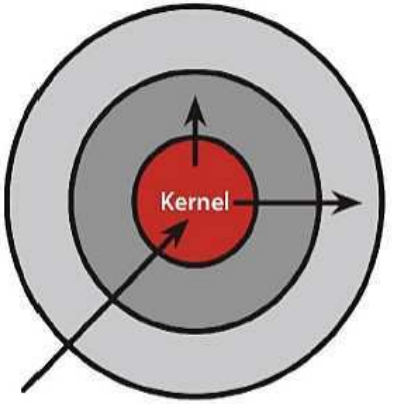
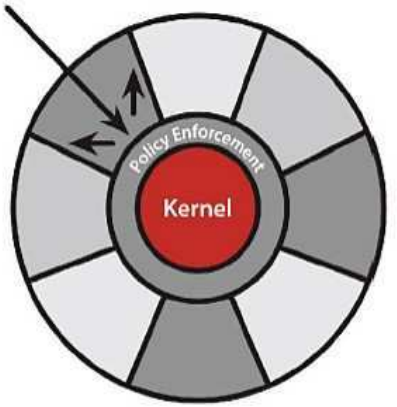
Discretionary Access Control

- Modelo usado por la mayoría de los sistemas operativos
- Los usuarios tienen el control (discreción) sobre sus ficheros y programas
- Los programas se ejecutan bajo los privilegios de un usuario
- El superusuario/root tiene todo el control
- El objetivo de un atacante es vulnerar un programa que se ejecute con privilegios de root



Discretionary Access Control

Once a security exploit gains access to priveleged system component, the entire system is compromised.

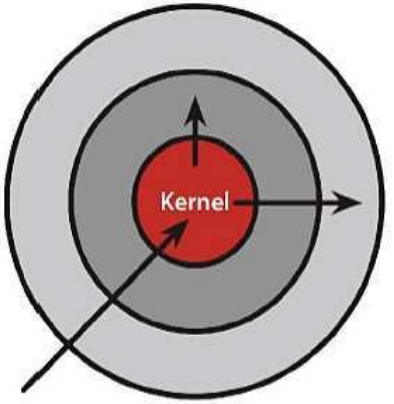


Mandatory Access Control

Kernel policy defines application rights, firewalling applications from compromising the entire system.

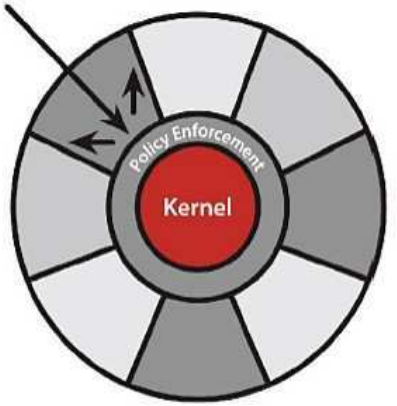
Mandatory Access Control

- Las aplicaciones seguras requieren un SO seguro
- La política de seguridad es el último árbitro de todas la decisiones de acceso; los usuarios no pueden ignorar/anular la política
- Suplementa a DAC
- Múltiples modelos: Type Enforcement, RBAC, Multi-Level Security
- Beneficios: integridad y/o confidencialidad



Discretionary Access Control

Once a security exploit gains access to priveleged system component, the entire system is compromised.



Mandatory Access Control

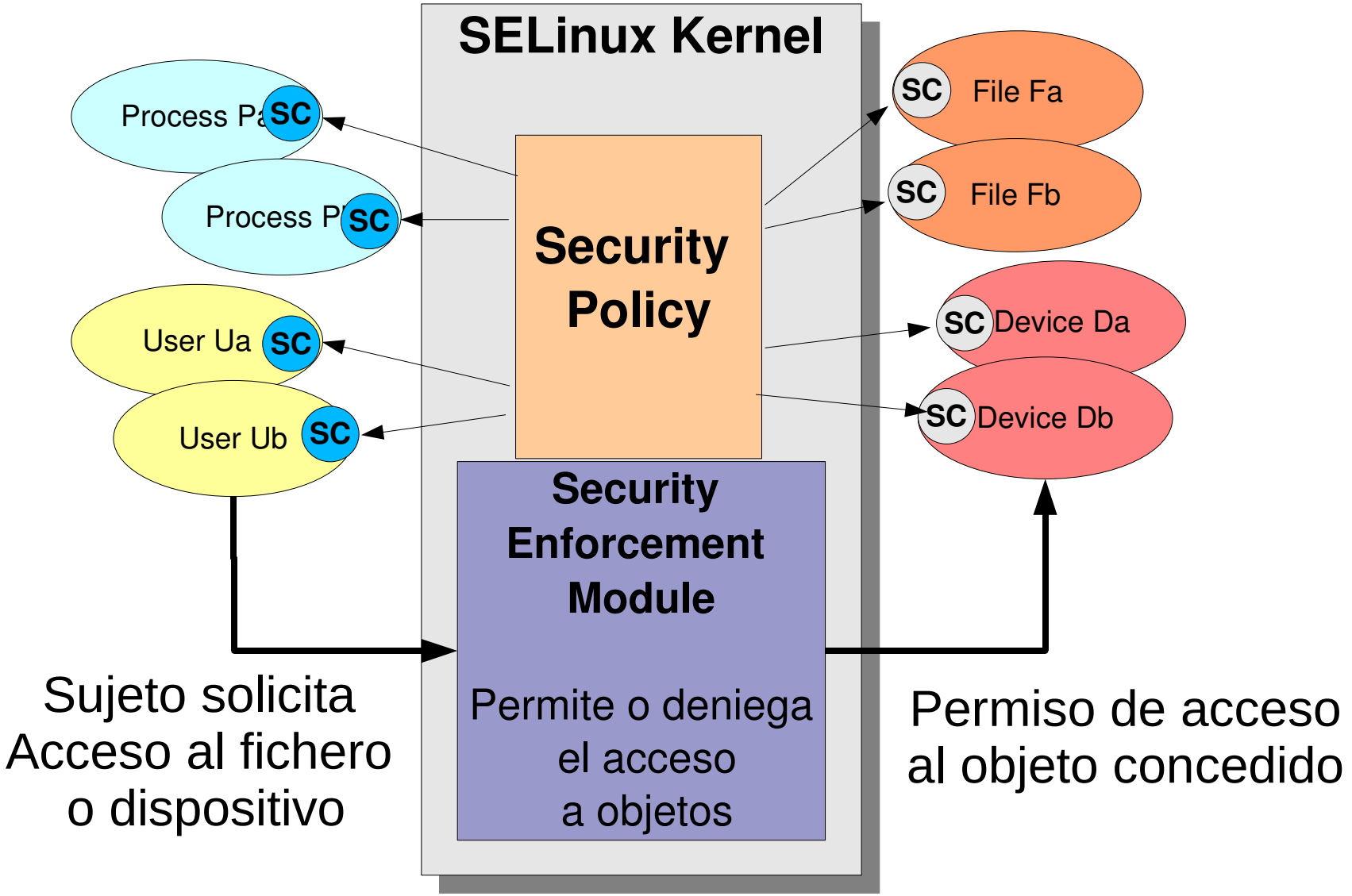
Kernel policy defines application rights, firewalling applications from compromising the entire system.

redhat

Discrecional versus Obligatorio

- Discretionary Access Control – El dueño de un objeto define el acceso al mismo
  - Este es el modelo actual de Linux
  - chmod, open, rename, write, ptrace (!)
- Mandatory Access Control – La seguridad es definida mediante una política centralizada
  - La política no puede evitarse ni accidental ni deliberadamente por software o usuarios maliciosos
  - Previene fugas de información o escalado de privilegios incluso a causa de una mala configuración
  - El administrador de seguridad puede asegurar que dos dominios nunca interactúen, incluso si ambos han sido comprometidos
    - Por ejemplo, el servidor web y la base de datos raw
  - La política es centralizada, lo que permite un fácil análisis
  - Permite protección contra código no confiable

SELinux – Cómo funciona



Estudio de caso: GPG

- Ejemplo de política estricta
- A veces se requiere que una aplicación que se ejecute por un usuario tenga un contexto de seguridad diferente
- Por ejemplo, GPG se ejecuta en un dominio distinto de modo que el dominio principal del usuario no pueda acceder a la clave secreta (para hacer más difícil robar la clave).
- Si el usuario ejecuta 'gpg' una transición automática al usuario _gpg_t desde user_t toma lugar:

  domain_auto_trans($1_t, gpg_exec_t, $1_gpg_t)
- Los ficheros GPG están protegidos de manera que sólo el binario GPG ejecutado por el propietario individual tiene acceso a los ficheros. El usuario no puede soslayar este comportamiento.

redhat

Agenda

- ¿Qué puedo hacer con SELinux?
  - Limitar los privilegios de los programas
  - Proteger de ataques
  - Prevenir acceso del sistema a detalles privados de los usuarios

¿Qué es SELinux?

- Mandatory vs. Discretionary Access Control
  - DAC – mecanismo estándar de Linux
    - Todos los procesos se ejecutan con un usuario y grupo. Si ese usuario/grupo tiene acceso a los ficheros, también el proceso
    - Root y usuarios tienen la capacidad (discreción) de cambiar o soslayar la seguridad con chmod, chown y otras utilidades
    - Procesos que corren como root (por ejemplo servicios de aplicación) pueden acceder a *todo*

¿Qué es SELinux?

- Mandatory vs. Discretionary Access Control
  - MAC – SELinux es una implementación MAC
    - Permisos de granularidad fina en todos los procesos, ficheros, dispositivos, sockets, puertos, etc.
    - Política definida administrativamente
    - Decisiones de seguridad tomadas en base a toda la información, no sólo identidad
    - Procesos ejecutándose como root pueden únicamente acceder a aquellas áreas que la política permite.

¿Qué puedo hacer con SELinux?

- Limitar los privilegios de los programas
  - Los programas son confinados en su propio contexto, incluso programas corriendo como root no pueden acceder a información fuera de su propio contexto de seguridad

¿Qué puedo hacer con SELinux?

- Prevenir accesos del sistema a detalles privados de los usuarios
  - Aún los procesos comprometidos no pueden acceder a los directorios home o ficheros de correo

redhat

Herramientas SELinux

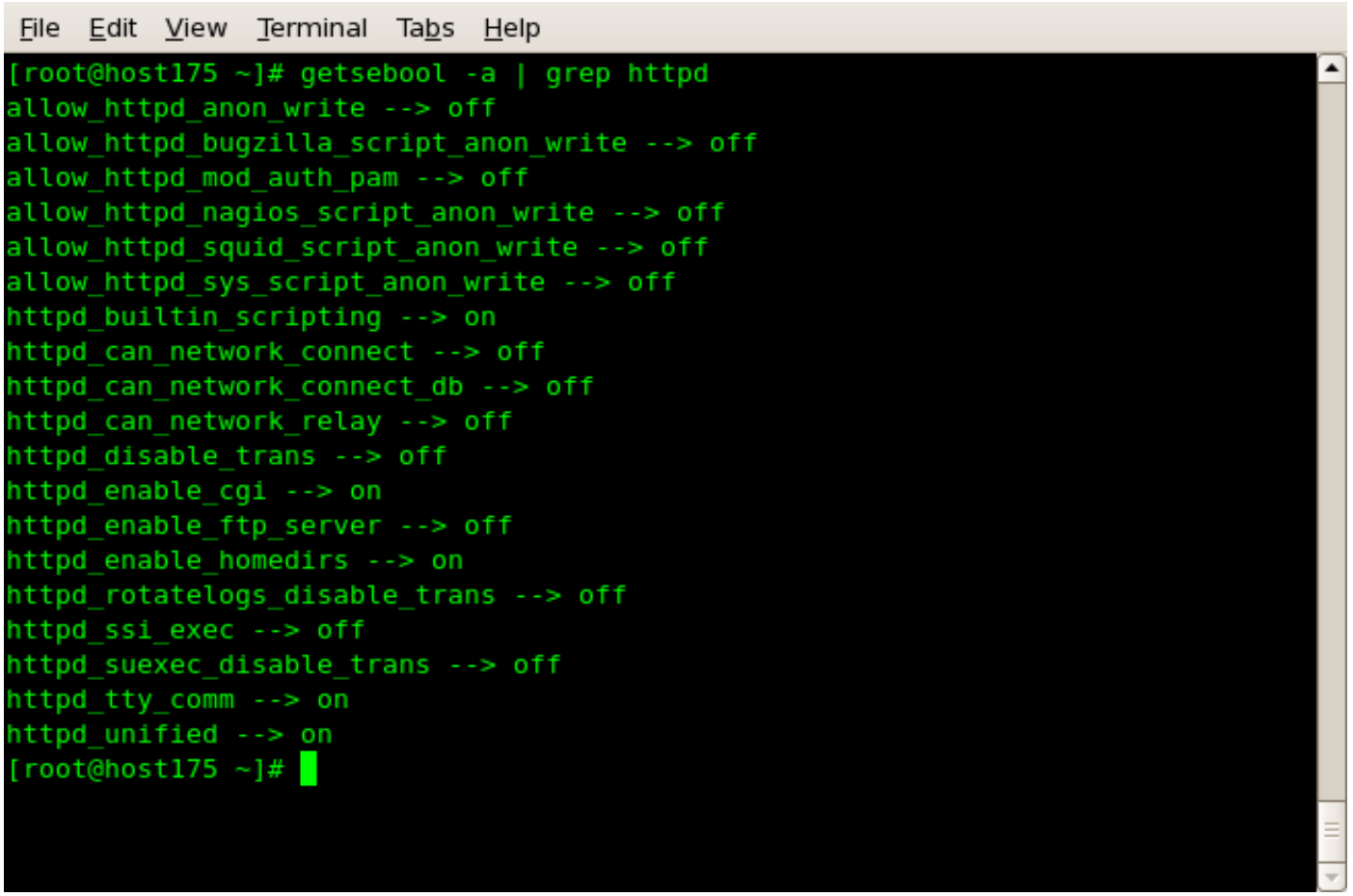
- system-config-selinux
- chcon
- restorecon
- setfiles
- fixfiles
- setenforce
- getenforce
- newrole
- getsebool
- setsebool
- sealert
- setroubleshoot

Valores lógicos de las políticas (Policy Booleans)

- Permiten modificación de la política en tiempo de ejecución
- Cada una tiene un valor por omición, usualmente falso
- 'getsebool' y 'setsebool' para manejarlos
- 'setsebool -P' recompila con los cambios
- Escribe los cambios a:
  - /etc/selinux/targeted/modules/active/booleans.local

Valores lógicos de las políticas (Policy Booleans)

- Se puede mostrar todos los booleanos usando 'getsebool -a' (hay cientos de ellos)



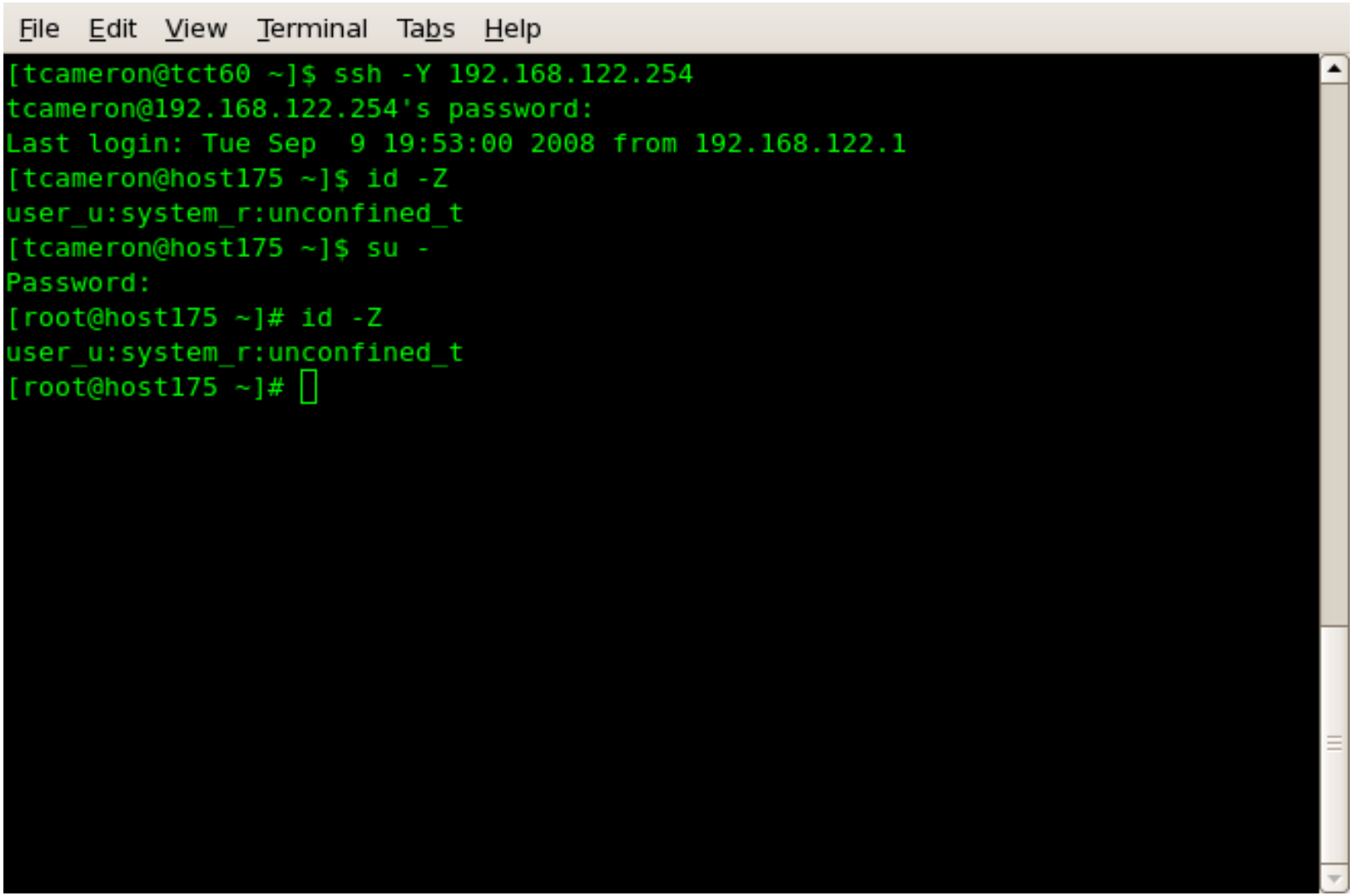
redhat

Información de Contexto de Seguridad

- Casi todos los comandos aceptan el argumento -Z
  - ls -Z
  - id -Z or secon
  - ps -Z
  - mkdir -Z
  - install -Z
  - cp -Z
  - find -context

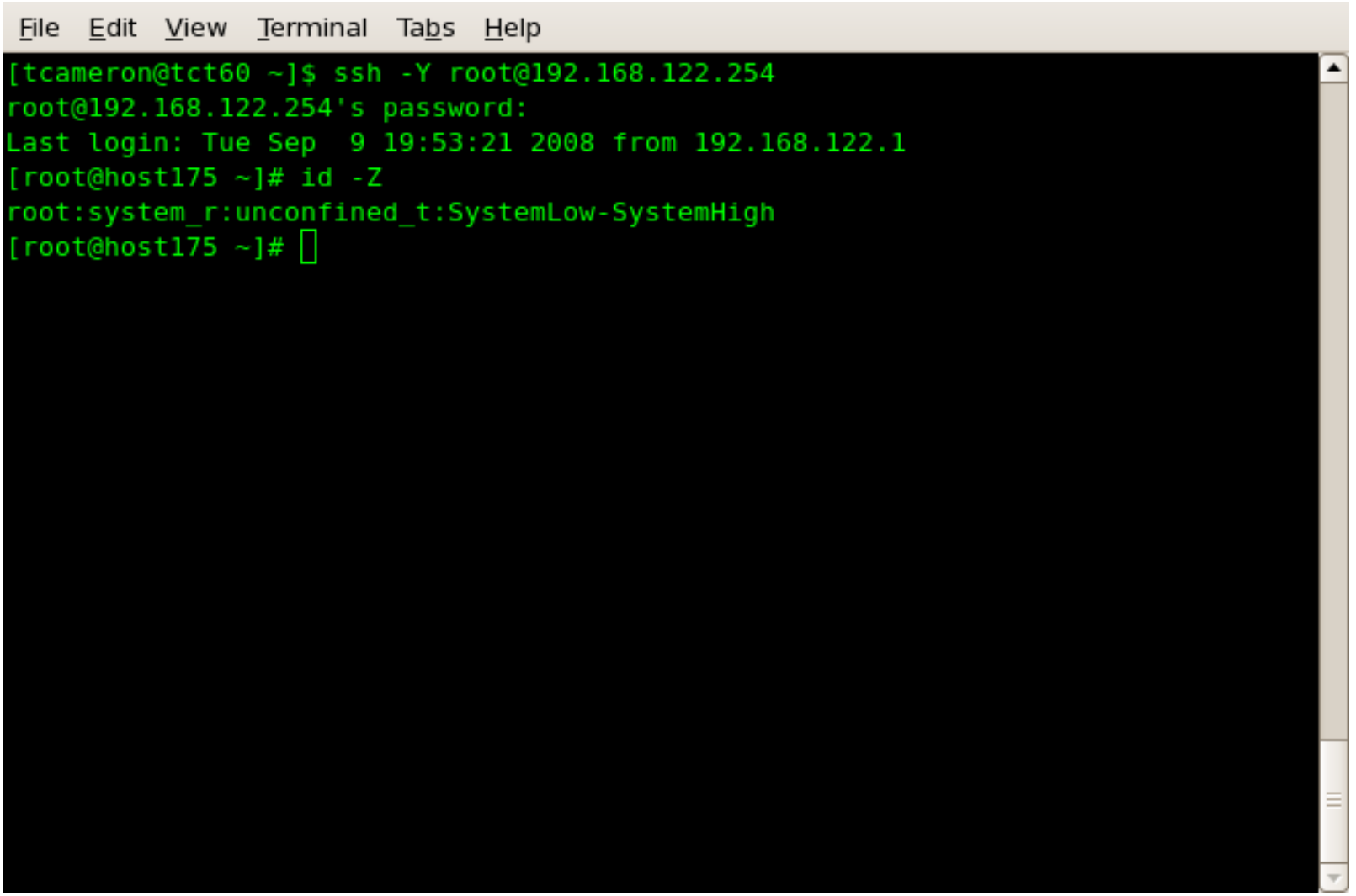
Información de Contexto de Seguridad

- ¡Notese que usando 'su' NO se cambia el contexto correctamente!
- Ejemplo:



Información de Contexto de Seguridad

- En este ejemplo, root entra mediante ssh:
- Ejemplo:



redhat

Ejemplos SELinux

File Edit View Terminal Tabs Help

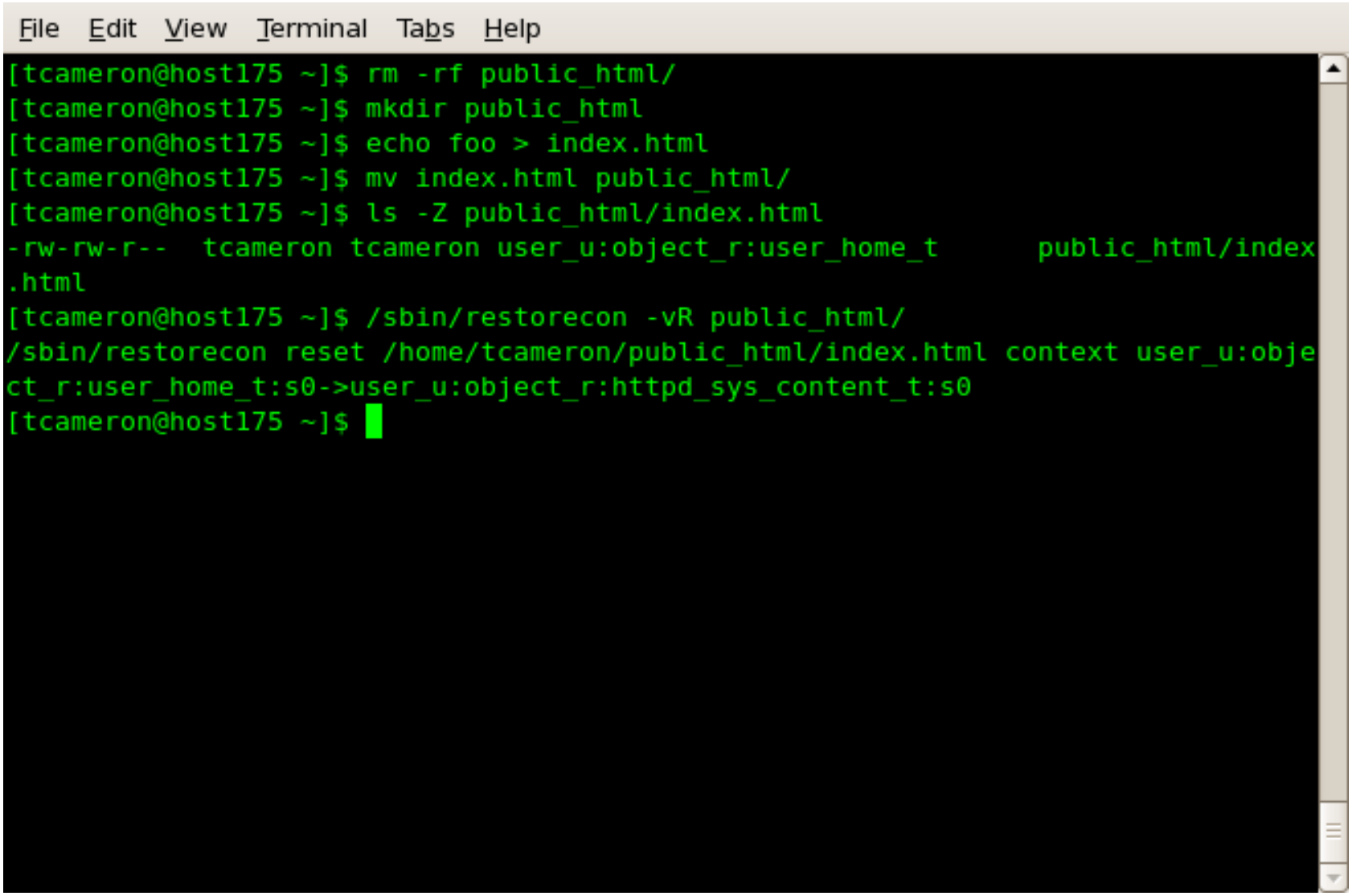
```
[tcameron@host175 ~]$ echo "This is my page" > index.html
[tcameron@host175 ~]$ ls -Z index.html
-rw-rw-r--  tcameron tcameron user_u:object_r:user_home_t      index.html
[tcameron@host175 ~]$ mv index.html public_html/
[tcameron@host175 ~]$ ls -Z public_html/index.html
-rw-rw-r--  tcameron tcameron user_u:object_r:user_home_t      public_html/index
.html
[tcameron@host175 ~]$
```

Ejemplos SELinux

- Usar 'chcon' para cambiar manualmente el contexto

Ejemplos SELinux

- O hacerlo de la manera fácil con 'restorecon':



redhat

Pensamientos finales

- ¡No lo apagues!
- SELinux puede realmente salvarte en el caso de una brecha de seguridad
- Es *mucho* más sencillo usar SELinux hoy que apenas hace unos meses
- Seguridad del nivel de la NSA está disponible sin coste extra - ¡úsala!