wirshark, filtros

Filtros en Wireshark

Filtros de Captura

Los filtros de captura se aplican a la hora de capturar el tráfico de red . Es decir vamos a filtrar todo el tráfico para quedarnos con la parte del tráfico de red que permita el filtro.

Filtros de Visualización

Los filtros de visualización se aplican sobre el tráfico capturado para visualizar los paquetes de interés dentro de una captura.

Sintáxis

calificador + operador + primitiva

El calificador puede tratarse de un protocolo, campo de la cabecera de un protocolo, o simplemente una característica de un protocolo.

Para visualizar los paquetes del un protocolo bastaría con poner en la línea de filtro el protocolo, así por ejemplo podrámos poner; arp, ip, tcp, udp, http, dns etc para visualizar los paquetes de ese protocolo.

Por ejemplo para visualizar los paquetes de una ip determinada → ip == 192.168.0.1

Los filtros de visualización utilizan una sintáxis diferente a la de los filtros de captura (BPF)

Es posible unir 2 o más filtros de visualización a través de concatenadores lógicos.

- &&: implica que ambos filtros deben cumplirse. Es como un operador lógico **AND**
- | |: implica que es suficiente con que uno de los filtros se cumpla. Es como el operador lógico **OR**

Ejemplos:

```
ip.src == 192.168.0.1 && tcp.port == 80
tcp.port == 80 || tcp.port == 443
```

From:
https://intrusos.info/ - **LCWIKI**

Permanent link:
https://intrusos.info/doku.php?id=red:wireshark:filtros&rev=1623243584

Last update: **2023/01/18 14:19**