

SELinux

(Security Enhanced Linux)

<http://www.nsa.gov/selinux>

Security Enhanced Linux features

- Reduced or eliminated risk from intrusion
- Mandatory Access Control (MAC)
- Role-based access control (RBAC)
- No concept of 'root' *nix permissions still apply
- Policy controlled
- Separates kernel, privileged applications and configurations

SELinux features 2

- Native in 2.6 kernel via LSM framework
- 100% open source
- Independently audited by MANY people worldwide
- Over 900 active users on the mailing list
- No hidden backdoors, traps, spy ware, etc..
- Employs the past 10 years of the NSA's security OS research
- Well documented at www.nsa.gov/selinux

Why secure Linux? / Pitfalls of DAC

- Processes are self governed
- Normal users can compromise the system
- 2 types of access, user and root
- No control over coarse grained services
- DAC assumes code is clean and offers no protection.

Reduced / eliminated intrusion

- Services and users granted minimal access needed to function. No concept of `setuid/setgid`, `su` beyond policy declaration
- Damage from malicious code is reduced or eliminated due to context labeling and domain restrictions
- Domains are unable to access other domains without transition rules
- Proper policy restricts sloppiness of service configuration

Intrusion part 2

- Last layer of protection. SELinux is complementary to existing security implementations
- Root kits: hiding processes, elevated process privileges, hindering forensics and backdoor services becomes extremely difficult or impossible to install
- Buffer overflow only affects the targeted service, not the entire system

Mandatory Access Control

- User can't decide on their objects
- Separate policies restrict classified data
- Containment Policies - Minimizing damage from malicious code
- Protects applications from modification and dangerous usage
- Offers data reliability by segmentation
- Flexibility – Custom policy based on YOUR needs

Role-based access control (RBAC)

- Centralized roles, user_r, staff_r, sysadm_r
- ANSI INCITS 359-2004 (approved 19 Feb 04)
- Access decisions are based on roles
- Roles can overlap for common tasks
- Great flexibility, customized, and spectrum of applications

Unique labeling

- Identity – not system users. Does NOT change with the system user, i.e. su, sudo, unlike DAC
- Domain – determines what a process can/can't do. Restricts processes to specific task, i.e. no setuid root
- Type – objects, decides who gets access, i.e. directory, files, sockets. Uses extended fs security attributes
- Role – defines the access of the domain. i.e. user, staff, sysadm. Restricts users to selected processes

Labeling part 2

- Sample file label: “ls -Z .bash_history”
blacknet:object_r:staff_home_t .bash_history
- Sample process label: “ps - -context | grep bash”
blacknet:sysadm_r:sysadm_t bash
- XATTR – (Extended FS attributes) format is security.selinux. Supported on ext2,ext3 and xfs.

Distro's

- Full support in fedora core 2, debian (woody and sid) and gentoo
- Needs additional patched/lsm aware user land apps, i.e. libselinux1, coreutils, policy
- LSM aware packages included in repositories
- More coming soon!

Needed packages

- libselinux1 - shared libraries
- selinux-policy-default - sample policy files
- checkpolicy - security policy compiler.
- polycoreutils - core utilities
- selinux-utils - operations such as querying the policy.

Packages part 2

- kernel-patch-2.x-lsm - kernel patch, not needed in 2.6 unless updated code/features is needed
- coreutils - modified cp, mv, ls, etc
- procps - modified ps and top
- sysvinit - loads the policy upon boot
- Mandatory packages - sysvinit, logrotate, cron, and pam

Pax/Execshield

■ PaX (Page eXec)

- Not part of SELinux
- I386 Memory Segmentation
- Non-exec data pages
- strict separation of executable pages
- all address are randomized
- Misc.

■ Execshield

- Not part of SELinux
- protection from stack, buffer or function pointer overflows, overwriting data structures and code injection.

Public accessible test boxes

- Root account is unprivileged
- NO PORTSCANS!
- These boxes are not for IRC use, psybnc, DOS attacks, floods or other disruptive tasks
- For your protection:
Disable X11 forwarding
Disable ssh agent forwarding

Fedora Test Box

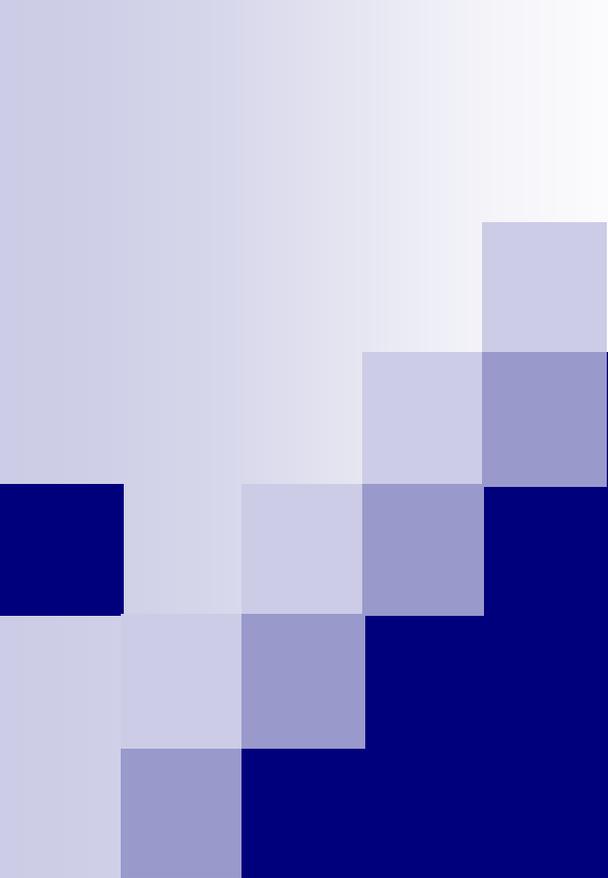
- Fedora project -
<http://www.coker.com.au/selinux/play.html>
- ssh root@**cable.coker.com.au** port **222**, root password is "**fedora**"
- Uses SELinux + Execshield

Gentoo Test Box

- Gentoo project - <http://selinux.dev.gentoo.org/>
- ssh root@**selinux.dev.gentoo.org** root password is “**gentoo**”
- Uses gentoo-hardening tool chain. SELinux + PaX + Misc

Debian Test Box

- Debian project - <http://selinux.simplyaquatics.com/>
- ssh root@**support.simplyaquatics.com** port **2000** root password is “**1234**”
- Uses SELinux + PaX



The end.

Majordomo@tycho.nsa.gov

[#SELinux](irc://irc.freenode.net)