

Re: Encrypted file system without initial password:

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-03/0521.html>

From: Bo Jacobsen (bjc@image.dk)

Date: 03/15/02

From: "Bo Jacobsen" <bjc@image.dk>
Date: Fri, 15 Mar 2002 12:12:17 +0100

"Kasper Dupont" <kasperd@daimi.au.dk> skrev i en meddelelse
news:3C90AB56.9A2AED35@daimi.au.dk...

> *Lee Sau Dan wrote:*

>>

>

> *Lee, I'm afraid you misunderstood Bo's question.*

>

>>>>>> *"Bo" == Bo Jacobsen <bjc@image.dk> writes:*

>>

>> *Bo> I have tried using the encrypted filesystem that comes with*

>> *Bo> SuSE 7.3. It works OK but my question is, can one make it boot*

>> *Bo> without asking for the password.*

>>

>> *So, where is the password stored? How does the system figure out the*

>> *password? That's the highest VULNERABILITY of your system. Any hack*

>> *who can gain root privilege will be able to find out the password and*

>> *hence will be able to access all the files stored on that filesystem*

>> *in plain text.*

>

> *This was not a question about potential root exploits. No*

> *question was asked about what could be done when the system*

> *is up and running. The question was about what could be done*

> *before and during boot of the system. BTW getting root*

> *privileges on the running system doesn't imply getting the*

> *password. But it obviously gets read access to all files.*

>

>>

>> *Bo> I just need to be sure that as long as one is not able to*

>> *Bo> login, my data is relatively safe.*

>>

>> *Unable to login doesn't imply unable to break in.*

>>

>> *Even if you "touch /etc/nologin", thereby making 'login' refuse to log*

>> *anyone in, a buffer overflow attack on the telnetd (if it is running*

>> *and has a buffer overflow bug) could still grant the hack root*

>> *privilege from remote!*

comp.os.linux.security: Re: Encrypted file system without initial password:

> >
> > *Bo> Without encryption, even a*
> > *Bo> novice user can just boot from another media (or move the disk*
> > *Bo> to another pc), manually mount a partition and read it.*
> >
> > *You could disable booting on other media through some CMOS/BIOS*
> > *settings. These settings can then be password-protected in the BIOS*
> > *menus. Any post 1993 Intel x86 PC system has a BIOS that provide*
> > *these functions.*
>
> *He actually asked how to make it more difficult to read*
> *the disk even if it was moved into another computer. The*
> *CMOS settings would not help there.*
>
> >
> > *Of course, if one discharges the CMOS to erase these settings, he can*
> > *still boot a floppy. But this guy won't be a "novice user" by any*
> > *standard.*
> >
> > *Moreover, as mentioned again and again, without physical security*
> > *(inside a safe or a highly secured room) on the machine, every*
> > *software-based security measure would be useless.*
>
> *Not useless, but depend on the attackers capabilities.*
> *In theory any capable programmer could bypass this*
> *software. But in practice it is can be very hard, and can*
> *actually stop novice attackers.*
>
> >
> > *Bo> Maybe someone knows the answer, or have some suggestions ? I*
> > *Bo> know that in cunning hands, no data is safe, but I just need*
> > *Bo> to make sure that it's not to easy to get access to it.*
> >
> > *Wouldn't locking the machine in a secure room and disconnecting it*
> > *from the Internet be a more straightforward solution?*
>
> *That would imply that it is currently connected to the*
> *internet. Who said that it is?*
>
> --

Right on target, I could not have said it better. As nothing can be secured 100%, I think one has to take into account what security level is appropriate for the information you are dealing with. If not, you just have to give up, and refuse to handle any information at all, because no matter what you do, there will always be someone that are able to get at it.

In this case the data is not super sensitive, and as the system in general is kept up to date

Re: Encrypted file system without initial password:

comp.os.linux.security: Re: Encrypted file system without initial password:

the system should be fairly secure. Except of course if persons can get at the harddisk. In this case the system is TOTALLY insecure.

I surely do not understand the argument that if it's not 100% secure (which of course is impossible in the first place) why bother trying to make it harder to access the data. If one follows this argument, why bother about security at all.

Bo Jacobsen bjc@image.dk

- *Next message:* [Wine Development: "Re: Linux iptables/netfilter and Netmeeting Remote Desktop Sharing"](#)
- *Previous message:* [Tim C: "Re: Linux iptables/netfilter and Netmeeting Remote Desktop Sharing"](#)
- *In reply to:* [Kasper Dupont: "Re: Encrypted file system without initial password:"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)