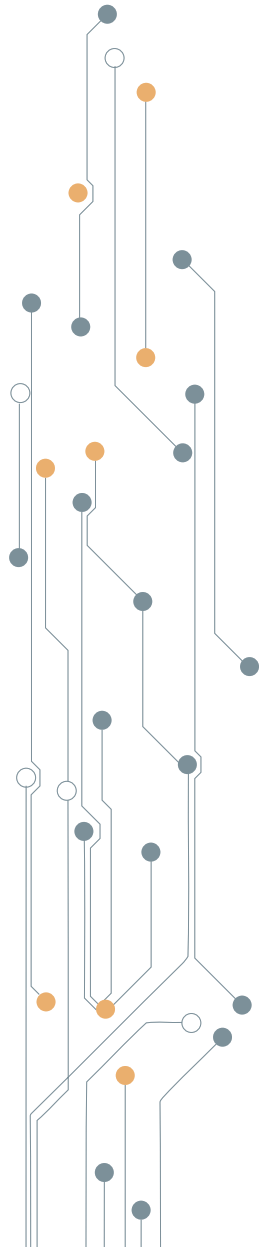
Implementación de prevención de intrusiones

Telefónica EDUCACIÓN DIGITAL

Índice



1. Implementación de prevención de intrusiones

Según la Wikipedia "Un Sistema de Prevención de Intrusos o Intrusion Prevention System ("IPS" en sus siglas en inglés), es un dispositivo de seguridad de red que monitoriza el tráfico de red y/o las actividades de un sistema, en busca de actividad maliciosa. Entre sus principales funciones, se encuentran no sólo la de identificar la actividad maliciosa, sino la de intentar detener esta actividad. Siendo esta última una característica que distingue a este tipo de dispositivos de los llamados Sistemas de Detección de Intrusos o Intrusion Detection Systems ("IDS" en sus siglas en inglés).

Entre otras funciones (como en el caso del IDS) se tiene que puede alertar al administrador ante la detección de intrusiones o actividad maliciosa, mientras que es exclusivo de un Sistema de Prevención de Intrusos (IPS) establecer políticas de seguridad para proteger al equipo o a la red de un ataque.

De ahí que se diga que un IPS protege a una red o equipo de manera proactiva mientras que un IDS lo hace de manera reactiva.

Otras funciones importantes de estos dispositivos de red, son las de grabar información histórica de esta actividad y generar reportes."

Imagen 87 Logo Snort

SNORT es una completa herramienta de seguridad basada en código abierto para la creación de sistemas de detección de intrusos en entornos de red.

Snort puede utilizarse tanto como sniffer de paquetes en una red pequeña como un sistema completo de detección de intrusos en tiempo real, esto debido a su capacidad de captura y registro de paquetes en redes TCP/IP.

A través de un mecanismo adicional de alertas y generación de ficheros de registro, Snort ofrece una buena cantidad de posibilidades para la recepción de alertas en tiempo real acerca de los ataques y las intrusiones detectadas.

Snort se comporta como “una auténtica aspiradora de datagramas IP”. Desde actuar como un simple monitor de red pasivo que se encarga de detectar el tráfico maligno que circula por la red, hasta la posibilidad de enviar a servidores de ficheros de registro o servidores de base de datos todo el tráfico capturado.

Snort está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

Snort cuenta un gran repertorio de accesorios que permiten reportar sus alertas y notificaciones en diferentes gestores de base de datos (como MySQL y Postgrest) y un gran número de preprocesadores de tráfico que permiten poder analizar llamadas RPC y escaneo de puertos antes de que ´estos sean contrastados con el conjunto de reglas asociado en busca de alertas.

La arquitectura central de Snort se basa en los siguientes cuatro componentes:

- Decodificador de paquetes o Sniffer
- Preprocesador
- Motor de detección
- Sistema de Alertas e Informes

Snort permitirá la captura y el preprocesador del tráfico de la red a través de los dos primeros componentes (decodificador de paquetes y preprocesador), realizando posteriormente un chequeo contra ellos mediante el motor de detección (según el conjunto de reglas activadas) y generando, por parte del ´último de los componentes, las alertas y los informes necesarios.

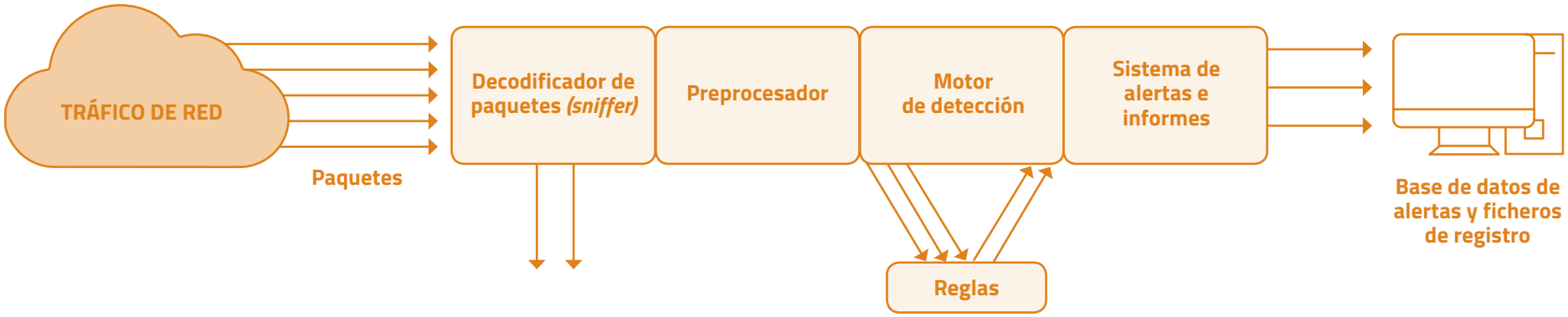


Imagen 88 Snort - Esquema

Esquema del funcionamiento del decodificador de paquetes de Snort.

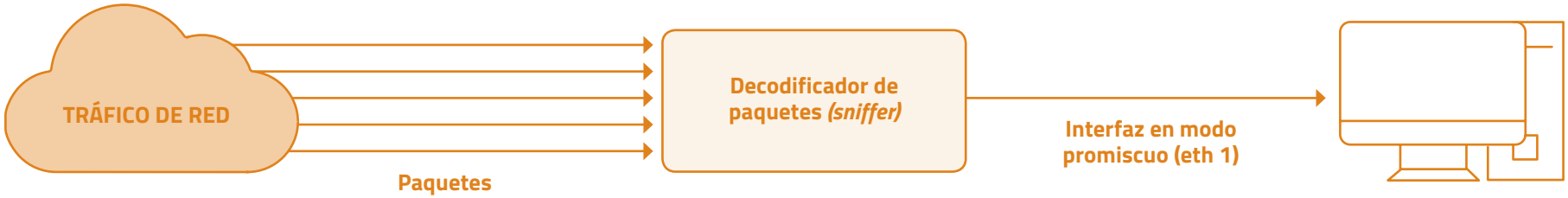


Imagen 89 Snort - Esquema decodificador

El preprocesador obtiene paquetes sin tratar (*raw paquets*) y los verificará mediante un conjunto de *plug-ins*. Estos *plug-ins* verificarán los paquetes en busca de ciertos comportamientos en estos que le permita determinar su tipo. Una vez determinado el comportamiento del paquete, ´este será enviado hacia el motor de detección.

Esta característica de preprocesamiento es realmente importante para una herramienta de detección, ya que es posible la utilización de terceras aplicaciones (en forma de *plug-ins*) que pueden ser activadas y desactivadas según las necesidades del nivel de preprocesado. Por ejemplo, si a un administrador de red no le preocupa el tráfico RPC que entra y sale de su red (y no necesita, por tanto, analizarlo) por cualquier motivo, no tendrá más que desactivar el *plug-in* de RPC y seguir utilizando el resto.

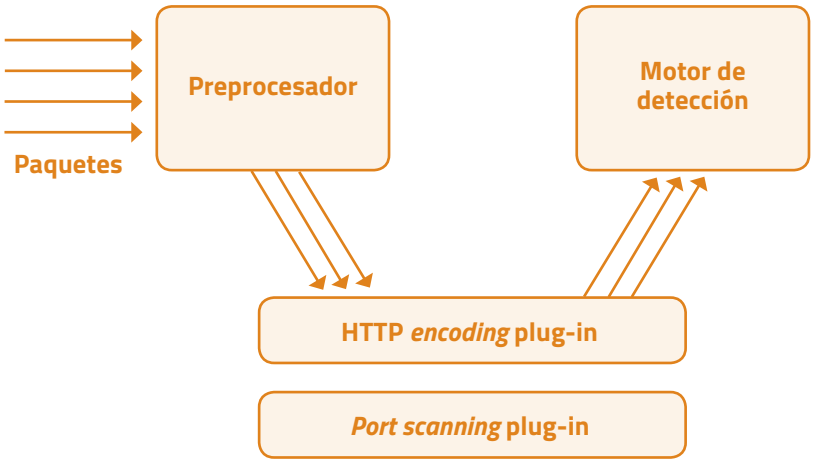


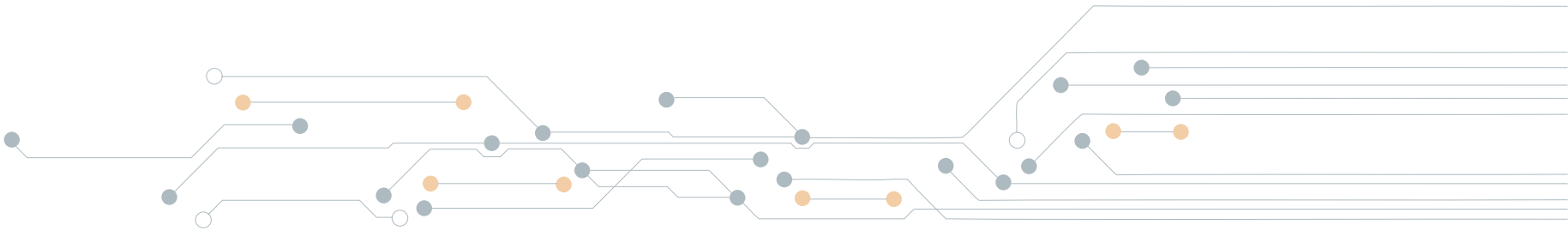
Imagen 90 Snort - Esquema preprocesador

El motor de detección es el corazón de Snort desde el punto de vista de sistema de detección de intrusos. A partir de la información proporcionada por el preprocesador y sus *plug-ins* asociados, el motor de detección contrastará estos datos con su base de reglas. Si alguna de las reglas coincide con la información obtenida, el motor de detección se encargará de avisar al sistema de alertas indicando la regla que ha saltado.

Snort posee una sintaxis propia para la creación de las reglas. Esta sintaxis incluye el tipo de protocolo, el contenido, la longitud, la cabecera, etc., que permiten especificar hasta el más mínimo detalle de la condición que ha de darse para que un paquete cumpla dicha regla.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP EXPLOIT STAT *
dos attempt"; flow:to_server,established; content:"STAT "; nocase;
content:"*"; reference:bugtraq,4482; classtype:attempted-dos;
sid:1777; rev:1;)
```

Imagen 91 Snort - Regla



El comportamiento general del motor de detección se detalla en el siguiente esquema:

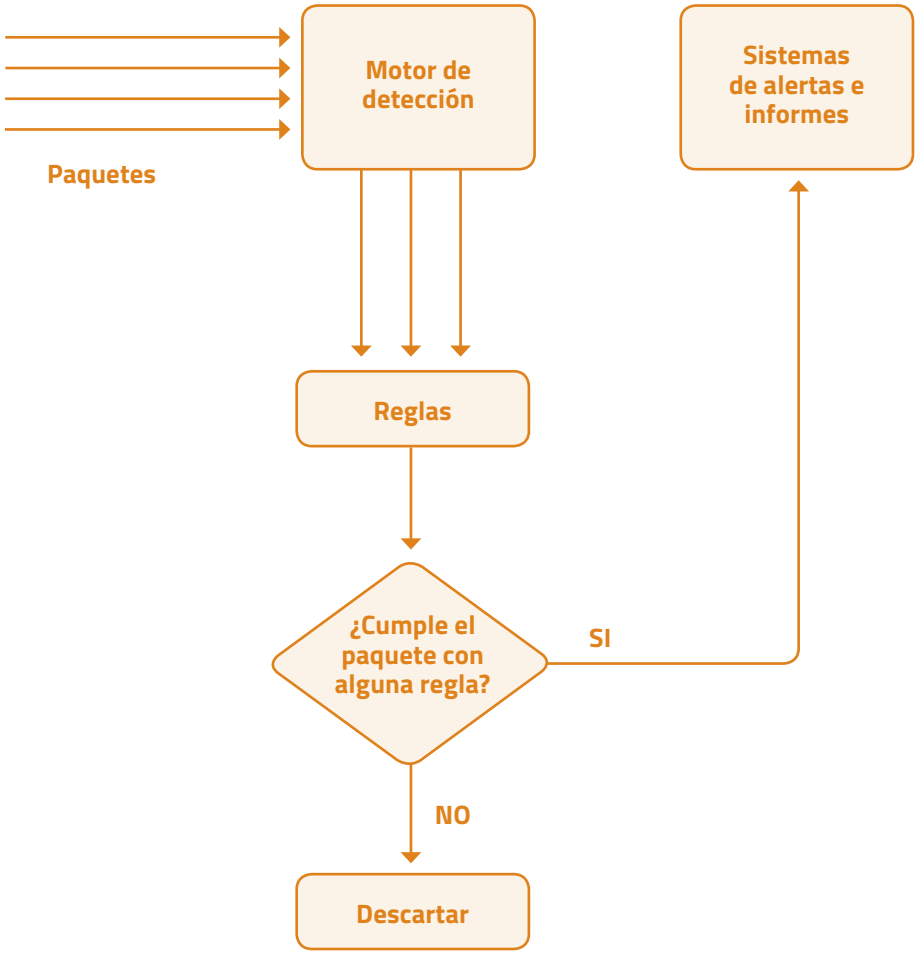


Imagen 92 Snort - Comportamiento general motor

El proceso de instalación lo tenemos detallado en la web oficial **https://www.snort.org/** ya que depende de la versión se realizará de una manera diferente.

Podemos comenzar la monitorización según la configuración establecida previamente.

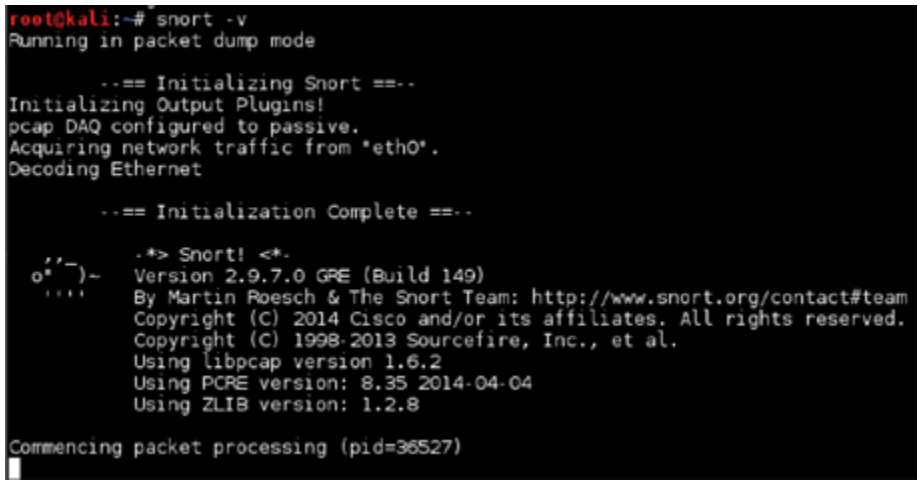


Imagen 93 Snort - Monitorización

Durante la captura del tráfico aparecen detallado los paquetes que se envían desde el cliente y las respuestas desde el equipo del servidor.

```
12/10-23:31:27.035464 216.58.211.206:80 -> 192.168.10.176:34256
TCP TTL:128 TOS:0x0 ID:34461 IpLen:20 DgmLen:40
***AP**F Seq: 0x138E1E02  Ack: 0xAF095C12  Win: 0xFAEF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/10-23:31:27.035496 192.168.10.176:34256 -> 216.58.211.206:80
TCP TTL:64 TOS:0x0 ID:42041 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xAF095C12  Ack: 0x138E1E03  Win: 0x7210  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/10-23:31:27.047209 216.58.211.206:80 -> 192.168.10.176:34254
TCP TTL:128 TOS:0x0 ID:34462 IpLen:20 DgmLen:40
***AP**F Seq: 0x9CA7991  Ack: 0x5B983301  Win: 0xFAEF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/10-23:31:27.047241 192.168.10.176:34254 -> 216.58.211.206:80
TCP TTL:64 TOS:0x0 ID:42044 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x5B983301  Ack: 0x9CA7992  Win: 0x7210  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Imagen 94 Snort - Captura de tráfico

A la finalización se muestra un resumen de la actividad realizada, como número total de paquetes recibidos, analizados, filtrados,... así como por protocolos.

```
===============================================================================
Run time for packet processing was 59.878637 seconds
Snort processed 1002 packets.
Snort ran for 0 days 0 hours 0 minutes 59 seconds
   Pkts/sec:           16
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       782336
  Bytes in mapped regions (hblkhd):      12906496
  Total allocated space (uordblks):      671888
  Total free space (fordblks):           110448
  Topmost releasable block (keepcost):   103200
===============================================================================
Packet I/O Totals:
   Received:         1002
   Analyzed:         1002 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         1002 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         1002 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:           66 (  6.587%)
        TCP:          785 ( 78.343%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
```

Imagen 95 Snort - Resumen detallado

Telefónica EDUCACIÓN DIGITAL