

Re: virus/worm hacker attack

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-10/4898.html>

From: N. O. Spam (nospam@NOSPAM.com)

Date: 09/15/02

From: "N. O. Spam" <nospam@NOSPAM.com>

Date: Sun, 15 Sep 2002 18:56:26 GMT

Thomas Reith wrote:

> *Hi,*
>
> *we run a server with former kernel 2.2.18/glibc 2.2.2 and*
> *now kernel 2.4.19/glibc 2.2.5.*
>
> *for about two weeks, we were victims of a hacker attack*
> *via apache/php. the security hole has been fixed, and*
> *further attacks are not possible.*
>
> *But now, we have a much more serious problem the*
> *guy infected our linux system with a strange virus.*

A root kit goes beyond virus. You did not fix the hole, you only closed 1 door. While the hole was open, the cracker added new holes. It isn't quite a virus, because you can email a virus or sneak it in...the root kit required finding another hole first to gain root privileges, and only then could it be added. If it had emailed to you and had itself bypassed security, you could call it a virus.

You can back up data, and then wipe the system and restore, making sure it is using current software before you even touch the Internet. Your original hole fix was like locking the front door again and changing the locks while the burglar was still in the house. You never booted the burglar out.

>
> *the mechanism seems to be related with the one*
> *used in "epcs2.c" (exploit for execve/ptrace race condition)*
> *see: <http://spisa.act.uji.es/spi/progs/codigo/www.hack.co.za/exploits/os/linux/misc/kernel/epcs2.c>*
>
> *infected elf binaries grow nearly 7k. they can be detected by*
> *"strings binary"*
>
> -----
> ...
> */tmp/extfsRNV23z*

> /dev
> /proc
> /bin
> /proc//////////exe
> SQRV
> ^ZY[
> gfff
> gfff
> WVS1
> -----
>
> *if there is something like above on the end of the output,*
> *the binary is infected.*
>
> *we tried to replace all infected binaries with clean ones,*
> *but after a while every binary was infected again.*
> *there seems to be no cronjob or daemon, which does this*
> *job, the shared libraries in /lib are clean, too.*
>
> *problems:*
> *– infected binaries have problems with pipes, which*
> *mean that gcc/as/ld cannot be used anymore. strace*
> *doesn't help, because it hangs completely.*
>
> *questions:*
> *– does anyone know more about this virus/worm*
> *– scanning could be done with "strings", but*
> *what about removing?*
>
> *regards*
>
> *Thomas Reith*

-
- **Next message:** : ["Re: KOREAN SPAM: HOWTO deal with it???"](#)
 - **Previous message:** [Allen Kistler: "Re: How to forward IPSec protocols?"](#)
 - **In reply to:** [Thomas Reith: "virus/worm hacker attack"](#)
 - **Next in thread:** [Richard Steven Hack: "Re: virus/worm hacker attack"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)