Linux kernel POSIX Capabilities

Alberto Molina Coballes

IES Gonzalo Nazareno

16 de enero de 2021

Introducción

- Tradicionalmente dos privilegios:
  - Procesos privilegiados: Se saltan las comprobaciones de permisos
  - Procesos no privilegiados: Comprobación estricta de permisos
- *Kernel Capabilities*: Mecanismo de seguridad basado en el principio de mínimo privilegio, agrupando ciertos privilegios en una “capacidad”
- Se le puede asignar a un proceso una capacidad específica a nivel del kérnel (*kernel capability*)
- No son originales de linux: POSIX capabilities, detalladas en el borrador (retirado) 1003.1e:
  `http://wt.tuxomania.net/publications/posix.1e/download.html`

Lista de capacidades

`man 7 capabilities`

Algunos ejemplos:

- `CAP_CHOWN`
- `CAP_KILL`
- `CAP_NET_ADMIN`
- `CAP_NET_BIND_SERVICE`
- `CAP_NET_RAW`
- `CAP_SYS_ADMIN`
- `CAP_SYS_MODULE`
- `CAP_SYS_RAWIO`
- `CAP_SYS_TIME`

Conjuntos de capacidades de un ejecutable

- Se pueden definir los siguientes conjuntos de capacidades a un ejecutable

  Permitidas(p) Automáticamente permitidas, independientemente de las capacidades heredadas del proceso padre

  Heredables(i) Se añaden al proceso junto con las del proceso padre para determinar las capacidades permitidas

  Efectivas(e) Usadas para permitir capacidades de linux en aplicaciones que no las soportan directamente

`Andy Pearce: File Capabilities In Linux`

Definiendo capacidades

- Se instala el paquete `libcap2-bin`
- `setcap`: Define las capacidades de un fichero
- `getcap`: Obtiene las capacidades de un fichero
- `getpcaps`: Lista las capacidades de un proceso