

RE: [fw-wiz] Looking for papers on protecting servers

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-04/0025.html>

From: Don Parker (*dparker_at_rigelksecurity.com*)

Date: 04/16/04

To: "Laura Taylor" <ltaylor@relevanttechnologies.com>, "'Lazlò Carreidas)'" <LazloCarreidas@nets

Date: Fri, 16 Apr 2004 11:57:32 -0400 (EDT)

Good points Laura, and I fully agree with them. One area that is often overlooked when deploying new servers or services is the architecture itself. Quite often a change in the network architecture itself can go a long ways in helping secure not only service itself, but also the internal network in case of a breach. This is not a popular option though I have found as many see it as too labour intensive or complicated.

Kind regards,

Don

Don Parker, GCIA
Intrusion Detection Specialist
Rigel Kent Security & Advisory Services Inc
www.rigelksecurity.com
ph :613.249.8340
fax:613.249.8319

On Apr 13, "Laura Taylor" <ltaylor@relevanttechnologies.com> wrote:

I think it would help if you were a little more specific. Depending on the application and the operating system, there is a good chance you may use a difference approach. If the server that is running a Microsoft operating system you can use automated security templates .inf files to lock it down so tight that leading scanners will not be able to discover that it is a Windows box however it is very different if you are talking about a UNIX server. If you are trying to secure an application, intrusion prevention works well. If you are trying to secure a DNS server, you use a different approach than say if you are trying to secure a SQL server. The best bet is to use a layered approach where you apply security the application, the operating system, and the infrastructure.

--

Laura Taylor
Relevant Technologies, Inc.

Firewall-Wizards: RE: [fw-wiz] Looking for papers on protecting servers

www.relevanttechnologies.com

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

From: firewall-wizards-admin@honor.icsalabs.com

[mailto:firewall-wizards-admin@honor.icsalabs.com]On Behalf Of Lazlò Carreidas)

Sent: Wednesday, April 07, 2004 6:58 AM

To: firewall-wizards@honor.icsalabs.com; focus-IDS@securityfocus.com; security-management@securityfocus.com

Subject: [fw-wiz] Looking for papers on protecting servers

My fellow experts,

I have been requested to write a document that would describe the different means to "protect" a specific server in a datacentre (except for the continuous patching process, of course...)

There are several possibilities (individual or combined):

- firewall as a "datacentre door"
- firewall (kind of "personal") over the server
- good HIDS and NIDS
- some kind of "security agent" that would raise an alert when needed
- etc...

I am looking for opinions, papers, etc... that could help me writing this document.

Thank you for your help

Lazlò

[Sorry for the multiple post]

Introducing the New Netscape Internet Service.

Only \$9.95 a month -- Sign up today at http://isp.netscape.com/register>

Netscape. Just the Net You Need.

New! Netscape Toolbar for Internet Explorer

Search from anywhere on the Web and block those annoying pop-ups.

Download now at http://channels.netscape.com/ns/search/install.jsp

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>

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

http://honor.icsalabs.com/mailman/listinfo/firewall-wizards