THE BRIDGE

BOOTCAMP Ciberseguridad en formato online

EJERCICIOS IDS/IPS: SNORT

Prerrequisitos

Para esta actividad lo que te pedimos es que establezcas una serie de reglas dentro de Snort instalado previamente con la configuraciones correspondientes.

El objetivo es que vayas familiarizándote en la creación de reglas dentro de este entorno, las cuales os ayudarán a simular un futuro entorno real de trabajo.

Requisitos

Para poder llevar a cabo el Challenge necesitarás de diversas máquinas:

➔ Kali: 10.0.2.X

➔ PfSense: 10.0.2.X y 192.168.56.0/24

Este ejercicio tiene una máquina virtual asociada: **Ubuntu_ExerciseIDS.ova**

Usuario **ubuntu:ubuntu**

La máquina virtual tiene configurados 3 servicios:

Servidor FTP (Puerto 21)

Servidor SSH (Puerto 22)

Servidor Web (Puerto 80)

La idea es crear reglas de Snort que permitan generar alertas para diferentes comportamientos/ataques que pueda sufrir la máquina.

Las reglas se crean en el fichero /etc/snort/rules/local.rules

Cada vez que se modifique el fichero con una regla nueva se debe reiniciar el servicio de snort para aplicar los cambios.

sudo service snort stop

sudo service snort start

Las alertas se almacenan en el fichero /var/log/snort/

Para monitorizar las nuevas alertas que se están creando es interesante dejar un terminal monitorizando las nuevas filas creadas en el fichero

tail -f /var/log/snort/

Ejercicio 1

Para la simulación de un entorno real crea las siguientes reglas dentro de Snort:

- La regla detecta cuando se hace un ping a una máquina de la red interna
- La regla detecta si alguien se ha autenticado con usuario anónimo por FTP.
- La regla detecta cuando se hace un escaneo de tipo SYN (por defecto NMAP) a una máquina de la red interna. Para eso cuenta si se han realizado más de 5 conexiones, hacia la misma máquina en menos de 5 segundos.
- La regla detecta más de 5 conexiones seguidas al servicio de SSH desde el mismo cliente.
- La regla detecta cuando se recibe una petición al servidor Web solicitando el recurso /test.html en la máquina interna.

THE BRIDGE