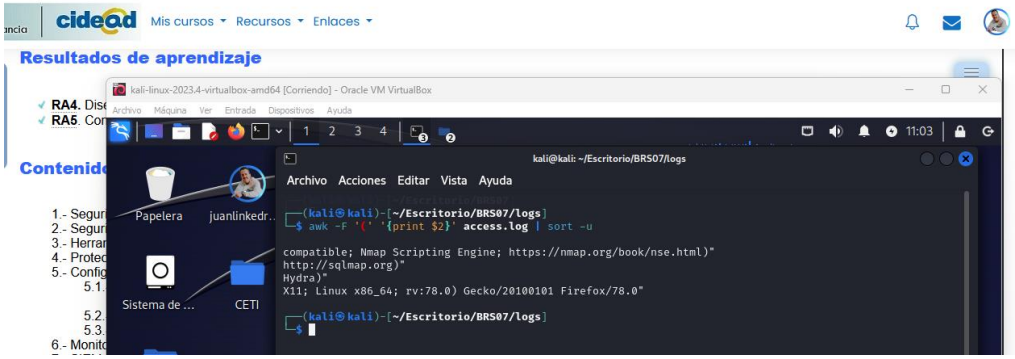
✓ Las herramientas ofensivas utilizadas por los atacantes

Vamos a utilizar el archivo **`access.log`**. Vista su distribución, se pueden observar que las herramientas están en un campo encerrado entre paréntesis.



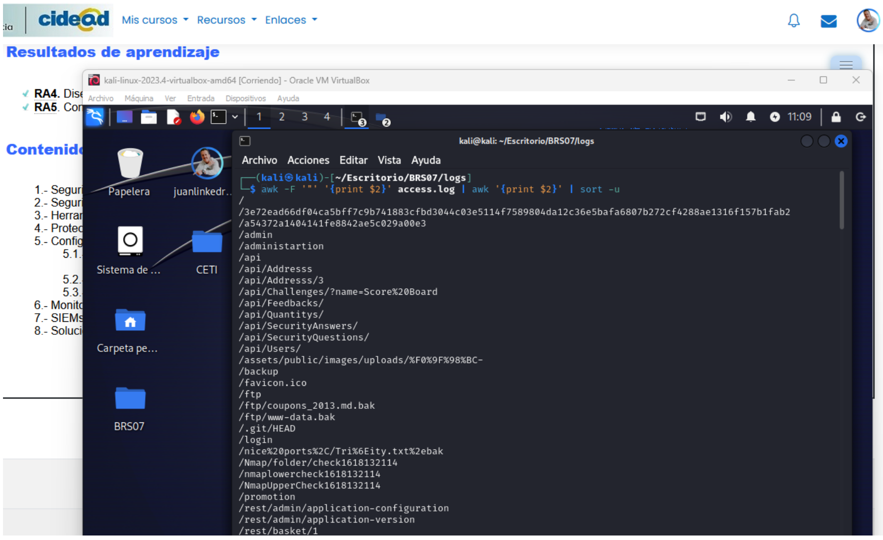
Utilizamos ese dato para recorrer el archivo, filtrar y mostrar los datos.

Encontramos que se han utilizado las herramientas: **`nmap`**, **`sqlmap`**, **`Hydra`** y **`X11`**.

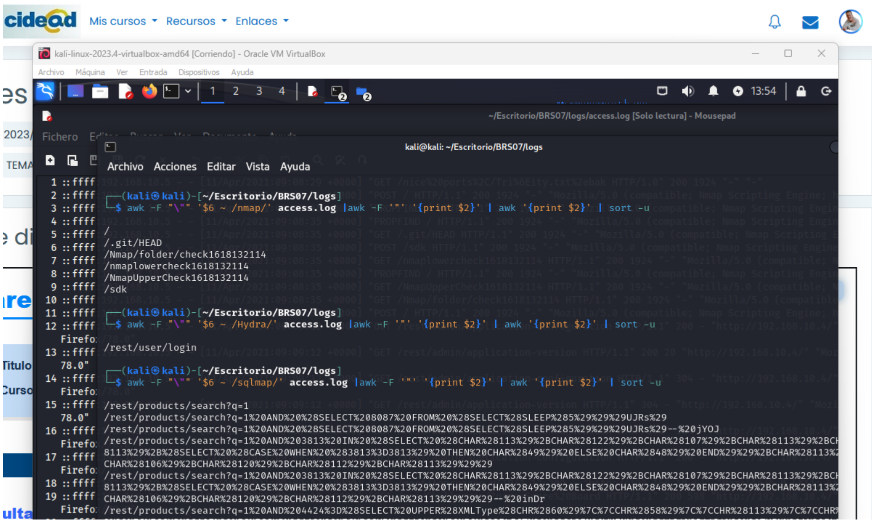


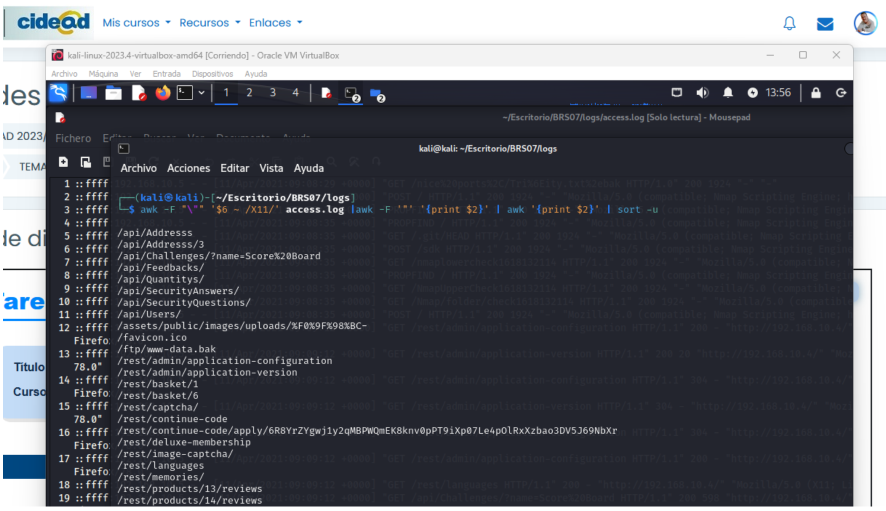
✓ Las páginas web sobre las que han realizado el ataque.

Seguimos trabajando sobre el mismo archivo y estructura. Puede observarse que las peticiones llegan entrecomilladas, por lo que la lógica empleada para este comando es similar a la vista en el punto anterior.



Aprovechamos que ya conocemos las herramientas utilizadas, para filtrar en base a ellas y saber que páginas web se han visto afectadas por cada una de ellas.

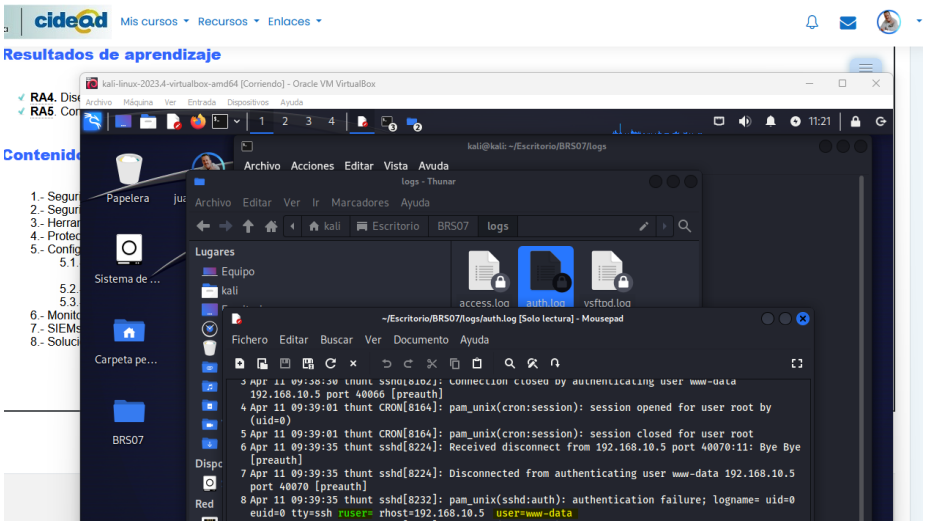




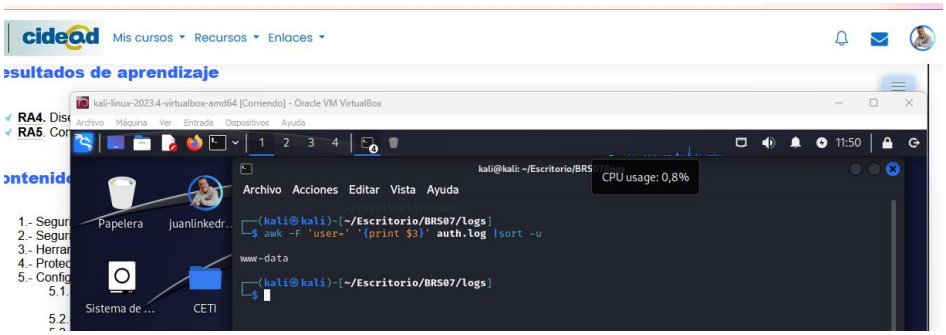
✓ Usuarios utilizados en cada uno de los servicios atacados.

Abrimos el archivo **`auth.log`** para ver la distribución de las columnas de datos y sus campos.

Tras ello, podemos ver que las líneas con mayor volumen de intentos tienen dos campos susceptibles de filtrar, pero uno de ellos, apunta a un servidor, por lo que filtramos por el campo **`user`**.

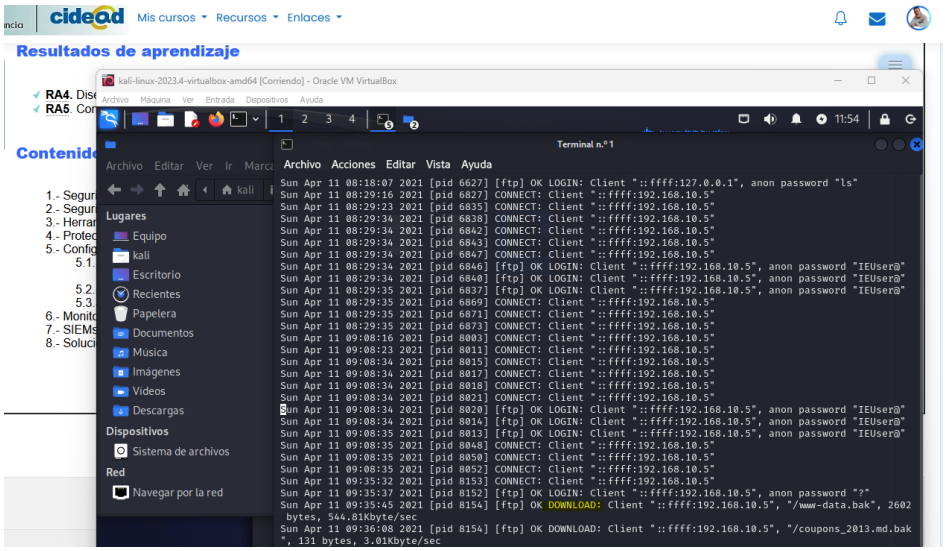


Nos devuelve el usuario utilizado.

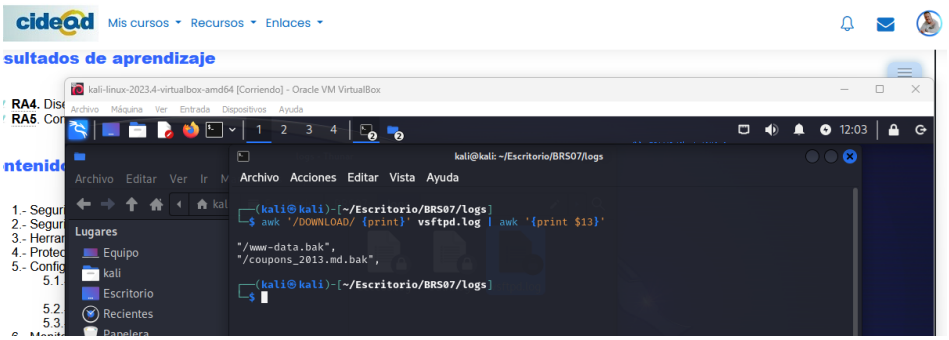


✓ Ficheros descargados

Tras una rápida revisión del archivo vsftpd.log podemos ver que debemos buscar en las líneas que contengan la palabra DOWNLOAD.



El campo que nos interesa está en la columna 13.



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

Webgrafía.

https://www.mecd.es/cidead/aulavirtual/course/view.php?id=2368#section-7

https://geekland.eu/uso-del-comando-awk-en-linux-y-unix-con-ejemplos/

https://ugeek.github.io/blog/post/2023-04-12-geolocalizacion-de-una-ip-en-la-terminal-y-offline.html