

Re: Detecting Brute-Force and Dictionary attacks

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2006-11/msg00008.html>

- *From:* Cy Schubert <Cy.Schubert@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 10 Nov 2006 05:43:41 -0800
-

In message <9555a4b00611080922u79c38d7dl8a7132cb7f299ec2@xxxxxxxxxxxxxxxx>, "Sebastian Veenstra" writes:

Hi,

I didn't read the whole discussion about this issue but I came up with an idea which might be useful to detect brute force attempt. By storing the passwords a certain user has used in the past along with the current password you could be able to compare to password (by pattern matching) used at the login attempts with the passwords list. If the password used differs significantly (this excludes typos) from the entries in the password list, there could be a possible brute force attempt. The reason for storing the previous passwords is that people tend to use every password they've used in the past when they forgot their password. Maybe this idea can be used along with the other methods of detecting brute force attempts. Anyway, it's just a random thought.

In many jurisdictions this would be an invasion of privacy and against the law. Not only that but a security exposure too. For example, people tend to use similar passwords, even the same passwords for various applications and machines. Once a sysadmin knows someone's password the victim could be impersonated without detection. Whereas su commands, access to Oracle databases, and other services the sysadmin would not normally have access to would require work on the part of the sysadmin to gain entry into and these attempts would surely be logged and hopefully detected. Logging people's passwords is a bad idea.

—
Cheers,
Cy Schubert <Cy.Schubert@xxxxxxxxxxxxxxxx>
Web: <http://www.komquats.com> and <http://www.bcbuilder.com>
FreeBSD UNIX: <cy@xxxxxxxxxxxxx> Web: <http://www.FreeBSD.org>
BC Government: <Cy.Schubert@xxxxxxxxxxxx>

"Lift long enough and I believe arrogance is replaced by

Re: Detecting Brute-Force and Dictionary attacks

humility and fear by courage and selfishness by generosity
and rudeness by compassion and caring."
— Dave Draper