Comandos Wireshark

2015-09-07

Concatenadores y Operadores

Concatenadores

```
&& -> AND lógico (y)
|| -> OR lógico (ó)
```

Operadores

```
contains -> Contener (se usa cuando no sabemos exáctamente todo)
== -> Comparación (igual)
!= -> Comparación (desigual)
```

> Nota: Cuando se trata de igualdades, siempre hay dos símbolos. Si la igualdad es un número, se pone este directamente. Si es una cadena de texto, se ha de poner con comillas.

Protocolos

```
ssl -> Protocolo SSL (capa segura).
telnet -> Telnet.
dns -> DNS.
msnms -> Mensajería Instantánea (Messenger).
ftp -> Protocolo FTP (podriamos ver el nombre de usuario y contraseña).
ftp-data -> Nos permite ver los datos del protocolo FTP.
ip -> Protocolo IP.

ip.src==192.168.1.1 -> Dirección IP de Origen.
ip.dst==192.168.1.1 -> Dirección IP de Destino.

tcp -> Protocolo TCP

tcp.port==80 -> Indicamos los paquetes con el puerto deseado.
tcp.srcport==80 -> Indicamos el puerto de origen.
tcp.dstport==80 -> Indicamos el puerto de destino.

http -> Protocolo HTTP

http.host=="www.google.com" -> Queremos ver los paquetes que tengan a Google como host.
http.date=="Wed, 30 Mar 2011 22:40:55 GMT" -> Paquetes con respecto a una fecha
http.content_type=="application/json" -> Según el tipo. Hay más tipos
http.content_type=="image/png" -> Imágenes PNG
http.content_type=="image/gif" -> Imágenes GIF
http.content_type=="image/jpeg" -> Imágenes JPEG
http.content_type=="text/html" -> Archivos HTML
http.content_type=="text/css" -> Hojas de estilo CSS
http.content_type=="video/quicktime" -> Vídeos
http.content_type=="application/zip" -> Archivos ZIP
http.request.method=="GET" -> Tipo de Petición GET
http.request.method=="POST" -> Tipo de Petición POST
http.user_agent contains "Mozilla" -> Navegador Mozilla
```

```
http.request.uri!=*-> Con esto me libro de los paquetes "NOTIFY * HTTP…"
http.request.uri matches "[0-9]" -> Uso de expresiones regulares.
```