www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

Snort installation

Snort is used for performing security checks on network boundaries. This can be done on the outside Untrust network but is sometimes more useful to look at what's getting thru your firewall into the web servers.

We will be installing Snort 2.7.0 on a Redhat 6 box. First, you need a compiler.

- yum install gcc

Redhat doesn't have a number of libraries needed by Snort so you need to add these before installing the main snort application.

Install flex – needed by libpcap

- Yum install flex

Install yacc (bison) – needed by libpcap

- Yum install bison

Install libpcap

- wget http://www.tcpdump.org/release/libpcap-1.3.0.tar.gz
- tar –xzf libpcap-1.3.0.tar.gz
- cd libpcap
- ./configure
- Make
- Make install

Once there, download yum and do a configuration check:

- cd /tmp/
- tar –xzf snort-2.7.0.1.tar.gz
- cd /tmp/snort-2.7.0.1
- ./configure

You'll need to download rules and setup automatic updates of the rules. They provide a perl script to do this. All that's needed is a login account with snort to complete and pulled pork:

http://code.google.com/p/pulledpork/

www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

- Wget http://pulledpork.googlecode.com/files/pulledpork-0.6.1.tar.gz
- Tar –xzf pulledpork-0.6.1.tar.gz
- Cd pulledpork-0.6.1
- ./configure
- Make
- Make install

Once installed successfully, be sure to update the pulledpork.conf file with your user/password. Running is as simple as:

/usr/local/bin/pulledpork.pl -c /usr/local/etc/pulledpork.conf

Here's an example update:

http://code.google.com/p/pulledpork/

```
      _____ ____
     `----,\    )
      `--==\\  /    PulledPork v0.6.1 the Smoking Pig <////~
       `--==\\/
     .-~~~~-.Y|\\_  Copyright (C) 2009-2011 JJ Cummings
  @_/        /  66\_  cummingsj@gmail.com
    |    \   \   _(")
     \   /-| ||'--'  Rules give me wings!
      \_\  \_\\
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Checking latest MD5 for snortrules-snapshot-2910.tar.gz....
     They Match
     Done!
Prepping rules from snortrules-snapshot-2910.tar.gz for work....
     Done!
Checking latest MD5 for opensource.gz....
     They Match
     Done!
Prepping rules from opensource.gz for work....
     Done!
Checking latest MD5 for emerging.rules.tar.gz....
     No Match
     Done
Rules tarball download of emerging.rules.tar.gz....
     They Match
     Done!
```

www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

```
 Prepping rules from emerging.rules.tar.gz for work....
      Done!
 Reading rules...
 Reading rules...
 Reading rules...
 Setting Flowbit State....
      Enabled 262 flowbits
      Enabled 23 flowbits
      Done
 Writing /usr/local/etc/snort/rules/snort.rules....
      Done
 Writing /usr/local/etc/snort/rules/so_rules.rules....
      Done
 Generating sid-msg.map....
      Done
 Writing /usr/local/etc/snort/sid-msg.map....
      Done
 Writing /var/log/sid_changes.log....
      Done
 Rule Stats....
      New:-------11
      Deleted:---0
      Enabled Rules:----18875
      Dropped Rules:----0
      Disabled Rules:---8041
      Total Rules:------26916
      Done
 Please review /var/log/sid_changes.log for additional details  Fly Piggy
Fly!
```