Linux Kernel Hardening

Alvaro Soto (@alsotoes)
http://headup.ws - alsotoes@gmail.com

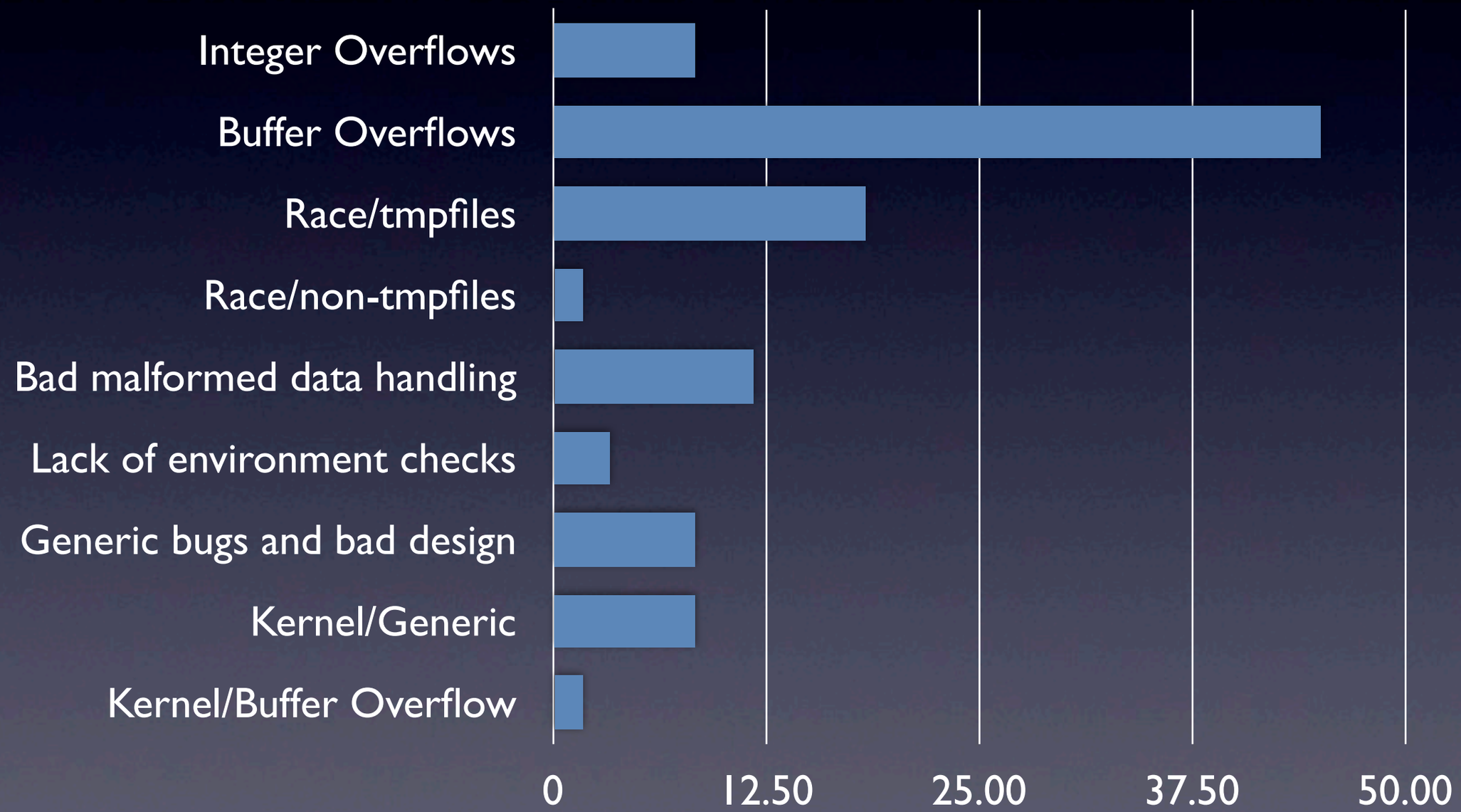
Alvaro que?

- Developer
- Infraestructura // Arquitecturas OpenSource
- Hardening & Tuning geek... freak
- Linux (Gentoo Lover)
- Kernel Vanilla Sources

Por que hardening al Kernel ?

- Por triste que suene... el Kernel de Linux no posee herramientas contra muchos tipos de ataques.
- En cuanto a la memoria, por defecto deja hacer lo que se antoje.
- Y en controles de acceso DAC estrictamente no cuenta como esquema de seguridad... avanzado

Estatus de vulnerabilidades



USN Analysis

Entonces:

¿ Es seguro el Kernel de Linux ?

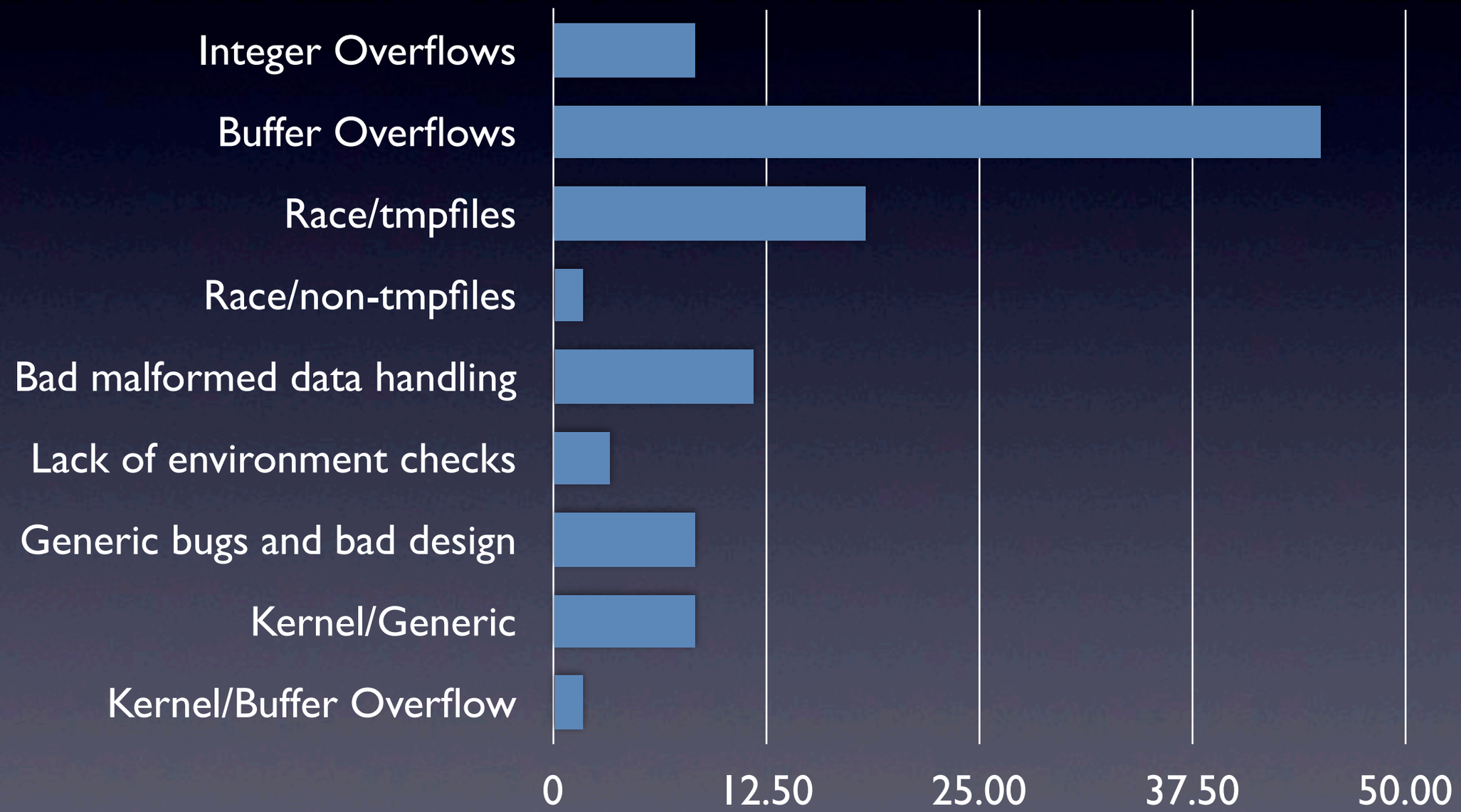
¿ Que tan seguro es ?

Entonces:

¿ Se puede asegurar ?

¿ Que tanto ?

Estatus de vulnerabilidades

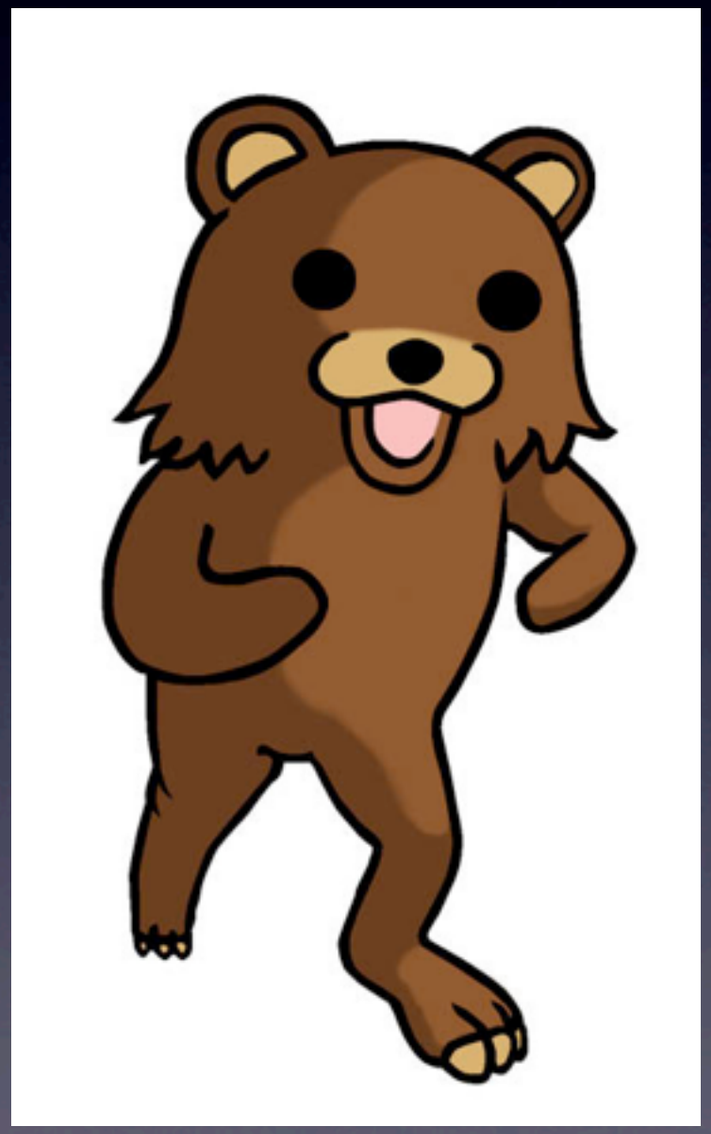


USN Analysis

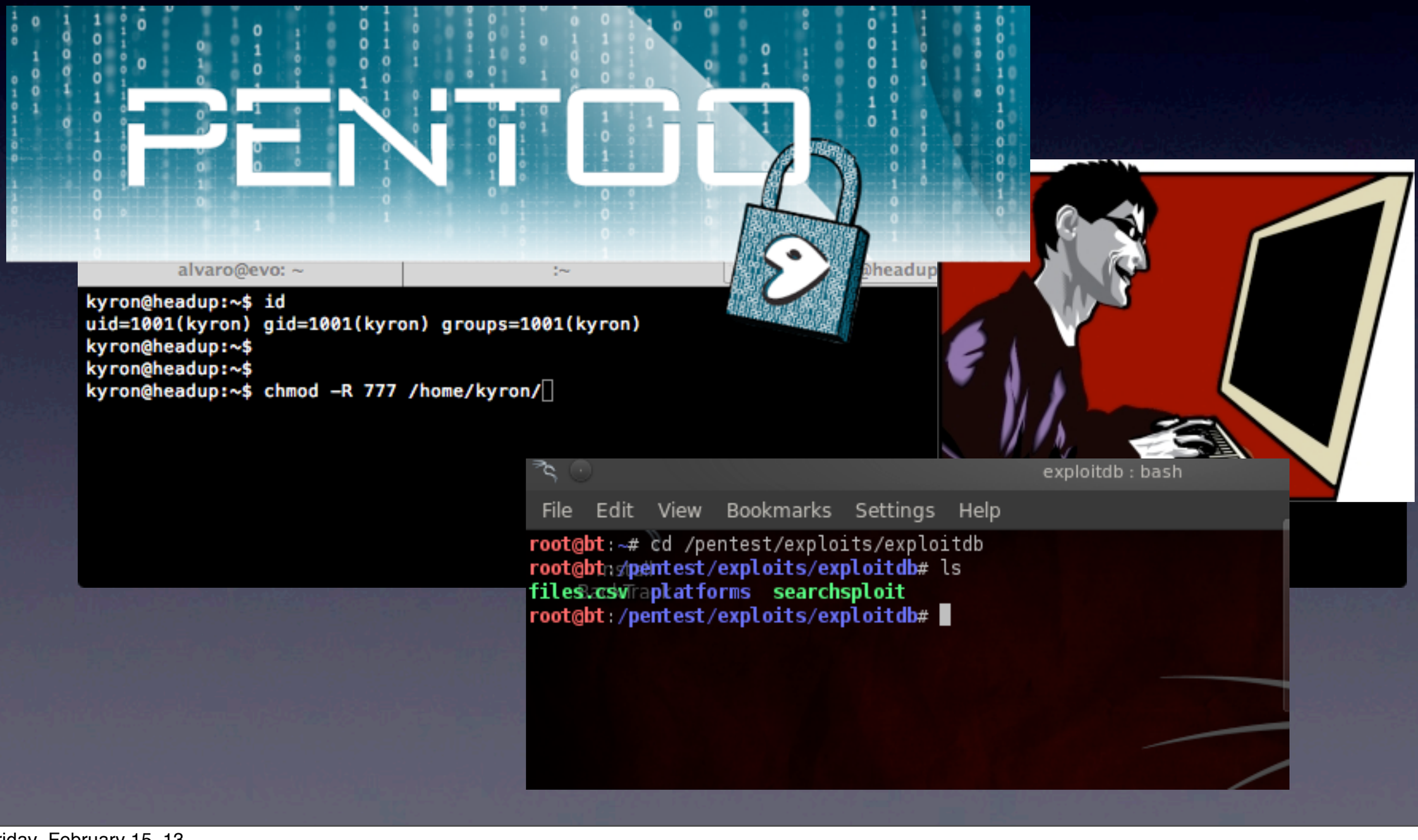
Contra que necesitamos protección?

?

Contra que necesitamos protección?



Contra que necesitamos protección?



Contra que necesitamos protección?

- Controles de acceso
  - DAC v/s MAC..... no mas chmod 777 a todo lo que se pueda.
  - El usuario root es omnipotente.
- Memoria.
  - Modificación del address space.
  - Ejecución de codigo arbitrario.
- Filesystem.
  - Races (tmp races).
  - chroot

Condideraciones “básicas”

- De bajo a alto nivel.
- Configurar cada rincón del sistema.
- Estándares y politicas de seguridad.
- Instalar parches de seguridad continuamente.
- Auditar cada acción del sistema.

RTEM

DAC v/s MAC

DAC v/s MAC

- Usuarios no pueden cambiar sus politicas de seguridad.
- Se puede separar el espacio de trabajo de los usuarios con distintos contextos.
- Politicas muy bien definidas:
  - Usuarios, archivos, directorios
  - Memory, Sockets, tcp/udp ports... etc., etc.

Memory Protection

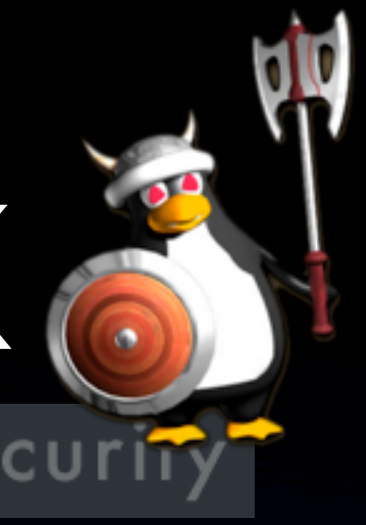
- DEP (Data execution prevention).
    - Se divide la memoria en ejecutable y lectura.
- ASLR (Address space layout randomization).
    - Tareas del kernel.
    - Posición de las librerias.
    - Tareas del usuario (userland stack).
- UNA VIOLACION DE ALGUNA DE ESTAS POLITICAS PRODUCE QUE EL KERNEL MATE EL PROCESO, CAMBIANDO UN POSIBLE ACCESO POR UN DOS.

GRSecurity & PAX

V/S

SELinux

GRSecurity & PAX



- Control de acceso Mandatorio por medio de RBAC definidas en ACL.
- Generación automatica de reglas.
- Proteccion del filesystem con bloqueos de:
    - chroot
    - mount
    - mknod

SELinux

- Un ejemplo de Mandatory Access Control para Linux.
- Etiquetar todo a lo que necesita aplicar una politica.
    - user:role:type:level(opcional)
- Comandos con argumentos extendidos ----->>>> -Z
    - ls -Z
    - id -Z
    - ps -Z
    - netstat -Z

Preguntas ????

GRACIAS !!!!!