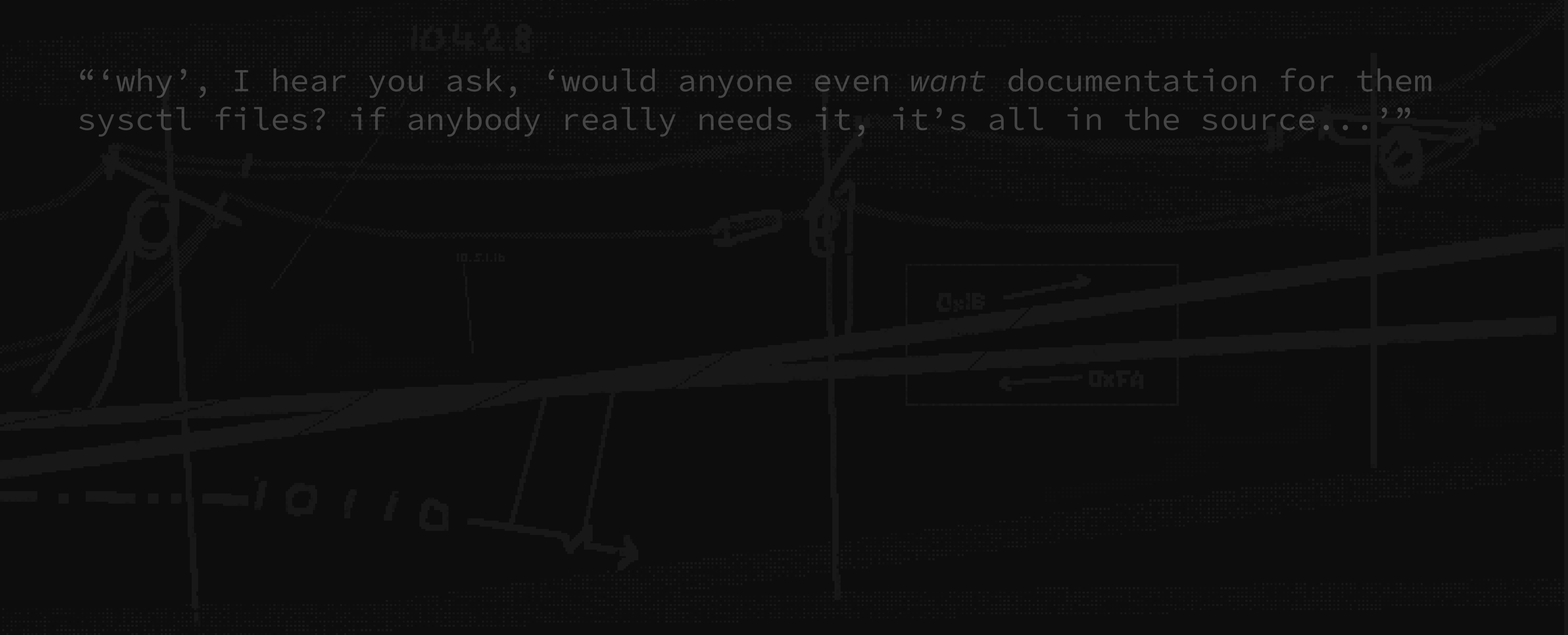


"'why', I hear you ask, 'would anyone even *want* documentation for them sysctl files? if anybody really needs it, it's all in the source...'"

17

/proc/sys/ Config via sysctl

Wait… What even is *sysctl*?

sysctl is a tool to modify kernel parameters at runtime. By modifying values using *sysctl*, we can adjust how the kernel runs without having to restart the system.

These kernel parameters are those available in */proc/sys/*.
(try running *tree /proc/sys/* and see what’s inside!)

The *procfs*

procfs is the process filesystem.
It is the file system in Linux systems that contains system and kernel data files, as well as process files.

It is mounted in */proc/* and is also where you will find all available *sysctl* options.

These are not “real” files, rather they are an interface to a data structure… a “*pseudo-filesystem*”.

sysctl allows us to interact with *procfs* during runtime.

Can’t I just use Klaver?

Klaver can help you with most points related to *sysctl*.

But!
I do advise at least looking into what each option does,
so you understand how to get these points and why they
appear on your score report…

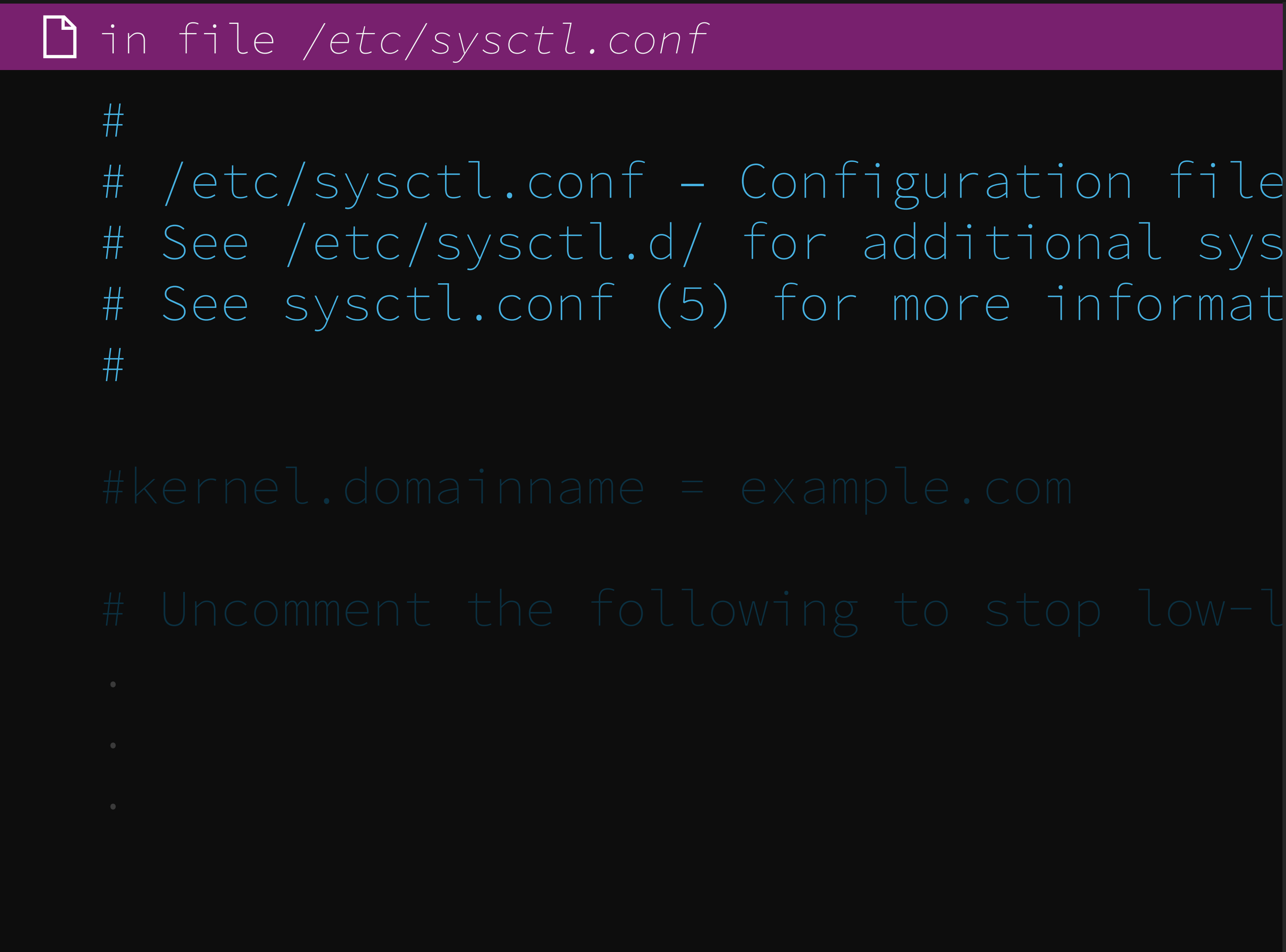
Command-Based Input of *sysctl*

in terminal

```
# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```

There are two methods for inputting *sysctl* options, the first is the *sysctl* command itself.

File-Based Input of sysctl



in file */etc/sysctl.conf*

```
#
# /etc/sysctl.conf - Configuration file
# See /etc/sysctl.d/ for additional sys
# See sysctl.conf (5) for more informat
#

#kernel.domainname = example.com

# Uncomment the following to stop low-l
.
.
.
```

sysctl reads a handful of files that also set configuration options, with */etc/sysctl.conf* taking precedence.

To apply changes to these files, run *sysctl --system*.

Preferred Configuration

in file */etc/sysctl.conf*

```
net.ipv4.conf.default.rp_filter = 1
net.ipv4.all.default.rp_filter = 1

net.ipv4.tcp.max_syn_backlog = 8192
net.ipv4.tcp_syncookies = 1

net.ipv4.ip_forward = 0
```

These configurations deal with the network configuration.

Here, we:

- Use reverse-path filtering to validate packets
- Prevent SYN flood attacks using queue length
- Prevent traffic from being forwarded through this system

Preferred Configuration

in file */etc/sysctl.conf*

```
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.all.secure_redirects = 0

net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```

Here, we prevent ICMP redirects to prevent possible man-in-the-middle attacks.

Preferred Configuration

in file */etc/sysctl.conf*

```
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
```

Here, we prevent routes from being accepted. We are not routers!

Preferred Configuration

in file */etc/sysctl.conf*

```
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.all.log_martians = 1

net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Here, we log any potentially spoofed “martian” packets. These are packets that have invalid destination or source addresses. We also disable IPv6 here, as it’s seldom used by services in competition.

Preferred Configuration

🗋 in file */etc/sysctl.conf*

```
net.ipv4.tcp_syn_retries = 2
net.ipv4.tcp_synack_retries = 5

net.ipv4.icmp_echo_ignore_all = 1
net.ipv6.icmp_echo_ignore_all = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

We limit the amount of TCP SYN and SYNACK attempts we have, as well as prevent the system to responding to *pings* and the like.

Preferred Configuration

in file */etc/sysctl.conf*

```
net.ipv4.tcp_rfc1337 = 1

net.ipv4.icmp_ignore_bogus_error_responses = 1
```

We heed to RFC 1337, TIME-WAIT Assassination Hazards in TCP.
We also ignore any bogus error messages from ICMP.

Preferred Configuration

in file */etc/sysctl.conf*

```
kernel.sysrq = 0
kernel.core_uses_pid = 1
kernel.pid_max = 65535
kernel.kptr_restrict = 2
kernel.ramdomize_va_space = 2
kernel.panic = 60
kernel.panic_on_oops = 1
kernel.yama.ptrace_scope = 1
```

We change certain kernel settings here, such as PID number settings, kernel panic behavior, and a bit more.

Preferred Configuration

in file */etc/sysctl.conf*

```
fs.suid_dumpable = 0
fs.file_max = 65535
fs.protected_hardlinks = 1
fs.protected_symlinks = 1

vm.panic_on_oom = 1
vm.swappiness = 10
```

We also change some filesystem settings and virtual memory settings.

Remember...

in terminal

```
# sysctl --system
```

If editing files directly, run this command!