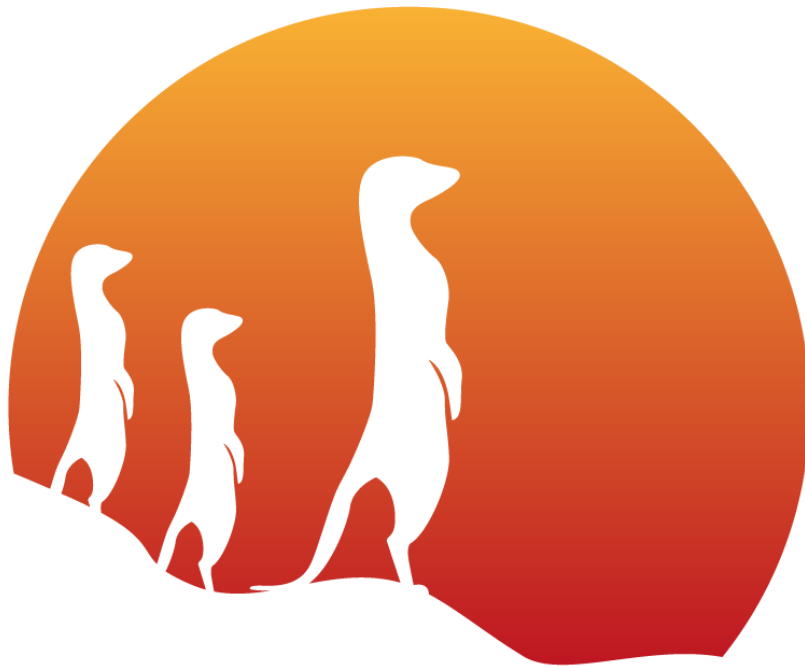




INSTALACIÓN Y CONFIGURACIÓN DE SURICATA

INCIDENTES DE CIBERSEGURIDAD



Contenido

1. Comando de instalación de suricata.....	2
2. Para que nos asocie un id que esté en la comunidad de suricata.	2
3. Comprobamos nuestra interfaz de red para ver si está igual que en el archivo suricata.yaml.	3
4. En el mismo archivo escribiremos una directiva.	3
5. Reiniciamos suricata para que se apliquen los cambios.....	3
6. Vamos a hacer que se apliquen algunas reglas básicas.	4
7. Para activar cualquiera de la lista usaremos enable-source junto al nombre. 4	
8. Ya tendríamos todo configurado, vamos a hacer un test al fichero de configuración.....	5

1. Comando de instalación de suricata.

sudo apt-get install suricata

```
(kali㉿kali)-[~]  
$ sudo apt-get install suricata  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no  
longer required:  
  cython3 debtags kali-debtags libjavascriptcoregtk-4.0-18
```

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

Cambiaremos el false por un true.

```
File Actions Edit View Help  
GNU nano 7.2 suricata.yaml *  
# Adds a 'community_id' field to EVE records  
# records a predictable flow ID that can be  
# output of other tools such as Zeek (Bro).  
#  
# Takes a 'seed' that needs to be same across  
# to make the id less predictable.  
# enable/disable the community id feature.  
community-id: true  
# Seed value for the ID output. Valid values  
community-id-seed: 0
```

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

```
(kali㉿kali)-[/etc/suricata]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.22.235.128 netmask 255.255.0.0 broadcast 172.22.255.255
    inet6 fe80::e437:802b:165:9825 prefixlen 64 scopeid 0x20<link>
    ether bc:24:11:4d:a7:d9 txqueuelen 1000 (Ethernet)
    RX packets 25898 bytes 76298867 (72.7 MiB)
    RX errors 0 dropped 2 overruns 0 frame 0
    TX packets 7439 bytes 701749 (685.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
# Linux high speed capture support
af-packet:
  - interface: eth0
    # Number of receive threads. "auto"
    #threads: auto
```

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.

```
#include:
# - include1.yaml
# - include2.yaml
detect-engine:
  - rule-reload: true
```

5. Reiniciamos suricata para que se apliquen los cambios.

```
(kali㉿kali)-[/etc/suricata]
$ sudo systemctl restart suricata
```

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.

```
(kali㉿kali)-[/etc/suricata]
$ suricata-update list-sources
5/2/2024 -- 10:23:29 - <Info> -- Using data-directory /var/lib/suricata.
5/2/2024 -- 10:23:29 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
5/2/2024 -- 10:23:29 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
5/2/2024 -- 10:23:29 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: scwx/enhanced
  Vendor: Secureworks
  Summary: Secureworks suricata-enhanced ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasure
s)
Name: scwx/malware
  Vendor: Secureworks
  Summary: Secureworks suricata-malware ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasure
s)
Name: scwx/security
  Vendor: Secureworks
```

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.

```
(kali㉿kali)-[/etc/suricata]
$ sudo suricata-update enable-source et/open
5/2/2024 -- 10:26:57 - <Info> -- Using data-directory /var/lib/suricata.
5/2/2024 -- 10:26:57 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
5/2/2024 -- 10:26:57 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
5/2/2024 -- 10:26:57 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
5/2/2024 -- 10:26:57 - <Info> -- Creating directory /var/lib/suricata/update/sources
5/2/2024 -- 10:26:57 - <Info> -- Source et/open enabled
```

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/suricata.yaml
5/2/2024 -- 10:38:22 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
5/2/2024 -- 10:38:22 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
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/open/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.
```