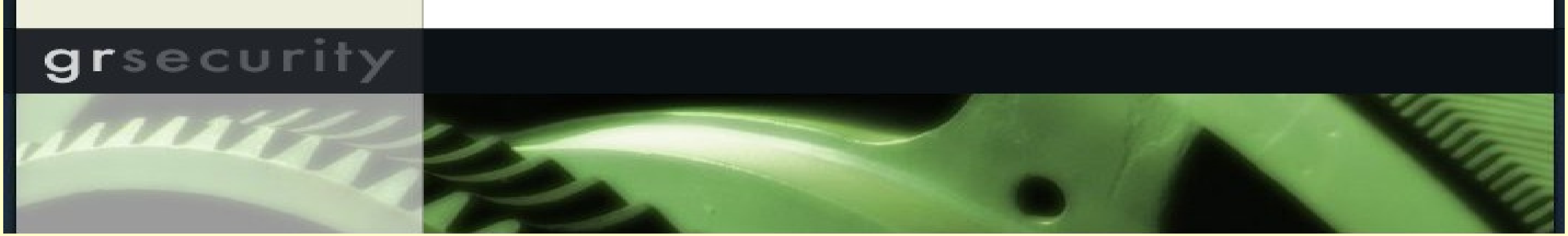
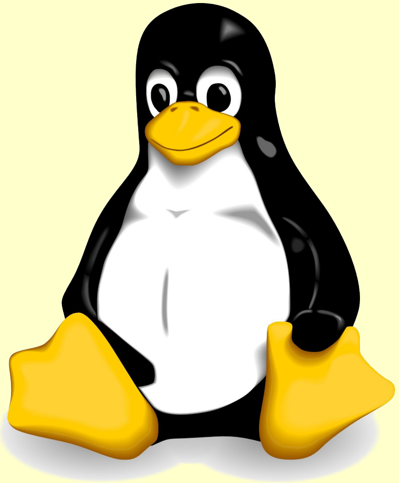


grsecurity

Antonín Slezáček



What is grsecurity?

- Patches for Linux kernel
- Security enhancement emphasis
- Typical usage:
  - Web servers
  - Systems offering shell access
- GNU General Public License

History

- Feb 2001 port of Openwall project
- Linux kernel 2.4
- První vydání pro kernel 2.4.1
- Autor Brad Spengler aka Spender

Installation

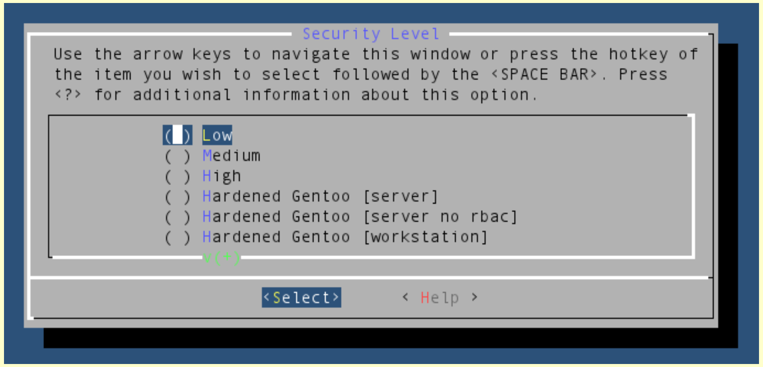
- Stable, Test
- Patches
- Distribution packages
  - Just Debian (.deb) :-(
- CVS checkout
- **Or Hardened Gentoo ;-)**
  - Includes much more ...

My installation experience

- 5 years Gentoo experience → smooth
- http://www.gentoo.org/proj/en/hardened/grsecurity.xml
- # emerge hardened-sources (2.6.34-r6)
- # emerge sys-apps/chpax
- # emerge sys-apps/paxctl
- # emerge pax-utils
- # emerge paxtest
- # emerge gradm
- # sysctl

Configuration

- grsecurity security levels:
  - Low, Medium, High, Custom
- Hardened Gentoo specific:
  - Hardened Gentoo server
    - RBAC
    - No RBAC
  - Hardened Gentoo workstation
    - RBAC
    - No RBAC
    - GRKERNSEC_IO, PAX_NOELFRELOCS, PAX_KERNEXEC



```
                          Security Level
 Use the arrow keys to navigate this window or press the hotkey of
 the item you wish to select followed by the <SPACE BAR>. Press
 <?> for additional information about this option.

                 ( ) Low
                 ( ) Medium
                 ( ) High
                 ( ) Hardened Gentoo [server]
                 ( ) Hardened Gentoo [server no rbac]
                 ( ) Hardened Gentoo [workstation]
                     v(+)
```

grsecurity “features”

- Over 100 security enhancements
- PaX
- RBAC
- Chroot restrictions
- Misc. features
  - Audits
  - Trusted path
  - Prevention gaining unnecessary system knowledge ...

PaX

- Patch that flags
  - data memory (stack) non-executable
  - program memory non-writable
- Prevents exploitation buffer overflow vulnerabilities
- ASLR – Address Space Layout Randomization
  - 32bit → just 16bit of address randomized
- Independent from grsecurity

PaX Demo

KERNEXEC1.gif
KERNEXEC2.gif
CVE-2008-0600

RBAC

- RBAC – Role Based Access Control
- Restrict access further than normal Unix ACL
- Fully least-privilege system
- Roles – granularity (DNS admin, Web admin ...)
- Policy
- Most O(1) time efficiency

RBAC configuration

- # gradmn
- Learning mode
  - Full system: `# gradm -F -L /etc/grsec/learning.logs`
  - Process and Role-based

⚠ Do not perform any administrative tasks outside of the admin role while full system learning is enabled.

  - `# gradm -a admin`
  - Remember to unautenticate with `gradm -u`

Chroot restrictions

- Priviledge escalation attacks
- No attaching shared memory outside of chroot
- No kill outside of chroot
- No mknod
- No mounting or remounting
- No raising of scheduler priority
- No viewing of any process outside of chroot, even if /proc is mounted

Misc. features

- dmesg(8) restriction
- FIFO/Named pipe restrictions
- Nearly all options are sysctl-tunable, with a locking mechanism
- Trusted path
- And much much more ...

Summary

- Plus
  - + Brings security to your system
  - + Easy installation with packages (deb, gentoo)
  - ++ RBAC learning mode !!!
  - + Logging, audits
- Minus
  - - Packages for other distributions
  - - Patching kernel requires at least read the docs ;-(
  - - RBAC configuring requires some knowledge ...

Q & A

Thanks for listening ...

+There are 10 types of people in the the world
-Those that understand binary and those that don't.

```
:(){ :|:& };:
```