

RE: [fw-wiz] Security Audit and Priorities

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-07/0052.html>

From: Bob Wanamaker – Avant Systems, Inc. (*rlw_at_avantsystems.com*)

Date: 07/14/03

To: "'Paul Ammann'" <pammann@execomm.net>, <firewall-wizards@honor.icsalabs.com>

Date: Mon, 14 Jul 2003 11:46:54 -0400

Greetings, Paul.

Congrats on the new gig!

Learn your network.

I'd not worry too much about IDS at this point. Harden servers; understand your firewall, routers, switches [I've seen folks attempt to do security via VLAN's – things like that are not immediately obvious if you don't have access to the original network designer]; learn what your workstation configs are like; spend some quality time with a sniffer – during low-use and peak-use times; pore over every log file you can find; examine-test backup/recovery strategies and tools.

Diagram how each "application level" network conversation takes place, and what devices/processes are involved: e.g., a workstation sends an e-mail: it hits the private mail server queue, is removed by content filtering software, is scanned for virii, is dropped off in the queue, is tagged for delivery to remote, transferred to gateway smtp server, etc. Then start asking the questions about who has access to that e-mail at each point in your diagram. Remember that we're not only concerned with securing machines, but with securing data. Then ask if that conversation is appropriate on your network.

As you do more and more of this, you'll naturally be starting an audit: e.g., as you go through logs, you'll notice which are missing; you'll notice if they're archived; you'll notice if you have the tools to pull them apart; you'll notice if timestamps are coordinated – in short, you'll discover if logging is adequate to put together a picture of who is accessing what resources when and how.

Once you get a solid grasp of what constitutes normal traffic and normal ops, you can start really tightening things down, and then consider implementing an IDS to help you keep things tidy.

Hope that helps,

Firewall-Wizards: RE: [fw-wiz] Security Audit and Priorities

Bob

-----Original Message-----

From: firewall-wizards-admin@honor.icsalabs.com
[mailto:firewall-wizards-admin@honor.icsalabs.com]On Behalf Of Paul
Ammann
Sent: Sunday, July 13, 2003 12:10 PM
To: firewall-wizards@honor.icsalabs.com
Subject: [fw-wiz] Security Audit and Priorities

Thanks to everyone for sharing your thoughts. I really do appreciate the help.

I was at the bookstore last night and found 3 books that'll provide me immediate solutions in the short term, and help plan long term:

- Linux Security Cookbook
- Building Secure Servers with Linux
- Hardening Cisco Routers

All books are from O'Reilly. It's one thing to be a firewall admin and write and maintain security policies. I've never given much thought to Oracle, Linux and Cisco routers before. But it is a huge opportunity to learn. ;-) And I bought "Honeypots: Tracking Hackers" by Lance Spitzner.

While I'm thinking about it, I know the company doesn't have a IDS system in place. I was looking at Snort as a possibility. Has anyone had experience with Snort?

Paul

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>