

SecurityFocus Secure Shell: RE: Multiple authorized\_keys2 files or how to achieve same effect.

## RE: Multiple authorized\_keys2 files or how to achieve same effect.

*Source:* [http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure\\_Shell/2005-09/0020.html](http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2005-09/0020.html)

---

**From:** Tay, Gary (*Gary\_Tay\_at\_platts.com*)

**Date:** 09/05/05

Date: Mon, 5 Sep 2005 10:18:12 +0800

To: "Jeremy Eder" <jeder@invision.net>, <seureshell@securityfocus.com>

If you are looking for docs on building Centralized LDAP Authentication with host access (netgroups) control, and user command execution (sudoers) control, you may find my HOWTOs useful, or not at all.

<http://web.singnet.com.sg/~garyttt/>

Gary

-----Original Message-----

From: Jeremy Eder [mailto:jeder@invision.net]

Sent: Friday, September 02, 2005 9:53 PM

To: seureshell@securityfocus.com

Subject: RE: Multiple authorized\_keys2 files or how to achieve same effect.

Thank you Jayson and Johan for your suggestions, they are exactly what I was looking for.

I will investigate both LDAP/MySQL with PAM and freeradius.

Are there any docs on your technique, Jayson ?

Other than man pages and freeradius.org... ?

Sincerely,

Jeremy Eder

-----Original Message-----

From: Jayson Anderson [mailto:sonick@sonick.com]

Sent: Friday, September 02, 2005 12:10 AM

To: seureshell@securityfocus.com; Jeremy Eder

Subject: Re: Multiple authorized\_keys2 files or how to achieve same effect.

RE: Multiple authorized\_keys2 files or how to achieve same effect.

SecurityFocus Secure Shell: RE: Multiple authorized\_keys2 files or how to achieve same effect.

Good recommendations so far, but I can't help but think with hundreds of hosts, and granularity of control spanning one-off host, global host, /etc/sudoers and more than you've not listed and more that you've not yet encountered: It's time to think about Radius.

I've scaled freeradius to levels that hurt a lot of vendor's feelings, on \$500 worth of DIY server hardware to boot; I enthusiastically recommend it. Performance alone it is the champ, without even mentioning the obnoxious amount of functionality options beyond most if not all commercial offerings. I definitely think freeradius would make you keyboard-smashing mad during planning and integration, and once integrated will slash an unbelievable amount of minutia and trouble out of your yearly operations tasks in addition to adding incredible amounts of applied and available user control. Better yet, all user activity [licit and otherwise] will become centralized where you can more effectively manage it (let alone even NOTICE it vs. your current arrangement). Just make sure to become a stickler about putting AAA on everything that even LOOKS at your networks. The day I resigned from INS (version 1.0) was shortly after the day they placed me in a radius-enabled, deployment-lax environment and said 'cull it all and fix it'.

Unless I misunderstood your obstacles which I sometimes do in grand fashion, I think it's time to bang out a couple freeradius servers once and for all; then enable AAA on everything with unwavering completeness. Massaging the groups and configs will evolve naturally over time; no need to perfect access to every single binary prior to rollout.

Best Regards,  
Jayson

On Thu, 2005-09-01 at 10:49 -0400, Jeremy Eder wrote:

- > *My situation: multiple admins needing root on hundreds of boxes.*
- >
- > *Currently: using pubkeyauth on openssh (mostly bsd but linux and solaris too)*
- >
- > *Goal: ease add/remove of credentials from machines (one-off or globally in our network)*
- >
- > *Each server may have a completely different (and still valid) list of users in the authkeys2 file.*
- >
- > *Instead of getting messy with sed/cat/grep...I began to research if it was possible to have multiple authorized\_keys2 files, or at least be able to put directives to separate public key files in the global authorized\_keys2. This would make the management of my setup much easier...*
- >

RE: Multiple authorized\_keys2 files or how to achieve same effect.

SecurityFocus Secure Shell: RE: Multiple authorized\_keys2 files or how to achieve same effect.

- > *Something like...*
- >
- > *AuthorizedKeysFile .ssh/authorized\_keys2*
- > *AuthorizedKeysFile .ssh/user1*
- > *AuthorizedKeysFile /ssh/user2*
- >
- > *Etc etc...*
- >
- > *Then I can control access to the box simply by creating or deleting that*
- > *file and one line in the conf.*
- >
- > *Am I looking in the right direction ? I haven't yet discovered a way to*
- > *do this under openssh; however .ssh/authorization under ssh2 seems to*
- > *provide the exact feature I am thinking of. Not an option...*
- >
- > *Is this possible ? Is there some other practice that is more accepted*
  
- > *that I'm not aware of ?*
- >
- > *Thanks for your help.*