

## Re: how did someone hack in my machine?

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.unix/2002-03/0092.html>

---

*From:* letterhead ([noname@ailias.net](mailto:noname@ailias.net))

*Date:* 03/07/02

From: "letterhead" <[noname@ailias.net](mailto:noname@ailias.net)>

Date: Thu, 07 Mar 2002 18:41:28 GMT

Well,

A: you have user "nobody" STILL on your box. Not so good. Unix installs some bullshit accounts when first installed. They got in as user "nobody"

Look here: A list of default UNIX username & passwords.

With an open ssh port and a bit of persistence (in many cases, there is still and account on a remote box that has permission to ssh in) someone with a bit of brains can get in.

This is a great resource....go here & learn!!!

<http://hackingtruths.box.sk/manuals.htm>

Manufacturer

Product

Revision

Protocol

User ID

Password

UNIX

Generic

Multi

adm

adm

Admin

UNIX

Generic

Multi

adm

(none)

Admin

UNIX

Generic

Multi

admin

comp.security.unix: Re: how did someone hack in my machine?

admin  
User

UNIX  
Generic

Multi  
administrator  
administrator  
User

UNIX  
Generic

Multi  
administrator  
(none)  
User

UNIX  
Generic

Multi  
anon  
anon  
User

UNIX  
Generic

Multi  
bbs  
bbs  
User

UNIX  
Generic

Multi  
bbs  
(none)  
User

UNIX  
Generic

Multi  
bin  
sys  
Admin

UNIX  
Generic

Multi  
bin  
sys  
Admin

UNIX  
Generic

Multi  
checkfs  
checkfs  
User

UNIX  
Generic

Multi  
checkfsys  
checkfsys  
User

UNIX  
Generic

Multi  
checksys  
checksys  
User

UNIX  
Generic

Multi  
daemon  
daemon  
User

UNIX  
Generic

Multi  
daemon  
(none)  
User

UNIX  
Generic

Multi  
demo  
demo  
User

UNIX  
Generic

Multi  
demo  
(none)  
User

UNIX  
Generic

Multi  
demos  
demos  
User

UNIX  
Generic

Multi  
demos  
(none)  
User

UNIX  
Generic

Multi  
dni  
(none)  
User

UNIX  
Generic

Multi  
dni  
dni  
User

UNIX  
Generic

Multi  
fal  
(none)

User

UNIX  
Generic

Multi  
fal  
fal  
User

UNIX  
Generic

Multi  
fax  
(none)  
User

UNIX  
Generic

Multi  
fax  
fax  
User

UNIX  
Generic

Multi  
ftp  
(none)  
User

UNIX  
Generic

Multi  
ftp  
ftp  
User

UNIX  
Generic

Multi  
games  
games  
User

UNIX  
Generic

Multi  
games  
(none)  
User

UNIX  
Generic

Multi  
gopher  
gopher  
User

UNIX  
Generic

Multi  
gopher  
(none)  
User

UNIX  
Generic

Multi  
guest  
guest  
User

UNIX  
Generic

Multi  
guest  
guestgue  
User

UNIX  
Generic

Multi  
guest  
(none)  
User

UNIX  
Generic

Multi  
halt  
halt  
User

UNIX  
Generic

Multi  
halt  
(none)  
User

UNIX  
Generic

Multi  
informix  
informix  
User

UNIX  
Generic

Multi  
install  
install  
Admin

UNIX  
Generic

Multi  
lp  
lp  
User

UNIX  
Generic

Multi  
lp  
bin  
User

UNIX  
Generic

Multi  
lp  
lineprin

User

UNIX  
Generic

Multi  
lp  
(none)  
User

UNIX  
Generic

Multi  
lpadm  
lpadm  
User

UNIX  
Generic

Multi  
lpadmin  
lpadmin  
User

UNIX  
Generic

Multi  
lynx  
lynx  
User

UNIX  
Generic

Multi  
lynx  
(none)  
User

UNIX  
Generic

Multi  
mail  
(none)  
User

UNIX  
Generic

Multi  
mail  
mail  
User

UNIX  
Generic

Multi  
man  
man  
User

UNIX  
Generic

Multi  
man  
(none)  
User

UNIX  
Generic

Multi  
me  
(none)  
User

UNIX  
Generic

Multi  
me  
me  
User

UNIX  
Generic

Multi  
mountfs  
mountfs  
Admin

UNIX  
Generic

Multi  
mountfsys  
mountfsys  
Admin

UNIX  
Generic

Multi  
mountsys  
mountsys  
Admin

UNIX  
Generic

Multi  
news  
news  
User

UNIX  
Generic

Multi  
news  
(none)  
User

UNIX  
Generic

Multi  
nobody  
(none)  
User

UNIX  
Generic

Multi  
nobody  
nobody  
User

UNIX  
Generic

Multi  
nuucp  
(none)

User

UNIX  
Generic

Multi  
operator  
operator  
User

UNIX  
Generic

Multi  
operator  
(none)  
User

UNIX  
Generic

Multi  
oracle  
(none)  
User

UNIX  
Generic

Multi  
postmaster  
postmast  
User

UNIX  
Generic

Multi  
postmaster  
(none)  
User

UNIX  
Generic

Multi  
powerdown  
powerdown  
User

UNIX  
Generic

Multi  
rje  
rje  
User

UNIX  
Generic

Multi  
root  
root  
Admin

UNIX  
Generic

Multi  
root  
(none)  
Admin

UNIX  
Generic

Multi  
setup  
setup  
Admin

UNIX  
Generic

Multi  
shutdown  
shutdown  
User

UNIX  
Generic

Multi  
shutdown  
(none)  
User

UNIX  
Generic

Multi  
sync  
sync  
User

UNIX  
Generic

Multi  
sync  
(none)  
User

UNIX  
Generic

Multi  
sys  
sys  
Admin

UNIX  
Generic

Multi  
sys  
system  
Admin

UNIX  
Generic

Multi  
sys  
bin  
Admin

UNIX  
Generic

Multi  
sysadm  
sysadm  
Admin

UNIX  
Generic

Multi  
sysadm  
admin

Admin

UNIX  
Generic

Multi  
sysadmin  
sysadmin  
Admin

UNIX  
Generic

Multi  
sysbin  
sysbin  
Admin

UNIX  
Generic

Multi  
system\_admin  
(none)  
Admin

UNIX  
Generic

Multi  
system\_admin  
system\_admin  
Admin

UNIX  
Generic

Multi  
trouble  
trouble  
User

UNIX  
Generic

Multi  
umountfs  
umountfs  
User

UNIX  
Generic

Multi  
umountfsys  
umountfsys  
User

UNIX  
Generic

Multi  
umountsys  
umountsys  
User

UNIX  
Generic

Multi  
unix  
unix  
User

UNIX  
Generic

Multi  
user  
user  
User

UNIX  
Generic

Multi  
uucp  
uucp  
User

UNIX  
Generic

Multi  
uucpadm  
uucpadm  
User

UNIX  
Generic

comp.security.unix: Re: how did someone hack in my machine?

Multi  
web  
(none)  
User

UNIX  
Generic

Multi  
web  
web  
User

UNIX  
Generic

Multi  
webmaster  
webmaster  
User

UNIX  
Generic

Multi  
webmaster  
(none)  
User

UNIX  
Generic

Multi  
www  
(none)  
User

UNIX  
Generic

Multi  
www  
www  
User

--  
18er

Letterhead

"I know enough, others know more..." -me|now-

Re: how did someone hack in my machine?

comp.security.unix: Re: how did someone hack in my machine?

"Tony" <[tandcwong@attbi.com](mailto:tandcwong@attbi.com)> wrote in message news:X%Bh8.25238\$e07.4763@scrrnsc01... > check this: > > auth.log.1:Dec 25 06:25:01 goteach su[10587]: + ??? root-nobody > auth.log.1:Dec 25 06:25:01 goteach PAM\_unix[10587]: (su) session opened for > user nobody by (uid=0) > auth.log.1:Dec 25 07:01:40 goteach sshd[10753]: Did not receive ident string > from 211.210.0.150. > auth.log.1:Dec 25 07:31:10 goteach sshd[412]: Generating new 768 bit RSA > key. > auth.log.1:Dec 25 07:31:10 goteach sshd[412]: RSA key generation complete. > auth.log.1:Dec 25 13:43:08 goteach sshd[10801]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:08 goteach sshd[10803]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:08 goteach sshd[10804]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:08 goteach sshd[10805]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:09 goteach sshd[10809]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:09 goteach sshd[10810]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:10 goteach sshd[10811]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:10 goteach sshd[10812]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:10 goteach sshd[10814]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:11 goteach sshd[10815]: Disconnecting: Corrupted > check bytes on input. > auth.log.1:Dec 25 13:43:11 goteach sshd[10817]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:15 goteach sshd[10819]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:22 goteach sshd[10822]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:26 goteach sshd[10824]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:30 goteach sshd[10826]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:35 goteach sshd[10828]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:37 goteach sshd[10830]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:38 goteach sshd[10833]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:38 goteach sshd[10834]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:38 goteach sshd[10835]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:41 goteach sshd[10854]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:45 goteach sshd[10878]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:46 goteach sshd[10881]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:46 goteach sshd[10882]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:46 goteach sshd[10883]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:51 goteach sshd[10914]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:52 goteach sshd[10915]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:52 goteach sshd[10916]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:54 goteach sshd[10929]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:54 goteach sshd[10930]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:43:54 goteach sshd[10931]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:44:00 goteach sshd[10962]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:44:00 goteach sshd[10963]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:44:00 goteach sshd[10964]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:44:02 goteach sshd[10974]: Disconnecting: crc32 > compensation attack: network attack detected > auth.log.1:Dec 25 13:50:17 goteach sshd[412]: Received SIGHUP; restarting. > auth.log.1:Dec 25 13:50:17 goteach sshd[412]: RESTART FAILED: av0='sshd', > error: Permission denied. > auth.log.1:Dec 25 13:53:41 goteach su[11186]: + pts/0 root-nobody > auth.log.1:Dec 25 13:53:41 goteach PAM\_unix[11186]: (su) session opened for > user nobody by (uid=0) > daemon.log.1:Dec 25 00:36:38 goteach identd[10504]: started > daemon.log.1:Dec 25 09:14:54 goteach wu-ftpd[10769]: connect from > 130.60.208.58 > daemon.log.1:Dec 25 09:41:28 goteach wu-ftpd[10772]: connect from > 130.60.208.58 > daemon.log.1:Dec 25 10:52:39 goteach wu-ftpd[10781]: connect from > AStrasbourg-202-1-2-138.abo.wanadoo.fr >

Re: how did someone hack in my machine?

comp.security.unix: Re: how did someone hack in my machine?

daemon.log.1:Dec 25 12:52:06 goteach telnetd[10793]: connect from > web1.gj.net > daemon.log.1:Dec 25 12:52:26 goteach telnetd[10793]: tloop: read: > Connection reset by peer > daemon.log.1:Dec 25 13:53:47 goteach identd[11192]: started > daemon.log.1:Dec 25 14:02:12 goteach identd[11201]: started > daemon.log.1:Dec 25 16:18:32 goteach wu-ftpd[11222]: connect from > B0309.pppool.de > daemon.log.1:Dec 25 18:53:20 goteach wu-ftpd[11239]: connect from > 213.237.71.207.adsl.vg.worldonline.dk > daemon.log.1:Dec 25 20:33:27 goteach identd[11250]: started > daemon.log.1:Dec 25 20:57:28 goteach identd[11262]: started > daemon.log.1:Dec 25 21:45:50 goteach telnetd[11275]: connect from > 1Cust34.tnt2.perris.ca.da.uu.net > daemon.log.1:Dec 25 21:53:52 goteach wu-ftpd[11280]: connect from > www.gis.minsk.by > > > Someone hack my debian box and replace some binaries. The one I found is > sshd. How the hell did they hack in? > > What can you tell from this log? > >

---

- ***Next message:*** [letterhead: "Re: how did someone hack in my machine?"](#)
- ***Previous message:*** [Paul B. Johnson: "repeated SYN packets to port 80"](#)
- ***In reply to:*** [Tony: "how did someone hack in my machine?"](#)
- ***Next in thread:*** [letterhead: "Re: how did someone hack in my machine?"](#)
- ***Reply:*** [letterhead: "Re: how did someone hack in my machine?"](#)
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)