

Re: Questions on secure remote access to Fedora Core 2

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2006-10/msg00255.html>

- *From:* responder <no@xxxxxxxxxxxxxx>
 - *Date:* Tue, 31 Oct 2006 02:42:07 -0500
-

C. J. Clegg wrote:

Heartfelt thanks to all of y'all who gave me so much help on the security questions, and everyone else who replied to the "Disabling telnet on Linux" thread.

After most of a day of research on iptables, and a bunch of trial and error, I came up with the following `/etc/sysconfig/iptables` file (I hope the formatting doesn't get screwed too badly):

[...]

Hey C. J., Glad you feel better. Actually iptables, a good interface for netfilter, a good firewall, makes me "crazy" to read. I won't expand on that or complain for the good tools that have been given to us freely.

What you see with `# iptables --list` is not what you put in with `# iptables` commands. What you define for commands makes several orders of magnitude more sense if one knows the precise topology and traffic requirements, and other contexts. I can't read or decipher it, even if it weren't (evilly?) reformatted by the Usenet softwarez ;)

When you have your systems running as you think you would like them, nmap them from inside and scan them from outside to test them. Other people may have fancier (more effective, more elegant) approaches, and they might write to say what they are. I suggest you go to grc.com (Gibson Research) and go to the "shieldsup" page, clicking through cookies and proceeds and all (many clicks). He gives you the options to scan your interface many ways and report the results to you.

If you have no better, more expensive, more proprietary, more private way of testing your systems' external appearance, then click away to your hearts' content, and see what your systems look like to someone else on the outside trying to scan you or trying to crack you. It is pedestrian, for sure. But it works.

Re: Questions on secure remote access to Fedora Core 2

There are always commercial pen-test services available if judged to be necessary or desirable. Ask and you will receive. If the powers that be insist on running FC2 on their server, they probably don't want to know, anyway.

And OK, so I'm not really a full newbie anymore and have a tendency to be less insecure and perhaps even slightly complacent. Even experts get cracked. But I wouldn't ever even be posting my firewall rules on usenet. Don't worry about it; – if the rules are good, they will hold regardless.

COMMIT

Objectives:

1. Keep HTTP and HTTPS open for everybody
2. Open inbound SSH, FTP, and mail for everybody ... but, they are severely restricted in /etc/hosts.allow, and the few allowed FTP users are kept in chroot jails. FTP is really just needed for three individual users who for whatever reason can't use SFTP.
3. Disable outgoing telnet and FTP
4. Log all other outbound activity EXCEPT: SSH going to three trusted networks; any SMTP, HTTP, DNS activity; any pings; any IMAP activity on the localhost.

I used DROP rather than REJECT because I don't want messages going out explaining why the connection is being rejected.

Look reasonable?

I would tell you if I knew. Best wishes.

.