**Informe de Práctica: Blue Team**

**1. Introducción**

En esta práctica, configuramos un entorno de red segregado utilizando **pfSense** como firewall y gestor de conexiones, además de configurar servicios en distintas zonas, como un honeypot en la DMZ y un servidor Apache en DMZ2. También implementamos la captura y envío de logs mediante **Filebeat** hacia **Elasticsearch** y **Kibana**, alojados en la máquina host. Este informe detalla los pasos, configuraciones y pruebas realizadas.

**2. Topología de la Red**

2.1 Descripción de la Topología

WAN: Red externa (Internet).

LAN: Red interna, donde se encuentra la máquina host que ejecuta Elasticsearch y Kibana.

DMZ: Zona desmilitarizada donde se ha implementado un honeypot (Cowrie).

DMZ2: Segunda DMZ donde se ha configurado un servidor Apache.

Incluye un diagrama de la topología de red (la imagen que previamente mostraste de la infraestructura con pfSense, Elastic Cloud, WAN, LAN, DMZ y DMZ2).

**3. Configuración de pfSense**

3.1 Configuración de Interfaces

Configura las interfaces para WAN, LAN, DMZ y DMZ2 en pfSense, asignando correctamente las direcciones IP.

WAN: 192.168.1.27/24

LAN: 192.168.100.1/24

DMZ: 192.168.200.1/24

DMZ2: 192.168.250.1/24

Captura:



3.2 Políticas de Conexión (Firewall Rules)

En esta sección, se describen las reglas de firewall configuradas en pfSense para permitir la comunicación adecuada entre las diferentes zonas de la red, incluyendo WAN, LAN, DMZ y DMZ2. A continuación se detallan las reglas establecidas:

Reglas en WAN

1. **Permitir respuestas de ICMP desde WAN hacia LAN, DMZ y DMZ2.**
   * **Protocolos:** IPv4 ICMP
   * **Descripción:** Esta regla permite que las respuestas de ICMP, como los pings, se envíen de la red WAN a las redes LAN, DMZ y DMZ2.
2. **Permitir tráfico SSH al honeypot.**
   * **Protocolos:** IPv4 TCP
   * **Puerto de destino:** 222
   * **Descripción:** Esta regla permite el acceso SSH al honeypot configurado en la DMZ, facilitando la gestión y el monitoreo.
3. **NAT (Network Address Translation)**
   * **Descripción:** Se utiliza para redirigir el tráfico de la WAN a la DMZ, asegurando que las solicitudes se dirijan correctamente al servidor en la DMZ.

Reglas en LAN

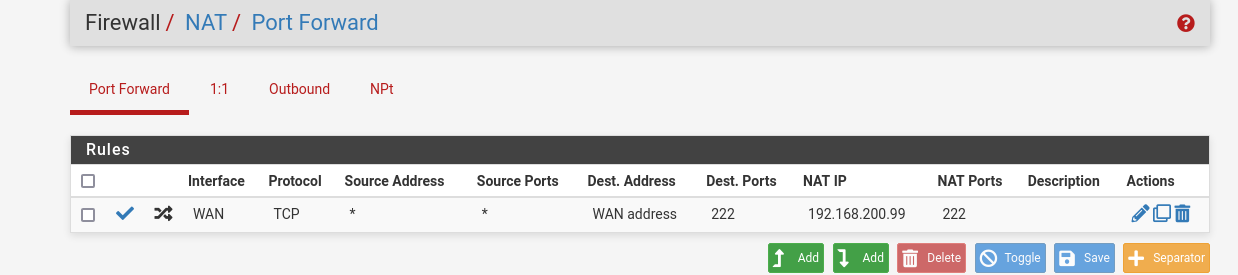
1. **Permitir tráfico ICMP desde LAN hacia WAN.**
   * **Protocolos:** IPv4 ICMP
   * **Descripción:** Esta regla permite que las solicitudes de ping desde la LAN sean respondidas.
2. **Permitir tráfico hacia Elastic.**
   * **Protocolos:** IPv4 TCP
   * **Puerto de destino:** 9200
   * **Descripción:** Permite que los dispositivos en la LAN envíen logs hacia Elasticsearch, asegurando que los datos de monitoreo lleguen al sistema de gestión.

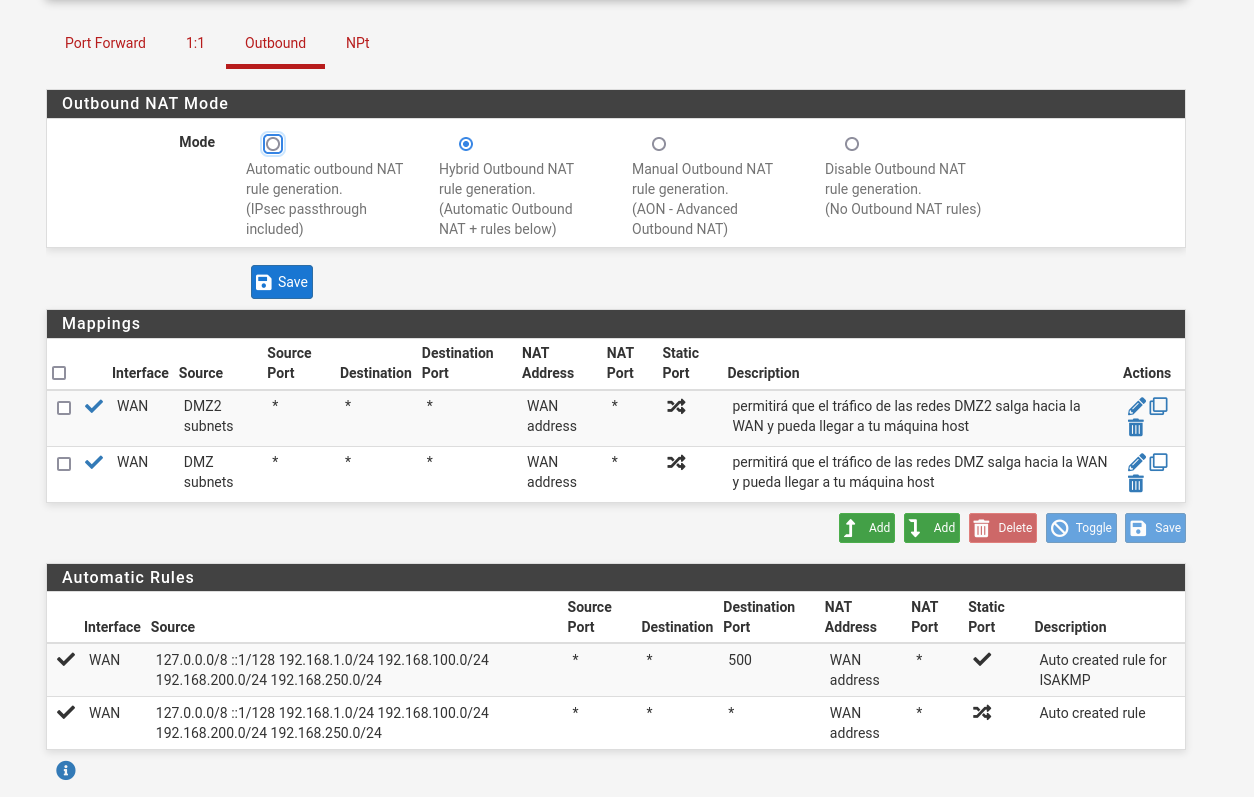
Reglas en DMZ

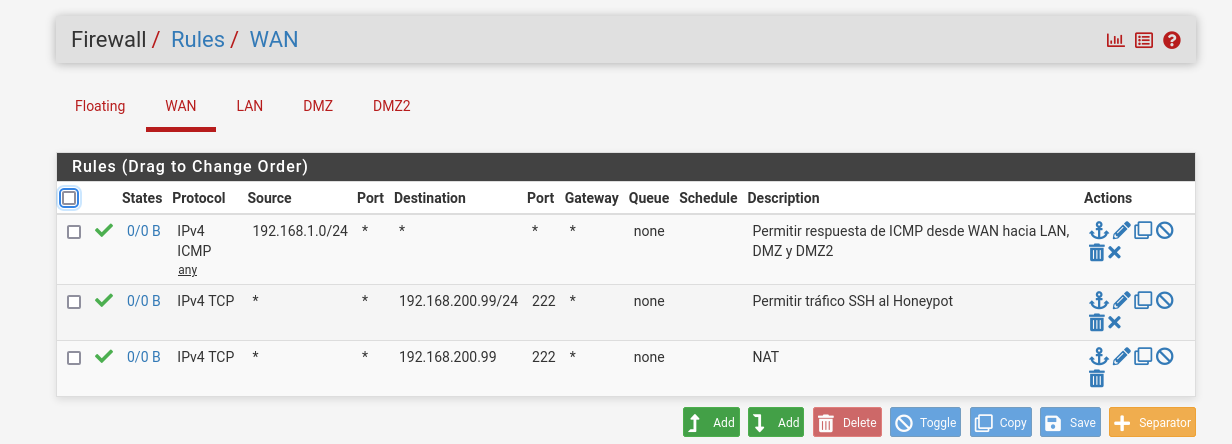
1. **Permitir ICMP desde DMZ hacia WAN.**
   * **Protocolos:** IPv4 ICMP
   * **Descripción:** Esta regla permite que las solicitudes ICMP desde la DMZ sean respondidas en la WAN.
2. **Permitir tráfico de logs desde DMZ hacia Elastic.**
   * **Protocolos:** IPv4 TCP/UDP
   * **Puerto de destino:** 9200
   * **Descripción:** Facilita el envío de logs generados por los servicios en la DMZ al sistema de gestión centralizado en Elasticsearch.
3. **Bloquear tráfico entre DMZ y LAN.**
   * **Protocolos:** IPv4
   * **Descripción:** Esta regla evita que el tráfico fluya entre la DMZ y la LAN, aumentando la seguridad al limitar la exposición de la LAN a posibles amenazas desde la DMZ.

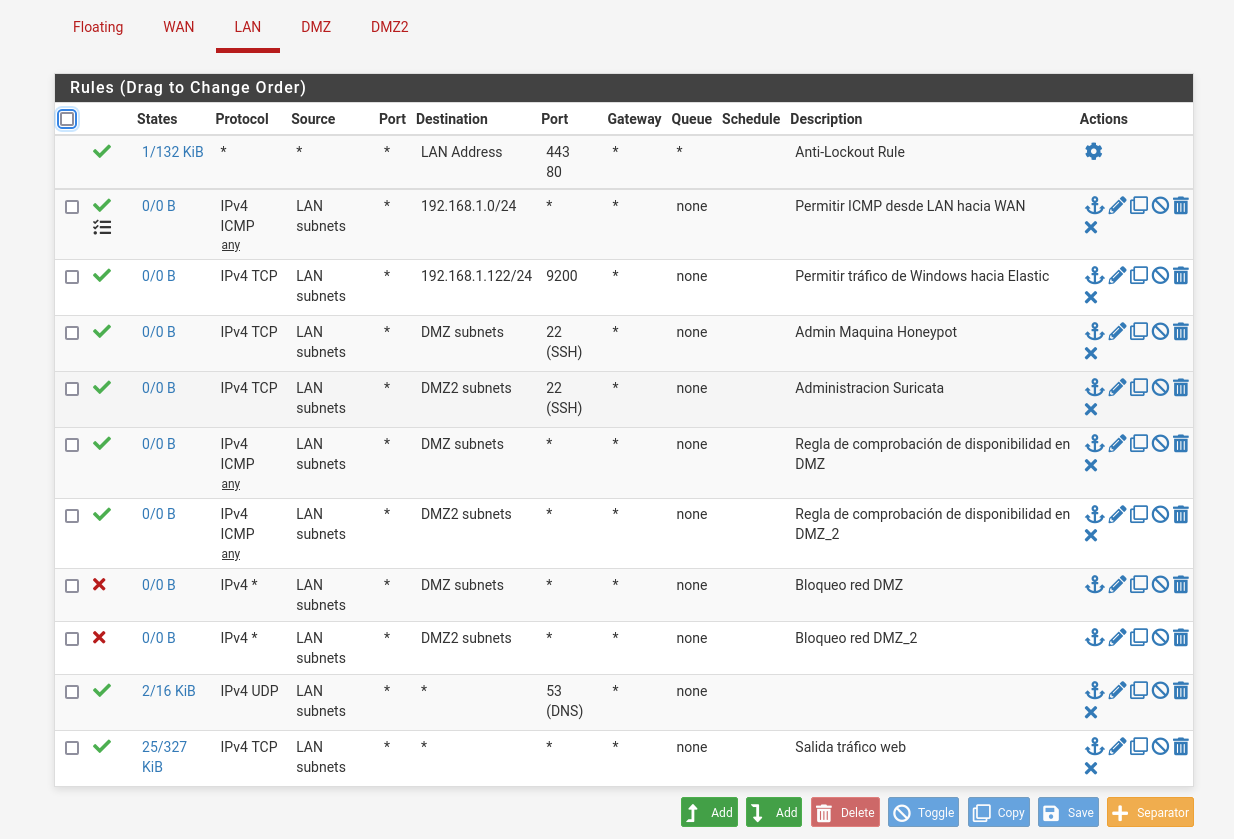
Reglas en DMZ2

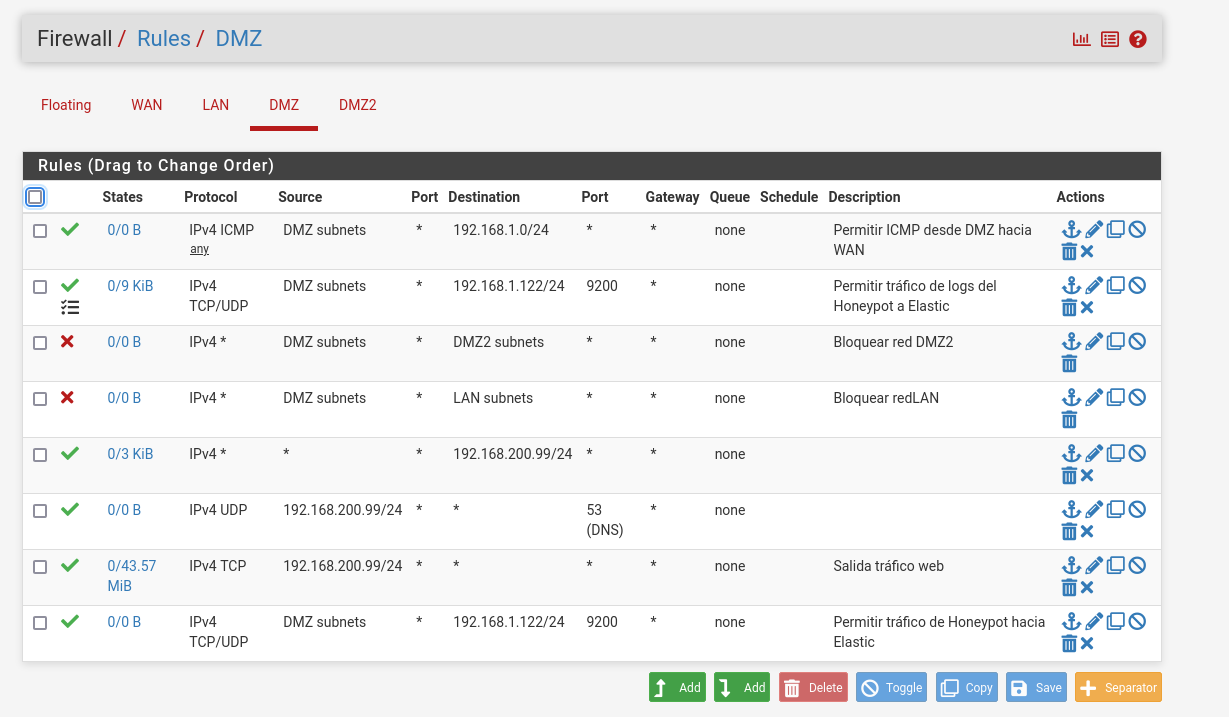
1. **Permitir ICMP desde DMZ2 hacia WAN.**
   * **Protocolos:** IPv4 ICMP
   * **Descripción:** Permite que las solicitudes de ping desde la DMZ2 sean respondidas.
2. **Permitir tráfico hacia Elastic desde DMZ2.**
   * **Protocolos:** IPv4 TCP
   * **Puerto de destino:** 9200
   * **Descripción:** Asegura que los logs generados por Apache en la DMZ2 se envíen a Elasticsearch.
3. **Permitir tráfico HTTP desde WAN hacia DMZ2.**
   * **Protocolos:** IPv4 TCP
   * **Puerto de destino:** 80
   * **Descripción:** Permite que las solicitudes HTTP desde la WAN lleguen a la configuración de Apache en la DMZ2, facilitando el acceso externo a los servicios web.
4. **Bloquear tráfico entre DMZ2 y LAN.**
   * **Protocolos:** IPv4
   * **Descripción:** Similar a la regla en la DMZ, esta regla evita que el tráfico fluya entre la DMZ2 y la LAN, manteniendo la seguridad de la red interna.
5. **Permitir tráfico de logs de Apache hacia Elastic.**
   * **Protocolos:** IPv4 TCP
   * **Puerto de destino:** 9200
   * **Descripción:** Asegura que los logs generados por el servidor Apache en DMZ2 se envíen a Elasticsearch para su monitoreo y análisis.

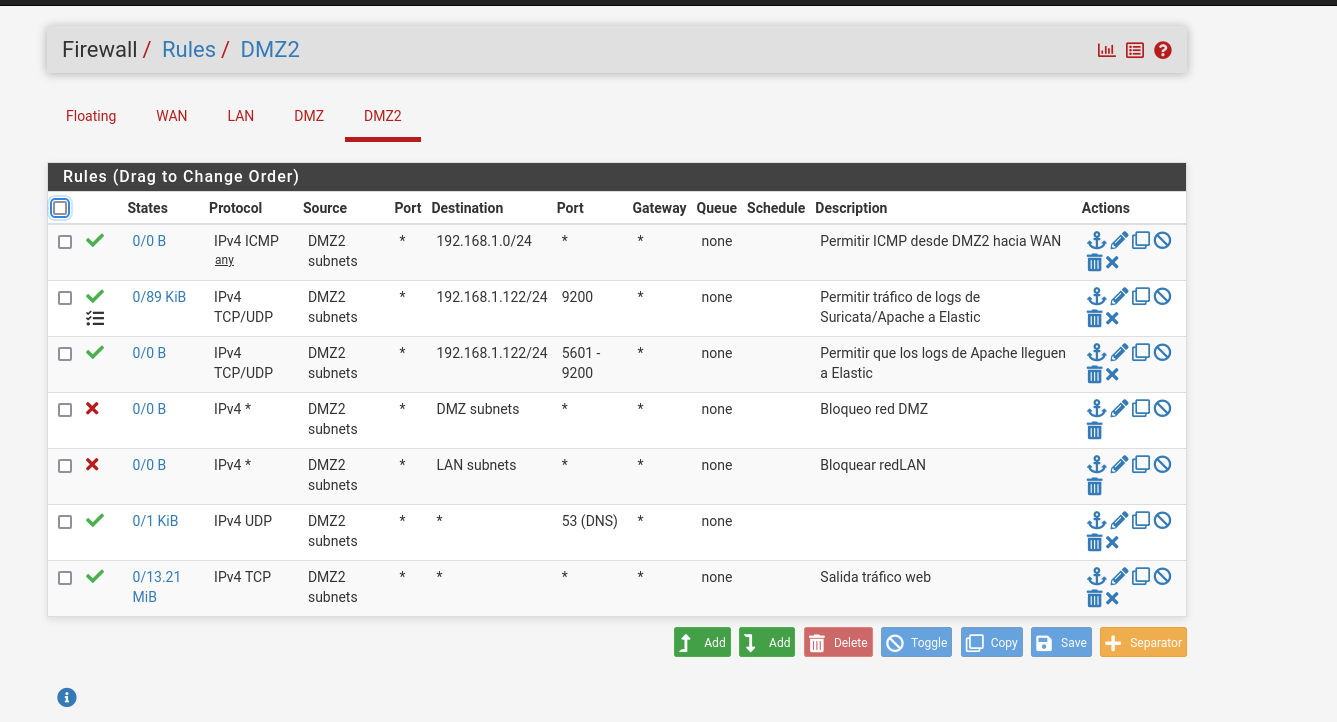
Capturas:











**4. Configuración de Cowrie (Honeypot)**

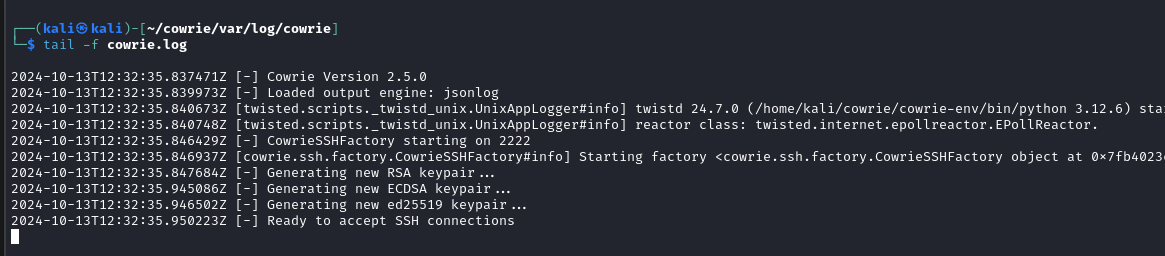
4.1 Instalación de Cowrie

Cowrie fue instalado en la máquina Kali DMZ (192.168.200.101). La instalación se realizó siguiendo los siguientes pasos:

Clonación del repositorio de Cowrie.

Configuración de Cowrie para ejecutar en el puerto SSH 2222.

Verificación del correcto funcionamiento de Cowrie.

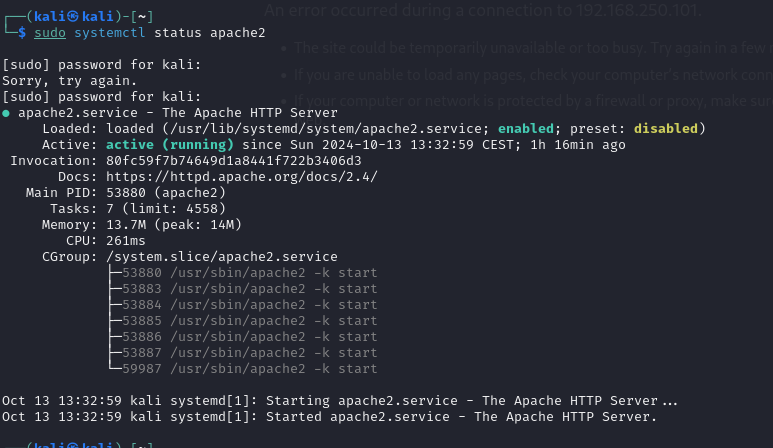
Captura:

**5. Configuración de Apache en DMZ2**

5.1 Instalación y Configuración de Apache

Se instaló Apache en la máquina Kali DMZ2 (192.168.250.101). Se configuró para servir en el puerto 80. La configuración del archivo apache2.conf se ajustó para definir el nombre del servidor (ServerName) a 192.168.250.1.

Captura:

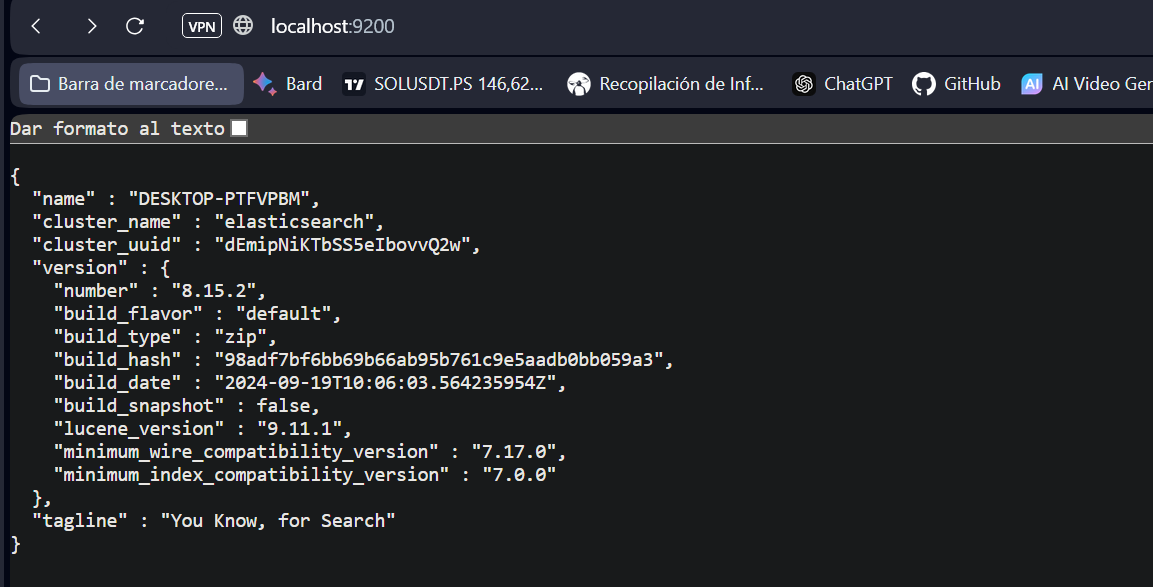
****

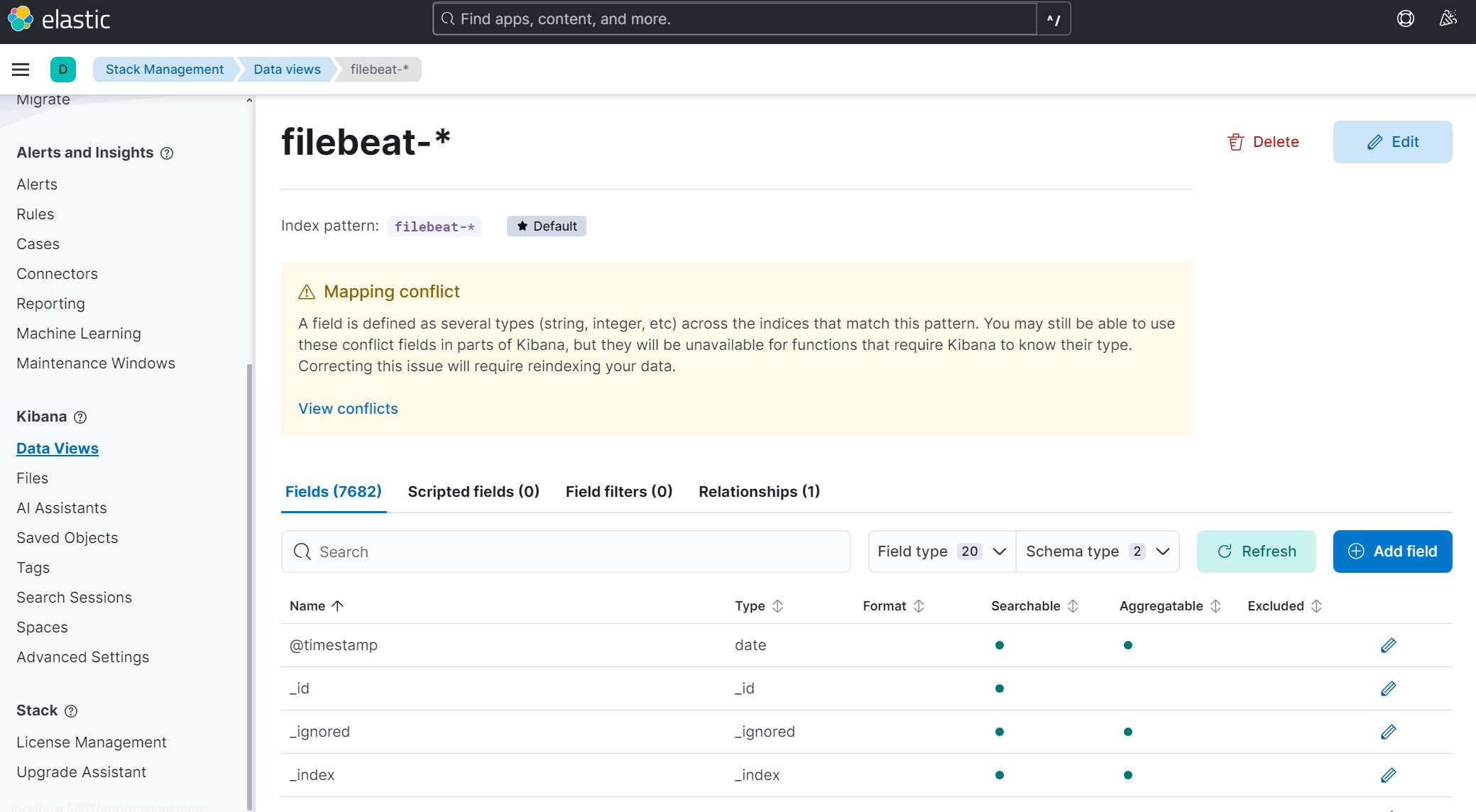
**6. Configuración de Elasticsearch y Kibana**

6.1 Instalación de Elasticsearch y Kibana

Elasticsearch y Kibana fueron instalados en la máquina host (Windows 11). Se ajustó la configuración para permitir conexiones externas y se configuró la autenticación con credenciales.

Captura:

****

**7. Configuración de Filebeat**

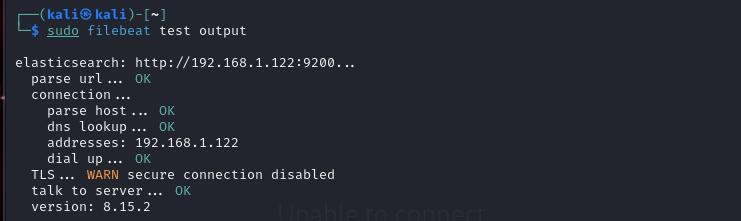
7.1 Instalación y Configuración de Filebeat  
Se instaló Filebeat en la máquina DMZ (192.168.200.101) para enviar logs desde Cowrie hacia Elasticsearch. La configuración se realizó de la siguiente manera:

Se habilitó el módulo de Apache para Filebeat:

**sudo filebeat modules enable apache**

Se editó el archivo filebeat.yml para apuntar la salida de logs a 192.168.1.122:9200, que es la dirección de Elasticsearch.

Captura:

****

**8. Logs Generados desde DMZ (Honeypot Cowrie)**

8.1 Generación de Logs  
Los logs generados por Cowrie se almacenan en el directorio /home/kali/cowrie/var/log/cowrie/. A través de Filebeat, estos logs se envían a Elasticsearch, donde pueden ser visualizados y analizados.

8.2 Visualización de Logs en Kibana  
Una vez que los logs han sido enviados a Elasticsearch, pueden ser visualizados en Kibana siguiendo estos pasos:

1. **Acceso a Kibana**  
   Ingresar a Kibana mediante el navegador en la dirección http://192.168.1.122:5601.
2. **Creación de un Data View**
   * Ir a "Stack Management" > "Kibana" > "Data Views".
   * Hacer clic en "Create data view".
   * Introducir el patrón de índices que corresponde a los logs de Cowrie (por ejemplo, filebeat-\*).
   * Guardar el Data View.
3. **Visualización de Logs**
   * Acceder a "Discover" en Kibana para explorar los logs generados por Cowrie.
   * Utilizar los filtros y opciones de búsqueda para analizar los logs específicos.

8.3 Captura de Logs Generados

A continuación, se presenta captura de los logs generados por Cowrie y enviados a Elasticsearch a través de Filebeat:

**Captura : Logs de Cowrie**  


**9 Generación de Logs DMZ2 Apache2**

Apache genera dos tipos principales de logs: access.log y error.log. Estos logs se almacenan en el directorio /var/log/apache2/ y se utilizan para registrar las solicitudes HTTP y los errores del servidor, respectivamente.

**access.log**: Registra todas las solicitudes de acceso al servidor, incluyendo la dirección IP del cliente, el código de estado de la respuesta y el tiempo de respuesta.

**error.log**: Registra errores del servidor, como fallos en la configuración o errores al procesar solicitudes.

9.1 Envío de Logs a Elasticsearch  
Para gestionar los logs generados por Apache, se configuró Filebeat en la máquina DMZ (donde se ejecuta el servidor Apache) para enviar estos logs a Elasticsearch. La configuración en el archivo filebeat.yml incluye el módulo de Apache para que Filebeat lea los logs de acceso y errores y los envíe al índice de Elasticsearch correspondiente.

Se habilitó el módulo de Apache para Filebeat:

sudo filebeat modules enable apache

Se configuró el archivo filebeat.yml para apuntar a la salida de logs hacia 192.168.1.122:9200.

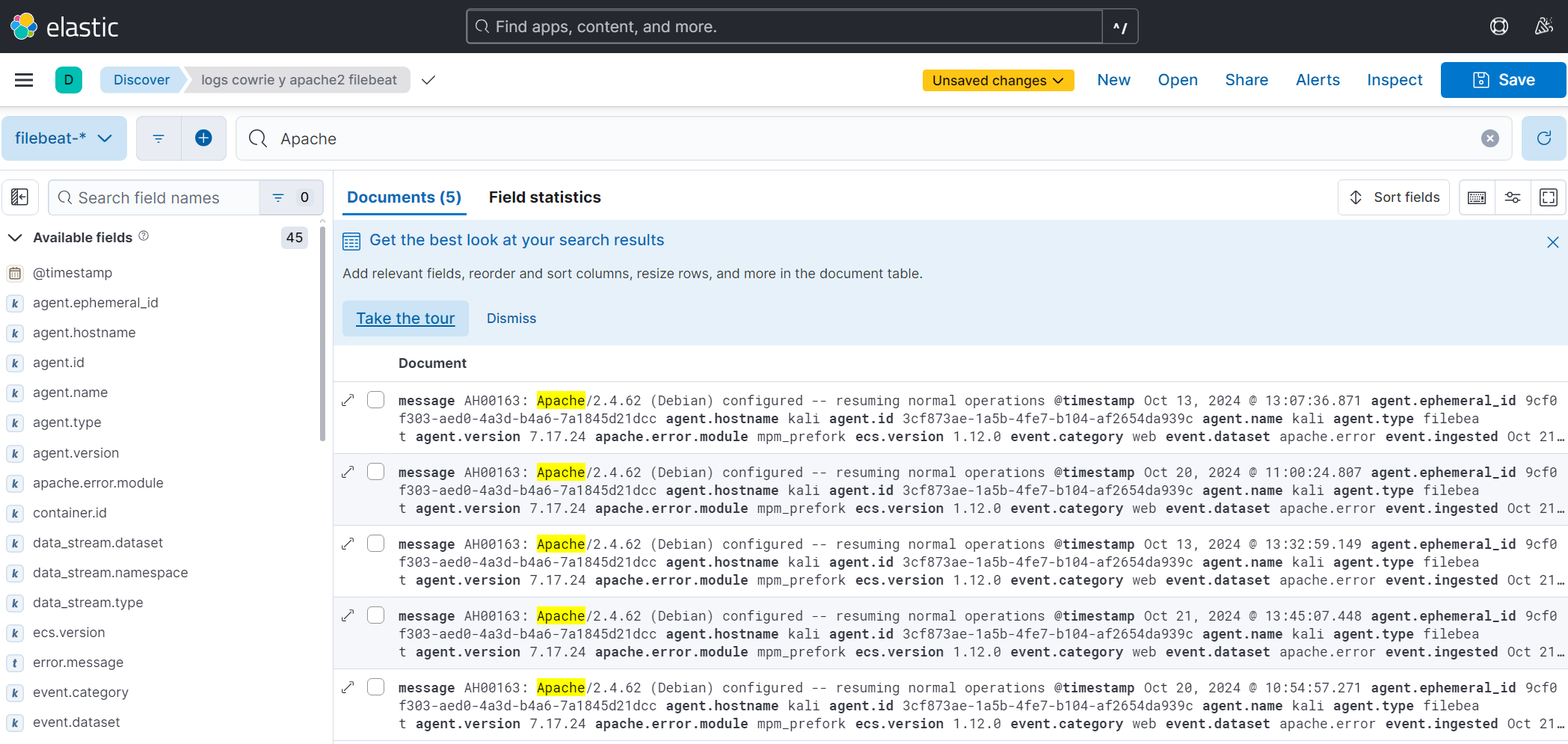
9.2 Visualización de Logs en Kibana

Los logs generados por Apache se pueden visualizar en Kibana. El proceso es el siguiente:

1. **Acceso a Kibana**  
   Ingresar a Kibana en http://192.168.1.122:5601.
2. **Creación de un Data View**
   * Navegar a "Stack Management" > "Kibana" > "Data Views".
   * Crear un nuevo Data View introduciendo el patrón de índices (por ejemplo, filebeat-\*).
   * Guardar el Data View.
3. **Visualización de Logs**
   * Ir a "Discover" para explorar los logs de Apache.
   * Aplicar filtros para analizar solicitudes y errores específicos.

9.3 Capturas de Logs Generados  
A continuación, se presenta captura de los logs generados por Apache y enviados a Elasticsearch a través de Filebeat:

**Captura : Logs de Acceso de Apache**

****

**8. Conclusión**

Este informe detalla la configuración de un entorno de red segregado utilizando pfSense, honeypots, y servidores Apache. El objetivo fue crear un entorno seguro y monitorizado, utilizando herramientas como Elasticsearch y Kibana para la recolección y análisis de logs.