Utilizing snort and acid as an intrusion detection device.

<tflat@astrocreep.net>

Abstract:

The use of Intrusion Detection Systems in todays networked computing environments is a necessity to the integrity and security of data.

An IDS can help you verify security and integrity of your network.

Integrity: Has your data been tampered with or services exploited?

Security: Is your data and servers secure?

Intrusion Detection Systems are simply applications that compare packets on the wire to known signatures on known attacks. There a pitfalls, packets can be fragmented and sent in a random order taking advantage of the fact that the IDS does not state-fully inspect packets. In solaris, the snoop command allows you to place the NIC in promiscuous mode and see most of the packet information with a limited payload dump. It is a great tool for troubleshooting network issues, but not so good at detecting rouge packets in the wild. Snort on the other hand, does everything snoop does, then adds detection of known signatures that can be construed as bad. Add the ability to log these alerts to a remote database, and you have the beginnings of an IDS. Once the database is up and running, you will need a way to sift through all those nasty packets that were logged. Unless you are well versed in SQL or borderline psycho you will want a better way to analyze the data. ACID (Everyone likes web pages right?) presents the data in a easy to use format.

If a systems engineer/administrator does not know what is flying across the wire, there is a good chance that they have been compromised or are being probed without the admins ever knowing. This places a huge advantage for the blackhat. If the admin is compromised, how does he expect to prosecute without a base line of information to prove the black hat guilty. There are other ways of gathering this data, but why make it harder than it needs to be? If data is being collected realtime and on a remote system, this gives the admin the upper hand, at least from a passive defensive point of view.

A multi-tiered security architecture must be implemented,

-> firewalls (pix,cp1,gauntlet)
-> ids (snort,nfr)
-> host based ids (tripwire, snort, portsentry)
-> host based acl's (iptables, ipfilters, portsentry)
-> host based log monitoring (logcheck)
-> backups (arkeia, amanda)
-> host patch management
-> monitoring mailing lists

After shopping around for tools to accomplish the IDS task, I found that using snort/acid to be more than adequate. NFR, a commercial IDS, is extremely pricey and in shops where there is a limit on spending in not possible as an option.

Introduction:

This document is aimed at installing Snort and Acid on a *nix platform. I have successfully accomplished the following 0n the following versions of *nix:

SuSE Linux 7.0, 7.1, 7.2
Slackware 7.0, 7.1
Solaris 7, 8

Installation on Win9x,NT,2000 is possible, however I have never done it.

This document is aims to be a checklist, the authors off all software below have written documentation the installation of each in more detail.

Installation overview (*nix):

```
        Install LibPcap
        Install Snort
        Install Apache/PHP (Use ApacheToolBox)
        Install Mysql (Use ApacheToolBox)
        Install ADODB
        Install PHPlot
        Install Acid
        Create .htaccess in acid document root or create user/password via
database/sessions.

AuthName  ACID
AuthGroupFile /dev/null
AuthType Basic
AuthUserFile /usr/local/apache/conf/htpasswd
require user tflat

# /usr/local/apache/bin/htpasswd -c /usr/local/apache/conf/htpasswd tflat
<password x2>

        Create MySQL database

$ cat create_mysql | mysql -u root -p
  <password>

        Create sql account with insert, select, create, delete privelegdes for acid
user.

$ echo  grant select,insert,delete,create on snort.* to USER@HOSTNAME identified by
 PASSWD  | mysql -u root -p
  <password>

        Create sql accout with insert priviledges for sensor user(s).

$ echo  grant select on snort.* to USER@HOSTNAME identified by  PASSWD  | mysql -u
root -p

        Configure snort.  Add the following line to /etc/snort/snort.conf

output database:  log,mysql,dbname=DB user=USER host=HOSTNAME password=PASSWD

        Start mysql

# /usr/local/mysql/bin/safe_mysqld &

        Start snort

        /usr/local/sbin/snort -D -d -b -c /etc/snort/snort.conf &

        -D Run in Daemon Mode
        -d Dump Application Layer
        -b Log packets in tcpdump format
        -c use configuration file <file>
        -N Turn off logging

        Go to https://astrocreep.net/acid/
        user: guest
        password: public

Prerequisite Software:

ADODB
http://php.weblogs.com/adodb

Analysis Console for Intrusion Databases (ACID)
http://www.cert.org/kb/acid/

Apache
http://httpd.apache.com

Apache Toolbox
```

http://www.apachetoolbox.com

Libpcap
ftp://ftp.ee.lbl.gov/libpcap.tar.Z

PHP
http://www.php.net/

PHPMyAdmin
http://phpmyadmin.sourceforge.net/download.html

PHPlot
http://www.phplot.com/

Snort
http://www.snort.org

--
$Id: snort_acid.txt,v 1.6 2001/08/01 01:42:12 tflat Exp $