Drop port scanners

To protect the Router from port scanners, we can record the IPs of hackers who try to scan your box. Using this address list we can drop connection from those IP

in **/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
```

Various combinations of TCP flags can also indicate port scanner activity.

```
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"
```

Then you can drop those IPs:

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

Similarly, you can drop these port scanners in the forward chain, but using the above rules with "chain=forward".