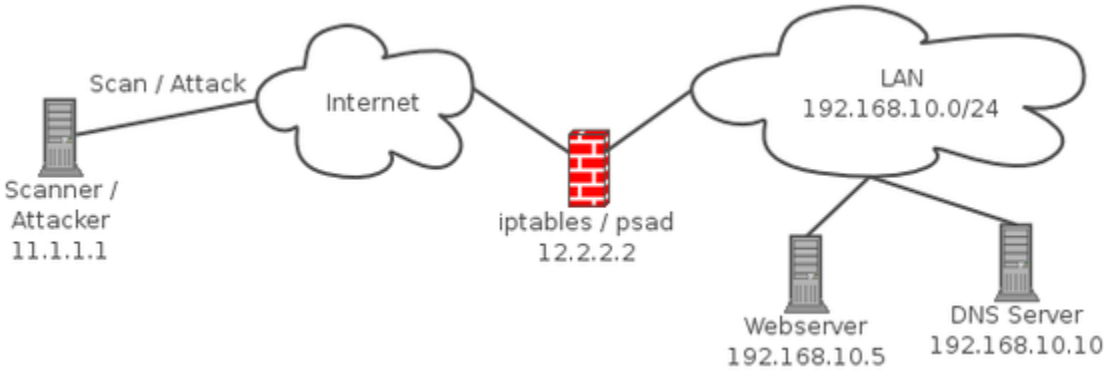
??

psad - Port Scan Attack Detector???????? Linux ?????????????????????????????????????? IP?

- ?????http://cipherdyne.org/psad/
- ? Perl ?????
- ???? iptables log ?????????
- ???????????????????????? iptables ??????????



????

?????CentOS 5.5 (Linux 2.6.18-194.26.1.el5)
?????http://cipherdyne.org/psad/download/

cd /usr/src
tar xzf psad-2.1.7.tar.gz
cd psad-2.1.7/
./install.pl

Notes:

- ???????? Enter?
- ?? Would you like to install the latest signatures from http://www.cipherdyne.org/psad/ signatures (y/n)????????? n ???
- ?? Enable psad at boot time ([y]/n)???? y ? Enter???????????????? chkconfig ????
- ?????? ./install.pl --uninstall?

?? iptables log

iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG

?? LOG ??

#iptables -L

Chain INPUT (policy DROP)
...
LOG all -- anywhere anywhere LOG level warning
...
Chain FORWARD (policy ACCEPT)
target prot opt source destination
LOG all -- anywhere anywhere LOG level warning

??????????? LOG
?? /etc/sysconfig/iptables?? *filter ???????? COMMIT ????

....
....
Enable LOG for psad daemon
-A INPUT -j LOG
-A FORWARD -j LOG
COMMIT

????

????? /etc/psad/psad.conf????????

?????

- EMAIL_ADDRESSES - ????????????????
- HOSTNAME - ?????
- SYSLOG_DAEMON - syslog ???????? syslogd?
- ETC_SYSLOG_CONF - syslog ????????? /etc/syslog.conf?

???????

- EMAIL_LIMIT - ??????? IP ???????????????? 0 - ????????????????????? 100?
- ALERTING_METHODS - ??????????? ALL - ??? email ???? syslog??????? nosyslog, noemail?
- EMAIL_ALERT_DANGER_LEVEL - ??? 1??????????? danger level ????????????????

?????

- ENABLE_AUTO_IDS - ??? N????? Y?????? IP ?????
- AUTO_IDS_DANGER_LEVEL - ??? 5??????????? danger level ???????????? IP ?????????? 3?????????? nmap ?? 3?
- AUTO_BLOCK_TIMEOUT - ??? 3600??? IP ????

????

1. psad ??????
   ENABLE_AUTO_IDS = Y
   AUTO_IDS_DANGER_LEVEL = 3
2. ???? Linux ????????????????????
   #nmap -sT <psad's ip address>
3. psad ????????????????? IP???????????
   #psad --fw-list
4. IP ?????????? AUTO_BLOCK_TIMEOUT(??? 3600) ???????????????

FAQ

Q: ???? Local ??????

Ans: ?? /etc/psad/auto_dl

```
# Ignore local subnet
192.168.7.0/24  0;
# Ignore a host
192.168.8.10    0;
```

Q: ???? ping ?????

Ans: ??????? iptables ?????? ping ??????? iptables ???????????

/etc/sysconfig/iptables?

```
# Accept responses to our pings
-A INPUT -p icmp -m icmp --icmp-type echo-reply -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type echo-request -j ACCEPT
```

Q: ???????? IP???????

Ans: ??????

```
iptables -D PSAD_BLOCK_FORWARD -d 123.123.123.123 -j DROP
iptables -D PSAD_BLOCK_FORWARD -s 123.123.123.123 -j DROP
iptables -D PSAD_BLOCK_INPUT -s 123.123.123.123 -j DROP
iptables -D PSAD_BLOCK_OUTPUT -d 123.123.123.123 -j DROP
```

Q: ??? danger level

Ans: ?????????? IP ????????????????????????? psad.conf ???????????????????????????

```
DANGER_LEVEL1           5;    ### Number of packets.
DANGER_LEVEL2           15;
DANGER_LEVEL3           150;
DANGER_LEVEL4           1500;
DANGER_LEVEL5           10000;
```

???? auto_dl ??????????? IP ???????????

????

- [?????? Port Scan Attack Detector (psad)]
- [Meet the Anti-Nmap: PSAD (EnGarde Secure Linux)]