**INFORME DE BLUETEAM**

TITULO:

Informe de redes BlueTeam

CURSO:

BlueTeam / Seguridad de la Información

PROFESOR:

Sergio Vilches Puerta

ALUMNO:

Jordan Andres Diaz Sanchez

**TABLA DE CONTENIDO**

1. Introducción
2. Infraestructura de red
   1. UTM
   2. LAN
   3. DMZ
   4. DMZ2
3. Firewall
   1. WAN
   2. NAT
   3. LAN
   4. DMZ
   5. DMZ2
4. SIEM (Elastic cloud)
   1. Políticas e integración
   2. Windows
   3. Honeypot
   4. Suricata
5. Elastic cloud - Logs
   1. Windows
   2. Honeypot
   3. Suricata
6. Conclusión
7. Referencias y Bibliografía
8. **INTRODUCCIÓN**

En este informe se detalla el diseño y la implementación de una arquitectura de red para un entorno de BlueTeam, este entorno esta diseñado para proporcionar capacidades de monitoreo y defensa frente a posibles amenazas cibernéticas, utilizando una red segmentada que incluye las redes LAN, DMZ y DMZ2, interconectadas a través de un firewall Pfsense. Cada segmento de tiene un propósito especifico, con dispositivos configurados para enviar registros de log a un servidor centralizado de Elastic, permitiendo la recolección y análisis de datos en tiempo real. Esta arquitectura busca asegurar la integridad y disponibilidad de la red, mientras se supervisan y gestionan posibles ataques.

1. **INFRAESTRUCTURA DE RED**

La infraestructura de red se implemento utilizando una UTM (unified Threat Management) basada en Pfsense el cual se configuro para actuar como el punto central de interconexión entre las redes LAN, DMZ, DMZ2, cada una asignada con un rango de direcciones IP dinámicas mediante DHCP esta configuración permite una gestión flexible.

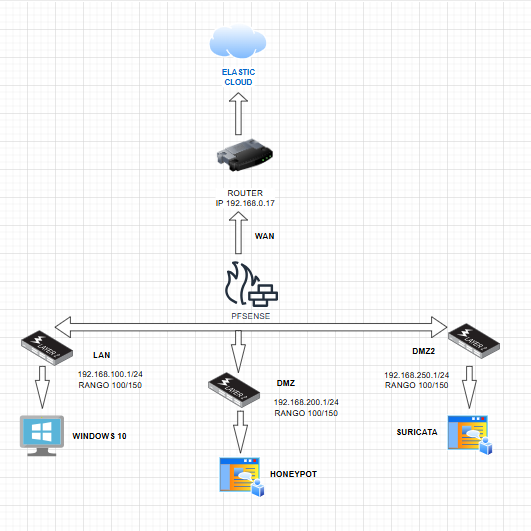


Ilustración 1 Estructura de red

En la red LAN, se encuentra un equipo con Windows 11, configurado para enviar registros al servidor Elastic, que centraliza la recolección y análisis de registros. La DMZ aloja un Honeypot accesible desde la WAN, pero sin acceso a las redes internas, garantizando un entorno aislado para la captura de intentos de intrusión. Por último, en la DMZ2 se implementó una fuente adicional de logs, con opciones como Suricata o Apache Server, para diversificar las fuentes de datos que alimentan el servidor Elastic.

* 1. UTM (unified Threat Management)

El corazón de la infraestructura de red es una UTM (Unified Threat Management) implementada con Pfsense. Pfsense es una solución de firewall de código abierto que proporciona funciones avanzadas de gestión de red y seguridad, incluyendo cortafuegos, VPN, filtrado de contenido y detección de intrusiones.

En esta práctica, Pfsense se configuró para manejar tres redes distintas: LAN, DMZ y DMZ2. Cada segmento está aislado para mejorar la seguridad y se interconecta a través del Pfsense, que actúa como un puente seguro entre ellos. Además, Pfsense administra la asignación de direcciones IP dinámicas a través de su servidor DHCP integrado, asegurando que los dispositivos en cada red reciban configuraciones IP adecuadas sin intervención manual.

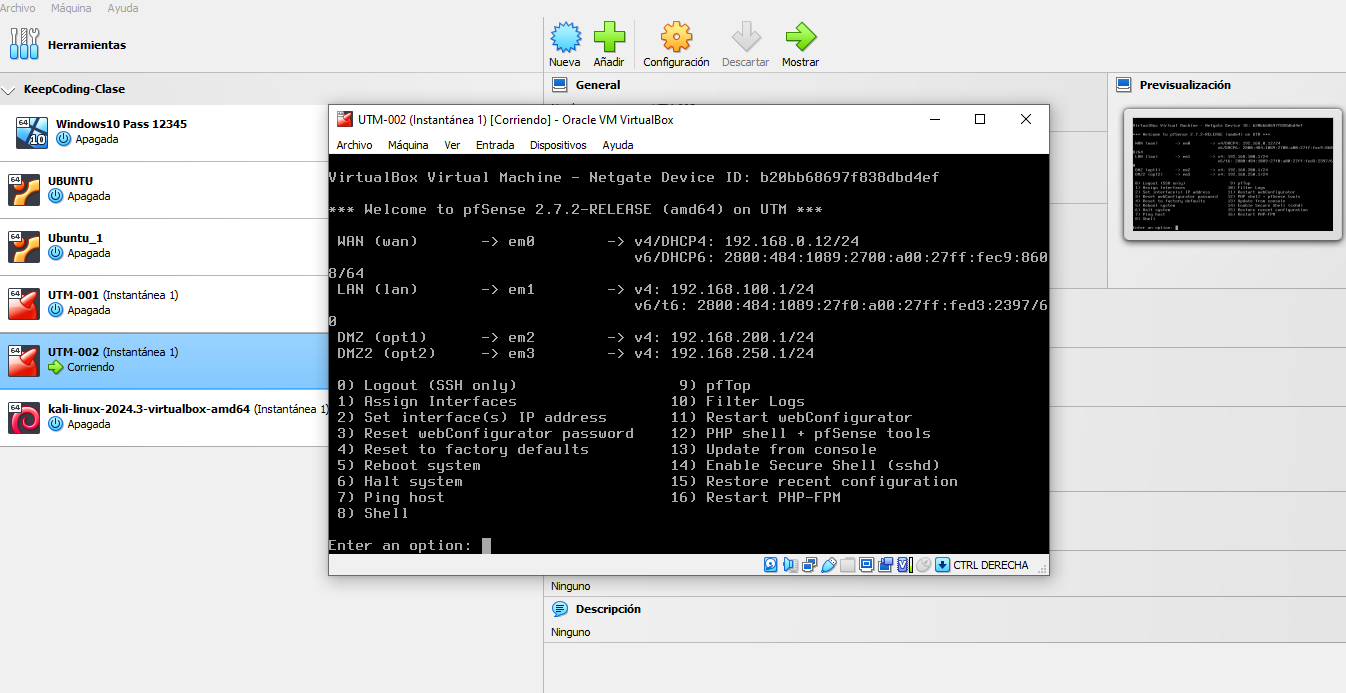


Ilustración 2 UTM-002 Pfsense

* 1. LAN

La red LAN esta infraestructura está diseñada para alojar dispositivos internos, con un enfoque en la seguridad y la facilidad de gestión. En este caso, la LAN contiene un equipo con Windows 11, configurado para enviar registros al servidor Elastic. Esto permite el monitoreo continuo de actividades y eventos del sistema, lo que es crucial para la detección y respuesta temprana a posibles incidentes de seguridad.

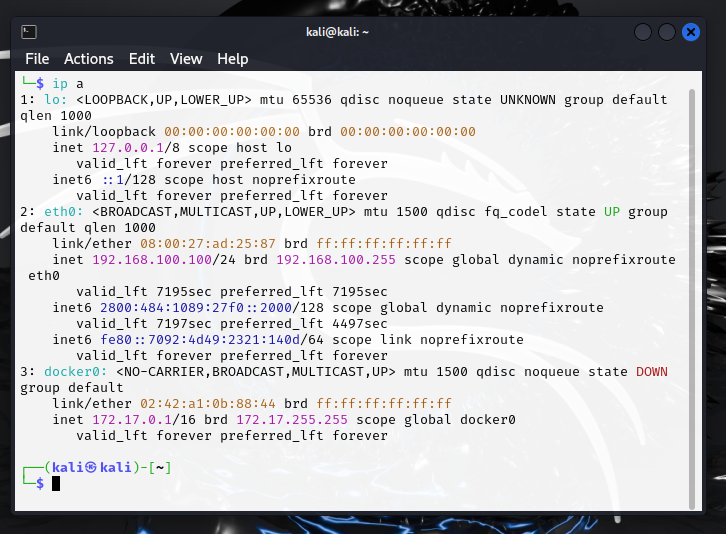


Ilustración 3 Red LAN



Ilustración 4 Red LAN rangos

* 1. DMZ

La red DMZ (Zona Desmilitarizada) está diseñada como una zona de seguridad intermedia entre la red interna (LAN) y la red externa (WAN). En esta infraestructura, la DMZ aloja un Honeypot, un sistema que simula ser un objetivo vulnerable para atraer y analizar intentos de intrusión. Este Honeypot está configurado para enviar registros al servidor Elastic, lo que permite monitorear las actividades sospechosas y obtener información sobre posibles ataques.

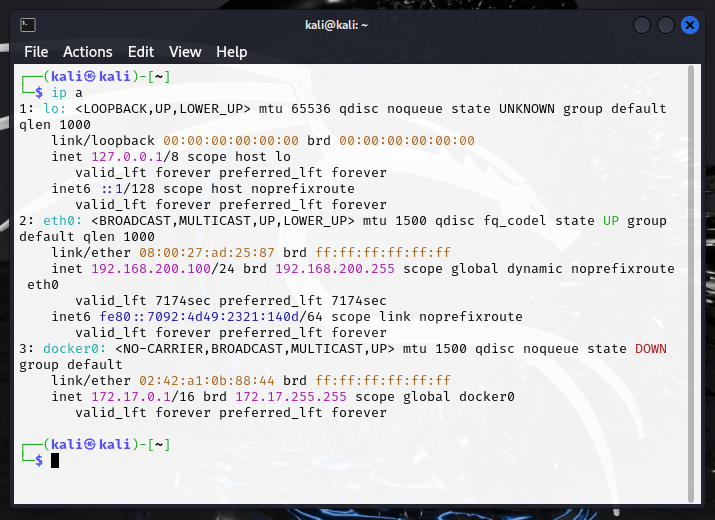


Ilustración 5 Red DMZ

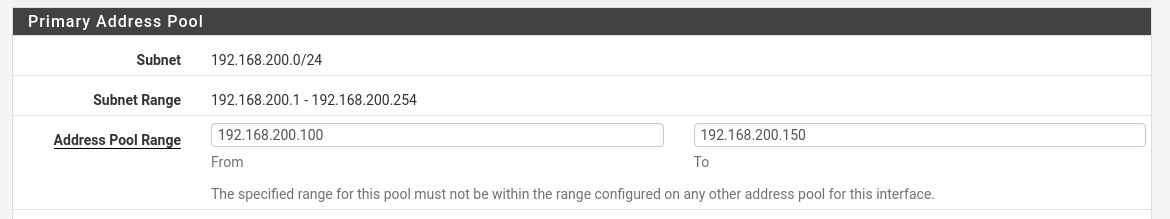


Ilustración 6 Red DMZ rangos

* 1. DMZ2

La red DMZ2 se establece como un segmento adicional de la infraestructura de seguridad, destinado a alojar una fuente diferente de logs, complementando la información recopilada en la LAN y la DMZ. En este caso, se implementó un servidor Suricata como fuente de registros en la DMZ2. Suricata proporciona capacidades de detección de intrusiones y análisis de tráfico en tiempo real, mientras que el Servidor Apache genera registros detallados de acceso y errores de aplicaciones web.

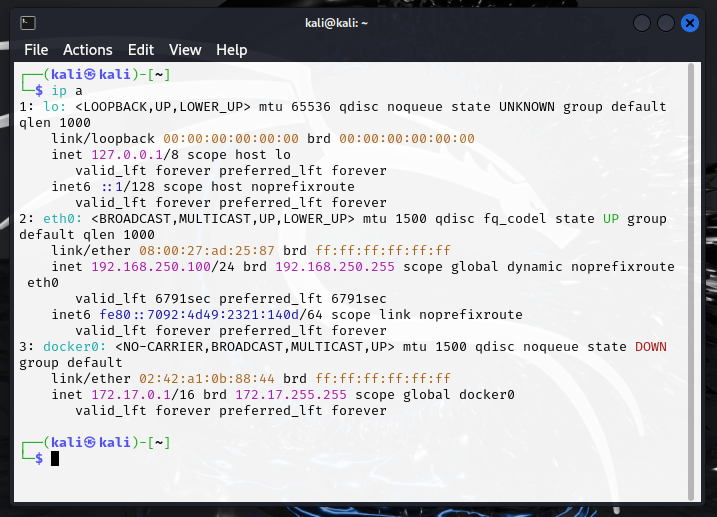


Ilustración 7 Red DMZ2

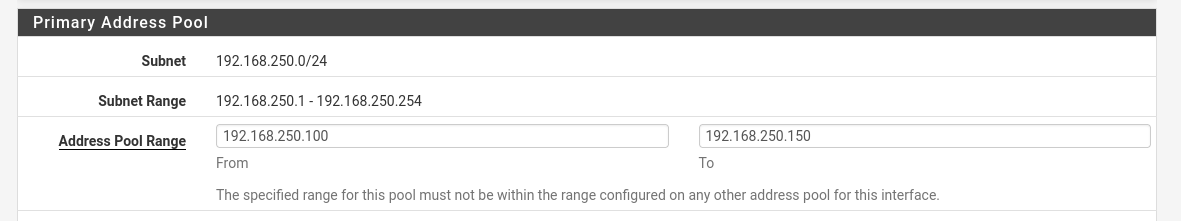


Ilustración 8 Red DMZ2 rangos

1. **FIREWALL**