Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > CentOS

Linux Kernel /etc/sysctl.conf Security Hardening

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

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):

```
# The following is suitable for dedicated web server, mail, ftp server etc.
# ---------------------------------------
# BOOLEAN Values:
# a) 0 (zero) - disabled / no / false
# b) Non zero - enabled / yes / true
# --------------------------------------
# Controls IP packet forwarding
net.ipv4.ip_forward = 0

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename
# Useful for debugging multi-threaded applications
kernel.core_uses_pid = 1
```

```
# Controls the use of TCP syncookies
#net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_synack_retries = 2

########## IPv4 networking start ##############
# Send redirects, if router, but this is just server
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Accept packets with SRR option? No
net.ipv4.conf.all.accept_source_route = 0

# Accept Redirects? No, this is not router
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0

# Log packets with impossible addresses to kernel log? yes
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

# Ignore all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Prevent against the common 'syn flood attack'
net.ipv4.tcp_syncookies = 1

# Enable source validation by reversed path, as specified in RFC1812
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

########## IPv6 networking start ##############
# Number of Router Solicitations to send until assuming no routers are present.
# This is host and not router
net.ipv6.conf.default.router_solicitations = 0

# Accept Router Preference in RA?
net.ipv6.conf.default.accept_ra_rtr_pref = 0

# Learn Prefix Information in Router Advertisement
net.ipv6.conf.default.accept_ra_pinfo = 0

# Setting controls whether the system will accept Hop Limit settings from a router advertis
net.ipv6.conf.default.accept_ra_defrtr = 0

#router advertisements can cause the system to assign a global unicast address to an inter
net.ipv6.conf.default.autoconf = 0

#how many neighbor solicitations to send out per address?
net.ipv6.conf.default.dad_transmits = 0

# How many global unicast IPv6 addresses can be assigned to each interface?
net.ipv6.conf.default.max_addresses = 1

########## IPv6 networking ends ##############

#Enable ExecShield protection
kernel.exec-shield = 1
kernel.randomize_va_space = 1

# TCP and memory optimization
# increase TCP max buffer size setable using setsockopt()
#net.ipv4.tcp_rmem = 4096 87380 8388608
#net.ipv4.tcp_wmem = 4096 87380 8388608

# increase Linux auto tuning TCP buffer limits
#net.core.rmem_max = 8388608
#net.core.wmem_max = 8388608
#net.core.netdev_max_backlog = 5000
```

```
#net.ipv4.tcp_window_scaling = 1

# increase system file descriptor limit
fs.file-max = 65535

#Allow for more PIDs
kernel.pid_max = 65536

#Increase system IP port limits
net.ipv4.ip_local_port_range = 2000 65000
```

How do I tune Linux VM subsystem?

- See FAQ: Linux Tuning The VM (memory) Subsystem [2]

How do I tune Linux network stack?

- See FAQ: Linux Tune Network Stack (Buffers Size) To Increase Networking Performance [3]

References:

- Linux kernel IP sysctl [4] documentation.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/linux-kernel-etcsysctl-conf-security-hardening/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/linux/**
[2] Linux Tuning The VM (memory) Subsystem: **http://www.cyberciti.biz/faq/linux-kernel-tuning-virtual-memory-subsystem/**
[3] Linux Tune Network Stack (Buffers Size) To Increase Networking Performance: **http://www.cyberciti.biz/faq/linux-tcp-tuning/**
[4] Linux kernel IP sysctl: **http://www.cyberciti.biz/files/linux-kernel/Documentation/networking/ip-sysctl.txt**