



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
TERCERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

Seminario web: Reglas de Snort

Material adicional



TU AYUDA EN
CIBERSEGURIDAD



INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Ejercicio práctico	3
2. Ejercicio de investigación	4

1. EJERCICIO PRÁCTICO

El objetivo del ejercicio es mejorar las reglas propuestas en los ejemplos de creación de reglas.

Por una parte, la regla de detección de tráfico a las páginas web de Facebook. Y por otro lado, reglas que permitan detectar tráfico IRC en nuestra organización.

Los usuarios deberán de investigar su creación y contestar a las siguientes preguntas:

- ¿Es posible buscar únicamente el dominio en las cabeceras HTTP? Aplicar a la regla de Facebook.
- ¿Se pueden crear búsquedas más complejas que solo texto o valores en hexadecimal? Aplicar a la regla de IRC.

Resolución del ejercicio:

Se puede utilizar la palabra clave “uricontent” en vez de “content” a la hora de buscar información únicamente de la URI de las peticiones HTTP.

La regla quedaría de este modo:

```
log tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "Conexión a Facebook";  
uricontent: "facebook.com"; sid:1000001)
```

En el caso de IRC, es posible realizar expresiones regulares en la consulta del contenido. Por ejemplo, para buscar varios comandos de IRC en la misma regla podríamos hacer lo siguiente:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 6666:7000 (msg: "Conexión a  
servidor IRC"; pcre: "/(JOIN|NICK|SERVER)/"; sid:1000002)
```

2. EJERCICIO DE INVESTIGACIÓN

Cómo se podría utilizar Snort para ajustar los valores de la regla que detecta errores de fallos de acceso a servidores FTP y si el servidor de origen es 10.0.0.250, no se ejecute esta regla ya que ese servidor es una honeypot.

Pista: revisar el archivo de configuración “threshold.conf” que trae por defecto Snort.

Resolución del ejercicio:

Se tendría que añadir una nueva línea de configuración a nuestro archivo de “threshold.conf” con los siguientes datos:

```
suppress gen_id 1, sig_id 1000003, track by_src, ip 10.0.0.250
```

Con esa línea se suprime la regla 1000003 para la ip de origen 10.0.0.250.