In the first article in this short series on personal firewalls, we looked at the basic reasons corporate network security managers should install personal firewalls on all their organizations' computers, including laptops, and why home computers used by employees should also be protected. In the second article, I summarized Gibson's tools for external testing of personal firewalls. In this article, we'll look at testing firewalls against leakage from the inside.

Steve Gibson writes <http://grc.com/lt/leaktest.htm>,

“This site has been most well-known for its FREE ShieldsUP! Internet security test. Crucial as it is to protect yourself from malicious hackers outside, those bad guys represent only half of the threat. The Internet has proven to be an extremely fertile transportation medium for all manner of nasty Trojan horse programs, rapidly proliferating viruses, and privacy invading commercial spyware. As a result, it is no longer true that all of the potential problems reside outside the computer.

Your Internet connection flows both ways . . . so must your security.

Not only must our Internet connections be fortified to prevent external intrusion, they also provide secure management of internal extrusion. Any comprehensive security program must safeguard its owner by preventing Trojan horses, viruses, and spyware from using the system's Internet connection without the owner's knowledge. Scanning for the presence of Trojans, viruses, and spyware is important and effective, but if a piece of malware does get into your computer you want to expose it immediately by detecting its communication attempts and cut it off from communication with its external agencies.”

The download of Gibson’s LeakTest v1.00 takes only a few seconds (the program uses only 27KB) and has only two function buttons: HELP and TEST FOR LEAKS. Clicking on the latter brings up a results screen almost instantly. In my case, the results were as follows:

Unable To Connect. LeakTest was unable to connect to the GRC NanoProbe Server. If your computer is currently connected to the Internet, the most likely cause for LeakTest's inability to connect is an aggressive and properly working firewall. If so, it is preventing LeakTest from connecting to our machine's FTP port number 21. That's GREAT news! . . .

. . . but to be completely certain that your firewall deserves the credit for blocking this outbound connection attempt, you should try permitting LeakTest to connect just to be sure it can. If it still can't, then perhaps something has changed on our end and you'll need to grab an updated copy.

To be sure that my firewall was in fact responsible for the negative results, I explicitly allowed
ZoneAlarm to permit outbound connections from LeakTest. This time the results showed,

Firewall Penetrated! LeakTest WAS ABLE to connect to the GRC NanoProbe Server!

LeakTest was not prevented from connecting to the Gibson Research NanoProbe server. You either have no firewall, you have deliberately allowed LeakTest to connect outbound, or (if neither of those), LeakTest has just slipped past your firewall's "protection"!

In summary, Gibson has once again contributed a valuable tool for all Internet users. This man deserves support, praise and lots of business. I suggest that at the very least, we should all buy licenses to his SpinRite utility. Keep up the good work, Steve!

* * *

In the next article in this series, I will summarize Gibson’s findings about the ZoneAlarm personal firewall product.

* * *

Mich Kabay can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from the Information Security University project, see <http://infosecu.com>.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.