

Firewall-Wizards: Re: [fw-wiz] I wonder, how to test..

## Re: [fw-wiz] I wonder, how to test..

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-07/0218.html>

---

**From:** Kevin Sheldrake ([kev\\_at\\_electriccat.co.uk](mailto:kev_at_electriccat.co.uk))

**Date:** 07/30/04

To: "Meindert Uitman" <[meindert.uitman@avic.nl](mailto:meindert.uitman@avic.nl)>, "firewall-wizards@honor.icsalabs.com" <[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)>  
Date: Fri, 30 Jul 2004 12:03:01 +0100

Hello

It depends on how thorough you want to be and how much you already know.

I would suggest you use nmap ([www.insecure.org](http://www.insecure.org)) to scan every box you own (internal, external, DMZ, DNS, etc) from inside and outside the firewall. This will give you a picture of the ports that you are exposing. You can compare this to your security policy. If the local scans (i.e. scans not through the firewall) show services running (ports open) that are not needed then you might want to stop them. Services that are needed for localhost should be configured to only accept connections from the loopback network interface.

You may wish to run nessus ([www.nessus.org](http://www.nessus.org)) against all your boxes too. This can take a very long time if not configured properly, but will evaluate running services against a vulnerability database. It'll basically tell you if it thinks your services are buggy.

You may wish to search a vulnerability/exploit list for the exact versions of services you are running. [www.packetstormsecurity.org](http://www.packetstormsecurity.org) has a comprehensive list of everything. [www.securityfocus.com](http://www.securityfocus.com) is also very good. [www.k-otik.com](http://www.k-otik.com) is a crazy french exploit site and is very good.

You might want to buy one/more of the Hacking Exposed series of books.

Kev

> *Hi list,*  
> *As a regular reader of this list, and (amongst many other tasks)*  
> *responsible for security at our company, I wonder. I've taken most*  
> *measures to make our business secure. It's all on a small scale,*  
> *everything runs well, but every now and then the tiny hairs on the back*  
> *of my head make me wonder how secure it all is. Yes, webservers are*  
> *locked down, are in DMZ, only http permitted, SQL on inside via data*  
> *layers, only necessary ports between DMZ and inside; this production*  
> *environment is colocated, office is connected via PIX to PIX vpn,*  
> *restricted access to this vpn, etc.*

Re: [fw-wiz] I wonder, how to test..

Firewall-Wizards: Re: [fw-wiz] I wonder, how to test..

>  
> *Are there any low cost means / tools out there to verify that what i*  
> *have done so far is reasonable proof?*

>  
> *Thanks in advance,*  
> *Meindert uitman*  
> *Avic B.V.*

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

>  
>

--  
Kevin Sheldrake MEng MIEE CEng CISSP  
Electric Cat (Bournemouth) Ltd

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