

USENIX'04 / UseBSD



**Using OpenBSD and Snort
to build ready to roll Network
Intrusion Detection System
Sensor**

<http://www.mycert.org.my/sensor/>

Tuesday, June 29, 2004

About Speaker

Kamal Hilmi Othman

khilmi@niser.org.my

Mohammad Rizal Othman

rizal@jaring.my

Agenda

- Overview of OpenBSD and Snort
- Deployment of Distributed Network Intrusion Detection System
- Building OpenBSD and Snort for Network Intrusion Detection System Sensor (x86)
- Wrap up (Ready To Roll)

Problem Statement


- We need to install / deploy multiple Network Intrusion Detection System (NIDS) sensor within our network.
- Basically – the sensor is scattered around and need that fast!
- We need to deploy for partner (case to case basis)

Motivation

Pre-Rolled OpenBSD+Snort - Mozilla

File Edit View Go Bookmarks Tools Window Help


http://www.undeadly.org/cgi?action=article&sid=20031123185936&thres= Search



Home : [Add Story](#) : [Archives](#) : [About](#) :

Pre-Rolled OpenBSD+Snort

Contributed by [jose](#) on Sun Nov 23 18:59:00 2003 (GMT)
from the ready-to-roll-IDS dept.



As seen on <http://www.hackinthebox.com/article.php?sid=11929> the guys at <http://www.my-snort.org/> have a pre-rolled OpenBSD/Snort setup ready to go:

Thanks to the hard work of one our member, Kamal, we are pleased to announce the release of customized OpenBSD ISO with Snort IDS.

Here's what Kamal has to say about the ISO:

installation goes as with openbsd. then only when it comes to packages selection - u need to select all.

it comes with

1. openbsd 3.4 with customised kernel
2. snort 2.0.4 /usr/local/bin/snort
3. rules /usr/local/snort/rules/
4. tcsh /usr/local/bin/tcsh

that's all

In addition, root ssh is disallowed.

Have a look at this if you're in need of a read-to-roll Snort system.

<< [Tepatche - Automatic OpenBSD System Patcher in current SysAdmin](#) | [Reply](#) | [Flattened](#) | [Expanded](#) | [Secure programmer: Validating input](#) >>

Threshold: [Change](#) [Help](#)

No Subject Given (mod 0/0)

By Anonymous Contributor on Sun Nov 23 20:06:00 2003 / (0) (0)

OpenBSD

- BSD code base maturity.
- “Secure By Default”.
- Support for Internet infrastructure.
- Easy distribution sets.
- <http://www.openbsd.org>

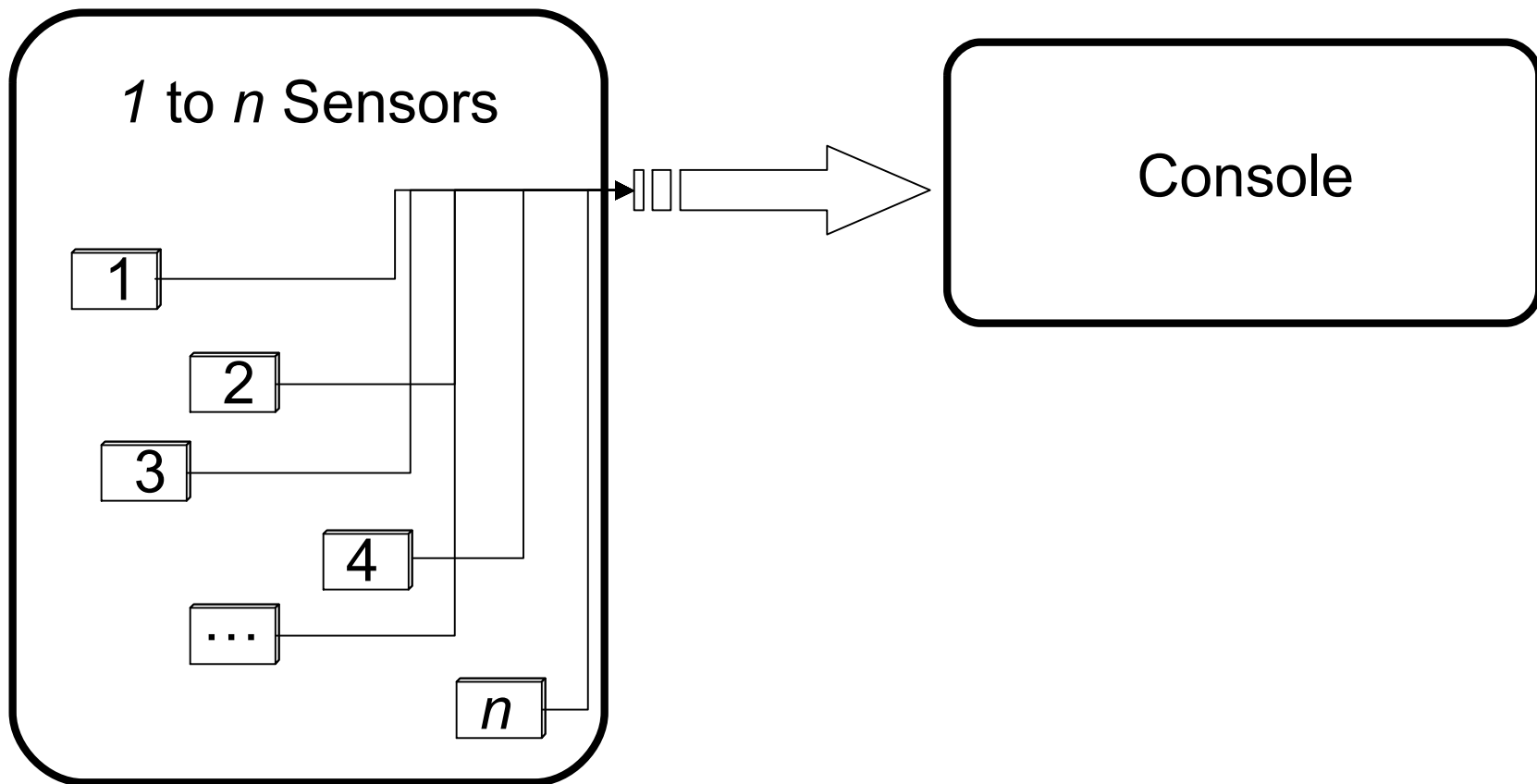
Snort

- Most notably Network Intrusion Detection System.
- Community signature support.
- Portable and configurable.
- <http://www.snort.org>

NIDS Sensor

- As an agent - it analyzes network packets in real time and compares them against a database of known 'attack signatures' or patterns.
- It will push the 'data' into remote database.

Distributed NIDS Generic Concept



Typical Installation

1. Install OpenBSD.
2. Tweak a kernel for performance tuning.
3. Install required third party software – MySQL client and PCRE.
4. Compile Snort with MySQL support and Snort related stuff - Barnyard, Stunnel, signature, user and group.
5. Take out unnecessary stuff.
6. Putting “in house” scripts.
7. Host hardening process.

Problem

- Time consume.
- Geographical boundary?
- Imagine when you need to roll 8 sensor?

Our approach

- Build one – install many.
- Installation process will cover all.
- Ideal sensor:
 - Performance
 - Minimal OS
 - No un-needed component
- Easy distribution – just iso / cdrom.

Building A Release

1. Install OpenBSD

- extract `sys.tar.gz` into `/usr/src/`
- cvs

2. Customise your kernel

- `/usr/src/sys/arch/i386/conf/MYKERNEL`

3. Test your kernel

- replace, reboot and monitor

Building A Release (cont)

4. Hacking the code

- You need to know the system.
- With this you can decide what you want.
- Code
 - /usr/src/Makefile
 - /usr/src/etc/Makefile
 - /usr/src/usr/bin/Makefile
 -

Building A Release (cont)

/usr/src/etc/Makefile

--- Makefile.ori Tue Jun 15 17:14:20 2004

+++ Makefile Thu Jun 17 16:20:51 2004

@@ -1,7 +1,7 @@

\$OpenBSD: Makefile,v 1.201 2004/02/29 18:02:14 deraadt Exp \$

TZDIR= /usr/share/zoneinfo

-LOCALTIME= Canada/Mountain

+LOCALTIME= Asia/Kuala_Lumpur

NOOBJ= oobj

@@ -17,8 +17,8 @@

- phones printcap protocols rbootd.conf rc rc.conf rc.local \

- rc.securelevel rc.shutdown remote rpc security services \

+ protocols rbootd.conf rc rc.conf rc.local \

+ rc.securelevel rc.shutdown remote security services \

Building A Release (cont)

/usr/src/etc/etc.i386/Makefile.inc

--- Makefile.inc.ori Tue Jun 15 17:16:53 2004

+++ Makefile.inc Tue Jun 15 17:17:20 2004

@@ -3,12 +3,12 @@

.ifdef DESTDIR

snap_md: bsd notes bootblocks distrib

- cp \${CURDIR}/../sys/arch/i386/compile/GENERIC/bsd \
+ cp \${CURDIR}/../sys/arch/i386/compile/SENSOR/bsd \
 \${DESTDIR}/snapshot/bsd

bsd:

- cd \${CURDIR}/../sys/arch/i386/conf && config GENERIC
- cd \${CURDIR}/../sys/arch/i386/compile/GENERIC && \
+ cd \${CURDIR}/../sys/arch/i386/conf && config SENSOR
+ cd \${CURDIR}/../sys/arch/i386/compile/SENSOR && \
 \${MAKE} clean && \${MAKE} depend && exec \${MAKE}

notes:

Building A Release (cont)

5. Build process configuration

- make your building runs faster
- /etc/mk.conf

```
SKIPDIR=usr.sbin/httpd share/doc share/dict games kerberosV gnu/egcs sys/netinet6 distrib/alpha  
distrib/amd64 distrib/cats distrib/hp300 distrib/hppa distrib/mac68k distrib/macppc distrib/mvme68k  
distrib/mvme88k distrib/mvmeppc distrib/sparc distrib/sparc64 distrib/vax share/man gnu/usr.bin/perl  
gnu/usr.bin/perl/lib gnu/usr.sbin/sendmail etc/etc.alpha etc/etc.amd64 etc/etc.cats etc/etc.hp300  
etc/etc.hppa etc/etc.mac68k etc/etc.macppc etc/etc.mvme68k etc/etc.mvme88k etc/etc.mvmeppc  
etc/etc.sparc etc/etc.sparc64 etc/etc.svr4 etc/etc.vax sys/arch/alpha sys/arch/amd64 sys/arch/arm  
sys/arch/cats sys/arch/hp300 sys/arch/hppa sys/arch/m68k sys/arch/mac68k sys/arch/macppc  
sys/arch/mvme68k sys/arch/mvme88k sys/arch/mvmeppc sys/arch/pegasos sys/arch/powerpc  
sys/arch/sparc sys/arch/sparc64 sys/arch/vax
```

Building A Release (cont)

6. Build your system

- /usr/src ; make obj && make build

7. Making your system

- setenv for RELEASEDIR and DESTDIR
- /usr/src/etc ; make release

Building A Release (cont)

```
/usr/src/distrib/sets/maketars
```

```
--- maketars.old    Wed Jun 16 18:55:32 2004
```

```
+++ maketars      Sat Jun 19 09:21:38 2004
```

```
@@ -49,7 +49,7 @@
```

```
cd $fsdir
```

```
-for i in base comp etc game man misc; do
```

```
+for i in base etc ; do
```

```
    echo -n "$i: "
```

```
    cat ${lists}/${i}/mi ${lists}/${i}/md.${arch} | sort | \
```

```
        pax -w -d | gzip -9 > ${tardir}/${i}${RELEASE}.tgz
```

Building A Release (cont)

8. Release tarballs

- RELEASDIR should contain binary distribution sets, kernel, cdrom and floppy bootable file-systems, checksum file and installation instruction.

9. Adding third party software

- uses siteXX.tgz
- example:

`/usr/local/lib/libpcre.so.0.1`

`/usr/local/lib/libmysqlclient.so.12.0`

`/usr/local/bin/snort`

`/usr/local/bin/barnyard`

`/usr/local/sbin/stunnel`

`/etc/rules/`

`/var/log/snort`

Build A Release (cont)

10. Write your iso

- follow the layout set ie: /version/arch/
- mkhybrid

11. Distribute your iso or cdrom

Installation

```
[X] bsd
[ ] bsd.rd
[X] base35.tgz
[X] etc35.tgz
[X] site35.tgz

File name? (or 'done') [bsd.rd] done
Ready to install sets? [yes] yes
Getting bsd ...
100% !*****! 4285 KB 00:04
Getting base35.tgz ...
100% !*****! 18959 KB 00:13
Getting etc35.tgz ...
100% !*****! 244 KB 00:00
Getting site35.tgz ...
100% !*****! 706 KB 00:00

Sets can be located on a (M)ounted filesystem; a (c)drom, (d)isk or (t)ape
device; or a (f)tp, (n)fs or (h)ttp server.
Where are the install sets? (or 'done') done
Do you wish sshd(8) to be started by default? [yes]
Saving configuration files...done.
Generating initial host.random file...done.
What timezone are you in? ('?' for list) [Asia/Kuala_Lumpur] _
```

Our Release

- Uses around 50M.
- Default installation with:
 - Snort, its dependency, signature, directory, user and group
 - Barnyard, Stunnel
- Has our own “in house” script.
- Sample release:
 - <http://www.my-snort.org/downloads/>
 - <http://www.mycert.org.my/sensor/>

Virtual PC demo

Maintenance

- Central server
- Second NIC is controlled by TCP-Wrapper and SSH-key
- All rules are 'cvs'
- Application / Snort upgrade use pkg_add

How To

- Collection of howto is
 - <http://www.openbsd.org/faq/index.html>
 - Man release
 - building an OpenBSD release
 - Man mk.conf
 - system-specific configuration parameters
 - misc@openbsd.org

Similar Project

<http://www.prowling.nu/main/openids/openids.html>

Conclusion

- We are still working on making a small distribution.
- Room for improvement.

end()

Thank You for Listening