

possible compromise or just misreading logs

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-12/0014.html>

From: Craig Riter (*criter_at_riter.com*)

Date: 12/07/03

To: <freebsd-security@freebsd.org>
Date: Sun, 7 Dec 2003 09:14:56 -0800

I am not sure if I had a compromise but I am not sure I wanted some other input.

I noticed in this in my daily security run output:

pc1 setuid diffs:

19c19

< 365635 -rwsr-xr-x 1 root wheel 204232 Sep 27 21:23:19 2003

/usr/X11R6/bin/xscreensaver

> 365781 -rwsr-xr-x 1 root wheel 205320 Dec 4 07:55:59 2003

/usr/X11R6/bin/xscreensaver

It was the only file listed and I didn't remember changing anything on my pc having to do with the screensaver and can't even remember for sure if I was on my computer at that time.

I also noticed this message on my screen (I still have syslogd write some messages there):

Dec 4 07:54:13 pc1 /kernel: pid 62069 (msgfmt), uid 0: exited on signal 6 (core dumped)

Dec 4 07:57:04 pc1 /kernel: pid 64543 (msgfmt), uid 0: exited on signal 6 (core dumped)

When looking in the /usr/X11/R6/bin I saw some other files that were modified around this time. I didn't have a reason to modify these other files so I don't think it was me.

```
drwxr-xr-x  3 root  wheel    10752 Dec  4 09:18 ./
-r--r--r--  1 root  wheel     5324 Dec  4 09:18 qtrename140
-r--r--r--  1 root  wheel     8065 Dec  4 09:18 qt20fix
-r--r--r--  1 root  wheel   218708 Dec  4 09:18 moc2
-r--r--r--  1 root  wheel     4160 Dec  4 09:18 findtr
-r--r--r--  1 root  wheel   206044 Dec  4 09:18 uic
-r--r--r--  1 root  wheel    41964 Dec  4 07:57 xscreensaver-gl-helper
dr--r--r--  2 root  wheel     3584 Dec  4 07:57 xscreensaver-hacks/
-r--r--r--  1 root  wheel      988 Dec  4 07:56
screensaver-properties-capplet
-r--r--r--  1 root  wheel     4790 Dec  4 07:56 xscreensaver-getimage-video
-r--r--r--  1 root  wheel   116916 Dec  4 07:56 xscreensaver-getimage
-r--r--r--  1 root  wheel     7271 Dec  4 07:56 xscreensaver-getimage-file
-r--r--r--  1 root  wheel   168360 Dec  4 07:56 xscreensaver-demo
-r--r--r--  1 root  wheel   205320 Dec  4 07:55 xscreensaver
-r--r--r--  1 root  wheel    17624 Dec  4 07:55 xscreensaver-command
```

I have since made them all read only since I didn't want to run them in case they had a trojan.

FreeBSD-Security: possible compromise or just misreading logs

So, my question is did I have a break-in? This machine is accessible only as a web server through NAT and ipfw (if I configed my ipfw correctly). I had just installed the Apache 1.3.29.

Second, what are people using for intrusion detection? This is something I have thought about but never really thought I needed until now.

Thanks,
Craig

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"