Build Securely a Shadow/Snort Sensor Step-by-Step Powered by Slackware Linux

By Guy Bruneau, GSEC, GCIA, GCUX
Version 5.1 – 26 April 2005

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Introduction

This configuration process is used to deploy Shadow/Snort sensors powered by the Slackware Linux (GNU) operating system. This setup was developed for sensors using IDE or SCSI drives. The full installation using this setup is ~225 MB in size and provides no remote services except through Secure Shell and Webmin for remote management. The Snort sensor logs are process via **Barnyard** backend processing.

This process doesn't address how to setup a Shadow Analysis station. More information available at: http://www.nswc.navy.mil/ISSEC/CID/

This installation contains three separate and ready to used Sguil packages that contains all the necessary files to install the Sguil as a sensor only, database only or all the components on the same systems. Sguil contains some very useful analysis function such as the Security Analyst Network Connection Profiler (sancp) that collects network traffic statistical information, has a script to log all the packets, uses tcpflow and p0f to get TCP session transcripts and can call Ethereal for in-depth packet analysis.

There are three packages on the CD: in the sguil directory you have a package to run all in one (database server and client), the sguildb for a central database installation only and the sensguil only contains the sensor software to report to a central database. The is a sguil.pdf document that explain how to setup Sguil and the Sguil client on a Windows workstation. Additional information including console snapshots can be viewed at: http://sguil.sourceforge.net.

This installation has a web management tool called Webmin used to securely manage a MySQL and Snort via a web browser through SSL and has its own web server built-in. Additional information about Webmin is available at: http://www.webmin.com/. In addition, a Snort plugin by MSB Networks (http://msbnetworks.net/snort/) has been adapted and included in Webmin to fully manage the Snort sensor (config file, plugins, ruleset, etc) to ease remote management of the sensor. See the Webmin section to correctly configure this package.

For those who would prefer using ACID instead of Sguil as their management console, the rel_note section contains the instructions to build a complete Linux Apache/ACID/Mysql database on a separate server to process the events from several sensors. Mark Rupright also supplied a Windows equivalent for those who prefer using a Windows console.

This setup includes both Shadow and Snort IDS sensor as well as Network Grep (Ngrep) as an additional tool to be combined with Shadow or use in standalone mode for those who want additional analysis flexibility with this multipurpose platform. **This package is built for a sensor that contains 2 NIC cards** (eth0 = control and eth1 = Shadow, Snort or Ngrep).

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Important: If you decide to install Sguil (sensor, database or both), Shadow will be automatically disabled and will not be collecting anything because Sguil will then do the collection.

In order to make Snort signature updates more flexible, I have included the oinkmaster script written by Andreas Östling available at http://www.algonet.se/~nitzer/oinkmaster/ .

The Snort sensor includes the Bleeding Edge Malware rules also updated daily via Oinkmaster. The rules are available at: http://www.bleedingsnort.com/

The Shadow/Snort ISO image powered by the Slackware Linux OS can be downloaded at: http://www.whitehats.ca/downloads/ids/shadow-slack/shadow.iso

The MD5 signature for the ISO image is available at:
http://www.whitehats.ca/downloads/ids/shadow-slack/shadow.md5

I invite you to read the release notes on the CD, which contains additional information not contained in this document. There is a document called stunnel.pdf which explains how to setup encryption between the sensor(s) and the database server.

Important: Before you start, make sure you are disconnected from the network until the sensor has been securely configured.

Partitioning the drive (example):

Drive partitioning can be done in multiple ways. This is an example that can be used if you have two drives and you are installing the database and the server on the same system:

Database and Sensor

Drive One		
/	Minimum of 512 MB	
swap	Minimum of 512 MB	
/var	Minimum of 25 MB	
/usr/local	Remainder of drive	(Contains MySQL DB and Snort)
Drive Two		
/LOG	Whole drive	(Contains the tcpdump Sguil logs)

- Boot on the system using the Slackware CD-ROM.

To partition the drive, login as root and run ***cfdisk /dev/hda*** (IDE drive), ***cfdisk /dev/sda*** (SCSI drive) or ***cfdisk /dev/cciss/c0d0*** (Raid drive). If this isn't a new drive, delete the old partitions before starting.

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

- hda1: / = 750 MB (Select new, select primary, size is 750, beginning, bootable)
- hda2: SWAP = 512 MB or same amount as the RAM (Select Pri/Log Free Space, new, primary, size is 512, beginning)
- Change hda2 to swap by selecting *type 82*
- hda3 (Select Pri/Log Free Space, new, primary, remainder of disk if you are going to only setup a Shadow sensor. *Otherwise, reserve at a minimum 500 MB for Snort for the hda4 partition*)
- *hda4 (Select Pri/Log Free Space, new, primary, remainder of disk for Snort)*
- Select Write to save the new settings to disk
- Select *Quit* to exit

Install the Software

Now that you have partitioned the drive, and saved your setting, you are ready to setup the Operating System.

- Run setup
- Select addswap
- Continue with installation: yes
- Select Linux installation partition
    - /dev/hda1 (format, reiserfs - default)
    - /dev/hda3 (format, reiserfs - default)
- Select mount point for /dev/hda3: /LOG → **Needed if using Shadow or Sguil**
- /dev/hda4 (format, reiserfs - default) → **Optional if using Snort**
- Select mount point for dev/hda4: /usr/local → **Needed if using Snort/MySQL**
    - Select add none and continue with setup
- Select *continue* to go to the SOURCE section
- Select *1* to install from a Slackware CD-ROM
- Select *auto* to scan automatically for the CD-ROM
- Make sure the CD is in the CD-ROM drive and select OK
- Select *Yes* on continue

- Install Shadow/Snort installation CD which only shows 5 packages:

A, AP, D, N, TCL

- Select *OK* to continue and go to the *INSTALL* section
- Select install everything (full)
- Install a Linux kernel from the CD-Rom
- Select default kernel
- Select *bare.i* if using IDE or *scsi.*or other SCSI depending of your drive or *raid.s* for RAID drive.
- Make a boot disk for recovery (LILO)
- After the boot disk, choose continue with the configuration
- Skip modem configuration (*no modem*)

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

- Install LILO and select expert
    - Select Begin, at the blank prompt press enter, select *standard*, install to *MBR* confirm location to install lilo (select default @/dev/hda, /dev/sda or /dev/cciss/c0d0) and none
    - Add Linux and choose the root partition (i.e. /dev/hda1, /dev/sda1 or /dev/ccisss/c0d0p1)
    - Use *Linux* as a partition name
    - Install LILO
- Configure the network with your settings
- Probe the network card
- When the network card has been probed, it will ask if the settings are correct
- Setup the hardware clock
- Setup the root password
- Exit setup
- Reboot (reboot at the prompt)
- Manually eject the CD-ROM
- Log back into the sensor as root
- Delete residual mail *rm /var/spool/mail/root*

TCP Wrapper - SSH

Configure SSH TCP Wrappers in the following way:

- vi /etc/hosts.allow
- Add in the TCP Wrappers file which host(s) are allowed to connect to the sensor

```
sshd: 192.168.3. \
      192.168.2.6 \
      .site.ca
```

- The /etc/hosts.deny has been configured to deny ALL (ALL: ALL) by default

IPTables Firewall

Configure iptables firewall (rc.firewall)

Note: You need a firewall (iptables) to allow the sensor to be as invisible as possible. You can use the firewall supplied with this installation or create your own.

O- Configured the firewall located in */etc/rc.d* directory or create your own
O- Edit the firewall scrip and change to variable according to your site
O- *chmod 755 /etc/rc.d/rc.firewall* to enable the firewall
O- To start the firewall now do: */etc/rc.d/rc.firewall* at the prompt
O- Check the firewall policy with the following command: iptables -L
O- The firewall will start upon the next reboot

Setting up the NICs if Undetected During the Installation

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Note: A list of the NIC kernel modules is in the /etc/rc.d/rc.modules file. I recommend using an Intel PCI card for the Shadow/Snort packet collection. If the NIC card detection setup fail, the card can be manually added to this script. The cards will be loaded in the order they are listed in this configuration file.

Setting up NIC modules (example)

If the sensor is using two different NIC, it will only detect the first one it sees and you will need to add the NIC module for the second one to the rc.netdevice file. You can look into the /etc/rc.d/rc.modules file for the NIC module and test it at the command line to see if it loads as follow:

```
modprobe eepro1000
dmesg
```

After dmesg displays its output, you should see the card loaded at the end of the dmesg output. If it loaded correctly, then add it to the rc.netdevice file to ensure it loads when the sensor or server reboots. You should have two module listed then. The order they are listed is the order they will load.

```
vi /etc/rc.d/rc.netdevice
# RealTek 8129/8139 to communicate with the Management station (eth0)
/sbin/modprobe rtl8139oo

# Intel EtherExpress Pro/100 PCI support used to collect packets (eth1):
/sbin/modprobe eepro100
```


Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Webmin Configuration

Webmin is a secure remote sensor and console manager. For example, the IDS can be remotely managed via an SSL browser to manage MySQL, Sguil, the logs, the entire Snort IDS including its plugins, the rules, the configuration files, etc. It is quite versatile and very easy to use for those who prefer using a GUI to manage the sensor.

After you log in Webmin, to manage the Snort sensor selects the **Servers** icon. You then are going to see Snort IDS Admin eth1 to eth4. The eth1 and eth2 are the only two-interface preconfigured in Webmin.

Configuring Webmin

You need to change the default account password before making this system operational. The default account is **admin** and the default password is **admin**. Change the default admin account password the following manner. At the sensor command line console do:

/usr/local/webmin/changepass.pl /etc/webmin admin newpassword

The Webmin service can be started and stopped this way:

/etc/webmin/start
/etc/webmin/stop

Access is via SSL this way:

https://yourIPaddress:10000

A FAQ is available on the Webmin site at:

http://www.webmin.com/faq.html

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Snort IDS configuration

Snort Version 2.3.3 (Build 14)
1 May 2005

If you are going to enable the firewall on the sensor, don't forget to add the IP of the Sguil database in the rc.firewall script if the sensor is going to be sending the events to a remote database.

Note about Sguil: You can install any of the 3 packages (sguil, sguildb and sensguil) available on the CD which has been expressly built to run on this sensor. Check the document called **sguil.pdf** in the rel_note on how to configure each of the packages. Snort is configured to automatically use Barnyard through its output log_unified function.

This Snort binary has been pre-built with the following options:

--with-mysql	Support for MySQL
--enable-smbalerts	SMB alerting capability via Samba
--enable-sourcefire	Enable Sourcefire specific build options
--enable-flexresp2	Flexible response on hostile connection attempts
--enable-perfmonitor	Enable perfmonitor preprocessor
--enable-linux-smp-stats	Enable statistics reporting through proc

Both Sguil patches have been applied to Snort to support the Sguil database.

To uninstall Snort on the IDS platform do:

- Run pkgtool and select remove packages from other directories
- Select Snort to remove the package

The necessary files have been installed into the /usr/local/snort directory. This version contains the latest signature libraries from http://www.snort.org as of the above date.

The Snort binary is compiled with the "-static" option and the sensor runs in a charrooted jail by default in the /usr/local/snort. Thanks to GJ Hagenaars' contribution, the Snort sensor is now controlled by a startup script located in /etc/rc.d/rc.snort.

Snort configuration files for multiple interfaces are located in /usr/local/snort/etc and each interfaces has a snort.internal.conf or snort.external.conf. Edit each of these files to reflect your settings.

Snort configuration files for multiple interfaces are located in /usr/local/snort/etc and each interface should be listed in snort.internal.nic and snort.external.nic. The eth2 interface is configured by default to snort.internal.nic. Edit each of these files to reflect your settings.

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

- The Snort unified logs are saved in /usr/local/snort/log/eth(1-5). Default installation will contain eth0 and eth1 directory.
- Test the configuration by running the ./**check_snort_eth1** and **check_snort_eth2** script. If the this is successful, start the sensor
- **/etc/rc.d/rc.snort start** script to starts the sensor

Important Snort pass Rule Order

By default, the sensor will not process any pass rules. In order for the sensor to correctly process pass rules, you must add the **–o** switch in the /etc/rc.d/rc.snort script to change the rule order from Alert, Log, Pass to **Pass, Alert, Log**. Be very careful that your pass rules will not disable other rules in the ruleset.

Example

```
$SNORTBIN/snort \
                    -d \
                    -o \
                    -I \
                    -g snort \
                    -u snort \
                    -i $NIC \
                    -c $SNORTETC/snort.${POLICY}.conf \
                    -l $SNORTLOG/$NIC \
                    -D
```


Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Configuring Barnyard to send to Sguil database

Barnyard Version 0.2.0 (Build 32)
15 September 2004

Barnyard unified logging output processor is used with this system to process all the data from the Snort sensor. The default scripts are setup to process the unified logs to binary logs format and can also be configured to process MySQL database logging as well as syslog. In order to use Barnyard with MySQL, you must configure the output process as per the instructions below.

This Barnyard binary has been pre-built with the following options:

--with-mysql Support for MySQL
--with-mysql-includes
--with-mysql-libraries

The Snort output processor is enable with **log_unified** filename snort.log, limit 128 in the **snort.external.conf** and **snort.internal.conf** (only if you are monitoring this interface) to log to the /usr/local/snort/log/eth* directory.

Before proceeding with this step, make sure you have setup your Snort database account, which is part of the previous section in "Setting up the database and its users". Configure Barnyard to forward data from a sensor to the Sguil database in the following manner:

vi /usr/local/barnyard/etc/barnyard.eth1.conf (External interface)
vi /usr/local/barnyard/etc/barnyard.eth2.conf (Internal interface)

```
# set the hostname (used for the sguil db output plugin)
config hostname: shadow

# Converts data from the dp_log plugin into standard pcap format
# Argument: <filename>

output log_pcap
```

Insert Data into Sguil Database

```
# Use this configuration if using Sguil

output sguil: mysql, sensor_id 0, database sguildb, server 127.0.0.1, user sguil, \
password password, sguild_host 127.0.0.1, sguild_port 7736
```

Note: If your server is something other than **127.0.0.1**, change it accordingly.

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

- Save the file and restart Barnyard

/etc/rc.d/rc.barnyard restart
- Ensure the Barnyard processes are running

ps –aef |grep barnyard

Local sid Rule Mapping

Note: If you are going to create some local rules (i.e. local-eth1.rules) you MUST include the SID and the SID name in the /usr/local/snort/rules/local-sid.map and can be done via Webmin. These must match the information put in the rule file as follow:

9001 || Local task rule
9002 || TCP connections to TCP 3127

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

New procedures for Snort Oinkmaster Updates

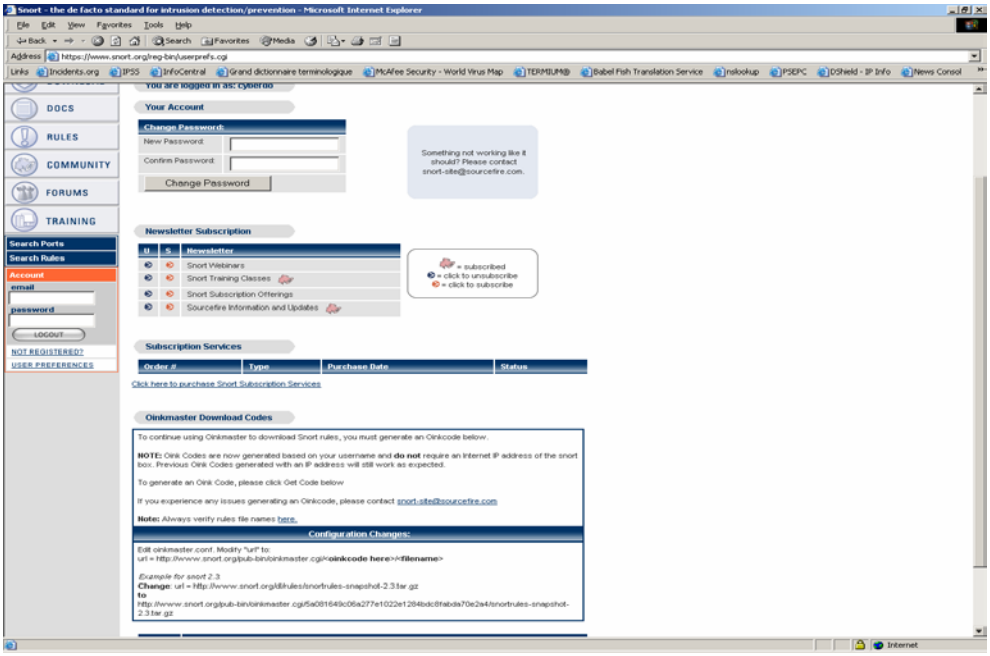
Oinkmaster

You should read the FAQ on how to configure oinkmaster to download the signature updates. http://oinkmaster.sourceforge.net/

Register with Snort to get an account

https://www.snort.org/pub-bin/register.cgi

You will receive your account information via e-mail
Login the site as per e-mail and password
Change your password if you want
In order for Oinkmaster to download the updated rules, you must generate a site string using the Get Code at the bottom of the page



Copyright © Guy Bruneau, 2001-2005. All rights reserved.

As per the instructions at the bottom of the page, copy the new download path with your sting in it into oinkmaster.conf

Old path:

url = http://www.snort.org/dl/rules/snortrules-snapshot-2.3.tar.gz

New path (code is invalid, it is just an example):

url = http://www.snort.org/pub-bin/oinkmaster.cgi/**5a081649c06a277e1022e1284bdc8fabda70e2a4**/snortrules-snapshot-2.3.tar.gz

- The bold portion is where your code goes.
- The file is located at: /usr/local/snort
- The oinkmaster.conf file can be updated using vi or with Webmin
- If using Webmin, goto Servers, Snort IDS Admin eth1, select Oink
- Find url = http://www.snort.org/dl/rules/snortrules-snapshot-2.3.tar.gz

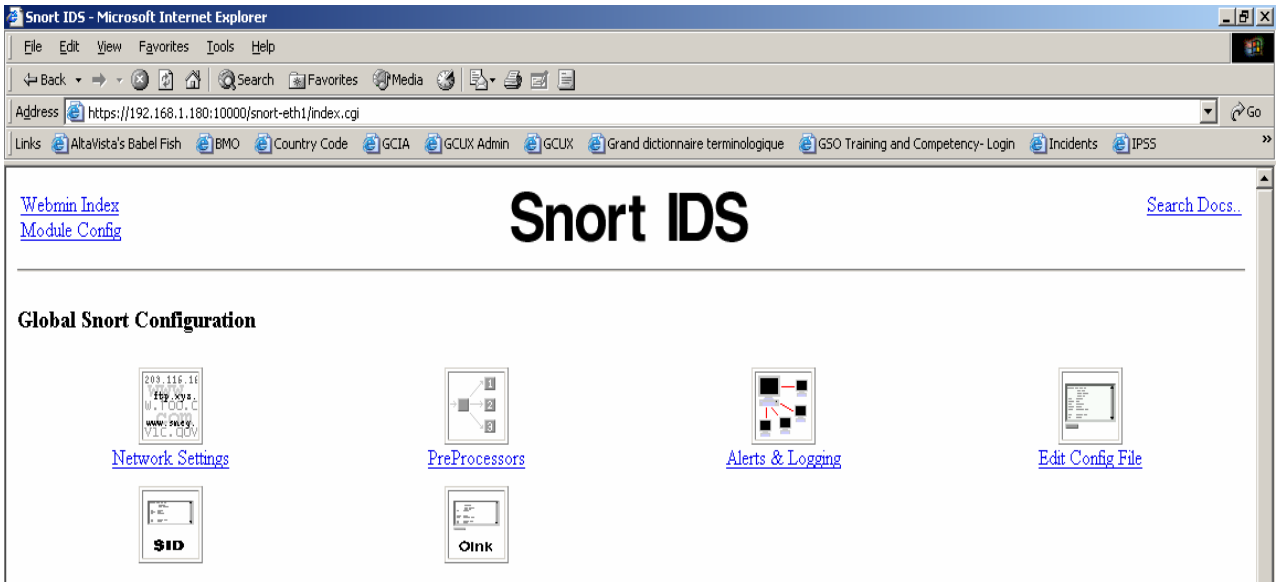
Change it to:

url = http://www.snort.org/pub-bin/oinkmaster.cgi/**INSERT YOUR ACCOUNT HERE**/snortrules-snapshot-2.3.tar.gz

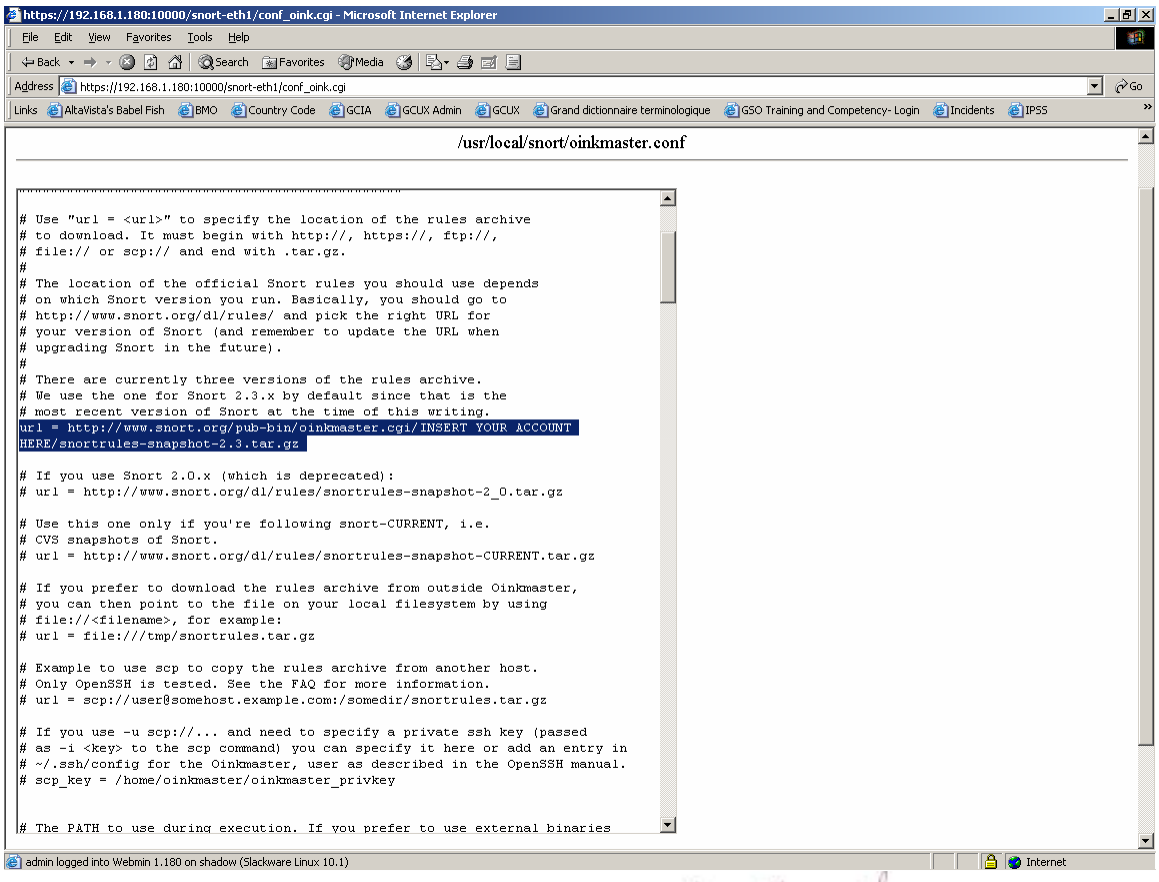
Webmin screenshots below

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Snort IDS Main Screen



Edit Oink



Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Shadow/Snort with Sguil Files and Scripts

/etc/rc.d	All system start/stop scripts
/etc/rc.d/rc.K	Kill all system script
/etc/rc.d/rc.S	Start up script for single-user mode
/etc/rc.d/rc.M	Start up script for multi-user mode
/etc/rc.d/rc.snort	Snort start/stop script
/etc/rc.d/rc.barnyard	Barnyard start/stop script
/etc/rc.d/rc.sguild	Sguil database start/stop script
/etc/rc.d/sancpd_eth1	sancp start/stop script for eth1
/etc/rc.d/sensoragent_eth1	Sensor Agent start/stop script to connect to database
/etc/rc.d/rc.mysqld	MySQL database script
/etc/rc.d/rc.netdevice	NIC module loading script
/etc/rc.d/rc.local	Script for all other configuration
/etc/issue	Banner message
/etc/motd	Banner message
/etc/rc.d/rc.firewall	Setup firewall
/var/adm/messages	General log file
/var/adm/syslog	Syslog file
/var/run	Various server pid files
/usr/local/snort	Snort directory files
/usr/local/snort/etc	Snort configuration scripts
/usr/local/snort/rules	Snort rules
/usr/local/snort/log	Snort log directory
/usr/local/snort/bin	Snort sensor binary
/usr/local/barnyard	Barnyard directory files (including Barnyard lock file)
/usr/local/barnyard/etc	Barnyard configuration scripts
/usr/local/barnyard/log	Barnyard log directory
/usr/local/barnyard/bin	Barnyard binary
/etc/sguild	Sguil configuration scripts
/etc/sguild/archive_sguildb.tcl	Archive/purge Sguil database script
/usr/local/sguil/bin	Sguil logging scripts (log_packets_eth1.sh)
/LOG/external	Sguil log directory (eth1)
/LOG/external/dailylogs	Sguil daily logs collected by log_packets_eth1.sh
/LOG/external/portscans	Snort portscan dump directory
/LOG/external/sancp	sancp log dump directory
/LOG/internal	Sguil log directory (eth2)
/usr/local/mysql	MySQL database
/usr/local/SHADOW	Shadow directory files
/LOG/RAW/gmt	Shadow log files
/usr/local/NGREP	Network Grep sensor files

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

sancp custom queries

SID 1 – shadow
SID 2 – Snort1

Source and Destination Port Search

WHERE sancp.start_time > '2005-01-05' AND (sancp.src_port = '11768') OR (sancp.dst_port = '11768') LIMIT 500

Source and Destination Port Search for Only SID 2

WHERE sancp.sid= 2 AND sancp.start_time > '2005-01-20' AND (sancp.src_port = '15118') OR (sancp.dst_port = '15118') LIMIT 500

Single Day Source and Destination IP Search for SID 2 only

WHERE sancp.sid=2 AND sancp.start_time > '2005-01-15' AND sancp.end_time < '2005-01-16' AND (sancp.src_ip = INET_ATON('192.168.158.186') OR sancp.dst_ip = INET_ATON('192.168.158.186')) LIMIT 500

Specific Source IP

WHERE sancp.start_time > '2005-03-15' AND (sancp.src_ip = INET_ATON('192.168.8.89')) LIMIT 500

Specific Sensor (sid=2) and Source Port

WHERE sancp.sid=2 AND sancp.start_time > '2005-03-30' AND (sancp.src_port='53') LIMIT 500

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Shadow Command Line Pattern Search script

A new script is now in the /root called ***pat_search.pl*** which can be used to search multiple days. The format is as follow:

./pat_search.pl –n –b YYYYMMDDHH –e YYYYMMDDHH –p PATTERN

-n Do not resolve addresses (faster)
-b Beginning day and hour
-e Ending day and hour
-p Pattern to search in BPF format. Ex: “tcp port 27374”

It is configured with the following tcpdump options:

-X Display HEX and ASCII data
-v Verbose
-s 0 Read back the maximum snaplen on each packets

The output can be redirected to a file by using **> *filename***

If you would like to install the Shadow console, you should read the following document from the Shadow Team at:

http://www.nswc.navy.mil/ISSEC/CID/SHADOW-1.8-Install.pdf

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Background Information About this Setup

How to manually mount a CD-ROM or diskette

To manually mount the CD-ROM do:

mkdir /cdrom	(create cdrom directory)
mount /dev/hdc /cdrom -t iso9660	(mount the cdrom)
umount /cdrom	(un-mount the cdrom)

The cdrom maybe hdb, hdc or hdd depending where it has been installed in the computer. To find out which device is the CD-ROM, do *dmesg |more*

To manually mount the floppy do:

mkdir /floppy	(create floppy directory)
mount /dev/fd0 /floppy -t vfat	(mount the floppy)
umount /floppy	(un-mount the floppy)

Operating System Patches

The Slackware web site should be monitored for any new patches that should be applied on the selected packages at Annex A. The site is http://www.slackware.com

The security list is available at:

http://www.slackware.com/security/list.php?l=slackware-security&y=2005

Slackware Patch Maintenance Script

http://128.173.184.249/slackupdate/

Patches can be maintained and downloaded by running the /root/slackupdate.sh script. This script will check for any package that are available for update and saves them in /tmp/slackupdate. To install the patch updates as follow:

cd /tmp/slackupdate
telinit 1
upgradepkg <patch>.tgz
lilo (*Must be run only if upgraded IDE kernel*)
telinit 3

Note with other kernels: If you are using a kernel other than IDE, you must download the new kernel that is normally a bzImage and copy it to /boot/vmlinuz and run lilo before you reboot to ensure the new kernel will be used.

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Open Secure Shell (openssh) is part of the installation on this CD

Note: Secure Shell is normally used to transfer data between the monitoring station and the sensor. The instructions on how to setup an analysis station are available at the NSWC site. The site is at: http://www.nswc.navy.mil/ISSEC/

Configure Shadow in the following way (Pre-configured with this installation):

- cd /usr/local/SHADOW/sensor and make the following changes:

    - vi gmt.ph and verify the following settings:

    * Decide whether you want to use local time or GMT (default GMT)
    * $LOGPROG = "/usr/sbin/tcpdump" (or its exact location)
    * $PROGPAR = "-i eth1" (or eth0 if using a single card as the traffic collector)
    * $GZIPPROG = "/bin/gzip" (or its exact location)
    * $LOGDIR = "/LOG/RAW/gmt" (if not using default, change it here)

Note: All of the Shadow files are owned by the shadow user and part of the shadow group. The account has been locked. In order to use this account, run "*passwd shadow*" to add your own user password.

The message of the day changed to reflect more proactive security (Pre-configured with this installation):

- vi /etc/motd

```
**********************************************************************
This is a controlled access system.
This station is monitored at all times.
Only authorized users may connect
**********************************************************************
```

- cp /etc/motd /etc/issue

Update rc.local to start local applications:

O- vi /etc/rc.d/rc.local and add the following services

```
#!/bin/sh
#
# /etc/rc.d/rc.local:  Local system initialization script.
#
# Put any local setup commands in here:
# Starting eth1
echo "Fire up eth1 now to start Shadow collection..."
/sbin/ifconfig eth1 promisc -arp
/sbin/ifconfig eth1 up
```


Copyright © Guy Bruneau, 2001-2005. All rights reserved.

```
#
echo "Starting mysql database..."
/usr/local/mysql/bin/mysqld_safe --user=mysql &
#
echo "Starting shadow sensor..."
/usr/local/SHADOW/sensor/start_logger.pl gmt
#
# Uncomment any of these to start Network Grep sensor
#
#echo "Starting Network Grep sensor..."
#/usr/local/NGREP/sensor/start_ngrep.pl kazaa
#/usr/local/NGREP/sensor/start_ngrep.pl gnutella
#/usr/local/NGREP/sensor/start_ngrep.pl dir_c
#
echo “Starting Webmin…”
/etc/webmin/start
#
echo "Starting firewall..."
/etc/rc.d/rc.firewall
#
echo "Starting Snort sensor..."

if [ -x /etc/rc.d/rc.snort ]; then
  . /etc/rc.d/rc.snort start
  . /etc/rc.d/rc.barnyard start
fi
#
# All done
```

Update cronjob to start Shadow, update time, and cut new logs each hour (Pre-configured on Shadow CD):

Crontab running as Root

```
# Sync with a time server on a daily basis

17 23 * * * /usr/sbin/ntpdate time-a.nist.gov
18 23 * * * /sbin/hwclock --systohc

# Cut a new Shadow log on a hourly basis
0 * * * * /usr/local/logger/SHADOW/sensor_driver.pl gmt > /dev/null 2>1&

# Restart snort every night at midnight after updated Snort
# signatures have been downloaded
#
5 0 * * * /etc/rc.d/rc.snort restart > /dev/null 2>1&
```


Copyright © Guy Bruneau, 2001-2005. All rights reserved.

```
# Cut a new ngrep log on a hourly basis
# You can uncomment any of these examples or create your own in the
# /usr/local/NGREP/sensor directory using the template.ph

#0 * * * * /usr/local/NGREP/sensor/ngrep_driver.pl kazaa > /dev/null 2>1&
#0 * * * * /usr/local/NGREP/sensor/ngrep_driver.pl gnutella > /dev/null 2>1&
#0 * * * * /usr/local/NGREP/sensor/ngrep_driver.pl dir_c > /dev/null 2>1&
# Check that sshd is running

0,5,10,15,20,25,30,35,40,45,50,55 * * * * /usr/local/sbin/chk-sshd.pl
```

Crontab running as Snort

```
# This crontab runs at 1 am to updated the Snort signatures using the oinkmaster.pl
# script and merge the new rules into the rules directory.
#
0 0 * * * /usr/local/snort/rc.snortupdate
```

Note: During the first reboot, you will notice some errors in directory /LOG/RAW/gmt with files sniff and sensor date. This is normal as those files do not exist yet and the sensor is creating them.

O- Log in as root
O- Run *ps -aef* and verify the services running. (See picture 1)
O- Run *netstat -at* and verify the active connections (See picture 2). ssh should be the only service listening for remote login.
O- Check Annex D for a NMAP port reconnaissance probe confirming ssh is the only available service.
O- cd /LOG/RAW/gmt and verify the sensor is collecting. Do an *ls -l* and look for the hourly file that looks like this: tcp.20010312.gz with 0 bytes.
O- The sensor is ready to be connected to the network.

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

Network Grep (Ngrep) configuration

Ngrep Version 1.42
5 January 2005

Configure Ngrep in the following way (Pre-configured with this installation):

I would like to thank Alex Arndt for supplying the scripts in this section to make them part of this sensor. In this section, you can run ngrep in the same manner as a Shadow sensor in real-time to monitor as in the example below, someone successfully gaining access to a workstation and running Directory of C.

- cd /usr/local/NGREP/sensor and make the following changes:

    - vi **template.ph** and verify the following settings:

$FILTER = '"[C|c][+][D|d][I|i][R|r][+][C|c]|Directory of [C|c]"';

The start_ngrep.pl and stop_ngrep.pl scripts are used by cron to rollover a new file hourly. Check the rc.local section to start ngrep when the sensor start and the cron section to see the rollover configuration.

- cd /usr/local/NGREP

You can use **ngreppm.pl** to download the files to a remote analysis station.

Note: Adapt the filter to the keyword being searched.

Ngrep Pattern Search script

A new script is now in the /root called ***ngrep_pat_search.pl*** which can be used to search multiple days. The format is as follow:

./ngrep_pat_search.pl –b YYYYMMDDHH –e YYYYMMDDHH –p PATTERN –i BPF filter

-b Beginning day and hour
-e Ending day and hour
-p Pattern to search. Ex: “kazaa”
-i BPF Filter. Ex: “tcp port 80”

It is configured with the following ngrep options:

-t Print a timestamp in the form of YYYY/MM/DD HH:MM:SS.UUUUUU everytime a packet is matched

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

-I Ignore the case of the expression
-I Read pcap_dump back into ngrep
This script match keywords and BPF filters. Here are some examples:

Print all the packets on TCP port 80 that contains http

./ngrep_pat_search.pl –b YYYYMMDDHH –e YYYYMMDDHH –p “http” –i “tcp port 80”

Print all the packets on TCP port 80

./ngrep_pat_search.pl –b YYYYMMDDHH –e YYYYMMDDHH –p “ ” –i “tcp port 80”

Print all the packets that contains the string http

./ngrep_pat_search.pl –b YYYYMMDDHH –e YYYYMMDDHH –p “http” –i “ ”

Note: The output can be redirected to a file by using **> *filename***

Copyright © Guy Bruneau, 2001-2005. All rights reserved.

References

Securing Linux – A Survival Guide for Linux Security
SANS Institute

Intrusion Detection: Shadow Style step-by-step guide, Version 1.2.2
SANS Institute 1998

Installing Shadow
http://www.nswc.navy.mil/ISSEC/CID/SHADOW-1.8-Install.pdf

Shadow step-by-step Intrusion Detection using TCPdump
http://www.nswc.navy.mil/ISSEC/CID/shadow.ppt

Snort IDS
http://www.snort.org

Oinkmaster
http://www.algonet.se/~nitzer/oinkmaster/

Webmin
http://www.webmin.com/

MSB Networks
http://msbnetworks.net/snort/

SlackUpdate
http://128.173.184.249/slackupdate/

MySQL Windows Control Center
http://www.mysql.com/downloads/mysqlcc.html

Chaosreader to replay tcpdump traffic in HTML
http://users.tpg.com.au/bdgcvb/chaosreader.html

Copyright © Guy Bruneau, 2001-2005. All rights reserved.