SSH

Aus ubuntuusers.de/ssh[1]

> Es gab einmal eine Zeit, als Computer im Netz über das Telnet-Protokoll zugänglich waren. Da dieses Protokoll keine Verschlüsselung bot, wurde das Mitschneiden von Passwörtern zur trivialen Angelegenheit.
>
> Um den Fernzugang zu sichern, schrieb Tatu Ylönen Mitte der 1990er eine Programmsuite – bestehend aus Server, Client und Hilfsprogrammen – die er ssh (secure shell) nannte.
>
> Später gründete er die Firma ssh.com {en} und bot die Version 2 der SSH-Suite nur noch kommerziell an. Daraufhin wurde von Entwicklern des Betriebssystems OpenBSD der öffentliche Quellcode der Version 1 geforkt. Sie entwickelten das Programm unter dem Namen "OpenSSH" weiter. Diese OpenSSH-Suite wurde fester Bestandteil quasi aller Linux-Distributionen.
>
> Drei wichtige Eigenschaften führten zum Erfolg von ssh:
>
> - Authentifizierung der Gegenstelle, kein Ansprechen falscher Ziele
> - Verschlüsselung der Datenübertragung, kein Mithören durch Unbefugte
> - Datenintegrität, keine Manipulation der übertragenen Daten

SSH-Client

Wichtiger Abschnitt aus dem Ubuntuusers-Artikel hierzu ist:

- https://wiki.ubuntuusers.de/SSH/#Der-SSH-Client

In unserem Beispiel wäre dies mit `ssh ubuntu@10.0.3.238` möglich.

Hier ein Beispiel:

```
vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh ubuntu@10.0.3.238
ubuntu@10.0.3.238's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Oct  2 12:28:18 2017 from 10.0.3.1
ubuntu@bsa-bashy:~$
```

[1] https://wiki.ubuntuusers.de/SSH/

Die kurz Variante wie `ssh 10.0.3.238` geht nicht, da der Benutzer `vagrant` des Hostsystems nicht gleich mit dem Benutzer `ubuntu` des Zielsystems ist.

Die Config

Zum Glück gibt es die ssh-config Datei unter `~/.ssh/config`.

Wichtiger Abschnitt hierzu:

https://wiki.ubuntuusers.de/SSH/#ssh-config

Wir können diese Datei etwas automatisiert erstellen.

BSA-BASHY IP-Adresse

Zunächst die IP des Containers ermitteln

```
sudo lxc-ls bsa-bashy --fancy
```

```
NAME      STATE   AUTOSTART GROUPS IPV4       IPV6
bsa-bashy RUNNING 0         -      10.0.3.167 -
```

Mit dem Programm awk können wir sehr einfach die Ausgaben der Spalten aufteilen.

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $1 }'
```

```
NAME
ais-bashy
```

Zu `awk` siehe auch

- https://wiki.ubuntuusers.de/awk/

Zu Pipe siehe auch

- https://wiki.ubuntuusers.de/Shell/Umleitungen/
- https://wiki.ubuntuusers.de/Shell/Umleitungen/#Der-Pipe-Operator

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $2 }'
```

```
STATE
RUNNING
```

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $3 }'
```

```
AUTOSTART
0
```

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $4 }'
```

```
GROUPS
-
```

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $5 }'
```

```
IPV4
10.0.3.15
```

Jetz nur noch die IP mit `grep` "regexen". Einfach nach einem Zeichen (regex: .) gefolgt von einem Punkt (regex: .).

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $5 }' | grep '.\.'
```

```
10.0.3.15
```

Zu `grep` siehe auch:

- https://wiki.ubuntuusers.de/grep/
- https://wiki.ubuntuusers.de/grep/#Besondere-Zeichen

Alternative Regex wären auch:

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $5 }' | grep -E '[0-9]+\.'
```

```
10.0.3.15
```

```
sudo lxc-ls ais-bashy --fancy | awk '{ print $5 }' | grep -E '[[:digit:]]+\.'
```

```
10.0.3.15
```

Umgebungsvariable erstellen

```
export BSA_IP=$(sudo lxc-ls ais-bashy --fancy | awk '{ print $5 }' | grep '.\.')
```

```
echo $BSA_IP
```

```
10.0.3.15
```

Mit dem Kommando `ssh ubuntu@${BSA_IP}` können wir uns mit dem Passwort `ubuntu` schon einloggen.

Im diesem Beispiel wird auch gezeigt, wie der Serverschlüssel ausgegeben werden kann.

```
vagrant@virtualbox-ubuntu1604:~/.ssh$ echo ${BSA_IP}
10.0.3.15
vagrant@virtualbox-ubuntu1604:~/.ssh$ ssh ubuntu@${BSA_IP}
The authenticity of host '10.0.3.15 (10.0.3.15)' can't be established.
ECDSA key fingerprint is SHA256:soF6eY4Ejqn2C5HP3SBAJM1GDiYW2ZrH73uidK5vzGo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.3.15' (ECDSA) to the list of known hosts.

ubuntu@10.0.3.15's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Oct  2 07:09:57 2017 from 10.0.3.1
```

```
ubuntu@ais-bashy:~$ ssh-keygen -f /etc/ssh/ssh_host_ecdsa_key.pub -l
256 SHA256:soF6eY4Ejqn2C5HP3SBAJM1GDiYW2ZrH73uidK5vzGo root@ais-bashy (ECDSA)
ubuntu@ais-bashy:~$ exit
Abgemeldet
Connection to 10.0.3.15 closed.

vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$
```

Erstellen der ssh-config

Diesmal mit Escape-Sequenzen:

```
echo -e "HOST BSA-BASHY\n\tHostName\t${BSA_IP}\n\tUser\tubuntu" > ~/.ssh/config
```

```
cat ~/.ssh/config
```

```
HOST BSA-BASHY
    HostName    10.0.3.15
    User    ubuntu
```

Einlogen via ssh-config Datei

```
vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh BSA-BASHY
ubuntu@10.0.3.15's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Wed Oct  4 12:07:52 2017 from 10.0.3.1

ubuntu@ais-bashy:~$ ls -lisa
insgesamt 32
3030309 4 drwxr-xr-x 4 ubuntu ubuntu 4096 Okt  3 07:49 .
3014694 4 drwxr-xr-x 3 root   root   4096 Okt  2 07:09 ..
3554207 4 drwx------ 3 ubuntu ubuntu 4096 Okt  2 07:09 .ansible
3037556 4 -rw------- 1 ubuntu ubuntu  115 Okt  4 12:09 .bash_history
3030310 4 -rw-r--r-- 1 ubuntu ubuntu  220 Aug 31  2015 .bash_logout
3030311 4 -rw-r--r-- 1 ubuntu ubuntu 3771 Aug 31  2015 .bashrc
3015450 4 drwx------ 2 ubuntu ubuntu 4096 Okt  2 07:09 .cache
3030312 4 -rw-r--r-- 1 ubuntu ubuntu  655 Mai 16 12:49 .profile
3030325 0 -rw-r--r-- 1 ubuntu ubuntu   0 Okt  2 07:09 .sudo_as_admin_successful
ubuntu@ais-bashy:~$ exit
Abgemeldet
Connection to 10.0.3.15 closed.
```

```
vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ exit
exit
```

Schlüssel erstellen und verteilen

Mit `ssh-keygen` erstellet man einen ssh-Schlüssel und mit `ssh-copy-id` kann dieser auf einen entfernten Rechner übertragen werden.

```
vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh-copy-id BSA-BASHY

/usr/bin/ssh-copy-id: ERROR: failed to open ID file '/home/vagrant/.pub': No such file
   (to install the contents of '/home/vagrant/.pub' anyway, look at the -f option)
vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vagrant/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/vagrant/.ssh/id_rsa.
Your public key has been saved in /home/vagrant/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:gXCelFlwnCQvOSbVy3YV0Wq3q6xVBT9Tm9a1bWOY6z0 vagrant@virtualbox-ubuntu1604
The key's randomart image is:
+---[RSA 2048]----+
|    . *O+.  o+. o|
|     *oB+   . +oO|
|    . O.o. . + X*|
|     o o+.. o =o+|
|       .S. . o.. |
|            ..o  |
|            .. E |
|           o  . .|
|          ..o.   |
+----[SHA256]-----+
vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh-copy-id BSA-BASHY
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/vagrant/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to i
ubuntu@10.0.3.15's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'BSA-BASHY'"
and check to make sure that only the key(s) you wanted were added.

vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh BSA-BASHY
```

```
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Wed Oct  4 12:25:20 2017 from 10.0.3.1

ubuntu@ais-bashy:~$ exit
Abgemeldet
Connection to 10.0.3.15 closed.

vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$
```

Entfernte Ausführen

Das entfernte Ausführen von Kommandos wäre jetzt auch via ssh möglich.

```
ssh BSA-BASHY pwd
```

```
/home/ubuntu
```

Kopieren von Dateien

Kopieren via ssh ist mit `scp` möglich.

```
scp ~/.ssh/id_rsa.pub BSA-BASHY:/tmp/
```

```
id_rsa.pub                                    100%  411     0.4KB/s   00:00
```

root ssh-Login

Ein SSH-Login für `root` mit **Passwort** sollte nicht erlaubt sein. Dagegen kann der Root-Login über eine **Passphrase** sprich mit Schlüssel erfolgen. Ein direktes verteilen des Schlüssels via `ssh-copy-id` ist für root nicht möglich. Daher geht hier der Umweg über `ubuntu`. Deiser wird zu root und kann dann den Schlüssel händisch importieren.

```
vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh BSA-BASHY
ubuntu@ais-bashy:~$ ls /tmp/id*
/tmp/id_rsa.pub
ubuntu@ais-bashy:~$ sudo su -
[sudo] Passwort für ubuntu:

root@ais-bashy:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
```

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:Dx/ekPlmOqE36BfAQisG65U7fja1BWImNPbiHjfynMw root@ais-bashy
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|  . + .          |
|   = = o         |
|  . B B +  o     |
| . + B oSo=      |
|  . * o .=+=     |
|   o X + =+o=    |
|    o E + =+     |
|     o o.o.o     |
+----[SHA256]-----+
root@ais-bashy:~# cat /tmp/id_rsa.pub >> .ssh/authorized_keys
root@ais-bashy:~# exit
Abgemeldet
ubuntu@ais-bashy:~$ exit
Abgemeldet
Connection to 10.0.3.15 closed.

vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ ssh root@${BSA_IP}
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Oct  2 07:14:07 2017 from 10.0.3.1

root@ais-bashy:~# exit
Abgemeldet
Connection to 10.0.3.15 closed.

vagrant@virtualbox-ubuntu1604:~/bsa/hands-on-bsa/00-Start$ exit
exit
```

Appendix ssh

https://superuser.com/questions/247564/is-there-a-way-for-one-ssh-config-file-to-include-another-one

```
ssh -V
OpenSSH_7.2p2 Ubuntu-4ubuntu2.2, OpenSSL 1.0.2g  1 Mar 2016
ls ~/.ssh
authorized_keys  config  id_rsa  id_rsa.pub  known_hosts
cat ~/.ssh/known_hosts
|1|DXlztx9meRadHdtQeA+VH/94j2I=|a2PVd2zcwW4eVJq7zNu89rYrSaY= ecdsa-sha2-nistp256 AAAAE2VjZHN
```