**Actividad Stack ELK**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

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

[**2. Configurar varias reglas de detección en el IDS Suricata:**](#_g59i8ewd3ed3) **2**

[**2.1 Crear una regla que detecte si se visita sitios web (HTTP o HTTPS) cuyo nombre de dominio contenga la palabra prohibida hack:**](#_ykezcd8mw12i) **2**

[**2.2 Crear una regla que detecte si se establece cualquier tipo de comunicación con un equipo ubicado en un país prohibido.**](#_1tbo83qyz512) **3**

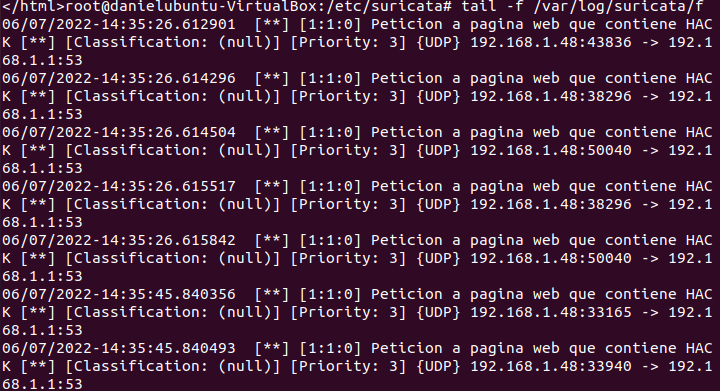
[**3. Instalar el servidor SSH en el equipo Linux ELK y configurar Logstash para que acceda al archivo de log del servicio SSH y pueda capturar sus eventos.**](#_5l44hk1xcz9y) **4**

[**4. Crear un nuevo dashboard en el SIEM ELK que muestre las siguientes gráficas a partir de los eventos recibidos:**](#_9ujyid9lc5yt) **6**

# **2. Configurar varias reglas de detección en el IDS Suricata:**

### **2.1 Crear una regla que detecte si se visita sitios web (HTTP o HTTPS) cuyo nombre de dominio contenga la palabra prohibida hack:**

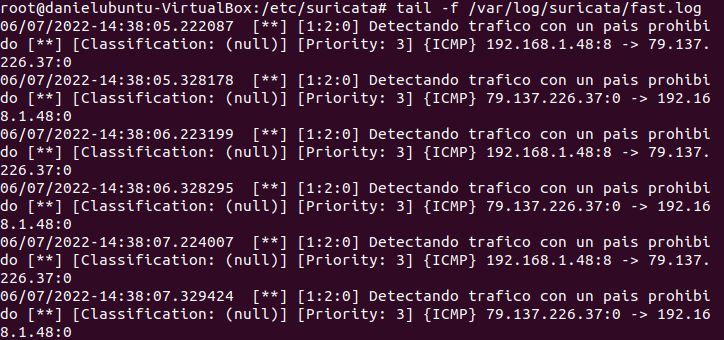
### 



### **2.2 Crear una regla que detecte si se establece cualquier tipo de comunicación con un equipo ubicado en un país prohibido.**

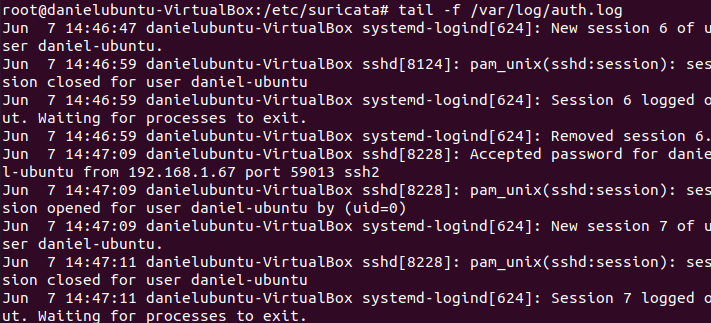
### 

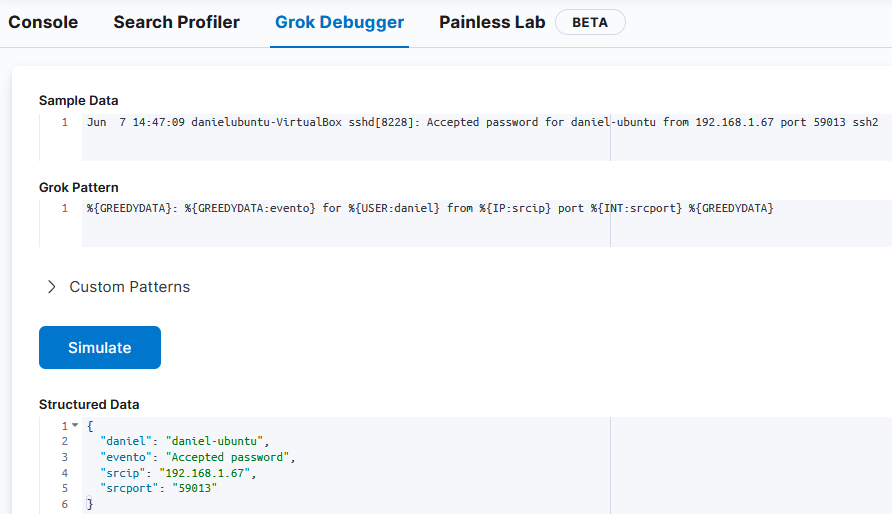


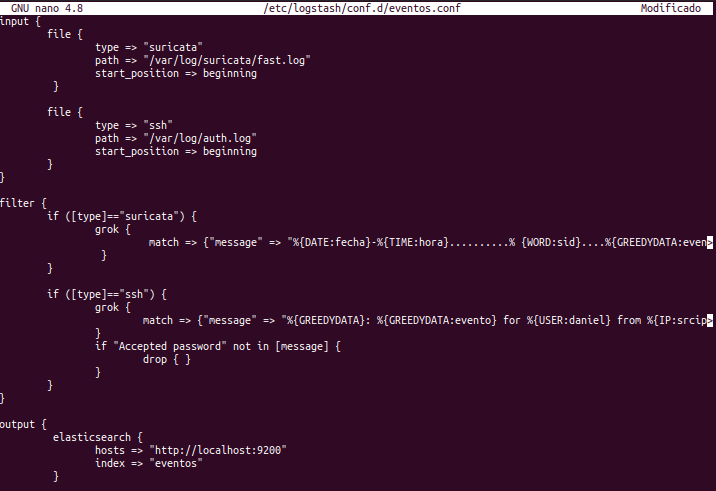


# **3. Instalar el servidor SSH en el equipo Linux ELK y configurar Logstash para que acceda al archivo de log del servicio SSH y pueda capturar sus eventos.**

# 







# **4. Crear un nuevo dashboard en el SIEM ELK que muestre las siguientes gráficas a partir de los eventos recibidos:**

