Mikrotik: Block port scanners

Getting tired of port scanners like I am? Block them with these few simple rules. It is not bullet proof but it will reduce your daily headache.

Paste this into Mikrotik terminal

```
/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
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"
add chain=input src-address-list="port scanners" action=drop
comment="dropping port scanners" disabled=no
```

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=mikrotik:scripting:block_portscanners

Last update: **2019/10/31 09:05**