

Re: Vulnerability scanners

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-03/0172.html>

From: Alex Russell (alex@netWindows.org)

Date: 03/27/03

From: Alex Russell <alex@netWindows.org>

To: "Jeff Williams @ Aspect" <jeff.williams@aspectsecurity.com>, "Dan Lynch" <dan.lynch@placer.ca>

Date: Thu, 27 Mar 2003 15:51:45 -0600

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

On Thursday 27 March 2003 12:58 pm, Jeff Williams @ Aspect wrote:

> *Let's assume that you're talking about 256 IPs (based on Qualys'*
> *published pricing), and you want to scan weekly. That's at least a day a*
> *week of effort for someone (probably more to generate a very nice report*
> *and summaries). The cost of a full-time sysadmin (including salary,*
> *benefits, office, etc...) probably costs well north of \$100K. You'd have*
> *to include some equipment costs in there. So I doubt you could do it*
> *much cheaper. I think vulnerability scanning is a reasonable thing to*
> *outsource for companies that are not in the security or networking field*
> *already.*

This sounds like a false economy to me.

First: how does the Qualis box remove the need for a sysadmin? It's just one more appliance to manage, and something your existing admin should be able to do anyway. And if you already didn't have an admin, you'd need one now that you're thinking in terms of security. No extra cost here (aside from incremental admin time).

Secondly: if you've got a trained monkey doing your report generation, then you're right about the costs. If, however, you have a developer automate most of that, then you can add more nodes to be scanned at much lower incremental cost (change a config file). Additionally, using public signature sets may have downsides, but using Open Source tools is good both for your own internal flexibility and for the world at large (checks aren't quite right? set that developer to work writing and contributing back better ones!).

All in all, your initial costs to do it in house with smart people and Open Source tools might be higher, but your incremental costs do not grow at nearly the same rate. OTOH, if you don't have any admins or developers, then Qualys might look like a very nice option.

SecurityFocus Penetration: Re: Vulnerability scanners

HTH

Alex Russell
alex@netWindows.org
alex@SecurePipe.com

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQE+g3J/oV0dQ6uSmkYRAvN6AJ44Qwzu3sSypJkLDRb11W1ZjrnswCZASf0
m88qoVsnBJR2vt7vXZaYyKc=
=kMak

-----END PGP SIGNATURE-----

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/zsfptl1>