

Re: Defense in Depth

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-11/0039.html>

From: Miles Stevenson (miles_at_mstevenson.org)

Date: 11/01/04

To: security-basics@securityfocus.com

Date: Mon, 1 Nov 2004 00:33:11 -0500

Hello Ronish,

This is an excellent question, and one that a lot of security beginners get conflicting advice about, which only leads them into becoming more confused later down the road. My posts to this list tend to be a bit longer in nature because I don't believe in answering questions without also answering "why?", so bear with me. =)

The idea of "Defense in Depth" is based on the idea of security "layers". Many beginners take the idea of "layers" to simply mean more and more defense "tools", which is often the source of so much confusion. This is the approach that I think you are trying to take, which is NOT the correct approach.

What is meant by "layers" of security, is this: the entry points that must be followed to get to your sensitive data/resources. I'd like to point out that Kenneth Swain was definitely on the right track in his response to your question, albeit a bit "brief". Applied to computer security, there are several generalized categories where those "entry points" are found. Here are the most common "general entry points", or "layers":

Physical Layer – Physical access to the resources.

Network Layer – Layer at which data is accepted into the system from the network.

Kernel/Process Layer – Layer at which the operating system and applications work with your data in memory.

File system Layer – Layer at which your resources are stored and accessed on the file system.

Applying the practice of "Defense in Depth" to computers, means implementing defenses at each of the above layers. A good security plan would ensure that there are effective controls in place to ensure security at each of the above "layers". Let's work with an example here: sensitive data stored in a database.

SecurityFocus BASICS: Re: Defense in Depth

Physical Layer: You may have the database server physically stored in a "server room" with only 1 entry point. Only authorized individuals can get through this entry point (using cypher lock, fingerprint scanner, or whatever). Those entering and leaving the computer room are monitored and tracked at all times.

Network Layers: You may decide to put the database server on a private LAN segment protected from the outside by your firewall. You may also decide to put individual access controls on the machine itself using tcpwrappers, configuring the database server itself to only accept connections from authorized machines.

Kernel/Process Layer: You may decide to implement a tool such as GRSec to help protect the server process itself from being exploited by buffer overflow attacks and other attacks that go after the software itself. You may consider anti-virus software.

File system Layer: You may run the server inside of a "chroot" environment so that just in case it does get exploited, it can't access other parts of the file system. You may also decide to implement file system access controls within the database itself, such as only giving the "manager" user access to the "payroll" tables. You may also decide to encrypt the information stored on the file system, so that if the data is stolen from the file system, it is useless.

This is a very simple example of implementing "Defense in Depth". Note that this is NOT the same as putting in lots of security controls on the same "layer" in one long chain (lots of firewalls).

Think about it like this:

You can have 1, 2, 5, or 20 firewalls in front of your database server, but they won't stop someone from just disconnecting the server and walking away with it. They won't stop internal attackers from throwing a buffer overflow attack against the server and getting access to the data. They won't stop someone who already has shell access to the server from escalating file system privileges and just copying the database to their laptop and walking away with it.

What is gained by "Defense in Depth" is that if security on one layer fails to protect your data, then security on another layer will likely succeed. For example, when a disgruntled employee decides to walk out with your companies payroll database, your firewall will fail to protect your database server. But your door locks will keep the intruder out of the server room, and your cameras will catch him attempting to break in (hopefully BEFORE he is successful).

I promise you that your time will be much better spent by adding effective security controls to all the other "layers" instead of adding more firewalls to the network layer. Of course, those controls have to be effective. If your current firewall isn't doing its job very well, and needs to be replaced, then that's an entirely different subject.

SecurityFocus BASICS: Re: Defense in Depth

The other question that is often asked is, "is it good to have 2 layers of firewalls, assuming I already have security at all the other layers and now I want to add even more security?".

Most of the time, my answer to this is no. The only reason to have 2 firewalls in front of your system, is because you are afraid that one of the firewalls will fail to filter packets due to a bug in the firewall software, or fail due to a DoS attack. If you are afraid that your rule-set isn't good enough, that's a people problem, not a software problem. The drawback of having 2 firewalls, is that you have now just added a lot more complexity to your network filters, which now have to be entered twice, and in 2 different languages (I'm assuming that you decide to use 2 DIFFERENT BRANDS of firewalls, which would be the whole point). Your asking for trouble here, and opening yourself up for making more people-mistakes by making things more complex. My advice, if you are not confident in the security of your firewall, drop it and use a good firewall, such as iptables, or pf.

What would be the RIGHT reason to have multiple firewalls? Well, I would first say that if you have to ask this question, then you shouldn't be using multiple layers of firewalls! However, this doesn't really answer the "why?" question, so I'll entertain it.

I can say that there exists companies that are under constant threat of DoS attacks, and that distributing the job of network filtering across many firewalls would make it harder for an attacker to saturate all the resources. But it is a VERY rare case that this would be effective. Most companies don't even have enough bandwidth to be able to ACCEPT enough traffic to warrant multiple firewalls. A well implemented Linux or *BSD firewall with a SANE rule-set, should be able to handle a fully saturated T3 line without any problems. Your network pipe is going to fail before your firewall will. So first, I would say that you are going to have to have some HUGE pipes to even accept enough traffic to DoS a good firewall.

But supposing this is the case, and you are dealing with the constant threat of DoS attacks (the on-line casino business would be a good example of this), it might be a good idea to have multiple firewalls implement smaller "subsets" of your rule-set, so that each firewall can concentrate on 1 particular type of packet. A company in this situation though, is likely to have many, very well trained security people on the job 24/7, constantly dealing with attack (man I would LOVE this kind of stress!), and another branch of security people simply doing R&D work to keep up with the threats and finding new ways to defend against new attacks. I'm going to go out on a limb (no offense intended) and say that you are not working for such a company.

If you ARE dealing with the threat of DoS attacks, you should be getting in contact with your upstream provider in hopes of enlisting their help to slow the attacks down, not putting up additional firewalls.

Hope that helps! And good luck!

SecurityFocus BASICS: Re: Defense in Depth

--

Miles Stevenson

miles@mstevenson.org

PGP FP: 035F 7D40 44A9 28FA 7453 BDF4 329F 889D 767D 2F63

- application/pgp-signature attachment: stored