

Re: System Security Audits

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-12/0093.html>

From: Dave Piscitello (dave_at_corecom.com)

Date: 12/11/03

Date: Thu, 11 Dec 2003 07:52:39 -0500

To: Peteris Krumins <newsgroups@lf.lv>, pen-test@securityfocus.com

I agree that chasing malware, trojans, viruses, etc. makes CD burning difficult.

W/R/T permissions, auditing, user rights assignment and other local and group policies, you might also want to look at the Center for Internet Security's Auditing Tools and security templates (<http://www.cisecurity.org>).

Lastly, you didn't mention security patches and hot fixes. Shavlik has an excellent tool HFnetchkPro, for individual and networked patch management at <http://www.shavlik.com>. It's license free for up to 10 PCs. They also have an enterprise policy checker and accounts checker. These are the folks who developed MBSA for Microsoft.

At 12:00 AM 11/29/2003 +0200, Peteris Krumins wrote:

- > Hello,
- >
- > I have a question about doing system (Windows) security
- > audits.
- > By system security audits I mean things like checking if computer
- > is free of malware, trojans, viruses, if user has appropriate
- > permissions (not too high or to say if user has restrictive
- > permissions) etc.
- >
- > I have a couple of ideas which i could use, one is to create
- > an universal CD with all the stuff needed. Everything is on the
- > CD, nothing will be installed on the client's computer.
- > The Audit Team just puts CD in, runs applications and that's it.
- >
- > The other is to boot from a CD on the client's computer
- > which would bring us to some different environment (probably
- > linux). As booted mount the filesystems and do all the
- > audit stuff from such environment.
- >
- > Or, please, suggest any other methods that could be used.
- >
- >

SecurityFocus Penetration: Re: System Security Audits

>*P.Krumins*

>

>

>-----

>-----
