Snort Overview

Transcribed on August 1, 2025 at 4:27 PM by Minutes AI

Speaker 1 (00:00)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la monitorización, detección y prevención de intrusiones utilizando Snort.

Snort es básicamente un IDS, un NIDS y un IPS todos juntos de código abierto y libre que permite registrar todo tipo de alertas y ataques.

Tiene un sistema de gestión de reglas muy sofisticado que permite crear todo tipo de filtros para por ejemplo ataques de delegación de servicios distribuidos, nmap, backdoor, entre otros.

Pero además de la funcionalidad de NIDS también puede funcionar en modo sniffer o packet logger y esto permite crear logs a nivel de paquetes.

La base de datos que registra los tipos de ataques así como las firmas se va actualizando a través de Internet desde de una forma constante, lo que ofrece una gran fiabilidad a la resiliencia ante ataques recientes.

En la diapositiva podéis ver un pequeño esquema que indica el proceso de detección y captura del paquete hasta finalmente su registro en los logs.

Antes de comenzar con Snort práctico quería mostraros el aspecto que tiene una regla, aunque después lo haremos a un nivel ya de detalle.

Utilizando Snort en una terminal de Linux, quería que vierais un poco cuáles son los diferentes elementos que vamos a encont en las alertas.

Bien, pasamos a la parte práctica, vamos a ver cómo funciona Snort con algunos ejemplos sencillos y por supuesto el primer paso será instalarlo, pues para hacer la instalación de Snort como siempre hacemos un sudo apt update Bien, pasamos a la parte práctica, vamos a ver por encima cómo funciona Snort con algunos comandos básicos y Y claro, la primera parte será instalarlo, para ello hacemos un sudo apt update Primero como siempre, después lo que haremos será la instalación sudo apt install Y en este caso es snort y a todo que sí Y en este punto ya aparece el asistente.

Bien, lo que aparece aquí es el nombre de la interfaz de red, en mi caso es eth por defecto y por norma la que te aparece ahí será la correcta, pero siempre es bueno tener claro cuáles son las tarjetas que tenemos en el sistema Linux, porque si hay varias podemos elegir cuál de ellas será la que va a utilizar el sistema de Snort.

El siguiente paso es determinar el CIDR, o sea la subred en la que estamos trabajando, en nuestro caso le pondremos la 10.

211 55 0 24 porque es en la que estamos trabajando entre las dos máquinas que hacen todas las pruebas y ya finalmente pues acabará la instalación, podemos comprobar que todo está correcto haciendo una snort version, nos dirá en qué versión estamos.

Bien, ahora vamos a ver cómo verificar que todo está correcto.

Hay un comando, si ponemos sudo, si ponemos sudo snort a console ahora os contaré que es cada cosa.

Snorkov quedaros con este fichero porque es fundamental, lo tocaremos después para el tema de las reglas.

Guión i interfaz que será dth y t.

Bien, ¿Que estamos haciendo hoy?

Pues fijaros, este comando lo que hace es, con el guión a console quiere decir que muestra las alertas y mensajes en la salida de la consola, o sea que lo vamos a ver después.

Tenemos el guión q, que lo que hace es que ejecuta snort en modo.

Después tenemos el guión q, que lo que hace es ejecutar snort en modo silencioso, minimizando la salida de mensajes innecesarios durante la prueba.

El guión C y esa ruta, lo que dice el guión C y esa rutA específica el archivo de configuración a utilizar, que en este caso es el snor conf, que es el que es más genérico, el que viene por defecto con la instalación.

La guión i eth lo que hace el guión i eth designa la interfaz de red que va a monitorizar.

Y finalmente t lo que hace es que realiza una prueba de configuración sin poner en marcha el sistema de detección, verificando errores en la configuración de las reglas, por ejemplo.

Bien, pues si le damos, esperemos un segundo y vemos que está todo OK porque no hay ningún tipo de salida de error.

Bien, ese fichero que antes hemos nombrado, este de aquí, es fundamental porque aquí es donde haremos los diferentes cambios en la tarjeta de red o en cómo se escanea todo.

Este fichero es el de configuración y es fundamental, de hecho lo vamos a editar para comprobar que todo está correcto y para ello utilizaremos con etc.

Bien, aquí hay multitud de parámetros, pero aquí nos interesa ahora mismo uno en concreto y es la red, este de aquí, este hiperbar de aquí.

Aquí en vez de poner any deberíamos de poner la máquina host en la que estamos, la IP, porque así se centrará en este equipo, con lo cual pondremos 200.

655 en.

En este caso era 5.

Almacenamos, si ponemos any lo que hará será escanear toda la red, pero yo en este caso me he centrado en un servidor, vamos a hacer una especie de HID, acordáis que era el host, vamos a escanear este host, guardo esta opción en este fichero.

Bien, es importante modificar dos permisos de dos carpetas, ahora os cuento por qué tiene, pero lo primero es hacerlo y es sudo chmod y ponemos r y hacemos otro sudo chmod r y esta vez lo hacemos contra los logs.

Esto básicamente es asegurarnos que snor tiene los permisos adecuados para acceder, leer y escribir en los directorios de configuración, que era el primero y en el de los logs.

Esto es fundamental porque sin esto no puede acceder y no puede modificar reglas ni añadir lograr.

Bien, pues ahora vamos a ir a la clave de todo esto, que son las reglas, esto es lo principal, las reglas son lo que definen qué vamos a monitorizar.

Aquí tenéis un pequeño resumen que ya vimos en la diapositiva de cómo son las reglas, pero ahora vamos a hacer alguna para que veáis cómo se implementa y ya os explico un poco qué es cada uno de los elementos.

Y bien, pues uno de los protocolos más monitorizados es ICMP, que ya conocemos porque es el que gestiona el comando ping por ejemplo, y es fundamental durante la fase de descubrimiento en un pentesting.

Pues bien, snor ya tiene un listado o un fichero con reglas que son específicamente orientadas a ICMP, o sea, no tenemos que crear reglas desde cero, nos va a dar muchísimas opciones Snor, de hecho prácticamente nos va a dar todas.

Lo bueno de esto es que podemos personalizarlo como queramos y adaptarlo a nuestra arquitectura, pero si de aquí directamente hacemos por ejemplo un nano, vamos a editar un fichero concreto, OK, más, vamos a ver este de snort, en la carpeta rules están todas las reglas, si aquí ponemos ICMP ya veréis que aparece un fichero que es el de las reglas ICMP exclusivos, aquí lo podéis ver, es súper completo, todo está aquí especificado para lo que es la detección asociada a paquetes.

Bien, vamos a ir por ejemplo a una de ellas, este de aquí por ejemplo, esta de aquí se llama esta que hace un ICMP ping nmap vale, Ya podéis ver que esto lo que hace es detectar cuando nmap hace un pin hacia tu máquina, esta es la regla que lo controla y vamos a ver un poco los diferentes componentes que tiene ahí.

El primero que veis que pone alert es la acción de la regla, alertar.

Hay otras, podemos hacer un log, que lo que haría sería almacenar en el sistema de log, hacer un pass, que lo que haría sería directamente no hacer nada.

Después activate dynamic drop, por ejemplo, para pararla como hacen los cortafuegos, etcétera.

Tenemos varias opciones, lo normal es alertar, pero como ya hemos visto, esto también es un sistema de prevención, con lo cual también activaría con el comando por ejemplo activate algún tipo de ejecución en caso de detectar algo que queremos parar con un script o cualquier otra cosa.

Después vemos que el protocolo que indica es el ICMP, esto está claro, es el del ping, pero podemos utilizar TCP, UDP, IP, etc.

Después cuando pone EXTERNAL net, lo que está diciendo es que cualquier red externa, vamos a monitorizar cualquier red externa y con any decimos justamente eso, cualquiera.

Después vemos que es el home net, si os acordáis antes cambiamos en el conf, una IP quiere decir que vamos a monitorizar nuestra red de este servidor, sólo la IP, sólo esta máquina, que es lo que yo he puesto antes en el conflicto.

Después sería el puerto any, aquí este era el puerto, cualquier puerto, cualquier puerto, no estamos especificando un puerto concreto en ninguno de los dos.

Después vemos una opción que pone msg, el msg es simplemente el mensaje que se va a almacenar cuando se registre este log o aparezca en pantalla, pondrá ICMP PIC nmap, que nos describe que se está estableciendo una llamada de ping con nmap.

Y después ya viene toda la parte un poco más compleja y más abajo nivel de cómo se hace toda la detección de la regla, pero os lo voy a explicar.

Por ejemplo el D size, este campo especifica el tamaño del datagrama ICMP, en este caso 0 significa que el tamaño del datagrama ICMP es de 0 bytes y esto indica que la regla se va a aplicar a todos los paquetes ICMP independientemente de su tamaño.

Esto de aquí os comentaba.

Bien, Después tenemos el EType 8, el Type 8, lo que dice que este campo especifica el tipo de mensaje ICMP.

Type 8 quiere decir que la regla se aplicará a paquetes ICMP del tipo 8, que corresponden a los paquetes de solicitud de un echo, de un pin.

Bien, después vemos aquí que pone reference arachnid total hasta aquí esto lo que es también el 162 es todo este bloque.

Este campo proporciona una referencia a una base de datos de amenazas o de información relacionada con esta regla.

En este caso se referencia al ID 162 en la base de datos Arachnid, que puede contener más detalles sobre una amenaza detectada.

El siguiente campo es el ClassType.

ClassType recon lo que dice es especificar el tipo de clasificación de esta regla.

En este caso esta regla se va a clasificar como intento de reconocimiento, que tiene sentido porque es una fase de descubrimiento, con lo cual esto es un intento de reconocimiento de nuestra máquina.

Después tenemos un SID que podéis ver aquí, el SID es el identificador único de esta regla.

Signature id significa cada regla de detección en snor tiene un SID único que se utiliza para identificarla y gestionar las alertas que se genera.

Y finalmente ref lo que indica es la revisión de la regla, cada vez que se actualiza una regla se incrementa el número de esta revisión, es este de aquí que podéis ver al final.

Bien, pues eso es un poco por encima, pero claro, fijaros la cantidad de parámetros que hay, sobre todo aquí.

Aquí podemos modificar muchísimo porque esto va en función del protocolo que utilicemos, en este caso tenemos ICMP pero puede ser otro, con lo cual esto es muy vasto, hay una gran cantidad de formas de personalizarlo.

Bien, pues ahora de vuelta al servidor vamos a activar snort para que de esta forma detecte las conexiones del pin que hemos visto antes.

Bien, pues para ello hacemos sudo snort a console q, eso ya hemos visto, etc.

Y le decimos guión interfaz y aquí cuidado, aquí tienes que poner la vuestra, en mi caso es la eth.

Bien, con esto debería de quedarse ahora esperando algún tipo de evento, pero como ya está el ping debería de dar como resultado esa detección de que alguien nos está haciendo pingüino.

Activamos y ahí está, lo veis directamente como tengo la otra máquina haciéndole pin a este equipo, Fijaros, ya nos está diciendo que, ojo, he detectado un PIN que viene desde la dirección IP, que es la otra, que es la máquina número 2, y de hecho seguirá aquí porque he puesto la opción de consola.

El guión a console lo que está haciendo es que todo está saliendo por la pantalla para que lo podáis ver.

Y aquí tenemos a ver que claramente que la orientación es de la 17 a la 5, como podéis ver aquí.

Y poco más, con esa pequeña regla ya vemos que snor nos detecta un pin, que no es poco, porque ya sabéis que en la parte de descubrimiento, como hicimos en la práctica del anterior módulo, es importante porque está dentro de la fase de descubrimiento y está dando mucha información y hay muchos programas como Nmap que utilizan el protocolo ICMP para descubrir más información.

Bien, voy a pararlo, paramos a Snor también, voy a parar el pin que lleva aquí un buen rato haciendo pin a la máquina, lo paramos desde la máquina número 2 y volvemos otra vez al servidor.

Bien, en esta primera parte hemos visto lo versátil y lo fácil que es configurar Snort y dejarlo ya preparado para que detecte todo tipo de intrusiones y y posibles ataques.

Ahora en la segunda parte veremos un poco más el tema de las reglas y alguna configuración un poco más avanzada y también la gestión de los logs.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.