Práctica sobre Sistemas de Detección de Intrusos

La práctica que vamos a realizar consiste en la instalación y configuración de un IDS de red, así como comprobar su funcionamiento en un entorno de red aislado como el que ya tenemos disponible en la asignatura.

En primer lugar, tenemos que buscar información sobre el uso y configuración de la herramienta Snort (https://www.snort.org/), para posteriormente instalar dicha aplicación en la máquina que ejecuta el firewall en el esquema de máquinas virtuales que tenemos desplegado de la práctica anterior.

En el caso de que nuestro firewall esté implementado sobre Kali Linux, podemos seguir estas instrucciones para que el proceso de instalación sea más sencillo:
https://bin3xish477.medium.com/installing-snort-on-kali-linux-9c96f3ab2910

Si hemos elegido Debian como sistema operativo para la máquina firewall, aquí hay unas instrucciones para facilitar el proceso de instalación:
https://upcloud.com/resources/tutorials/installing-snort-on-debian

Una vez instalado Snort, debe configurarse la herramienta para que realice las siguientes acciones:

1- Registrar el tráfico que circula por todas las interfaces de red de la máquina firewall. Indicar la regla usada.
2- Generar una alerta cada vez que firewall reciba una petición *ping* procedente de la máquina srv_interno. Indicar la regla usada y mostrar el resultado obtenido.
3- Añadir una regla que detecte intentos de conexión desde la máquina srv_externo hacia el servicio web disponible en firewall. Indicar la regla usada y mostrar el resultado obtenido.
4- Añadir una regla que genere una alerta en caso de detectarse una exploración de puertos tipo XMAS TREE. Indicar la regla usada y mostrar el resultado obtenido. resultado de un experimento donde se vea su funcionamiento.

Como resultado de la práctica se entregará un documento en formato PDF donde se especifiquen las reglas Snort utilizadas, junto con una captura del resultado obtenido en cada caso y una explicación de la regla elegida.

Se valorará el cumplimiento de los requisitos, la correcta configuración de las reglas y la documentación del trabajo.