This repository has been archived by the owner. It is now read-only.

Amet13 / **ddos-deflate** Archived

Shell script blocking DDoS attacks. Not maintained since 2016

#shell #ddos #netstat

59 commits **1** branch **0** packages **0** releases **1** contributor

Branch: **master** ▾ Find File Clone or download ▾

Amet13 README edit Latest commit `1b3e088` on Oct 21, 2016

README.md	README edit	3 years ago
ddos-deflate.conf	Install script renamed config	4 years ago
ddos-deflate.sh	Deleted record to ignoreip.list	3 years ago
ignoreip.list	edited uninstall script	4 years ago
install.sh	Install script renamed config	4 years ago
uninstall.sh	correct filenames	4 years ago

README.md

ddos-deflate

Shell script blocking DDoS attacks. Simplified fork of (D)DoS Deflate.

Not maintained since 2016.

Installation

```
sudo -i
cd /tmp
wget -q -O - https://raw.githubusercontent.com/Amet13/ddos-deflate/master/install.sh | bash
```

Setup config for example:

```
vim /usr/local/ddos-deflate/ddos-deflate.conf
NO_OF_CONNECTIONS=500
EMAIL_TO="mail@example.com"
BAN_PERIOD=60
CUSTOM_PORTS=":80|:443:|:53|:21"
ENABLE_LOG=YES
```

Add your ignore IP's to ignore list:

```
vim /usr/local/ddos-deflate/ignoreip.list
127.0.0.1
192.168.0.1
1.1.1.1
2.2.2.2
```

Check:

```
bash /usr/local/ddos-deflate/ddos-deflate.sh
    724 127.0.0.1
    214 2.2.2.2
     59 3.3.3.3
...
```

Testing

Run ab from another computer:

```
user@192.168.0.100 ~ $ ab -n 200000 -c 100 http://server-ip/
```

Check new IPTables rules on server:

```
iptables -t raw -L PREROUTING
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.100        anywhere
```

Check logs:

```
tail -1 /var/log/ddos-deflate.log
26/12/2015 [17:50:00] -- 192.168.0.100 blocked on 60 seconds
```

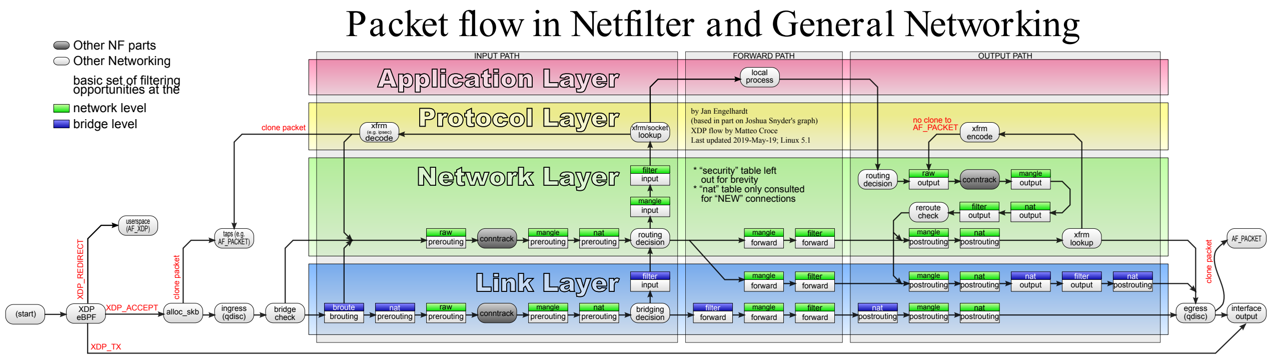
Check your inbox:

```
Subject: IP addresses banned on 26/12/2015 [17:50:02]

Banned the following IP addresses on 26/12/2015 [17:50:02]
From: hostname.tld (192.168.0.13)

192.168.0.100 with 4183 connections blocked on 60 seconds
```

Uninstallation

```
sudo -i
cd /tmp
wget -q -O - https://raw.githubusercontent.com/Amet13/ddos-deflate/master/uninstall.sh | bash
```

Why RAW table instead FILTER?


Packet flow in Netfilter and General Networking

by Jan Engelhardt
(based in part on Joshua Snyder's graph)
XDP flow by Matteo Croce
Last updated 2019-May-19; Linux 5.1

* “security” table left out for brevity
* “nat” table only consulted for “NEW” connections

Original author

zaf@vsnl.com

License

Artistic License 2.0