Lock IT Down: Develop a strategy for securing ports on your servers

by Ray Geroski | Jan 23, 2003 8:00:00 AM

TAGS: PRODUCTIVITY, NETWORKING, Network technology, Ray Geroski, information technology, strategy, Foundstone, Fport, network, server, tool

11 comment(s)

- Email
- Save
- Print
- Digg This
-

Takeaway: Find out what TCP/IP ports you need to block to secure your network

---

Open TCP/IP ports on your servers can be an invitation to hackers, especially if they're well-known ports such as 21 (FTP), 80 (HTTP), and 25 (SMTP). Many Trojans also monitor certain ports that are often unused (and therefore often unmonitored by admins), allowing intruders to take advantage of these ports as well—if they are open.

In response to a recent article on TCP/IP filtering, many IT professionals expressed concerns about determining which ports to leave open and which to close. It’s a dilemma that could leave networks open to attacks, but the tips and resources members presented in response to these concerns offer valuable insights that can help you better secure your networks.

Knowing what’s open

Before you can shut down the ports that represent vulnerabilities, you have to know what’s open and which applications monitor which ports. Inexperienced admins may be unfamiliar with many of the issues involved in TCP/IP filtering.

One TechRepublic member, for example, wrote that as an inexperienced server admin, he wasn’t sure which ports should be left open.

“My [Windows 2000] box acts as a central share repository, so I’ve got some shared folders and CD units. It also [serves as] a simple Web [server].”

The member wanted to know what ports besides port 80 should be left open and specifically, which ports the Windows shares use.

In response to this question members suggested a variety of tools that can scan ports and extract usage information. Member **Michael Schaeffner**, for example, suggested using Ethereal to analyze traffic on the network. In terms of simply gathering information on ports, however, Ethereal may not be the friendliest tool for the inexperienced admin. **MasterYoda** pointed out that the information Ethereal displays isn't easy to decipher unless you have a firm understanding of the product and the underlying networking technologies.

Other members suggested using Foundstone tools, such as SuperScan, which is free to download. Another Foundstone tool that Member **bigaldepr** mentioned Foundstone's Vision, which can identify "PID number, process name, port, and protocol." Bigaldepr also agreed that Foundstone's SuperScan is useful.

"[It] can be configured to ping all addresses in a range on the network and then check for open ports according to a pick list on each machine that replies."

In addition to Vision and SuperScan, Foundstone offers Fscan, which can be run with various switches from the command line to filter and organize the scan results. And for simply determining which applications are associated with which port numbers, Fport is handy. It's simple to use and presents straightforward information that isn't bogged down with unnecessary detail. For more information or to download Fport, visit this page on Foundstone's site.

Another member suggested simply using NETSTAT to view data on ports in use. When run with the –a switch, NETSTAT displays a list of all listening ports on the network.

All of these tools present you with detailed data about port activity on your network. Of course, before you can determine which doors to close, you have to find out which ones are open on your servers and why. Fport and other free utilities can deliver this information quickly and easily. For a detailed report on identifying and securing vulnerabilities, see the SANS article on security best practices. Section 2.2 of the article discusses scanning and suggests tools to use to determine vulnerabilities. You can also find detailed information on port assignments in this document from the IANA's Web site.

What to open

The data you gather won't necessarily tell you what you should leave open, however, and there are no universal rules to fit every network. For example, TechRepublic member **Benjamin Zachary** pointed out that "anyone running Windows 2000 AD will need to know that DNS uses ports 53 and ports above 1023 UDP." The bottom line is that locking down ports is not so simple. Zachary said his organization uses IPSec policies to create filters "because they can be modified without rebooting."

Other ports you may need to keep open *within* your network include 137-139, which are used by

NETBIOS. These ports are usually open to allow resource sharing, but again, that will depend on the configuration of your network.

Many argue that it's necessary to keep port 80 open for HTTP and 443 for HTTPS, but you may want to close them unless the server in question functions as a Web server and requires them.

For the most part, it's a matter of knowing what services you need to run and their associated ports and closing everything that's unneeded. So the answer to the question of what ports should be left open can be answered only once you do the research on the services and applications running on your network.

Danger ports

Knowing which ports to close is made easier by knowing which ones have been linked to security threats. The SANS Intrusion Detection FAQ lists ports used by well-known Trojans and presents some guidelines for shutting down these known vulnerabilities. Keep in mind that this list has not been updated recently, so the information may be incomplete. One of the values of this list is that it can tip you off to suspicious activity. If you detect someone scanning one of these ports on your network, it could be a hacker attempting to find a Trojan listening on its default port.

You also have to consider the services activated by default in Windows that listen on default ports. Running NETSTAT reveals which hosts are running such services.

Other resources

Resources such as the SANS and IANA Web sites offer essential information about ports, services, and Trojans that can help give you a clear idea of which ports you need to keep open, especially when cross-referenced with the results of a *netstat –a* scan.

Schaeffner also suggested visiting DShield's Web site. DShield provides a means of sharing information about intrusions. You can use the site to view firewall log reports uploaded by others that show where and how intrusions occur. You can also share you own data. This may be a useful way to determine which ports are vulnerable and where intruders are looking for openings.