

SSH LAB

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 4 October 17th, 2005

SSH Remote Login

- Install SSH server
- Login to remote (neighbor)
- Accept key
- Compare `~/.ssh/known_hosts` to neighbor's `/etc/ssh_host_rsa_key.pub`
- Note addition of hostname and IP address
- If hostname, IP address or key is changed you get a warning

Authenticate via Public Keys

- `ssh-keygen -t rsa`
- Enter a passphrase
- Copy over to remote machine
- `scp ~/.ssh/id_rsa,pub username@IP address/hostname:~/.ssh/`
- `ssh username@IP address/hostname`
- Open text editor and copy and paste key
- Make sure text editor did not leave an automatic backup
- Remember: key is one, unbroken line
- Go into Webmin and change authentication parameters

SSH Agent

- Allows you to start a session and load keys only once
- Add key to two remotes
- `ssh-agent`
- `ssh-add`
- Now ssh to each of the remote servers
- Tied to particular bash shell. Will disappear when you log out (`exit`).
- `ps -T`

SSH Keychain

- Like ssh-agent except keeps keys in memory even if you logout
- Install keychain
- Add to ~/.bash_profile:

```
keychain id_rsa  
. ~/.keychain/$HOSTNAME-sh
```

- Null passphrase allows unattended reboots but allows easier exploitation of private key
- Add line to cron jobs for passwordless cron:

```
source ~/.keychain/$HOSTNAME-sh
```

Tunneling X Over SSH

- Enable in Webmin
- `ssh -X`
- X is a hog
- VNC better alternative

Port Forwarding with SSH

```
ssh -f -N -C -T -l [username] -L[localport]:localhost:[r  
[server hostname/IP address]
```

- -L option forwards stuff from localport on the client box to remoteport on hostname
- -f option allows ssh to run in background after it prompts for the login password
- -N means don't execute any remote command (like a shell initialization script). This is used because all we want is port forwarding.
- -C means use compression.
- -T disables a pseudo-tty allocation (again because all we want to do is port forwarding, not open a remote shell).

- -l is login as username
- On Macintosh use `127.0.0.1` instead of `localhost`

Port Forward Webmin

```
ssh -f -N -C -T -l [username] -L10001:localhost:10000  
[server hostname/IP address]
```

Port Forward VNC

- Install vncserver and vncclient

- On server:

```
vncserver -geometry 800x600 -depth 16 :1
```

- This starts VNC on port 5901

- On client:

```
ssh -f -N -C -T -l [username] -L5902:localhost:5901  
[server hostname/IP address]
```

```
vncviewer [-shared] localhost:2
```

SSH File Permissions

- For user accounts in `~/.ssh`, use the following permissions:

`~/.ssh` mode 700

`~/.ssh/id_dsa` and other private keys mode 400

`~/.ssh/id_dsa.pub` and other public keys mode 644

`~/.ssh/ssh_config` mode 644

`~/.ssh/known_hosts` mode 644

`~/.ssh/authorized_keys` mode 644

- Files in `/etc/ssh` should have these permissions:

`/etc/ssh` mode 755

`/etc/ssh/sshd_config` mode 644

`/etc/ssh/ssh_config` mode 644

/etc/ssh/ssh_host_dsa_key and other private keys mode 400

/etc/ssh/ssh_host_dsa_key.pub and other public keys mode 644

/etc/ssh/moduli mode 644