

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/2004-08/0003.html>

From: Vinicius Moreira Mello (*fake-anti-spam-addr_at_inf.ufrgs.br*)

Date: 07/31/04

To: firewall-wizards@honor.icsalabs.com

Date: Fri, 30 Jul 2004 23:32:20 -0300

On Thu, 29 Jul 2004, Meindert Uitman wrote:

>

>

>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 buisness 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 nessesary ports between DMZ and inside; this production

>environment is colocated, office is connected via PIX to PIX vpn,

>restricted access to this vpn, etc.

Hi,

When you say your servers are locked down I think it's implied that you've done some basic vulnerability scanning and port/protocol mapping.

Now I see two possibilities:

1) Internally locking down the servers (if they aren't already):

A good approach is to locally lock down your systems against local users. Even if the servers don't have local users and you external services are secure, it protects the servers from your indiscipline and some other potencial threats, such as bad programmed CGIs. With local systems locked down it would be much harder for an attacker to get administrator's privileges if he managed to execute code with webserver user privileges, for example.

On Unix systems you could remove setid bits from privileged binaries, set special permissions for some very particular groups to run some tasks, patch syslog and crontab systems to run with decreased privileges, mount world-writable directories as non-executable, prevent filesystems from being umonted, firewall rules from being flushed, set a binary system integrity checker, etc.

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

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

And some other measures, like chrooting daemons, running them with decreased privileges, building a central logging infrastructure, reliably synchronizing clocks, etc (again, if it's already done).

2) Imagine attack scenarios

Since you've verified that your systems are individually, internally and externally secure it's time to look for trust relationships between your servers and networks. Look if snooped passwords wouldn't lead to server/internal systems access, webpage/database/intranet access. If local compromised systems wouldn't lead access to other parts of your networks. Recheck VPN trust relations.

CERT's.org tech tips addresses various system and network hardening measures: http://www.cert.org/tech_tips/

Also a very good paper is Mixer's "Protecting against the unknown" that addresses various security concerns in a broad and preventive way: <http://mixter.void.ru/protecting.txt>

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

You've reached a stage that automatic tools can't give you a reliable approach of your security state. It's time to review your infrastructure by yourself or by contracting third part penetration test service if your core business security requires it.

Regards,
vmm.

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

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