Advanced SSH and Linux Server

Franz Schäfer

Linux LV, WU Wien

April 17, 2015

Table of contents

Basic SSH

- Text based connection to remote servers
- Copy files to and from remote servers
- Remote command execution

```
# ssh anna@meinserver.daheim.at
# scp meinedatei.txt hansi@woanders.at:/var/www/
# sftp root@meinserver.daheim.at:blabla.tgz .
# ssh hansi@meinserver.daheim.at "find /tmp"
```

What is Secure in SSH

- Encrypts traffic
- Checks the identitiy of remote hosts

- does **NOT** protect you from compromized local host
- does **NOT** always protect you from compromized remote host

Interactive Remote Login with SSH

```
# ssh h7788999@login.wu-wien.ac.at
The authenticity of host 'login.wu-wien.ac.at (137.208.3.7
# established.
RSA key fingerprint is a2:61:d0:f8:1a:13:f7:71:51:26:b8:c2
Are you sure you want to continue connecting (yes/no)?
```

Kerberos and SSH

```
# kinit h7788999
# ssh -K h7788999@pecuchet
# klist

-K .... Enables forwarding (delegation) of GSSAPI credenti


a .5login files enables passwordless login:

e.g. /root/.k5login

user1@WU-WIEN.AC.AT
user2@WU-WIEN.AC.AT
```

Man in the Middle

```
# ssh  irgendwohin

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now
(man-in-the-middle attack)!
It is also possible that the RSA host key has just been
changed. The fingerprint for the RSA key sent by the
remote host is
90:9c:46:ab:03:1d:30:2c:5c:87:c5:c7:d9:13:5d:7
```

Copy Files with SSH

```
# echo bla >bla.txt
# scp bla.txt  anna@example.com:
# scp jemand@irgendwo.at:bla .
# scp -r diplomarbeit/ h7788999@login:
# sftp
```

SSH Configuration

- .ssh/config

```
Host wu
HostName pecuchet.wu-wien.ac.at
User h7788999
```

- .ssh/known_hosts
- .ssh/authorized_keys
- Sitewide: see /etc/ssh/sshd_config and /etc/ssh/ssh_config

Public Key (RSA/DSA) Login

```
# ssh-keygen (eventuell -f)

(choose a good passphrase)

# ssh-copy-id  hansi@meinserver.at

or do it manually:

# scp .ssh/id_rsa.pub  wu:
# cat id_rsa.pub >>.ssh/authorized_keys

you can have your keys in any file e.g:
```

Remote Command Execution

```
# ssh hans@meinserver.at  "ls -l /tmp"

echo bla | ssh hans@meinserver.at \
"cat - > bla.txt"

ssh hans@meinserver.at "ls -l /tmp" | grep bla
```

Usefull for scripts...

Limit the rights of a key

In the file .ssh/authorized_keys

```
from="137.208.77.7",no-pty,no-port-forwarding,
  command="/root/bla.sh" ssh-dss AAAUH7T9Y....
```

X11 Forwarding

```
# ssh -X user@woanders.at
# echo $DISPLAY
# localhost:10.0
# xterm &
# xauth list
```

Beware: A remote attacker might be able to spy on you. You have to trust the remote host in this case.

ssh agent

ssh-agent can cache the access to your private key.

```
# ssh-agent xterm &
# ssh-add

... type passphrase ...
```

Usually included in the graphical login.
SSH option a allows forwarding of access to the ssh agent.

Port Forwarding

```
# ssh  -L 3333:proxy.wu-wien.ac.at:8080 h778899@login
```

allows access to remote proxy on local port 3333

optional: use -g

```
# ssh -R 4567:localhost:80 h778899@login
```

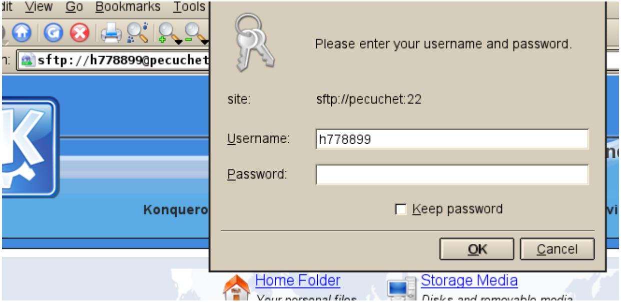
allow a remote user to conntect to port
4557 to access your local server

Built in Socks Proxy

```
# ssh -D 9999 hans@woanders.at
```

GUI access to Files

Use URL like `sftp://hans@remote.at:bla/blah/`


dit View Go Bookmarks Tools
n: sftp://h778899@pecuchet
Konquero
Home Folder
Your personal files
Storage Media
Disks and removable media

Please enter your username and password.

site: sftp://pecuchet:22

Username: h778899

Password:

☐ Keep password

netcat - the swiss army knife

```
# apt-get install netcat
# netcat -h
# nc -h
# echo bla bla| netcat -l -p 7777
telnet localhost 7777

Some netcat like tools in debian:

netcat-traditional - TCP/IP swiss army knife
netcat-openbsd - TCP/IP swiss army knife
ncat - part of the nmap package
netsed - network packet-altering stream editor
```

inetd - the superdaemon

config in /etc/inetd.conf

```
pop-3 stream tcp nowait root
      /usr/sbin/tcpd /usr/sbin/in.pop3d
4567  stream tcp nowait  nobody
      /usr/sbin/tcpd /bin/nc  -t 192.168.1.1 80
```

Reread the configuration file:

```
# killall -HUP inetd
```

tcp wrapper

Built in firewall library for applications

- /etc/hosts.allow
- /etc/hosts.deny

Example:

```
ALL:127.0.0.1,192.168.0.0/255.255.255.0
man hosts_access
```

Apache Webserver

Marketshare of Apache Web Serers (Number of Sites)

- 52% Apache
- 21% Nginx
- 11% Microsoft IIS

(Netcraft Survey March 2015)

Access a Webserver via Commandline

```
# telnet www.wu.ac.at 80
GET /
# telnet www.wu.ac.at 80
 HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Wed, 05 Dec 2007 12:38:35 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=iso-8859-1

# wget -S http://www.wu.ac.at
```

Install Apache on Debian/Ubuntu

```
# apt-get install apache
# apachectl configtest
# apachectl restart
# /etc/init.d/apache2 restart
```

Apache Configuration

```
/etc/apache2/httpd.conf
/etc/apache/httpd.conf
/etc/apache2/apache2.conf

some options can be configured in .htaccess

Most options in otherfiles that are included like this

Include /etc/apache2/mods-enabled/*.load
Include /etc/apache2/mods-enabled/*.conf

Include /etc/apache2/sites-enabled/
```

Scopes of the Apache Config

- Sitewide

```
Listen 80
DocumentRoot /var/meinwww/
```

- Virtual Host
- Directory
- Location

A simple HTML Document

create a file named index.html

```
<html>
<h2>test &uuml;berschrift</h2>
test <b>fett</b>
</html>
```

Per default: index.html will be served if you go to a URL that points to a directory.

Example: VirtualHost

Can be based on Name or IP

```
<VirtualHost 123.23.17.9:80>
ServerAdmin webmaster@meinserver.at
DocumentRoot /var/www/meinserver/
ServerName www.meinserver.at
ServerAlias meinserver.at
php_flag register_globals 0
RedirectPermanent /w/ http://wuw.at/bla/
</VirtualHost>
```

Example: Configuration for a Directory

```
<Directory /var/www/scripts/>

 AllowOverride AuthConfig
 Options +ExecCGI -Indexes
 Addhandler cgi-script .cgi
</Directory>
ScriptAlias /cgi/ /var/www/scripts/
```

Securing a Webserver via HTTPS

```
<VirtualHost 12.34.56.78:443>
SSLEngine on
SSLCertificateFile /etc/cert/mein.crt
SSLCertificateKeyFile /etc/cert/mein.key
ServerName meinserver.at
DocumentRoot /var/www-secure
</VirtualHost>
```

VirtualHosts with SSL should have different IPs But will now also work via SNI.
You need to generate your keys with e.g. openssl

Generate your keys with openssl

```
# openssl req -new -nodes \
   -newkey rsa:1024 -keyout mein.key \
   -out mein.csr

# openssl x509 -req -in mein.csr \
   -signkey mein.key -out mein.crt \
   -days 365
```

Check it via:

```
# openssl rsa -in mein.key -text
# openssl req -in mein.csr -text
```

Get your keys certified

- Verisign, Thawte , & Co... $$
- TCS Terena (aconet) - free for .ac.at
- Peer2Peer: cacert.org

A simple CGI Script

```
#!/bin/bash
echo Content-type: text/plain
echo
echo my process id
id
echo date and time
date
```

A simple PHP Script

```
<HTML>
<?
  for($i=1; $i<20 ; $i++) {
    echo $i," squared is ",$i*$i,"<br>";
  }
?>
</HTML>
```

Security for Web Scripts

- Update Often
- Update Regularily
- Off the shell scripts and packages - keep track of new versions

SQL Injection anc Cross Site Scripting

```
$res=mysql_query(
 ’SELECT * FROM bla WHERE id="’ . $_GET[’id’] . ’"’
);

echo "Your id is ",$_GET[’id’];
```

Top PHP Secruity Mistakes

- Use Unfiltered Input (and Include File, Build SQL Query, etc
- Unfilter Output XSS

Mailserver Basics

- Store and Forward via port 25 (SMTP)
- Per default mail end up in an mbox file in /var/spool/mail/
- Per default mail end up in an mbox file in /var/spool/mail/
- Later: Download mails via pop3
- Then: Manage mailbox on server via IMAP

Overview Mailserver

MTA

sendmail	Old but good
exim	small, simple, GPL
postfix	the contender
qmail	exotic

IMAP

cyrus	stable, powerful
courier	simpler for small sites
uw-imapd	standard mbox format

Email via Telnet

```
host -t mx wu.ac.at
telnet mx1.wu.ac.at 25
220 mx1.wu.ac.at ESMT..
helo .
mail from: fs@mond.at
rcpt to: mond@wu-wien.ac.at
data
bla
.
quit
```

Commandline Email - mutt

```
# echo test | \
   mutt -s test xx@mond.at

# mutt -f  \
  imaps://h7788999@sslmail.wu-wien.ac.at
```

mysql commands

```
# mysqladmin -uroot -p create bladb
# mysqldump -uroot -p bladb >other.dump
# cat other.dump | mysql -uroot -p blidb
# echo "select * from blatable;" \
  | mysql -uroot -p  bladb

# mysql -uroot -p  bladb

  CREATE USER ’anna’@’localhost’;
  SET PASSWORD FOR ’anna’@’localhost’ = PASSWORD(’geheim’)
  GRANT SELECT ON bladb.* TO ’anna’@’localhost’ ;
```

Samba - Fileserver for Windows

in the file /etc/samba/smb.conf

```
[musik]
comment = meine mp3sammlung als share
writable = no
locking = no
path = /extraplatte/mp3/
public = yes
hosts allow = 192.186.0.0/255.255.0.0
```

NFS - the Unix Network Filesystem

in the file /etc/exports

```
/home/       gss/krb5i(rw,sync,fsid=0,no_subtree_check)
/data/       10.11.12.13(rw,no_subtree_check)
```

kvm virtualization

```
# wget \
http://distro.ibiblio.org/tinycorelinux/5.x/x86/release/Cor

# qemu-img create -f qcow2 tinycore.qcow2 2G
# kvm -hda tinycore.qcow2 -cdrom CorePlus-current.iso -boot
```

Other Server Applications

asterisk	IP telephony (sip, h323, isdn, . . .)
nagios, icinga	monitoring
small services	dhcp, dnc, ntp, tftp . . .
X11	terminal server
kerberos, ldap, radius	authentication and directory
kvm, xen, qemu, LXC	virtualization
irc, jabber	chat
. . .	. . .