Trouble with Fail2Ban UFW Portscan Filter

Asked 6 years, 6 months ago Active 6 years, 6 months ago Viewed 4k times

1

I'm trying to create a filter for fail2ban that recognises port scans in the UFW logs.
I've confirmed my ban action is working correctly on other filters and am having trouble creating the correct filter/regex expression on this occasion - I'm sure it'll turn out to be a silly mistake on my part.
I have tried the fail2ban-regex utility and got 0 hits.

My `jail.local` contains:

```
[ufw-port-scan]
enabled = true
port = all
filter = ufw-port-scan
banaction = ufw-action
logpath = /var/log/ufw.log
maxretry = 10
```

The filter I'm attempting to create (placed in `/etc/fail2ban/filter.d/ufw-port-scan.conf`) looks like this:

```
[Definition]
failregex = kernel: \[UFW BLOCK\] IN=.* SRC=<HOST>
ignoreregex =
```

A sample line that I am trying to identify in the `ufw.log` :

```
Sep 18 21:06:08 trial kernel: [ 3014.939702] [UFW BLOCK] IN=eth0 OUT=
MAC=00:00:00:00:00:00:00:00:00:00:00:00:00 SRC=192.168.0.5 DST=192.168.0.10
LEN=44 TOS=0x00 PREC=0x00 TTL=45 ID=36825 PROTO=TCP SPT=50704 DPT=80
WINDOW=1024 RES=0x00 SYN URGP=0
```

Any guidance would be appreciated - thank you.

firewall | log-files | regex | fail2ban | ufw

Share Improve this question Follow

asked Sep 19 '14 at 1:17

Touff
163 1 3 12

1 Answer

Active | Oldest | Votes

1

You were close.

```
failregex = .*\[UFW BLOCK\] IN=.* SRC=<HOST>
```

And possibly remove `port = all` (Its optional)

You can run tests using fail2ban-regex. eg:

```
fail2ban-regex  /var/log/ufw.log '.*\[UFW BLOCK\] IN=.* SRC=<HOST>'
```

answered Sep 19 '14 at 4:04

ticoombs
148 4