Problema de seguridade no acceso dende os clientes Linux ás carpetas compartidas

- Neste apartado imos expoñer un problema de seguridade que se pode dar seguindo os pasos expostos no material do curso para montar as carpetas compartidas do dominio usando *pam_mount*.

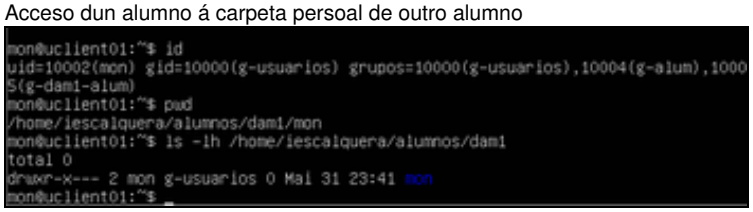
- Este problema podería permitir a lectura por parte dun alumno do contido da carpeta persoal de outro alumno. Veremos cal é o motivo e como resolvelo.

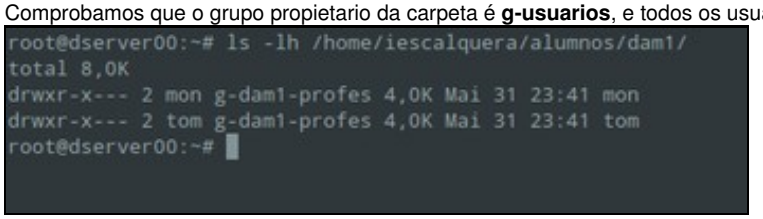
- Amosaremos o problema e a súa solución no escenario baseado en Samba3+LDAP, pero sería similar no caso de Samba4 e integrando o almacenamento en FreeNAS.

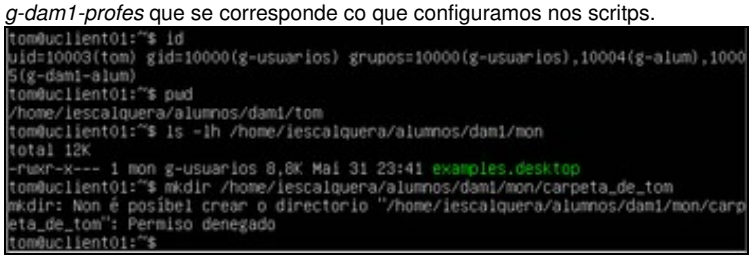
Sumario

Problema de seguridade no acceso ás carpetas com pam_mount

- Nas seguintes imaxes imos mostrar como un alumno (*tom*) podería chegar a acceder á carpeta de outro (*mon*). Móstrase abrindo a sesión en *uclient01* en modo de texto, pero podería facerse en modo gráfico.

- Acceso dun alumno á carpeta persoal de outro alumno
- 

mon inicia sesión en *uclient01*. Está situado na súa carpeta persoal e usamos o comando *ls* para ver os permisos nesta carpeta. Comprobamos que o grupo propietario da carpeta é **g-usuarios**, e todos os usuarios deste grupo poderán ler na carpeta.
- 

Se comprobamos os permisos da carpeta persoal de *mon* en *dserver00*, o grupo propietario da carpeta en realidade non é *g-usuarios*... É *g-dam1-profes* que se corresponde co que configuramos nos scritps.
- 

Se coa sesión de *mon* aberta imos a outra consola virtual e iniciamos sesión con *tom*, vemos como pode ler o contido da carpeta persoal de *mon*, cousa que non deberiamos permitir. Se intentamos escribir na carpeta, os permisos non nolo permitirán.

- No caso exposto, iniciamos sesión nun cliente con un usuario (*tom*) ao mesmo tempo que temos outra sesión aberta (a de *mon*). En principio, *pam_mount* debería desmontar as carpetas montadas cando se pecha a sesión, así que se intentamos facelo pechando a sesión dun usuario e abrindo a do outro pode xa non teríamos o problema.

- Non obstante, temos detectado que en ocasións, seguramente debido a que algún proceso do sistema mantén ficheiros abertos da carpeta persoal, *pam_mount* non desmonta as carpetas ao pechar sesión e continúan montadas. Isto facilitaría aínda máis a posibilidade de que un usuario accedese á carpeta persoal de outro.

- Podemos configurar *pam_moun* para forzar que desmonte as carpetas no peche da sesión, cambiando a seguinte liña do ficheiro de configuración:

```
<logout wait="0" hup="0" term="0" kill="0" />
```

- Deixando o seguinte contido:

```
<logout wait="2000" hup="0" term="1" kill="1" />
```

- Aínda así, o problema podería darse se dous usuarios abren sesións de forma simultánea no equipo, ben en local ou de forma remota (accedendo por ssh, por exemplo).

Explicación: Causa do problema

- Agora ben, por que ocorre isto? Que é o que provoca que os permisos das carpetas persoais nos equipos cliente non se corresponda cos que teñen en *dserver00*?

- A razón de que os propietarios e grupos non se correspondan no cliente e no servidor é que CIFS non propaga os permisos do servidor no cliente; hai que ter en conta que aínda que no noso caso os usuarios e grupos que existen nun tamén existen no outro porque os dous están configurados para autenticar contra o mesmo servidor LDAP, isto non tería por que ser así e os usuarios e grupos do servidor polos que se establecen os permisos nas carpetas non teñen que existir no cliente.

- Por iso, o que fai o cliente é poñer sempre como usuario propietario o do usuario que monta a carpeta e como grupo o seu grupo principal, aínda que logo é o servidor o que vai verificar os permisos no acceso á carpeta por CIFS.

- O problema é que sempre vai usar as credenciais que se introduciron ao montar a carpeta, e por iso *tom* pode fisgonear na carpeta de *mon*, xa que está usando as súas credenciais.

Proposta para resolver o acceso ás carpetas persoais dos usuarios

- Polo tanto, unha solución pode ser establecer uns permisos na carpeta na que se monta que só permita o acceso ao usuario que a monta, e no caso dos alumnos ao grupo dos profes do seu curso.

- O comando **mount.cifs** (que é o que usamos en *pam_mount* para montar as carpetas por cifs) permite forzar o uid e o gid que o cliente vai poñer como permisos das carpetas aos que nos queiramos, en lugar de que sexan o usuario que monta a carpeta e o seu grupo principal (que é *g-usuarios*, e aí é onde temos o problema).

- Así que podemos modificar as liñas do ficheiro *pam_mount.conf.xml* que montan as carpetas persoais dos usuarios:

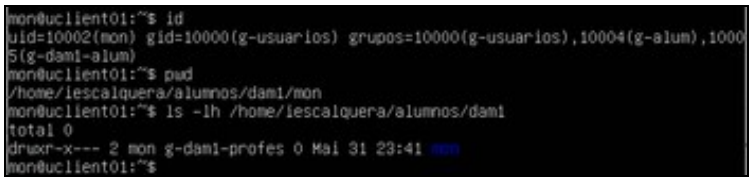
```
<volume sgrp="g-profes" fstype="cifs" server="dserver00" path="%(USER)" mountpoint="/home/iescalquera/profes/%(USER)" options="iochar


<volume sgrp="g-dam1-alum" fstype="cifs" server="dserver00" path="%(USER)" mountpoint="/home/iescalquera/alumnos/dam1/%(USER)" option

<volume sgrp="g-dam2-alum" fstype="cifs" server="dserver00" path="%(USER)" mountpoint="/home/iescalquera/alumnos/dam2/%(USER)" option
```

- Deixándoas da seguinte maneira:

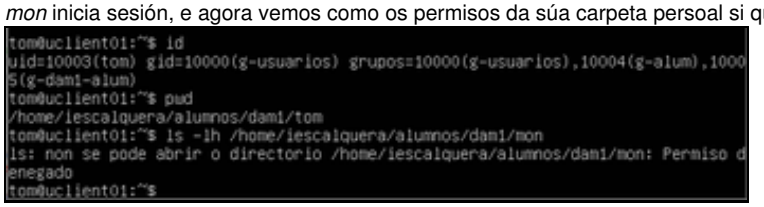
```
<volume sgrp="g-profes" fstype="cifs" server="dserver00" path="%(USER)" mountpoint="/home/iescalquera/profes/%(USER)" options="iochar


<volume sgrp="g-dam1-alum" fstype="cifs" server="dserver00" path="%(USER)" mountpoint="/home/iescalquera/alumnos/dam1/%(USER)" option

<volume sgrp="g-dam2-alum" fstype="cifs" server="dserver00" path="%(USER)" mountpoint="/home/iescalquera/alumnos/dam2/%(USER)" option
```

- Desta forma, veremos como *tom* xa non poderá acceder á carpeta de *mon*:

- Solución ao acceso ás carpetas de outros usuarios

- 
```
mon@uclient01:~$ id
uid=10002(mon) gid=10000(g-usuarios) grupos=10000(g-usuarios),10004(g-alum),1000
5(g-dam1-alum)
mon@uclient01:~$ pwd
/home/iescalquera/alumnos/dam1/mon
mon@uclient01:~$ ls -lh /home/iescalquera/alumnos/dam1
total 0
drwxr-x--- 2 mon g-dam1-profes 0 Mai 31 23:41 mon
mon@uclient01:~$
```

mon inicia sesión, e agora vemos como os permisos da súa carpeta persoal si que se corresponden cos de *dserver00*.

- 
```
tom@uclient01:~$ id
uid=10003(tom) gid=10000(g-usuarios) grupos=10000(g-usuarios),10004(g-alum),1000
5(g-dam1-alum)
tom@uclient01:~$ pwd
/home/iescalquera/alumnos/dam1/tom
tom@uclient01:~$ ls -lh /home/iescalquera/alumnos/dam1/mon
ls: non se pode abrir o directorio /home/iescalquera/alumnos/dam1/mon: Permiso d
enegado
tom@uclient01:~$
```

Desta maneira, *tom* non pode acceder á carpeta de *mon* aínda que estea montada, xa que non pertence ao grupo *g-dam1-profes*.

Proposta para resolver o acceso a outras carpetas compartidas

- Este mesmo problema podería darse con outras carpetas montadas con *pam_mount*, como no noso caso é carpeta *comun* ou a das carpetas persoais dos alumnos á que acceder os profes.

- Se revisamos a configuración de *pam_mount* para a montaxe destas carpetas:

```
<volume sgrp="g-usuarios" fstype="cifs" server="dserver00" path="comun" mountpoint="/media/comun" options="iocharset=utf8"/>


<volume sgrp="g-profes" fstype="cifs" server="dserver00" path="alumnos" mountpoint="/home/iescalquera/alumnos" options="iocharset=utf
```

- Podemos concluír que se dous usuarios inician sesión simultaneamente nun equipo cliente montarán a mesma carpeta remota sobre a mesma carpeta do equipo cliente, o que podería permitir a un usuario acceder a esa carpeta coas credenciais do outro.

- Para evitalo, podemos facer as montaxes de cada usuario nunha carpeta co seu nome dentro de */media*, modificando o ficheiro de configuración de *pam_mount*:

```
<volume sgrp="g-usuarios" fstype="cifs" server="dserver00" path="comun" mountpoint="/media/%(USER)/comun" options="iocharset=utf8"/>


<volume sgrp="g-profes" fstype="cifs" server="dserver00" path="alumnos" mountpoint="/media/%(USER)/alumnos" options="iocharset=utf8"/
```

- E para asegurarnos que na carpeta */media/usuario* só pode acceder o usuario correspondente introducimos no ficheiro */etc/profile* (que se executa cada vez que o usuario inicia sesión) o seguinte comando:

```
chmod 700 /media/$USER
```

- Así se inicia sesión *tom* (que é alumno), monta *comun* en */media/tom/comun*, e se inicia sesión *sol* (que é profe) monta *comun* en */media/sol/comun*. *tom* non pode entrar no *comun* de *sol* e *sol* non pode entrar no *comun* de *tom*.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez