**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)

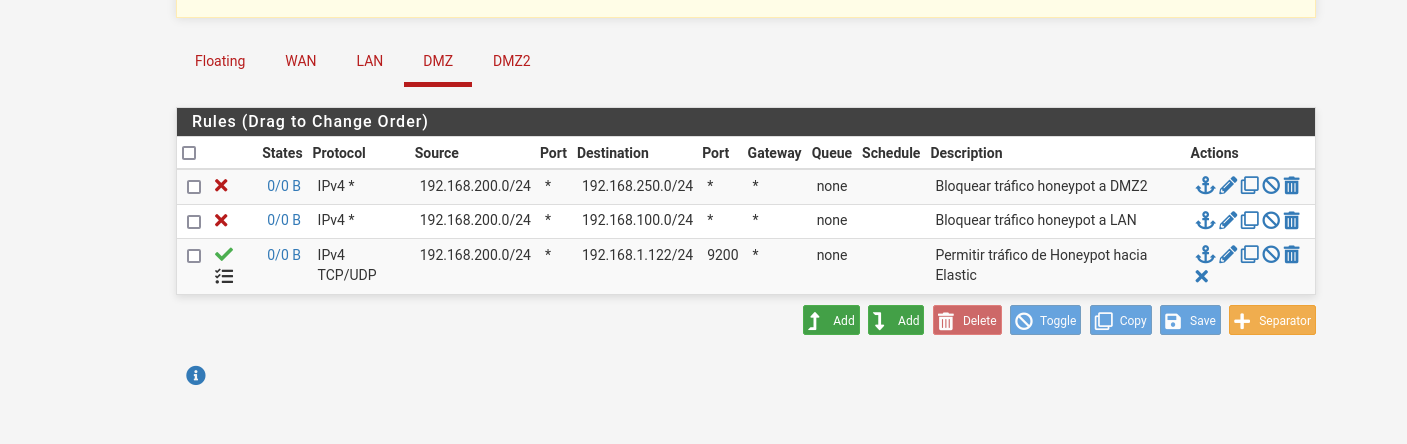
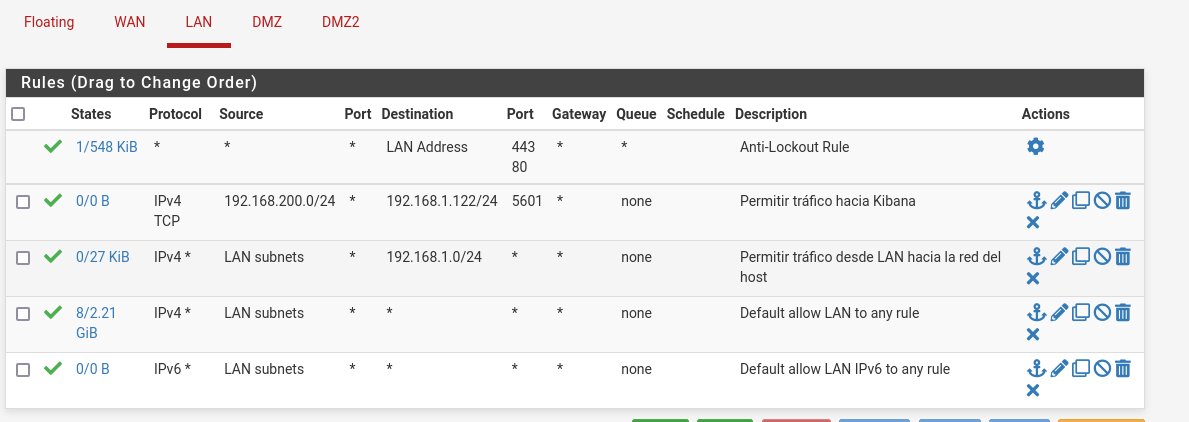
Se configuraron las siguientes reglas de firewall para permitir el tráfico entre las diferentes zonas de la red:

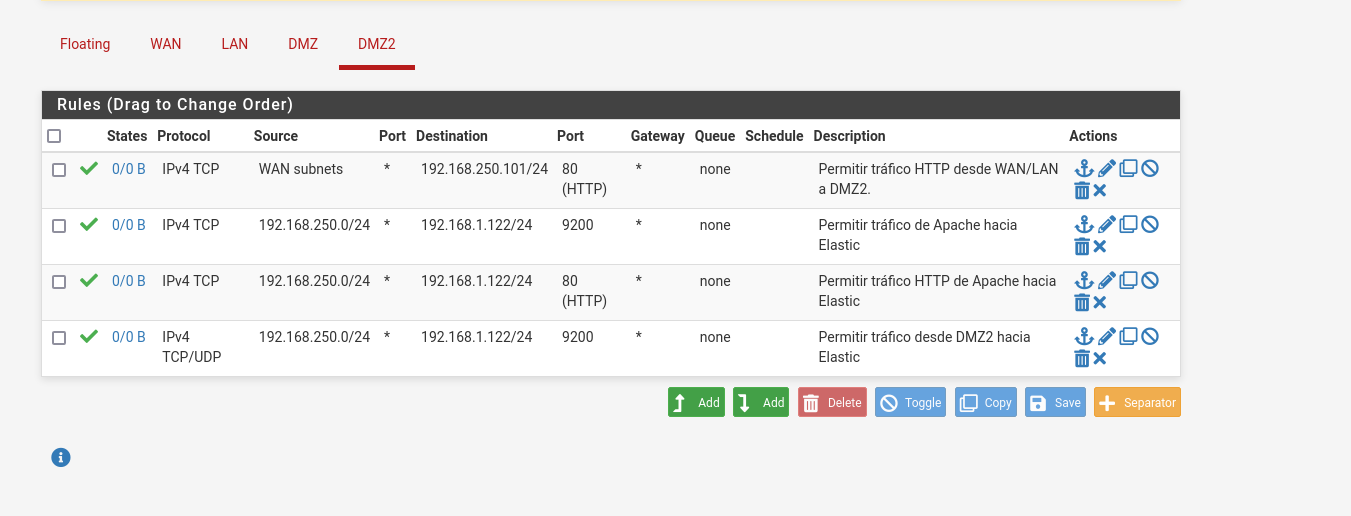
Permitir tráfico HTTP desde WAN/LAN hacia DMZ2 (Apache).

Permitir tráfico desde DMZ hacia Elastic (Filebeat y Cowrie).

Permitir tráfico desde DMZ2 hacia Elastic (Apache y Kibana).

Captura:

****

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

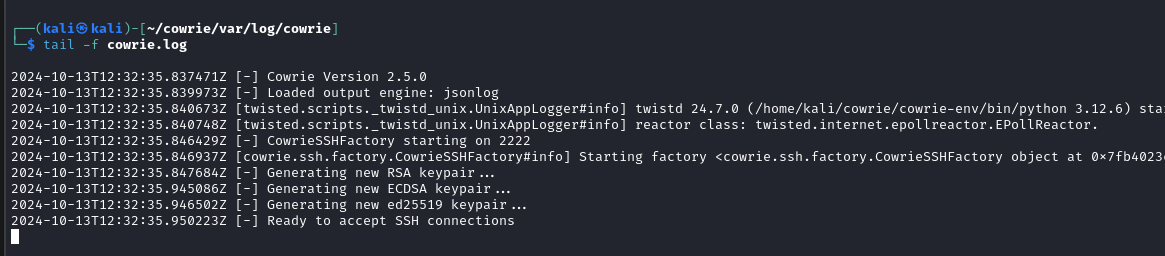
4.1 Instalación de Cowrie

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.

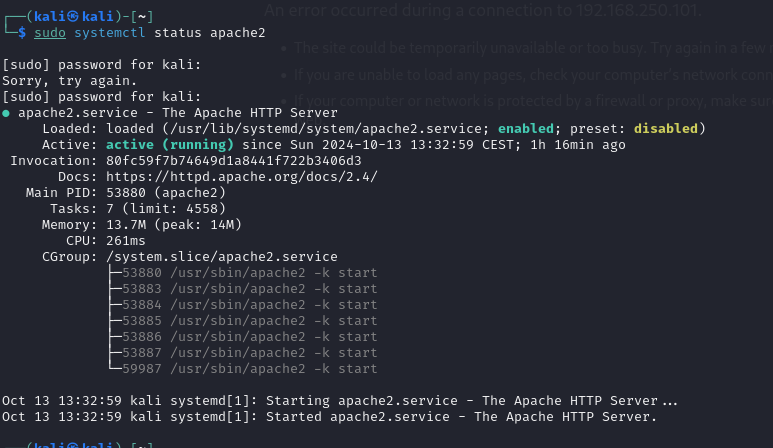
Captura:

**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.

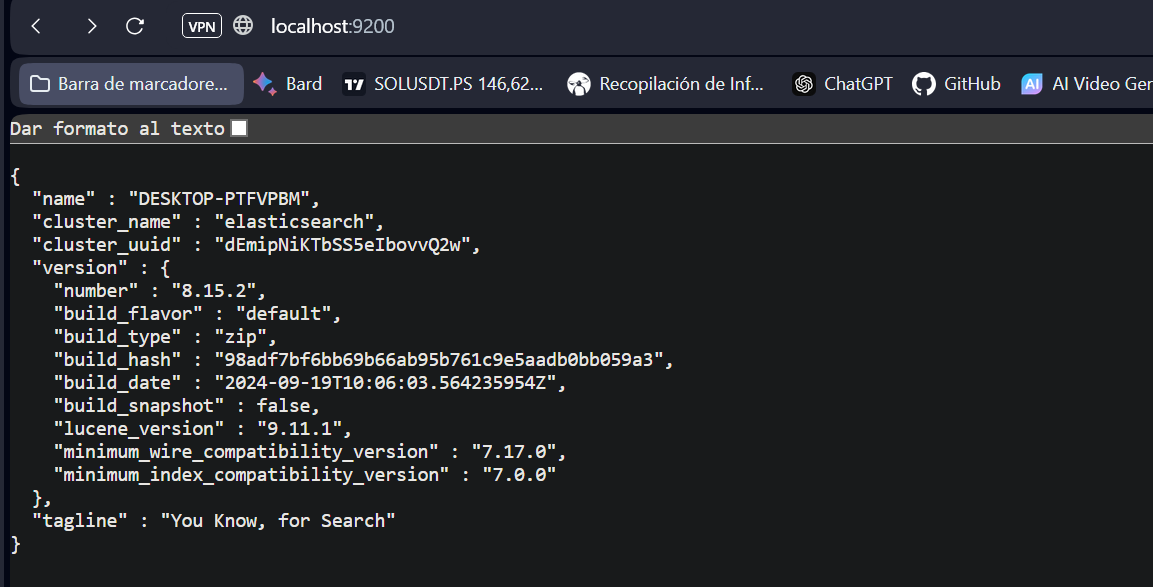
Captura:

**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.

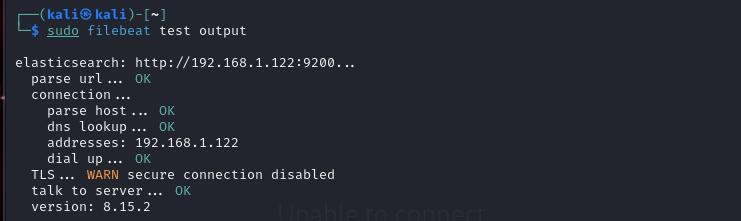
Captura:

**7. Configuración de Filebeat**

7.1 Instalación y Configuración de Filebeat

Se instaló Filebeat en la máquina DMZ para enviar logs hacia Elasticsearch. Se editó el archivo filebeat.yml para apuntar la salida de logs a 192.168.1.122:9200.

Captura:

**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.