

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Basic DoS | DDoS protection ||| FOR FREE! \[/TUTORIAL\]](#)

bish0p - January 6, 2013, 3:23 am

Hi everyone.

I just thought about doing a little securing-for-noobs tutorial. So here it comes. Be advised that this is just very very basic and the only real DDoS protection will not work with any software, no matter how expensive it is.

DDoS and DoS protection in real case is:

- a good infrastructure
- external firewalls
- core routers external from firewall
- a good overwatch
- fallback systems

and much more.

So this wont keep you from a real DDoS attack but however it could keep some idiot skids from taking you down.

What we basically take to establish a little security is iptables. it should be preinstalled on nearly every servers but in case it isnt you can do it e.g. in the following ways:

Debian:

Code apt-get install iptablesCentos:

Code yum install iptablesAnd so on and so on. Off course you need to run this with administrative rights.

Now we can do some configuration.

So at first we will just block a connection if its hitting an UDP port X more then Y times a second:

Code iptables -A INPUT -p udp -m udp --dport X -m state --state NEW -m recent --set --name DEFAULT --rsource
iptables -A INPUT -p udp -m udp --dport X -m state --state NEW -m recent --update --seconds 1 --hitcount Y --name DEFAULT --rsource -j REJECT

Next we could control some established connections.

Code iptables -A INPUT -p tcp --syn -m limit --limit 1 /s --limit-burst X -j DROP

This will actually drop all new connection attempts after X connections are established.

Off yourse you have to think of a reasonable value here and insert it. Just before the skids start asking.

And furthermore since we are on a Linux-System we could drop all microshit (SMB&CIFS&Stuff). You can also modify this rule to block every port your server does not need:

Code \$IPTABLES -A INPUT -p tcp -m multiport --dports 135,137,138,139,445,1433,1434 -j DROP
\$IPTABLES -A INPUT -p udp -m multiport --dports 135,137,138,139,445,1433,1434 -j DROP
However this was some basic playaround with the IPtables. You can from this just get a bit further. Just think.

Depending on your configuration you may need some Administrative rights ro insert the rules as well as to display them. By the way you can see all the rules and status of your firewall with:

Code iptables -L -n

So what else can you do?

ATTENTION: Everything I'll show now will contain kernel modification. I am not an will neither be responsible for any damage taken to your system.

It may be that under a certain configuration besides the kernel, this changes can cause damage to your system! Handle with care!

You could disable all SYN/SSYN flood attacks, with setting a TCP-Syncookie for every connection. To do so, edit your /proc/sys/net/ipv4/tcp_syncookies, or do:

Code echo 1 > /proc/sys/net/ipv4/tcp_syncookies

Also its a good idea to ignore all incoming ICMP echo requests:

Code echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_all

Furthermore you have kind of some inbuilt spoofing protection, what only needs to be activated. I'd do this in bash:

Code Well this was a little entry to protectional systems that are free.

I hope this helped you.

Regards

#!/bin/bash

for i in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 1 > \$i; done

Oh last but not least maybe you should make your server neither accept nor resend any ICMP redirects:

Code #!/bin/bash

for i in /proc/sys/net/ipv4/conf/*/accept_redirects; do echo 0 > \$i; done

for i in /proc/sys/net/ipv4/conf/*/send_redirects; do echo 0 > \$i; done

I hope this helped some of you.

Regards

alexmkd1 - January 6, 2013, 4:18 am

Thank you for your tutorial!

This is helpful!

Telppa - January 6, 2013, 4:19 am

Thanks for the tutorial. Helped me a lot.

F A I T H - January 6, 2013, 5:07 am

Thank you for your tutorial! helped me alot.

Query. - January 6, 2013, 8:50 am

A word from the wise: this method is effective, ONLY if your pipe does not get saturated. If you have a 100 Mbps line, do not expect this to block anything more than a 100 Mbps flood.

bish0p - January 6, 2013, 11:30 am

(Jan 6, 2013 09:50 AM)Query. Wrote: [\[CITE\]](#) A word from the wise: this method is effective, ONLY if your pipe does not get saturated. If you have a 100 Mbps line, do not expect this to block anything more than a 100 Mbps flood.

Thats what I mentioned with: Only a good infrastructure will keep you from a real attack.

But however some more stuff works for me as I am on a 10G line...

But I think not many ppl will have that luck.

Sekret - February 23, 2014, 3:36 am

Great TUT, thanks for the effort ... found it very useful.

thegodhello - February 23, 2014, 6:08 am

thanks for the effort of writing this
i will surely use this on my hosting!

ChapTs - *February 23, 2014, 6:10 am*

Danke für die tutorial. It actually helped me a lot with dis :)

Gangolian - *January 27, 2015, 10:03 am*

Always appreciative of references & tutorials for iptables solutions.

Thank you man

janace101 - *January 27, 2015, 4:05 pm*

How can i apply ddos protection on a windows vps?