

Re: Moving from Defense to Offense (or vice versa) to secure your network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-11/0263.html>

From: Bob Radvanovsky (*rsradvan_at_unixworks.net*)

Date: 11/27/05

To: "Erin Carroll" <amoeba@amoebazone.com>, <pen-test@securityfocus.com>

Date: Sun, 27 Nov 2005 15:10:20 -0600

Much of what you are considering depends on where in the "network security lifecycle" your organization is located. If your organization is in the "immature" stage of the lifecycle, they are investigating all possible methods, what are the ramifications, costs, etc. If your organization is in the "discovery" stage (meaning that they know now who they are, what are their goals and objectives, etc.) they are determining what areas need to be secured. If your organization is in the "defensive" stage, they are routinely conducting risk assessments annually, performing matrix comparisons between other organizations, and determining what future direction to go. If your organization is in the "mature" stage, they are concerned about cost mostly, and what they will tackle — next year.

As one who has done quite a number of security assessments, pentesting isn't the only thing to be concerned with; consequently, neither is sitting around waiting for something to happen, or stating that "we don't have any security issues on our networks" routine. There **MUST** be a balance between the pentesting aspect and the remainder. I used to think that being always on the offensive was the best method. **WRONG!** There is a lot more out there that must be addressed, some of which neither you nor I have much say in, esp. when politics or money come into the "Big Picture". Pentesting is just **ONE** aspect of several aspects that make up a risk assessment evaluation. Conducting routine audits (both scheduled and un-scheduled), forensics management (break-in attempts, viruses, trojans, etc.), policy management (in most cases, this can represent almost as much as 70% of the network securification process — without a good policy, nothing will have any significance or meaning), and more. Pentesting is just 1–3% of the entire securification process.

As an aside, perhaps we need a motto similar to: "The Last Defendable Frontier."

Cheers.

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

From: "Erin Carroll" <amoeba@amoebazone.com>

SecurityFocus Penetration: Re: Moving from Defense to Offense (or vice versa) to secure your network

To: <pen-test@securityfocus.com>
Sent: Saturday, November 26, 2005 7:37 PM
Subject: Moving from Defense to Offense (or vice versa) to secure your network

> All,
>
> I was having an interesting discussion with a coworker the other day about
> the differences between pen-testing (offense) and network security work
> (defense) which we do in our day jobs. The majority of my security
> background has been from a penetration standpoint so the way I view
network
> security defense setups and priorities tends to be of the "how would I
break
> this and get in" viewpoint rather than the "how do I secure this and
ensure
> reliable reporting/monitoring" view that my coworker is more centered on.
> The differences in the priorities and methods we would choose to secure
our
> network for defense was much different than I anticipated.
>
> So I was hoping some list members would share some similar experiences
with
> us. How many of you have switched between offense/defense and what were
some
> of the stumbling blocks or key differences you found in how you approached
> your goals? Is it worth it to cross-train in some manner? How have you
sold
> someone on the advantages of penetration-testing your network to quantify
> and test the effectiveness of your existing defenses?
>
> I would be interested to hear some cases you have run into out there.
>
> --
> Erin Carroll
> "Do Not Taunt Happy-Fun Ball"
>
> --
> No virus found in this outgoing message.
> Checked by AVG Free Edition.
> Version: 7.1.362 / Virus Database: 267.13.8/183 – Release Date: 11/25/2005
>
>
>
>

> Audit your website security with Acunetix Web Vulnerability Scanner:
>
> Hackers are concentrating their efforts on attacking applications on your
> website. Up to 75% of cyber attacks are launched on shopping carts, forms,

Re: Moving from Defense to Offense (or vice versa) to secure your network

SecurityFocus Penetration: Re: Moving from Defense to Offense (or vice versa) to secure your network

> login pages, dynamic content etc. Firewalls, SSL and locked-down servers
are
> futile against web application hacking. Check your website for
vulnerabilities
> to SQL injection, Cross site scripting and other web attacks before
hackers do!
> Download Trial at:
>
> http://www.securityfocus.com/sponsor/pen-test_050831
> -----

>

Audit your website security with Acunetix Web Vulnerability Scanner:
Hackers are concentrating their efforts on attacking applications on your
website. Up to 75% of cyber attacks are launched on shopping carts, forms,
login pages, dynamic content etc. Firewalls, SSL and locked-down servers are
futile against web application hacking. Check your website for vulnerabilities
to SQL injection, Cross site scripting and other web attacks before hackers do!
Download Trial at:
http://www.securityfocus.com/sponsor/pen-test_050831
