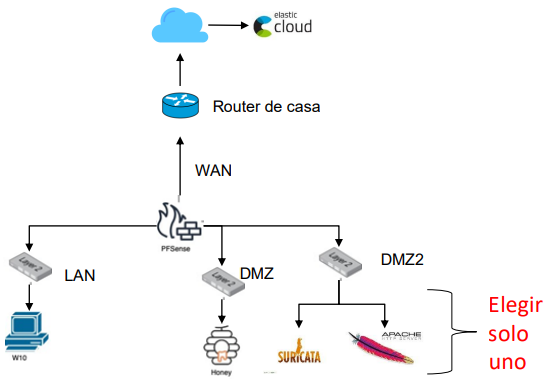
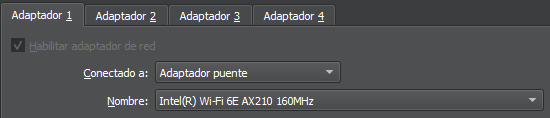
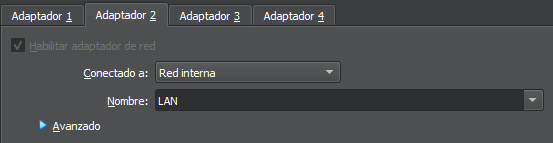
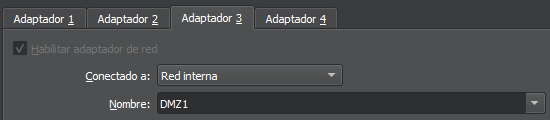
INFRAESTRUCTURA DE RED

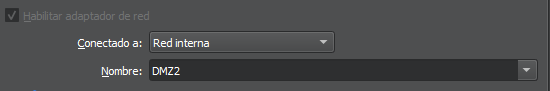


La configuración del firewall tiene 3 adaptadores:

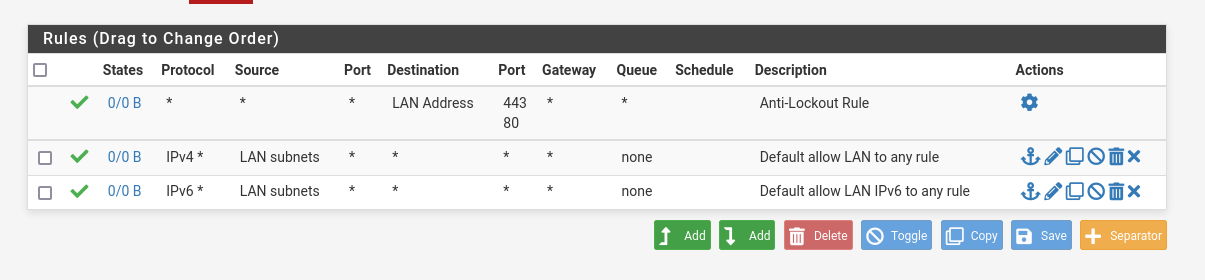


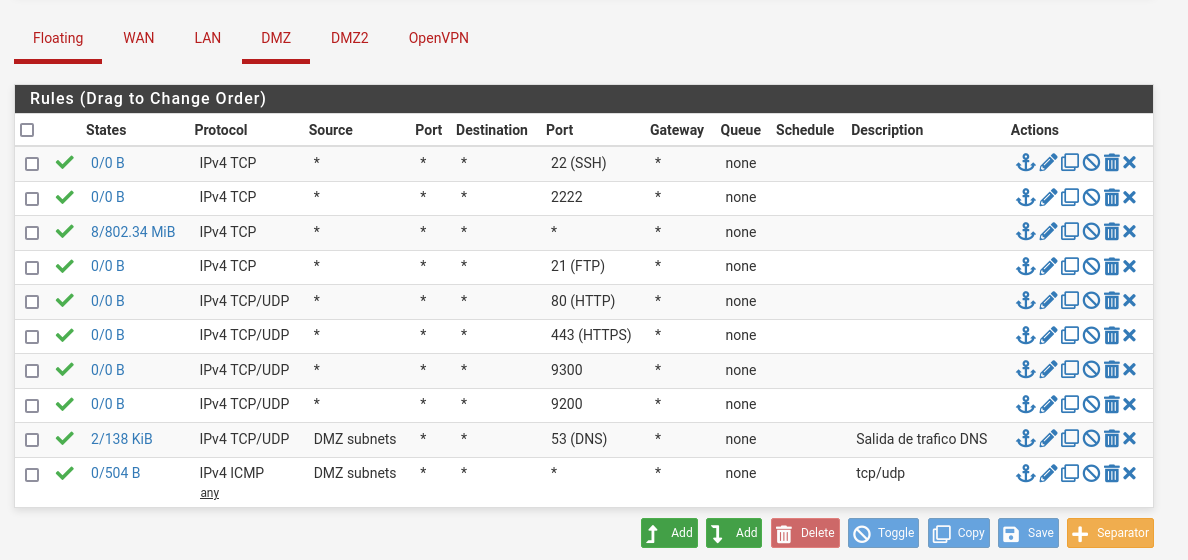


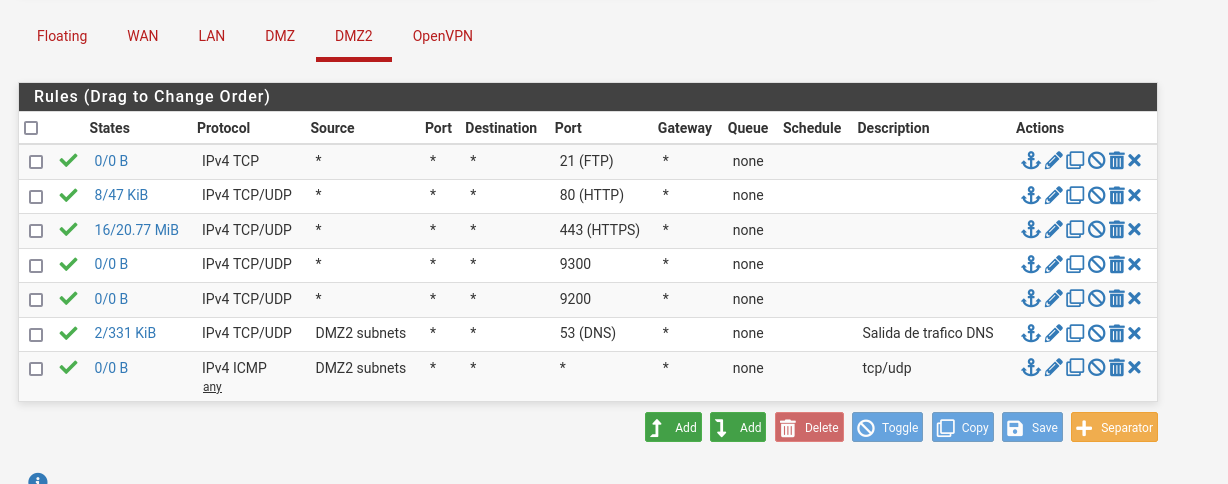




Y estas son las reglas que he establecido para cada uno:

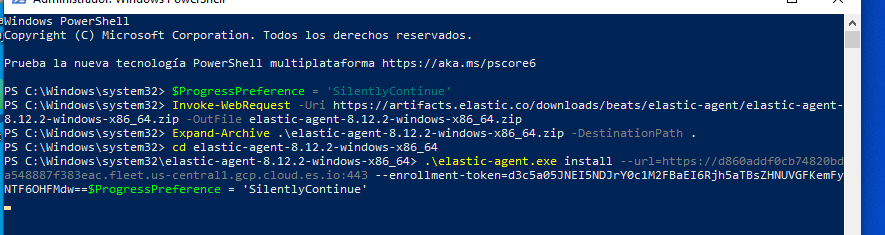


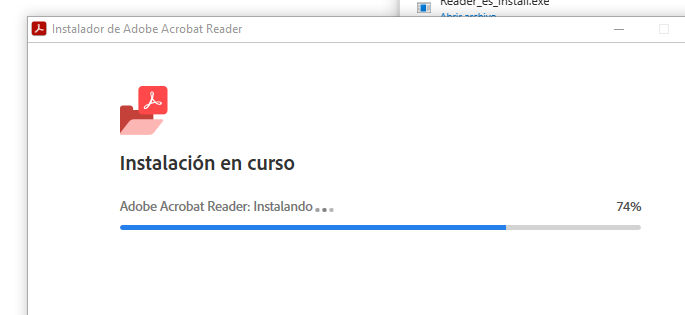
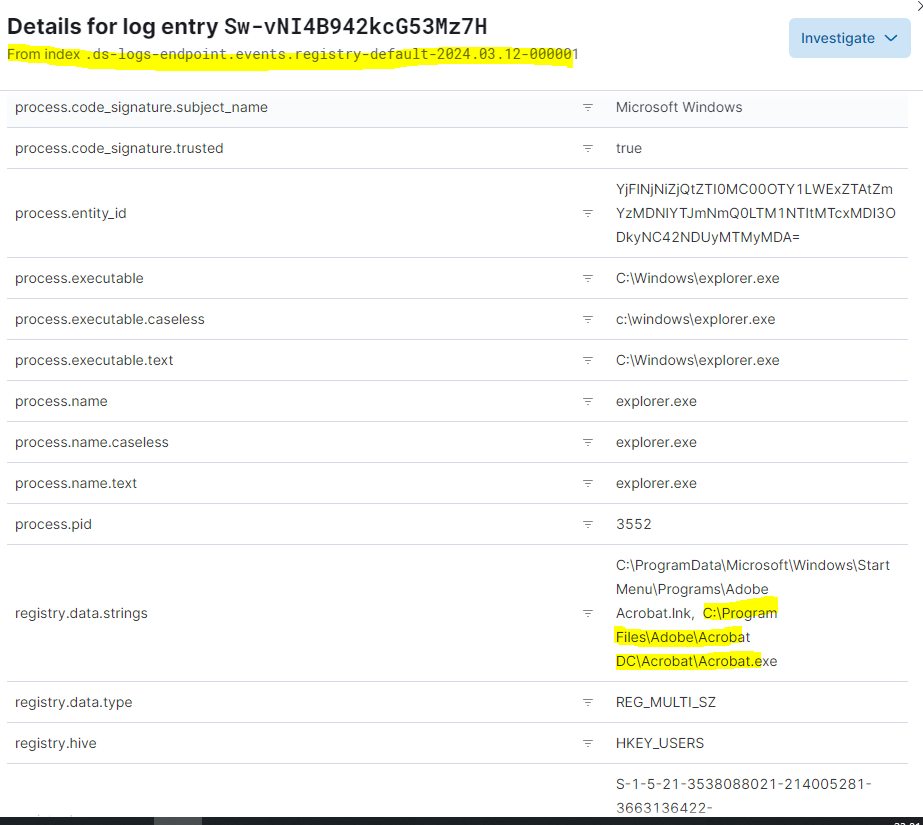




Equipo Windows:

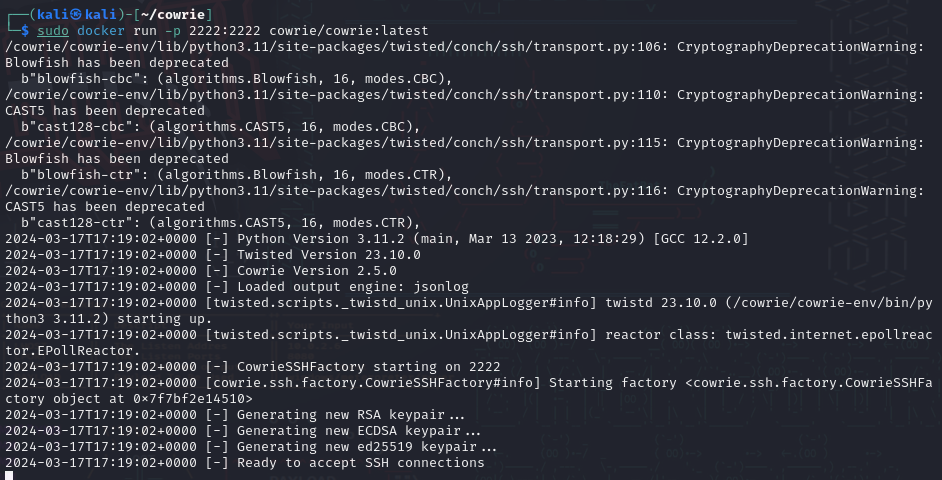
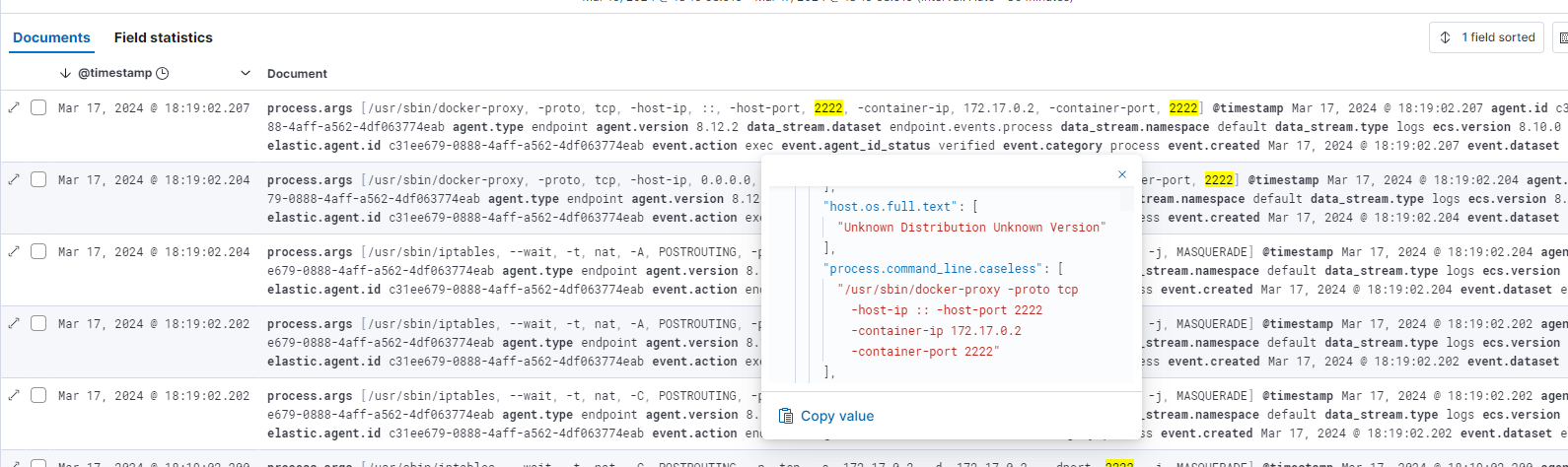
1. Instalamos Agente de Elastic



1. Procedo a realizar una instalación con el fin de generar logs: 
2. Los resultados: 

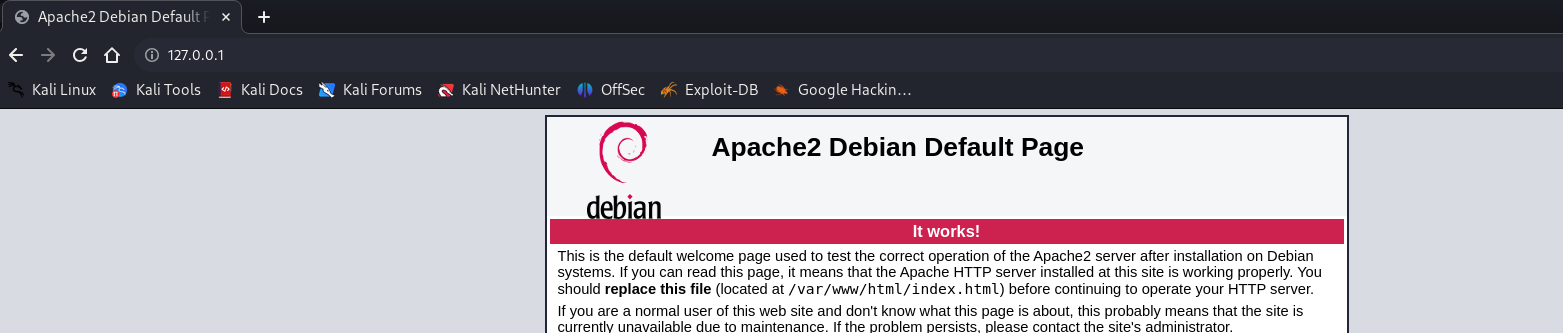
Equipo HoneyPot:

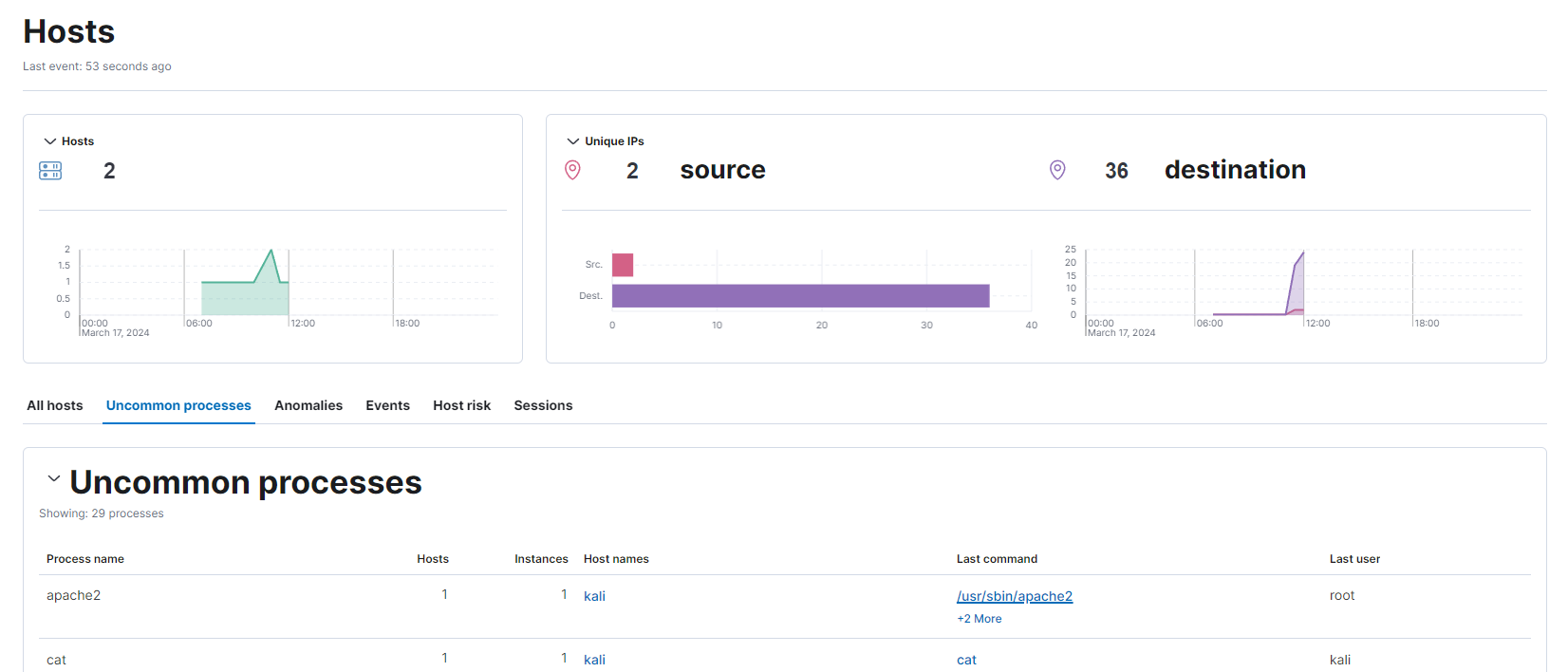
* He elegido una maquina kali y he instalado un honeypot ssh para generar logs a través de Elastic

1. Descargo el repositorio de github y lo ejecuto con docker mediante el puerto 2222
2. Estos son los logs al ejecutar el servicio:
3. 

Equipo con Apache

* He elegido una maquina kali
* Una vez levantado el apache entramos en localhost(127.0.0.1)



1. Comprobamos que Elastic recoge el proceso
2. En los log podemos comprobar como que estamos accediendo a localhost a través de apache
3. Por si queda alguna duda comprobamos que el agent name es “kali”
4. 