SSH Setup & Security

SSH File Structure

File-/Folder Structure	Description	Security
~	User Home Directory (e.g. ~ can be /home/username)	
~/.ssh	SSH Ordner im Home Verzeichnis	`chmod 700 ~/.ssh`

~/.ssh/config	Erstelle einen neuen Host Eintrag in der ssh config, der Aufbau sollte wie folgt aussehen:
	`Host SomeHostAliasName`
	`  HostName domain.tld # or IP`
	`  User root # or another user`
	Eine Verbindung kann dann wie folgt durchgeführt werden:
	`ssh SomeHostAliasName`
		`chmod 600 ~/.ssh/config`

~/.ssh/id_rsa	Dein Private Key (niemals an andere übermitteln!!)	`chmod 600 ~/.ssh/id_rsa`
~/.ssh/id_rsa.pub	Dein Public Key (zum übermitteln an Dritte für Remote-Server Einrichtung)	`chmod 600 ~/.ssh/id_rsa.pub`
~/.ssh/authorized_keys	Public Keys die Zugriff auf den aktuellen Host haben	`chmod 600 ~/.ssh/authorized_keys`
~/.ssh/known_hosts	Einträge zu (trusted) Hosts (Einträge werden i.d.R. automatisch ermittelt und per User Prompt zur Bestätigung erfragt)	`chmod 600 ~/.ssh/known_hosts`

SSH Commands

Command	Description
ssh someHostAliasName	Connect to a host from your ~/.ssh/config
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"	Create a 4096Bit encrypted SSH Key
ssh-copy-id someHostAliasName	Copies your current ssh pub key to a remote host (Alternatively connect to the ssh host and add your public key content to the file ~/.ssh/authorized_keys)
ssh -Tv git@github.com	Analyze if a ssh connection is possible to a host (e.g. git@github.com)
ssh -o PubkeyAuthentication=no -o PreferredAuthentications=password someHostAliasName	Check if a host allows password authentication

SSH Hardening:

This hardens SSH + Disables Root Access (do this only if you know what you are doing!!)
Edit sshd_config (e.g. `vim /etc/ssh/sshd_config`) and change/add the following:

```
PermitRootLogin no           # or "prohibit-password"
PubkeyAuthentication yes
PasswordAuthentication no    # or use Match Blocks instead (see:
https://ostechnix.com/disable-ssh-password-authentication-for-specific-user-or-group/)
PermitEmptyPasswords no
ChallengeResponseAuthentication no
UsePAM no
X11Forwarding no

# Optional:
# Match User app-*
#         PasswordAuthentication yes
#
# Match User admin-*
#         PasswordAuthentication no
```

After changing the file restart the ssh service: `systemctl restart sshd` and verify if you are still able to connect (use a different user than root)!

Revision #37
Created 2023-07-31 18:36:32 UTC by Admin
Updated 2023-09-26 12:47:44 UTC by Christian Hackl