Subject: iptables!!1
Posted by denever on Mon, 18 Jul 2011 14:00:32 GMT
View Forum Message <> Reply to Message

```
sbin/iptables -F
/sbin/iptables -t nat -F
/sbin/iptables -t mangle -F

# other network protection
echo 1 > /proc/sys/net/ipv4/tcp_syncookies                    # enable syn cookies (prevent
against the common 'syn flood attack')
echo 0 > /proc/sys/net/ipv4/ip_forward                        # disable Packet forwarning between
interfaces
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts           # ignore all ICMP ECHO and
TIMESTAMP requests sent to it via broadcast/multicast
echo 1 > /proc/sys/net/ipv4/conf/all/log_martians                 # log packets with impossible
addresses to kernel log
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses       # disable logging of bogus
responses to broadcast frames
echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter                # do source validation by reversed
path (Recommended option for single homed hosts)
echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects               # don't send redirects
echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route          # don't accept packets with
SRR option


/sbin/iptables -P INPUT   DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT  DROP

# drop Bad Guys
/sbin/iptables -A INPUT -m recent --rcheck --seconds 60 -m limit --limit 10/second -j DROP

# drop unwanted services
/sbin/iptables -A INPUT -m multiport -p tcp --dports 25,110,111,119,143,465,563,587,993,995 -j
DROP
/sbin/iptables -A INPUT -m multiport -p tcp --dports 25,110,111,119,143,465,563,587,993,995 -j
DROP

# accept everything from loopback
/sbin/iptables -A INPUT  -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
```

```
# disable ping
/sbin/iptables -A INPUT  -p icmp -j DROP
# internet (established and out)
/sbin/iptables -A OUTPUT -o eth0 -j ACCEPT
/sbin/iptables -A INPUT  -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT


/sbin/iptables -A INPUT -p tcp --dport 2106 -j ACCEPT

/sbin/iptables -A INPUT -p tcp --dport 7777 -j DROP

###



/sbin/iptables -I INPUT -p tcp -s 95.72.242.107 --dport 3306 -j ACCEPT
/sbin/iptables -I INPUT -p tcp -s 94.142.139.88 --dport 3306 -j ACCEPT

/sbin/iptables -A INPUT -p tcp --dport 3306 -j DROP



/sbin/iptables -A INPUT -p tcp --dport 22 -s 95.72.242.107 -j ACCEPT

/sbin/iptables -A INPUT -p tcp --dport 22 -j DROP


login as: denever
root@92.53.104.12's password:
Linux *.*.ru 2.6.27-openvz-chistyakov.1-vps3 #3 SMP Mon Aug 2 18:40:47 MSD 2010 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jul 18 03:10:06 2011 from 95.72.242.107
denever:~# cd server/teste
denever:~/server/teste# ./aE.sh
FATAL: Could not load /lib/modules/2.6.27-openvz-chistyakov.1-vps3/modules.dep: No such file
or directory
iptables v1.4.2:
```

HELP!!!!

Subject: Re: iptables!!1
Posted by kir on Thu, 21 Jul 2011 15:52:03 GMT
View Forum Message <> Reply to Message