Linux SSH Server Zugriff nur per SSH Private Keys

Absicherung des Servers durch Private Keys

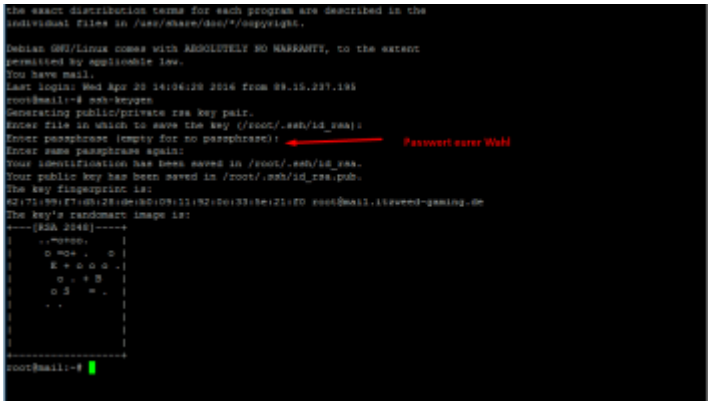
Hier zeige ich euch wie ihr euren Server durch Private Keys absichern könnt und somit fremden Personen die diesen Key nicht haben Zugriff verwehrt.

Das ganze wird hier auf einen Debian 8 Server durchgeführt und kann auf manchen Distributionen abweichen oder nicht funktionieren.

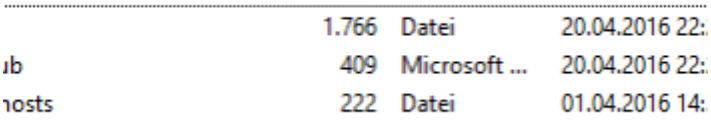
Dieses wurde mit einen extra Benutzer erstellt. Natürlich kann das ganze auch mit den Benutzer Root usw gemacht werden. Wichtige Information jeder User braucht einen SSH Key sonst bekommt dieser keinen Zugriff der Public Key abgelehnt wird.

Als erstes generiert ihr ein Schlüsselpaar falls noch eins vorhanden ist.
Hier geb ihr einfach "ssh-keygen" per SSH ein

Hier noch einmal dargestellt wie vorgegangen wird. Das Passwort ist nur da um den SSH Key ab zu sichern und so fremden Zugriff zu verhindern.



Nun wurden in dem User Ordner ein Verzeichnis erstellt mit den Namen .ssh und hat folgende 2 Dateien einmal die Datei "id_rsa" was der Private Key ist und einmal "id_rsa.pub" was der Public Key ist.



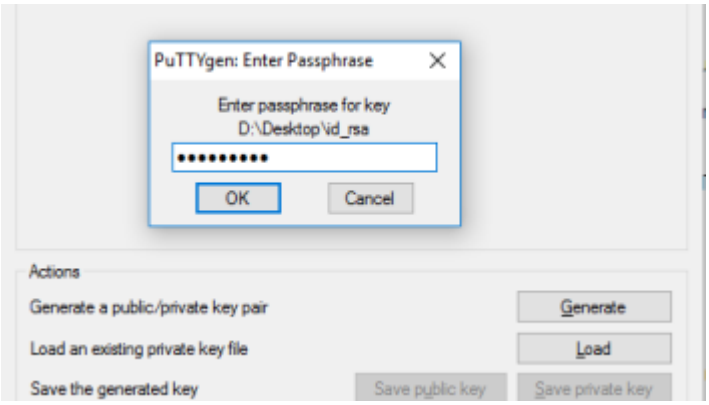
Um den Key auch zu den autorisierten Keys hinzugefügt werden. Dazu gehen wir in den .ssh Ordner vom User und geben folgenden Befehl ein "mv id_rsa.pub authorized_keys". Würde dieses durchgeführt ist die "id_rsa.pub" verschwunden und die Datei "authorized_keys" erstellt worden.

Als nächsten Schritt laden wir uns den dem Ordner die Datei "id_rsa" herunter und packen Sie uns auf den Computer in einen Ordner der am besten für diesen Key ist.

Nun benötigen wir das Programm PUTTYgen und öffnen dieses. PUTTYgen ist automatisch auf dem Computer wenn man Putty installiert hat. Hier zählt es nicht nur die Putty.exe zu nehmen sondern es muss vorher per Installer Putty installiert sein.

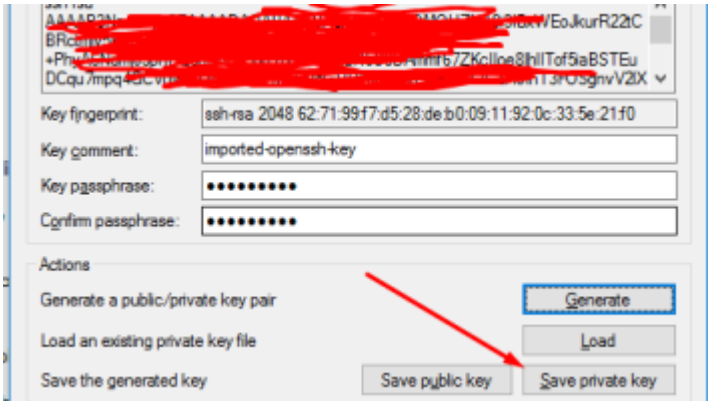
Nun gehen wir in PUTTYgen auf Conversions und klicken auf Import Key

Dort kommt nun ein Fenster wo ihr eure "id_rsa" suchen müsst. Hier wird nachdem Passwort gefragt was ihr dem Public Key zugewiesen habt.

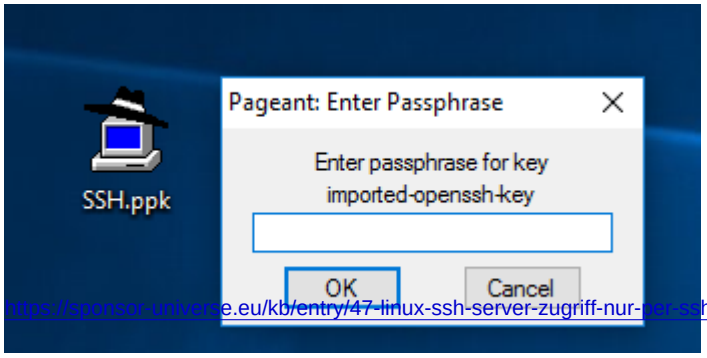


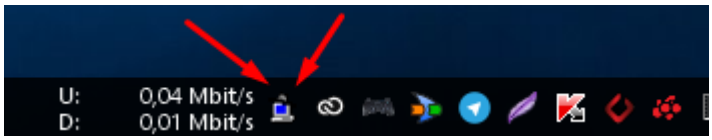
Nachdem ihr das Passwort eingegeben habt sieht ihr einige Daten eingetragen. Hier klick ihr in diesem Fenster auf Save Private Key. Dieser ist nur für euren oder eure Rechner gedacht mit den ihr Zugreifen wollt. Sprich per Putty oder Filezilla (bei Verwendung von SFTP)

Hier speichert ihr diese Datei einfach in dem Ordner wo auch die "id_rsa" ist. Wie in diesem Ordner habt ihr dann eine Datei mit ...name.ppk diese Datei ist jetzt euer Schlüssel um Zugriff auf diesen Server zu bekommen.



Wenn ihr diese Datei öffnet wird immer nach dem Passwort gefragt was zu dem Private Key gehört. Habt ihr euer Passwort richtig ein gegeben kommt unten in der Taskleiste ein Logo vom Pagent





Jetzt kommen wir aber zu den Schritt wo es **wichtig** ist Putty nicht zu beenden ohne genau vorher wissen das der Key akzeptiert wird.

Hier bei müssen wir als User Root angemeldet sein oder einem User der Rootrechte hat.

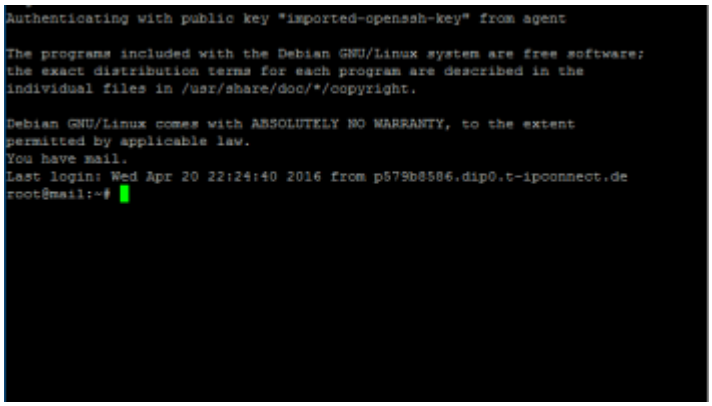
Mit den Befehlt "nano /etc/ssh/sshd_config" editieren wir die SSH config und suchen dort die Zeile mit "PasswordAuthentication yes"
Diese wird zu "PasswordAuthentication no" geändert. Nachdem dieses getan wurde speichern wir die Datei ab und starten mit "service ssh restart" den SSH Server neu.

Ab jetzt ist es nur noch möglich sich mit den Keys auf den Server anzumelden!

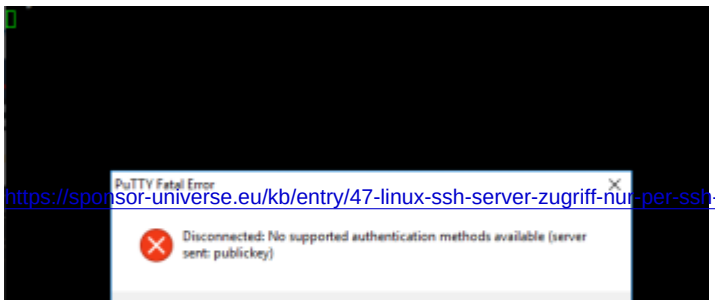
Wichtig das noch geöffnete Putty Fenster darf nicht geschlossen werden!!! Da sonst kein Zugriff per SSH möglich ist falls der Private Key nicht funktioniert. Der User Root sollte immer einen Private Key bekommen und vorher keinen anderen User!

Da der Private Key schon geöffnet ist auf dem Computer wie man unten an dem Symbol sehen kann siehe Screenshot vom Logo des Pagents kann man nun ein neues Putty Fenster zum Server öffnen und sich mit dem User einloggen für den der Private Key ist.

Bei einen erfolgreichen Login sieht das ganze so aus



Bei einen fehlgeschlagen Login wo der Key nicht funktioniert so oder der Key noch nicht im Pagent gestartet ist.



Bei einem Neustart des Computers oder beenden vom Pagent muss der Key wieder ausgeführt werden wenn man sich mit den Server verbinden möchte bzw sich anmelden.