

Re: Opieaccess file, is this normal?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-06/0058.html>

From: Jilles Tjoelker (*jilles_at_stack.nl*)

Date: 06/24/04

Date: Thu, 24 Jun 2004 15:57:48 +0200

To: Didier Wiroth <didier.wiroth@mcesr.etat.lu>

On Tue, Jun 22, 2004 at 05:55:55PM +0200, Didier Wiroth wrote:

> *I'm trying to setup one-time passwords on freebsd5.2.1*

> *>From what I've read so far, if the user is present in opiekeys, the
> opieaccess file determines if the user (coming from a specific host or
> network) is allowed to use his unix password from this specific network.*

> *As my opieaccess file is empty and the default rule (as mentionned in the
> man file) is deny, I should not be able to get an ssh shell with my standard
> unix password.*

> *I've made a test on test machine running ssh (version sshd version
> OpenSSH_3.6.1p1 FreeBSD-20030924).*

> *The opiekey contains one user, me actually.
> The opieaccess file is empty so (by default) unix password should not be
> allowed when connecting through ssh.*

> *I enter a few times "enter" and sshd switches to the next authentication
> method "password".
> Now I can enter my standard password and I'm logged in, even if I should
> only be allowed to use the opie passwords.*

> *Why? Isn't this a bug?*

>

> *Here is the ssh -v output:*

>

[snip]

> *debug1: Authentications that can continue:
> publickey,password,keyboard-interactive
> debug1: Next authentication method: publickey
> debug1: Trying private key: /home/didier/.ssh/identity
> debug1: Trying private key: /home/didier/.ssh/id_rsa
> debug1: Trying private key: /home/didier/.ssh/id_dsa
> debug1: Next authentication method: keyboard-interactive
> otp-md5 300 pw9999 ext
> Password:*

FreeBSD-Security: Re: Opieaccess file, is this normal?

```
> otp-md5 300 pw9999 ext
> Password [echo on]:
> debug1: Authentications that can continue:
> publickey,password,keyboard-interactive
> otp-md5 300 pw9999 ext
> Password:
> debug1: Authentications that can continue:
> publickey,password,keyboard-interactive
> otp-md5 300 pw9999 ext
> Password:
> debug1: Authentications that can continue:
> publickey,password,keyboard-interactive
> debug1: Next authentication method: password
> didier@localhost's password:
> debug1: Authentication succeeded (password).
[snip]
```

Use PasswordAuthentication no in /etc/ssh/sshd_config. The PasswordAuthentication doesn't obey many PAM restrictions.

ChallengeResponseAuthentication yes gives the "Password:" prompt and will allow unix passwords if permitted.

For this reason, PasswordAuthentication no has become the default in -CURRENT.

--

Jilles Tjoelker

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

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