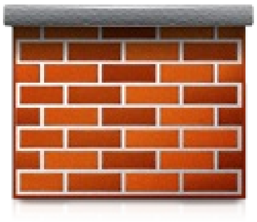
Table Of Contents

Home > Faq > CentOS

psad: Linux Detect And Block Port Scan Attacks In Real Time

Posted by Vivek Gite <vivek@nixcraft.com>



[1]

Q. How do I detect port scan attacks by analyzing Debian Linux firewall log files and block port scans in real time? How do I detect suspicious network traffic under Linux?

A. A port scanner (such as nmap) is a piece of software designed to search a network host for open ports. Cracker can use nmap to scan your network before starting attack. You can always see scan patterns by visiting /var/log/messages. But, I recommend the automated tool called psad - the port scan attack detector under Linux which is a collection of lightweight system daemons that run on Linux machines and analyze iptables log messages to detect port scans and other suspicious traffic.

psad makes use of Netfilter log messages to detect, alert, and (optionally) block port scans and other suspect traffic. For tcp scans psad analyzes tcp flags to determine the scan type (syn, fin, xmas, etc.) and corresponding command line options that could be supplied to nmap to generate such a scan. In addition, psad makes use of many tcp, udp, and icmp signatures contained within the Snort intrusion detection system.

Install psad under Debian / Ubuntu Linux

Type the following command to install psad, enter:

```
$ sudo apt-get update
$ sudo apt-get install psad
```

Configure psad

Open /etc/syslog.conf file, enter:

```
# vi /etc/syslog.conf
```

Append following code

```
kern.info       |/var/lib/psad/psadfifo
```

Alternatively, you can type the following command to update syslog.conf:

```
echo -e 'kern.info\t|/var/lib/psad/psadfifo' >> /etc/syslog.conf
```

psad Syslog needs to be configured to write all kern.info messages to a named pipe /var/lib/psad/psadfifo. Close and save the file. Restart syslog:

```
# /etc/init.d/sysklogd restart
# /etc/init.d/klogd
```

The default psad file is located at /etc/psad/psad.conf:

```
# vi /etc/psad/psad.conf
```

You need to setup correct email ID to get port scan detections messages and other settings as follows:

```
EMAIL_ADDRESSES             vivek@nixcraft.in;
```

Set machine hostname (FQDN):

```
HOSTNAME                    server.nixcraft.in;
```

If you have only one interface on box (such as colo web server or mail server), sent HOME_NET to none:

```
HOME_NET                NOT_USED;  ### only one interface on box
```

You may also need to adjust danger levels as per your setup. You can also define a set of ports to ignore, for example to have psad ignore udp ports 53 and 5000, use:

```
IGNORE_PORTS                udp/53, udp/5000;
```

You can also enable real time iptables blocking, by setting following two variables:

```
ENABLE_AUTO_IDS             Y;
IPTABLES_BLOCK_METHOD       Y;
```

psad has many more options, please read man pages for further information. Save and close the file. Restart psad:

```
# /etc/init.d/psad restart
```

Update iptables rules

psad need following two rules with logging enabled:

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

Here is my sample Debian Linux desktop firewall script with logging enabled at the end:

```
#!/bin/bash
IPT="/sbin/iptables"

echo "Starting IPv4 Wall..."
$IPT -F
$IPT -X
$IPT -t nat -F
$IPT -t nat -X
$IPT -t mangle -F
$IPT -t mangle -X
modprobe ip_conntrack

BADIPS=$(egrep -v -E "^#|^$" /root/scripts/blocked.fw)
PUB_IF="eth0"

#unlimited
$IPT -A INPUT -i lo -j ACCEPT
$IPT -A OUTPUT -o lo -j ACCEPT

# DROP all incomming traffic
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP

# block all bad ips
for ip in $BADIPS
do
    $IPT -A INPUT -s $ip -j DROP
    $IPT -A OUTPUT -d $ip -j DROP
done

# sync
$IPT -A INPUT -i ${PUB_IF} -p tcp ! --syn -m state --state NEW  -m limit --limit 5/m --limi

$IPT -A INPUT -i ${PUB_IF} -p tcp ! --syn -m state --state NEW -j DROP

# Fragments
$IPT -A INPUT -i ${PUB_IF} -f  -m limit --limit 5/m --limit-burst 7 -j LOG --log-level 4 --
$IPT -A INPUT -i ${PUB_IF} -f -j DROP
```

```
# block bad stuff
$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP
$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL ALL -j DROP

$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL NONE -m limit --limit 5/m --limit-burst
$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL NONE -j DROP # NULL packets

$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags SYN,FIN SYN,FIN -m limit --limit 5/m --limit
$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP #XMAS

$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags FIN,ACK FIN -m limit --limit 5/m --limit-bur
$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags FIN,ACK FIN -j DROP # FIN packet scans

$IPT  -A INPUT -i ${PUB_IF} -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP

# Allow full outgoing connection but no incomming stuff
$IPT -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A OUTPUT -o eth0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# allow ssh only
$IPT -A INPUT -p tcp --destination-port 22 -j ACCEPT
$IPT -A OUTPUT -p tcp --sport 22 -j ACCEPT

# allow incoming ICMP ping pong stuff
$IPT -A INPUT -p icmp --icmp-type 8 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
$IPT -A OUTPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# No smb/windows sharing packets - too much logging
$IPT -A INPUT -p tcp -i eth0 --dport 137:139 -j REJECT
$IPT -A INPUT -p udp -i eth0 --dport 137:139 -j REJECT

# Log everything else
# *** Required for psad ****
$IPT -A INPUT -j LOG
$IPT -A FORWARD -j LOG
$IPT -A INPUT -j DROP

# Start ipv6 firewall
# echo "Starting IPv6 Wall..."
/root/scripts/start6.fw

exit 0
```

How do I view port scan report?

Simply type the following command:

```
# psad -S
```

Sample output (some of the sensitive / personally identified parts have been removed):

```
[+] psadwatchd (pid: 2540)  %CPU: 0.0  %MEM: 0.0
    Running since: Sun Jul 27 07:14:56 2008

[+] kmsgsd (pid: 2528)  %CPU: 0.0  %MEM: 0.0
    Running since: Sun Jul 27 07:14:55 2008

[+] psad (pid: 2524)  %CPU: 0.0  %MEM: 0.8
    Running since: Sun Jul 27 07:14:55 2008
    Command line arguments: -c /etc/psad/psad.conf
    Alert email address(es): radhika.xyz@xxxxxxxx.co.in

    src:            dst:            chain:  intf:  tcp:  udp:  icmp:  dl:  alerts:  os_gues
    117.32.xxx.149  xx.22.zz.121    INPUT   eth0   1     0     0      2    2        -
    118.167.xxx.219 xx.22.zz.121    INPUT   eth0   1     0     0      2    2        -
    118.167.xxx.250 xx.22.zz.121    INPUT   eth0   1      0      0       2    2          -
    118.167.xxx.5   xx.22.zz.121    INPUT   eth0   1      0      0       2    2          -
    122.167.xx.11   xx.22.zz.121    INPUT   eth0   4642   0      0       4    50         -
    122.167.xx.80   xx.22.zz.121    INPUT   eth0   0      11     0       1    2          -
    123.134.xx.34   xx.22.zz.121    INPUT   eth0   20     0      0       2    9          -
    125.161.xx.3    xx.22.zz.121    INPUT   eth0   0      9      0       1    4          -
    125.67.xx.7     xx.22.zz.121    INPUT   eth0   1      0      0       2    2          -
    190.159.xxx.220 xx.22.zz.121    INPUT   eth0   0      9      0       1    3          -
    193.140.xxx.210 xx.22.zz.121    INPUT   eth0   0      10     0       1    2          -
    202.xx.23x.196  xx.22.zz.121    INPUT   eth0   0      13     0       1    10         -
    202.xx.2x8.197  xx.22.zz.121    INPUT   eth0   0      20     0       2    17         -
    202.97.xxx.198  xx.22.zz.121    INPUT   eth0   0      17     0       2    12         -
    202.97.xxx.199  xx.22.zz.121    INPUT   eth0   0      18     0       2    15         -
    202.97.xxx.200  xx.22.zz.121    INPUT   eth0   0      17     0       2    14         -
    202.97.xxx.201  xx.22.zz.121    INPUT   eth0   0      15     0       2    12         -
    202.97.xxx.202  xx.22.zz.121    INPUT   eth0   0      21     0       2    16         -
    203.xxx.128.65  xx.22.zz.121    INPUT   eth0   12     0      0       2    6          Windows
    211.90.xx.14    xx.22.zz.121    INPUT   eth0   1      0      0       2    2          -
    213.163.xxx.9   xx.22.zz.121    INPUT   eth0   0      0      1       2    2          -
    221.130.xxx.124 xx.22.zz.121    INPUT   eth0   0      35     0       2    31         -
    221.206.xxx.10  xx.22.zz.121    INPUT   eth0   0      33     0       2    21         -
    221.206.xxx.53  xx.22.zz.121    INPUT   eth0   0      33     0       2    27         -
    221.206.xxx.54  xx.22.zz.121    INPUT   eth0   0      39     0       2    26         -
    221.206.xxx.57  xx.22.zz.121    INPUT   eth0   0      33     0       2    19         -
    60.222.xxx.146  xx.22.zz.121    INPUT   eth0   0      40     0       2    33         -
    60.222.xxx.153  xx.22.zz.121    INPUT   eth0   0      14     0       1    11         -
    60.222.xxx.154  xx.22.zz.121    INPUT   eth0   0      18     0       2    15         -

    Netfilter prefix counters:
        "SPAM DROP Block": 161519
        "Drop Syn Attacks": 136

    Total scan sources: 95
    Total scan destinations: 1

    Total packet counters:
        tcp:  5868
        udp:  164012
        icmp: 2
```

How do I remove automatically blocked ips?

Simply type the following command to remove any auto-generated firewall block

```
# psad -F
```

How do I view detailed log for each IP address?

Go to /var/log/psad/ip.address/ directory. For example, view log for IP address 11.22.22.33, enter:

```
# cd /var/log/psad/11.22.22.33
# ls -l
```

Sample output:

```
-rw------- 1 root root 2623 2008-07-30 13:02 xx.22.zz.121_email_alert
-rw------- 1 root root   32 2008-07-30 13:02 xx.22.zz.121_packet_ctr
-rw------- 1 root root    0 2008-07-29 00:27 xx.22.zz.121_signatures
-rw------- 1 root root   11 2008-07-30 13:02 xx.22.zz.121_start_time
-rw------- 1 root root    2 2008-07-30 13:02 danger_level
-rw------- 1 root root    2 2008-07-30 13:02 email_count
-rw------- 1 root root 1798 2008-07-29 00:27 whois
```

Use cat / more or less command to view rest of the information.

Further readings:

- man pages - psad, syslog.conf
- psad project home page [2]
- I highly recommend - Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort [3] for further information.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/linux-detect-port-scan-attacks/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/iptables/**
[2] psad project home page: **http://cipherdyne.org/psad/**
[3] Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort: **http://www.amazon.com/gp/redirect.html?ie=UTF8&location=http%3A%2F%2Fwww.amazon.com%2FLinux-Firewalls-Detection-Response-iptables%2Fdp%2F1593271417%3Fie%3DUTF8%26s%3Dbooks%26qid%3D1218020190%26sr%3D8-1&tag=cyberciti-20&linkCode=ur2&camp=1789&creative=9325**