CSF - ConfigServer Security & Firewall

? perl ??? scripts??? iptables ??????

?????https://configserver.com/index.html

?????CentOS 7.2

?? CSF

// CentOS 7
yum install wget vim perl-libwww-perl.noarch perl-Time-HiRes unzip bind-utils

// CentOS 5/6
yum install perl-libwww-perl wget vim

// Ubuntu 16.04
sudo apt-get install libgd-graph-perl libwww-perl

cd /usr/src/
wget https://download.configserver.com/csf.tgz

tar -xzf csf.tgz
cd csf
sh install.sh

??

...
...
'csf/jquery.min.js' -> 'webmin/csf/images/jquery.min.js'
'csf/LICENSE.txt' -> 'webmin/csf/images/LICENSE.txt'
'csf/loader.gif' -> 'webmin/csf/images/loader.gif'
'/etc/csf/csfwebmin.tgz' -> '/usr/local/csf/csfwebmin.tgz'

Installation Completed

????

cd /usr/local/csf/bin/
perl csftest.pl

??

Testing ip_tables/iptable_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 xt_connlimit...OK
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/ipt_REDIRECT...OK
Testing iptable_nat/ipt_DNAT...OK

RESULT: csf should function on this server
```

?? CSF

Stop the firewalld

```
// CentOS 7
systemctl stop firewalld
systemctl disable firewalld

// CentOS 6
chkconfig iptables off
service iptables stop

// Ubuntu 16.04
sudo ufw disable

cd /etc/csf/
vim csf.conf
```

- ? TESTING ?? 0
- ?? TCP_IN ?????? SSH ????????????
- SSH ?? 5 ?????????? IP 3600 ????????????? 1

```
...
TESTING = "0"

...

RESTRICT_SYSLOG = "3"
...
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"

...

LF_SSHD = "5"
LF_SSHD_PERM = "3600"
```

?? CSF & LFD

// CentOS 7
systemctl start csf
systemctl start lfd
systemctl enable csf
systemctl enable lfd

// CentOS 5/6
service csf start
service lfd start
chkconfig csf on
chkconfig lfd on

????

iptables -L -nv
???????? csf ????

ps -ef | grep lfd
?? lfd ???? lfd ????

CSF ????
?????????

csf -l

??????

csf -f

??????

csf -s

????????

csf -r

?? IP ?????csf.allow?

csf -a 192.168.1.109

?????? IP

csf -ar 192.168.1.109

?? IP ?????csf.deny?

csf -d 192.168.1.109

?????? IP

csf -dr 192.168.1.109

??????????

csf -df

???? (csf.ignore)
??? IP ??? lfd ???

vi /etc/csf/csf.ignore

1.2.3.4
2.3.0.0/16

?????

- csfpre.sh??? CSF ???
- csfpost.sh : ?? CSF ???

NOTE?????????? /etc/csf ? /usr/local/csf/bin ????

/etc/csf/csfpost.sh?
?????? csf.conf ??? 80 & 443??? white-ip.lst ????????????

reference to undefined name 'syntax' Exception of type
'MindTouch.Deki.Script.Runtime.DekiScriptUndefinedNameException' was thrown. (click for details)
Q & A
Q: ?? lfd ????

   Main Process: Unable to send SENDMAIL alert via [/usr/sbin/sendmail]: No such file or directory
   at /usr/sbin/lfd line 4149

A: yum install sendmail

????????????? csf.conf

LF_EMAIL_ALERT = "0"

Q: ?? csf -r ????

   Error File does not exist: [/etc/crontab] at /usr/sbin/csf line 3307

A: yum install crontabs

Q: ?? csf -r ????

WARNING Binary location for [UNZIP] [/usr/bin/unzip] in /etc/csf/csf.conf is either incorrect, is not installed or is not executable

A: yum install unzip

Q: ?? csf -r ????

WARNING Binary location for [HOST] [/usr/bin/host] in /etc/csf/csf.conf is either incorrect, is not installed or is not executable

A: yum install bind-utils

????

- [How to Install and Configure CSF (Config Server Firewall) on CentOS 7](#)
- http://fyshung.blogspot.tw/2015/02/csf.html
- [How to Add Custom iptables Rules with CSF](#)