SELinux

Security Enhanced Linux

Gonzalo Nina Mamani
gonzalo@hiperborea.com.bo

Debian Day - Cochabamba

Contenido

¿Quien esta aqui delante?

- Gonzalo Nina Mamani.
- Director Area Seguridad en **Hiperborea IT Security**.
- Fedora Ambassadors Bolivia.
  lorddemon@fedoraproject.org
- Linux user from 2008.
  Started with Debian.

- Correo: *gonzalo@hiperborea.com.bo*
  Twitter: *@lorddemon*
  Facebook: *www.fb.com/gonzalon*

DebianDay

¿Como relacionamos la seguridad informática y GNU/Linux?

DebianDay

Mandatory Access Control

"Mandatory Access Control" o MAC, añade la posibilidad de limitar, denegar, a cualquier sujeto, la posibilidad de iniciar procesos, subprocesos, o en general, el acceso a recursos:

- Archivos
- Directorios
- Bloques de memoria
- puertos TCP/UDP, entre otros.

Operan a nivel del núcleo, por ejemplo, acceder a la red vía un puerto específico, una regla en el propio núcleo le permitirá consultar si ese recurso está disponible para ese servicio.
En GNU/Linux hay al menos 4 MAC conocidos:

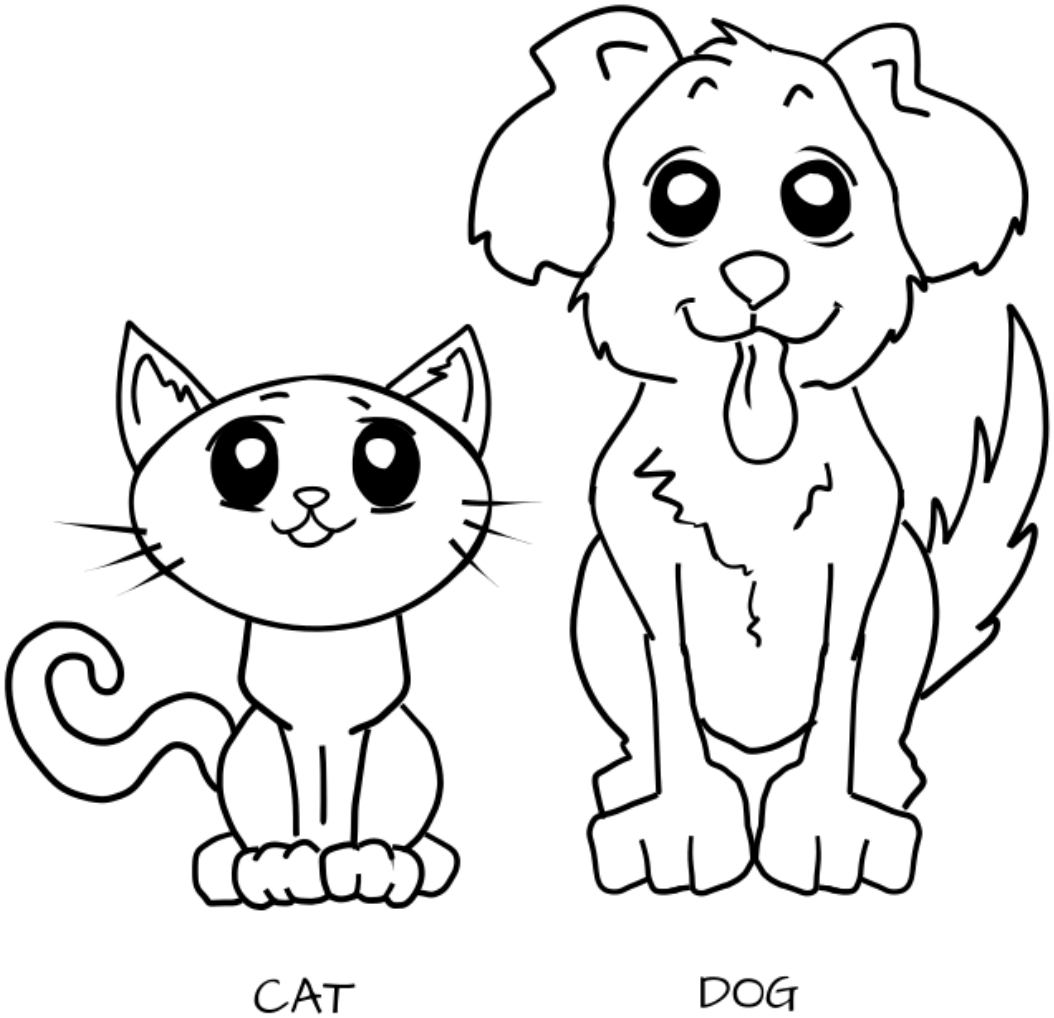
- Tomoyo Linux
- GRSecurity
- AppArmor
- SELinux

SELinux Securiy Enhanced Linux

SELinux Securiy Enhanced Linux

SELinux (Security Enhanced Linux) es uno de los proyectos de un MAC Security Linux más antiguos, SELinux basa sus reglas en tratar “todo elemento” como un objeto, luego, etiquetarlo con permisos que puedan ser entendidos por el núcleo, los procesos son etiquetados y corren cada uno en su propio dominio. Así, se pueden definir reglas de cómo un dominio interactua con los otros, permitiendo un control granular en la seguridad.

Tipos de procesos

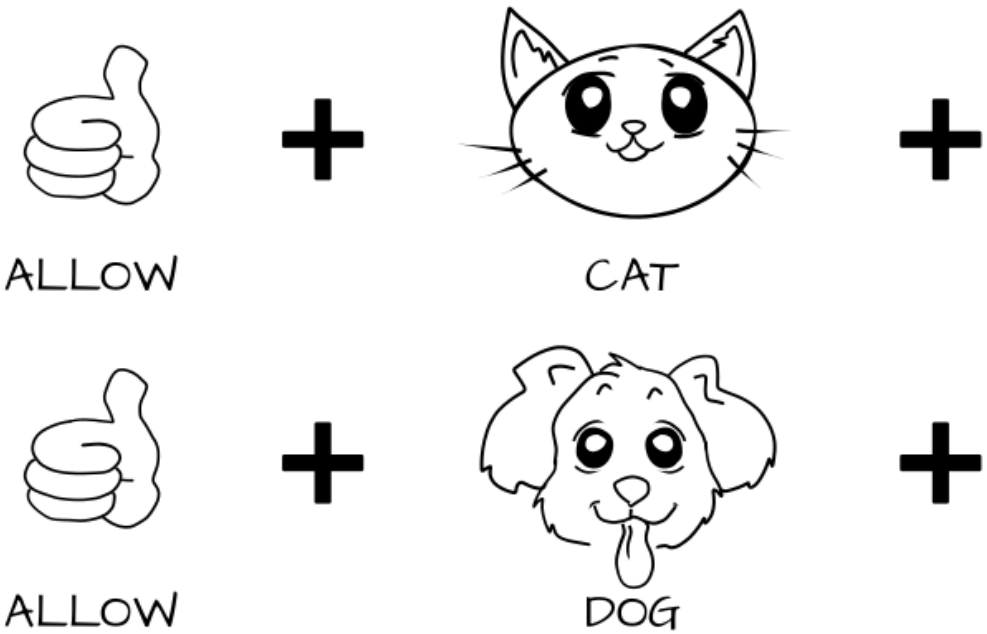


DebianDay

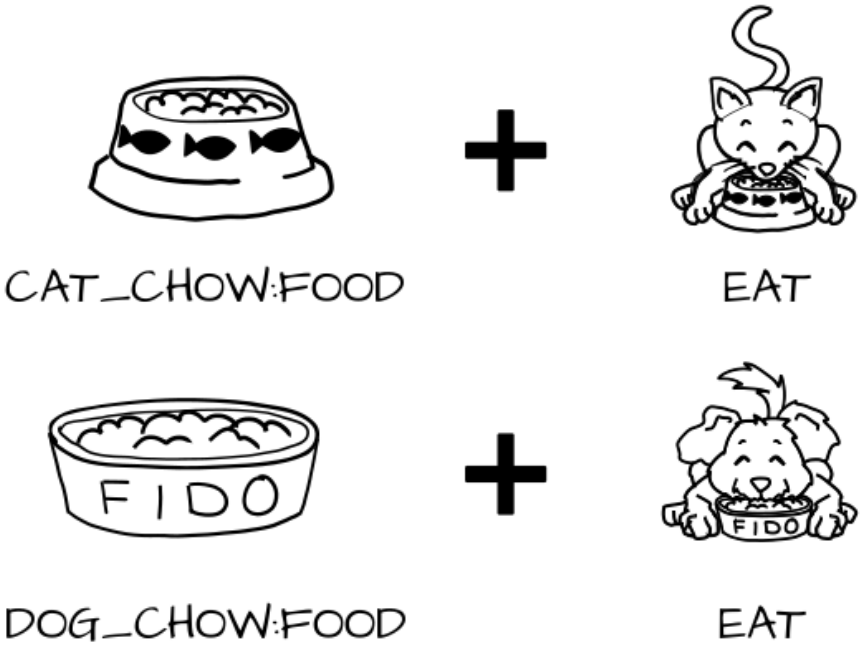
Tipos de Objetos

DebianDay

Politicas por Reglas

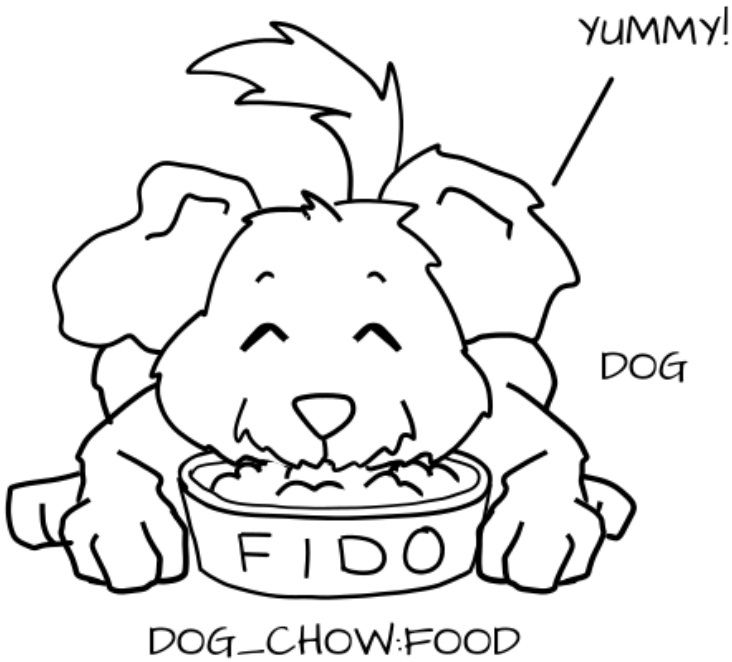


Politicas por Reglas



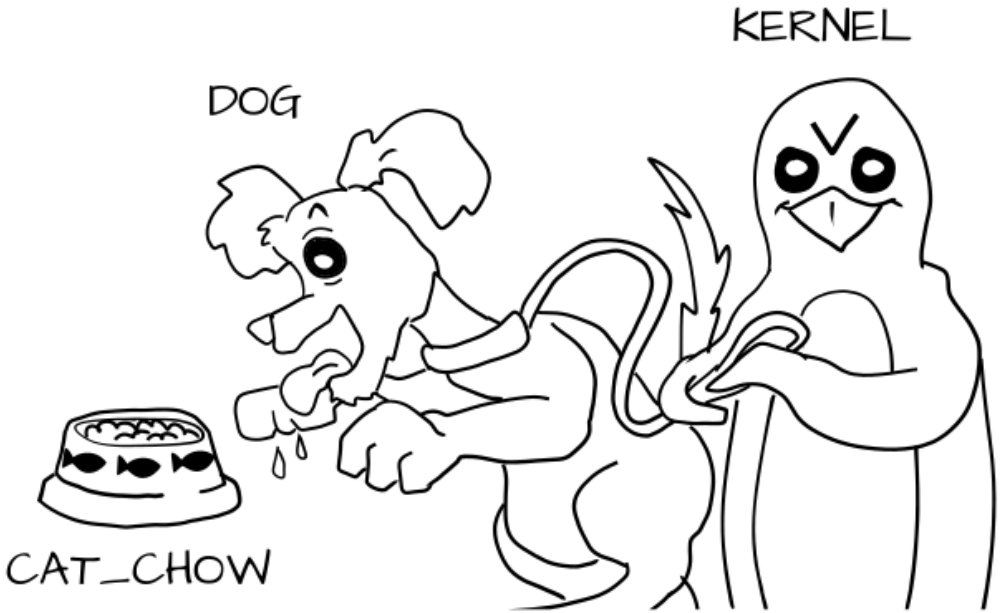
DebianDay

Yummy Yummy



DebianDay

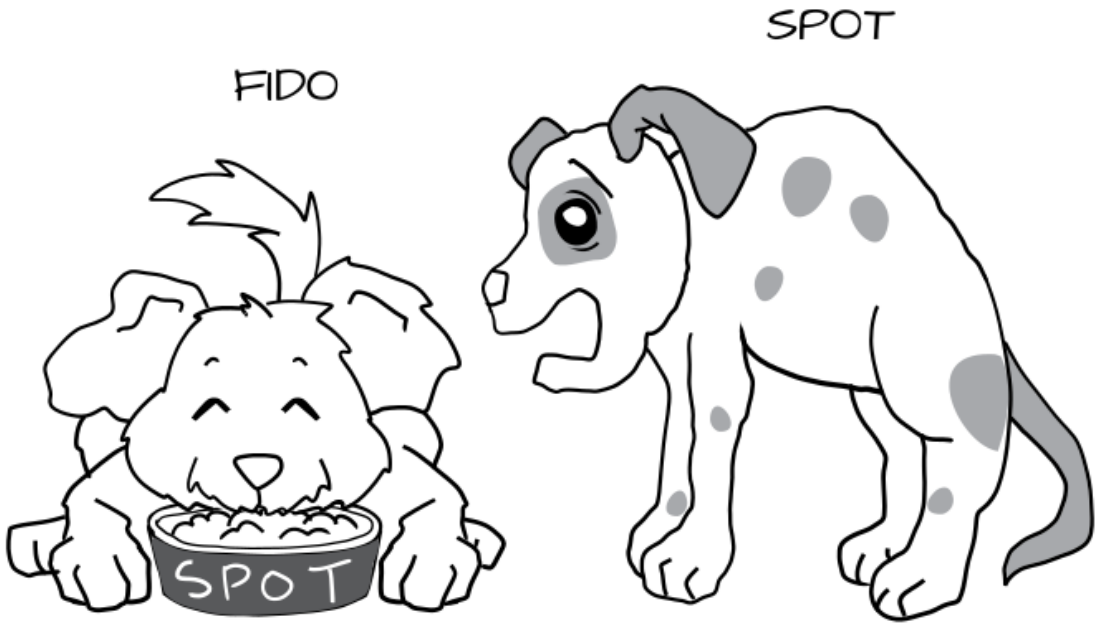
Perro Malo



DebianDay

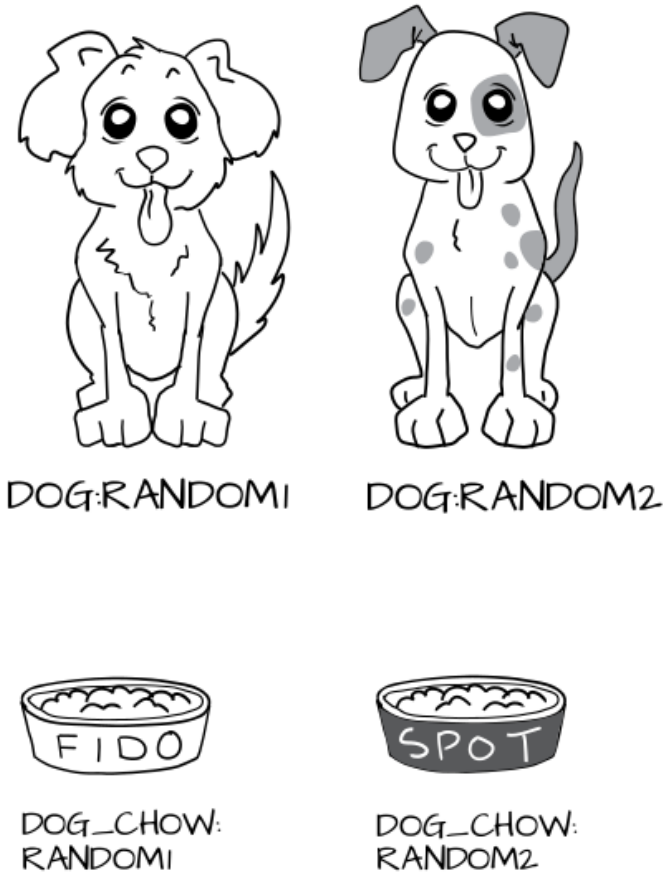
Gato Malo

Multi Category Security MCS



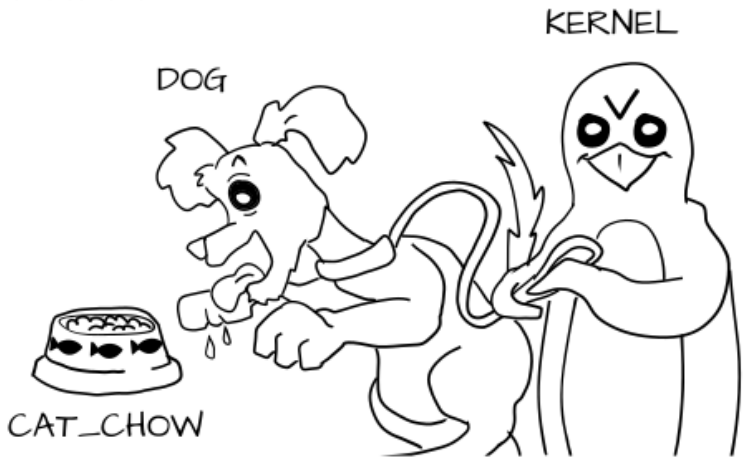
DebianDay

Multi Category Security MCS



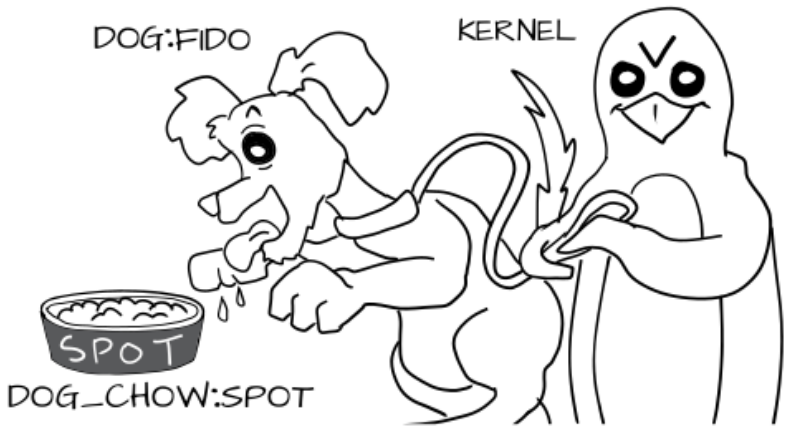
DebianDay

Type Enforcement



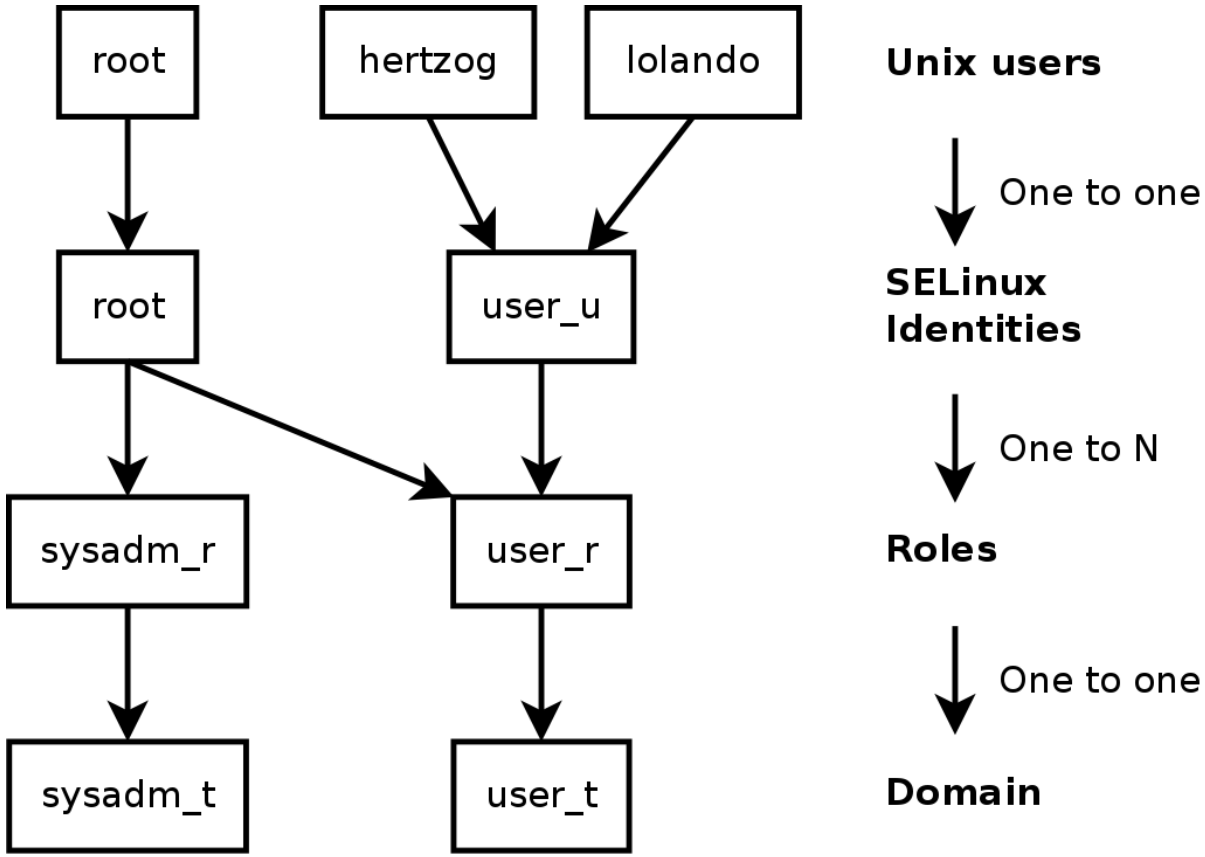
DebianDay

Multi Category Security Enforcement

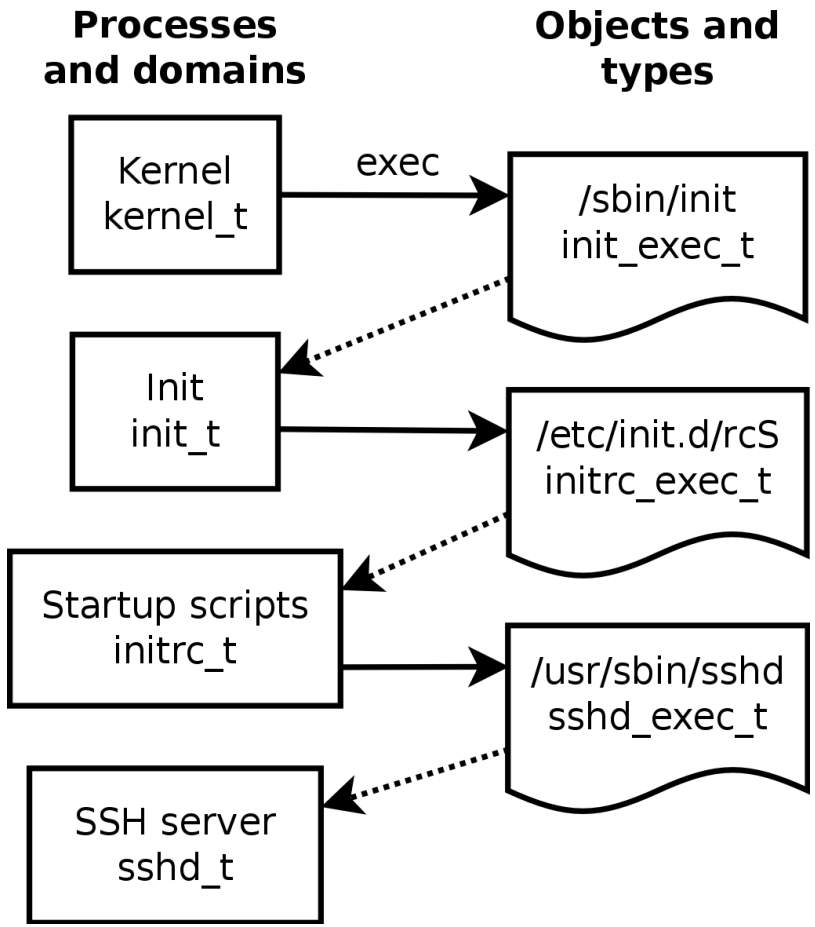


DebianDay

Contextos de seguridad y usuarios Unix



Transiciones automáticas entre dominios



Averiguar el contexto de seguridad

Averiguar el contexto de seguridad

Para averiguar el contexto de seguridad de un proceso

- ps -axZ

Para averiguar el contexto de seguridad em una consola

- id -Z

Por último, para averiguar el tipo asignado a un archivo

- ls -Z /usr/bin/ssh

Referencias


Debian Asegurando Rapidamente Con SELinux
http://blog.phenobarbital.info/2013/07/debian-asegurando-rapidamente-con-selinux/


El libro del administrador de Debian
Seccion 14.4. Introducción a SELinux
https://debian-handbook.info/browse/es-ES/stable/sect.selinux.html


The SELinux Coloring Book
Un libro interesante para entender SELinux.
https://people.redhat.com/duffy/selinux/selinux-coloring-book_A4-Stapled.pdf