THE GEEK STUFF

Linux | DB | Open Source | Web

≡ Menu

- Home
- Free eBook
- Start Here
- Contact
- About

Snort: 5 Steps to Install and Configure Snort on Linux

by SathiyaMoorthy on August 6, 2010

Snort is a free lightweight network intrusion detection system for both UNIX and Windows.

In this article, let us review how to install snort from source, write rules, and perform basic testing.

1. Download and Extract Snort

Download the latest snort free version from snort website. Extract the snort source code to the /usr/src directory as shown below.

```
# cd /usr/src

# wget -O snort-2.8.6.1.tar.gz http://www.snort.org/downloads/116

# tar xvzf snort-2.8.6.1.tar.gz
```

Note: We also discussed earlier about Tripwire (Linux host based intrusion detection system) and Fail2ban (Intrusion prevention framework)

2. Install Snort

Before installing snort, make sure you have dev packages of libpcap and libpcre.

```
# apt-cache policy libpcap0.8-dev
libpcap0.8-dev:
  Installed: 1.0.0-2ubuntu1
  Candidate: 1.0.0-2ubuntu1

# apt-cache policy libpcre3-dev
libpcre3-dev:
  Installed: 7.8-3
  Candidate: 7.8-3
```

Follow the steps below to install snort.

```
# cd snort-2.8.6.1

# ./configure

# make

# make install
```

3. Verify the Snort Installation

Verify the installation as shown below.

```
# snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.8.6.1 (Build 39)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
           Copyright (C) 1998-2010 Sourcefire, Inc., et al.
           Using PCRE version: 7.8 2008-09-05
```

4. Create the required files and directory

You have to create the configuration file, rule file and the log directory.

Create the following directories:

```
# mkdir /etc/snort

# mkdir /etc/snort/rules

# mkdir /var/log/snort
```

Create the following snort.conf and icmp.rules files:

```
# cat /etc/snort/snort.conf
include /etc/snort/rules/icmp.rules

# cat /etc/snort/rules/icmp.rules
alert icmp any any -> any any (msg:"ICMP Packet"; sid:477; rev:3;)
```

The above basic rule does alerting when there is an ICMP packet (ping).

Following is the structure of the alert:

```
<Rule Actions> <Protocol> <Source IP Address> <Source Port> <Direction Operator> <Destination IP Address> <Destination > (rule options)
```

Table: Rule structure and example

Structure	Example
Rule Actions	alert
Protocol	icmp
Source IP Address	any
Source Port	any
Direction Operator	->
Destination IP Address	any
Destination Port	any
(rule options)	(msg:”ICMP Packet”; sid:477; rev:3;)

5. Execute snort

Execute snort from command line, as mentioned below.

```
# snort -c /etc/snort/snort.conf -l /var/log/snort/
```

Try pinging some IP from your machine, to check our ping rule. Following is the example of a snort alert for this ICMP rule.

```
# head /var/log/snort/alert
[**] [1:477:3] ICMP Packet [**]
[Priority: 0]
07/27-20:41:57.230345 > l/l len: 0 l/l type: 0x200 0:0:0:0:0:0
pkt type:0x4 proto: 0x800 len:0x64
209.85.231.102 -> 209.85.231.104 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:24905   Seq:1  ECHO
```

Alert Explanation
A couple of lines are added for each alert, which includes the following:

- Message is printed in the first line.
- Source IP
- Destination IP
- Type of packet, and header information.

If you have a different interface for the network connection, then use -dev -i option. In this example my network interface is ppp0.

```
# snort -dev -i ppp0 -c /etc/snort/snort.conf -l /var/log/snort/
```

Execute snort as Daemon

Add -D option to run snort as a daemon.

```
# snort -D -c /etc/snort/snort.conf -l /var/log/snort/
```

Additional Snort information

- Default config file will be available at **snort-2.8.6.1/etc/snort.conf**
- Default rules can be downloaded from: http://www.snort.org/snort-rules

G+1 3 Like 36 > Add your comment

If you enjoyed this article, you might also like..

1. 50 Linux Sysadmin Tutorials
2. 50 Most Frequently Used Linux Commands (With Examples)
3. Top 25 Best Linux Performance Monitoring and Debugging Tools

- Awk Introduction – 7 Awk Print Examples
- Advanced Sed Substitution Examples
- 8 Essential Vim Editor Navigation Fundamentals
- 25 Most Frequently Used Linux IPTables Rules Examples

4. Mommy, I found it! – 15 Practical Linux Find Command Examples
5. Linux 101 Hacks 2nd Edition eBook Free

- Turbocharge PuTTY with 12 Powerful Add-Ons

Tagged as: Snort Examples, Snort for Windows, Snort Ubuntu

{ 18 comments… add one }

- Diptanu paul August 6, 2010, 3:58 am

  good tutorial for keeping a track of the foreign activities on internet facing systems.
  Thanks reamsh.I will definately give it a try to understand that

  Link
- Catalin Festila August 6, 2010, 4:23 am

  snort -dev -i ppp0 -c /etc/snort/snort.conf -l /var/log/snort/
  and error is :
  ERROR: Unable to open rules file "/etc/snort//etc/snort/rules/local.rules": No such file or directory.
  Distro i use Fedora 13 .

  Link
- Adam Gonnerman August 6, 2010, 6:28 am

  In the first step you have us download the compressed file, then navigate to another directory to open. Shouldn't you have us move the file to the other directory first? Either way it doesn't work. If I try to unpack the compressed file from the usr/src directory it isn't found (because we didn't move it), and if I move the file to that directory and try it, I get a series of fails at unpacking.

  A little help?

  Link
- karthik August 6, 2010, 8:26 am

  Can I use snort to monitor my webapp's logs like Python / Java ??

  Link
- Kevin August 6, 2010, 11:37 pm

  karthik, you can use OSSEC (http://www.ossec.net) to monitor web server logs

  Link
- Francesco Talamona August 7, 2010, 2:46 am

  To Catalin:

  First of all create your /etc/snort/rules/icmp.rules
  Then modify /etc/snort/snort.conf in the following way:

  # cat /etc/snort/snort.conf
  include rules/icmp.rules

  Link
- Jaydeep October 11, 2010, 5:44 am

  I think here is a more better solution and it works grt…!

  Link

- elle October 8, 2013, 4:41 am

  why command snort not found after installing snort…???
  i have been trying for so many days and the when i type snort –version its says command snort not found… please help me to resolve this

  Link
- Sagar December 11, 2013, 2:47 am

  Aritcle is very nice.

  However can you please also tell me how do i set snort to send alert to external mail id.

  Link
- niry February 4, 2014, 7:43 am

  when I run snort there is error like this:
  “Unable to open rules file: /etc/snort/../rules/local.rules ”
  can you help me?
  thanks!

  Link
- Lampk April 3, 2014, 3:06 am

  Thanks, this tutorial is still working for the newest snort version 2.9.6.0

  Link
- Lauwko June 19, 2014, 2:25 am

  Thank you very much for the easy installation tutorial.
  Had one or two bumps (installing it on ubuntu server 12.04)
  I had to install the following packets:
  flex, bison and daq(can be found on snort webpage),
  Flex and bison could be installed using apt-get install.
  Cheers.

  Link
- vishnu December 12, 2014, 12:24 pm

  If we add snort as demon, snort will startup automatically when the pc is on. right? If so how can i remove from starup demon?

  Link
- muhammad March 10, 2015, 11:51 am

  Hi Everyone,
  i am having difficulty with snort installation. snort installation keeps giving me same error again and again for different versions of snort.

  Error
  ERROR! daq_static library not found, go get it from

  can anyone help to figure out the issue ?
  i would be grateful for the help.
  thanks

  Link
- lahiru July 6, 2015, 4:25 pm

  thanks, i installed snort and added the rule. But when i try to ping another machine i dont get any alert. any idea why ?

  Link
- levy November 11, 2015, 1:14 am

  can anyone help me to configure snort at the first time because am using opensuse12 ,so when i tried to install snort there is a message that asking me to put dependances first of all,can someone plz help this?

  Link
- ghanmi houda March 27, 2016, 5:18 am

  when i tape this commande snort -c /etc/snort/snort.conf -l /var/log/snort/ poster this commenter Commencing

packet processing (pid=3220)
What is the problem

Link

- Christopher Jackson April 14, 2016, 6:44 pm

  Just a Question
  I know this may sound stupid, however is there any advantage to using snort over just an IPTABLES rule if all you're doing is logging the activity? Does snort offer any other notification capabilities, such as e-mail or storing alerts in a database?

  Link

Leave a Comment

Name

Email

Website

Comment

Submit

□ Notify me of followup comments via e-mail

Next post: RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams

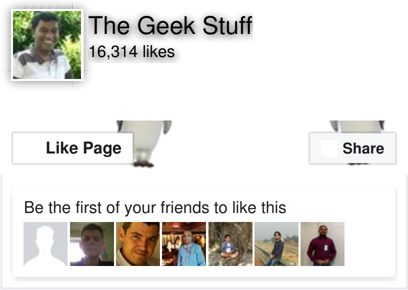
Previous post: How to Register RHEL/OEL Linux to Oracle Support (ULN) using up2date

RSS | Email | Twitter | Facebook | Google+

Search

EBOOKS

- Free Linux 101 Hacks 2nd Edition eBook - Practical Examples to Build a Strong Foundation in Linux
- Bash 101 Hacks eBook - Take Control of Your Bash Command Line and Shell Scripting
- Sed and Awk 101 Hacks eBook - Enhance Your UNIX / Linux Life with Sed and Awk
- Vim 101 Hacks eBook - Practical Examples for Becoming Fast and Productive in Vim Editor
- Nagios Core 3 eBook - Monitor Everything, Be Proactive, and Sleep Well



The Geek Stuff

16,314 likes

Be the first of your friends to like this

POPULAR POSTS

- 12 Amazing and Essential Linux Books To Enrich Your Brain and Library
- 50 UNIX / Linux Sysadmin Tutorials
- 50 Most Frequently Used UNIX / Linux Commands (With Examples)
- How To Be Productive and Get Things Done Using GTD
- 30 Things To Do When you are Bored and have a Computer
- Linux Directory Structure (File System Structure) Explained with Examples
- Linux Crontab: 15 Awesome Cron Job Examples
- Get a Grip on the Grep! – 15 Practical Grep Command Examples
- Unix LS Command: 15 Practical Examples
- 15 Examples To Master Linux Command Line History
- Top 10 Open Source Bug Tracking System
- Vi and Vim Macro Tutorial: How To Record and Play
- Mommy, I found it! -- 15 Practical Linux Find Command Examples
- 15 Awesome Gmail Tips and Tricks
- 15 Awesome Google Search Tips and Tricks
- RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams
- Can You Top This? 15 Practical Linux Top Command Examples
- Top 5 Best System Monitoring Tools
- Top 5 Best Linux OS Distributions
- How To Monitor Remote Linux Host using Nagios 3.0
- Awk Introduction Tutorial – 7 Awk Print Examples
- How to Backup Linux? 15 rsync Command Examples
- The Ultimate Wget Download Guide With 15 Awesome Examples
- Top 5 Best Linux Text Editors
- Packet Analyzer: 15 TCPDUMP Command Examples
- The Ultimate Bash Array Tutorial with 15 Examples
- 3 Steps to Perform SSH Login Without Password Using ssh-keygen & ssh-copy-id
- Unix Sed Tutorial: Advanced Sed Substitution Examples
- UNIX / Linux: 10 Netstat Command Examples
- The Ultimate Guide for Creating Strong Passwords

- 6 Steps to Secure Your Home Wireless Network
- Turbocharge PuTTY with 12 Powerful Add-Ons

CATEGORIES

- Linux Tutorials
- Vim Editor
- Sed Scripting
- Awk Scripting
- Bash Shell Scripting
- Nagios Monitoring
- OpenSSH
- IPTables Firewall
- Apache Web Server
- MySQL Database
- Perl Programming
- Google Tutorials
- Ubuntu Tutorials
- PostgreSQL DB
- Hello World Examples
- C Programming
- C++ Programming
- DELL Server Tutorials
- Oracle Database
- VMware Tutorials

Ramesh Natarajan

G+ Follow

About The Geek Stuff

My name is **Ramesh Natarajan**. I will be posting instruction guides, how-to, troubleshooting tips and tricks on Linux, database, hardware, security and web. My focus is to write articles that will either teach you or help you resolve a problem. Read more about Ramesh Natarajan and the blog.

Contact Us

Email Me : Use this Contact Form to get in touch me with your comments, questions or suggestions about this site. You can also simply drop me a line to say hello!.

Follow us on Google+

Follow us on Twitter

Become a fan on Facebook

Support Us

Support this blog by purchasing one of my ebooks.

Bash 101 Hacks eBook

Sed and Awk 101 Hacks eBook

Vim 101 Hacks eBook

Nagios Core 3 eBook