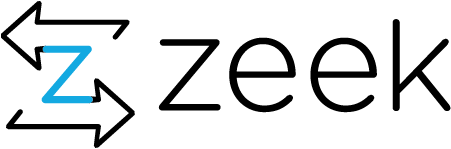
**Zeek (IDS pasivo)**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Configuración Inicial**](#_g59i8ewd3ed3) **2**

[**3. Instalación Zeek**](#_n18rs06g9arv) **3**

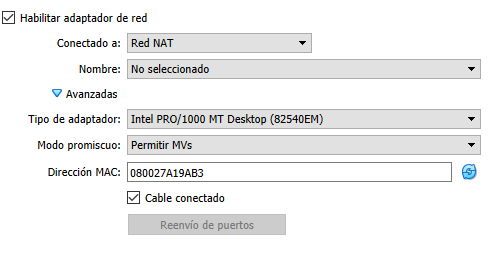
[**4. Configuración Zeek**](#_4ntsfczidjjg) **4**

[**5. Pruebas básicas de funcionamiento**](#_zh86zsi8onzt) **6**

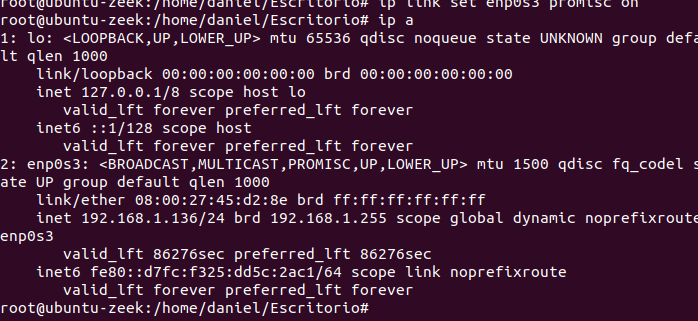
[**6. Scripts**](#_4gz85pcpe7ym) **7**

# **2. Configuración Inicial**

A continuación, se procederá a la configuración de una de las interfaces de red en modo promiscuo para lograr escuchar todo el tráfico de dicho rango de red. El primer paso, es la configuración a nivel del software de virtualización, VirtualBox, en donde tenemos que permitir a dicha máquina el modo promiscuo.

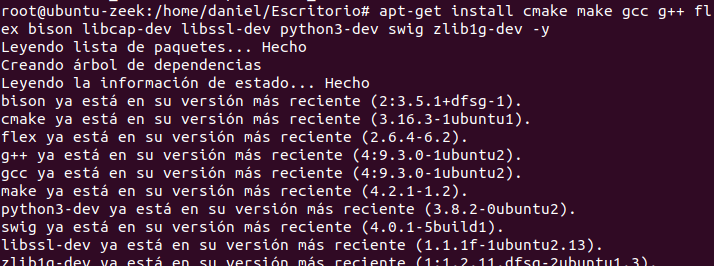


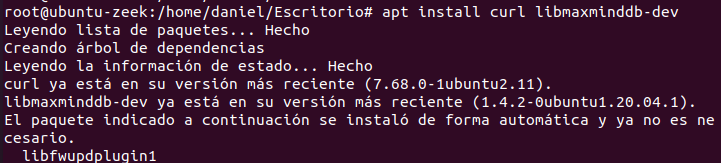
Aparte de esta configuración, es necesario habilitar la interfaz de red correspondiente en modo promiscuo:



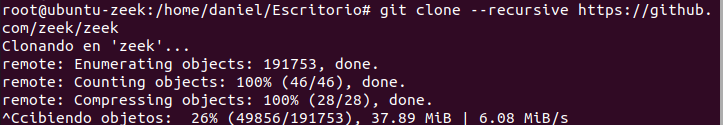
# **3. Instalación Zeek**

Una vez que se tiene configurada la interfaz en modo promiscuo, se procede a la instalación de Zeek: Revisamos e instalamos las dependencias obligatorias y de las dependencias opcionales se instalarán curl y libmaxminddb





Instalamos Zeek desde el repositorio de GitHub.



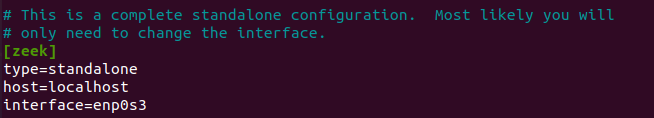
Añadimos la siguiente ruta, a nuestra variable de entorno $PATH



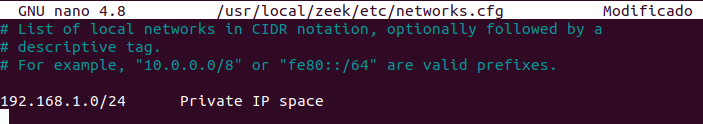
# **4. Configuración Zeek**

Una vez que se ha instalado Zeek, se procede a su configuración para el entorno en el que se encuentra. La principal configuración de Zeek se realiza en los siguientes 3 ficheros del directorio /usr/local/zeek/etc/:

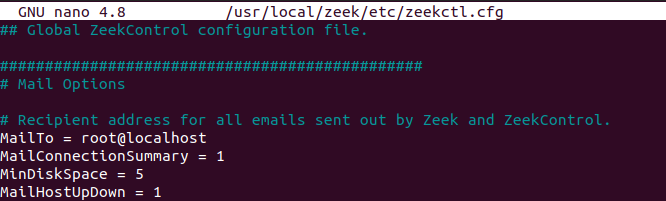
* nodes.cfg

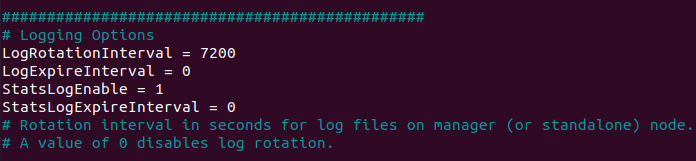


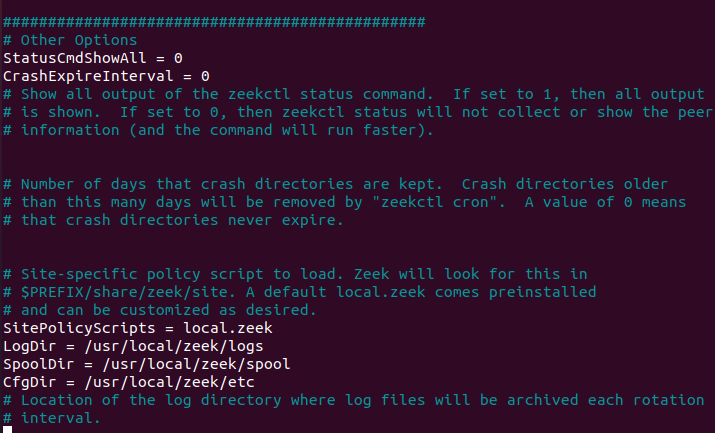
* networks.cfg



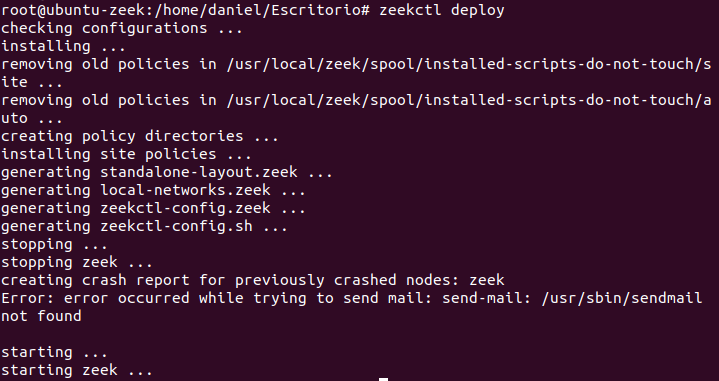
* zeekctl.cfg







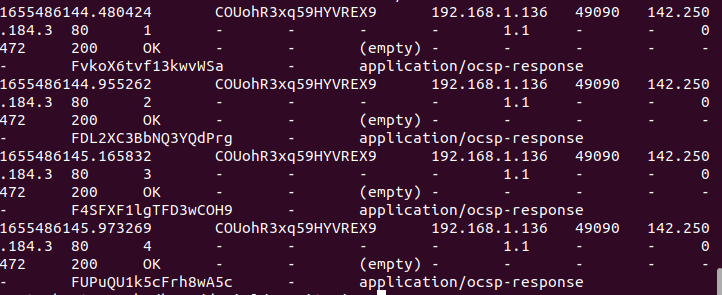
Una vez que se ha instalado y configurado correctamente Zeek, procedemos a aplicar la configuración y a su arranque mediante el comando zeekctl deploy



# **5. Pruebas básicas de funcionamiento**

Por último, vamos a realizar unas pequeñas comprobaciones, que nos permitirán comprobar el correcto funcionamiento del IDS que acabamos de configurar.

Podemos, por ejemplo, realizar una conexión http. Veremos que automáticamente Zeek crea el http.log, y si lo abrimos, veremos que ha registrado dicha conexión:

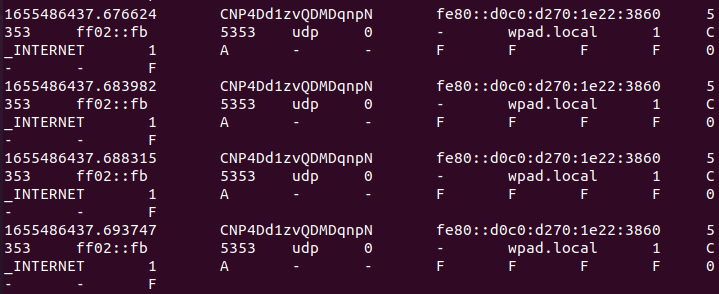


Aunque podríamos hacer innumerables pruebas, para ver como Zeek va generando los diferentes log files, se recomienda que al menos se hagan las siguientes, con la intención de que vayamos observando y entendiendo su funcionamiento:

Consultar dhcp.log después de agregar alguna MV a nuestra red

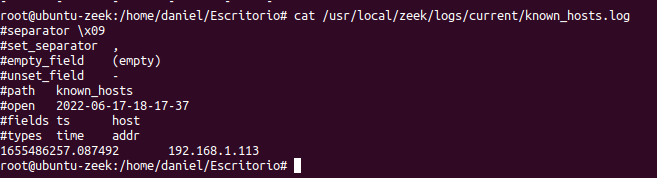


Las consultas DNS registradas en dns.log tras haber navegado por algunas webs.



Verificando ssh.log y know\_hosts.log después de haber realizado diferentes tipos de conexiones a través del protocolo ssh.

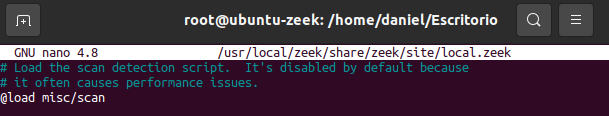




# **6. Scripts**

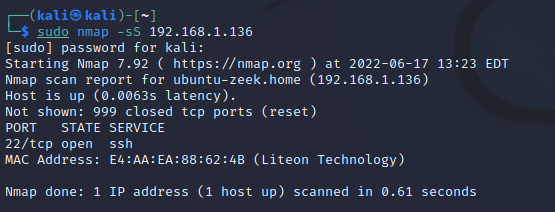
Como se ha comentado en el estudio previo de este IDS, Zeek viene con unos scripts que permiten realizar diferentes tipos de detecciones. Nosotros vamos a dejar los scripts que vienen por defecto, pero tendríamos la posibilidad de añadir o modificar los que quisiéramos para activar nuevas funcionalidades en nuestro sistema. Para nuestro ejemplo, vamos a trabajar script ‘scan’:

Para habilitar/deshabilitar scripts se debe modificar el siguiente fichero /usr/local/zeek/share/zeek/site/local.zeek



Y volvemos a desplegar Zeek

Para poner a prueba nuestro IDS, y ver si el script es capaz de detectar un escaneo de puerto, vamos a usar una MV con Kali



Estos scripts personalizados registran las alertas en el fichero de log notice.log. Si accedemos a él, veremos como el IDS ha registrado su correspondiente alerta, informando del tipo de ataque.

