Lista de Filtros

YACHA

Sintáxis

Los filtros de visualización utilizan una sintáxis diferente a la de los filtros de captura (BPF). Los filtros de visualización son más complejos porque nos permiten mayor granularidad. Además de filtrar nodos o aplicaciones, logran filtrar los campos dentro de las cabeceras de los protocolos, e inclusive filtros adicionales a ellos, que sirven para buscar características específicas de algunos protocolos.

La sintáxis básica de los filtros de visualización es la siguiente:

ip == 192.168.0.1

calificador + *operador* + *primitiva*

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

Tipos de filtros

Protocolo

arp	protocolo ARP
ip	protocolo IP
ipv6	protocolo IPv6
tcp	protocolo TCP
udp	protocolo UDP
bootp	protocolo Bootstrap (DHCP)
dns	protocolo DNS
tftp	protocolo TFTP
http	protocolo HTTP
icmp	protocolo ICMP (ping)

Campo (de la cabecera de un protocolo)

http.host	Campo HOST de la cabecera HTTP
ftp.request.command	Campo REQUEST COMMAND de la cabecera FTP
bootp.option.hostname	Campo OPTION HOSTNAME de la cabecera BOOTSTRAP

Característica (de un protocolo)

tcp.analysis.flags	Etiquetas añadidas como: *Next expected sequence number, etc.*
tcp.analysis.zero_window	Campo habilitado cuando la ventana es cero.

Operadores de comparación

==	eq	igual a
!=	ne	no igual a
>	gt	mayor a
<	lt	menor a
>=	ge	mayor o igual a
<=	le	menor o igual a
	contains	contiene a

Concatenadores

&&	and	todos
||	or	cualquiera

Ejemplos

Simples

ip.addr == 192.168.0.1 Filtrar paquetes que incluyan la IP
!ip.addr == 192.168.0.1 Filtrar paquetes que no incluyan la IP
ipv6.addr == 2406:da::3f42:487a Filtrar paquetes que incluyan la IPv6
ip.src == 192.168.0.1 Filtrar paquetes que incluyan la IP de origen
ip.dst == 192.168.0.1 Filtrar paquetes que incluyan la IP de destino
ip.host == www.cnn.com Filtrar paquetes que incluyan el hostname
ip.addr == 192.168.0.0/24 Filtrar paquetes que incluyan IPs de la subred
!ip.addr == 192.168.0.0/24 Filtrar paquetes que no incluyan IPs de la subred

Avanzados

ip.src == 192.168.0.1 Filtrar paquetes que contengan a la IP 192.168.0.1
tcp.src.port != 80 Filtrar paquetes que no contengan al puerto origen TCP 80
frame.time_relative > 1 Filtrar tiempo mayores a 1s respecto a la primera trama
tcp.window_size < 1460 Filtrar ventana TCP mayores a 1460 bytes
dns.count.answers >= 10 Filtrar respuestas DNS con más de 10 direcciones IP
ip.ttl <= 10 Filtrar paquetes con valores de TTL menores a iguales 10
http contains "GET" Filtrar paquetes HTTP que contengan el comando GET

Concatenadores

ip.src == 192.168.0.1 && tcp.port == 80 Filtrar paquetes que cumplan ambas condiciones
tcp.port == 80 || tcp.port == 443 Filtrar paquetes que cumplan alguna de las condiciones