

## RE: Vulnerability scanners

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-03/0183.html>

---

**From:** Rapaille Max ([Max.Rapaille@nbb.be](mailto:Max.Rapaille@nbb.be))

**Date:** 03/28/03

Date: Fri, 28 Mar 2003 08:54:48 +0100

From: "Rapaille Max" <[Max.Rapaille@nbb.be](mailto:Max.Rapaille@nbb.be)>

To: <[mdwelch@sendsecure.com](mailto:mdwelch@sendsecure.com)>, "Paris Stone" <[paris@ciscoinstructor.net](mailto:paris@ciscoinstructor.net)>, "Alex Russell" <[alex@net](mailto:alex@net)>

Totally agree, but Qualys allows you to download the result from their Datacenter (in Html or XML format) and so you delete the report from their servers.. At this time you just loose the comparison features, and have to do it yourself.

But anyway, it has to stay on their network a certain amont of time... I know they had a project to make an internal report server, avoiding to send data to their servers.. They didn't achived the project, but I think the API's are available...

Cheers

Max

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

From: Michael Welch [mailto:[mdwelch@sendsecure.com](mailto:mdwelch@sendsecure.com)]

Sent: vendredi 28 mars 2003 00:46

To: Paris Stone; Alex Russell; Jeff Williams @ Aspect; Dan Lynch; [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)

Subject: RE: Vulnerability scanners

About 4 months ago I performed a comparison of Qualys, Foundscan, and Vigilante. They all have there good and bad point's. The nice things about Qualys was that all you had to do is plug the appliance into your network and you were ready to go. My concern was that although your scan data was transferred via https it was stored on another companies network. Being a security professional I have a hard time allowing my internal network scanning results sitting on another's network.

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

From: Paris Stone [mailto:[paris@ciscoinstructor.net](mailto:paris@ciscoinstructor.net)]

Sent: Thursday, March 27, 2003 5:25 PM

To: Alex Russell; Jeff Williams @ Aspect; Dan Lynch; [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)

Subject: Re: Vulnerability scanners

The Qualys box is an appliance that is configured once. It connects out your firewall using SSL (TCP 443) to hit Qualys's web/scanner server. It then retrieves the information(database of exploits, etc...) and runs them against your internal network. It then uploads the info to their database servers using SSL. Then all of your information is available via the web with nice reporting, pretty graphics, etc... It breaks it down into reports for techies and reports for non-techies

(CxO's) daily, weekly, monthly. The economies thing is simply that you have a yearly subscription based upon number of hosts scanned. A fixed cost, 24x7x365 tool that doesn't have HR or benefit issues and doesn't

SecurityFocus Penetration: RE: Vulnerability scanners

get kids sick and have to take days off. It IS easy to setup and administration is easy for those who can RTFM.

Alex Russell ([alex@netWindows.org](mailto:alex@netWindows.org)) wrote:

>  
>-----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.*  
>  
>*HTH*  
>  
>---  
>Alex Russell  
>[alex@netWindows.org](mailto:alex@netWindows.org)  
>[alex@SecurePipe.com](mailto:alex@SecurePipe.com)  
>-----BEGIN PGP SIGNATURE-----  
>Version: GnuPG v1.0.7 (GNU/Linux)  
>

RE: Vulnerability scanners

SecurityFocus Penetration: RE: Vulnerability scanners

> iD8DBQE+g3J/oV0dQ6uSmkYRAvN6AJ44Qwzu3sSypJkLDRbl1WIZjrrnswCZASf0  
> 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>  
>  
>

-----  
Paris Stone  
CISSP, CCNP, CNE/CNI, MCSE/MCT,  
Master CIW Administrator, CIW Security Analyst, NSA  
A+, Network+, iNet+  
<http://www.ciscoinstructor.net/>  
-----

"The rich man is not the one with the most, but the one who needs the least"

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>

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>

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>