

Learning IT Security. Seguridad Informática.

Aprendiendo Seguridad Informática.

Compartiendo conocimientos

Instalación IDS Snort para Windows

Publicado el 18 febrero, 2014 por Agustí Pons

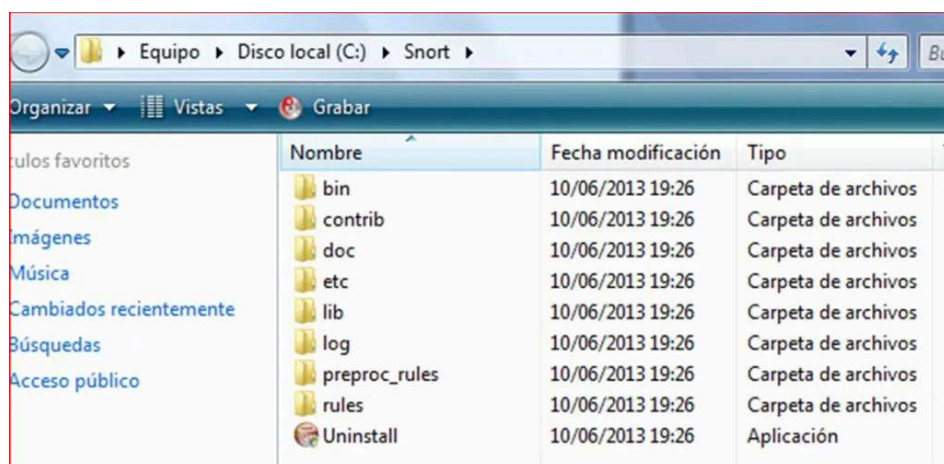
Para instalar snort en un sistema windows necesitamos seguir los siguientes pasos:

- Descargamos una copia de Winpcap.exe de www.winpcap.org.

Después de instalar Win-Pcap, reiniciar el sistema.

- Descargar la última versión de Snort para Windows de la página: www.snort.org e instalar
- Durante la instalación real, Snort crea una estructura de directorio en **C: \ Snort** que separece a esto:

- **C: \snort \ bin** directorio donde se encuentra el ejecutable de la herramienta
- **C: \ snort \ contrib**
- **C: \snort \ doc** documentación de la herramienta
- **C: \snort \ etc** directorio principal para los archivos de configuración
- **C: \snort \ log**
- **C: \snort\ rules** juegos de reglas



Nombre	Fecha modificación	Tipo
bin	10/06/2013 19:26	Carpeta de archivos
contrib	10/06/2013 19:26	Carpeta de archivos
doc	10/06/2013 19:26	Carpeta de archivos
etc	10/06/2013 19:26	Carpeta de archivos
lib	10/06/2013 19:26	Carpeta de archivos
log	10/06/2013 19:26	Carpeta de archivos
preproc_rules	10/06/2013 19:26	Carpeta de archivos
rules	10/06/2013 19:26	Carpeta de archivos
Uninstall	10/06/2013 19:26	Aplicación

Los ficheros más importantes son:

- **etc/snort.conf**: archivo de configuración principal.
- **etc/classification.config**: información sobre la priorización de las reglas, incluyendo un nombre clasificatorio y una pequeña descripción.



Descanso Transformador

El colchón Blick de Memory Foam mejora tu descanso y bienestar. ¡Descúbrelo!

[Compra Ahora](#)
[Ajustes de privacidad](#)

- **etc/gen-msg.map:** incluye correspondencia entre un identificador de elemento generador de un evento y su descripción.
- **etc/reference.config:** define las URL asociadas a las referencias de más información que suelen indicarse junto a las reglas de detección.
- **etc/sid-msg.map:** hace corresponder el identificador de una alerta (Snort ID, SID) con su mensaje descriptivo.
- **etc/threshold.conf:** configuración de umbrales límite que permiten la reducción de alarmas por repetición de eventos.
- **etc/unicode.map:** correspondencias de formato entre diferentes tipos de código.

Nombre	Fecha modificación	Tipo
classification.config	15/04/2013 21:57	Archivo CONFIG
gen-msg.map	21/09/2012 2:09	Archivo MAP
reference.config	15/04/2013 21:57	Archivo CONFIG
snort.conf	15/04/2013 21:59	Archivo CONF
threshold.conf	15/04/2013 21:57	Archivo CONF
unicode.map	14/07/2011 0:43	Archivo MAP

Una vez que está instalado Snort, debemos continuar con la configuración

- Lo primero que tenemos que hacer es acceder a la carpeta **C:\Snort\etc** en este directorio encontraremos un fichero llamado **snort.conf**, que es el fichero de configuración que utilizaremos para configurar Snort.

Accedemos al fichero con un editor de texto que no corrompa el formato original del archivo (notepad o wordpad). En la parte final donde hay una serie de «includes» con tipos de reglas, que en función de que tengan delante el signo almohadilla, «#», o no, se incluirán en la revisión de los paquetes.

Para ello vamos a utilizar notepad++

- Antes de todo descargamos las reglas y sobre escribimos todos los ficheros... Uno de ellos es snort.conf, ficheros que vamos a modificar ahora.

Quitamos la # a las siguientes líneas y las dejamos de la siguiente forma:

```
# decoder and preprocessor event rules
```

```
include $PREPROC_RULE_PATH/preprocessor.rules
```

```
include $PREPROC_RULE_PATH/decoder.rules
```

```
include $PREPROC_RULE_PATH/sensitive-data.rules
```

Con esto, las reglas descargadas ya están operativas.

- En el archivo snort.conf, cambiar por:

```
var RULE_PATH c:\snort\rules
```

```
var SO_RULE_PATH c:\snort\so_rules
```

```
var PREPROC_RULE_PATH c:\snort\rules\preproc_rules
```

- Buscamos la declaración de la variable **var HOME_NET Any**. Se puede modificar de tres modos dependiendo de lo que se quiera: **1) Una red C: var HOME_NET 192.168.1.0/24** **2) Host específico : var HOME_NET 192.168.1.3/32** **3) Varios Host: var HOME_NET 192.168.1.2/32,192.168.1.3/32,192.168.1.4/32** Ojo: por defecto vendrá ipvar en vez de var. Deberemos cambiarlo para que no se nos produzca un error. Cambie a la configuración de la red (por ejemplo, var HOME_NET 192.168.1.1/24). Vamos a eliminar **# ipvar HOME_NET any** Y en su lugar por ejemplo:

```
var HOME_NET 192.168.1.102/32
```

- Buscamos la declaración **include classification.config** y realizamos el siguiente cambio **Comentamos el primero y añadimos el segundo...# include classification.config** **include c:\snort\etc\classification.config**
- Buscamos la declaración **include reference.config** y cambiarlo para incluir **c:\snort\etc\reference.config** **Comentamos el primero y añadimos el segundo...# include reference.config** **include c:\snort\etc\reference.config**
- Y finalmente guardamos el archivo
- Antes de ejecutar snort es conveniente bajarse las últimas reglas de detección. Para esto hay que ir a la página de snort, **downloads -> rules**.
- Solamente nos queda por modificar lo siguiente, cambiar la línea donde aparece:

```
Dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/
```

por:

```
dynamicpreprocessor directory c:\snort\lib\snort_dynamicpreprocessor
```

- Y la línea que pone:

```
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
```

Por:

```
dynamicengine c:\snort\lib\snort_dynamicengine\sf_engine.dll
```

- Además dynamicdetection directory /usr/local/lib/snort_dynamicrules

por

dynamicdetection directory c:\snort\lib\snort_dynamicrules

- Una vez realizados estos cambios podemos probar Snort desde la línea de comandos. Accedemos a la carpeta **c:\Snort\bin** en este directorio escribimos:

```
C:\Snort\bin>snort -dev -c c:\snort\etc\snort.conf -l c:\snort\log -i2
```

Errores que pueden producirse

Error.Missing/incorrect dynamic engine lib specifier.

Dejamos el código de snort.conf de la siguiente forma:

```
# dynamicpreprocessor directory c:\snort\lib\snort_dynamicpreprocessor\  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_dce2.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_dnp3.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_dns.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_ftptelnet.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_gtp.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_imap.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_modbus.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_pop.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_reputation.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_sdf.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_sip.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_smtp.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_ssh.dll  
  
dynamicpreprocessor c:\snort\lib\snort_dynamicpreprocessor\sف_ssl.dll
```

Error. Unable to open rules file «c:\snort\etc\c:\snort\rules\preproc_rules\preprocessor.rules»:

Invalid argument.

El código en snort.conf:

```
var SO_RULE_PATH c:\snort\so_rules
```

```
var PREPROC_RULE_PATH c:\snort\rules\preproc_rules
```

cambiar por

```
var SO_RULE_PATH ../so_rules
```

```
var PREPROC_RULE_PATH ../preproc_rules
```

Error. Unknown preprocessor: «normalize_ip4».

Cambiar código en snort.conf:

```
#preprocessor normalize_ip4
```

```
#preprocessor normalize_tcp: ips ecn stream
```

```
#preprocessor normalize_icmp4
```

```
#preprocessor normalize_ip6
```

```
#preprocessor normalize_icmp6
```

Error. Unable to open address file c:\snort\etc\../rules/white_list.rules, Error: No such file or directory

```
var WHITE_LIST_PATH ../rules
```

```
var BLACK_LIST_PATH ../rules
```

Por

```
var WHITE_LIST_PATH ../rules
```

```
var BLACK_LIST_PATH ../rules
```

Y

```
whitelist $WHITE_LIST_PATH/white_list.rules, \
```

```
blacklist $BLACK_LIST_PATH/black_list.rules
```

por

```
whitelist $WHITE_LIST_PATH\white_list.rules, \
```

```
blacklist $BLACK_LIST_PATH\black_list.rules
```

Error. Unable to open address file c:\snort\etc\rules\white_list.rules, Error: No such file or directory

Creamos white_list.rules y black_list.rules en la ruta.... Usamos notepad, se crean vacíos. Estos ficheros solo se descargan para usuarios suscriptores. No es suficiente ser registrado.

- Finalmente ya funciona...

snort -dev -c c:\snort\etc\snort.conf -l c:\snort\log -i2

Las opciones que le hemos pasado en la línea de comandos a Snort son:

- -d: visualizar los campos de datos que pasan por la interface de red.
- -e: snort nos mostrará información más detallada.
- -v: Iniciamos snort en modo sniffer visualizando en pantalla las cabeceras de los paquetes TCP/IP.
- -c: archivo que utilizará snort como fichero de configuración.
- -l: directorio donde guardar las alertas y logs.
- -i: interfaz que monitorizaremos.

Prueba final

Si ejecutamos aun comando agresivo veremos el resultado:

nmap -T4 -A -v 192.168.1.1 (escan intenso contra la puerta de enlace)

En alert.ids aparece la información detectada...

```
[**] [119:31:1] (http_inspect) UNKNOWN METHOD [**]
```

```
[Classification: Unknown Traffic] [Priority: 3]
```

```
06/13-20:07:20.197014 00:1F:3C:16:56:0B -> 00:0F:66:4D:45:2E type:0x800 len:0x1AD
```

```
192.168.1.102:1353 -> 192.168.1.1:80 TCP TTL:64 TOS:0x0 ID:19479 IpLen:20 DgmLen:415 DF
```

```
***A*** Seq: 0xB531B7EF Ack: 0x3F41FDBF Win: 0x1920 TcpLen: 20
```

.....

Significado de la captura.

Por ejemplo:

- Tipo aviso y clasificación de la amenaza... Inclusive su prioridad. clasificación de la alerta contenida en el archivo classification.config.
- Marca de tiempo
- MAC Address origen y MAC Address destino

- Tipo del paquete y tamaño
- IP origen e IP destino
- Protocolo asociado a la generación de la alerta
- TTL:64 tiempo de vida
- TOS:0x0 tipo de servicio
- ID:43469 Identificador de sesión
- IpLen:20 corresponde con la cabecera IP Tamaño de la cabecera o Header Length (20 bytes).
- DgmLen:40 corresponde con total Length (40)

Esta entrada fue publicada en [Seguridad](#) y etiquetada [IDS](#), [Snort](#), [windows](#). Guarda el [enlace permanente](#).

4 Responses to *Instalación IDS Snort para Windows*

[akil3s \(@1GbDeInfo\)](#) dice:

19 febrero, 2014 a las 14:27

Genial entrada, muy bien explicado todo.

Hace poco probé la instalación para CentOS con el post de los chicos de HihgSec y ahora este me viene perfecto.

[Responder](#)

Agustí Pons dice:

19 febrero, 2014 a las 19:37

Muchas gracias

[Responder](#)

algodelinux dice:

24 agosto, 2016 a las 19:53

Gracias por tu buen tutorial. Me aparece un problema que no esta descrito ni encuentro por la red: me dice improperly formatted directory name para C:\Snort\lib\snort_dynamicengine\sف_engine.dll

[Responder](#)

algodelinux dice:

24 agosto, 2016 a las 21:51

Probé a poner sólo la ruta de la forma
dynamicengine c:\snort\lib\snort_dynamicengine
sin el nombre de la dll y así me funcionó. Gracias de todas formas.

[Responder](#)

Learning IT Security. Seguridad Informática.

Crea un blog o un sitio web gratuitos con WordPress.com.