

Re: process accounting

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2003-05/0029.html>

From: Anders Gustafsson (andersg_at_0x63.nu)

Date: 05/27/03

Date: Tue, 27 May 2003 20:58:45 +0200
To: Craig Holmes <Leusent@link-net.org>

On Mon, May 26, 2003 at 08:27:07PM -0400, Craig Holmes wrote:

> > *There is a patch for bash which makes bash logs everything*
> > *that is typed (I don't remember the url, search for bash+logging+patch).*
> *I have written a very basic patch for bash 2.05b which logs everything which*
> *would normally be written to your .bash_history file to a single remote file*
> *(No matter what a person does the master file is still written too). It is*
> *pretty rough and I used it only briefly in a honeypot exercise, though you*
> *may find it usefull.*
> <http://gearbox.gearbolt.net/files/patches/bash-masterhist.diff>

There is a program called snoopy too:

<http://sourceforge.net/projects/snoopylogger/>

It logs all execve() calls to syslog. It's installed in /etc/ld.so.preload so it only works with dynamically linked programs, but most are.

--

Anders Gustafsson - andersg@0x63.nu - <http://0x63.nu/>