

Re: Odd situation, advice needed on penetration test results

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-03/0150.html>

From: Raven Alder (raven@oneeyedcrow.net)

Date: 03/26/03

Date: Wed, 26 Mar 2003 17:41:59 -0500
From: Raven Alder <raven@oneeyedcrow.net>
To: pen-test@securityfocus.com

Heya --

Quoth Ido Dubrawsky (Wed, Mar 26, 2003 at 03:19:32PM -0500):
> *I would recommend that the your client unplug the power from the*
> *system (hopefully the intruder has not setup a logic bomb that*
> *triggers if the network interface goes down). Then it's a matter of*
> *getting the system into a state where imaging the drive(s) can be*
> *done.*

Also, if they want to capture some of the forensic information that's lost with a power-cycle (running process list, etc), just yank the network connection. If you want to ensure that the Ethernet interface stays up, leave it connected to a hub with no other connections and no uplink. Or just make yourself a loopback plug (connect pin 1 to pin 3, pin 2 to pin 6, crimp and go -- <http://www.juniper.net/techpubs/software/nog/nog-interfaces/html/fe-ge-loopback25.html> has diagrams) and insert that in place of the network cable.

Of course, this still won't save you if the software is checking reachability to a given external site before doing whatever self-destructive thing, or if the momentary drop in connectivity when you switch cables is enough to set it off. But it does keep your compromised system isolated from the rest of the network while you begin your forensic analysis. (Or while your client does -- touching that system after you know it's been compromised by someone else may be opening yourself up to some sort of liability. I am not a lawyer -- but it would make me nervous, unless this sort of situation was accounted for in my contract with the client. If they just signed you on for a pen-test, I'd probably tell the client exactly what I had found and what I had done to find it, and let them make the decisions about what they wanted to do from there.)

Cheers,
Raven

SecurityFocus Penetration: Re: Odd situation, advice needed on penetration test results

top spam and e-mail risk at the gateway.

SurfControl E-mail Filter puts the brakes on spam & viruses and gives you the reports to prove it. See exactly how much junk never even makes it in the door. Free 30-day trial:

<http://www.surfcontrol.com/go/zsfpt11>