**SECURE SYSCTL**

Sysctl is a powerful tool used to configure kernel parameters on Linux systems. However, it is important to ensure that it is configured securely to prevent unauthorized access or modifications to the system. Here's how to configure sysctl securely in CentOS and Ubuntu:

**CentOS:**

Open the **/etc/sysctl.conf** file in a text editor with root privileges.

**sudo vi /etc/sysctl.conf**

Uncomment the following lines to enable security-related settings:

**# Kernel sysctl configuration file for Red Hat Linux**

**#**

**# Security settings**

**# Controls IP packet forwarding**

**net.ipv4.ip\_forward = 0**

**# Ignore ICMP broadcast requests**

**net.ipv4.icmp\_echo\_ignore\_broadcasts = 1**

**# Enable source validation by reversed path, as recommended by RFC1812**

**net.ipv4.conf.all.rp\_filter = 1**

**# Disable source routing**

**net.ipv4.conf.all.accept\_source\_route = 0**

**# Ignoring bogus ICMP errors**

**net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1**

**# Do not accept ICMP redirect**

**net.ipv4.conf.all.accept\_redirects = 0**

**net.ipv6.conf.all.accept\_redirects = 0**

**# Disable the magic-sysrq key**

**kernel.sysrq = 0**

**# Disable core dumps**

**fs.suid\_dumpable = 0**

Save and close the file.

Apply the changes to the running system by running the following command:

sudo sysctl -p

**Ubuntu:**

Open the /etc/sysctl.conf file in a text editor with root privileges.

sudo vi /etc/sysctl.conf

Uncomment the following lines to enable security-related settings:

# **Controls IP packet forwarding**

**net.ipv4.ip\_forward = 0**

**# Ignore ICMP broadcast requests**

**net.ipv4.icmp\_echo\_ignore\_broadcasts = 1**

**# Enable source validation by reversed path**

**net.ipv4.conf.all.rp\_filter = 1**

**# Do not accept source routing**

**net.ipv4.conf.all.accept\_source\_route = 0**

**# Ignore send redirects**

**net.ipv4.conf.all.send\_redirects = 0**

**# Ignore ICMP redirects**

**net.ipv4.conf.all.accept\_redirects = 0**

**# Disable IPv6 autoconfiguration**

**net.ipv6.conf.all.autoconf = 0**

**net.ipv6.conf.default**.**autoconf = 0**

**# Disable the magic-sysrq key**

**kernel.sysrq = 0**

**# Disable core dumps**

**fs.suid\_dumpable = 0**

Save and close the file.

Apply the changes to the running system by running the following command:

**sudo sysctl -p**

Note: These settings are just an example of some of the most commonly used security-related sysctl settings. You may need to adjust them based on your specific requirements and the applications running on your system.