



**APUNTES 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**



## ÍNDICE

1. Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, Antimalware.
2. Seguridad del correo electrónico.
3. Herramientas de almacenamiento de logs.
4. Protección ante ataques de denegación de servicio distribuido (DDoS).
5. Configuración segura de cortafuegos, enrutadores y proxies.
  - 5.1. Firewalls.
    - 5.1.1. Medidas de evasión.
  - 5.2. Router.
  - 5.3. Proxy.
6. Monitorización de sistemas y dispositivos.
7. SIEMs.
8. Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs.

### Caso práctico

En la empresa ACME SL desde hace unos días no paran de recibir incidentes de seguridad en el SOC. De todos ellos hay dos urgentes que deben resolver. Uno relacionado con una denegación de servicio distribuido y otro relacionado con un ataque a la web de la compañía. Sus administradores y analistas de seguridad están analizando la información recopilada del incidente de DDoS (Denegación de Servicio Distribuida). El objetivo es buscar desde qué ISPs viene el ataque para informar a nuestro SOC, y se puedan tomar las acciones oportunas con los ISP del país sobre las IPs detectadas. La nalidad de todo ello es aplicar las contramedidas necesarias y disminuir el impacto del ataque.

En los siguientes puntos iremos estudiando materias que tienen que ver con el servicio de vigilancia de un sistema como es el servicio de monitorización, el almacenamiento de la información de monitorización (logs) y el SIEM. Ya que están directamente relacionados con los servicios que presta un SOC y que servirá para gestionar incidentes y detectar problemas de configuración relacionados con la seguridad.

Otra de la materias que trataremos será la configuración de dispositivos perimetrales como son los rewall, los routers y los proxy. Ya que nos ayudarán en la defensa de los ataques que impactan en la disponibilidad: DoS y DDoS.

## 1.- SEGURIDAD DEL PUESTO DE TRABAJO Y ENDPOINT FIJO Y MÓVIL. ANTIAPT, ANTIMALWARE.

### Caso práctico

Los mecanismos de defensa en los equipos de usuarios son uno de los primeras líneas de defensa, que puede prevenir el acceso inicial de los atacantes al sistema. Bien por descarga de malware escondido en aplicaciones gratuitas, correos electrónicos, navegación a páginas web infectadas,... Los atacantes han recopilado información de los usuarios de la empresa que son administradores del sistema para intentar atacar sus equipos, ya que saben que son los que tienen privilegios en la red. De esta manera los atacantes pueden evitar tener que escalar privilegios en el ataque. El método que va a utilizar es infectar páginas web de descargas de software de administración: MobaXterm, putty, OpenVnc,...

¿Por qué es útil tener mecanismos de defensa en los puestos de trabajo? ¿Se debe incrementar esta protección en los puestos de administración?.

### Cuidado Administrador

Los mecanismos de defensa en los equipos de usuarios son uno de los primeras líneas de defensa, que puede prevenir el acceso inicial de los atacantes al sistema. Bien por descarga de malware escondido en aplicaciones gratuitas, correos electrónicos, navegación a páginas web infectadas,...

Los usuarios con permisos de administración deberían estar más vigilados y tener mecanismos de protección y detección de amenazas por el impacto que tienen en sus cuentas en el sistema.

### Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, Antimalware

Los puestos de trabajo o puestos de clientes son el punto más débil de la seguridad de un sistema, ya que son los operados por los usuarios y los que más errores de seguridad comenten si la compañía no dispone de un nivel de concienciación adecuada sobre la seguridad. Por lo que están siendo el principal objetivo de los atacantes.

Inicialmente estas zonas estaban más desprotegidas al no considerarse críticas, pero con el crecimiento del número de incidentes, se descubrió que eran las más vulnerables para el acceso inicial al sistema. Se ha producido en los últimos años un cambio de paradigma en la seguridad. Protegiendo los equipos nales de los sistemas (endpoint), ,equipos de los usuarios, en lugar de proteger únicamente los servidores que es dónde se almacenaba la información.

Los equipos de los usuarios son los que elevan el riesgo del sistema ya que son los que se conectan a páginas web, descargan archivos, reciben correo,... Es otro de los motivos por los que proteger los equipos de los usuarios, disminuirá el riesgo de sufrir un incidente de seguridad. Muchos de los ataques requieren de acciones de los usuarios, aunque no sean conscientes de la realización de las acciones, por lo que sus acciones son necesarias muchas veces para que se produzcan las infecciones. Aquí entra también en juego la ingeniería social.

Si analizamos a información de los múltiples ataques realizados a los sistemas, muchos de ellos tienen su origen en los equipos nales del sistema, y a través de escalado se privilegios los atacantes se hacen con el control de los puntos más críticos del sistema. Por lo que es importante no dejar desprotegidos los puntos nales de los sistemas y protegerlos con medidas de seguridad.

Una de los mecanismos de protección de los equipos de los usuarios nales son los endpoint, Estos endopints tienen capacidad de configuración y permiten desplegar una serie de reglas para la detección de nuevas amenazas. Además de tener la capacidad de remitir la información de lo que está sucediendo en el equipo a un servidor central, para que dicha información sea enviada al SOC y analizada por los equipos de respuesta a incidentes o también por el equipo de threat hunting.

Existen actualmente varios modelos de software libre que tiene la capacidad de incluir reglas de detección, así como realizar consultas a los clientes (por ejemplo: osquery). Esto es bastante efectivo cuando se quieren tener información actual ante un incidente de seguridad.

Esta medida de protección permite tener información real sobre las máquinas, incluso recopilar información actual y actualizada en el momento del análisis del incidente, lo que permita recopilar información que no está siendo enviada o analizada por el SOC.

Las herramientas antiAPT están más orientadas a poder reaccionar de manera autónoma ante un incidente o ciertos IOCs, de manera que el tiempo de reacción disminuya (dwell time). Ya que a pesar de lo múltiples mecanismos de seguridad que se implanten en el sistema debemos tener en cuenta un eficiente mecanismo de reacción ante incidentes.

Las herramientas antiAPT se irán actualizando con la inteligencia de amenazas que proporciona el departamento de threat intelligence.

En el siguiente video podemos visualizar la importancia de la inteligencia de amenazas.

## 2.- SEGURIDAD DEL CORREO ELECTRÓNICO.

Caso práctico

El correo electrónico es uno de los principales vectores de entrada en los ataques. Aprovechándose de la ingeniería social, muchos de los usuarios de los sistemas descargan adjuntos, acceden a enlaces de páginas web infectadas, introducen información personal sensible como claves, ... Por lo tanto es necesario establecer mecanismos de seguridad que nos permitan contrarrestar los fallos de seguridad de los usuarios.

Vamos a identificar mecanismos de seguridad que configuraríamos para los usuarios en el servidor de correo.

Correo seguro

- Establece listas blancas de dominios contables
- No permitas correos con adjuntos ejecutables.
- Alerta con los avisos y campañas de phishing para configurar reglas temporales asociados a campañas
- No permitas correos comprimidos con contraseñas. Hay campañas que utilizan este método para evadir los mecanismos de análisis.

Las principales amenazas del correo electrónico son la entrada de malware a través de:

- Enlaces maliciosos en el cuerpo del mensaje.
- Documentos adjuntos en el correo.
- Campañas de desinformación.

Frente a estas amenazas los mecanismos de protección son:

- Protección del servidor de correo frente a enlaces maliciosos.
- Protección del servidor de correo frente a correos que contengan malware.
- Limitación al reenvío automático de correos que nos proteja de la fuga de información.
- Concienciación y formación de ciberseguridad a los usuarios.

Hay 3 protocolos principales que gestionan la entrada y salida de correos electrónicos:

- SMTP (Simple Mail Transfer Protocol) – Para el envío de correos.
- POP3 (Post Office Protocol) – Realiza la transferencia de correos entre el cliente y el servidor de correo

electrónico. Los mensajes son eliminados una vez que son descargados en el dispositivo a no ser que se indique que se guarden en el servidor. Una vez descargado el mensaje no requiere conexión a Internet.

- IMAP (Internet Message Access Protocol) – Realiza la transferencia de correos entre el servidor de correo electrónico y el cliente. Los mensajes pueden ser transferidos a múltiples dispositivos porque se guardan en el servidor.

De cara a tener una configuración segura del servicio de correo, la información tiene que estar cifrada en tránsito. A continuación indicamos los puertos más comunes de funcionamiento de los protocolos de correo electrónico:

También se debe tener en cuenta el acceso a los servicios de webmail sobre HTTPS, para que siga existiendo el cifrado de la información de la información del servicio en tránsito.

De cara poder implantar mecanismos de protección y seguridad en el correo electrónico, es importante conocer cada uno de los campos de un mail. Por lo que a continuación os adjuntamos las siguientes referencias:

- INCIBE - Campos de un correo.
- Cabeceras de un correo

Con el objetivo de aplicar reglas de seguridad asociadas al correo y poder analizar los campos del correo electrónico que permitan implementar reglas que minimizan los riesgos de que los usuarios sean infectados al recibir campañas fraudulentas de correo que contengan:

- Ficheros adjuntos maliciosos: correos automáticos con macros, correos ejecutables enmascarados.
- Remitentes de dominios maliciosos
- Enlaces maliciosos
- Ficheros comprimidos con contraseña, para evitar el análisis por las herramientas de seguridad (antivirus)
- Cabeceras de seguridad del correo electrónico.

A continuación se indicarán protocolos que nos permitirán aumentar la seguridad para proteger la suplantación del correo electrónico y añadir funcionalidades de autenticación:

### SPF (Sender Policy Framework).

Nos permite proteger el correo contra falsificaciones de remitentes. Los propietarios de los dominios registran en el DNS los servidores de correos desde los que realizan los envíos. Eso sirve para que el resto de los usuarios que reciban un correo puedan consultar estos servidores SMTP autorizados a través de los servidores DNS, identificando las máquinas por su dirección IP.

Aunque este sistema puede ser menos eficiente para el reenvío de correos, ya que el mensaje puede viajar entre diferentes dominios y sería necesario mantener esa lista de dominios desde los que se permite el reenvío. Se debería configurar el SPF en modo monitor.

**DKIM (Domain Keys Identified Mail)**

Otra forma de autenticar un correo añadiendo un texto cifrado difícilmente falsable que contiene la procedencia del mensaje. Esta información es validada en destino con mecanismos de clave público/privada que confirman la autenticidad y la integridad.

Las claves públicas que necesitan los destinatarios para realizar estas comprobaciones se almacenan en los registros de los servidores DNS.

**DMARC (Domain-based Message Authentication Reporting, & Conformance)**

Suma los beneficios de SPF y DKIM

Todos estos mecanismos de protección no son suficientemente eficientes por sí solos, ya que los usuarios juegan un papel muy importante en la seguridad de un sistema. Ya que si no tenemos estos mecanismos técnicos alineados con el nivel de concienciación de los usuarios, a veces no son válidos.

**3.- HERRAMIENTAS DE ALMACENAMIENTO DE LOGS.**

Caso práctico

Almacenar los registros(logs) de lo que sucede en el sistema es un mecanismo que permite proteger los sistemas y mejorarlos. Tiene un coste asociado porque es necesario proveer al sistema de infraestructura del almacenamiento de la información y así como el procesamiento y análisis de dicha información. Esta información ha crecido exponencialmente con los años debido a requisitos legales y el cumplimiento de marcos (frameworks) y sistemas de gestión de la seguridad de la información. Pero tienen un beneficio mayor ya que nos permiten mejorar la seguridad y nos previene de ataques con más impacto.

Vamos a establecer un cálculo del dimensionamiento de la infraestructura de almacenamiento de logs, para la fuente de información del firewall perimetral. Cada log ocupa 500 bytes y se de media 2000 eventos por segundo.

Almacenamiento de Logs

$(2000 \text{ eventos por segundo} * 86400 \text{ segundos del día}) * 20 \text{ días} * 500 \text{ bytes} = 2592 \text{ GB de almacenamiento mensual}$  Como vemos es importante elegir bien las fuentes y la información que llega al sistema para no consumir recursos ineficientemente.

Los logs nos permiten realizar las tareas de vigilancia para evitar los incidentes (monitorización). Estos logs están almacenados en los equipos que los generan, pero deben enviarse a un sistema centralizado que obtiene información de diferentes fuentes:

- Sistemas operativos
- Aplicaciones
- Bases de datos
- Herramientas de seguridad: antivirus, NIDS, HIDS,
- Dispositivos de red: switches, firewalls, NAC, ...

El almacenamiento centralizado de logs además permitirá utilizar otras herramientas de apoyo con tecnologías como el Big Data que permitirán encontrar patrones de comportamientos anómalos.

Uno de los problemas a los que se enfrentan las herramientas que almacenan log son:

- Incremento de la información recibida
- Incremento del número de ataques y la duración del ataque en el tiempo, que obligan al sistema a tener mayor capacidad de retención
- La regulación que obliga al almacenamiento de los registros (logs) para utilizarlos como evidencias.

En conclusión es como buscar “una aguja en un pajar”, cuando el pajar cada vez es más grande y la aguja va cambiando forma.

Algunas de las herramientas más extendidas actualmente son: Logstash, GrayLog,... Lo que se impide a las nuevas herramientas, al tener un volumen muy alto de información, es tener la capacidad de localizar información con indexación de manera eficiente. Una de las herramientas que se ha popularizado en el mercado gracias a esta características es Splunk.

Splunk no fue creada para utilizarse en el mundo de la seguridad, pero su capacidad de búsqueda y análisis de datos, etc. permite realizar ciertas tareas en la búsqueda de información que son importantes en los procesos de un SOC:

- Mejora en la búsqueda de datos para la detección de amenazas
- Agilidad en las tareas de investigación
- Cortos tiempos de respuesta en la búsquedas de gran volumen de datos

A continuación describimos los elementos más importantes de la arquitectura de Splunk que permiten buscar y almacenar logs. En esta arquitectura el “Splunk Indexer” es el responsable de:

- Procesa los logs y los almacena con índices para facilitar su análisis y búsqueda
- Existe una organización eficiente de índices que permiten hacer eficiente la herramienta

El camino que recorre un registro hasta que es almacenado en disco es:

- Recopilación de la fuente
- Envío al punto central de recogida de información
- Parseo
- Indexado
- Almacenamiento en disco Sam Bowne (Dominio público)

En relación al almacenamiento de logs en los sistemas operativos más comunes se apoya en las siguientes herramientas: en Windows la herramienta que almacena los logs es el EventViewer y en Linux la herramienta que almacena y gestiona los logs es el servicio de syslog.

Se deben establecer en ambos las políticas de seguridad que permiten almacenar los logs tanto en los equipos como en un sistema centralizado. En los equipos deben guardarse logs con una menor retención, pero que evite la pérdida de información en caso de no poder enviar la información al servicio centralizado SOC.

De cara a que cada vez la información que necesitamos para investigar un incidente es mayor, es necesario establecer la arquitectura de monitorización: red de monitorización, almacenamiento y procesamiento de la información. La información que proporcionan los logs relativos al sistema tienen un carácter sensible, ya que en los logs se almacena mucha información y a veces con un alto nivel de detalle acerca de los dispositivos, configuraciones, protocolos, ... dependiendo del nivel que hayamos conjurado (verbose). Por lo que esta información tiene que ser enviada y tratada con seguridad.

El almacenamiento de logs es una de las tareas de SOC. Algunas herramientas almacenan los logs posteriormente a su tratamiento y otras los almacenan con anterioridad. Un log no tiene un volumen de ocupación alta, sobre todo en modo "raw", pero sí que el aumento del número de estos logs hace que las dimensiones de almacenamiento de logs dependan del número de equipos y de las fuentes que se vayan a monitorizar.

#### 4.- PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDOS).

Caso práctico

Cada vez son de mayores dimensiones los ataques de DoS y DDoS por la capacidad que tienen los atacantes de ir aumentando su infraestructura desde la que realizan el ataque en base a Bots. Incluso el ataque se hace desde diferentes países y localizaciones que dificulta la mitigación y medidas de protección frente al ataque.

Para poder realizar una protección frente a los ataques de DoS/DDoS debemos articular medidas de protección no sólo técnicas sino también procedimentales. Una opción es subcontratar el servicio de protección de denegación de servicio a través de empresas especializadas. Además, deberás tener documentados los procedimientos de activación de defensa de este tipo de ataques poniéndote en comunicación con los ISPs desde los que se realiza el ataque, o desde tu ISP para que filtren el tráfico y mitiguen la dimensión del ataque.

La disponibilidad de los servicios afecta a una de las dimensiones de la seguridad. La mayoría de los servicios que una compañía ofrece a sus clientes, están publicados en las DMZ. Estos servicios están protegidos por dispositivos de protección perimetral que evitan que el servicio se vea interrumpido. Además de la pérdida de servicio y las sanciones asociadas al incumplimiento de los SLA.

La protección frente a ataques de denegación de servicios se debe dimensionar acorde a un estudio de volumen de tráfico esperado. Además de aplicar las configuraciones asociadas a la protección de esta amenaza.

Los primeros mecanismos que afrontan los medios técnicos para la defensa de esta amenaza son los dispositivos de protección perimetral. Por lo que se deben establecer alarmas en dichos dispositivos que permitan tomar las primeras acciones de mitigación. Estas acciones tienen que estar documentadas en los procedimientos de defensa ante los ataques, para que la reacción al ataque sea lo más eficiente posible.

Además de las acciones de defensa de nuestra infraestructura contra ataques externos, se debe proteger los ataques realizados desde nuestra infraestructura por una mala configuración, o por la utilización de nuestro sistema de una manera fraudulenta ante el aviso de otra organización u organismo. Para estos casos también debemos poner los mecanismos de protección necesarios, para que no podamos dañar otros sistemas frente a ataques no controlados que se realizan desde nuestro sistema.

Los ataques de DoS y DDoS son mitigados por los firewalls y routers perimetrales, aunque dependiendo de la magnitud del ataque puede que estos no tengan la capacidad de contrarrestarlo. Empresas especializadas en ciberseguridad ofrecen este servicio de manera externalizada, ya que ciertos ataques de DDoS requieren de una infraestructura potente y unos conocimientos muy específicos en la materia.

Algunos de los ataques más comunes de DoS son:

- Syn Flood: su método se basa en utilizar el método de apertura de conexión TCP en 3 pasos (3-way-handshake), dejando sin terminar el último paso (envío ACK por parte del cliente) y por lo tanto quedando el servidor a la espera y consumiendo recursos. Con la herramienta hping podremos simular este tipo de ataques: `hping --syn --ood --randsource -p`

- Connection Flood: Consiste en realizar un elevado número de peticiones sobre un servicio.

- UDP Flood: Consiste en realizar un elevado número de peticiones sobre el protocolo UDP. Ya que cada vez que un equipo envía una petición al puerto UDP cerrado, el servidor responde con un paquete ICMP del tipo destino inalcanzable. Para que el atacante pueda destinar sus recursos a enviar paquetes UDP sin tener que gestionar los ICMP recibidos, utiliza IPs falsas.

Una medida preventiva y alineada con los mecanismos de prevención es poder obtener información previa ante posibles ataques. Ya que los grupos de ciberdelincuentes previamente preparan su infraestructura de Botnet para lanzar los ataques.

Algunas medidas de protección contra Syn Flood son:

- Aumentar los recursos asociados a las conexiones semiabiertas. No es efectivo si la dimensión del ataque supera los recursos del dispositivo. Reciclaje de la conexión TCP semiabierta más antigua
- Establecer una cola LIFO en los recursos asociados a las conexiones semiabiertas. De tal manera que la última conexión será la primera en liberarse ante un determinado número de conexiones.
- Almacenar menos información sobre el establecimiento de la conexión. TBC mínimo.
- Servicio de un proveedor externo basado en la nube debido al aumento de los bots y sus dimensiones. La idea de los proveedores es tener una infraestructura que permita distribuir la carga del ataque.

## 5.- Configuración segura de cortafuegos, enrutadores y proxies.

### Caso práctico

El router lleva muchos años funcionando perfectamente en la empresa en la que Alejandro es el administrador de la red. Con la llegada del nuevo responsable de tecnologías a la empresa quiere que se revise la configuración desde el punto de vista de la seguridad. Podemos ayudar Alejandro a qué debería mirar en el firewall. Si quieres acercarlo a un caso específico entra en la web de un fabricante y mira el comando que te ayudaría a configurarlo.

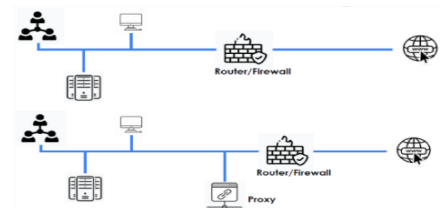
### Configuración del router

- El firmware del router está actualizado
- Se ha eliminado las contraseñas por defecto
- Se han deshabilitado los protocolos de enrutamiento que no se utilizan
- Deshabilitar los puertos sin uso y asignados a una VLAN específica.
- Activación auditoría. Envío auditoría a servidor externo.
- Cambio VLAN por defecto para ciertos protocolos
- Arranque seguro
- La red de administración y de operación están separadas
- Las contraseñas del equipos se almacenan cifradas
- Eliminación de protocolos inseguros.

Abordaremos en este capítulo, la configuración de tres de los principales dispositivos de protección perimetral de las redes y sistemas. Todas las tareas de configuración de estos dispositivos tienen el objetivo de proteger estos dispositivos en sí mismo así como de la redes y sistemas que los albergan.

A continuación se detallan cada uno de los aspectos a considerar en la configuración segura estos dispositivos, que puede ser aplicado para cualquier elemento del sistema.:

- Control de acceso
- Autenticación
- Control de sesión
- Configuración de servicios
- Mantenimiento
- Certificación de seguridad del producto.
- Auditoría
- Gestión de eventos.
- Protección de las comunicaciones



También debemos saber que estos dispositivos se pueden colocar en cualquier parte de la red para separar zonas, pero están en las zonas más perimetrales que se conectan con las redes de menos confianza para la compañía. A continuación se muestra un diseño de una red con el componente de un firewall/router.

En la siguiente imagen se puede visualizar un diseño de una red con un firewall, router y proxy.

En los siguientes apartados iremos detallando la configuración de seguridad de cada uno de los dispositivos.

### 5.1.- FIREWALLS.

Los firewall han evolucionado desde los simples dispositivos perimetrales en las redes, en los que sólo había uno y separaba la parte interna a la parte externa, a los firewall en nube donde este cambio de paradigma ha permitido difuminar el perímetro y controlar los flujos de información hacia servicios alojados fuera de nuestras instalaciones. En la integración de la red IT y OT también cobran un papel importante el firewall, para separar estas dos redes de la empresa que ahora se integran. Donde la red OT es una red más crítica y de más importancia que la red IT y por lo tanto tiene que estar protegida por estos dispositivos.

En este apartado ampliaremos la información relativa a los firewalls debido a la importancia que tienen como dispositivo de defensa. Estos dispositivos nos ayudarán a:

- Impedirá obtener información de los sistemas y de los puertos que están abiertos y cerrados la capas más internas de la red.
- Proteger y realizan el control de acceso a IP internas y puertos.
- Controlar los flujos de información de entrada y de salida de las distintas redes del sistema.
- Las reglas de los firewalls asociadas a los flujos de salida impedirán a los dispositivos conectarse contra IPs y dominios maliciosos
- No permitirán tener un mayor conocimiento de la red, a través del análisis de la información que recogen.

- Constituye el dispositivo principal de protección de la defensa en profundidad basado en capas.
- Permite reducir y mantener controlada la exposición de tu sistema frente ataques.

El firewall será uno de los puntos críticos del sistema ya que estará expuesto frente a las amenazas externas. Por lo que las vulnerabilidades de estos dispositivos son críticas y constituyen un elemento crítico de parcheo.

Otro de los firewall que existen en la red, son los firewall locales de software que residen en los equipos. El objetivo de aplicar medidas de protección a los firewalls locales de los equipos es complementar la seguridad de los firewall de red. Controlando la entrada de protocolos en los equipos. ¿Para qué necesitamos abrir un protocolo en el firewall de un equipo si no necesitamos que esté habilitado ese servicio?. Por lo tanto debemos activar el firewall de los equipos para aumentar el control de las comunicaciones

La administración de los dispositivos es un punto muy importante desde el punto de vista de la seguridad, ya que si el acceso con permisos de administración a los dispositivos fuese vulnerado tendría un alto impacto en el sistema, por lo que se debe realizar desde dispositivos controlados, apoyado por la segmentación.

La medidas generales de bastionado de estos dispositivos es:

- Mantener el software actualizado. Estos equipos debe estar entre los prioritarios para su actualización al ser un punto crítico del sistema.
- Segmentación de acceso para los administradores. Filtrando el acceso para ciertos equipos.
- Habilita el doble factor de autenticación para los administradores del firewall,
- Elimina las contraseñas y usuarios por defecto del dispositivo.
- Eliminar los servicios de administración administración no confiables.
- Realzar auditorías de seguridad sobre el firewall

### 5.1.1.- MEDIDAS DE EVASIÓN DE ANTIVIRUS

Una vez hayamos configurado el firewall, debemos realizar una auditoría de seguridad que nos permita saber que el equipo está bastionado correctamente al nivel de seguridad que deseamos. Se puede realizar una auditoría manual del dispositivo o combinarla con scripts que automaticen parte del proceso. La herramienta nmap nos permitirá realizar todas estas tareas.

Las pruebas son para intentar evadir las medidas de seguridad del firewall modificando:

- MAC/IP a través de métodos de MAC/IP spoofing. Para las tares de IP spoofing podemos utilizar modificadores el comando nmap "señuelos" (-D), proxy (--proxies) y spoofing (-S). En el caso de MAC spoofing se realizará con --spoof-mac, pero hay que tener en cuenta que para este ataque tenemos que utilizar una MAC de la red en la que estoy conectado, a no ser que nuestro único objetivo sea ocultar el ataque en lugar de capturar el tráfico.
- La fragmentación, MTU, y longitud de los datos. La fragmentación de paquetes servirá para aquellos firewalls que no analizan el paquete entero y para aquellos comunicaciones en las que los paquetes están fragmentados. Los paquete se pueden fragmentar con la opción -f, -ff o en base a la MTU que será múltiplo de 8 (-mtu). Otra opción es fijar la longitud de la capa TCP con datos aleatorios una vez que hemos introducido los datos en la capa (--data-length).
- Cabeceras de los campos. Estableciendo específicamente TTL(--ttl) o checksum (--badsum) inválidos nos pueden dar información del sistema auditar ya que cada sistema responde de una manera diferente.

### 5.2.- ROUTER.

Los router son dispositivos que trabaja en la capa 3 (red) del modelo OSI. Se encargan de realizar el control de la comunicaciones en una red. Es un elemento fundamental para interconectar redes. Con el objetivo de aislar dispositivos y crear capas dentro de un sistema, estos dispositivos constituyen un elemento de la red que permite aislar determinadas zonas.

También tienen la capacidad de crear reglas que permitan o denieguen el tráfico entre dos zonas, mediante listas de control de acceso (ACL). Al se un dispositivo de control, es un elemento crítico en la seguridad, por lo que la configuración del dispositivo es una tarea necesaria para mantener el sistema securizado.

Estas son las medidas de configuración segura que debemos aplicar a:

- Deshabilitar los puertos que no se utilicen que formen parte una VLAN específica de "puertos sin uso".
- Deshabilitar los servicios de un router que no se utilicen como: BOOTP, CDP, FTP, TFTP, HTTP, DNS, ...
- Utiliza las versiones seguras de los protocolos como por ejemplo SNMP v3 o HTTPS.
- Elimina los usuarios y contraseñas por defecto.
- Establece grupos de usuarios con diferentes perfiles, administrador, operador, monitorización,...
- El acceso remoto a los sistema debe ser con mínimo privilegio.
- Sólo permitir protocolos seguros de conexión remota como SSH2
- Establecer políticas de password complejas alineadas con las del resto de la compañía
- Restringe el acceso al equipo desde el segmento específico de administración y para determinados IP/equipos.
- Activa la auditoría (loggin) en el dispositivo y configúralo para que pueda enviar la información al SOC, para que pueda vigilar los comportamientos anómalos.
- Establece un tiempo de inactividad de las sesiones de administrador.
- Las password almacenadas en el dispositivo estarán cifradas.
- Limita el número de intentos en la autenticación, con el fin de evitar los ataques de fuerza bruta.



- Mantén actualizado el software del dispositivo.
- Incluye al dispositivo en el procedimiento de copias de seguridad. Realizando copias de seguridad de la configuración de manera periódica, para poder recuperara la operatividad del dispositivo de manera rápida en caso de desastre.
- Habilitar únicamente los protocolos de enrutamiento que se estén utilizando.

SNMP es un protocolo de recopilación de información acerca del dispositivo. Existen diferentes herramientas que permiten auditar la configuración de este protocolo utilizado en los router. Como son smpccheck, snmpwalk, snmpget, módulos específicos de metasploit (snmp-scan),...

### 5.3.- PROXY

Un proxy es un dispositivo colocado entre los equipos de nuestra red e Internet. Este dispositivo intermedio permite analizar el tráfico intercambiado y en base a reglas definidas permitir o no la conexión. Además este dispositivo es el que identifica el servidor al que nos conectamos como solicitante, lo que permite anonimizar al solicitante original. Se trata de un dispositivo que trabaja a nivel de aplicación. Los proxies pueden trabajar específicamente con diferentes protocolos: SNMP, POP, POP3, FTP, HTTP,...

Existe 2 tipos de arquitecturas para este servicio.

- Disponer de un proxy central al que se conectan todos los usuarios de la red. Esto permite tener una política común para toda la compañía.

- Externalizar el servicio hacia un proveedor que controle este componente de la seguridad de nuestro sistema.

Son los denominados proxy en nube.

Desde el punto de vista de la seguridad proporcionan control , anonimización y vigilancia de las conexiones.

Muchos de los proxies tiene capacidades para incluir listas de IOCs en sus dispositivos con el objetivo de impedir la conexión contra estas IPs y dominios.

Una de las características que debemos activar en el proxy es la vigilancia del dispositivo, integrando la información que se recoge en el dispositivo con el centro de operaciones de seguridad (SOC).

### 6.- MONITORIZACIÓN DE SISTEMAS Y DISPOSITIVOS.

Caso práctico

Los administradores del servidor se ha quejado al director de seguridad por el bloqueo de PowerShell en el entorno. Después de varias reuniones finalmente se aprobó el uso de PowerShell en el entorno. Ahora se necesita vigilar su uso para saber cómo se está utilizando. Durante un mes se investiga si se detecta algún evento sospechosos que relacionado con la activación.

Identifica el ID que visualiza evento de powershell que pueden detectar su uso.

Powershell: ID de evento Evento 400 y 800 para el Event Viewer de Windows.

La monitorización del sistema debe de estar dimensionada a los recursos que se destinen a esta tarea, ya que no por tener más dispositivos monitorizados es más efectivo, si no se dispone de personal que permita tratar las alertas y la información.

Muchos de los sistemas de monitorización están automatizando el tratamiento de los incidentes más comunes a través de los SOAR.

La primera tarea de la monitorización de sistemas consiste en la configuración de los dispositivos y software para que realice un registro de las actividades realizadas y que permita detectar actividades maliciosas e intrusiones. Todas las fuentes de información pueden proporcionar información relativa a la seguridad, pero los dispositivos relacionados con la seguridad son las que aportan información más específica. Por lo que debemos centrarnos en estos dispositivos.

Ejemplo. Configuración de "logging" en un firewall de Checkpoint.

Debemos tener en cuenta que los dispositivos de seguridad de nuestro sistema son los que están más directamente relacionados con la información más relevante y crítica de seguridad, ya que son dispositivos de control hacia los elementos más críticos.

Tradicionalmente la monitorización se centraba sólo en los dispositivos más críticos, pero actualmente lo que se intenta es abordar los incidentes para su detección en una fase más temprana de la Kill-Chain de los atacantes, por lo que el concepto de EDR ha cobrado mucha importancia a la hora de poder reaccionar y resolver un incidente de manera rápida. Por lo que la monitorización y la búsqueda de artefactos están recayendo en estas herramientas y es uno de los requisitos de bastionado de la red, que se pueda activar la monitorización de los elementos del sistema.

Los sistemas de monitorización también tienen que estar configurados de manera segura, ya que los atacantes intentarán desactivar estos mecanismos para que los métodos de defensa se desactiven y no permitir que la información de seguridad llegue al SOC y los equipos DFIR puedan responder al ataque. Por lo tanto se establecerán reglas de detección de la desactivación de la monitorización o la falta de información usual de la misma.

A continuación se muestra una imagen con las múltiples fuentes de información que podría tener un SIEM, para que fueran tratadas a través de la correlación y obtener de ese proceso las alertas y avisos de seguridad.

## 7.- SIEMs

### Caso práctico

Un equipo de SOC utiliza como herramienta un SIEM para monitorizar el sistema de amenazas. Como analista de seguridad tenemos que aprender a priorizar los incidentes según su criticidad. Empezando por los niveles más críticos a los más bajos. Las herramientas de monitorización correctamente configuradas nos facilitan las tareas de reducir las amenazas a detectarlas y gestionarlas en menos tiempo.

Los analistas de seguridad juegan un papel muy importante en la investigación de incidentes, analizando y comprendiendo cómo funciona el ataque y cómo pararlo. Durante la investigación, como analistas tenemos que preguntarnos el ¿Cómo? ¿Cuándo? ¿por qué? y encontrar las respuestas dentro de los logs.

¿Qué acciones tomarías para mejorar la resolución de una alerta?

Analiza: Haz uso de tu experiencia y utiliza herramientas que te ayuden analizar los datos (IA, Big Data). En cada incidente ayuda a entender el funcionamiento de la red, y apóyate en la documentación del sistema.

Propón mejoras para que no se vuelvan a producir los incidentes o falsos positivos.

Un SIEM es un dispositivo que recoge información de diversas fuentes de manera centralizada y que relaciona esta información de las diferentes fuentes para detectar anomalías de seguridad en el sistema: usuarios que inician sesión desde IPs no conocidas, fuera de horario, desde dos IPs distintas en un corto periodo de tiempo (viaje imposible),....

El SIEM está en continua aprendizaje y mejora, por lo que muchas veces se detectan anomalías que en realidad son comportamientos legítimos, en ese caso es necesario implementar las excepciones para que este "falso positivo" no se vuelva a producir, ya que este tipo de evento consumen recursos de nuestro servicio de SOC que podríamos destinar a eventos que realmente tienen importancia.

Por lo tanto, el SIEM es el dispositivo central del SOC que recopila toda la información de las diferentes fuentes y en base a reglas de seguridad y análisis de la información, proporciona alertas de seguridad.

Este método de seguridad es reactivo y ante estas alertas de seguridad se debe establecer el procedimiento de actuación en base a los SOP (Security Operation Playbook).

Dentro del ciclo de gestión de incidentes, las fases que tiene que ver directamente con el SIEM son:

1. Dentro de la fase de configuración de los dispositivos de seguridad de nuestra infraestructura: antivirus, EDR, proxy, firewalls, IDS / IPS, etc, debemos configurar la auditoría de estos dispositivos para que puedan enviar información al SIEM. También tendremos que aplicar al SIEM las reglas de detección de amenazas acorde al contexto de nuestra organización.
2. En la fase de detección gestionaremos las alertas de seguridad y realizaremos las investigaciones que sean necesarias para encontrar el origen de la alerta.
3. Una vez que se ha resuelto el ataque aplicaremos las lecciones aprendidas a la mejora del sistema y que el ataque vuelva a ocurrir otra vez. Esto nos permitirá indicar a los administradores del sistema si necesitamos mejorar las vulnerabilidades del sistema para aplicar nuevas medidas de configuración segura o disponer de más recursos económicos y humanos.

Existen diferentes productos en el mercado que nos permiten implementar nuestro SIEM en el sistema. Algunos de estos productos son de libre distribución y requieren de un mantenimiento y actualización por parte del personal interno de la organización, aunque también existe la posibilidad de adquirir un producto con licencia que tenga el apoyo y soporte de un equipo externo especializado.

- SIEM recomendados por CCN
- SELKS
- Splunk
- Security Onion
- Elastic SIEM

Muchas empresas de ciberseguridad están ofreciendo este servicio a las empresas para que puedan externalizarlo y delegar la detección de amenazas a empresas especializadas. Aunque es necesario la implicación de la empresa en los mecanismos de reacción cuando se produce un incidente, de tal manera que los protocolos de actuación permitan detener el ataque.

## 8.- SOLUCIONES DE CENTROS DE OPERACIÓN DE RED, Y CENTROS DE SEGURIDAD DE RED: NOCS Y SOCS.

### Caso práctico

En los últimos años y a medida que los ciclos de desarrollo se han hecho más complejos y el software evoluciona en ciclos tecnológicos más cortos se acumulan errores funcionales y fallos de seguridad, muchos sin resolver. Los administradores acumulan tareas y presión y se genera desconfianza con el software y sus dispositivos. Esta presión acaba en las personas y las fricciones entre los equipos de IT y seguridad.

La resolución de problemas de seguridad de los dispositivos se ha convertido en la causa principal de incidentes de seguridad.

Delimitar las tareas del equipo de seguridad y los operadores de equipos no ayudan a repartir las tareas asociadas a la seguridad y eliminar fricciones.

Vamos a llevarnos bien: Debemos establecer una matriz de responsabilidades donde la operación del dispositivo debe ser responsabilidad NOC. El NOC es el responsable de recoger la información que ayude de operaciones y proporcionar información al SOC para ayudarlo en la seguridad. Las indicaciones precisas de lo que se debe hacer ante un incidente de seguridad son del SOC. Además, cuando existe un incidente de seguridad el SOC debe establecer las prioridades, pero estas acciones no deben tomarse sobre la marcha, sino que tienen que ser entrenadas previamente en ejercicios de simulación.

Una vez implementadas las medidas de seguridad preventivas para los sistemas, las tareas de seguridad no finalizan en este punto, sino que requieren de un mantenimiento y mejora continua. Esto se logra con tareas de mejora y revisión de la seguridad de manera periódica. Pero otro de los pilares básicos de la seguridad es la vigilancia de dichos sistemas. Esto se logra con la monitorización de los sistemas.

Debido al incremento de sistemas y de información que recopilamos acerca de su funcionamiento y uso. Se crean los centros de operaciones de seguridad (SOC o CyOC). Son centro con servicios relativos a la seguridad que suelen operara en tiempos de 24x7 o 8x5, dependiendo de la criticidad del sistema y de los recursos que podamos invertir. El otro centro de control de las operaciones del sistema es el Network Operation Center (NOC) que se encarga de gestionar la disponibilidad de la red. Muchas de las herramientas utilizadas en el SOC y el NOC son comunes. Aunque el objetivo de su uso suele ser distinto.

La dimensión de la disponibilidad relativa a la seguridad está siendo uno de los elementos comunes entre el NOC y el SOC, de ahí que deban ser complementarios. Ej: Un incidente de DDoS. Aunque los objetivos son diferentes ya que en el NOC la prioridad es el funcionamiento, en el SOC es mantener el nivel de seguridad del sistema.

El SOC (Centro de Operaciones de Seguridad) es una unidad centralizada y servicio interno del sistema de una organización donde se monitorean, evalúan y defienden los sistemas de información de una empresa.

Típicamente tiene herramientas para monitorizar la red, gestionar incidentes y reaccionar ante diferentes eventos.

Estos centros tienen como misión detectar actividades anómalas que deriven en la creación y tratamientos de incidentes de seguridad, para que los sistemas no se vean dañados por las amenazas externas que deriven en fugas de información o robo, inoperatividad del sistema o destrucción de la información.

Para el funcionamiento de los SOC es necesario recopilar información de los sistemas y de la red que lo soportan.

Algunos ejemplos de fuentes de información (logs) útiles que deben ser centralizados en un punto común para posteriormente darle tratamiento: logs de firewalls, logs de DNS, logs DHCP, logs de acceso al sistema,...

Toda esta información es centralizada en un único punto, y mediante herramientas como los SIEM se normalizan y se correlacionan.

El proceso de normalización conlleva a unificar todos los datos de las diferentes fuentes de información que son enviados en diferentes formatos, para posteriormente poder realizar búsqueda de anomalías en relación a los sistemas.

El SIEM además puede añadir información adicional a la información recopilada por las fuentes que pueda ayudar a procesar y detectar de una manera más eficiente la búsqueda de anomalías.

El SOC al ser un servicio de seguridad, concentra multitud de tareas:

- Gestión de registros
- Gestión de vulnerabilidades. Únicamente parte de detección y estado del sistema.
- Análisis de malware
- Threat Hunting
- Threat Intelligence (Inteligencia)
- Generación de informes técnicos y ejecutivos.
- Ejercicios de defensa.

Los integrantes del SOC son también denominados como personal del equipo de blue team.

Hay personal especializado dentro del equipo que se encarga de tareas forense, análisis de malware, threat intelligence, threat hunting,...

Las fases de una gestión de incidentes se pueden resumir en el siguiente diagrama de estados

- **Preparación y prevención**

Es la fase en la que se crea y se forma al Equipo de Respuesta a Ciberincidentes (ERC) y la utilización de herramientas y recursos necesarios, identificando y desplegando las medidas de seguridad que hayan determinado de acuerdo con un análisis de riesgos.

- **Identificación**

En esta fase se detectan los ciberincidentes que pueda sufrir la organización a partir de las medidas de seguridad implantadas, desencadenando procesos de notificación.

- **Contención**

Esta fase tiene lugar para reducir y abordar las consecuencias directas del ciberincidente de una manera rápida y efectiva impidiendo la propagación, estableciendo las acciones necesarias que permitan recoger evidencias forenses.

A través del triaje del ciberincidente se evalúa la importancia e impacto en base a la información de la que se dispone en dicho momento. Además, se contempla el proceso para realizar la comunicación interna y externa sobre este tipo de ataques.

- **Mitigación**

El propósito de esta fase es la eliminación del incidente. Esta fase se compone de acciones inmediatas como desconexiones, controles de acceso, revisiones, etc.; y de acciones a posteriori como gestión de actualizaciones, cambios de infraestructura, etc.

- **Recuperación**

Devolver a la normalidad los sistemas afectados para retomar la actividad priorizando los sistemas más críticos para el negocio y, aplicar las medidas de seguridad que eviten la repetición del ciberincidente. Además, se establece cómo debe ser la comunicación para la vuelta a la normalidad de los afectados.

- **Post-Incidente**

Se lleva a cabo el proceso de registro de todo el ciberincidente: trazabilidad, escalado y notificación, actuaciones y lecciones aprendidas.

La gestión de incidentes permitirá realizar una mejora en el proceso de monitorización de sistema ante nuevos ataques.

#### Autoevaluación I

¿En qué protocolo nos apoyamos para darle seguridad al servicio de correo electrónico?

- a. NTP
- b. DNS
- c. HTTP

#### Autoevaluación III

¿Qué amenazas nos ayuda a detectar un firewall tradicional?

- a) Virus
- b) Phishing
- c) Enlaces con IPs maliciosas

#### Autoevaluación II

¿Sólo es necesario tener un firewall para defender perimetralmente una red?

- a) Verdadero
- b) Falso

#### Autoevaluación IV

Administrarías el firewall de tu sistema a través de la web que viene por defecto es totalmente seguro.

- a) Verdadero
- b) Falso

#### TEST I

1-Cuál es el orden secuencial correcto en el tratamiento de un log antes de que llegue al SIEM

- a) Envío, extracción y parseo
- b) Parseo, extracción y envío
- c) Extracción, envío y parseo

2- Qué ataque de denegación de servicios, DoS, se aprovecha del protocolo TCP de inicio de conexión de 3 vías (handshake).

- a) Syn Flooding
- b) IP Spoofing
- c) Ping de la muerte

3- Durante el proceso de almacenamiento de logs, ¿qué es el parseo?

- a) Un procedimiento para añadir información al log
- b) El proceso de envío cifrado de logs al servidor central de información.
- c) Proceso por el que se extrae la información útil de los logs de cada una de las fuentes

4- Qué fase del almacenamiento de los logs es el más crítico para poder posteriormente realizar búsqueda de manera rápida y eficiente:

- a) Parseo
- b) Indexado
- c) Reenvío

5- Reducir el tiempo de inoperatividad de un firewall es responsabilidad del

- a) Seguridad física
- b) Soc
- c) NOC

6- Las herramientas antiAPT no necesitan actualizarse. ¿Verdadero o falso?

- a) Verdadero
- b) Falso

7- ¿Quién puede ayudarnos en la protección de los ataques de DoS/DDOS?

- a) ISP
- b) AEPD
- c) ENISA

8- Los logs de los diferentes dispositivos de una red tienen diferentes formatos, cantidad de información y número de campos ¿Verdadero o falso?.

- a) Verdadero
- b) Falso

9- Qué protección aplica las mejoras prácticas de seguridad de SPF y DKIM:

- a) OSPF
- b) DMARC
- c) NTLM

10- El SIEM es una herramienta de seguridad:

- a) Nula
- b) Reactiva
- c) Proactiva

## TEST II

- 1- De las siguientes alternativas, qué parte de un SOC es necesario tener en cuenta para que esté bien dimensionado:
  - a) La planta en la que esté situado
  - b) El número de recursos humanos que dispone
  - c) La ciudad donde se aloje
- 2- El protocolo SNMP permite obtener información de un dispositivo de la red. ¿Qué versión del protocolo es considerada segura?
  - a) v3
  - b) v1
  - c) v2
- 3- ¿Qué mecanismo complementario necesitan los atacantes para infectar los equipos de los usuarios?
  - a) El Blockchain
  - b) Ingeniería social
  - c) Los medios de comunicación
- 4- Si una de las alertas que se ha producido en el SIEM finalmente no corresponde a un incidente se denomina:
  - a) Falsa alarma
  - b) Error de búsqueda
  - c) Falso positivo
- 5- Las herramientas de almacenamiento de logs tiene que dimensionarse en base a:
  - a) Cantidad de fuentes
  - b) Tamaño y formato de los logs
  - c) Todas son correctas
  - d) Tiempo de retención
- 6- ¿Cuál es uno de los principales vectores de entrada en el sistema y objetivo de los atacantes?
  - a) SIEM
  - b) Equipos de los usuarios
  - c) Infraestructura en la nube (IaaS)
- 7- ¿El personal de un NOC tiene que tener visibilidad de las alertas del SIEM?. ¿Verdadero o falso?
  - a) Verdadero
  - b) Falso
- 8- ¿Qué es un SOAR?
  - a) Sistema automático de tratamiento de incidentes más comunes
  - b) Dispositivo de red
  - c) Antivirus de última generación
- 9- Ante un incidente que deriva en un resultado de falso positivo no es necesario hacer nada sobre el SIEM o el dispositivo que la genera. ¿Verdadero o falso?.
  - a) Verdadero
  - b) Falso
- 10- ¿Qué información puede ser de utilidad a la hora de diseñar reglas de filtrado en el servicio de correo electrónico?
  - a) Cabeceras
  - b) Firma del correo
  - c) El idioma en el que está escrito

## Soluciones:

Autoevaluación I: b)

Autoevaluación II: b)

Autoevaluación III: c)

Autoevaluación IV: b)

TEST I 10/10: 1 c), 2 a), 3 c), 4 b), 5 c), 6 b), 7 a), 8 a), 9 b), 10 b)

TEST II 10/10: 1 b), 2 a), 3 b), 4 c), 5 c), 6 b), 7 b), 8 a), 9 b), 10 a)

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 (archivo - [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:

Necesitamos:

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

Relativo al ataque web, debemos identificar ([archivo 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 (archivo - [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 →  | 10.16.54.6:19532 | 2       | 58    |
| 3  | 2007-02-24 04:55:06.552 | 15.202   | UDP   | 84.77.114.176:57024 →  | 10.16.54.6:18278 | 2       | 58    |
| 4  | 2007-02-24 04:54:54.806 | 13.998   | UDP   | 84.77.114.176:57024 →  | 10.16.54.6:31991 | 2       | 58    |
| 5  | 2007-02-24 04:54:52.434 | 96.322   | UDP   | 89.106.22.3:54606 →    | 10.16.54.6:38662 | 166     | 4814  |
| 6  | 2007-02-24 04:55:03.714 | 72.352   | UDP   | 84.77.114.176:57024 →  | 10.16.54.6:34036 | 2       | 58    |
| 7  | 2007-02-24 04:54:54.830 | 91.019   | UDP   | 213.144.110.130:3656 → | 10.16.54.6:4027  | 160     | 4640  |
| 8  | 2007-02-24 04:54:54.941 | 80.638   | UDP   | 84.77.114.176:57024 →  | 10.16.54.6:34197 | 2       | 58    |
| 9  | 2007-02-24 04:52:22.421 | 232.040  | UDP   | 207.150.178.78:1225 →  | 10.16.54.6:44569 | 213     | 6177  |
| 10 | 2007-02-24 04:53:04.149 | 160.703  | UDP   | 89.106.22.3:54606 →    | 10.16.54.6:1740  | 388     | 11252 |
| 11 | 2007-02-24 04:53:03.199 | 163.115  | UDP   | 89.106.22.3:54606 →    | 10.16.54.6:31515 | 213     | 6177  |
| 12 | 2007-02-24 04:54:54.753 | 0.000    | UDP   | 84.77.114.176:57024 →  | 10.16.54.6:29543 | 1       | 29    |
| 13 | 2007-02-24 04:54:52.944 | 73.631   | UDP   | 213.144.110.130:3656 → | 10.16.54.6:29656 | 325     | 9425  |
| 14 | 2007-02-24 04:53:05.527 | 161.315  | UDP   | 213.144.110.130:3656 → | 10.16.54.6:5150  | 335     | 9715  |
| 15 | 2007-02-24 04:54:54.954 | 68.255   | UDP   | 84.77.114.176:57024 →  | 10.16.54.6:35195 | 2       | 58    |
| 16 | 2007-02-24 04:53:30.287 | 147.940  | UDP   | 207.150.178.78:1225 →  | 10.16.54.6:40608 | 110     | 3190  |
| 17 | 2007-02-24 04:55:00.620 | 86.756   | UDP   | 84.77.114.176:57024 →  | 10.16.54.6:11034 | 3       | 87    |
| 18 | 2007-02-24 04:54:53.675 | 53.077   | UDP   | 89.106.22.3:54606 →    | 10.16.54.6:13797 | 64      | 1776  |

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'`

```

1 10.16.54.100
2 10.16.54.129
3 10.16.54.140
4 10.16.54.2
5 10.16.54.29
6 12.166.24.72
7 12.47.192.116
8 125.130.3.142
9 125.76.238.162
10 128.242.113.131
11 128.242.113.132
12 128.63.2.53
13 128.8.10.90
14 130.239.5.114
15 139.91.1.20
16 149.156.1.6
17 151.198.0.39
18 157.22.13.62
19 165.21.86.49

```

```

kali@kali:~/Desktop
$ awk '/UDP/ {print $5}' datos_conexiones.txt | awk -F ':' '{print $1}' | sort -u | uniq -c | sort -nr > ip_unicas.txt
375 ip_unicas.txt

```

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"*

```

1 116956 213.144.110.130
2 115142 207.150.178.78
3 91692 89.106.22.3
4 90229 89.106.24.78
5 83334 84.77.114.176
6 507 221.208.208.91
7 205 202.97.238.204
8 177 10.16.54.129
9 121 10.16.54.29
10 118 221.208.208.92
11 111 61.138.137.10
12 85 221.208.208.212
13 72 71.146.22.111
14 59 10.16.54.100
15 51 221.12.113.247
16 30 35.52.216.193

```

```

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

```

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 "$ip: "
    geolookup "$ip"
done < unicasip.txt

```

```

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

```

```

kali@kali:~/Desktop
$ cat geolocalizarip.sh
while read -r ip;
do
    echo -n "$ip: "
    geolookup "$ip"
done < unicasip.txt
$ sudo chmod +x geolocalizarip.sh
kali@kali:~/Desktop
$ ./geolocalizarip.sh > geolocalizarip.txt

```

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

```

```

Bulk mode: whois.cymru.com [2025-02-15 19:20:20 +0000]
1 25145 | 213.144.110.130 | AS-TEKNOTEL Teknotel Telekomunikasyon A.S., TR
2 25019 | 207.150.178.78 | SAUDINETSTC-AS, SA
3 834 | 89.106.22.3 | IPKO, US
4 834 | 89.106.24.78 | IPKO, US
5 12479 | 84.77.114.176 | UN12-AS, ES
6 4837 | 221.208.208.91 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
7 4837 | 202.97.238.204 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
8 NA | 10.16.54.129 | NA
9 NA | 10.16.54.29 | NA
10 4837 | 221.208.208.92 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
11 4837 | 61.138.137.10 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
12 4837 | 221.208.208.212 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
13 7018 | 71.146.22.111 | ATT-INTERNET4, US
14 NA | 10.16.54.100 | NA
15 4837 | 221.12.113.247 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
16 16509 | 35.52.216.193 | AMAZON-02, US
17 NA | 72.30.177.83 | NA
18 NA | 74.6.86.121 | NA
19 12302 | 62.121.117.72 | VODAFONE_RO Charles de Gaulle nr.15, RO
20 NA | 10.16.54.2 | NA
21 4766 | 220.73.220.4 | KIXS-AS-KR Korea Telecom, KR
22 5617 | 217.98.63.167 | TPNET, PL
23 3257 | 213.254.204.197 | GTT-BACKBONE GTT, US

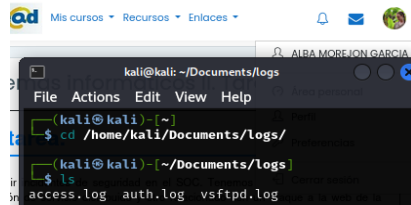
```

## Incidente de ataque a la web de la compañía

Relativo al ataque web, debemos identificar (**fichero logs.zip**):

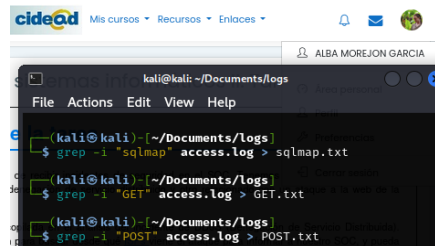
- Las herramientas ofensivas utilizadas por los atacantes
- Las páginas web sobre las que han realizado el ataque
- Usuarios utilizados en cada uno de los servicios atacados
- Ficheros descargados

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

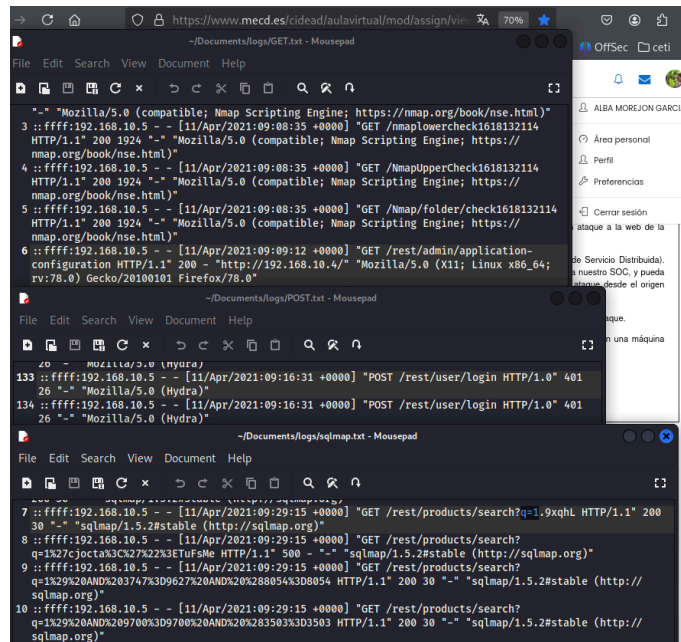


Vamos a empezar a analizar el primer fichero, el access.log.

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>)"

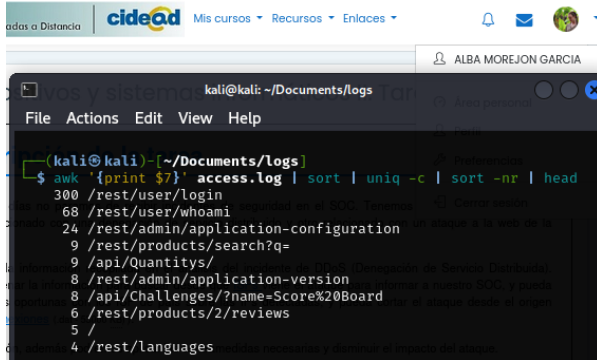
- Feroxbuster: identificado por el user-agent:

"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:

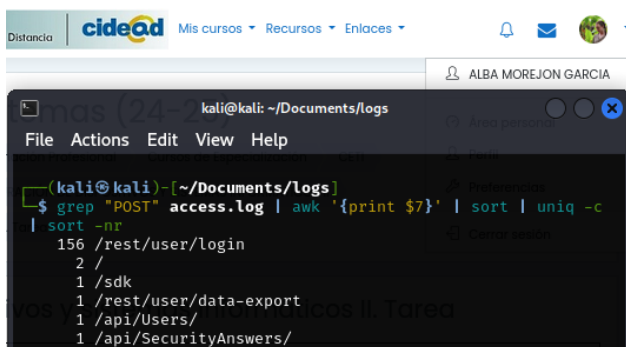
- Nmap: identificado en el user-agent:

"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/Quantities/`
- `/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`

```

(kali@kali)-[~/Documents/logs]
$ grep "Failed password" auth.log | awk '{print $11}' | sort | uniq -c | sort -nr
98 192.168.10.5

(kali@kali)-[~/Documents/logs]
$ 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 LOGIN" vsftpd.log` vemos los intentos de inicio de sesión.

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

```

(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 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 08:16:07 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 "?"
  
```

```

(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:
  - o /www-data.bak (2602 bytes)
  - o /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.baky /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.baky/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.