

Forum:[Hack Forums](#)

Thread: [Make your system - RASPBERRY PI - a bit more secure!\[Tutorial\] No more bruteforce](#)

slober - December 17, 2016, 4:38 am

Make your system - RASPBERRY PI - a bit more secure!

IoT is awesome!

Code FailIP.txt

AttemptsFailedPasswords. IP

1 109.226.102.146

1 111.243.15.91

1 111.249.213.229

361 112.132.231.1

3634 116.31.116.23

44926 116.31.116.28

1 14.161.76.196

1 14.162.122.119

1 14.162.185.114

1 14.169.136.214

1 14.184.39.191

1 14.186.205.101

1 14.186.27.1

12 142.54.173.251

989 153.99.182.2

1 176.51.134.101

1 176.51.64.33

1 178.123.206.23

1 178.65.64.34

6 179.40.164.41

294 182.100.67.120

1 182.74.203.78

6 185.110.132.202

1 188.17.152.177

6 191.82.60.217

4 192.162.101.217

4 194.63.141.141

1 195.168.172.14

1 195.20.3.210

1 195.77.36.85

1 201.71.141.79

8 212.83.128.148

1 213.228.79.39

360 218.65.30.134

223 218.65.30.43

1 36.228.79.35

1 36.239.147.49

1 37.252.92.220

1 37.252.94.26

```
1 37.252.94.89
1 37.252.95.86
4 38.84.132.236
1 41.237.108.112
6 45.21.91.114
12 51.254.116.228
5 5.196.76.41
9205 59.63.166.83
1 81.90.227.12
1 90.232.44.4
47 91.224.160.108
47 91.224.161.88
1 91.44.158.238
186 92.63.249.14
1 93.183.253.205
```

Due to the increasing number of connected devices the number of Bots and crawlers are also increasing.

which can and will! result in your server being attacked sooner or later.

Code 44926 116.31.116.28

44 926 Failed login Attempts from this guy!

Let's fix this!

First of all you should check if you are being attacked or something like that you could do this with this script:

If it looks nasty you should keep reading. ?

We'll use the tool Fail2Ban to secure our system

www.fail2ban.org Wrote:Fail2ban scans log files (e.g. /var/log/apache/error_log) and bans IPs that show the malicious signs -- too many password failures, seeking for exploits, etc. Generally Fail2Ban is then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action (e.g. sending an email) could also be configured. Out of the box Fail2Ban comes with filters for various services (apache, courier, ssh, etc).

Fail2Ban is able to reduce the rate of incorrect authentications attempts however it cannot eliminate the risk that weak authentication presents. Configure services to use only two factor or public/private authentication mechanisms if you really want to protect services.

Code sudo apt-get install fail2ban

After this you're pretty much done but there are some extras you could do.

goto /etc/fail2ban/jail.conf

Code sudo nano /etc/fail2ban/jail.conf

OR

sudo vi /etc/fail2ban/jail.conf

find the line [ssh] or another service [YOUR_SERVICE] you wish to change.

Code banaction = iptables-allports

bantime = 3600

maxretry = 3Ban user on all ports after 3 failed passwords for 1hour

After this you just need to restart the server:

Code sudo service fail2ban restartYou successfully installed fail2ban onyour system!

Some usefull commands

Code # View all banned ip's

sudo iptables -L -n

Reset iptables

sudo iptables -F

Now we're at least a little bit safer!

Code	target	prot	opt	source	destination	
REJECT	all	--		218.65.30.134	0.0.0.0/0	reject-with icmp-port-unreachable
REJECT	all	--		182.100.67.120	0.0.0.0/0	reject-with icmp-port-unreachable
REJECT	all	--		115.239.248.35	0.0.0.0/0	reject-with icmp-port-unreachable
REJECT	all	--		106.247.230.226	0.0.0.0/0	reject-with icmp-port-unreachable
REJECT	all	--		116.31.116.48	0.0.0.0/0	reject-with icmp-port-unreachable
REJECT	all	--		185.110.132.202	0.0.0.0/0	reject-with icmp-port-unreachable
REJECT	all	--		51.254.116.228	0.0.0.0/0	reject-with icmp-port-unreachable
REJECT	all	--		116.31.116.23	0.0.0.0/0	reject-with icmp-port-unreachable
RETURN	all	--		0.0.0.0/0	0.0.0.0/0	

?Anubis - December 17, 2016, 9:55 am

Nice thread. Thanks for making a tutorial on this.

webdev77 - December 17, 2016, 1:06 pm

While I am assuming you mean for this to be used on a Raspberry Pi, you should probably explain that since a lot of people here won't get what this means.

slober - December 17, 2016, 1:45 pm

(Dec 17, 2016 02:06 PM)webdev77 Wrote: [\[CITE\]](#) While I am assuming you mean for this to be used on a Raspberry Pi, you should probably explain that since a lot of people here won't get what this means.

Like this? ? I've added it to the title. also added general description of fail2ban. this should clear up some of the confusion. Thx!