

Snort 3

¿Qué es Snort 3?

Snort es esencialmente un **analizador de tráfico de red** en tiempo real que inspecciona los paquetes de datos que fluyen a través de una red.

- **Sistema Basado en Reglas:** Su funcionamiento se basa en un motor que compara el tráfico de red con un extenso conjunto de **reglas** (firmas) predefinidas y personalizables. Estas reglas definen qué patrones de tráfico son maliciosos o sospechosos (por ejemplo, intentos de *exploit*, tráfico de *malware*, o *escaneo de puertos*).
- **Código Abierto:** Es un software gratuito y de código abierto, desarrollado inicialmente por Martin Roesch y actualmente mantenido por Cisco.
- **Snort 3:** Esta versión se enfoca en mejoras significativas respecto a las versiones anteriores, incluyendo:
 - **Mejor Rendimiento:** Soporte para el procesamiento de paquetes con **múltiples hilos (multithreading)**, aprovechando mejor los procesadores modernos.
 - **Configuración Simplificada:** Mayor facilidad para escribir reglas y una estructura de configuración más modular.
 - **Detección Automática de Servicios:** Capacidad para detectar automáticamente servicios de red sin tener que especificar puertos manualmente.

¿Para qué se Utiliza?

Snort 3 se utiliza principalmente para **monitorizar y proteger las redes** en tres modos operativos clave:

1. Sistema de Detección de Intrusiones (IDS)

- **Detección de Amenazas:** Es su uso principal. Snort monitoriza el tráfico, lo analiza contra sus reglas y **genera alertas** cuando detecta actividad que coincide con una firma de ataque conocido o un patrón sospechoso (como

desbordamientos de búfer, ataques de Denegación de Servicio (DoS), o actividad de *gusanos*).

- **Análisis Forense:** Registra el tráfico de red y las alertas, lo que permite a los analistas de seguridad investigar incidentes *a posteriori*.

2. Sistema de Prevención de Intrusiones (IPS)

- **Bloqueo en Tiempo Real:** Configurado en modo IPS (*inline*), Snort no solo detecta el tráfico malicioso, sino que también lo **bloquea activamente** antes de que pueda llegar a su destino dentro de la red, actuando como una capa de seguridad proactiva.

3. Registrador de Paquetes (*Packet Logger*)

- **Captura de Tráfico:** Puede utilizarse como un simple **capturador de paquetes (sniffer)**, registrando todo el tráfico que pasa a través de la interfaz de red en archivos (logs) para su posterior análisis o depuración de red.

En resumen, Snort 3 es una herramienta **poderosa y flexible** fundamental para cualquier equipo de seguridad que necesite visibilidad del tráfico de red, detección de amenazas y capacidad de prevención activa contra ciberataques.

La instalación más común para Snort 3 en versiones recientes de Ubuntu se realiza a través de la **compilación desde el código fuente**, ya que el paquete apt a veces instala una versión anterior (Snort 2) o no está disponible con todas las características.

Instalación

Pasos para Instalar y Configurar Snort 3 en Ubuntu 24.04

Paso 1: Actualizar el Sistema e Instalar Dependencias

Abre tu terminal y ejecuta los siguientes comandos para asegurarte de que tu sistema está actualizado y tienes todas las librerías necesarias para compilar Snort.

1. Actualizar el sistema:

```
sudo apt update && sudo apt upgrade -y
```

2. Instalar dependencias de compilación:

```
sudo apt install -y build-essential libpcap-dev libpcre3-dev  
libdumbnet-dev zlib1g-dev liblzma-dev openssl libssl-dev ethtool
```

```
sudo apt install build-essential autoconf libtool
```

Paso 2: Descargar y Compilar Snort 3

Descargaremos la última versión estable de Snort 3 desde el sitio web oficial y la compilaremos.

1. Descargar el código fuente de Snort 3:

(Busca la versión más reciente en la página oficial si esta ha cambiado.)

```
wget
```

```
https://github.com/snort3/libdaq/archive/refs/tags/v3.0.21.tar.gz
```

2. Descomprimir el archivo:

```
tar -xf libdaq-3.0.21.tar.gz
```

3. Acceder al directorio descomprimido:

```
cd libdaq-3.0.21
```

4. Configurar la compilación y compilar e instalar:

```
./bootstrap
```

```
./configure
```

```
make  
sudo make install
```

Siguiente Paso: Instalación de Snort 3

Ahora que tienes instalada la librería DAQ (Data Acquisition), el sistema está listo para compilar e instalar el motor principal de Snort 3, que depende de ella.

Necesitamos descargar las otras librerías que identificaste anteriormente:

1. Descargar las Librerías Restantes

Vamos a retroceder al directorio *home* y descargar los otros dos componentes principales que necesitarás.

Retrocede al directorio *home*

```
cd ~
```

Descargar el motor principal de Snort 3

```
wget  
https://github.com/snort3/snort3/archive/refs/tags/3.9.5.0.zip -  
O snort3-3.9.5.0.zip
```

```
sudo apt install unzip  
unzip snort3-3.9.5.0.zip  
cd snort3-3.9.5.0
```

(Nota: El nombre del directorio podría ser *snort3-3.9.5.0*, verifica con *ls*.)

3. Configurar y Compilar Snort 3

A diferencia de libdaq, Snort 3 utiliza **cmake** para la configuración y compilación.

1. Instalar dependencias de compilación adicionales (si no lo hiciste al inicio):

```
sudo apt install cmake libluajit-5.1-dev libhwloc-dev  
sudo apt install flex  
sudo apt install libpcre2-dev
```

2. Ejecutar el script de configuración de CMake:

```
./configure_cmake.sh --prefix=/usr/local/snort
```

3. Compilar e instalar (dentro del nuevo directorio build):

```
cd build  
make -j $(nproc)  
sudo make install
```

Una vez que estos pasos se completen, Snort 3.9.5.0 debería estar instalado en /usr/local/snort/.

Todos los archivos binarios, librerías, archivos de configuración, módulos DAQ, y documentación se han copiado a sus destinos finales bajo el prefijo que especificamos:
/usr/local/snort/.

Verificación y Pruebas Iniciales

Ahora que Snort está instalado, el siguiente paso es verificar que el binario se ejecuta correctamente y que puede detectar la librería DAQ que compilamos.

1. Verificar la Instalación de Snort

Debido a que instalamos Snort en `/usr/local/snort/bin/`, debemos llamar al binario usando esa ruta completa o añadiendo ese directorio a tu PATH.

Ejecuta el siguiente comando para verificar la versión instalada:

```
/usr/local/snort/bin/snort -V
```

```
' ,,_      -*> Snort++ <*-  
o" )~ Version 3.9.5.0  
' ' By Martin Roesch & The Snort Team  
http://snort.org/contact#team  
Copyright (C) 2014-2025 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using DAQ version 3.0.21  
Using libpcap version 1.10.4 (with TPACKET_V3)  
Using LuaJIT version 2.1.1703358377  
Using LZMA version 5.4.5  
Using OpenSSL 3.0.13 30 Jan 2024  
Using PCRE2 version 10.42 2022-12-11  
Using ZLIB version 1.3
```

2. Verificar la Configuración Básica

Ahora, comprueba que Snort puede encontrar el archivo de configuración principal (`snort.lua`) que se instaló y que las rutas son correctas. Esto validará la configuración base.

```
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort/snort.lua
```

```
-----  
fast pattern groups  
    to_server: 1  
    to_client: 1  
-----  
search engine (ac_bnfa)  
    instances: 2  
    patterns: 438  
    pattern chars: 2602  
    num states: 1832  
    num match states: 392  
    memory scale: KB  
    total memory: 71.2812  
    pattern memory: 19.6484  
    match list memory: 28.4375  
    transition memory: 22.9453  
appid: MaxRSS diff: 2944  
appid: patterns loaded: 300  
-----  
pcap DAQ configured to passive.  
  
Snort successfully validated the configuration (with 0 warnings).  
o")~ Snort exiting
```

Si ambos comandos se ejecutan sin errores (especialmente el segundo), significa que Snort está listo para ser configurado y usado para monitorear el tráfico.

El mensaje final **Snort successfully validated the configuration (with 0 warnings)**. es la confirmación que necesitábamos. Esto significa que Snort ha cargado correctamente:

1. El archivo de configuración principal
`/usr/local/snort/etc/snort/snort.lua`.
2. Todos los módulos internos y *service inspectors* listados.
3. Las reglas predeterminadas de ejemplo (`file_magic.rules`),
cargando **219 reglas** sin errores.
4. La configuración del **DAQ** (pcap DAQ configured to passive).

El sistema ahora está listo para la fase de **configuración de entorno y reglas**.

Pasos Iniciales de Configuración de Snort 3

Para que Snort sea útil, debes realizar dos tareas clave:
definir la red que vas a proteger (la red doméstica) y obtener el *set* completo de reglas.

1. Configurar la Red Doméstica (HOME_NET)

Debes editar el archivo de configuración por defecto para especificar el rango de IP de tu red local. Esto es crítico para que Snort sepa qué tráfico es interno (de confianza) y cuál es externo (potencialmente hostil).

- 1. Edita el archivo de configuración principal:**

```
sudo nano /usr/local/snort/etc/snort/snort.lua
```

2. Busca la sección de variables de entorno:

Localiza la línea donde se define HOME_NET. Originalmente puede estar comentada o definida como any.

Lua

```
-- Define HOME_NET and EXTERNAL_NET  
-- The default is 'any'  
-- HOME_NET = 'any'  
-- EXTERNAL_NET = 'any'
```

3. Actualiza HOME_NET:

Reemplaza any con el rango IP de tu red. Dado que estás en una VirtualBox y en Kali Linux, tu red local probablemente esté en el rango 192.168.X.0/24 o similar. Usa el resultado de ip a para verificar.

- **Ejemplo:** Si tu red es 192.168.1.0/24:

```
HOME_NET = '192.168.1.0/24'
```

```
EXTERNAL_NET = '!$HOME_NET'
```

```
-- HOME_NET and EXTERNAL_NET must be set now  
-- setup the network addresses you are protecting  
HOME_NET = '192.168.1.0/24'  
  
-- set up the external network addresses.  
-- (leave as "any" in most situations)  
EXTERNAL_NET = '!$HOME_NET'  
  
include 'snort_defaults.lua'
```

4. Guarda y sal (Ctrl+O, Ctrl+X).

2. Obtener Reglas (Opcional, pero Recomendado)

Las 219 reglas que cargaste son solo las de ejemplo (file_magic). Necesitas reglas de detección de amenazas reales.

- Puedes obtener el *set* de reglas gratuitas (Community Rules) o las reglas actualizadas de Talos (requieren registro en Snort.org).
- **Recomendación:** Descarga las reglas de la comunidad.

Pasos de ejemplo para reglas de la comunidad (Community Rules):

1. Navega a un directorio temporal:

```
cd ~
```

2. Busca la URL de las reglas de la comunidad de Snort 3

El enlace de descarga para las reglas de la comunidad para Snort 3 es:

<https://www.snort.org/downloads/community/snort3-community-rules.tar.gz>

3. Descargar y Configurar Reglas de la Comunidad

1. Descargar las reglas:

```
cd ~
```

```
wget https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
```

2. Descomprimir y mover las reglas:

Mueve los archivos .rules al directorio de reglas de tu instalación de Snort (/usr/local/snort/etc/snort/rules/).

Primero, crea el directorio si no existe:

```
sudo mkdir -p /usr/local/snort/etc/snort/rules
```

```
sudo tar -xf snort3-community-rules.tar.gz -C /usr/local/snort/etc/snort/rules/ --strip-components 1
```

(--strip-components 1 es necesario para eliminar el directorio principal dentro del .tar.gz.)

3. Habilitar las reglas en snort.lua:

Crear un Archivo de Reglas de Referencia (Si Aún No Existe)

Si no tienes un archivo de reglas vacío o con referencias, vamos a crear uno.

1. Crea el archivo:

```
sudo nano /usr/local/snort/etc/snort/rules/local.rules
```

2. Añade una regla de prueba (opcional, pero buena práctica):

```
alert icmp any any -> $HOME_NET any (msg:"Test ICMP Echo Request";  
sid:1000000; rev:1;)
```

```
GNU nano 7.2                               /usr/local/snort/etc/snort/rules/local.rules *  
alert icmp any any -> $HOME_NET any (msg:"Test ICMP Echo Request"; sid:1000000; rev:1;)  
[REDACTED]
```

Guarda y sal.

Guía de Uso Esencial de Snort 3

El ejecutable principal de Snort 3 es /usr/local/snort/bin/snort. El uso más básico siempre requiere especificar el archivo de configuración.

1. Sintaxis Básica de Ejecución

El comando fundamental para ejecutar Snort es:

```
/usr/local/snort/bin/snort [MODO] [OPCIONES]
```

2. Modos Operacionales Clave

Snort 3 opera principalmente en dos modos que determinan su función:

Modo	Comando	Descripción
Aspiradora / Sniffer (Modo Predeterminado)	sudo /usr/local/snort/bin/snort -i <interfaz>	Simplemente lee los paquetes en vivo de una interfaz de red,

Modo	Comando	Descripción
		mostrando los encabezados en la consola. Es útil para diagnóstico.
Detección de Intrusos (IDS)	sudo /usr/local/snort/bin/snort -c <config> -i <interfaz>	Este es el modo estándar. Ejecuta el motor de reglas (IPS) y genera alertas si encuentra tráfico malicioso.
Lectura de PCAP	sudo /usr/local/snort/bin/snort -c <config> -r <archivo.pcap>	En lugar de escuchar en vivo, procesa un archivo de captura de tráfico (.pcap) contra tus reglas. Ideal para análisis forense.

3. Uso en Modo IDS (Sistema de Detección de Intrusos)

Este es el modo más importante para la seguridad de la red.

3.1. Identificar la Interfaz de Red

Antes de ejecutar Snort, necesitas saber qué interfaz usar. Si estás en VirtualBox, probablemente sea eth0 o enp0s3.

ip a

3.2. Ejecutar Snort en Modo IDS

Ejecuta Snort en la interfaz de red con tu archivo de configuración. Usa sudo porque necesita acceso de bajo nivel a la red.

sudo /usr/local/snort/bin/snort -i enp0s3

- **-c**: Especifica el archivo de configuración Lua que acabas de modificar.
- **-i**: Especifica la interfaz de red para escuchar (ej. `eth0`).

Snort está en su **modo Sniffer/Aspiradora** (`-i enp0s3` sin un archivo de configuración `-c`). Esto confirma lo siguiente:

1. **El binario de Snort funciona.**
2. **Los permisos de sudo son correctos.**
3. **Snort puede encontrar y acceder a la interfaz de red `enp0s3`** (que es tu interfaz activa en VirtualBox).
4. **Snort está escuchando** (Commencing packet processing).

Pasos de Uso en Modo Sniffer

En este modo, Snort está funcionando como un `tcpdump` avanzado. Si empiezas a generar tráfico en tu máquina virtual (por ejemplo, navegando a un sitio web o haciendo un ping), Snort mostrará los encabezados de los paquetes.

- Para ver los encabezados de paquetes detallados, haz un ping a una IP externa desde otra terminal:

```
ping 8.8.8.8
```

- **Para detener Snort** en este modo, simplemente presiona **Ctrl+C**.

```
rx_bytes: 70241
-----
codec
    total: 529          (100.000%)
    discards: 37        ( 6.994%)
    arp: 58            ( 10.964%)
    eth: 529           (100.000%)
    icmp4: 20           ( 3.781%)
    icmp6: 41           ( 7.750%)
    icmp6_ip: 12         ( 2.268%)
    igmp: 139           ( 26.276%)
    ipv4: 379           ( 71.645%)
    ipv6: 92            ( 17.391%)
    ipv6_hop_opts: 25   ( 4.726%)
    tcp: 45             ( 8.507%)
    udp: 224            ( 42.344%)
-----
Module Statistics
-----
detection
    analyzed: 529
-----
tcp
    bad_tcp4_checksum: 17
    bad_tcp6_checksum: 14
-----
udp
    bad_udp4_checksum: 4
-----
Summary Statistics
```

Análisis del Resumen de Paquetes

- **daq received: 529:** Snort recibió 529 paquetes de la red.
- **daq analyzed: 529:** Snort pudo analizar todos los paquetes recibidos.
- **detection analyzed: 529:** El motor de detección (IPS) también procesó todos los paquetes (aunque sin reglas de detección de amenazas cargadas).
- **Distribución de Protocolos:** El tráfico es típico de una red moderna, con una gran cantidad de tráfico IPv4 (71.645%), IPv6 (17.391%), y mucho tráfico de multidifusión (igmp: 139).
- **Advertencias de Checksum:** Vemos bad_tcp4_checksum (17) y bad_tcp6_checksum (14). Esto es **común y normal** en entornos de máquinas virtuales debido a la descarga de checksum (checksum offloading) que realiza el hardware o la capa de virtualización. Snort lo detecta, pero no es necesariamente un error.

Siguiente Paso: Activar la Detección de Intrusos (Modo IDS)

Ahora que sabes que Snort puede ver el tráfico, el siguiente paso es ejecutarlo en su función principal: **el modo IDS**, donde utiliza tu archivo de configuración snort.lua y las miles de reglas de la comunidad que intentamos cargar.

Para poner Snort en modo IDS, necesitas cargar la configuración:

```
sudo /usr/local/snort/bin/snort -c  
/usr/local/snort/etc/snort/snort.lua -i enp0s3
```

3.3. Opciones Comunes Adicionales

Opción	Propósito	Ejemplo
-A console	Envía las alertas directamente a la consola (útil para pruebas).	... -i eth0 -A console
-l /var/log/snort	Escribe los logs de Unified2 (binarios de Snort) en un directorio específico. Necesitas crear el directorio primero.	... -i eth0 -l /var/log/snort
-D	Ejecuta Snort en modo Daemon (en segundo plano), ideal para producción.	... -i eth0 -D

4. Interpretación de Resultados y Logs

Cuando Snort detecta una amenaza, genera una **Alerta**.

4.1. Ejemplo de Alerta en Consola (-A console)

Si usas la opción -A console, verás una salida similar a esta (asumiendo que tienes una regla ICMP simple):

```
02/11-12:00:00.123456 [**] [1:1000000:1] Test ICMP Echo Request  
[**] [Priority: 0] {ICMP} 192.168.1.5 -> 192.168.1.1
```

- [1:1000000:1]: El **SID** (Signature ID) de la regla. Este número es único y es la clave para identificar la amenaza.
- Test ICMP Echo Request: El **MSG** (Mensaje) de la regla, que describe la amenaza.
- {ICMP}: El protocolo involucrado.
- 192.168.1.5 -> 192.168.1.1: La dirección IP de origen y destino.

4.2. Log de Eventos (-l y Logs Binarios)

En producción, Snort genera logs en formato binario (Unified2) para un rendimiento rápido. Para leer estos logs, necesitas herramientas como **u2spewfoo** (que se instaló con Snort).

1. Ejecuta Snort en modo logging:

```
sudo mkdir -p /var/log/snort
sudo /usr/local/snort/bin/snort -c
/usr/local/snort/etc/snort/snort.lua -i enp0s3 -l /var/log/snort
```

2. Detén Snort (presionando Ctrl+C).

3. Convierte los logs binarios a texto:

```
/usr/local/snort/bin/u2spewfoo /var/log/snort/*
```

Esto mostrará el contenido de las alertas y los paquetes capturados en un formato legible.

```
feval@feval-VirtualBox:~$ /usr/local/snort/bin/u2spewfoo /var/log/snort/*
ERROR: Failed to open file: /var/log/snort/*
      Errno: No such file or directory
ERROR: failed to create new iterator with file: /var/log/snort/*
```

El error al final con u2spewfoo ocurre por una razón muy sutil: **Snort solo escribe logs de alerta cuando detecta algo malicioso, o logs de tráfico si lo configuras explícitamente.**

```
ERROR: Failed to open file: /var/log/snort/*
```

¿Por qué ocurre?

1. **Snort se Ejecutó Correctamente:** Al revisar las estadísticas de tu ejecución de Snort:
 - received: 26 y analyzed: 26: Esto confirma que Snort estuvo activo, capturó 26 paquetes de la interfaz enp0s3 y los procesó.
 - ^C** caught int signal: Confirmas que detuviste Snort manualmente (probablemente con Ctrl + C).
 - **No hay Alertas:** La sección de estadísticas de Snort **no muestra ninguna alerta** generada (la mayoría de los 26 paquetes eran tráfico de red normal como ARP, ICMP6, IGMP y UDP).
2. **No hay Archivos de Log:** Por defecto, Snort solo genera archivos de log de formato **unified2** (los que lee u2spewfoo) cuando:
 - **Genera una alerta:** Cuando detecta una amenaza que coincide con las reglas cargadas.
 - **Se le pide que registre todo el tráfico:** Esto requiere una opción de salida específica.
3. **La Carpeta Sigue Vacía:** Como no hubo alertas y no configuraste un registro completo de paquetes, Snort no creó ningún archivo de log en /var/log/snort. Por lo tanto, cuando ejecutas /usr/local/snort/bin/u2spewfoo /var/log/snort/*, el *shell* intenta expandir * pero no encuentra archivos, resultando en el error "No such file or directory".

Cómo Generar el Log

Tienes dos opciones para que u2spewfoo funcione:

Opción 1: Forzar una Alerta (Recomendada para Pruebas)

Debes generar tráfico que **active una de las 219 reglas** que Snort cargó.

1. **Regla de Prueba (Ping):** La forma más fácil de asegurarte de que Snort generará un log es usando la opción **-T (Test)**

o, mejor aún, añadiendo reglas de prueba. Si estás en un entorno de prueba, puedes modificar el archivo snort.lua para añadir una regla de prueba que se active con un simple ping.

```
ping 8.8.8.8
```

2. **Generar Tráfico Malicioso (Si tienes reglas activas):** Si tienes reglas de detección de intrusiones cargadas (que en tu caso solo cargaste file_id por defecto, que son muy limitadas), deberías simular un ataque o un escaneo de puertos.

Opción 2: Generar un Log de Paquetes (Si no hay Alertas)

Si quieres ver el log de los 26 paquetes que capturó (aunque no sean alertas), debes añadir una opción de **salida de tráfico explícita** a tu comando de Snort:

Añade la opción **-K ascii** o **--dump-payload** para forzar la salida de *Logs de tráfico* legibles por humanos, o edita el archivo snort.lua para configurar la salida unified2 aunque no haya alertas.

Comando de Ejemplo con Salida Verbosa

Simplemente ejecuta Snort en modo "**verbose**" con **-A console** y sin especificar el *output* de logs, lo que te mostrará las alertas directamente en pantalla:

```
sudo /usr/local/snort/bin/snort -c  
/usr/local/snort/etc/snort/snort.lua -i enp0s3 -A alert_fast
```

Comando de Ejemplo para Generar un Log que u2spewfoo pueda Leer

Para que Snort genere un archivo **unified2** que u2spewfoo pueda leer, debes usar la opción de salida de log **unified2** en el archivo de configuración snort.lua y luego generar una alerta.