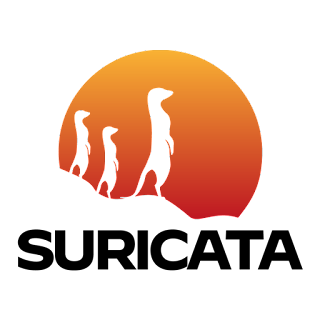
**Actividad Suricata**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Configuraciones previas**](#_g59i8ewd3ed3) **2**

[**2.1 Descarga, instalación y configuración de paquetes**](#_9cdwmqp67u7b) **2**

[**2.2 Comprobación**](#_aubrxqb617c0) **2**

[**3. Configuración de reglas**](#_u79m232doevd) **3**

[**3.1 Configurar una regla que detecte y alerte las conexiones a Facebook**](#_ykezcd8mw12i) **3**

[**3.1.1 Creación de la regla**](#_7h8n05y9vtqi) **3**

[**3.1.2 Comprobación**](#_vdqp81sjolde) **3**

[**3.2 Configurar una regla que detecte y alerte cuando, desde nuestra red interna, se haga alguna petición GET al exterior.**](#_rth59cja48a8) **3**

[**3.2.1 Creación de la regla**](#_rujoph41qes6) **3**

[**3.2.2 Comprobación**](#_32w9efi3bd2w) **4**

[**3.3 Configurar una regla que detecte y alerte cuando se realiza una conexión utilizando ssh.**](#_1iuw57e5w0zf) **4**

[**3.3.1 Creación de la regla**](#_wriw2chdy87v) **4**

[**3.3.2 Comprobación**](#_qxhosky5j5ie) **4**

[**3.4 Configurar una regla que detecta y alerta en el caso de que, desde nuestra red interna, se esté intentando acceder a un sitio web que pueda tratarse de una simulación de la web de Paypal (ataque phishing)**](#_6ilrrnp9uspc) **5**

[**3.4.1 Creación de la regla**](#_94jfw5w5nl3j) **5**

[**3.4.2 Comprobación**](#_xtb32twvt1qy) **5**

[**3.5 Configurar un conjunto de reglas capaces de detectar y alertar cuando nuestra máquina está recibiendo un escaneo de puertos.**](#_emj3ogiaubjr) **6**

[**3.5.1 Creación de la regla**](#_6aml79uy8oz) **6**

[**3.5.2 Comprobación**](#_nk8rvpmhg9fd) **6**

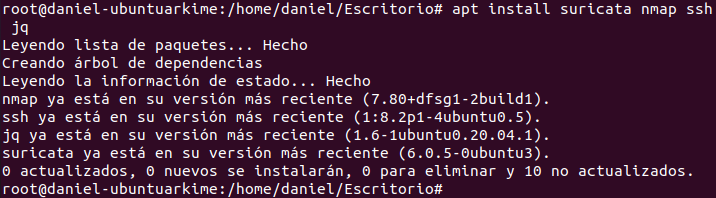
[**3.6 Utilizar JQ para realizar una búsqueda concreta (la que tú elijas), sobre el archivo json que se ha generado durante nuestras pruebas.**](#_s1hjn5vyl9vs) **7**

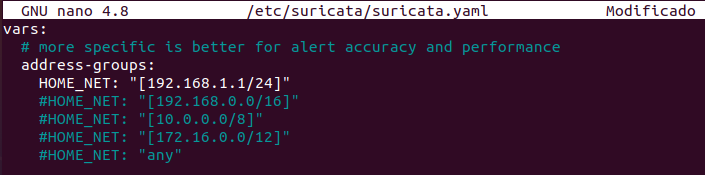
[**3.7 Configurar Suricata como IPS para que, a partir de las reglas que hemos creado en los apartados a, b, c y d, además de alertar, también bloquee esas conexiones**](#_wfpxskmgij44) **7**

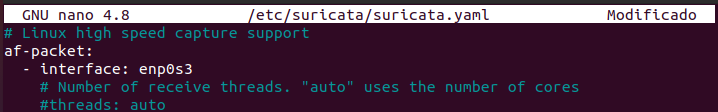
[**3.8 Descarga y añade las reglas de la comunidad ‘Emerging Threats’**](#_sbvtw5rj6nga) **8**

# **2. Configuraciones previas**

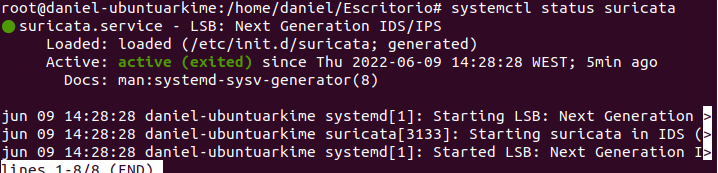
### **2.1 Descarga, instalación y configuración de paquetes**







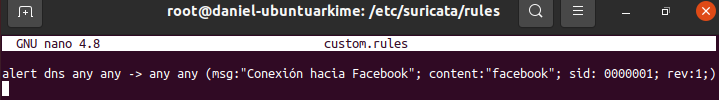
### **2.2 Comprobación**



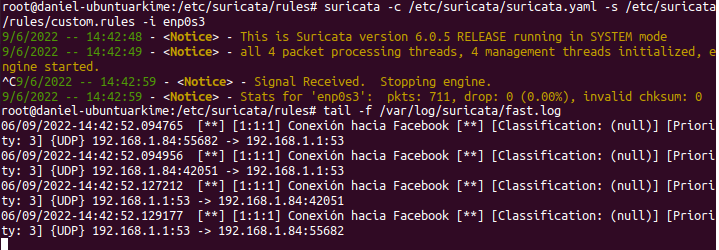
# **3. Configuración de reglas**

### **3.1 Configurar una regla que detecte y alerte las conexiones a Facebook**

#### **3.1.1 Creación de la regla**

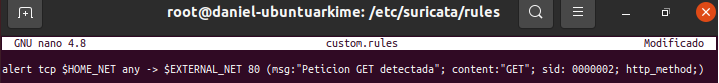


#### **3.1.2 Comprobación**

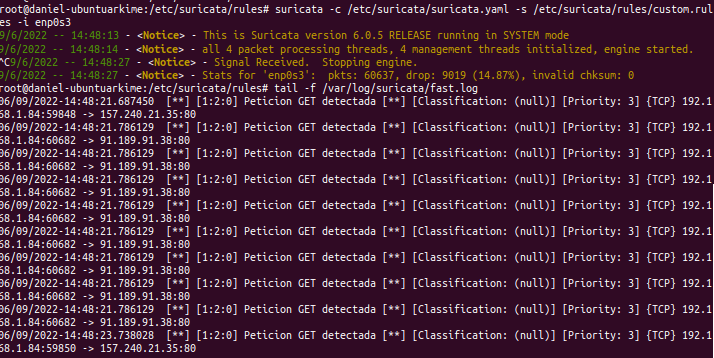


### **3.2 Configurar una regla que detecte y alerte cuando, desde nuestra red interna, se haga alguna petición GET al exterior.**

#### **3.2.1 Creación de la regla**

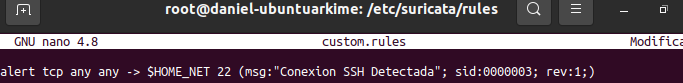


#### **3.2.2 Comprobación**

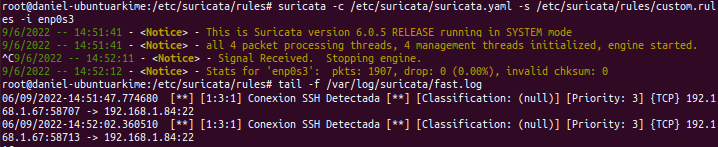


### **3.3 Configurar una regla que detecte y alerte cuando se realiza una conexión utilizando ssh.**

#### **3.3.1 Creación de la regla**

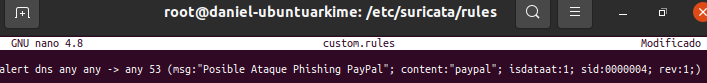


#### **3.3.2 Comprobación**

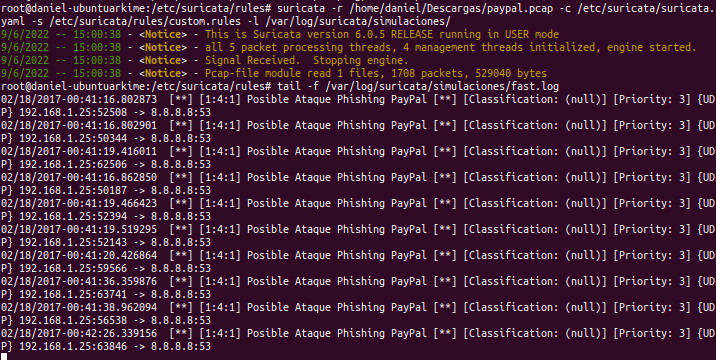


### **3.4 Configurar una regla que detecta y alerta en el caso de que, desde nuestra red interna, se esté intentando acceder a un sitio web que pueda tratarse de una simulación de la web de Paypal (ataque phishing)**

#### **3.4.1 Creación de la regla**

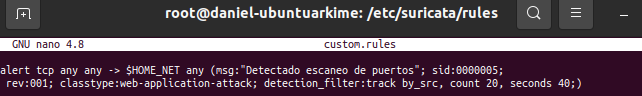


#### **3.4.2 Comprobación**

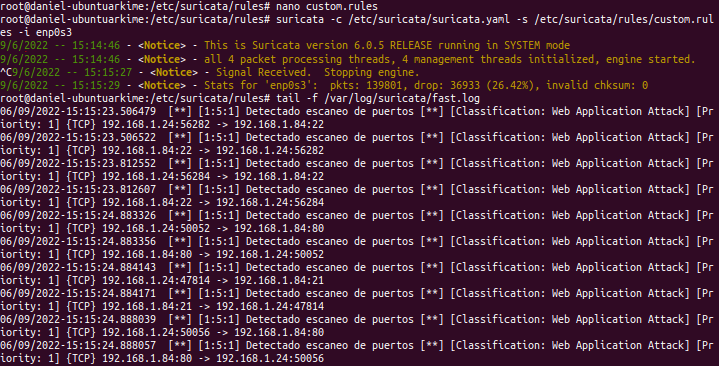


### **3.5 Configurar un conjunto de reglas capaces de detectar y alertar cuando nuestra máquina está recibiendo un escaneo de puertos.**

#### **3.5.1 Creación de la regla**



#### **3.5.2 Comprobación**



### **3.6 Utilizar JQ para realizar una búsqueda concreta (la que tú elijas), sobre el archivo json que se ha generado durante nuestras pruebas.**

Realizaremos una búsqueda donde el protocolo sea TCP, así se mostraran las detecciones de escaneo de puertos.

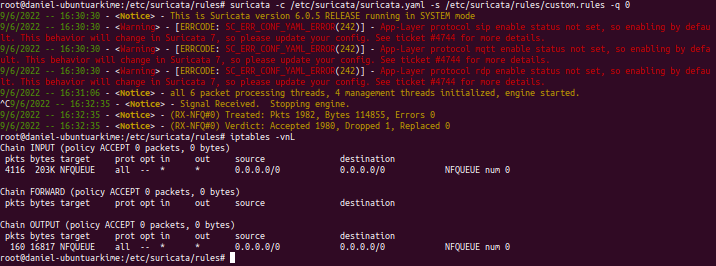


### **3.7 Configurar Suricata como IPS para que, a partir de las reglas que hemos creado en los apartados a, b, c y d, además de alertar, también bloquee esas conexiones**

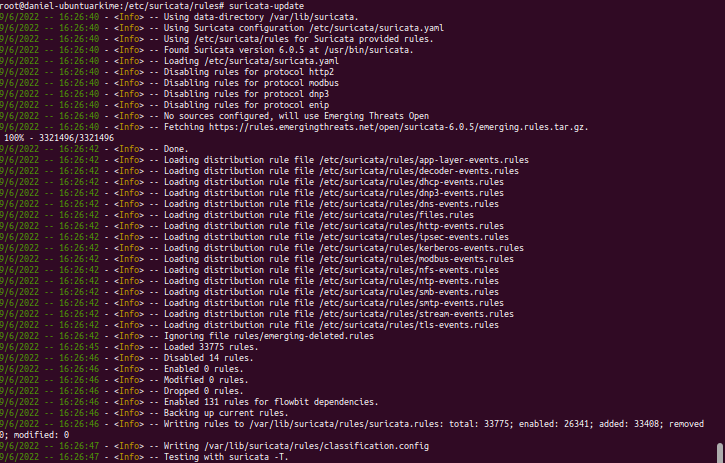
Necesitamos de estos comandos para que Suricata actúe como IPS.



Ejecutamos Suricata, con el parámetro -q, para hacer uso de la cola 0:



### **3.8 Descarga y añade las reglas de la comunidad ‘Emerging Threats’**

.

Comprobamos revisando el fichero donde se almacenan las reglas:

