

curso “Experto en Ciberseguridad de Redes y Sistemas”

TEMAS

1. Fingerprinting
2. Footprinting
3. IDSs - Snort
4. Nessus
5. Firewalls
6. SGSI
7. Antiphishing
8. MITRE
9. Red Team y Blue Team
10. Principales procesos de Seguridad



IDSs – Snort (IDS: Intrusion Detection System)

3.1 Snort - Presentación



Todo el desarrollo de este tema, estará basado en “**Snort**”, pues se trata de una herramienta Open Source, que ha sido pionera y sigue siendo el precursor y motor de un gran número de los IDSs comerciales de la actualidad.

Snort es un sistema de detección de intrusos (IDS) que sigue siendo ampliamente utilizado para la monitorización y protección de redes. Desarrollado inicialmente por **Martin Roesch**, Snort analiza el tráfico en tiempo real y detecta actividades sospechosas mediante el uso de reglas definidas que identifican patrones de ataque conocidos.



Este IDS puede funcionar en tres modos principales: como sniffer de paquetes, como registrador de tráfico y como sistema de detección de intrusos propiamente dicho. Su capacidad para inspeccionar paquetes en profundidad (Deep Packet Inspection) permite identificar amenazas como intentos de

intrusión, escaneos de red, ataques de denegación de servicio (**DoS**) y otros comportamientos maliciosos.

Una de las principales ventajas de Snort es su flexibilidad, ya que, como iremos viendo a lo largo de este capítulo, permite a los administradores personalizar reglas según las necesidades específicas de su red. Además, cuenta con una amplia comunidad que mantiene y actualiza constantemente las firmas de detección.

En resumen, Snort es una herramienta potente, versátil y accesible que ayuda a mejorar la seguridad de redes mediante la detección temprana de amenazas, siendo especialmente útil tanto en entornos educativos como empresariales.

Para iniciar este capítulo, lo primero que te invitamos a ver es el libro **“Seguridad por Niveles”** (que puedes descargar gratuitamente desde: www.darFe.es). En el ANEXO 4 (Metodología Nessus – Snort) puedes comenzar a analizar los primeros conceptos y experiencias con este tipo de dispositivos.



También tienes a tu disposición el Artículo: **“Metodología Nessus- Snort”**, que puedes descargar del siguiente enlace:

<https://darfe.es/download/metodologianessus-snort/?wpdmdl=38042&refresh=6a685ce64843d1785224422>

También tienes a tu disposición el curso: **“curso de Snort-Nessus”**, que puedes descargar del siguiente enlace:

<https://darfe.es/download/curso-de-snort-y-nessus/?wpdmdl=38724&refresh=6a686156c34861785225558>

En la actualidad, tal cual podemos ver en el **video 101** de nuestro ciclo “Aprendiendo Ciberseguridad paso a paso”, Snort ha sido comprado por la empresa **Cisco System**, pero sigue manteniendo su código abierta y libre uso. Cisco, ofrece todo un muy buen soporte comercial y herramientas que optimizan su empleo, pero la versión libre y gratuita, veremos que es más que suficiente para implantarla en cualquier tipo de organización... como siempre, si sabemos controlarla, personalizarla y mantenerla adecuadamente, y por esta razón es que este capítulo se centra en que puedas adquirir esta capacidad.

Para comenzar a comprender Snort y familiarizarnos con su manejo, os invitamos a ver el siguiente video **(Obligatorio)**.

 **IDS - Snort - (Parte 1) - Charla 101 - Aprendiendo Ciberseguridad paso a paso**

<https://youtu.be/PHwaH6z0MJ0>



3.2 Snort – EasyIDS

En el siguiente video, instalaremos le herramienta **“EasyIDS”** ...ya sabemos... es viejita... pero aún así a efectos didácticos y para que podamos dar estos primeros pasos con Snort, veréis que nos será de mucha utilidad.

Se trata de una herramienta diseñada para simplificar la implementación y gestión de sistemas de detección de intrusos (IDS), especialmente pensada para usuarios que buscan una solución más accesible que configuraciones manuales complejas como las de Snort.

Es una interfaz, o entorno, que automatiza gran parte del proceso de instalación, configuración y mantenimiento de un IDS, integrando normalmente motores de detección como Snort bajo una capa más amigable. Su objetivo principal es facilitar la monitorización del tráfico de red y la detección de amenazas sin necesidad de conocimientos avanzados en ciberseguridad.

Características principales:

- Instalación simplificada: permite desplegar un IDS de forma rápida sin configuraciones complicadas.
- Interfaz gráfica: ofrece paneles visuales para consultar alertas, eventos y estado del sistema.
- Gestión de reglas: facilita la activación, desactivación o modificación de reglas de detección.
- Monitorización en tiempo real: muestra el tráfico y las posibles amenazas conforme ocurren.
- Enfoque educativo y práctico: muy utilizada en entornos de aprendizaje o laboratorios.

¿Para qué nos será de utilidad?

EasyIDS es especialmente útil para:

- Estudiantes y principiantes en ciberseguridad.
- Laboratorios de prácticas.
- Pequeñas redes donde no se requiere una configuración altamente personalizada.

En resumen:

EasyIDS actúa como una capa de simplificación sobre herramientas IDS más potentes, permitiendo a los usuarios centrarse en el análisis de seguridad sin enfrentarse a la complejidad técnica de la configuración manual.

Pasemos a estudiarla directamente sobre el video 102 **(Obligatorio)**.

 **IDS - Snort - (Parte 2) - Charla 102** - Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/1r-QQjYJA2Y>



3.3 Snort – Configuración inicial

En este punto, comenzaremos a desarrollar los cuatro componentes básicos de Snort que son:

- Decodificador de paquetes (Packet Decoder)
Se encarga de capturar y analizar los paquetes de red que llegan. Extrae información clave como direcciones IP, puertos y protocolos.
- Preprocesadores (Preprocessors)
Preparan los datos antes del análisis principal. Detectan anomalías, normalizan el tráfico y pueden identificar comportamientos sospechosos iniciales.

- **Motor de detección (Detection Engine)**
Es el núcleo de Snort. Compara el tráfico con un conjunto de reglas para identificar posibles ataques o actividades maliciosas.
- **Sistema de salida (Output Plugins)**
Gestiona cómo se muestran o almacenan los resultados. Puede generar alertas, guardar logs o enviar información a otras herramientas.

En conjunto, estos componentes permiten a Snort analizar, detectar y reportar amenazas en la red de forma eficiente.

Para analizarlos de forma práctica pasemos a ver el video 103 **(Obligatorio)**.

 **IDS - Snort - (Parte 3) - Charla 103 - Aprendiendo**
Ciberseguridad paso a paso

<https://youtu.be/5yYEDafYiSM>



3.4 Snort – el fichero “snort.conf”

El fichero **snort.conf** es el archivo principal de configuración de Snort. En él se definen todos los parámetros necesarios para que el sistema funcione correctamente, incluyendo qué tráfico analizar, qué reglas aplicar y cómo gestionar las alertas.

Este archivo actúa como el “cerebro” de la configuración, ya que permite adaptar Snort a las necesidades específicas de cada red.

Elementos principales de snort.conf:

Variables de red (Network Variables)

Definen aspectos como la red interna (HOME_NET) y externa (EXTERNAL_NET), lo que permite a Snort identificar el origen y destino del tráfico.

Configuración de preprocesadores

Incluye módulos que preparan el tráfico antes de ser analizado, como la normalización de paquetes o la detección de anomalías.

Inclusión de reglas (Rule Sets)

Se especifican las rutas a los archivos de reglas que Snort utilizará para detectar amenazas. Estas reglas contienen firmas de ataques conocidos.

Configuración de salidas (Output Plugins)

Determina cómo y dónde se registran las alertas (por ejemplo, en archivos de log o bases de datos).

Opciones generales

Ajustes como el nivel de detalle de los logs, directorios de trabajo o configuraciones de rendimiento.

En resumen:

El fichero snort.conf es esencial para el funcionamiento de Snort, ya que centraliza toda su configuración y permite personalizar el sistema de detección de intrusos según el entorno y los requisitos de seguridad.

Veámoslo de forma práctica en el video 104 (**Obligatorio**).

 **IDS - Snort - (Parte 4) - Charla 104** - Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/8OoZe1P3stk>



3.5 Snort – Uso de la interfaz gráfica de EasyIDS

La interfaz gráfica de **EasyIDS** está pensada para que puedas supervisar la seguridad de una red sin necesidad de usar comandos complejos. Su uso básico se resume así:

- **Panel principal (dashboard):** al abrir EasyIDS verás un resumen del estado del sistema, con indicadores de tráfico, alertas recientes y posibles amenazas detectadas.
- **Monitorización en tiempo real:** permite observar el tráfico de red en directo, identificando conexiones sospechosas o patrones anómalos.
- **Gestión de alertas:** muestra una lista de eventos detectados (intrusiones, escaneos, etc.), donde puedes filtrarlos, analizarlos y marcarlos como revisados.
- **Configuración:** desde la interfaz puedes ajustar reglas, definir umbrales de detección o seleccionar qué tipo de tráfico quieres vigilar.
- **Registro (logs):** acceso a historiales detallados para analizar incidentes pasados y mejorar la seguridad.

En resumen, la GUI de EasyIDS facilita la vigilancia, análisis y configuración del sistema de seguridad de forma visual e intuitiva, sin necesidad de trabajar directamente con la línea de comandos.

Pasemos a verlo de forma práctica en el video 105 (**Obligatorio**).

 **IDS - Snort - (Parte 5) - Charla 105** - Aprendiendo Ciberseguridad paso a paso

https://youtu.be/irD_rTJjGsc



3.6 Snort – Los preprocesadores

En Snort, los preprocesadores son módulos fundamentales que actúan antes del motor de detección. Su función es preparar, normalizar y analizar el tráfico de red para que las reglas de detección puedan aplicarse de forma más precisa y eficaz.

¿Qué hacen los preprocesadores?

Los preprocesadores se encargan de:

- Normalizar el tráfico: eliminan ambigüedades en los paquetes (por ejemplo, distintas formas de codificar una misma petición).

- Reensamblar datos: reconstruyen flujos de red (como sesiones TCP) para analizar el contenido completo y no solo paquetes individuales.
- Detectar anomalías: identifican comportamientos sospechosos que no siempre encajan en reglas simples.
- Preparar los datos: facilitan que el motor de reglas trabaje con información más clara y coherente.

Tipos principales de preprocesadores en Snort

1. Reensamblado de tráfico

frag3: reconstruye fragmentos IP para evitar evasiones mediante fragmentación.

stream5: reensambla sesiones TCP, permitiendo analizar conversaciones completas.

Son esenciales porque muchos ataques se esconden fragmentando paquetes.

2. Normalización de protocolos

http_inspect: analiza y normaliza tráfico HTTP (URLs, cabeceras, codificación).

ftp_telnet: trata comandos FTP y Telnet, detectando anomalías.

Evitan técnicas de evasión como codificación maliciosa o formatos extraños.

3. Detección de anomalías

sfPortscan: detecta escaneos de puertos (actividad típica de reconocimiento).

arpspoof: identifica ataques de suplantación ARP.

Funcionan más por comportamiento que por firmas concretas.

4. Preprocesadores específicos

dns: analiza tráfico DNS en busca de irregularidades.

ssl: examina conexiones cifradas (limitado, pero útil para metadatos).

¿Por qué son importantes?

Sin preprocesadores:

El motor de detección vería paquetes aislados → menor precisión.

Sería más fácil evadir el sistema mediante técnicas de fragmentación o codificación.

Muchas amenazas complejas pasarían desapercibidas.

Con preprocesadores:

Se obtiene una visión completa del tráfico.

Se reducen falsos positivos y falsos negativos.

Se mejora la capacidad de detectar ataques sofisticados.

Resumen

Los preprocesadores de Snort actúan como una “fase de limpieza y análisis previo” del tráfico de red. Transforman datos crudos en información estructurada y fiable, permitiendo que el sistema de detección funcione de forma mucho más eficaz.

Vamos a verlos con más detalle en el video 106 **(Obligatorio)**.

 **IDS - Snort - (Parte 6) - Charla 106 - Aprendiendo Ciberseguridad paso a paso**

<https://youtu.be/ijJ4Qhp5a7Y>



3.7 Snort – Las salidas

En **Snort**, las *salidas* (output plugins) son los componentes encargados de **registrar y mostrar los resultados** generados por el motor de detección. Es decir, una vez que Snort detecta una actividad sospechosa o un ataque, las salidas determinan **cómo, dónde y en qué formato** se guarda o presenta esa información.

¿Para qué sirven las salidas?

Las salidas permiten:

- **Registrar alertas** generadas por las reglas.
- **Guardar paquetes capturados** para su análisis posterior.
- **Integrar Snort con otras herramientas** (bases de datos, SIEM, etc.).
- **Visualizar resultados** en distintos formatos (texto, binario, red, etc.).

Tipos principales de salidas en Snort

1. Salida en consola

- Muestra alertas directamente en pantalla.
- Útil para pruebas o monitorización en tiempo real.
- Ejemplo: modo -A console.

Ventaja: inmediata.

Desventaja: no persistente.

2. Archivos de registro (logs)

Guarda alertas y paquetes en archivos.

Formatos comunes:

- **texto plano**
- **pcap** (para análisis con Wireshark)

Muy útil para auditorías y análisis forense.

3. Salida en base de datos

Permite almacenar eventos en bases de datos como MySQL o PostgreSQL.

Facilita consultas, informes y correlación de eventos.

Se suele usar junto con herramientas de visualización.

4. Formato unificado (unified2)

- Formato binario optimizado para rendimiento.
- Muy utilizado en entornos profesionales.
- Compatible con herramientas como **Barnyard2** para procesar los datos.

Ventaja: eficiente y escalable.

5. Envío remoto

- Puede enviar alertas a otros sistemas a través de red.
- Ejemplo: integración con SIEM o sistemas de gestión de seguridad.

Permite centralizar la monitorización.

¿Por qué son importantes?

Las salidas son clave porque:

- Transforman la detección en **información útil**.
- Permiten **analizar incidentes** posteriormente.
- Facilitan la **integración con infraestructuras de seguridad**.
- Hacen posible la **automatización y respuesta ante incidentes**.

Resumen

Las salidas de Snort son el mecanismo mediante el cual el sistema comunica sus hallazgos. Sin ellas, las detecciones no tendrían utilidad práctica, ya que no se podrían consultar, analizar ni integrar en otros sistemas de seguridad.

Vamos a verlas con más detalle en el video 107 **(Obligatorio)**.

 **IDS - Snort - (Parte 7) - Charla 107 - Aprendiendo Ciberseguridad paso a paso**

<https://youtu.be/kx1zliziYNc>



3.8 Snort – Las reglas

Las **reglas de Snort** son el núcleo del sistema de detección: definen **qué tráfico es sospechoso o malicioso** y qué acción debe tomar Snort cuando lo detecta. Funcionan como patrones o firmas que se comparan con el tráfico de red.

¿Qué es una regla de Snort?

Una regla es una instrucción que indica:

- **Qué tipo de tráfico analizar**
- **Qué condiciones deben cumplirse**
- **Qué hacer si se detecta una coincidencia** (alertar, registrar, bloquear, etc.)

Estructura básica de una regla

Una regla típica tiene dos partes principales:

acción protocolo origen puerto -> destino puerto (opciones)

Ejemplo sencillo:

alert tcp any any -> 192.168.1.10 80 (msg:"Acceso HTTP sospechoso"; sid:1000001;)

Componentes de una regla

1. Acción

Indica qué hace Snort si se cumple la regla:

alert: genera una alerta

log: registra el paquete

pass: ignora el tráfico

drop: bloquea el paquete (en modo inline)

2. Protocolo

Define el protocolo de red:

- tcp, udp, icmp, ip

3. Dirección y puertos

Especifica origen y destino:

- any: cualquier IP o puerto
- IP concreta o rango
- Puertos específicos (ej. 80, 21, etc.)

4. Dirección de flujo

- ->: de origen a destino
- <->: bidireccional

5. Opciones (entre paréntesis)

Aquí está la parte más potente. Algunas opciones comunes:

msg: mensaje de alerta

content: busca un patrón en los datos

sid: identificador único de la regla

rev: versión de la regla

flow: estado de la conexión (ej. establecida)

flags: flags TCP

threshold: control de frecuencia de alertas

Ejemplo más completo:

```
alert tcp any any -> any 80 (msg:"Posible ataque SQL Injection";  
content:"SELECT"; nocase; sid:1000002; rev:1;)
```

Tipos de reglas

- **Reglas de detección**: buscan patrones de ataques conocidos.
- **Reglas de anomalía**: detectan comportamientos inusuales.
- **Reglas personalizadas**: creadas por el administrador según necesidades específicas.

¿Por qué son importantes?

- Permiten detectar ataques como **escaneos, exploits o malware**.
- Son altamente **configurables y adaptables**.
- Se pueden actualizar constantemente para nuevas amenazas.

Resumen

Las reglas de Snort son el mecanismo que define qué es una amenaza. Combinan condiciones sobre el tráfico con acciones específicas, permitiendo detectar y responder a incidentes de seguridad de forma flexible y precisa.

Vamos a verlas con más detalle en el video 108 **(Obligatorio)**.

 **IDS - Snort - (Parte 8) - Charla 108** - Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/VyzjcMYt-pc>



3.9 Snort – Las local.rules

El archivo local.rules de Snort es el lugar donde se definen las reglas personalizadas creadas por el administrador. Sirve para adaptar el sistema de detección a las necesidades concretas de una red, sin modificar directamente las reglas oficiales.

¿Qué es local.rules?

Es un fichero de texto incluido en la configuración de Snort (normalmente desde snort.conf) que contiene reglas propias. Por defecto suele estar vacío o con ejemplos básicos.

Su objetivo principal es:

- Añadir reglas específicas del entorno.
- Probar nuevas firmas.
- Personalizar la detección sin interferir con reglas estándar.

¿Cómo se utiliza?

- a) **Se edita el archivo** local.rules.

- b) **Se añaden reglas de Snort** (con la misma sintaxis estándar).
- c) Snort carga este archivo al iniciar si está incluido en snort.conf.

Ejemplo de inclusión:

include \$RULE_PATH/local.rules

Ejemplo básico de regla en local.rules

alert icmp any any -> any any (msg:"Ping detectado"; sid:1000001; rev:1;)

Esta regla genera una alerta cada vez que detecta tráfico ICMP (ping).

Buenas prácticas

- **Usar identificadores únicos (sid):**
 - Se recomienda usar valores altos (por ejemplo, a partir de 1.000.000) para evitar conflictos con reglas oficiales.
- **Documentar las reglas:**
 - Añadir mensajes claros (msg) para entender fácilmente la alerta.
- **Probar antes de desplegar:**
 - Evitar falsos positivos que saturen el sistema.
- **Mantenerlo separado:**
 - No modificar reglas oficiales; usar siempre local.rules para cambios propios.

¿Por qué es importante?

- Permite adaptar Snort a **amenazas específicas de tu entorno**.
- Facilita la **personalización sin perder compatibilidad** con actualizaciones.
- Es clave para entornos donde hay **políticas o comportamientos particulares**.

Resumen

El archivo local.rules es el espacio dedicado a las reglas personalizadas en Snort. Gracias a él, puedes ampliar y ajustar la capacidad de detección del sistema de forma segura, flexible y organizada.

Vamos a verlas con más detalle en el video 109 **(Obligatorio)**.

 **IDS - Snort - (Parte 9) - Charla 109** - Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/1eYh6JfstKw>

