

Re: SUN Solaris User

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2001-11/0015.html>

From: Tony Moran (focus-sun@ayahuasca.net)

Date: 11/10/01

Date: Sat, 10 Nov 2001 02:29:29 +0000 (GMT)
From: Tony Moran <focus-sun@ayahuasca.net>
To: Paul Julias <pjulias@cbz.co.zw>
Subject: Re: SUN Solaris User
Message-ID: <Pine.LNX.4.30.0111100150030.29049-100000@vortex.ukshells.co.uk>

Hi Paul, I guess it depends on the rest of the system and how it is currently configured and permissions arranged. I would probably just create him a normal user account, and assuming the standard network information tools like traceroute and so on are setuid still then he can run the commands he needs as a regular user. I dont think there would be a need to provide him root access. All he needs is ping traceroute and netstat (-rn) if he really only needs to check the situation.

However if the situation changes whereby he is then looking to be allowed to make changes, such as using the route command, then you will want to look into sudo, or set specific facts using setfacl/getfacl. (<http://www.samag.com/documents/s=1151/sam0105g/0105g.htm>)

You may also want to turn on process accounting (

```
/usr/lib/acct/accton /var/adm/pacct
```

)

and then you know what he's been up to. It depends on your paranoia levels :)

U might also be able to leverage Solaris Rolebased Access Control.

<http://www.sun.com/software/whitepapers/wp-rbac/>

You could then create a Role based Rights Profile combining the normal rights of a normal User along with Network Management Rights. At the bottom of <http://www.sun.com/software/whitepapers/wp-rbac/index5.html> theres also a useful comparison between Sudo and RBAC.

To be honest though, if youre the one responsible for network security and this firewall in particular and the administration of the box itself, and he's

SecurityFocus SUN: Re: SUN Solaris User

just a network engineer and not part of the security team then I would not be inclined to provide willy-nilly access to the firewall. If something needs to be checked then it should be requested of you and it would be your responsibility to provide either a timely response to the query or the appropriate fix. You know what network engineers are like – he'll have a hole and route to allow him in from his home before you can say 'Security breach'.

Hope that helps some.. Tony

On Wed, 7 Nov 2001, Paul Julias wrote:

> *To: "focus-sun@securityfocus.com" <focus-sun@securityfocus.com>*
> *From: Paul Julias <pjulias@cbz.co.zw>*
> *Date: Wed, 7 Nov 2001 12:51:42 +0200*
> *Message-ID: <4782AA6D7B40D511A17C0002A55161697A2A64@CBZUNHRE1>*
> *Subject: SUN Solaris User*
>
>
> *I running a Sunscreen Firewall and have been requested to provide system*
> *access to our Networks Engineer who from time to time may want to*
> *troubleshoot comms including routing details. What is the best approach to*
> *creating such a user and what minimum level access should be provided.*
>
> *Regards*
>
> *Paul Julias*
>
>
--

"It is not enough to curse the darkness.....it is necessary to light a candle" <http://www.amnesty.org>

"Man, once surrendering his reason, has no remaining guard ..against absurdities the most monstrous, and like a ship without a rudder, is the sport of every wind. With such persons, gullibility, which they call faith, takes the helm of reason, and the mind becomes a wreck." Thomas Jefferson.

-
- **Previous message:** [Sean Boran: "RE: SUN Solaris User"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)