Lista de Filtros

YACHA

Sintáxis BPF

Berkeley Packet Filter

La sintáxis BPF determina el formato que deben cumplir los filtros de captura de Wireshark. Bajo ese formato, los filtros tienen 2 partes: 1) el calificador, que determina el objetivo del filtro y 2) la primitiva, que es el valor específico a filtrar. Una expresión o filtro tiene el siguiente formato:

host 192.168.0.1

calificador + *primitiva*

- Existen 3 tipos de calificadores:
  - Type: host, net, port, portrange
  - Dir: src, dst, src or dst, src and dst, ra, ta, addr1, addr2, addr3, addr4
  - Proto: ether, fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp, udp

Filtrado de nodos

Tráfico hacia/desde una dirección IP

host 192.168.0.1	Capturar tráfico hacia/desde IP
host 2406:da00:f00::6b16:f02d	Capturar tráfico hacia/desde IPv6
not host 192.168.0.1	Capturar todo el tráfico excepto de/desde IP
src host 192.168.0.1	Capturar tráfico desde IP
dst host 192.168.0.1	Capturar tráfico hacia IP
host 192.168.0.1 or host 192.168.20.1	Capturar tráfico hacia/desde ambas IP
host www.cnn.com	Capturar tráfico hacia/desde URL

Tráfico hacia/desde un rango de direcciones IP

net 192.168.0.0/24	Capturar tráfico hacia/desde cualquier IP de la subred
net 192.168.0.0 mask 255.255.255.0	Capturar tráfico hacia/desde cualquier IP de la subred
ipv6 net 2406:da00:f00::/64	Capturar tráfico hacia/desde cualquier IPv6 de la subred
not dst net 192.168.0.0/24	Capturar todo el tráfico excepto hacia la subred
not src net 192.168.0.0/24	Capturar todo el tráfico excepto desde la subred

Tráfico hacia/desde un rango de direcciones IP

ip broadcast	Capturar tráfico hacia/desde 255.255.255.255
ip multicast	Capturar tráfico hacia/desde 224.0.0.0 – 239.255.255.255
dst host ff02::1	Capturar tráfico para direcciones multicast IPv6 (nodos)
dst host ff02::2	Capturar tráfico para direcciones multicast IPv6 (routers)

Tráfico hacia/desde una dirección MAC

ether host 00:08:15:00:08:15	Capturar tráfico hacia/desde MAC
ether src host 00:08:15:00:08:15	Capturar tráfico desde MAC
ether dst host 00:08:15:00:08:15	Capturar tráfico hacia MAC
not ether host 00:08:15:00:08:15	Capturar todo el tráfico menos para MAC

Filtrado de servicios

Tráfico de puertos TCP/UDP

port 53	Capturar tráfico UDP/TCP del puerto 53
not port 53	Capturar todo el tráfico excepto UDP/TCP del puerto 53
udp port 67	Capturar tráfico UDP del puerto 67
tcp dst port 21	Capturar tráfico TCP del puerto destino 21
portrange 1-80	Capturar tráfico UDP/TCP del rango de puertos 1 al 80

Combinar nodos y puertos

port 20 or port 21	Capturar tráfico UDP/TCP del puerto 21
host 192.168.0.1 and port 80	Capturar tráfico UDP/TCP del socket IP:80
host 192.168.0.1 and not port 80	Capturar todo el tráfico de la IP, excepto del puerto 80
udp src port 68 and udp dst port 67	Capturar tráfico DHCP desde nodo
udp src port 67 and udp dst port 68	Capturar tráfico DHCP desde servidor