

LAB 6: sftp/ssh Setup for comp232.com

John Dempsey

COMP-232 Programming Languages
California State University, Channel Islands

September 27, 2023

The following steps allow you to use ssh (Secure Shell) and sftp (Secure FTP) from your laptop to comp232.com (143.198.238.179) without requiring a password using private and public keys. Both ssh and sftp encrypt the data sent and received from your laptop to the comp232.com site.

Open an Ubuntu terminal window and type:

% uname -a

```
Linux oho 4.4.0-19041-Microsoft #1237-Microsoft Sat Sep 11 14:32:00 PST 2021 x86_64 x86_64 x86_64  
GNU/Linux
```

% id

```
uid=1000(john) gid=1000(john)  
groups=1000(john),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(pl  
ugdev),117(netdev)
```

% pwd

```
/home/john
```

% ls -l .ssh

```
.ssh: No such file or directory
```

%mkdir .ssh

% ls -ld .ssh

```
drwxr-xr-x 1 john john 4096 Sep 22 09:50 .ssh
```

% chmod 700 .ssh

% ls -ld .ssh

```
drwx----- 1 john john 4096 Sep 22 09:50 .ssh
```

← **Must be rwx for john user only.**

% cd .ssh

Note: <CR> represents the ENTER key, or Carriage Return, on your keyboard.

% ssh-keygen -t rsa

Generating public/private rsa key pair.

Enter file in which to save the key (/home/john/.ssh/id_rsa): <CR>

Enter passphrase (empty for no passphrase): <CR>

Enter same passphrase again: <CR>

Your identification has been saved in /home/john/.ssh/id_rsa

Your public key has been saved in /home/john/.ssh/id_rsa.pub

The key fingerprint is:

SHA256:tDDuHhB/dQxPGLTZz5/rzdkHeeAwX7UnDSu5MMWIDGs john@oho

The key's randomart image is:

```
+---- [RSA 3072] ----+
|           .+=... |
|           .%o... |
|   . o . E.B. +o |
|   + + +o.=o+.+ |
|   . o S o Bo=. |
|   o . . =.o |
|   o           +. |
|   . .           .* |
|   .           .+= |
+----- [SHA256] -----+
```

% ls -l

total 4

-rw----- 1 john john 2590 Sep 22 09:52 id_rsa

-rw-r--r-- 1 john john 562 Sep 22 09:52 id_rsa.pub

On comp232.com as user john, run:

% uname -a

Linux comp232 5.4.0-73-generic #82-Ubuntu SMP Wed Apr 14 17:39:42 UTC 2021 x86_64 x86_64
x86_64 GNU/Linux

% id

uid=1012(john) gid=1012(john) groups=1012(john)

% pwd

/home/john

% ls -l .ssh

.ssh: No such file or directory

% mkdir .ssh

← If .ssh doesn't exist already.

% ls -ld .ssh

drwxrwxr-x 2 john john 2 Sep 22 16:59 .ssh

% chmod 700 .ssh

← If .ssh isn't 700 already.

% ls -ld .ssh

drwx----- 2 john john 4096 Sep 22 16:59 .ssh

% cd .ssh

% vi authorized_keys

Copy/Paste the public key id_rsa.pub on your laptop for user john into authorized_keys. Make sure the key is one single line without any spaces in key. In vi, you can type "1G" to go to line 1 and then type "\$" to see if the cursor goes to the last character in the authorized_keys file.

```
% ls -l
total 8
-rw-rw-r-- 1 john john 562 Sep 22 16:59 authorized_keys
-rw-r--r-- 1 john john 444 Sep 22 16:49 known_hosts
```

```
% chmod 400 authorized_keys
```

```
% ls -l
total 2
-r----- 1 john john 562 Sep 22 16:59 authorized_keys ← Must be r only for john.
```

On your laptop as user john, lets test things out. Run:

```
% sftp john@comp232.com ← sftp stands for Secure File Transfer Protocol (SFTP).
← First time you'll need to confirm connecting to comp232.com
```

```
The authenticity of host 'comp232.com (143.198.238.179)' can't be established.
ECDSA key fingerprint is SHA256:Nlt2g1v4/qqh5f13d7Gpj3Xelb8RgzbzIN6tML0YVJnA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'comp232.com,143.198.238.179' (ECDSA) to the list of known hosts.
Connected to comp232.com.
sftp> quit
```

```
% ls -l
total 4
-rw----- 1 john john 2590 Sep 22 09:52 id_rsa
-rw-r--r-- 1 john john 562 Sep 22 09:52 id_rsa.pub
-rw-r--r-- 1 john john 444 Sep 22 10:01 known_hosts
```

On comp232.com, we see only one file in .ssh:

```
% pwd
/export/home/john/.ssh
```

```
john@comp232:~/ssh$ ls -l
total 8
-r----- 1 john john 562 Sep 22 16:59 authorized_keys
-rw-r--r-- 1 john john 444 Sep 22 16:49 known_hosts
```

On Your laptop as user john, we can manually run sftp without a password:

```
% sftp john@comp232.com
```

Connecting to comp232.com ...

```
sftp> ll -l test.txt
```

```
-rw-rw-r-- 1 john john      12 May 17 23:49 test.txt
```

```
sftp> put test.txt
```

```
Uploading test.txt to /export/home/john/test.txt
```

```
test.txt          100% 12  0.0KB/s  00:00
```

```
sftp> ls -l test.txt
```

```
-rw-r--r--  0 110  103      12 May 18 00:00 test.txt
```

```
sftp> quit
```

On your laptop as user john, we can connect to comp232.com using ssh:

```
john@oho:~/ssh$ ssh john@comp232.com
```

```
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com
```

```
* Management:   https://landscape.canonical.com
```

```
* Support:      https://ubuntu.com/advantage
```

```
System information as of Wed Sep 22 17:21:43 UTC 2021
```

```
System load: 0.0          Users logged in: 2
```

```
Usage of /: 7.7% of 48.29GB IPv4 address for eth0: 143.198.238.179
```

```
Memory usage: 18%        IPv4 address for eth0: 10.48.0.5
```

```
Swap usage: 0%           IPv4 address for eth1: 10.124.0.2
```

```
Processes: 130
```

```
68 updates can be applied immediately.
```

```
1 of these updates is a standard security update.
```

```
To see these additional updates run: apt list --upgradable
```

```
*** System restart required ***
```

```
Last login: Wed Sep 15 02:04:46 2021 from 23.241.58.212
```

```
john@comp232:~$ uname -a
```

```
Linux comp232 5.4.0-73-generic #82-Ubuntu SMP Wed Apr 14 17:39:42 UTC 2021 x86_64 x86_64 x86_64  
GNU/Linux
```

```
john@comp232:~$
```

To transfer multiple files to comp232.com, you could create a shell script like:

```
% cat test_sftp.sh
#!/bin/sh
sftp john@comp232.com > sftptemp.txt <<EOF
lcd LAB3
cd /home/john/LAB3
mput *.c
bye
EOF
```

```
% test_sftp.sh
Connecting to comp232.com ...
%
```

```
% cat /tmp/sftptemp
sftp> lcd /var/log
sftp> cd /home/john/LAB4
sftp> mput c.*
Uploading /home/john/LAB4/*.c
sftp> bye
```

On Your laptop as user john, we can run scp (secure copy) command to perform the same secure transfer:

```
% scp -qr *.c john@comp232.com:/home/john/LAB4
%
```

Or on Your laptop as user john, run scp in a script:

```
% cat test_scp.sh
#!/bin/sh
run_date=""date '+%m/%d/%Y'""
start_time=""date '+%H:%M:%S'""
echo "$run_date^$start_time^$USER^scp -qr /var/log/syslog*
john@COMP232.COM:/export/home/john/sftp_test.dir \c"

scp -qr /var/log/syslog* john@COMP232.COM:/export/home/john/sftp_test.dir

end_time=""^date '+%H:%M:%S'""
echo "$end_time"

% test_scp.sh >> scp_audit_log.txt

% test_scp.sh >> scp_audit_log.txt
```

```
% test_scp.sh >> scp_audit_log.txt
```

```
% cat scp_audit_log.txt
```

```
05/18/2021^00:56:39^john^scp -qr /var/log/syslog* john@COMP232.COM:/home/john/sftp_test.dir ^00:56:39
05/18/2021^00:56:44^john^scp -qr /var/log/syslog* john@COMP232.COM:/home/john/sftp_test.dir ^00:56:44
05/18/2021^00:56:49^john^scp -qr /var/log/syslog* john@COMP232.COM:/home/john/sftp_test.dir ^00:56:50
```

The scp_audit_log.txt file can now be loaded into an Excel spreadsheet for further analysis if needed.

To generate the public key from the private key, you can run:

```
john@oho:~/ssh$ ssh-keygen -y -f id_rsa > id_rsa.public_key.txt
```

```
john@oho:~/ssh$ more id_rsa.public_key.txt
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQGBgQDExpF6lIdPs4LiLer4T/yNEbl8MXLFFES2gU9eGAVj/bpW5Ou97n
3skfV6GXy8eSJMUEdXdlInzleBQIG
prl02/XdWTH6/HGzmTANcj3nIAZ2J0eu4vAKhSTS5PhuJV11qgRZtdAv0l+SE8Cpcx3FtKHSYrwmF2+QryOOg
JHHmHB/1f15UPXp/woqD5hzEWADbynBostn
KHKXk8PQSmHWM4/sq/LOWl3uFsExVkfLxCNd4h5iP9N1+ozYXEWI9CUJCZwA6nA7XKJyxKAT5RDEbelJogF
56aLx2FEvM0Da4J61HEQmIkZKt5oaGW3v1RZP
TBVPjDN6l5lIdekjhNiFnWiUbZhQ4JpmN/3ZCef6k5W2nYgHEbQ59vT51Ak1TgN5Co5EOvUqCEO7My4c6+l
e2wuBd5TnZoEnl3842snjbFwXth++pZl3bcVh
GktE4B7wwzV6QpbNhJe5PYNGCg4Dv8ykuJiAJnP+CEViHS8wZ6FGWuuYnS7lSdQRWDvPEAc=
```

```
john@oho:~/ssh$ cat id_rsa.pub
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQGBgQDExpF6lIdPs4LiLer4T/yNEbl8MXLFFES2gU9eGAVj/bpW5Ou97n
3skfV6GXy8eSJMUEdXdlInzleBQIGprl02/XdWTH6/HGzmTANcj3nIAZ2J0eu4vAKhSTS5PhuJV11qgRZtdAv0l
+SE8Cpcx3FtKHSYrwmF2+QryOOgJHHmHB/1f15UPXp/woqD5hzEWADbynBostnKHKXk8PQSmHWM4/sq
/LOWl3uFsExVkfLxCNd4h5iP9N1+ozYXEWI9CUJCZwA6nA7XKJyxKAT5RDEbelJogF56aLx2FEvM0Da4J61HE
QmIkZKt5oaGW3v1RZPTBVPjDN6l5lIdekjhNiFnWiUbZhQ4JpmN/3ZCef6k5W2nYgHEbQ59vT51Ak1TgN5C
o5EOvUqCEO7My4c6+lE2wuBd5TnZoEnl3842snjbFwXth++pZl3bcVhGktE4B7wwzV6QpbNhJe5PYNGCg4
Dv8ykuJiAJnP+CEViHS8wZ6FGWuuYnS7lSdQRWDvPEAc= john@ohojohn@oho
```

```
john@oho:~/ssh$ diff id_rsa.pub id_rsa.public_key.txt
```

```
% ssh-keygen -y -f id_rsa > id_rsa.public_key
```

```
% ls -l
```

```
total 8
```

```
-rw----- 1 john john 883 May 17 23:37 id_rsa
-rw-r--r-- 1 john john 226 May 17 23:37 id_rsa.pub
-rw-rw-r-- 1 john john 209 May 18 10:30 id_rsa.public_key
-rw-r--r-- 1 john john 409 May 17 23:48 known_hosts
```

% more id_rsa.pub

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxYH8LMFZB5XM4FHv+HmLDuJW87fneROuQszTFwrOS/w9
+yXqH8aL+IVDxXzUw3In9UPD5tYGuuBJ/tVqDo24rGSsZXRmqyyMtMffRKYSOn1Ks2Dkgig9uqek7N23
6DiT45yo2WHusMp8DmHDuKHdbyX1zknPkBwohgxFLe+aUk= john@your laptop2-z1
```

% more id_rsa.public_key

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxYH8LMFZB5XM4FHv+HmLDuJW87fneROuQszTFwrOS/w9
+yXqH8aL+IVDxXzUw3In9UPD5tYGuuBJ/tVqDo24rGSsZXRmqyyMtMffRKYSOn1Ks2Dkgig9uqek7N23
6DiT45yo2WHusMp8DmHDuKHdbyX1zknPkBwohgxFLe+aUk=
```

Don't share your private key with anyone!!! Doing so will allow access to your account! That said, here's what the id_rsa file looks like:

```
john@oho:~/ssh$ cat id_rsa
```

← Don't share your private key to anyone!!!

```
-----BEGIN OPENSSH PRIVATE KEY-----
```

```
b3BlbnNzaC1rZXktbjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAxMSKRepSHT7OC4i3q+E/8jRG5fDFyxXxETofPXhgFY/26VuTrve5
97JH1ehl8vHkiUDLhMXZZ85XgUCBqa5dNv13Vlx+vx55kwDXI955QGdidHruLwCoUk0u
T4biVddaoEWbXQL9CPkhPAqXMdxSh0mK8Jhdvkk8jjoCRx5hwhf9X9eVD16f8KKg+YcxFg
A28pwaLLZyhyI5PD0Eph1jOP7KvyzsJd7hbBMVZHy8QjXeIeYj/TdfqM2FxFiPQICQmcAO
pwO1yicsSgE+UQxG3i4zoBeemi8dhRLzNA2uCetRxEJiJGSreaGhlt79UWT0wVT4wzpeZ
ZXXpi4TYhZ1oIG2YUOCaZjf92Qnn+pOVtp2IBxG0Ofb0+dQJNU4DeQqORDr1KghDuzMuHO
viHtsLgXeU52aBJ5d/ONrJ42xcF7YfvqWZd23FYRpLROAe8MM1ekKWzYSXuT2DRgoOA7/M
pLiYgCZz/ghFYh0vMGehRlrmJ0u5bHUEVg7zxAAAAFgHYGZbl2BmW5AAAAB3NzaC1yc2
EAAAGBAMTEikXqUh0+zgult6vhP/IORuXwxcv8RLaBT14YBWP9ulbk673ufeyR9XozfLx
5IIAy4TF2WWfOV4FAGamuXTb9d1ZMfr8cbOZMA1yPeeUBnYnR67i8AqFJNLk+G4IXXWqBF
m10C/Qj5ITwKlZhcW0odJivCYxb5CvI46AkceYch/V/XIQ9en/CioPmHMRYANvKcGiy2co
cpeTw9BKYdYzj+yr8s7CXe4WwTFWR8vEI13iHml/03X6jNhCRyJ0JQkInADqcDtconLEoB
PIEMRt4uM6AXnpovHYUS8zQNrgrnUcRCYiRkq3mhoZbe/VFk9MFU+MM3qXmWV16SOE2IWD
aJRtmFDgmmY3/dkI5/qTlbadiAcRtDn29PnUCTVOA3kKjkQ69SoIQ7szLhzr4h7bC4F3IO
dmgSeXfzjayeNsXBe2H76lmXdtWEaS0TgHvDDNXpClS2EI7k9g0YKDgO/zKS4mlAmc/4I
RWldLzBnoUZa65idLuWx1BFYO88QBwAAAAMBAAEAAAGAMPjVjTcXfs3dzEMXq4ChQK/AIY
R+ReBNlqr+eOEX0OYGxueS5w4iy8IkXNm9XezUO1DUFISDmeY6CetnKK6g7SHCbMkXFou
Fkv/CKmxPly72vZfwglbShL/KjnwlsFX9Gv/LzCwAuZ+hRXDcqkC9OzTBaCrQTO+AZ2FVP
cs0SdggICK2IHM4pMmPXeqMqFVayVkmBvjUeZgNteA+bs5hG1K2dWl1c3MQPCK3rOhpNZJ
ExmvBDbsc0WLfmHgsIhKq2BdrZAnolrfu+kulGEfBbwdM5gJRUBtfm6+S1TgzG3uLhXTus
E4CrGEkkGxTxr1DysbAXTwoPsaD9dYVvbUEAhX7/f966+c43w45UMjdMF/MqnNk9BMfU+j
ezd2HxmHJVAvothQF8Tbim7kFuWakCQL5hBqYzw6Yk4gVRrORIFH+t4DyHerLZEtzw3eWm
2rIU9ReKPyavxuTPxzD9xvJIFMDRvwmqHr7nvtSz+pRZ5Qat1t/DVb9y2H7uAYTFGxAAAA
wQDiMI2DOBe+S+O2DfkQPBRpFs8hmHET+IhWHLceeqiMzi96kav6nCwGpTWihxeUEXLz+P
O6km1umw8cUfP8+5Du6Ci0LbutaMHmg8GvsST5U40nwwwHG0F63tL9idpUktRoz4/YMITm
Swv0dJbx7KAZH52BKdMug4w0HNPKCop1cJdEzLhMvmOMR2IJK4cbAI+BfG2WWfdJBnslym
kW6IuuLseymQiuRKLn/kdaQtWqPut1NIOIK9XDY951ZCUB7tUAAADBAPHUbZfvrBailRdR
wU8bIT6oOfar0oyR6FqmyWrxly5yk/aMaVowBr15BKF5sMimsbT2VK/pwBT7PjuAzOoAl
O3E0Zqu/fPPozD92e0gYs1U8xZMmvRqoRm/ynHeUCLi6vtNCWOzIfVRyzON2puHm7I24w8
eOLXaOrFkSq5w1jpa+SHYV83t9fI0/HaQEVwYkbH6I+PtVxrwhtLjvxdzvRVBzFp2gkHCh
```

```
OC/YBZODkZ0tt/FmdsTJcFBeYhXrgJmQAAAMEA0EwoZmiAjNbNCvNjX0tJ4J8IXc/qcfo4
3UCyyYXICV61si3IGYgGiol9bes0669DM7bmxVmE7fi6xR9R7c3Q9HqmmX08X+MArRDz6k
MyzOUf7t2Tb05o47APQaZeCZORYJxDFF6ciBFg+6IBk6Y34+4HosvTRvxmb+Ih/HBLd+OA
ZxHy7Ywts3ojGvk0kapvkiB8NM271nkSPWzcSQ2OAnY1BPDmMihFw6ns8by8o6gNNcPiec
pQnlmy7oWGHiqfAAAACGpvaG5Ab2hvAQI=
-----END OPENSsh PRIVATE KEY-----
```

```
john@oho:~/ssh$
```