

Assignment 0x01

Frank Kaiser – 1742945, Jan Martin – 1796943

November 17, 2017

1 Task 1

Snow is white.

```

[aro@arch-aro ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/aro/.ssh/id_rsa): /home/aro/.ssh/id_rsa_psi
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/aro/.ssh/id_rsa_psi.
Your public key has been saved in /home/aro/.ssh/id_rsa_psi.pub.
The key fingerprint is:
SHA256:E/pB4YMB3Mhgfoa0LrcTl1MzLw23/T/LMFPctS9sgDo aro@arch-aro
The key's randomart image is:
+---[RSA 2048]---+
|.O+..+|.
|..B..+|.
|..=..+0..|
|..O..O..+O..|
|..S..+..|
|..*O..E..+..|
|..%*..+..|
|..*..+..|
|..+..+..|
|..+..+..|
+---[SHA256]---+

```

Figure 1: ssh-keygen

```

[aro@arch-aro ~]$ ssh-copy-id kaiser@88.99.184.129
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 2 key(s) remain to be installed -- if you are prompted now it is to install the new keys
kaiser@88.99.184.129's password:

Number of key(s) added: 2

Now try logging into the machine, with: "ssh 'kaiser@88.99.184.129'"
and check to make sure that only the key(s) you wanted were added.

```

Figure 2: save public key on server

2 Task 2 - Public-Key Authentication in SSH

2.1 GNU/Linux

To generate the ssh-key pair I used the command `ssh-keygen` which generates by default a 2048 bit long rsa key.

To copy the key on the server `ssh-copy-id user@88.99.184.129` was used. Since I already had a public key for another server and the exercise was to create one, both keys got uploaded to the server as seen in the picture 2.

The following log-in worked without the user password for the server. Only the optional password for the private ssh key was required. The keys on the server are stored in `~/.ssh/authorized_keys`. See figure 3

```

[aro@arch-aro ~]$ ssh kaiser@88.99.184.129
Linux psi-introsp 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) x86_64

Last login: Fri Nov 17 20:32:43 2017 from 188.194.245.11
kaiser@psi-introsp:~$ cd .ssh/
kaiser@psi-introsp:~/.ssh$ ls
authorized_keys  known_hosts
kaiser@psi-introsp:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCOuXvB7Y614gRvtXefF15YnBgILx2XYV5BR346fvmPGrKsrla0Z5MAK5VQJUsmAXTe0IIImyBy01VOT
0IMKrsPervscl+HKKURMEfAlG6q1d8f6CwLW4s9y5G0DX/DE6d2Z/TBtD4LopTmL3BT+00veLw6fKufqmwKv5GnlZV/Lhr2UPJhD-clutq8InWNTp
E+770oFhmCSaye4+BCGWTf99waFqB51806wsgRe51kMor05lmsGusfZ4W1f6EaSoz/N756F2rtkDh70JY1lyh0b+aduN/rtoDhexDqtPvIEDTpkAa
+B05TECHKvbuUnZeQsGLxLHN+3LTmVvgmQ8Pask5RVze9HJMVf3eVyp8V2LYnQD/Tv73KUSZVZc327TFN56LKc693svHFYkTctZmc9L+5LN/9uaw
UDFNSxLwTata29G0vKkAZdX0wmkUBSQM/LH8NorWYw7u3L4XCNzU57Fhcwktf3lctL14mCwmN+Xr/BDPfDyZypn/wnu0XdrRrogU5og6y1f337bxxNB
86J4ZUUDIP25HdEly8pppCuf7c500dCgWfXwVKW6w46eDeu64dtXoazpc9WwIa/s1Na6Bw9MHj0dPJ7b9s45VEGH185Ee+W09MMFKA1Eb661aOMT
30vJ0zYv0pQe= frank-phillip.kessler@stud.uni-bamberg.de
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBA092znTHVnQdJK0f4Ech3Croox1Gha20vdJ3SpFZPMBZuJz7ae7mKeGmTzGyae0L5lyh99ka03t1rIP2
Niw3PILVKKX09Bd+K+G4H2pXuy8Zgdqfgk1dM1K9WLB4t1PZu501MWTJhgmWBY19XqbHzkcmzXzMY052IDBD/+ELCKHL4tyZy58sA3icSq3X0rMHL
93N4TFx8757tq/9H/kHo7yqBL7699R231CqJ21LzCuOfs0J5pyIozTtV+ukzTHUWIZ/gT0PB/entk1ZDXUxCKbhcDpd9/IWSUpmw4+T0BJgsLbnk3420
r/mnC3CKKcD70G0K2+uXyB09 aro@arch-aro
kaiser@psi-introsp:~/.ssh$

```

Figure 3: location of keys on server

```

[aro@arch-aro ~]$ cd .ssh/
[aro@arch-aro .ssh]$ ls
id_rsa  id_rsa.pub  id_rsa.psi  id_rsa.psi.pub  id_rsa.pub  known_hosts
[aro@arch-aro .ssh]$ cat id_rsa.psi.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQ9znThVngbJK0f4EchJcRooxIghaZDvdJjSpFZPwB2uJNz7ae7mkeGmIzGyae0l5jlynp9ka03tjrIP2
Nne3PILVAXO29BdK+G4R2pXuy8epqTqk1ldHlKwQL84tIPZuS01HMTJHgmMBV19XzqbMakentZxZAY02z1BBD/+ELCKHLtyZy5b5A3lcsq3X8fPwE
93N4tF877td/9H/KHo7yqBL7099R23lqZl1Cu0Fs0J5pyIo2TtV+Iuk2ThuWIZ/gT0PB/entk1ZDXUjxCkhhQcpnd9/IW5uPmw4+TQbJgsIDmk3429
sRYmC3CMKcJ070GOKZ+tuYB89 aro@arch-aro
[aro@arch-aro .ssh]$ pwd
/home/aro/.ssh

```

Figure 4: location of keys on local machine

```

martin@psi-introsp:~/.ssh$ ls
authorized_keys  known_hosts
martin@psi-introsp:~/.ssh$ ls -l
total 8
-rw-r--r-- 1 martin martin 398 Nov 17 21:22 authorized_keys
-rw-r--r-- 1 martin martin 215 Nov  6 18:00 known_hosts
martin@psi-introsp:~/.ssh$

```

Figure 5: permission check

The ssh-keys on your local machine are by default stored in `~/.ssh/id_rsa.pub` for the public part and the private one in `~/.ssh/id_rsa`. (Provided you did create a rsa key) See figure 4.

2.2 Windows

On a windows machine the same tools from openSSH were not available. That's why the procedure was a little bit different. Here PuTTY was used.

To generate the key the tool `putty-gen` was used. Then we logged into the server via ssh and created the file `authorized_keys` in `~/.ssh/` and pasted the key into it using nano. Lastly, we checked that only we have write access to the file by `ls -l`

In figure 6 you can see the successful login by using the ssh-key pair.

```

login as: martin
Authenticating with public key "rsa-key-20171117"
Passphrase for key "rsa-key-20171117":
Linux psi-introsp 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) x86_64

Last login: Fri Nov 17 20:55:56 2017 from 185.53.42.56
martin@psi-introsp:~$

```

Figure 6: windows ssh-key login

3 Task 3

Snow is white.

4 Task 4

Snow is white.