Manual básico de detección de escaneos con snort

Snort es una herramienta de seguridad muy utilizada en linux, con la cual podemos asegurar nuestro equipo o nuestra red. Ofrece muchas posibilidades, pero en este pequeño manual nos centraremos en las mas básicas.
Una de ellas es la detección de escanéos de puertos. Snort nos ofrece de forma muy clara las ips que han intentado escanear nuestro equipo, asi como la hora del escaneo y detalles sobre los paquetes empleados.

Una vez instalado snort ya sea desde las fuentes o desde los cds de nuestra distribución de linux hemos de configurarlo modificando el archivo snort.conf, estableciendo las variables oportunas a la configuración de nuestra red. Por ejemplo si que queremos establecer que nuestra interfaz externa la tenemos en la conexión del módem 56K, lo que tenemos que hacer es editar dicho archivo y buscar la siguiente linea:

var EXTERNAL_NET any

Y cambiarla por esto:

var EXTERNAL_NET $ppp0_ADDRESS

Aunque si la dejamos como estaba también nos detectará los escaneos, solo que de la segunda forma podemos especificar exactamente en que interfaz queremos detectar los escaneos.
En snort.conf también podemos establecer todas las variables correspondientes a nuestros servidores web, DNS o cualesquiera estuvieran presentes en nuestra red.

Una vez configurado este archivo hemos de asegurarnos de que snort va a poder escribir los logs en el sitio adecuado. Asi que nos vamos a /var/log/ y nos aseguramos de que existe un directorio llamado snort y si no lo hubiera lo crearíamos.

Solo nos queda arrancar snort indicándole donde está el archivo snort.conf y la interfaz que ha de vigilar y si se produciera algún escaneo, dentro de /var/log/snort/ nos aparecería un directorio con la ip que tenia en ese momento esa interfaz, y la ip que nos ha escaneado y dentro de él, distintos archivos con información sobre el escaneo, desde donde se produjo, hora, etc.

Un ejemplo, una vez instalado y configurado snort en mi sistema, lo arranco de la siguiente manera:

[root@localhost vlad]# snort -c /compilados/snort-2.2.0/etc/snort.conf -i ppp0

Snort se pone a vigilar. Ahora nos vamos a un escaner on-line, por ejemplo el de la Asociación de Internautas:

http://www.internautas.org/w-scanonline.php

Nos escaneamos y una vez finalizado nos vamos a /var/log/snort/ y vemos lo que se nos ha creado:

[root@localhost /]# cd /var/log/snort/
[root@localhost snort]# ls
216.121.96.120/ 62.83.204.24/ alert

Tenemos dos directorios, uno con la ip que nos ha escaneado y otro con la ip que en ese momento teníamos mediante la conexión a internet de nuestro módem analógico. Vamos a que información nos da la primera ip:

[root@localhost snort]# cd 216.121.96.120/
[root@localhost 216.121.96.120]# ls
TCP:4047-161 TCP:4108-161

Vamos a ver uno de esos archivos:

[root@localhost 216.121.96.120]# nano TCP\:4047-161

[**] SNMP request tcp [**]
09/16-17:15:53.145243 216.121.96.120:4047 -> 62.83.204.24:161
TCP TTL:51 TOS:0x0 ID:17309 IpLen:20 DgmLen:60 DF
******S* Seq: 0xF0F8991C Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 513484567 0 NOP WS: 0
=+=
+=+=+=+=+=+=+=+

Fecha, hora, ip que nos escaneo, puerto desde el que lo hizo, puerto al que nos llego a nosotros... Muy completo.

Si miramos en el directorio que lleva nuestra ip encontraremos lo siguiente:

[root@localhost 216.121.96.120]# cd ../62.83.204.24/

```
[root@localhost 62.83.204.24]# ls
TCP:1000-80  TCP:1074-80  TCP:1214-80  TCP:1900-80
TCP:1021-80  TCP:1119-80  TCP:1889-80  TCP:1973-80
```

Vemos el último archivo:

```
[**] BAD-TRAFFIC loopback traffic [**]
09/16-17:17:00.709208 127.0.0.1:80 -> 62.83.204.24:1973
TCP TTL:124 TOS:0x0 ID:57676 IpLen:20 DgmLen:40
***A*R** Seq: 0x0  Ack: 0x1DED0001  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+=+=+=+
```

aquí nos dice que el escaneo se realizó desde 127.0.0.1:80, eso quiere decir que se trataba de un escaneo on-line.