**Laboratorio SNORT:**

**¿Qué es SNORT?:** es un sistema de detección de intrusos en red (NIDS) de código abierto y gratuito. Monitoriza el tráfico de la red en busca de actividades sospechosas o maliciosas.

**¿Para qué sirve?:**

* **Detectar intrusiones:** Reconoce patrones de ataques conocidos y comportamientos inusuales en la red.
* **Analizar el tráfico:** Examina en detalle los paquetes de datos que circulan por la red.
* **Generar alertas:** Avisa cuando detecta algo sospechoso, permitiendo actuar a tiempo.
* **Proteger la red:** Ayuda a identificar y detener ataques antes de que causen daños.

**¿Cómo funciona SNORT?:** utiliza dos técnicas principales para detectar intrusiones

* **Búsqueda de firmas:** Compara el tráfico de la red con patrones conocidos de ataques, como firmas de malware o exploits.
* **Detección de anomalías:** Analiza el comportamiento de la red y busca patrones inusuales que podrían indicar un ataque.

**¿Qué se puede hacer con SNORT?:** es una herramienta versátil que permite

* **Configurar reglas personalizadas:** Adaptar SNORT a las necesidades específicas de la red.
* **Integrarlo con otros sistemas de seguridad:** Combinar SNORT con otras herramientas para una protección completa.
* **Ampliar su funcionalidad:** Utilizar plugins y módulos adicionales para obtener más capacidades.

**PROCESO INSTALACION**

Actualiza el sistema

*sudo apt update*

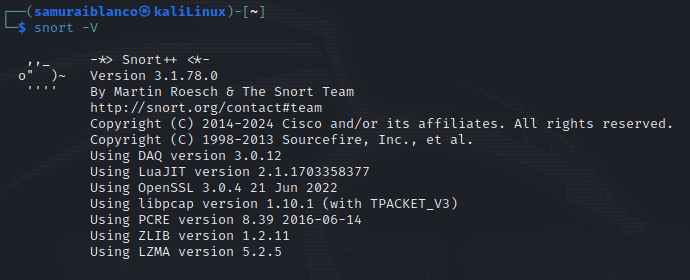
Instala Snort sin interactuar con la pantalla

*sudo apt install snort -y*

Verifica la versión de Snort y si está correctamente instalado

*snort -V*

Después de ejecutar el comando anterior, debes estar viendo un mensaje como el siguiente:



Para la próxima clase (marzo 14) trae configurado Snort con una regla funcionando (no importa que regla, por ejemplo: que alerte cuando le hacen ping al equipo). Ten en cuenta que es posible que debas realizar alguna configuración adicional como por ejemplo. Colocar la tarjeta de red en modo promiscuo y/o “afectar” el archivo de configuración de Snort */etc/snort/snort.conf*

Sugerencias:

* Coloca la tarjeta de la máquina virtualizada en modo bridge
* Antes de iniciar cualquier instalación y/o configuración, realiza un snapshot de la máquina virtual
* Consultar el manual/sitio oficial de SNORT: <https://www.snort.org/>
* Consulta el repositorio con multiples reglas preconfiguradas:

<https://github.com/secnnet/Snort-Rules/>

**NOTA:** el estudiante deberá hacer uso del tiempo restante de la sesión del 12 de marzo y de parte de la sesión del 14 de marzo cuando el profesor revisará individualmente el trabajo realizado. A continuación debe consignarse con imágenes y texto el trabajo realizado:

**DESARROLLO**

…….