

Re: Local Admin

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-06/msg00039.html>

- *From:* Billy Beaudoin <wrbeaudo@xxxxxxxxxxxxx>
 - *Date:* Fri, 02 Jun 2006 10:32:08 -0400
-

What it sounds like you are trying to determine is whether or not the administrator account has been changed while the OS is offline. That's a might tricky. The only thing I can up with was periodically dumping the hashes and info on the administrator out of the SAM and diffing it. Which would mean you'd have to keep all that info somewhere, which would be a security hole, but we'll ignore that for a moment. If you cron'd up something that ran with system permissions you could dump this key from each of the machines every day and do a compare.

HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users\000001F4

IF you decide that people booting off CD's and mucking with clients is more of an issue than storing hashes of all of the local admin accounts, read up on this site for how the SAM is structured:

<<http://www.beginningtoseethelight.org/ntsecurity/>>

Billy

—On Thursday, June 01, 2006 10:43 PM -0400 Steven <steven@xxxxxxxxxxxxx> wrote:

Hello,

Let me try a response to your question and precursor it with my assumptions about your environment.

I am assuming that you are currently in an Active Directory (AD) environment and that your users are local administrators of their own machines once logged into their domain account. My next guess is that you have a local administrator account on each machine and this is the one you are interested in watching.

To the best of my knowledge there is no way to do this through AD. The local account on the machine is separate from your AD and resides only on the local installation. The only way that I know of that you could be notified of a change is if you have some kind of additional log monitor. This could alert you to password changes (event id 628) or attempted(failed) changes (event id 627). You might also want to look for account created/deleted events in your logs as well.

Depending on the size of your environment and number of your staff I

Re: Local Admin

would not say it's unreasonable or impossible to set administrative BIOS passwords on all of the machines. This can go a decent way to protecting machines from being booted from a CD. It of course will not stop a determined attacker that's in front of the box.

Hope this helps.. just post back if you have more questions.

Steven

----- Original Message ----- From: "Mohamed Abdel Kader"
<mak.pen@xxxxxxxx>
To: <pen-test@xxxxxxxxxxxxxxxxxxxx>
Sent: Thursday, June 01, 2006 4:58 AM
Subject: Local Admin

Hello List,

I was wondering if their is a way to monitor if someone changed the local Administrator, on his/her computer, through an active directory, and how can

This be prevented in large organizations. It is not practical to change the

Bios password on all of the computer and the boot order and lock the Machines; at least in this case.

Thanks all...

----- This List Sponsored by: Cenzic

Concerned about Web Application Security?
Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software

Re: Local Admin

(Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.

This List Sponsored by: Cenzic

Concerned about Web Application Security? Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.

This List Sponsored by: Cenzic

Concerned about Web Application Security? Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.
