

Re: privilege escalation techniques

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-01/0132.html>

From: Chuck Herrin (*me_at_chuckherrin.com*)

Date: 01/17/05

Date: Mon, 17 Jan 2005 10:16:14 -0600

To: Dan Rogers <pentestguy@gmail.com>

Hi Dan,

One of my favorite methods is to gain local admin via a linux boot disk (like ntchpw), install a keylogger, then break something or disable a needed service and call the help desk. Since they usually can't fix anything detailed, the 2nd level tech usually comes around and logs in with an admin account to take a look.

Sometimes the responding tech is Domain Admin (yay!), but in any case his are good credentials to have, and a nice place to start.

You can skip a step and just go with a hardware keylogger, but I'm wary of doing that before asking an admin to come over. Also, test your keylogger against whatever A/V software they're using before you install it there. Antivirus alerts = not subtle.

Those are the most fun assignments – Enjoy!

Chuck Herrin
www.chuckherrin.com

Quoting Dan Rogers <pentestguy@gmail.com>:

> *Hi List,*
>
> *I have been asked to test the network security of my organisation from*
> *an internal perspective. My boss has not been particularly specific in*
> *his requirements (other than asking that I don't break any operational*
> *infrastructure) so I can approach the problem from whichever way I*
> *deem most appropriate.*
>
> *I suspect the first thing I will attempt is privilege escalation*
> *techniques from a workstation with a domain user account to see if I*
> *can install my own software/toolset. Can anyone suggest any good*
> *whitepapers or tools that I can use to get a head start?*
>
> *I intend to follow this up by scanning/targeting critical parts of our*

SecurityFocus Penetration: Re: privilege escalation techniques

- > *infrastructure – domain controllers, mail servers, routers etc.*
- > *However, I am interested to know what other people would do when given*
- > *free reign to identify internal weaknesses – so how should I approach*
- > *this? This is not an 'audit' exercise, as I will not be given access*
- > *to server/infrastructure configurations.*
- >
- > *Any advise on this appreciated.*
- >
- > *Dan*
- >