

RE: SecurID Question

Source: http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2006-02/msg00005.html

- *From:* "Chris Macneill" <chris.macneill@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 1 Feb 2006 22:37:18 -0000
-

Asif's advice to use RADIUS is OK in theory; however SecurID sometimes doesn't work too well with RADIUS. It entirely depends on the RADIUS Client implementation.

I have never tried RADIUS and SecurID with OpenSSH, so I don't know how well it works in practice. I'm just issuing a word of caution.

The problem stems from the fact that the SecurID ACE/Server doesn't just send a binary response of authentication accepted or denied; it can have two intermediate states, New PIN Mode and Next Tokencode Mode, which require the RADIUS Server and Client to go through a specialised exchange of prompts and responses. It was just these extended prompts and responses that gave me the most headaches when integrating the SecurID API directly with OpenSSH and getting it to work in Privilege Separation mode.

For the most part RADIUS servers and certainly the one embedded in ACE/Server function well these days. However, just last week I was using Cisco's latest VPN Client v4.7 with RADIUS and SecurID, the Next Tokencode mode interface is OK, but the New PIN mode is horribly broken and instead of prompting "Enter PASSCODE:", it seems to be hard coded to prompt "Enter Password:". The correct prompt is supplied by the ACE/Server RADIUS Server when the authentication channel is established; it seems Cisco are just ignoring it.

I'm not saying RADIUS won't work in this scenario, but just be sure to test the interface fully and be happy that it delivers what you want, not just a kludgy interface that may cause confusion to users.

In my experience many people have cut corners when implementing SecurID and not bothered to properly handle New Pin and Next Tokencode modes, most have regretted it and had to re-engineer the solution later. It's not a major problem when you have a small user base, but when you get into the realms of hundreds of users, the support overhead of having to reset PINs and Tokens on behalf of users, instead of them being able to handle it interactively with the interface, can become significant.

Chris Macneill
-----Original Message-----

RE: SecurID Question

From: Asif Iqbal [<mailto:iqbala-secureshell@xxxxxxxxxxxxx>]

Sent: 01 February 2006 15:10

To: secureshell@xxxxxxxxxxxxxxxxxxxxx

Subject: Re: SecureID Question

1. Download and compile latest OpenSSH w/ PAM on your host.
2. Start the radius daemon on your SecurID server.
3. Compile radius auth pam library on your host from the source code found in freeradius website
4. Choose a radius key for the host and place it in /etc/raddb/server page with the IP of the SecurID server
5. Add the host using ACE Client and place the same radius key there
6. Set UsePAM to yes on your host's sshd_config file. Privilege Separation should work just fine
7. Send a HUP--no need to kill and restart--to your parent ssd process if you already have the pam enabled sshd running. Otherwise start the just compiled one. If you do not want to kill your existing sshd yet just do make (and make install yet) and run the newly compiled sshd on a different (not port 22) port.

Now you can ssh (on that non-default port may be) to your host using securid. It is using the radius port on the securid server to authenticate against the securid database.

Thanks

On Thu, Jan 19, 2006 at 10:17:34AM, Steve Calderoni wrote:

Hello all,

I have openssh installed and am having a small problem that I hoping someone will be able to help with.

When I log into my openssh server I then try to ssh to a server from there

that uses SecureID. The session connects then the banner text appears and from there it should display the PASSCODE: prompt but never makes it. Directly from the server I can log in just fine. It just does not work

from

within a session.

If anyone has any ideas that may help I would appreciate it!

Thanks,

Steve

RE: SecurID Question

RE: SecurID Question

Don?t just search. Find. Check out the new MSN Search!
<http://search.msn.click-url.com/go/onm00200636ave/direct/01/>

--

Asif Iqbal
PGP Key: 0xE62693C5 KeyServer: pgp.mit.edu
"..there are two kinds of people: those who work and those who take the
credit...try
to be in the first group;...less competition there." – Indira Gandhi

--

No virus found in this outgoing message.
Checked by AVG Anti-Virus.
Version: 7.1.375 / Virus Database: 267.14.25/247 – Release Date: 31/01/2006

RE: SecurID Question

3