

(mis)using RBAC...

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2005-04/0003.html>

From: Jonathan Katz (jonathan.katz_at_gmail.com)

Date: 04/12/05

Date: Tue, 12 Apr 2005 14:19:51 -0500

To: focus-sun@securityfocus.com

All,

I was recently charged with setting up RBAC so that the group I work with will 'su to root' less often.

The first project I've picked is to either establish a role and/or profile that will allow a normal user to start and stop our webserver. Here is what I came up with, bypassing the concept of a 'role'...

1) I created a profile called "Web Administration"
in /etc/security/prof_attr
Web Administration:::Role for restarting webserver::

2) I gave the profile the ability to run the start and stop webserver scripts as root:
in /etc/security/exec_attr
Web Administration:suser:cmd:::/opt/app/iplanet/https-myserver/start:uid=0
Web Administration:suser:cmd:::/opt/app/iplanet/https-myserver/stop:uid=0

3) I then added the role to my account on the server in /etc/user_attr:
jkatz:::type=normal;profiles=Web Administration,Basic Solaris User

4) Finally, I changed my shell to /bin/pfsh. Now, with my regular user account I can start and restart our webserver.

My questions are, is this a normal practice (are there other people doing it) and is it supported? What unintended consequences am I missing? I understand that if a user's account is compromised, the webserver services can be stopped and started at-will. I also understand that our sysadmin group will be restricted to using pfsh/pfksh/pfsh and cannot use bash or tcsh (although we can still leave those set, type 'exec pfsh' and then do what we need to do as the Profile.)

Thanks!

--

(mis)using RBAC...

SecurityFocus SUN: (mis)using RBAC...

-Jon

Jonathan Katz -- J. Random BOFH