

## Re: [Full-Disclosure] Automated ssh scanning

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-08/1228.html>

---

**From:** KF\_lists ([kf\\_lists\\_at\\_secnetops.com](mailto:kf_lists_at_secnetops.com))

**Date:** 08/26/04

To: Mailing List - Full-Disclosure <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>

Date: Thu, 26 Aug 2004 14:54:37 -0400

Will \*ANYONE\* that actually got hacked do me a favor and type:

"uname -a"

Then include that in your next email. I keep hearing "fully patched" server however I have a feeling the Kernel was left out of the patching.

-KF

Todd Towles wrote:

> *Hey Ron,*

>

> *Guest isn't a admin so they let the tool get in. But the real questions is, how does it get root access on a fully patched server? It appears to use a local exploit to gain root access. This is a problem.*

>

> *Sorry about the eariler e-mail, I haven't had my coffee today. Trying to cut back and spend that money on IT security =P*

>

> -----Original Message-----

> *From: full-disclosure-admin@lists.netsys.com*

> *[mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of Ron*

> *DuFresne*

> *Sent: Thursday, August 26, 2004 9:08 AM*

> *To: Tig*

> *Cc: full-disclosure@lists.netsys.com*

> *Subject: Re: [Full-Disclosure] Automated ssh scanning*

>

>

>

> *the real thing this user most likely suffered from was the weak account passwd double, guest:guest. Now, if the admin and other account were setup with strong passwd's and this account was either setup with a strong passwd or not setup at all might be a better test of the stability of ssh and the debain setup in question.*

>

> *Thanks,*

>

> *Ron DuFresne*

Full-Disclosure: Re: [Full-Disclosure] Automated ssh scanning

>  
> *On Thu, 26 Aug 2004, Tig wrote:*  
>  
>  
>>*On Wed, 25 Aug 2004 19:43:47 -0400*  
>>*Gerry Eisenhaur <GEisenhaur@Cisco.com> wrote:*  
>>  
>>  
>>>*I am confused, you said you knew about some SSH scanning going on,*  
>>>*then set up those accounts on a box. Now you are curious way that*  
>>>*box got rooted?*  
>>>  
>>>*Maybe I am missing something, but it seems you already have a pretty*  
>  
>  
>>>*good assumption of why it got rooted.*  
>>>  
>>>*The software, as you seem to know, is a few exploits, a backdoor and*  
>  
>  
>>>*some IRC stuff(bot and proxy).*  
>>>  
>>>*/gerry*  
>>>  
>>  
>>*I think you did miss the point (which was a very good one). Basically,*  
>  
>  
>>*once you have unprivileged access to a currently patched Woody box,*  
>>*you can quickly gain root access.*  
>>  
>>*I would love to see this tested against other version of Linux and*  
>>*\*BSD with default (and updated) installations. Anyone have a spare box*  
>  
>  
>>*and a few hours?*  
>>  
>>*-Tig*  
>>  
>>  
>>\_\_\_\_\_

---

>>*Full-Disclosure - We believe in it.*  
>>*Charter: <http://lists.netsys.com/full-disclosure-charter.html>*  
>>  
>  
>  
> ~~~~~

> *"Cutting the space budget really restores my faith in humanity. It*  
> *eliminates dreams, goals, and ideals and lets us get straight to the*  
> *business of hate, debauchery, and self-annihilation." -- Johnny Hart*  
> *\*\*\*testing, only testing, and damn good at it too!\*\*\**  
>

Full-Disclosure: Re: [Full-Disclosure] Automated ssh scanning

- > *OK, so you're a Ph.D. Just don't touch anything.*
- >
- > \_\_\_\_\_
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*
- >
- > \_\_\_\_\_
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*
- >

\_\_\_\_\_  
Full-Disclosure – We believe in it.  
Charter: <http://lists.netsys.com/full-disclosure-charter.html>