

Re: Best free firewall software

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-05/msg00472.html>

- *From:* Sebastian Gottschalk <seppi@xxxxxxxxxx>
 - *Date:* Sat, 27 May 2006 15:47:04 +0200
-

zzy wrote:

Sebastian Gottschalk wrote:

zzy wrote:

Thanks! I've downloaded, installed, and tried it.

Eh... didn't you want to scan your router or direct-dialup computer from the WAN side?

Eventually, yes, to test the effectiveness of my router. But I'm frankly more worried about the effectiveness of the software firewall on my laptop, since it's my only defense when I travel.

A firewall is a concept any serious firewall concept includes host security, so far that the host itself should not be vulnerable even if the packet filtering part of the concept fails.

Claiming that your firewall is the only defense is either technically wrong (e.g. your host is already secure and you're just misunderstanding the hole issue) or logically wrong (if your host is vulnerable, then you're insecure and your packet filter won't change that).

That's why it's called online scan and why I referred to linux-sec.net instead of Nmap's Homepage at insecure.org

What's called online scan? I went to linux-sec.net -- that's where I found NMap. What can I do at linux-sec.net?

There's a link "OpenPorts Audit". This is an online port scan based on Nmap, and supposed exactly what you want: someone else scanning you from the WAN side, but with the full flexibility of Nmap command line.

Re: Best free firewall software

Sorry, but an incomprehensible output is a useless output.

Incomprehensible to you != someone with clue can't help you interpreting it

I scanned my laptop from my desktop machine on my LAN, and vice-versa.

As long as your "firewall" didn't oppose any trust relationship between these machines, this should be quite effective to audit the machine's security itself.

Sorry for asking, a lot of people get this wrong and are either scanning local loopback or the router.

Anyway, what about `-sS`, `-sF`, `-sN`, `-sX`, `-sA`, `-sW`, `-sM`, `-sU`, `-sO`, the first with and without `-f`, all with `-O`. Not to mention auditing against IP spoofing, MAC spoofing and IPv6.

Not all of these are available in online scans, and not all can expose weaknesses in a router. Try a scan in a local subnet (each other, not each themselves).

Sorry, I don't have a clue how to do that. Is there some documentation that explains how? I went through the tutorial, and if it said something about a subnet I missed it. You're suggesting that I do 18 more scans with various switches. But it doesn't seem to make any sense to do that until I understand the results of the one scan I did.

`sS` – TCP–SYN scan, good for discovering open ports
`sF`, `sN`, `sX` – good for scanning the behaviour of the TCP/IP stack, just try some few ports
`sA`, `sW` – good for scanning the firewall's behaviour
`sM` – good for checking
`sU` – UDP scan, as TCP is not your only problem
`sO` – IP protocol scan for exposing other potentially vulnerable protocols (ICMP, ESP, AH, EPIP are typical)
`f` – doing the TCP SYN scan with fragments exposes firewall problems as is usually very good for bypassing the router from the WAN side
`O` – useful output with fingerprinting
IP–Spoofing, MAC–Spoofing – for circumvention
IPv6 – just in case you're using it

Now better read a good book about typical TCP/IP and firewall weaknesses, or got someone for has a clue to do this auditing for you.

Re: Best free firewall software

How do I go about closing them, without the benefit of a hardware router? The laptop has to stand on its own.

A good firewall offers to respond with a TCP-RST or ICMP-DestinationUnreachable instead of DROPPing the packets. Most (reads: every known) "personal firewalls" don't.

A hardware router usually won't help your either, it will rather make it pretty impossible – this and the NAT thing is why I prefer direct dial-up. Better connectivity!

Looks like I have a problem in that two ports are open. (A google search on "tcpwrapped" didn't bring up anything which explained its meaning and significance in this context, so I don't know whether it's a Good Thing or Bad Thing.)

Well, it's just a registered port. What about "netstat -anbo" to see what exactly is listening on those ports?

I don't see anything in the output which shows either of those port numbers.

Now either there's a serious network problem or you've got a rootkit. Repeat the scan.

Well, I care about firewalling because I don't want any malware getting into my machine. It's not trivial to me to disable "any unwanted service" -- I've disabled one or another from time to time and later discovered that it's essential to some application.

Disabling a network doesn't necessarily mean disabling the service program, but just disabling its network binding. So far this is pretty painless even on Windows.

I've found it difficult and very time consuming to find out exactly what each service does, and I certainly don't know which might be "vulnerable" services.

Huh? Actually it's pretty well documented. "Controlling Communication in

Re: Best free firewall software

a managed environment", downloadable at Microsoft, has a detailed description on services, network communication and configuration. And we've written a nice tutorial at <http://www.ntsvcfg.de>.

There are currently 104 services running on my machine.

WTF?

It sounds like you're recommending removing the firewall and protecting myself by restricting my ability to use my computer by shutting down services and running as a limited user. Or am I misinterpreting what you're suggesting?

No, exactly. This is quite usual on Linux, but not likely on Windows.

I know this doesn't mean I'm safe from all attacks, but it's been adequate for me so far.

What about user's mistakes?

I'd like to do what I can to keep at least this level of protection in the future or improve it, but I'm not willing to restrict the usability of my machine for the sake of being pure or to establish an unneeded level of protection.

This is not about protection, this is about least privilege which is generally a good idea.

.