Linux Kernel /etc/sysctl.conf Security Hardening

Article Number: 347 | Rating: Unrated | Last Updated: Fri, Aug 3, 2018 11:52 AM

How do I set advanced security options of the TCP/IP stack and virtual memory to improve security and performance of my system? How do I configure Linux kernel to prevent certain kinds of attacks using /etc/sysctl.conf? How do I set Linux kernel parameters?

sysctl is an interface that allows you to make changes to a running Linux kernel. With /etc/sysctl.conf you can configure various Linux networking and system settings such as:

1. Limit network-transmitted configuration for IPv4
2. Limit network-transmitted configuration for IPv6
3. Turn on execshield protection
4. Prevent against the common ‘syn flood attack’
5. Turn on source IP address verification
6. Prevents a cracker from using a spoofing attack against the IP address of the server.
7. Logs several types of suspicious packets, such as spoofed packets, source-routed packets, and redirects.

sysctl command

The sysctl command is used to modify kernel parameters at runtime. /etc/sysctl.conf is a text file containing sysctl values to be read in and set by sysct at boot time. To view current values, enter:
sysctl -a
sysctl -A

sysctl mib
sysctl net.ipv4.conf.all.rp_filter
To load settings, enter:
sysctl -p

Sample /etc/sysctl.conf

Edit /etc/sysctl.conf and update it as follows. The file is documented with comments. However, I recommend reading the official Linux kernel sysctl tuning help file (see below):