

# **Suricata: Guía Completa de Instalación, Configuración, Pruebas, Administración y Ejemplos (con Reglas Predeterminadas)**

## **¿Qué es Suricata?**

Suricata es un sistema de detección y prevención de intrusiones (IDS/IPS) de código abierto. Monitorea el tráfico de red en tiempo real, lo analiza en busca de patrones sospechosos y puede tomar medidas para bloquear actividades maliciosas.

## **Funcionamiento de Suricata (Resumen por Puntos):**

- **Captura de Tráfico:** Suricata "escucha" el tráfico de red que pasa por una interfaz específica.
- **Decodificación:** Descompone los paquetes de datos en elementos comprensibles (direcciones IP, puertos, protocolos, etc.).
- **Inspección Profunda de Paquetes (DPI):** Analiza el contenido de los paquetes para identificar aplicaciones, comandos y posibles datos maliciosos.
- **Comparación con Reglas:** Compara el tráfico con reglas predefinidas que describen patrones de actividad maliciosa o sospechosa.
- **Generación de Alertas:** Si el tráfico coincide con una regla, Suricata genera una alerta con detalles del evento.
- **Registro:** Guarda un registro detallado de todos los eventos, incluyendo alertas, para análisis posterior.
- **Prevención (Opcional):** Si se configura como IPS, Suricata puede bloquear el tráfico malicioso en tiempo real.

## **Listas de Reglas:**

Las reglas son el núcleo de Suricata. Son instrucciones que definen qué tráfico es sospechoso. Suricata viene preconfigurado para usar las reglas de Emerging Threats Open (ET Open), pero debes descargarlas.



## **Instalación y Configuración:**

### **Preparación del Sistema:**

Objetivo: Asegurarse de que el sistema esté actualizado y tenga los repositorios necesarios para instalar Suricata.

Comandos:

- `sudo apt update`
- `sudo apt upgrade`

### **Instalación de Suricata:**

Objetivo: Descargar e instalar el software Suricata y sus componentes necesarios.

Debian y Kali Linux:

`sudo apt install suricata`

### **En Ubuntu:**

- `sudo add-apt-repository ppa:oisf/suricata-stable`
- `sudo apt update`
- `sudo apt install suricata`

## Descarga de Reglas:

**Objetivo:** Obtener las reglas de detección de ET Open, que son esenciales para que Suricata funcione correctamente.

Comando:

- `sudo suricata-update`

## Configuración:

**Objetivo:** Personalizar el comportamiento de Suricata según tus necesidades y entorno de red.

Cómo: Edita el archivo de configuración `suricata.yaml` (ubicado en `/etc/suricata/suricata.yaml`).

## Ejemplo de Configuración (¡SOLO UN EJEMPLO! Ajusta según tus necesidades):

### YAML

---

```
-----
af-packet:
  - interface: eth0 # Especifica la interfaz de red a monitorear (e.g., eth0).

default-rule-path: /var/lib/suricata/rules # Ruta a las reglas de ET Open.

outputs:
  - fast: {} # Habilita el registro rápido en formato binario.
  - eve-log: # Habilita el registro en formato JSON (fácil de analizar).
    enabled: yes
    filetype: json

# Ejemplo de regla personalizada (detecta intentos de acceso SSH desde una IP
# específica)
vars:
  $EXTERNAL_NET: "[192.168.1.0/24,10.0.0.0/8]" # Define redes externas.
  $SSH_PORT: 22 # Define el puerto SSH.

rule:
  - action: alert # Genera una alerta si la regla coincide.
    protocol: tcp # Aplica la regla al tráfico TCP.
    source: $EXTERNAL_NET any # Tráfico proveniente de redes externas.
    destination: any $SSH_PORT # Tráfico dirigido al puerto SSH.
    msg: "External SSH connection attempt" # Mensaje de la alerta.
```

---

## **Validación de la Configuración:**

**Objetivo:** Asegurarse de que el archivo de configuración no tenga errores de sintaxis que puedan impedir que Suricata funcione correctamente.

### **Comando:**

- `sudo suricata -T`

## **Inicio, Detención y Administración de Suricata:**

Objetivo: Iniciar, detener y administrar el servicio de Suricata.

Comandos:

- `sudo systemctl start suricata` # Inicia Suricata.
- `sudo systemctl stop suricata` # Detiene Suricata.
- `sudo systemctl restart suricata` # Reinicia Suricata.
- `sudo systemctl status suricata` # Verifica el estado de Suricata.
- `sudo systemctl enable suricata` # Habilita Suricata para que se inicie automáticamente al arrancar el sistema.
- `sudo systemctl disable suricata` # Deshabilita el inicio automático de Suricata.

## **Pruebas:**

- Ataques Simulados: Utiliza herramientas como Metasploit o Nmap para simular ataques y verificar si Suricata los detecta.
- Generación de Tráfico Malicioso: (Con precaución) Genera tráfico que coincida con tus reglas para probar la detección.
- Análisis de Registros: Examina los archivos de registro de Suricata (ubicados en `/var/log/suricata/`) para verificar que los eventos se registran correctamente.

## **Herramientas Adicionales:**

- Suricata Management Console (SMC) o Scirius Community Edition (SCE): Facilitan la gestión de reglas y la configuración de Suricata.
- EveBox o Kibana: Visualizan y analizan los registros y alertas de Suricata de forma gráfica.