SSH Authentifizierung über Public Key

Diese Dokumentation beschreibt die Vorgehensweise, wie man den Zugang zu einem SSH Server mit der Authentifizierung über öffentliche Schlüssel realisiert.

Wer einen Server im Internet betreibt und einen SSH Zugang vorhält, der sollte in jedem Fall die Authentifizierung über UserID und Kennwort deaktivieren. Verschiedene Hackertools ermöglichen großflächige und automatisierte Brute-Force-Angriffe gegen den SSH Server. Um vor solchen Attacken geschützt zu sein und trotzdem die Vorteile eines SSH Zugang zu seinem Server nutzen zu können, sollte die Authentifizierung gegen den SSH Server über öffentliche Schlüssel erfolgen.

Vorbereitung der SSH Server Konfigurationsdatei

Ist der SSH Server bereits aktiv, dann gibt es eine Konfigurationsdatei

/etc/ssh/sshd_config

Folgende Einträge sind dort entsprechend zu modifzieren:

PasswordAuthentication no

und

ChallengeResponseAuthentication no

Zusätzlich sollte man auch das Login mit dem Root User unterbinden. Diese Einstellung in der SSH Konfigurationsdatei lautet

PermitRootLogin no

Der Eintrag steht aber nicht in direktem Zusammenhang mit der SSH Authentifizierung via Public Key.

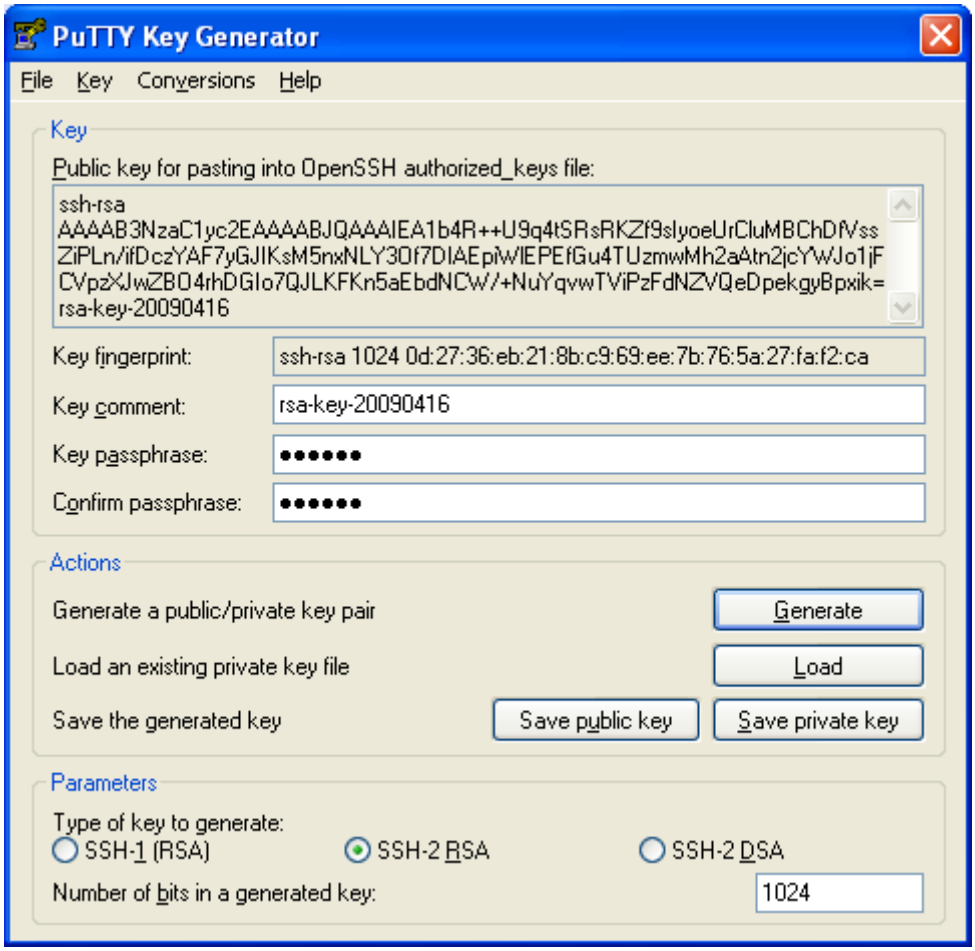
Nachdem die Änderungen durchgeführt worden sind muß der SSH Server mit

service sshd restart

neu gestartet werden (Befehl kann bei anderen Linux Distributionen anders lauten).

Schlüsselerstellung

Für die Erstellung des Schlüssels kann man die "puttygen.exe" verwenden. Nach dem Start des Programmes auf der Client Seite (Windows) den "Generate" Button anklicken und die Maus im leeren Feld bewegen. Der Schlüssel wird erstellt. Eine sogenannte Key Phrase für den Private Key (verbleibt beim Anwender) ist einzugeben. Danach sollte man den Public Key und den Private Key über das Programm abspeichern.



Für den Zugriff auf ein Linux System ist der im Fenster angezeigt Public Key für die OpenSSH authorized_keys Datei in die Zwischenablage zu kopieren.

Bereitstellung des Public Key

In dem Home Verzeichnis des Anwenders auf dem Server ist ein .ssh Verzeichnis zu erstellen, sofern es noch nicht vorhanden ist. Da hinein erstellt man die Datei

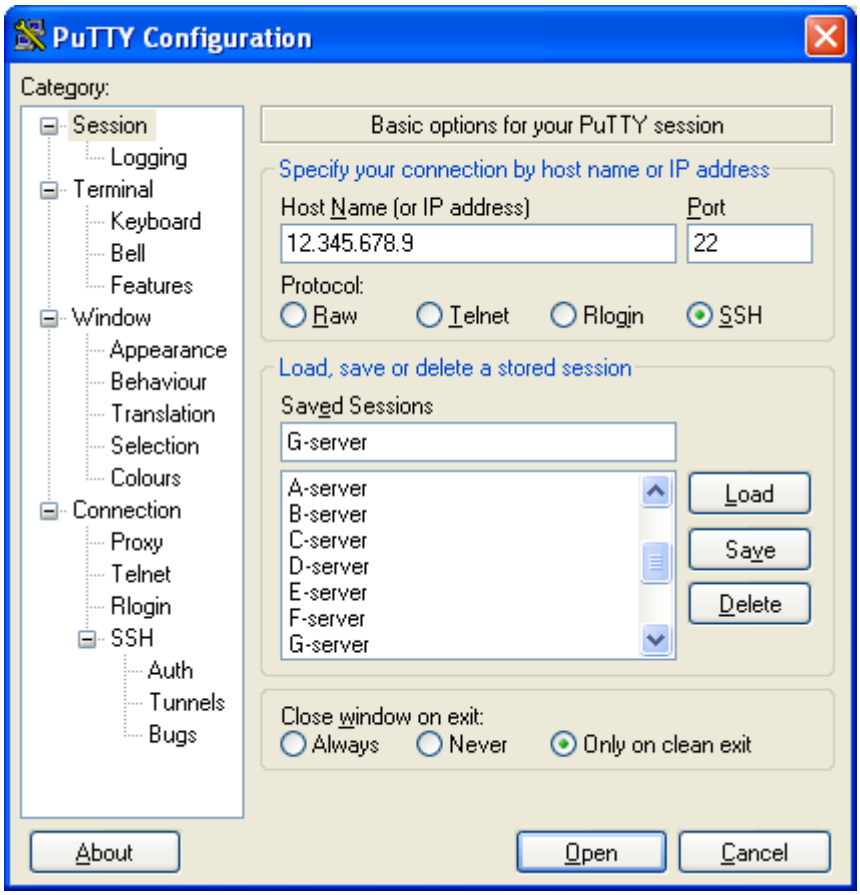
authorized_keys

In diese Datei hinein wird der in der Zwischenablage gespeicherte öffentliche Schlüssel kopiert und die Datei abgespeichert.

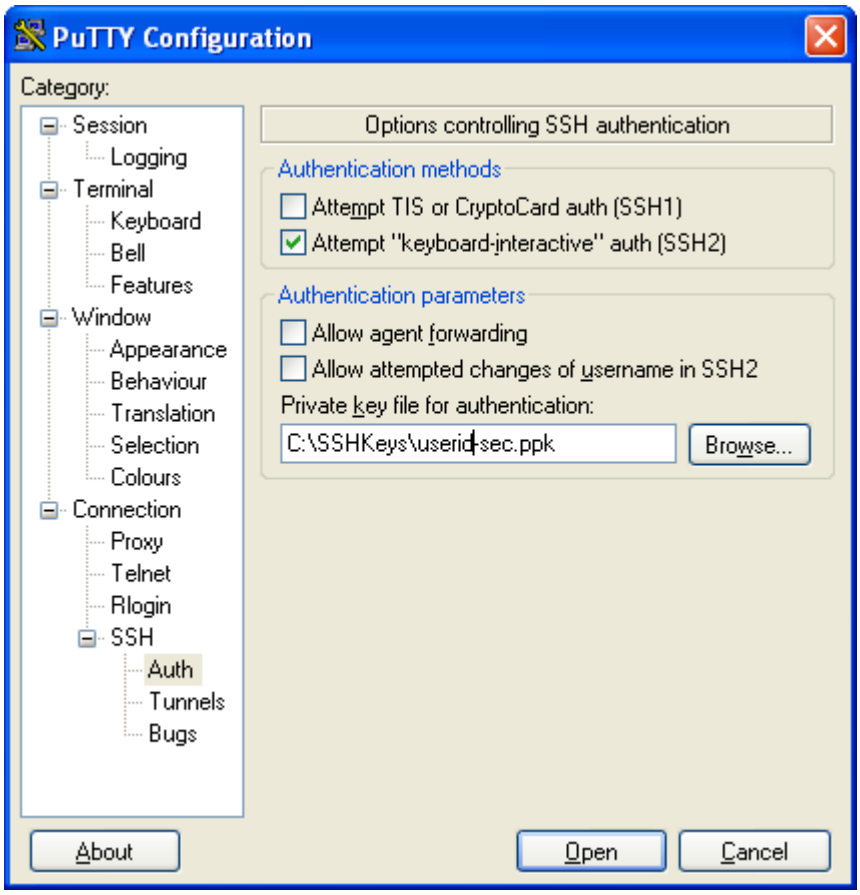
Zugriff mit Putty herstellen

Mit dem Programm Putty kann man nun eine SSH Verbindung über Public Key Authentifizierung herstellen. Dazu ist nach dem Aufruf des Programmes folgendes einzugeben:

- Hostname/IP Adresse
- Protokoll SSH auswählen



Danach unter SSH - Auth den "Private Key File" für die Authentifizierung auswählen:



Nun sind die Vorbereitungen getroffen und eine Verbindung über Putty zu dem SSH Server kann über "Open" hergestellt werden. In einem Terminalfenster erscheint die Abfrage

login as:

Hier ist nun die BenutzerID anzugeben. Danach erscheint folgende Anzeige im Fenster:

Authenticating with public key "rsa-key-nnnnnnnn"
Passphrase for key "rsa-key-nnnnnnnn":

Es ist nun die Key Phrase einzugeben, die man bei der Erstellung des Schlüssels eingegeben hat. Da die Key Phrase im privaten Schlüssel gespeichert ist, welcher sich beim Anwender befindet, wird die Key Phrase nicht übertragen. Sie dient lediglich dem Schutz des privaten Schlüssels. Erst danach erfolgt die Authentifizierung gegen den öffentlichen Schlüssel des Anwenders, welcher sich auf dem Server befindet.

Zusätzliche Hinweise

Versucht man eine normale SSH Verbindung (ohne Public Key) aufzubauen und verwendet einen vorhanden Benutzer (z. B. root) dann wird das Fenster nach Eingaben des "login as:" kurze Zeit später geschlossen. Das gleiche gilt bei der Verwendung eines ungültigen Benutzernamens.

Links

Aktuelle Putty und Puttygen Version
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Impressum

Diese Dokumentation wurde erstellt von

Peter Neugebauer
Kiebitzgrund 50

D-49477 Ibbenbüren

mailto: kontakt@neugebauer-ibb.de

Version: 1.0
Datum: 16.04.2009

Für Hinweise über eventuelle Fehler in dieser Dokumentation an die o. a. Mailadresse wäre ich sehr dankbar.