

## Re: How to Test Firewalls Guide?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/11823.html>

---

**From:** David ([davidwnh@adelphia.net](mailto:davidwnh@adelphia.net))

**Date:** 10/16/02

From: "David" <[davidwnh@adelphia.net](mailto:davidwnh@adelphia.net)>

Date: Wed, 16 Oct 2002 21:19:38 GMT

Do a bunch of searches on the web. Look for some of the nonprofit security organizations and continue downward from there. The quantity of information on the internet is astounding. Be wary of using the vendors information only (but do use it) since it is of no benefit to them to reveal their program's vulnerabilities. Check out the sites support and troubleshooting section, but again be wary, some have minimal information not because they are troublefree programs. All these programs have potential holes so you want to chose one that provides the information you need to avoid these problems. Subscribe to all the specific boards as this will show you what problems people are having with certain programs. Be wary of recommendations for specific software you see on the boards, since they are often biased, and do not take into consideration your own needs.

As far as scanning your always best using several sources. If you wish to do some yourself you may want to try something like nmap. Others may be able to suggest programs that are even more thorough or easier to use. Seek later advice if you need to as to how to set up your scanning simulations if you decide to do that. To do it affectively depends on your specific setup. Be careful with the results from internet scanning sites. Symantecs for example is biased towards them trying to sell you their products. Symantec for example tells me I need privacy protection that they provide. However I have this already using other vendors solutions.Hmm. Many others sites scans are only basic. See if they provide information on the site as to how thorough and what types of scans they are performing. There are several methods being used today to probe someone's system.

As far as logs that will depend on the specific software you are using. The product documentation, other users, and websites directed at the specific program or type of program will all help.

Give a lot of weighting to your personal experience with each product you try. If it is too difficult for you or your users to configure and use, you risk the chance of misconfiguration and misuse and will have less protection than if you choose a simpler program. An enterprise solution is one thing and a personal firewall is a whole different ballgame because much more interaction is left to the individual user.

As you get further through the process post post post because you will get

comp.security.firewalls: Re: How to Test Firewalls Guide?

better answers as your queries become more refined.

"NeoSadist" <neos@dist> wrote in message  
news:uqoorkliddotba@corp.supernews.com...

>  
> *"Speakeasy" <arptro@hotmail.com> wrote in message*  
> *news:nvydnbXew8Mv8jagXTWcqw@News.GigaNews.Com...*  
>> *I will be evaluation some software firewalls for laptops in my org and*  
*was*  
>> *wondering if anyone knows of a guide for testing firewalls. I'd like to*  
> *know*  
>> *of some testing tools to scan ports, send different types of pings, or*  
>> *emulate attacks and what I should look for in the logs. A step by step*  
> *"how*  
>> *to" would be great.*  
>>  
>> *If you want to make sure I'm on the up and up, contact me. Thanks*  
>>  
>>  
>>  
>  
>  
> *I guess you'd have to do a simulation run yourself, as those internet*  
*scans*  
> *leave something to be desired.*  
> *However, there's www.grc.com, but that's only a port scan. There's also*  
> *www.symantec.com, i think it's port scanning plus trojan attack*  
*simulation,*  
> *but i'm not sure how accurate it is.*  
> *Also, if you have win2k, there's microsoft baseline security analyzer,*  
*which*  
> *tests your OS.*  
> *But I'd LOVE to be able to set up some as a simulation. I was going to*  
*get*  
> *some computers and do a simulation like that. However, I'm still puzzled*  
*as*  
> *how to make them think it's an internet attack, not a LAN attack. I guess*  
> *maybe I gotta buy my neighbors a computer and internet or something.*  
> *Any suggestions?*  
>  
>

- 
- **Next message:** [David: "Re: LAN + firewall problem"](#)
  - **Previous message:** [David: "Re: How to protect my computer from the bad attention of administrator"](#)
  - **In reply to:** [: "Re: How to Test Firewalls Guide?"](#)
  - **Next in thread:** [Graham Bayley: "Re: How to Test Firewalls Guide?"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)