

Como falsear a autenticación do usuario en NFS

No apartado anterior xa vimos que en NFS, un usuario pode facerse pasar por outro, simplemente con que o seu *uid* coincida. Nese caso o falseamento da identidade non foi intencionado, pero xa deixa en evidencia o fácil que resulta poder acceder a datos compartidos por NFS sobre unha carpeta na que non temos permisos. Poñamos un caso intencionado:

Se queremos acceder aos datos do usuario *felipe*, simplemente precisamos unha máquina que non tome os usuarios do LDAP; válenos perfectamente un live-CD, mesmamente o de instalación de Ubuntu. Faríamos o seguinte:

- Montar a carpeta compartida por NFS á que queremos acceder:

```
sudo mkdir /home/iescalquera  
sudo mount 10.0.0.100:/home/iescalquera /home/iescalquera
```

- Engadimos un usuario local na máquina que teña o mesmo *uid* que o usuario polo que nos queremos facer pasar (se o equipo toma os usuarios do LDAP, isto nos daría un erro ao estar o *uid* repetido):

```
sudo useradd -u 10001 falsofelipe
```

- Nos poñemos como o usuario que acabamos de crear:

```
sudo su falsofelipe
```

- Xa podemos acceder á carpeta persoal de *felipe* cos mesmos privilexios que *felipe*. Neste caso, aínda que os permisos da carpeta persoal de *felipe* permiten ler a calquera, veremos que podemos escribir e modificar:

```
cd /home/iescalquera/felipe  
touch ficheiro_na_carpeta_de_felipe.txt
```

Así, podemos ver non é necesario utilizar ferramentas de *cracking* nin ter

grandes coñecementos para "reventar" o sistema de seguridade de NFS: con un live-CD de calquera distribución de Linux e uns mínimos coñecementos de NFS podemos acceder a toda a información que queiramos. ¿Cal é a causa desta vulnerabilidade? Pois un erro de seguridade básico. En NFS o servidor **confía** na autenticación realizada polos equipos cliente, e asume que o usuario é o que o equipo cliente lle di que é. Desta forma, se podemos tomar o control ou simplemente suplantar un equipo cliente, poderemos comprometer seriamente a seguridade do servidor. ¿Podemos confiar na autenticidade e seguridade de todos os equipos cliente da nosa rede?

Solucións en NFSv3

En NFS versión 3, as solucións ofrecidas para aumentar a seguridade no servidor NFS consisten na restrición segundo as direccións IP dos equipos cliente. Aínda que eleva algo a seguridade do sistema, realmente a restrición de direccións IP non supón un método de autenticación seguro, xa que calquera pode arrancar un live-CD e configuralo coa mesma dirección IP que un cliente do noso dominio, e xa ten acceso ao servidor... ¿E se bloqueamos na BIOS dos equipos o arranque de CD, ou usb? Calquera pode cambiar a BIOS e arrancar co CD ¿E se protexemos a BIOS con contrasinal? Calquera pode abrir o equipo e retirar a pila da BIOS para borrar ese contrasinal ¿E se pechamos os equipos con un candado para que non se poidan abrir? Calquera pode usar unha máquina virtual e facer o ataque igualmente ¿E se bloqueamos o uso das máquinas virtuais? Calquera pode traer un portátil, miniportátil, PDA,... e facer o ataque igualmente ¿E se...?

Poderíamos seguir indefinidamente, pero en realidade sempre haberá algunha forma de saltarse a restrición. Aínda que, por suposto, ningún método é realmente seguro, neste caso non podemos considerar que a restrición por direccións IP garanta un nivel mínimo de seguridade para o servidor NFS, así que haberá que buscar unha mellor solución.

Solucións en NFSv4: Kerberos

Esta solución que buscamos apórtaa NFS versión 4 con **Kerberos**, xa que así temos un servidor de autenticación que nos permitirá verificar que os usuarios que acceden ao servidor realmente son os que din ser, porque será o servidor de kerberos os que os "avale". Esta opción si que proporciona un nivel de seguridade aceptable ao servidor NFS, xa que conseguimos unha forma de autenticar os usuarios no servidor e non "confiar" nos equipos cliente.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez