SSH and FTP on Ubuntu 9.04

WNYLUG
Neal Chapman
09/09/2009

SSH (Secure Shell)

Secure Shell or **SSH** is a network protocol that allows data to be exchanged using a secure channel between two networked devices. Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plaintext, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH - Server and Client

- SSH uses the client/server model where many clients can connect to a single server
- Clients can be console based or have a limited graphic interface
- A variety of SSH servers and clients are available
- Favorite clients?
  - Linux: ssh
  - Windows: Putty

SSH Server Features

- Encrypted shell access using a symmetric cipher
- Authentication
  - Host based
  - Public key
  - Challenge response
  - Password
- Tunneling
  - Client to server
  - Server to client

SSH Server - sshd

- Install SSH Server on Ubuntu 9.04
  - sudo apt-get install openssh-server
- Initial Configuration
  - sudo nano /etc/ssh/sshd_config
  - Server listen port
    - Port 22
    - PermitRootLogin no
    - RSAAuthentication yes
    - PubleyAuthentication yes
    - PasswordAuthentication yes
    - X11Forwarding yes

First SSH Connection

```
deldavis@Rodan:~$ ssh megalon -l deldavis
The authenticity of host 'megalon (192.168.55.10)' can't be established.
RSA key fingerprint is 25:d5:5d:8e:cb:3a:58:4c:5e:0c:f1:b1:8b:f8:fa:ea.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'megalon,192.168.55.10' (RSA) to the list of known hosts.
deldavis@megalon's password:
Linux Megalon 2.6.28-15-generic #49-Ubuntu SMP Tue Aug 18 18:40:08 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sun Sep  6 08:55:22 2009 from 192.168.55.229
deldavis@Megalon:~$
```

Protect SSH with Public Key

- Using password authentication leaves you open to brute force attack
- Enable Public Key to stop brute force

```
skinner@Megalon:~$ ssh rodan -l skinner
The authenticity of host 'rodan (192.168.55.12)' can't be established.
RSA key fingerprint is 73:53:3b:c9:b6:7f:4b:a4:48:42:db:d0:38:02:8a:d2.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'rodan,192.168.55.12' (RSA) to the list of known hosts.
Permission denied (publickey).
skinner@Megalon:~$
```

Create Public Key on Client Side

- To use Public Key authentication the server needs the public key and the client needs the private key
- Generate public and private keys

```
skinner@Megalon:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/skinner/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/skinner/.ssh/id_rsa.
Your public key has been saved in /home/skinner/.ssh/id_rsa.pub.
The key fingerprint is:
80:53:e1:23:ce:25:cc:76:1a:d2:ff:0d:07:b3:65:6a skinner@Megalon
```

- Add public key to ~/.ssh/authorized_keys on server

Tunnel - Client to Server

- Traffic can be tunneled over SSH
- Tunnel provides secure encrypted channel for traffic
- Example - Tunnel VNC:
  - Establish SSH connection tunneling client port 5901 to server port 5901
  - From client establish VNC connection to localhost: 5901
- Other examples
  - FTP, HTTP, NNTP

Tunnel - Server to Client

- Bring GUI to client

```
deldavis@Megalon:~$ ssh rodan -X
Last login: Tue Sep  8 08:31:01 2009 from megalon.monsterisland.net
deldavis@Rodan:~$ gedit &
[1] 19614
deldavis@Rodan:~$ ps
  PID TTY          TIME CMD
19596 pts/1    00:00:00 bash
19614 pts/1    00:00:00 gedit
19619 pts/1    00:00:00 dbus-launch
19623 pts/1    00:00:00 ps
```

SFTP

- An additional service provided by an SSH Server is SFTP or FTP over SSH
- Allows FTP like file transfer over an SSH connection
- Advantages over an FTP transfer
  - Encrypted
  - File transfer progress
- Disadvantages
  - Slower due to encryption
  - Giving someone SFTP access is the same as giving them SSH access
- Clients: sftp, FileZilla

SFTP Example

```
skinner@Megalon:~$ sftp skinner@rodan
Connecting to rodan...
Enter passphrase for key '/home/skinner/.ssh/id_rsa':
sftp> ls
examples.desktop
sftp> mput *.mp3
Uploading 01 - The Moan.mp3 to /home/skinner/01 - The Moan.mp3
01 - The Moan.mp3                             100% 8810KB   8.6MB/s   00:01
Uploading 02 - Heavy Soul.mp3 to /home/skinner/02 - Heavy Soul.mp3
02 - Heavy Soul.mp3                           100% 6114KB   6.0MB/s   00:00
Uploading 03 - No Fun.mp3 to /home/skinner/03 - No Fun.mp3
03 - No Fun.mp3                               100% 5960KB   5.8MB/s   00:01
Uploading 04 - Have Love Will Travel.mp3 to /home/skinner/04 - Have Love Will Travel.mp3
04 - Have Love Will Travel.mp3                100% 6018KB   5.9MB/s   00:01
sftp> ls
01 - The Moan.mp3                 02 - Heavy Soul.mp3
03 - No Fun.mp3                   04 - Have Love Will Travel.mp3
examples.desktop
```

FTP (File Transfer Protocol)

File Transfer Protocol (**FTP**) is a standard network protocol used to exchange and manipulate files over an Internet Protocol computer network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications. Client applications were originally interactive command-line tools with a standardized command syntax, but graphical user interfaces have been developed for all desktop operating systems in use today. FTP is also often used as an application component to automatically transfer files for program internal functions.

FTP Client and Server

- FTP uses the client/server model where many clients can connect to a single server
- Clients can be console based or have a graphic interface
- A variety of FTP servers and clients are available
- Favorite servers?
  - Linux: PureFTPd
  - Windows: FileZilla Server
- Favorite clients?
  - Linux: ftp, FileZilla, GFTP
  - Windows: ftp, FileZilla

FTP Server - Pure-FTPd

- Install FTP Server on Ubuntu 9.04
  - sudo apt-get install pure-ftpd
- Initial Configuration
  - Pure-FTPd uses the Linux host to manage its user accounts, if you create a user on your system then you have also given that user FTP access
  - To jail a user, keep them in their home directory, edit \etc\passwd
    - Change skinner:x:1002:1002:,,,:/home/skinner:/bin/bash
    - To skinner:x:1002:1002:,,,:/home/skinner/./:/bin/bash

FTP Example

```
skinner@Megalon:~$ ftp rodan
Connected to rodan.monsterisland.net.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 09:35. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (rodan:skinner): skinner
331 User skinner OK. Password required
Password:
230-User skinner has group access to:  1002
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mput *.mp3
mput 01 - The Moan.mp3? y
200 PORT command successful
150 Connecting to port 43642
226-File successfully transferred
226 0.768 seconds (measured here), 11.20 Mbytes per second
9021755 bytes sent in 0.75 secs (11805.2 kB/s)
```

Additional Resources

- SSH
  - http://en.wikipedia.org/wiki/Secure_Shell
  - http://www.chiark.greenend.org.uk/~sgtatham/putty/
- FTP
  - http://en.wikipedia.org/wiki/Ftp
  - http://www.pureftpd.org/project/pure-ftpd