Deleghe di amministrazione in sistemi Linux/Unix
Introduzione

Nell'ambito dell'amministrazione di una rete locale di grandi dimensioni può essere utile avere la possibilità di delegare ad altri utenti non privilegiati alcuni compiti specifici dell'amministratore, riducendo così il carico di lavoro dell'amministratore stesso senza per questo far conoscere a troppe persone la *password* di superutente. Ad esempio, alcuni compiti tipici che potrebbero essere delegati ad altri utenti sono la gestione degli *account* di utente, delle stampanti, delle operazioni di *backup*, o di alcuni servizi di rete come il *server Web*.

Bit Set User ID

Tradizionalmente, nei sistemi *Linux/Unix* la modalità di delegare ad utenti non privilegiati l'utilizzo di alcuni comandi di amministrazione si è basata tipicamente sull'impiego del cosiddetto *bit Set User ID*. Si è già visto in **Gestione dei permessi** che ogni *file* o *directory* nel *file system* è caratterizzato da nove *bit* che determinano i permessi di lettura, scrittura ed esecuzione (r, w, x) per il proprietario, il gruppo del proprietario e per gli altri utenti del sistema (u, g, o). Oltre a questi nove *bit*, ad ogni *file* o *directory* sono associati tre *bit* ulteriori che fanno riferimento a speciali modalità di accesso:

1. SUID (*Set User ID*) - si accede al *file* utilizzando l'identificativo del proprietario (UID).
2. SGID (*Set Group ID*) - si accede al *file* utilizzando l'identificativo del gruppo a cui appartiene il proprietario (GID).
3. *Sticky* - se applicato ad una *directory*, i *file* contenuti in essa non possono essere cancellati o rinominati da un utente diverso dal proprietario, pur avendo il permesso di scrittura nella *directory*.

In particolare, se un *file* eseguibile di proprietà di *root* ha il *bit* SUID settato, chiunque lo esegua, lo farà assumendo l'identificativo di *root* (UID = 0) e, quindi, avrà tutti i privilegi del superutente, limitatamente al campo d'azione del comando in questione. Un esempio di eseguibile con il *bit* SUID attivo è il comando `passwd`, utilizzato per cambiare la *password*: poiché ogni utente deve essere in grado di cambiare la propria *password* e poiché solo *root* ha il diritto di scrivere sui *file* `/etc/passwd` e `/etc/shadow`, è necessario che tale comando sia eseguito con i privilegi dell'amministratore. Naturalmente, l'implementazione di `passwd` è tale da negare comunque ad un utente diverso da *root* la possibilità di cambiare la *password* di altri utenti o dello stesso *root*.

Per verificare se il *bit* SUID del comando `passwd` sia settato, si può procedere come nell'esempio che segue:

```
[root@host1 root]# ls -l /usr/bin/passwd
-r-s--x--x 1 root root 15368 mag 28 2002 /usr/bin/passwd
```

Il carattere s al posto della x nei permessi del proprietario denota l'attivazione di SUID.

Se si vuole delegare un utente diverso da *root* ad eseguire un particolare comando, si può settare il *bit* SUID dell'eseguibile tramite il comando `chmod`. Ad esempio, per delegare la creazione degli utenti è necessario che *root* attivi il *bit* SUID al comando `useradd`:

```
[root@host1 root]# chmod u+s /usr/sbin/useradd
```

A questo punto l'utente *user*1 è in grado di creare un altro utente chiamato *user*2:

```
[user1@host1 user1]$ /usr/sbin/useradd user2
```

cosa che può essere verificata controllando il contenuto del *file* `/etc/passwd`:

```
[user1@host1 user1]$ cat /etc/passwd |grep user2
user2:x:1002:1002::/home/user2:/bin/bash
```

Allo scopo di delegare l'esecuzione di un comando con i privilegi di *root*, l'utilizzo di SUID non consente tuttavia di ottenere un uso selettivo di questa funzionalità sulla base dell'utente che esegue il comando stesso. In altre parole, qualunque utente può utilizzare il comando in questione con i privilegi di *root*.

Comando sudo

Per una gestione più efficiente delle deleghe si può utilizzare il comando *sudo* (che sta per *superuser do*), disponibile nelle versioni più recenti dei sistemi operativi *Linux/Unix* o reperibile dal sito http://www.sudo.ws/. Questo comando svolge la funzione di permettere a determinati utenti (e solo a loro) di eseguire determinati comandi (e solo quelli) da determinati *host* (e solo da quelli) con i privilegi di amministratore. Inoltre, consente di monitorare l'attività dei delegati inserendo nel registro di sistema (*syslog*) tutte le chiamate a *sudo* con i relativi argomenti. L'impostazione delle deleghe viene realizzata tramite il *file* di configurazione `/etc/sudoers`, che tipicamente è accessibile solo a *root* e che deve essere modificato tramite l'editor `visudo` (una versione dell'editor vi dedicata a questo scopo).

Esempio

Come esempio, supponiamo di voler impostare le seguenti deleghe:

1. consentire all'utente *user*1 di aggiungere utenti tramite il comando `useradd` da qualunque *host*;
2. consentire all'utente *user*2 di cambiare la *password* di ogni utente, *root* escluso, operando solo dall'*host host*1.

Il *file* `/etc/sudoers` in questo caso dovrà contenere le seguenti righe:

```
...
user1 ALL=/usr/sbin/useradd
user2 host1=/usr/bin/passwd [A-z]*,!/usr/bin/passwd root
...
```

Nella prima riga dell'esempio sono indicati: l'utente delegato (*user*1), gli *host* da cui è permesso l'uso della delega (*ALL*, cioè tutti), il comando del quale si vuole consentire l'esecuzione a *user*1 indicandone il percorso completo (`/usr/sbin/useradd`).

La seconda riga, invece, mostra che l'utente *user*2 può eseguire solo dall'*host host*1 il comando `/usr/bin/passwd` con alcune restrizioni: innanzitutto è richiesto di specificare sempre un argomento che inizi con un carattere alfabetico e che contenga uno o più caratteri (che soddisfi, cioè, l'espressione regolare [A-z]*); poi, è negata (tramite il carattere di negazione !) l'esecuzione di `/usr/bin/passwd` con argomento *root*, che permetterebbe a *user*2 di modificare la *password* dell'amministratore.

Una volta stabilite queste regole, gli utenti possono eseguire i comandi suddetti con i diritti di *root* facendoli precedere dal comando *sudo* e rispettando le restrizioni specificate in `/etc/sudoers`. La prima volta che si invoca un comando tramite *sudo*, il programma chiede di inserire la *password* dell'utente delegato per effettuarne l'autenticazione, dopodiché controlla che la sintassi del comando da eseguire sia coerente con quanto specificato in `/etc/sudoers`. Da quel momento in poi, ogni

altra invocazione tramite *sudo* non richiede la *password*, a meno che non sia trascorso un certo intervallo di tempo (tipicamente 5 minuti) dall'ultima invocazione.

Quindi, per poter creare un *account* l'utente *user*1 dovrà procedere nel seguente modo:

```
[user1@host1 user1]$ sudo useradd user3
Password: *********
```

Per quanto riguarda *user*2, gli è consentito di cambiare la *password* all'utente appena creato:

```
[user2@host1 user2]$ sudo passwd user3
Password: **************
Changing password for user user3.
New password: ********
Retype new password: ********
passwd: all authentication tokens updated successfully.
```

mentre non può farlo per l'utente *root*:

```
[user2@host1 user2]$ sudo passwd root
Sorry, user user2 is not allowed to execute '/usr/bin/passwd root'
as root on host1.
```

Conclusioni

Le funzionalità messe a disposizione dal comando *sudo* sono molteplici e permettono un'efficiente automazione delle procedure di delega di amministrazione in reti locali di grandi dimensioni basate su sistemi *Linux/Unix*. L'applicazione ad un *case study* particolare è disponibile all'indirizzo:

http://www.komar.org/pres/sudo

Per maggiori informazioni, fare riferimento alle seguenti pagine del manuale in linea: *man sudo*, *man sudoers* e *man visudo*, disponibili anche agli indirizzi:

http://www.sudo.ws/sudo/man/sudo.html,

http://www.sudo.ws/sudo/man/sudoers.html,

http://www.sudo.ws/sudo/man/visudo.html.