Security & Firewalls: SSH-Authentifizierung per RSA

Wer häufig per SSH auf anderen Rechnern arbeitet, muss viele Kennwörter im Kopf haben und in die Tastatur tippen. Mit der Zeit wächst der Wunsch nach Erleichterung...

Abhilfe schafft die automatische Authentifizierung per SSH mittels öffentlichen Schlüsseln.

So wird's gemacht:

Zunächst wird ein SSH-Schlüsselpaar erzeugt:
`ssh-keygen -t rsa`
oder:
`ssh-keygen -t dsa`

Nach der Eingabe eines längeren Kennwortes oder eines Satzes (engl. Passphrase) werden in `~/.ssh/` die Dateien `id_rsa` und `id_rsa.pub` erzeugt.
Nun kopiert man die Datei `id_rsa.pub` mittels `scp` in das `~/.ssh/` des Rechners, auf den man sich automatisch einloggen lassen möchte, und nennt die Datei dort `authorized_keys2` bzw. erweitert eine vorhandene Datei entsprechend:
`cat id_rsa.pub ›› authorized_keys2`

Beim nächsten Login wird nicht mehr das bisherige Login-Passwort abgefragt, dafür allerdings das SSH-Kennwort.
Alternativ verzichtet man auf die Eingabe eines Passwortes und kann ganz ohne Interaktion eine SSH-Verbindung aufbauen.
Dies ist zwar deutlich unsicherer (sollte man auf keine Fall mit einem root-Account machen), aber sehr praktisch bei automatisierten Dingen, wie Mirrors, Backups, Replikationen, etc.

SSH-Agent

Ein anderer Ansatz, als auf das SSH-Passwort zu verzichten, ist ein sogenannter SSH-Agent..
Dieser wartet, nachdem das SSH-Kennwort beim Rechnerstart einmal abgefragt wurde, auf bevorstehende SSH-Logins und kümmert sich um die Authentifizierung, damit der Nutzer nichts mehr machen muss.

Windows:

Für Windows-SSH-Clients (z.B. Putty & WinSCP3) kann man den Putty-Keygen nutzen um die Schlüsselpaare zu erzeugen.
U.a. ist im Putty-Paket auch ein SSH-Agent.

Eindeutige ID: #1036
huschi
2005-12-11 20:44