

Forum:[Hack Forums](#)

Thread: [Tutorial Block DDoS Attacks on a Dedi](#)

hax0r - February 3, 2012, 2:37 am

Hey, heres my Tutorial How to block some DDoS Attacks =)

```
nano /etc/sysctl.conf
add this
Code net.ipv4.tcp_syncookies = 1
net.ipv4.conf.default.rp_filter = 1
save it, and do this: sysctl -p or reboot your server.
```

```
now we install csf firewall by doing this:
Code cd
mkdir csf
cd csf
wget http://www.configserver.com/free/csf.tgz
tar xfvz csf.tgz
cd csf
./install.sh
to test if it will work correctly on your server
Code cd /etc/csf
./csftest.pl
Code [root@loadbalancing1 csf]# ./csftest.pl
Testing ip_tables/iptables_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing ipt_owner...OK
Testing iptable_nat/iptables_REDIRECT...OK
If you see this, everything seems to be fine.
If not, you have to activate the Modules by pasting this:
Code modprobe iptable_nat
modprobe ipt_owner
modprobe ipt_recent
then we have to make some changes to make the csf firewall work creamy
```

```
nano /etc/csf/csf.conf
```

```
then u change
Code TESTING = "1"to
Code TESTING = "0"to activate it and stop testing mode.
```

```
Code # Allow incoming PING
ICMP_IN = "1"to
Code # Allow incoming PING
```

ICMP_IN = "0"so you cant ping the server =)

Code # Allow outgoing PING

ICMP_OUT = "1"to

Code # Allow outgoing PING

ICMP_OUT = "0"

Code DROP_PF_LOGGING = "0"to

Code DROP_PF_LOGGING = "1"

Code SYNFLOOD = "0"

SYNFLOOD_RATE = "100/s"

SYNFLOOD_BURST = "150"to

Code SYNFLOOD = "1"

SYNFLOOD_RATE = "300/s"

SYNFLOOD_BURST = "300"

note if "ipt_recent" module not working, you can skip this step.

Code PORTFLOOD = ""to

Code PORTFLOOD = "80"

Code /etc/init.d/csf start

ok, now we have csf firewall installed.

now you do syn deflate

Code wget <http://www.Anti-Hack.net/scripts/synd/install.sh>

mv install.sh?drgn=1 install.sh

chmod 0700 install.sh

./install.sh

Code cd /usr/local/synd

./synd.sh --cron

if it says

Code Stopping crond: [OK]

Starting crond: [OK]

Stopping crond: [OK]

Starting crond: [OK]

it should be fine, if not you create the cronjob manually.

by typing

Code crontab -eand pasting this:

Code */1 * * * * root /usr/local/synd/synd.sh

Now we do synblock.

Code wget <http://www.Anti-Hack.net/scripts/synblock/install.sh>

mv install.sh?drgn=1 install.sh

chmod 0700 install.sh

./install.sh

To block some Attacks by Hand.

Code cd /usr/local/synblock

nano synblock.conf

u change Intervall to 0

Code #Intervall des Monitors

speed=0

u change MAX_REQ to 15

Code MAX_REQ=15

then u save it and if u are under attack u can type synblock -m

then u let it load a bit...

then u press ctrl + c and press synblock -b

and some ips should be blocked.

Hope I helped a bit.

Questions? Or you are under DDoS and need help blocking it?
PM ME!

nikentic - February 3, 2012, 3:01 am

Nice guide, but it's not very useful unless you tell what the changes actually do. Do they change the TTL or something else?

Blue_x33 - February 3, 2012, 12:37 pm

great tutorial :)

I like all in one guides!

please add some stuff like nikentic told u! this would help all cypaste newbs to set it up ;D

Thanks for that HQ Thread!

ItsFluffy - February 3, 2012, 2:21 pm

seems legit info but i personally wouldn't know the first thing about what the info you presented

if i manage to learn then i will use this tut so thanks

lolsonlols - February 3, 2012, 4:05 pm

Basically, I think this is using IPTABLES to ban/drop IP's that are sending/requesting too much data in a short time span.

menagerie - February 3, 2012, 5:43 pm

its very simple to comprehend this guide you don't need a deep education of linux to set all this up if you follow the tutorial command par command.

csf is only a software firewall it helps alot against syn floods from my own experience running a cheating community - combining csf with a custom modified version of ddos deflate and running litespeed webserver (alot better off the shelf then apache!) i was taking hits all day and suffering 0 downtime except for when the port finally got clogged by someone using udp.

even that was pretty easy to clean up with.

back on topic this is a great guide and i saved it incase any of my colleagues need something like this.

Regards.

hax0r - February 3, 2012, 8:17 pm

Edited it a bit, thanks for your feedback guys =)

PS: I will add a guide for hosting etc. too ! =)

Ha4xor - February 5, 2012, 8:55 am

nice thread bro i hope you release more creamy things

an0nym0use - February 5, 2012, 8:57 am

Wow, great tutorial!

Thanks about that man !

BabaNugga - February 9, 2012, 11:03 am

Great Tutorial!

Thanks alot !

~ dies, das

??? - February 9, 2012, 11:52 am

This is a helpful guide, great Tutorial.

FaberCastell - February 9, 2012, 11:56 am

Not into things like that. But i doubt you wrote this.

From where did you copy paste this? It's right to post to who the credits goes to or what's the source, unless it's 100% yours.

Tony Montana - March 28, 2012, 4:39 pm

i TRIED all of thsis, none of it helped. I think its a SSYN attack, :(can u help?

??h™ - March 28, 2012, 5:14 pm

I'm sorry bro, but if someone hits you with like 10 gb/sec you're going down and a firewall won't help you...

hax0r - March 28, 2012, 9:44 pm

I dont think that his site is that big that hes getting 10gbps attacks.

yes I can help you, PM me please.