**Block Port Scanner di Mikrotik**

Assalamu'alaikum...  
di bagian filter:  
  
Code:  
/ip firewall filter  
add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w comment="Port scanners to list " disabled=no

**Chain ini dipakai untuk mendaftar ip ke black-list address list  
Chain selanjutnya untuk mendeteksi apakah ada indikasi aktifitas port scanner:**  
  
add chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg  
action=add-src-to-address-list address-list="port scanners"  
address-list-timeout=2w comment="NMAP FIN Stealth scan"  
  
add chain=input protocol=tcp tcp-flags=fin,syn  
action=add-src-to-address-list address-list="port scanners"  
address-list-timeout=2w comment="SYN/FIN scan"  
  
add chain=input protocol=tcp tcp-flags=syn,rst  
action=add-src-to-address-list address-list="port scanners"  
address-list-timeout=2w comment="SYN/RST scan"  
  
add chain=input protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack  
action=add-src-to-address-list address-list="port scanners"  
address-list-timeout=2w comment="FIN/PSH/URG scan"  
  
add chain=input protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg  
action=add-src-to-address-list address-list="port scanners"  
address-list-timeout=2w comment="ALL/ALL scan"  
  
add chain=input protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg  
action=add-src-to-address-list address-list="port scanners"  
address-list-timeout=2w comment="NMAP NULL scan"  
  
**jika ada tanda tanda dari kejadian di atas, maka harus didrop scanning IPnya pakai perintah ini:**  
  
add chain=input src-address-list="port scanners" action=drop comment="dropping port scanners" disabled=no