NAME

hardening - HardenedBSD Hardening

SYNOPSIS

#include <sys/types.h>
#include <sys/pax.h>

In the kernel configuration file:
options PAX
options PAX_HARDENING

DESCRIPTION

Various system hardening features have been implemented in HardenedBSD. Many of them deal with restricting what non-root users are able to do. When the kernel is compiled with **option PAX_HARDENING**, certain sysctl(8) options are modified from their defaults. See Appendix A for a list of all the sysctl(8) option modifications.

procfs(5) and linprocfs(5) are modified to prevent arbitrary writes to a process's registers. This behavior is controlled by the *hardening.procfs_harden* sysctl option.

kld(4) related system calls are restricted to non-jailed, root-only. Attempting to list using modfind(2), kldfind(2), and the other KLD-related system calls will result in permission denied if used by a non-root or jailed user.

APPENDIX A

- security.bsd.unprivileged_read_msgbuf
  - Type: integer
  - Description: Unprivileged processes may read the kernel message buffer.
  - Default: 1
  - Hardened: 0

- kern.randompid
  - Type: integer
  - Description: Random PID modulus.
  - Default: 0, read+write
  - Hardened: randomly set at boot and made read-only

- security.bsd.see_other_uids
  - Type: integer
  - Description: Unprivileged processes may see subjects/objects with different real uid.

  - Default: 1
  - Hardened: 0

- security.bsd.see_other_gids
  - Type: integer
  - Description: Unprivileged processes may see subjects/objects with different real gid.
  - Default: 1
  - Hardened: 0

- security.bsd.unprivileged_proc_debug
  - Type: integer
  - Description: Unprivileged processes may use process debugging facilities.
  - Default: 1
  - Hardened: 0

- security.bsd.hardlink_check_uid
  - Type: integer
  - Description: Unprivileged processes cannot create hard links to files owned by other users.
  - Default: 0
  - Hardened: 1

- security.bsd.hardlink_check_gid
  - Type: integer
  - Description: Unprivileged processes cannot create hard links to files owned by other groups.
  - Default: 0
  - Hardened: 1

- kern.msgbuf_show_timestamp
  - Type: integer
  - Description: Show timestamp in msgbuf.
  - Default: 0
  - Hardened: 1

- net.inet.ip.random_id
  - Type: integer
  - Description: Assign random IP ID values.
  - Default: 0
  - Hardened: 1

- security.bsd.stack_guard_page

- Type: integer
- Description: Insert stack guard page ahead of the growable segments.
- Default: 0
- Hardened: 1

SEE ALSO

kldfind(2), modfind(2), sysctl(8)

AUTHORS

This manual page was written by Shawn Webb. The hardening implementation was written by Shawn Webb and Oliver Pinter.