

Tru64-UNIX-Managers: SUMMARY: Allow group of users to su to a locked administrative account.

SUMMARY: Allow group of users to su to a locked administrative account.

Source: <http://unix.derkeiler.com/Mailing-Lists/Tru64-UNIX-Managers/2005-01/0005.html>

DavidStacks1964_at_netscape.net

Date: 01/06/05

Date: Thu, 06 Jan 2005 11:03:29 -0500

To: tru64-unix-managers@ornl.gov

Want to thank all who responded with suggestions. Most everyone including HP Support has suggested using SUDO. Only other ideal came from Tom. I've included his suggestion below. Thanks Tom.

I've been on break or would have responded earlier. We have a solution that we use that involves altering the system-wide login files.

Lets assume that your accounts are orauserone and secondora.

In /etc/profile, add the following up at the top:

```
----- snip ----- snip ----- snip ----- snip ----- snip -----
for logname in orauserone secondora
do
  [ `logname` = $logname ] && { echo "unauthorized login"; kill -9 $$;
}
done
----- snip ----- snip ----- snip ----- snip ----- snip -----
```

In /etc/csh.login, add the following up at the top:

```
----- snip ----- snip ----- snip ----- snip ----- snip -----
foreach logname (orauserone secondora)
  [ `logname` = $logname ] && ( echo "unauthorized login"; kill -9 $$;
)
end
----- snip ----- snip ----- snip ----- snip ----- snip -----
```

This will allow users to su to the account, but not log in directly. It won't keep the DBAs from su-ing form accounts other than oracle, but it solves the problem of direct logins.

I didn't come up with solution, I think it was someone on the mailing list a couple years back. It may be possible to circumvent, but it at least stops our DBAs and ensures that we know who is doing what based on the logs from su.

Hope this helps,

SUMMARY: Allow group of users to su to a locked administrative account.

Tru64-UNIX-Managers: SUMMARY: Allow group of users to su to a locked administrative account.

Tom

--

Tom Webster <webster@ssdpdc.lgb.cal.boeing.com>

davidstacks1964 wrote:

>Hello All!

>

>First want to say that I hope all has had a wonderful holiday season.

>

>Also want to say that I did find one solution to the problem that I have, but the solution was n

>

>Here is the task that I am working on:

>

>I have severel UNIX Tru64 servers with Oracle Administrative accounts. What I want to do, is l

>

>I'll cut and past the solution that I found below, and if anyone knows how to incorporate the us

>

>I have already tried locking a test account then attempting to su to the test account. Per the

>

>Thanks,

>

>David Stacks

>Sr. System Analyst

>Entergy Corp.

>(870) 543-5436

>dstacks@entergy.com

>

>

>

>*****

>

>Solution that I found:

>

>[SUMMARY] Preventing application account access

>

>[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

>[SUMMARY] Preventing application account access

>

>

>

> To: "Tru64-Unix-Managers@xxxxx Gov (E-mail)" <tru64-unix-managers@xxxxxxxx>

> Subject: [SUMMARY] Preventing application account access

> From: "Roberts, Blake" <broberts@xxxxxxxx>

> Date: Thu, 15 Aug 2002 15:40:57 -0500

> Delivered-to: tru64-unix-managers@sws1.ctd.ornl.gov

> Followup-to: poster

> Sender: tru64-unix-managers-owner@xxxxxxxx

> Thread-Index: AcJEigcoPesPw3PMQeWW+Hymt0/x0AAAShEgAAQnmwA=

> Thread-Topic: Preventing application account access

>

>

>

>Thanks goes to Chris Ford (Chris.Ford@acxiom.com)

>

>To do this properly, there is no easy way. You have to make an addition to the profile of

> each user (will probably add it to /etc/skel) and call a script which reads a file similar

> to /etc/securettys. I tested the solution, and it works like a champ!

>

>Best regards,

>--Blake Roberts

>UNIX Systems Administrator

>ERCOT-Austin

SUMMARY: Allow group of users to su to a locked administrative account.

Tru64-UNIX-Managers: SUMMARY: Allow group of users to su to a locked administrative account.

```
>512.225.7178
>512.695.5071 (cell)
>
>
>-----Original Message-----
>From: Roberts, Blake
>Sent: Thursday, August 15, 2002 1:42 PM
>To: Tru64-Unix-Managers@Ornl. Gov (E-mail)
>Subject: [ADDENDUM] Preventing application account access
>
>
>I forgot to mention, I have sudo installed on the system, but I have not found a way for it
> to prompt me for the password of the administrative account. Since, by default anyway,
> it prompts for your own password, if the user's password is compromised (by writing it down
> and leaving it on their desk, etc), there is no way to keep people away from the big accounts.
>
>--Blake
>
>
>-----Original Message-----
>From: Roberts, Blake
>Sent: Thursday, August 15, 2002 1:32 PM
>To: Tru64-Unix-Managers@Ornl. Gov (E-mail)
>Subject: Preventing application account access
>
>
>Folks,
>
>I'm running a Tru64 5.1 PK5 Enhanced Security environment. Per a new (and decent) password
> policy that is being implemented, I need to restrict the application admin accounts so that
> they will su from a personal account to the administrative account (such as oracle), similar
> to what you need to do if root is locked down properly.
>
>My problem is, in base security, if I lock the account, you can log in as a user, then su to
> it just fine. In enhanced security, you can't do that. It needs to be unlocked to be able
> to log into it. Does anyone know of a trick, edauth flag, etc, that needs to be set for the
> account to be able to be su'd to, but not directly logged in to?
>
>Best regards,
>
>--Blake Roberts
>UNIX Systems Administrator
>ERCOT-Austin
>512.225.7178
>512.695.5071 (cell)
>
>
>
>-----
>Switch to Netscape Internet Service.
>As low as $9.95 a month -- Sign up today at http://isp.netscape.com/register
>
>Netscape. Just the Net You Need.
>
>New! Netscape Toolbar for Internet Explorer
>Search from anywhere on the Web and block those annoying pop-ups.
>Download now at http://channels.netscape.com/ns/search/install.jsp
>
>-----
Switch to Netscape Internet Service.
As low as $9.95 a month -- Sign up today at http://isp.netscape.com/register
Netscape. Just the Net You Need.
```

SUMMARY: Allow group of users to su to a locked administrative account.

Tru64–UNIX–Managers: SUMMARY: Allow group of users to su to a locked administrative account.

New! Netscape Toolbar for Internet Explorer

Search from anywhere on the Web and block those annoying pop-ups.

Download now at <http://channels.netscape.com/ns/search/install.jsp>