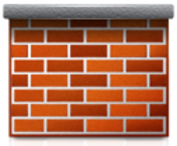
psad: Linux Detect And Block Port Scan Attacks In Real Time

Author: Vivek Gite • Last updated: August 6, 2008 • 34 comments



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 --limit-bu


$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 --log-
$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 7 -j
$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-bur
$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-burst 7
$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:  d
    117.32.xxx.149  xx.22.zz.121    INPUT   eth0   1     0     0      2
    118.167.xxx.219 xx.22.zz.121    INPUT   eth0   1     0     0      2
    118.167.xxx.250 xx.22.zz.121    INPUT   eth0   1     0     0      2
    118.167.xxx.5   xx.22.zz.121    INPUT   eth0   1     0     0      2
    122.167.xx.11   xx.22.zz.121    INPUT   eth0   4642  0     0      4
    122.167.xx.80   xx.22.zz.121    INPUT   eth0   0     11    0      1
    123.134.xx.34   xx.22.zz.121    INPUT   eth0   20    0     0      2
    125.161.xx.3    xx.22.zz.121    INPUT   eth0   0     9     0      1
    125.67.xx.7     xx.22.zz.121    INPUT   eth0   1     0     0      2
    190.159.xxx.220 xx.22.zz.121    INPUT   eth0   0     9     0      1
    193.140.xxx.210 xx.22.zz.121    INPUT   eth0   0     10    0      1
    202.xx.23x.196  xx.22.zz.121    INPUT   eth0   0     13    0      1
    202.xx.2x8.197  xx.22.zz.121    INPUT   eth0   0     20    0      2
    202.97.xxx.198  xx.22.zz.121    INPUT   eth0   0     17    0      2
    202.97.xxx.199  xx.22.zz.121    INPUT   eth0   0     18    0      2
    202.97.xxx.200  xx.22.zz.121    INPUT   eth0   0     17    0      2
    202.97.xxx.201  xx.22.zz.121    INPUT   eth0   0     15    0      2
    202.97.xxx.202  xx.22.zz.121    INPUT   eth0   0     21    0      2
    203.xxx.128.65  xx.22.zz.121    INPUT   eth0   12    0     0      2
    211.90.xx.14    xx.22.zz.121    INPUT   eth0   1     0     0      2
    213.163.xxx.9   xx.22.zz.121    INPUT   eth0   0     0     1      2
    221.130.xxx.124 xx.22.zz.121    INPUT   eth0   0     35    0      2
    221.206.xxx.10  xx.22.zz.121    INPUT   eth0   0     33    0      2
    221.206.xxx.53  xx.22.zz.121    INPUT   eth0   0     33    0      2
    221.206.xxx.54  xx.22.zz.121    INPUT   eth0   0     39    0      2
    221.206.xxx.57  xx.22.zz.121    INPUT   eth0   0     33    0      2
    60.222.xxx.146  xx.22.zz.121    INPUT   eth0   0     40    0      2
    60.222.xxx.153  xx.22.zz.121    INPUT   eth0   0     14    0      1
    60.222.xxx.154  xx.22.zz.121    INPUT   eth0   0     18    0      2

    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
- I highly recommend – Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort for further information.

🙁 Was this helpful? Please add your comment below ↓

🐧 Get the latest tutorials on Linux, Open Source & DevOps via

RSS feed ➔ Weekly email newsletter ➔

🔎 To search, type & hit enter...

Related Tutorials

How To Set Up PF Firewall on FreeBSD to Protect a Web Server

How to set up a UFW firewall on Ubuntu 16.04 LTS server

CentOS / RHEL: Install nmap Network Security Scanner

Linux Block Port With IPtables Command

How to block an IP address with ufw on Ubuntu Linux server

BSD PF Firewall Block FTP Bruteforce Attacks

Linux: Scan An Image With HP Scanners

Category	List of Unix and Linux commands
Download managers	wget

Category	List of Unix and Linux commands
Driver Management	Linux Nvidia driver • lsmod
Documentation	help • mandb • man • pinfo
Disk Management	df • duf • ncdu • pydf
File Management	cat • cp • less • mkdir • more • tree
Firewall	Alpine Awall • CentOS 8 • OpenSUSE • RHEL 8 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 20.04
Linux Desktop apps	GIMP • Skype • Spotify • VLC 3
Modern utilities	bat • exa
Network Utilities	NetHogs • dig • host • ip • nmap • ping
OpenVPN	CentOS 7 • CentOS 8 • Debian 10 • Debian 11 • Debian 8/9 • Ubuntu 18.04 • Ubuntu 20.04
Power Management	upower
Package Manager	apk • apt-get • apt • yum
Processes Management	bg • chroot • cron • disown • fg • glances • gtop • iotop • jobs • killall • kill • pidof • pstree • pwdx • time • vtop
Searching	ag • egrep • grep • whereis • which
Shell builtins	compgen • echo • printf
System Management	reboot • shutdown
Terminal/ssh	tty
Text processing	cut • rev
User Environment	exit • who
User Information	groups • id • lastcomm • last • lid/libuser-lid • logname • members • users • whoami • w
WireGuard VPN	Alpine • CentOS 8 • Debian 10 • Firewall • Ubuntu 20.04 • qrencode

34 comments… add one ↓

Diya • Aug 6, 2008 @ 14:28

I was not aware of psad. Thanks for writing out tutorial.

reply link

tachiiNiiJinx • Aug 7, 2008 @ 19:35

I append the following code (kern.info |/var/lib/psad/psadfifo) to /etc/syslog.conf. Which will save just fine, but I enter the following at the command line with or without sudo, echo -e ’kern.info\t|/var/lib/psad/psadfifo’ >> /etc/syslog.conf. I am getting am Permission Denied error. Do I need to use chmod to set the permission’s to the User, Group, or Other?

reply link

John Allen • Aug 13, 2008 @ 8:17

You must be the real root user for the >> to work.

When using sudo you will execute the echo command as root, but the >> redirect is executed as the current user.

reply link

somename • Nov 9, 2011 @ 5:57

that’s what `sudo su` is for :p

reply link

S0AndS0 • Jun 16, 2015 @ 23:23

I prefer using sudo tee with option ‘-a’ to append to files, it uses pipes ‘|’ instead of redirects ‘>’ or ‘>>’ and has an added bonus of displaying what was written.
echo “text to add” | sudo tee -a /file/path/file.ext
echo “text to fill” | sudo tee /file/path/new_file.ext
~ To keep variables from being expanded premeturly replace double quotes with single
echo ‘text to add’ | sudo tee -a /file/path/file.ext
echo ‘text to fill’ | sudo tee /file/path/new_file.ext
~ to be safe always use -a to append with tee; it’s kinda like the differance between ‘>’ and ‘>>’ one will over-write and the other will add.

reply link

Noah • Aug 18, 2008 @ 19:45

PSAD has been only an annoyance to me as an administrator. Often I use nmap to do perfectly legitimate scans of a clients machine for debugging purposes. I setup tools for automating data feeds between my servers and client servers. Data feeds can go over HTTP, SSH, various direct database sockets, FTP, etc. Often there are firewalls in the way or a client might not have a required service active and running or they might have configured a service on a non-standard port. I’m sure there are lots of other reasons that I can’t even remember now.

Clients that use PSAD hinder debugging. All of my servers are under constant automated attack by bots. This is simply the nature of the internet. None of these bots do port scanning. Some of them do scan a range of IP addresses looking for specific ports with running services, so I can see the value of a system could be to detect when someone may be scanning a range of IP address. But systems that detect port scans on an individual IP address seem overkill.

reply link

Ryan • Jan 6, 2009 @ 7:09

Nice howto. Thank you.

reply link

Asaduzzaman Shuvo • Feb 18, 2009 @ 7:59

How to observe deny web site Ip address or port in Linux Redhat squid server?

reply link

Linuxnoob • Mar 31, 2009 @ 16:07

Anyone know if I could some how run this in the firmware DD-WRT. Like in a SSH session? or can I just save thos IPtables to the firewall.

reply link

Munch • Jun 23, 2009 @ 12:41

What version of psad should I use for centOS?
Is installation procedure of psad for centOS same as above?

reply link

glas • Oct 22, 2009 @ 20:18

apt-get install Thank you very much.
Nice tutorial.

reply link

bonkhi • Nov 3, 2009 @ 10:15

Had no ideal of psad……………….. thanks

reply link

cybernet • Nov 16, 2009 @ 10:28

what i do with this ?
#!/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
……

reply link

deni • Dec 8, 2009 @ 14:05

any commands how to detect the ddos from where attacking my servers pls.?

reply link

tunmsk • Dec 22, 2009 @ 17:17

hi
do psad can be configured with rsyslog on a debian lenny?
thanks

reply link

Vlado • Mar 24, 2010 @ 18:04

One thing to have in mind is the huge hdd space required for psad. My /var/log/ grew up with around 1Gb for like 20mins!

reply link

Istvan C • Mar 27, 2015 @ 13:21

Use logrotate to shrink your logs

reply link

emcgfx • Jun 16, 2010 @ 10:25

This option bellow:
BADIPS=$(egrep -v -E "^#|^$" /home/tux/blocked.fw)

Needs to be this in Ubuntu 10.04:
BADIPS=$(egrep -v -e "^#|^$" /home/tux/blocked.fw)

NOTES: Simply use lower case "e" instead of capital one ;-)

Works like a charm, thanks CyberCiti Authors.

reply link

rokin • Jun 22, 2010 @ 20:58

Hello all, thank for the tuto.

But psad “don’t work” with Debian Lenny and rsyslog (default) :(
cf : http://www.mail-archive.com/debian-bugs-dist@lists.debian.org/msg794354.html
I have test modifications, after, psad launch good but the psadfifo are empty and no detections :(

sorry for my bad english.
can you have a solution or a similar software ?

thank you very much !

reply link

cviniciusm • Sep 3, 2010 @ 14:41

PSAD is broken on the Ubuntu 10.04 (Lucid Lynx) and on the new beta 10.10 (Maverick).

And nice job.

Cheers.

reply link

skullboxx • Sep 21, 2010 @ 13:19

Can’t confirm that, PSAD is working fine on my Ubuntu 10.04.1 LTS Box.

Cheers

reply link

sniper • Dec 10, 2010 @ 7:56

Hi all
How could I whitliste IPs? PSAD is everytime blocking my resolver in my network and the lo interface… :-(

Thanks

reply link

sniper • Dec 10, 2010 @ 19:31

Hi All
On Ubuntu Server 10.10 it works fine.
On Debian Lenny psad does not work. The counters be ever 0.
What could I do on the Debian Lenny Server, to become psad to work?
Thanks
sniper

reply link

Gargonzo Bastardo van Rothschildt • Jan 30, 2011 @ 0:50

This is a stupid configuration, because it will write Gigabytes of Data in your log directory – you will literally DOS yourself. Are you using this in real life anywhere? I assume, that you are not a sysadmin anymore then?
PSAD documentation explains that you should redirect the iptables info into the fifo file – and if your harddisk is filled up with iptables logs you will understand why.

reply link

Raul • Mar 12, 2011 @ 7:53

sniper psad on Debian Lenny works well.If your not, that's your mistake.You have to pay attention to configure psad.conf file.
Best regards,
Raul

reply link

cviniciusm • Mar 12, 2011 @ 12:55

Hello,

There is a bug on the 10.04 package, I filed a bug on Ubuntu Launchpad.

The original psad there is not the bug.

I solved the bug disabling the line that sends e-mail to dshield.org .

Regards.

reply link

Prakash • May 13, 2011 @ 4:13

Hello,

Please let me know the steps for installation of above for centos.

Awaiting for your reply.

Regards,
Prakash

reply link

Alex • Oct 9, 2011 @ 8:26

Thank you!
It works perfect!

reply link

Yonatan Ryabinski • Nov 15, 2011 @ 4:58

Thank you very much!

reply link

fix • Jan 3, 2012 @ 20:07

what kind of an asshole would want to block outgoing nmap scans???

reply link

joshlinx • Jan 14, 2012 @ 19:31

Note the authors other software as well excellent security software. fwsnort to use snort rules with firewall and fwknop for single packet authentication for port access. I have also bought the book and recommend reading it, very useful security software.

http://cipherdyne.org

reply link

sanchit • Jan 19, 2013 @ 19:56

Can you post a psad tutorial for centos?

reply link

Silvio • Mar 4, 2014 @ 20:58

Thanks for howto, on Gentoo run perfect. Only one problem is, the logfile will be full is there a way to limited?

reply link

Nix Craft • Mar 5, 2014 @ 6:03

Configure logrotate.

reply link

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name

Post Comment

Use HTML <pre>...</pre> for code samples. Your comment will appear only after approval by the site admin.

Next FAQ: Ubuntu Linux Install GDesklets GNOME Program

Previous FAQ: Linux bnx2: eth1: No interrupt was generated using MSI, switching to INTx mode

To search, type & hit enter...

FEATURED ARTICLES

1 30 Cool Open Source Software I Discovered in 2013

2 30 Handy Bash Shell Aliases For Linux / Unix / Mac OS X

3 Top 32 Nmap Command Examples For Linux Sys/Network Admins

4 25 PHP Security Best Practices For Linux Sys Admins

5 30 Linux System Monitoring Tools Every SysAdmin Should Know

6 40 Linux Server Hardening Security Tips

7 Linux: 25 Iptables Netfilter Firewall Examples For New SysAdmins

8 Top 20 OpenSSH Server Best Security Practices

9 Top 25 Nginx Web Server Best Security Practices

10 My 10 UNIX Command Line Mistakes

→ Linux shell scripting tutorial

→ RSS/Feed

→ About nixCraft