Cool SSH Tricks

QCLUG

By Aaron Johnson

fppt.com

What is SSH?

- Abbreviation for secure shell
- Cryptographic network protocol
- Used primarily for remote login to computer systems
- But it can do so much more...

fppt.com

Transfer files via tar + stdout + cat over SSH!

```
tar zcvf - ~/directory_of_files | ssh user@host "cat > /archive.tar.gz"
```

Live Demo!

fppt.com

Edit remote files directly using SSH/SCP + VIM!

NOTE: The extra / after the host is not a mistake!

```
vim scp://user@host//absolute/path/to/file
```

Live Demo!

fppt.com

Local and Remote Port Fowarding!

Local port forwarding

```
ssh yourserver -L 0.0.0.0:80:remoteserver:80
```

If you do a port forward frequently you can add it to ~/.ssh/config

```
    Host remoteserverfw
    HostName yourserver
    LocalForward 80 remoteserver:80
```

Remote port forwarding

```
ssh yourserver -R 80:remoteserver:80
```

If you want to to allow nonlocal users to be able to connect then enable GatewayPorts on the remote /etc/sshd_config:

```
    GatewayPorts yes
```

Pipe mic audio to another computer over SSH

Example:

```
arecord -f dat | ssh -C user@host aplay -f dat
```

Live Demo!

fppt.com

Single Sign-on with LDAP and sshPublicKey openssh-lpk schema attribute

There is a relatively simple way to achieve single sign-on in an environment that has LDAP thanks to a nifty schema attribute called sshPublicKey.

Warning! This does require custom schema changes to be made to your Active Directory/LDAP domain, AD compatible example here: https://gist.github.com/hsw0/5132d5dabd4384108b48

Once the schema has been modified you can add the sshPublicKey attribute to any user account.

Also SSSD includes a program called sss_ssh_authorizedkeys that works with SSH to pass the value of this attribute directly to sshd thus enabling single sign-on!

Live Demo!

fppt.com

Single Sign-on with LDAP and sshPublicKey openssh-lpk schema attribute

The magic for this is in two files:

/etc/sssd/sssd.conf:

```
ldap_user_ssh_public_key = sshPublicKey
```

/etc/ssh/sshd_config:

```
AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys
AuthorizedKeysCommandUser nobody
```

fppt.com

But wait there's more!

During my research I found examples of how to do these other cool tricks:

- Play an mp3 to a remote machine using SSH
- Create a VPN tunnel using Sshuttle + SSH
- Avoid firewalls or multiple connection hops (or via an ssh bastion) by piping port 22 over netcat + ssh
- Create a SOCKS proxy that can be used with your favorite web browser + SSH
- Interface with remote filesystems in real-time using the sshfs FUSE userspace driver
- Replace your old FTP server that is sending passwords in the clear using SFTP (SSH FTP)
- The list goes on and on!

fppt.com

The End

fppt.com