Forum: CentOS 6 - Security Support

Topic: iptables: RH-Firewall-1-INPUT vs. INPUT, and the wiki

Subject: iptables: RH-Firewall-1-INPUT vs. INPUT, and the wiki

Posted by: mdfx

Posted on: 2012/3/29 19:41:57

Hello,

I feel like I have started to grasp of the basics of iptables through experiment/logging and reading. I got my start at the CentOS iptables wiki. But one thing still puzzles me that I haven't been able to google up a clear answer on:

Why is the chain "RH-Firewall" used in some cases I've read (like the Samba HowTo , but not others?

For example, in the hardening CentOS wiki there is the following code (I've pared it down a bit):
:INPUT DROP [0:0] :FORWARD DROP [0:0] :OUTPUT ACCEPT [0:0] :RH-Firewall-1-INPUT - [0:0] -A INPUT -j RH-Firewall-1-INPUT -A FORWARD -j RH-Firewall-1-INPUT -A RH-Firewall-1-INPUT -i lo -j ACCEPT -A RH-Firewall-1-INPUT -p icmp --icmp-type echo-reply -j ACCEPT -A INPUT -i eth0 -s 10.0.0.0/8 -j LOG --log-prefix "IP DROP SPOOF A: " -A INPUT -i eth0 -s 172.16.0.0/12 -j LOG --log-prefix "IP DROP SPOOF B: " -A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT # Accept ssh traffic. Restrict this to known ips if possible. -A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT #Log and drop everything else -A RH-Firewall-1-INPUT -j LOG -A RH-Firewall-1-INPUT -j DROP COMMIT

Some specific parts that confuse me about this:
:RH-Firewall-1-INPUT - [0:0] ~ *Seems to be defining a chain, but with no default (a "-")?*
-A INPUT -j RH-Firewall-1-INPUT ~ *Seems to forward INPUT packets to the RH-Firewall chain, but then rules are defined later for -A INPUT?*

All of my experimentation and iptables rules have been absent of any RH-Firewall, using just INPUT, FORWARD, and OUTPUT chains. Is there a reason to use it? Where does it come from/Why does it crop up so often?

I'm running CentOS 6.2 and iptables v1.4.7. Thanks for any responses to these basic questions. Linux is fun!