

## Re: Possible compromise ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-01/0123.html>

---

**From:** Paul Schenkeveld (*fb-security\_at\_psconsult.nl*)

**Date:** 01/28/04

Date: Wed, 28 Jan 2004 00:49:26 +0100

To: security at FreeBSD <freebsd-security@freebsd.org>

Hi Peter,

On Tue, Jan 27, 2004 at 10:15:10PM +0100, Peter Rosa wrote:

>

> *Thanks for pointing me. But lastlogin returns only local and only few last*

> *connects.*

> *If I understand well, the bottom of lastlogin is the oldest. So may be, that*

> *connections was done in the deep past.*

Every login gets logged to wtmp, but wtmp gets rotated by newsyslog. BTW, oldest logins are at the top of the file but the last(1) command reads the file backwards for convenience.

/var/log/astlog holds one record for every user that ever logged in into the system with the time and date, tty line and remote host of that last login. It never gets truncated so that's why it's normal to see entries for tty0 and tty1 there even if these ttys have been disabled afterwards.

I know of no standard program to list the entire lastlogin file (/bin/login only shows your own record when logging in) so I've thrown a few bytes in the right order to visualize its contents.

Just compile it with "cc -o showlast showlast.c"

There's a uuencoded copy of the source at the end just in case your mailer scrambles the listing.

Regards,

Paul Schenkeveld, Consultant  
PSconsult ICT Services BV

*/\* showlast.c – show contents of lastlog \*/*

```
#include <sys/types.h>
```

```
#include <fcntl.h>
```

## FreeBSD–Security: Re: Possible compromise ?

```
#include <pwd.h>
#include <stdio.h>
#include <utmp.h>

#define LASTLOG "/var/log/lastlog"

int
main(int argc, char *argv[])
{
    struct lastlog lbuf;
    struct passwd *pw;
    int fd, n;
    uid_t uid = 0;
    if ((fd = open(LASTLOG, O_RDONLY)) < 0) {
        perror(LASTLOG);
        exit(1);
    }
    printf("Username UID Line Remote host Date/time\n");
    printf("-----
    "-----\n");
    while ((n = read(fd, &lbuf, sizeof(lbuf))) == sizeof(lbuf)) {
        if (lbuf.ll_time > 0) {
            pw = getpwuid(uid);
            printf("%-16.16s %5d %-*.*s %-*.*s %s",
                pw ? pw->pw_name : "(unknown)",
                uid,
                UT_LINESIZE, UT_LINESIZE, lbuf.ll_line,
                UT_HOSTSIZE, UT_HOSTSIZE, lbuf.ll_host,
                ctime(&lbuf.ll_time));
        }
        uid++;
    }
    close(fd);
    switch (n) {
        case -1:
            perror(LASTLOG);
            exit(1);
        case 0:
            break;
        default:
            fprintf(stderr, "%s: corrupted\n", LASTLOG);
            exit(1);
    }
    exit(0);
}

begin 644 showlast.c
M+RH@<VAO=VQA<W0N8R`M(-H;W<@8V]N=&5N=',@;V8@;&%S=&QO9R`J+PH*
M(VEN8VQU9&4@/'-Y<RJT>7!E<RYH/@HC:6YC;'5D92`9F-N=&PN:#X*(VEN
M8VQU9&4@/'!W9"YH/@HC:6YC;'5D92`<W1D:6\N:#X*(VEN8VQU9&4@/'5T
M;7`N:#X*"B-D969I;F4)3$%35$Q/1PDB+W9A<B]L;V<O;&%S=&QO9R(*"FEN
```

Re: Possible compromise ?

FreeBSD-Security: Re: Possible compromise ?

M= IM86EN\*&EN=!A<F=C+!C:&%R("IA<F=V6UTI"GL\*(" @('T<G5C="!L
M87-T;&]G(&QB=68["B`@("S=)U8W0@<&%S<W=D("IP=SL\*(" @(&EN="!F
M9"P@;CL\*(" @('5I9%]T('5I9")(#["B`@("I9B`H\*&9D(#T@;W!E;BA,
M05-43\$]'+!/7U)\$3TY,62DI(#P@,"D@>PH)<&5R<F]R\*\$Q!4U1,3T<L.PH)
M97AI="@Q\*3L\*(" @("T\*(" @('R:6YT9B@B57-E<FYA;64@(" @(" @(" @
M(%5)1"!,:6YE(" @("!296UO=&4@:&]S=" @(" @(\$1A=&4O=&EM95QN(BD[
M"B`@("P<FEN=&8H(BTM+2TM+2TM+2TM+2TM+2T@+2TM+2T@+2TM+2TM+2T@
M+2TM+2TM+2TM+2TM+2TM+2`B"@D@("B+2TM+2TM+2TM+2TM+2TM+2TM+2TM
M+2TM7&XB\*3L\*(" @('=H:6QE(" @H;B`])E860H9F0L("9L8G5F+"!S:7IE
M;V8H;&)U9BDI\*2`]/2!S:7IE;V8H;&)U9BDI(L\*"6EF("AL8G5F+FQL7W1I
M;64@/B`P\*2!["@D@(" @<'<@/!G971P=W5I9"AU:60L.PH)(" @('R:6YT
M9B@B)2TQ-BXQ-G,@)35D("4M\*BXJ<R`E+2HN\*G,@)7,B+`H)"2`@('W(#@
M<'<M/G!W7VYA;64@.B`B\*5N:VYO=VXI(BP\*"0D@("U:60L"@D)(" @551?
M3\$E.15- )6D4L(%547TQ)3D5325I%+"!L8G5F+FQL7VQI;F4L"@D)(" @551?
M2\$]35%- )6D4L(%547TA/4U1325I%+"!L8G5F+FQL7VAO<W0L"@D)(" @8W1I
M;64H)FQB=68N;&Q?=&EM92DI.PH)?0H)=6ED\*RL["B`@("!"B`@("C;&]S
M92AF9"D["B`@("S=VET8V@\* &XI('L\*"6-A<V4@+3\$Z"@D@(" @<&5R<F]R
M\*\$Q!4U1,3T<L.PH)(" @(&5X:70H,2D["@EC87-E(#`Z"@D@(" @8G)E86L[
M"@ED969A=6QT.@H)(" @(&9P<FEN=&8H<W1D97)R+"`B)7,Z(&-O<G)U<'1E
M9%QN(BP@3\$%35\$Q/1RD["@D@(" @97AI="@Q\*3L\*(" @("T\*(" @(&5X:70H
&,"D["GT\*
`

end

frebsd-security@frebsd.org mailing list
http://lists.frebsd.org/mailman/listinfo/frebsd-security

To unsubscribe, send any mail to "frebsd-security-unsubscribe@frebsd.org"