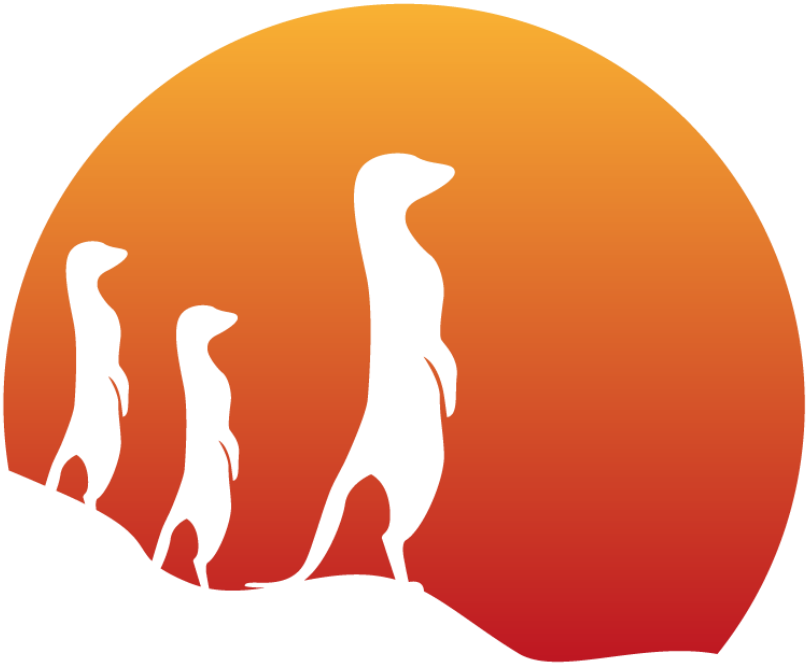
INSTALACIÓN Y CONFIGURACIÓN DE SURICATA

INCIDENTES DE CIBERSEGURIDAD

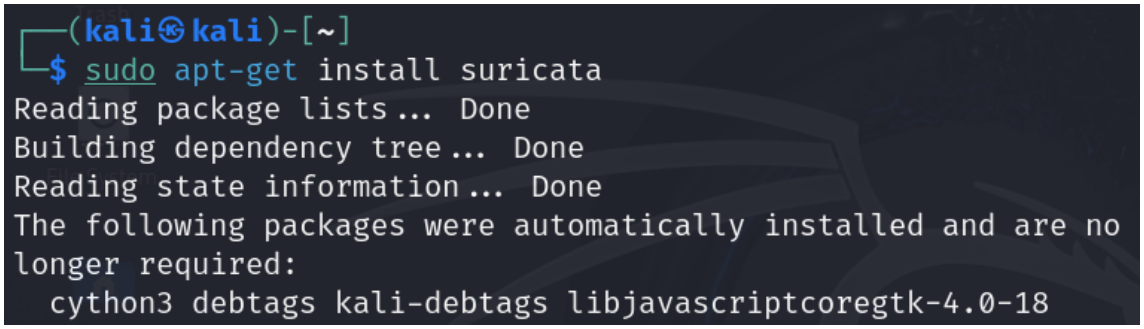


ERIC SERRANO MARÍN

Contenido

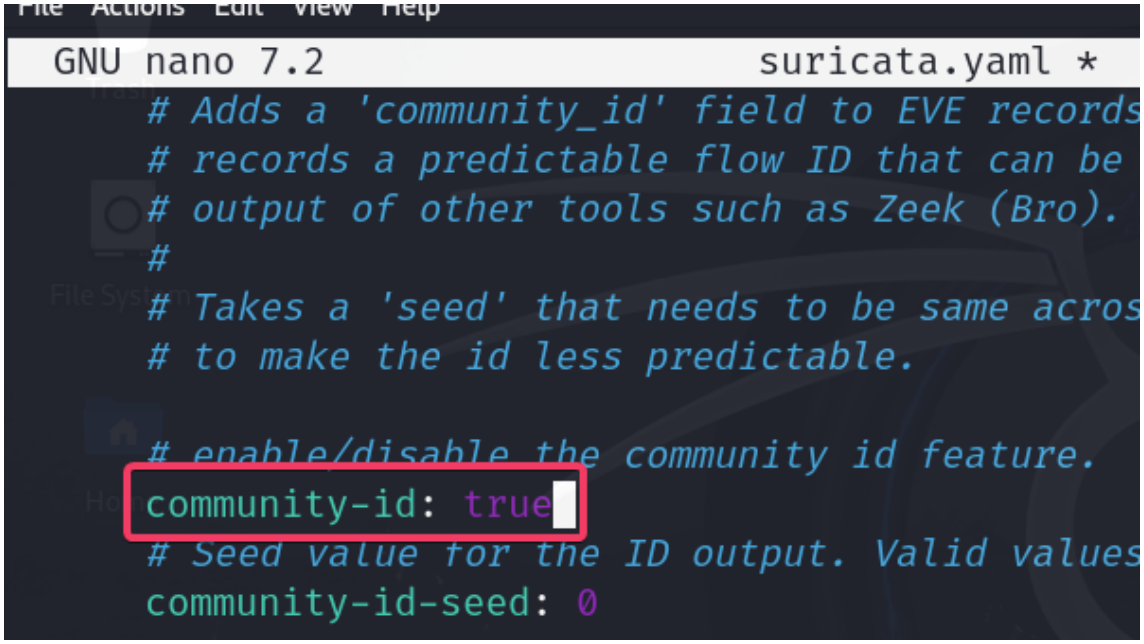
1. Comando de instalación de suricata.

sudo apt-get install suricata

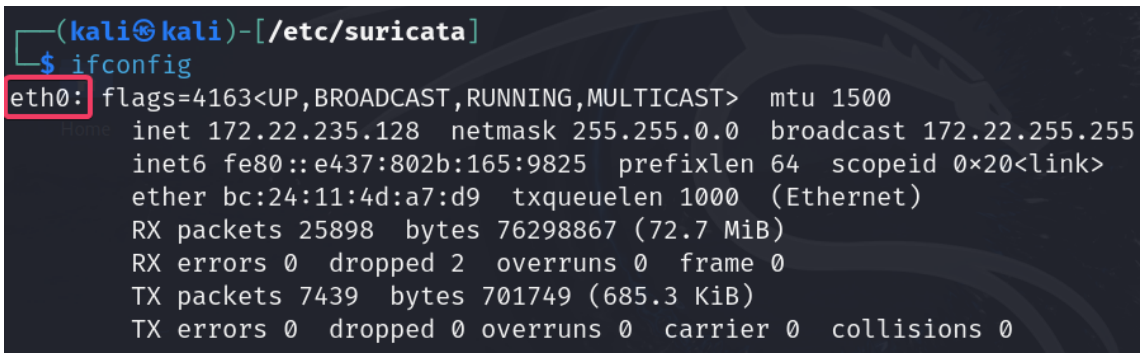


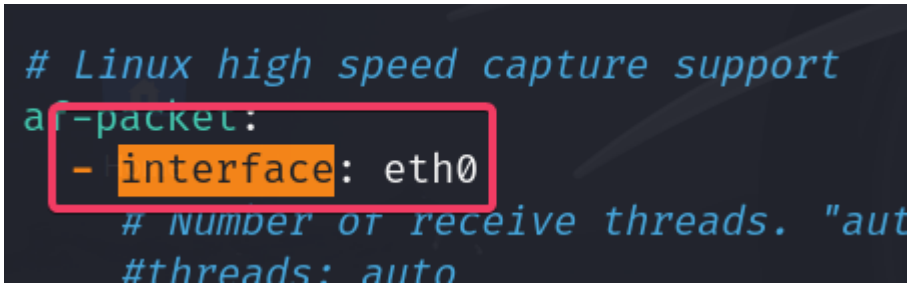
2. Para que nos asocie un id que esté en la comunidad de suricata.

Cambiaremos el false por un true.



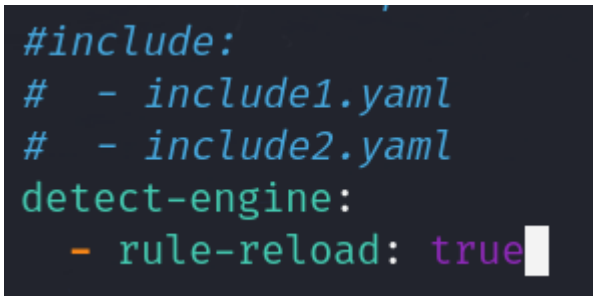
3. **Comprobamos nuestra interfaz de red para ver si está igual que en el archivo suricata.yaml.**





4. **En el mismo archivo escribiremos una directiva.**

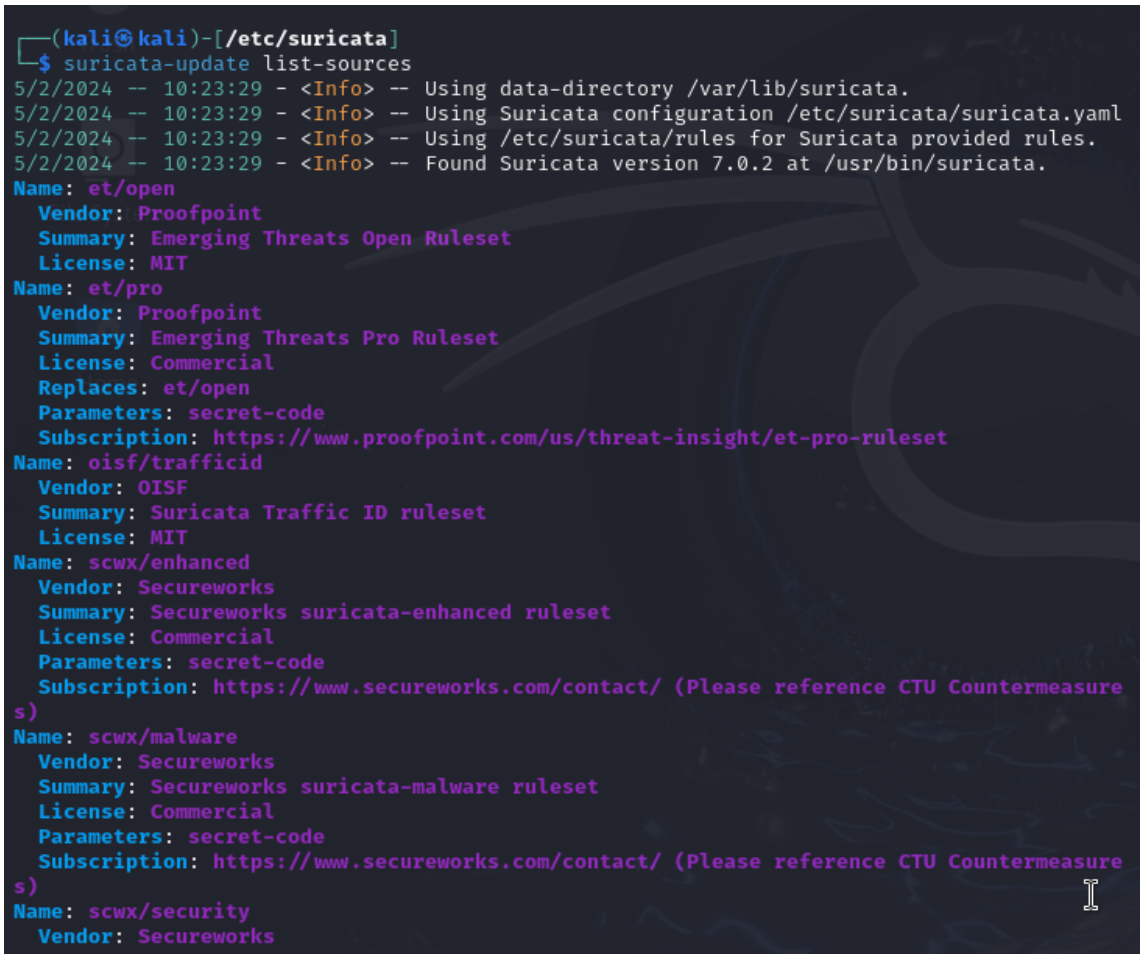
Para que cuando editemos las reglas, los cambios se hagan inmediatamente y no haga falta reiniciar el servicio.



5. **Reiniciamos suricata para que se apliquen los cambios.**

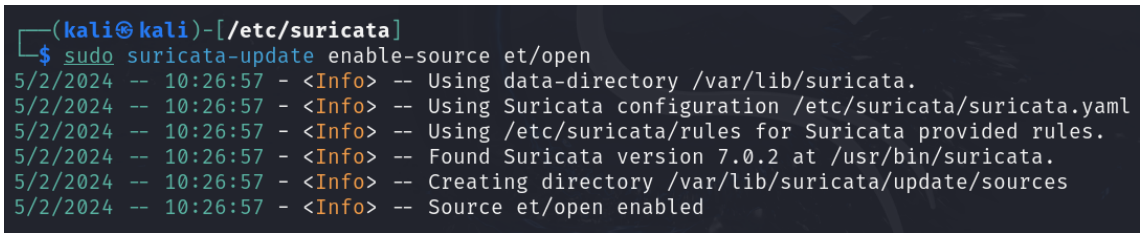
6. Vamos a hacer que se apliquen algunas reglas básicas.

Con el comando suricata-update con “list-sources”, nos informará de las reglas que podemos usar.



7. Para activar cualquiera de la lista usaremos enable-source junto al nombre.

En nuestro caso vamos a activar et/open. Con esto, después de hacer un suricata update ya se nos aplicarían todas las reglas.



8. Ya tendríamos todo configurado, vamos a hacer un test al fichero de configuración.

En caso de que esté todo correcto nos dirá que se ha realizado con éxito.

No me funcionaba, al final no me daba el complete, y era porque la carpeta rules estaba totalmente vacía. No tengo la captura del error, ya que lo he solucionado sin hacerla captura y se me ha olvidado.

Aquí lo que he hecho para arreglarlo.

sudo suricata-update

Este comando anteriormente lo puse directamente con “list-sources” y no lo puse sin nada, yo creo que ese fue el problema.

```
┌──(kali㉿kali)-[/var/lib/suricata/rules]
└─$ sudo suricata-update
5/2/2024 -- 10:38:22 - <Info> -- Using data-directory /var/lib/suricata.
5/2/2024 -- 10:38:22 - <Info> -- Using Suricata configuration /etc/suricata/s
uricata.yaml
5/2/2024 -- 10:38:22 - <Info> -- Using /etc/suricata/rules for Suricata provi
ded rules.
5/2/2024 -- 10:38:22 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/sur
icata.
5/2/2024 -- 10:38:22 - <Info> -- Loading /etc/suricata/suricata.yaml
5/2/2024 -- 10:38:22 - <Info> -- Disabling rules for protocol pgsql
5/2/2024 -- 10:38:22 - <Info> -- Disabling rules for protocol modbus
5/2/2024 -- 10:38:22 - <Info> -- Disabling rules for protocol dnp3
5/2/2024 -- 10:38:22 - <Info> -- Disabling rules for protocol enip
5/2/2024 -- 10:38:22 - <Info> -- Fetching https://rules.emergingthreats.net/o
pen/suricata-7.0.2/emerging.rules.tar.gz.
 100% - 4228540/4228540
5/2/2024 -- 10:38:28 - <Info> -- Done.
5/2/2024 -- 10:38:28 - <Info> -- Loading distribution rule file /etc/suricata
```

Ahora ya parece que tenemos cosas en Rules.

```
┌──(kali㉿kali)-[/var/lib/suricata/rules]
└─$ ls
classification.config  suricata.rules

┌──(kali㉿kali)-[/var/lib/suricata/rules]
└─$
```

Ahora podemos observar como se ha hecho correctamente.

```
┌──(kali㉿kali)-[/etc/suricata]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM
 mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 36576 rules successfully loaded, 0 r
ules failed
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 36579 signatures processed. 1204 are IP-only rules, 4944 are
 inspecting packet payload, 30219 inspect application layer, 108 are decod
er event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```