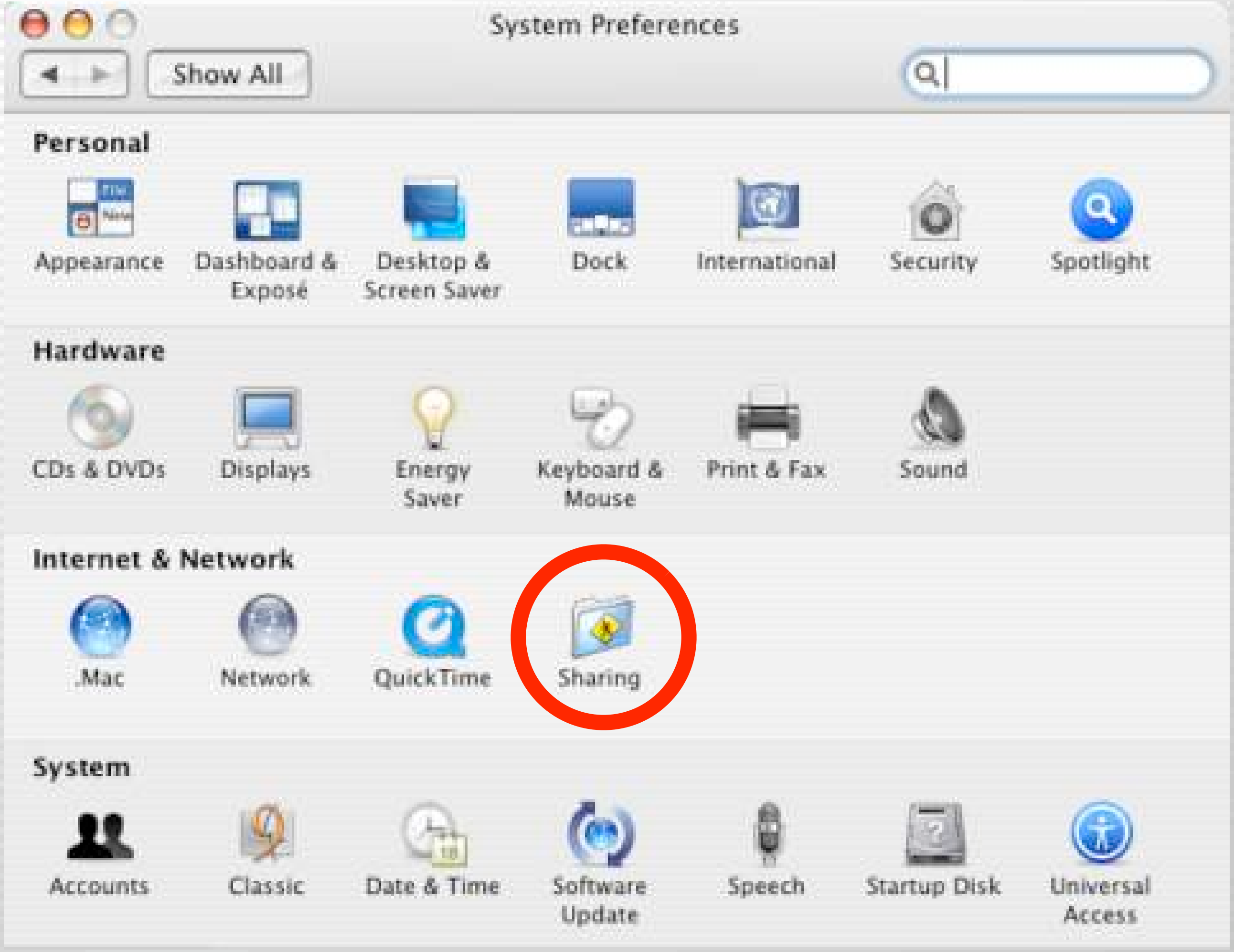
UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Enabling and Securing SSH

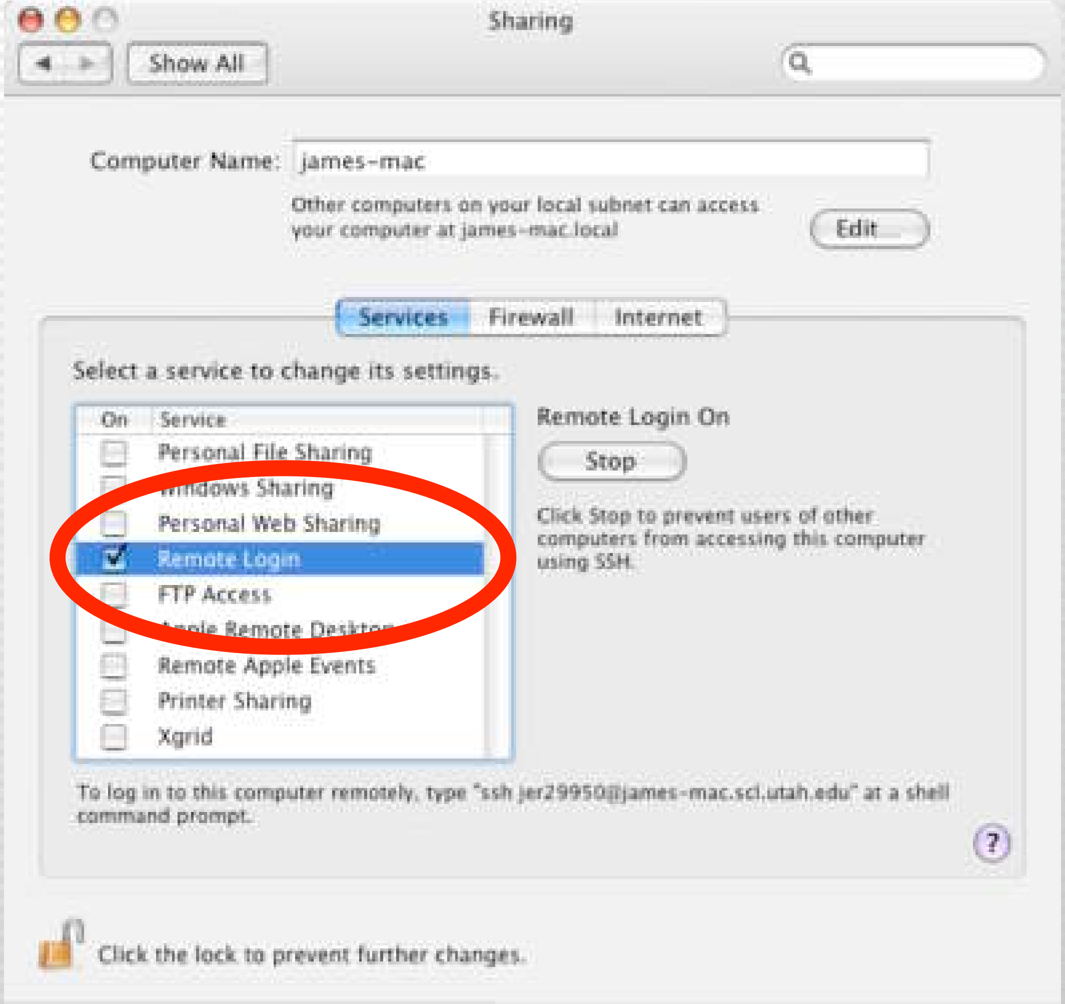
James Reynolds
University of Utah
Student Computing Labs
Macintosh Support
mac@scl.utah.edu

First, the enabling part...



UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

First, the enabling part...



Computer Name: james-mac

Other computers on your local subnet can access your computer at james-mac.local

Select a service to change its settings.

On	Service
□	Personal File Sharing
□	Windows Sharing
□	Personal Web Sharing
☑	Remote Login
□	FTP Access
□	Apple Remote Desktop
□	Remote Apple Events
□	Printer Sharing
□	Xgrid

Remote Login On

Click Stop to prevent users of other computers from accessing this computer using SSH.

To log in to this computer remotely, type "ssh jer29950@james-mac.scl.utah.edu" at a shell command prompt.

Click the lock to prevent further changes.

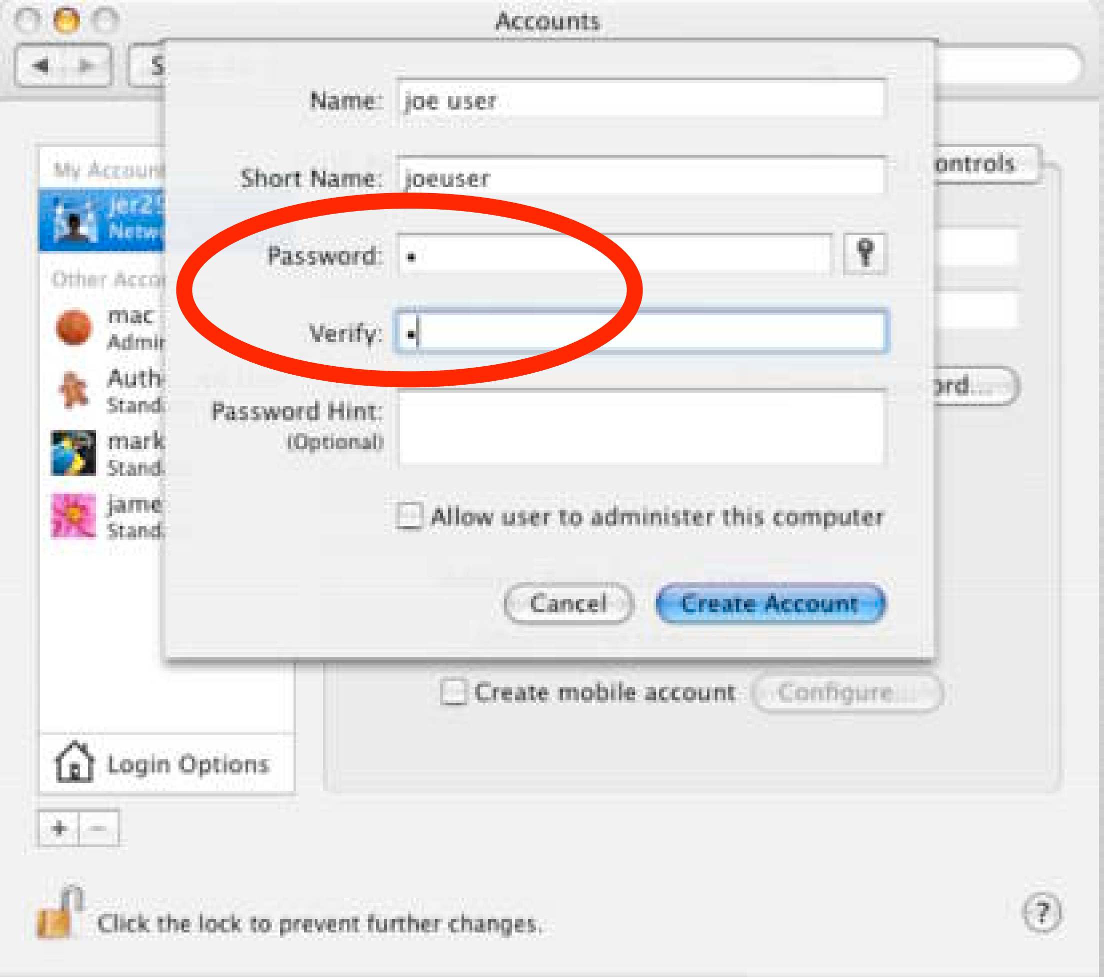
UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Questions?

All secure, right?

- I mean, this is SSH, it isn!t cleartext, so you have nothing to fear, right?
  - Right?

What about….



Name: joe user

Short Name: joeuser

Password: •

Verify: •

Password Hint: (Optional)

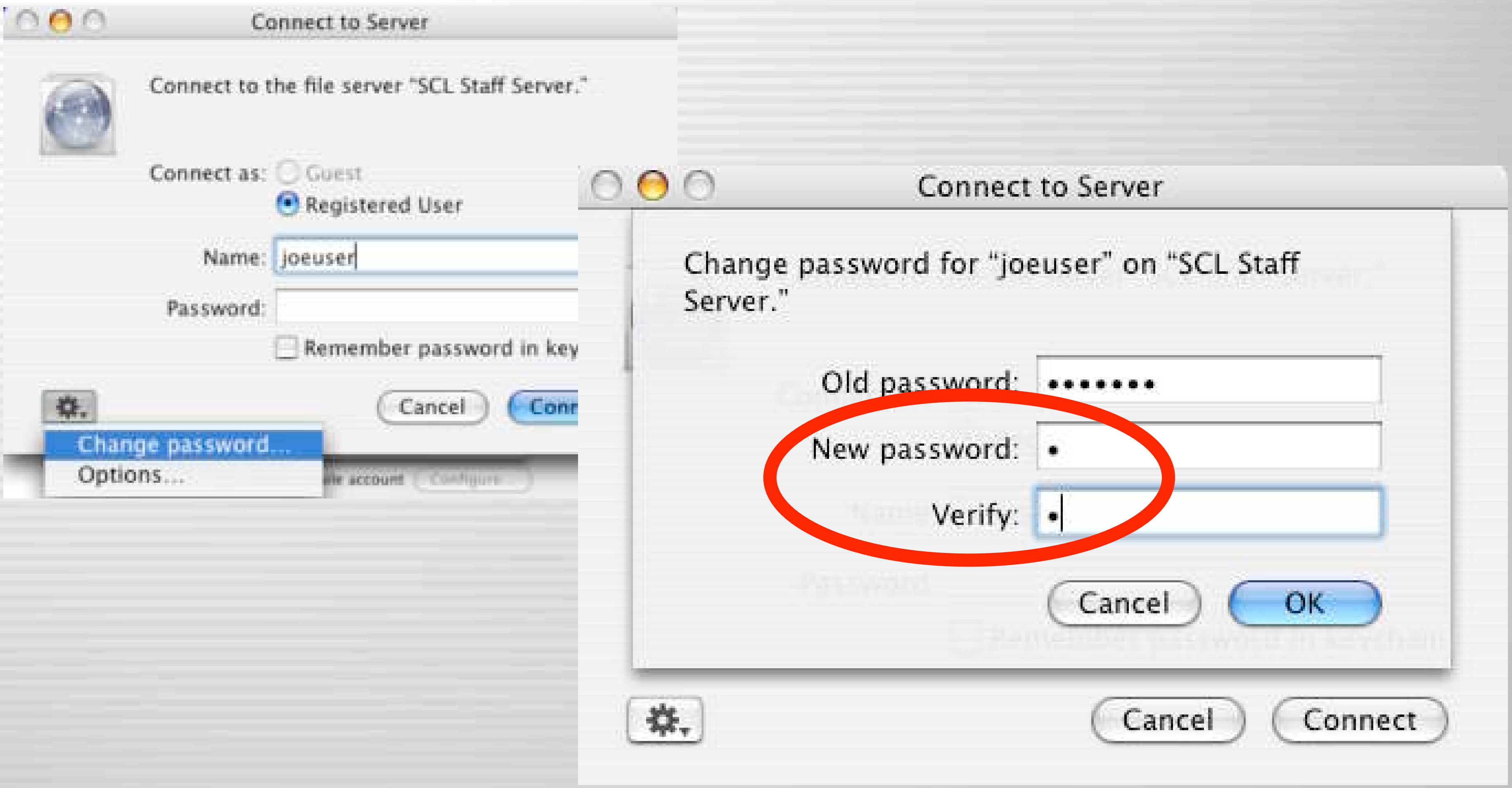
□ Allow user to administer this computer

□ Create mobile account

Click the lock to prevent further changes.

UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Or...



Connect to Server

Connect to the file server "SCL Staff Server."

Connect as: ○ Guest
● Registered User

Name: joeuser

Password:

□ Remember password in key

Connect to Server

Change password for "joeuser" on "SCL Staff Server."

Old password: •••••••

New password: •

Verify: •

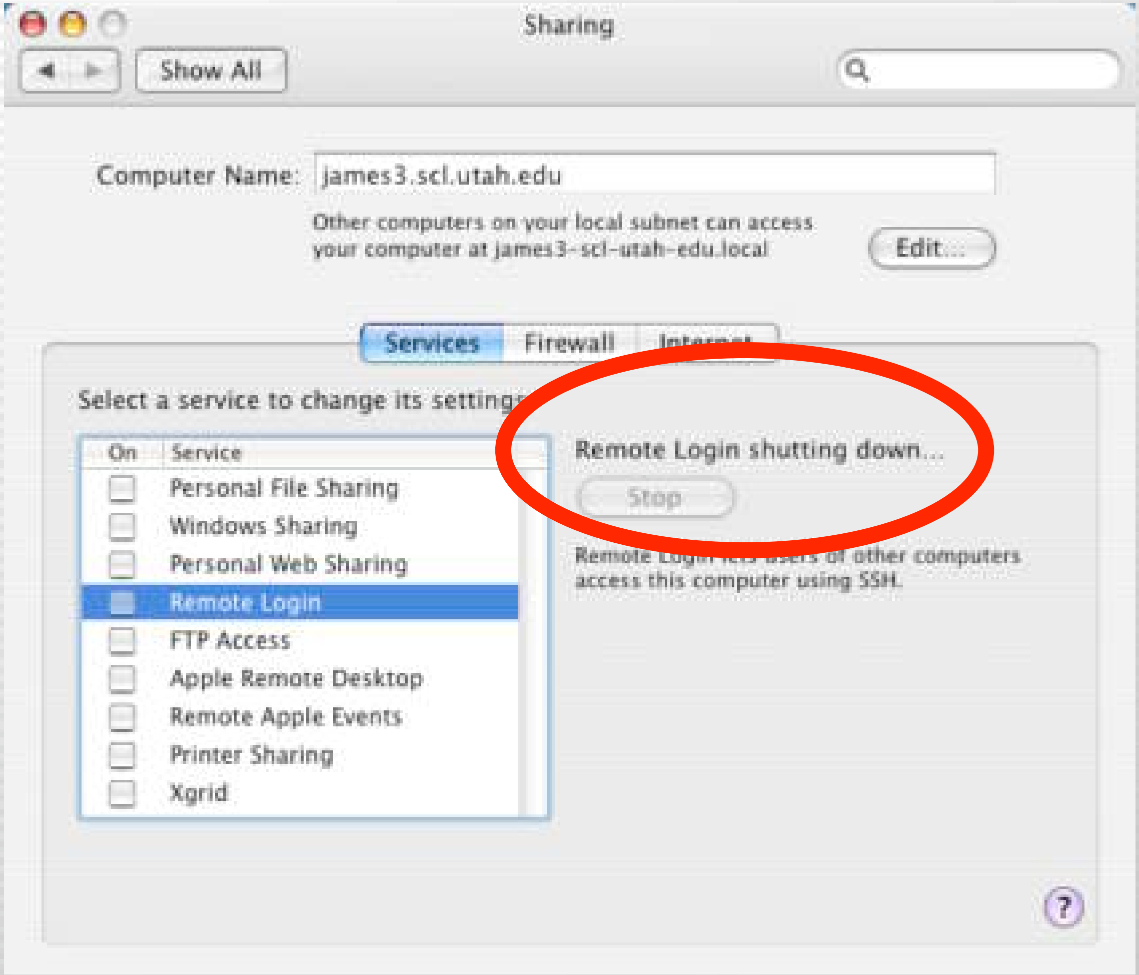
UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

"A certain institution of higher learning has discovered that fleets of their OS X boxes have been compromised... through weak passwords for SSH-enabled accounts..."

http://lists.grok.org.uk/pipermail/full-disclosure/2005-March/032951.html

Oh my! What to do?

- First:



Sharing

Computer Name: james3.scl.utah.edu

Other computers on your local subnet can access your computer at james3-scl-utah-edu.local

Select a service to change its settings.

On	Service
□	Personal File Sharing
□	Windows Sharing
□	Personal Web Sharing
□	Remote Login
□	FTP Access
□	Apple Remote Desktop
□	Remote Apple Events
□	Printer Sharing
□	Xgrid

Remote Login shutting down...

Remote Login lets users of other computers access this computer using SSH.

UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

If you must have SSH on...

- Disable protocol 1
- Add “AllowUsers”
- Enable TCP-Wrappers
- Enable IPFW
- Change the SSH port
- Autoscan ports with NMAP
- Autoscan /var/log/system.log
- Redirect root emails to yourself
- Perhaps use certs and not passwords

Diable Protocol 1

- Edit /etc/sshd_config and change

```
#Protocol 2,1
```

To

```
Protocol 2
```

- Restart SSH

Add “AllowUsers”

- Edit /etc/sshd_config and at end of file, add:

```
AllowUsers name1 name2 etc
```

- (Add names of allowed users)
- Restart SSH

Enable TCP-Wrappers

- /etc/hosts.deny contains:

```
ALL:ALL:deny
```

- /etc/hosts.allow contains:

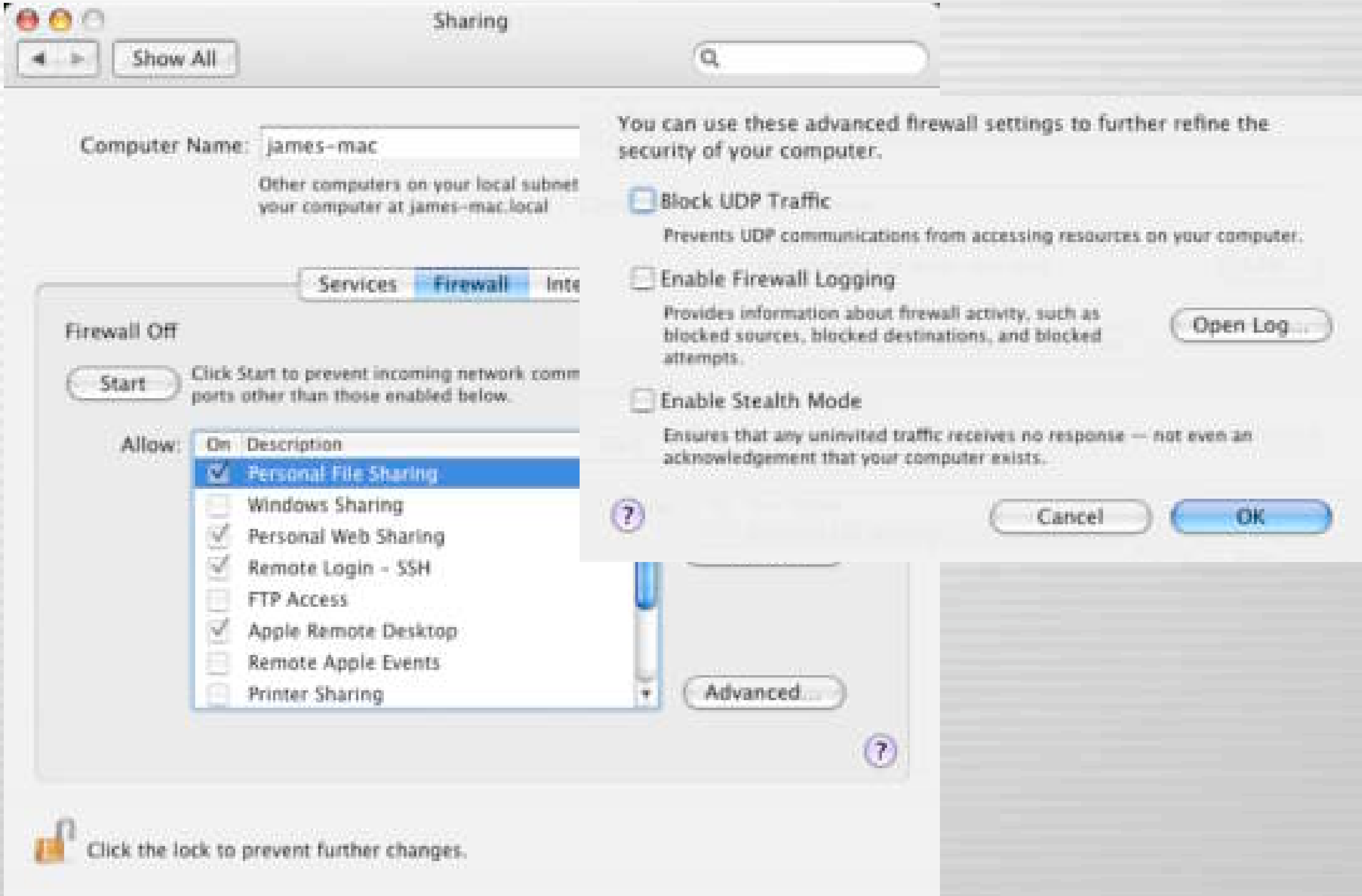
```
ALL:10.0.1.
ALL:10.0.2.1
```

- (Add IP!s of allowed machines)

Enable IPFW

- System Preferences on Mac OS X
  - Mostly closed - you must poke holes for services
  - Not very configurable
- Server Admin on Mac OS X Server
  - Mostly closed -you must poke holes for services
  - Very configurable
- Manual
  - IPFW doesn!t use a configure file, it is “configured” with a command, so it requires a startup script
- If you change SHH port, fix it in firewall settings!

IPFW on Mac OS X



Sharing

Show All

Computer Name: james-mac

Other computers on your local subnet
your computer at james-mac.local

Services | Firewall | Inte

Firewall Off

Start — Click Start to prevent incoming network comm
ports other than those enabled below.

Allow:

On	Description
☑	Personal File Sharing
☐	Windows Sharing
☑	Personal Web Sharing
☑	Remote Login - SSH
☐	FTP Access
☑	Apple Remote Desktop
☐	Remote Apple Events
☐	Printer Sharing

Advanced...

Click the lock to prevent further changes.

You can use these advanced firewall settings to further refine the security of your computer.

☐ Block UDP Traffic

Prevents UDP communications from accessing resources on your computer.

☐ Enable Firewall Logging

Provides information about firewall activity, such as blocked sources, blocked destinations, and blocked attempts.

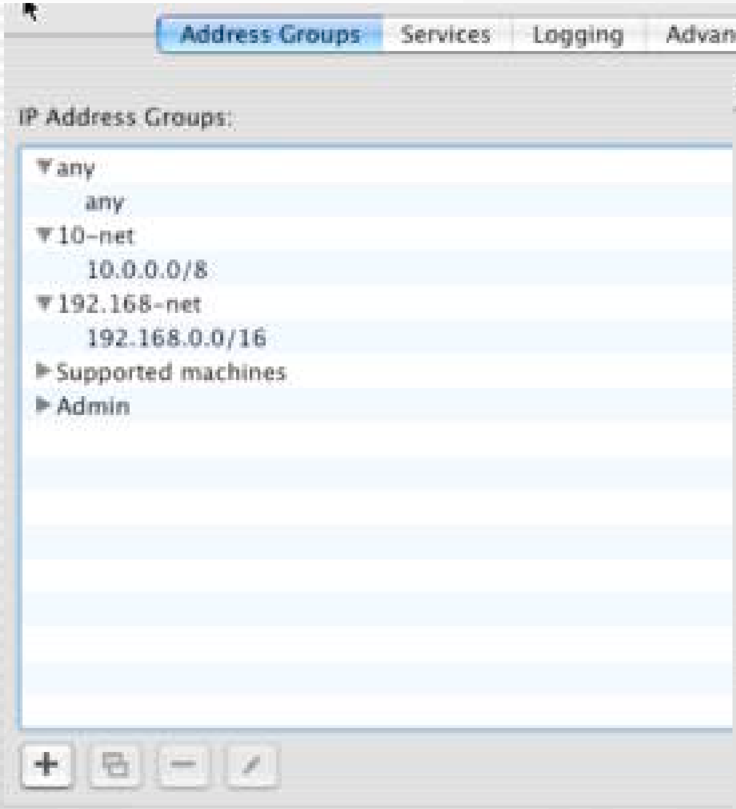
Open Log...

☐ Enable Stealth Mode

Ensures that any uninvited traffic receives no response — not even an acknowledgement that your computer exists.

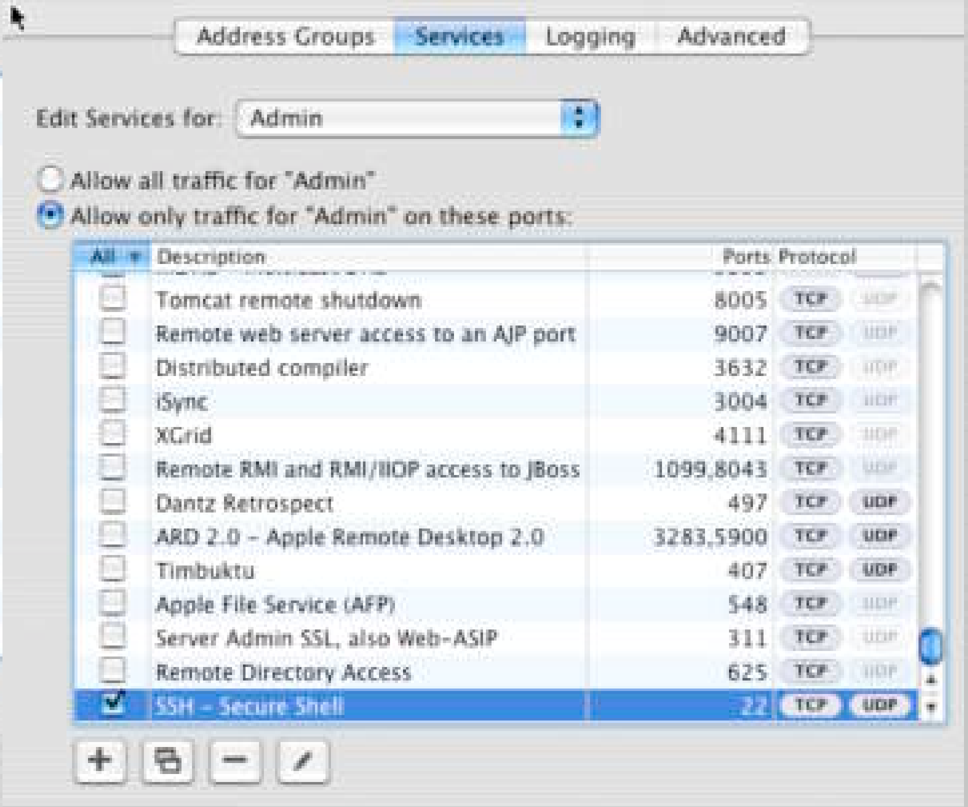
Cancel OK

IPFW on Mac OS X Server



IP Address Groups:

- ▼any
  - any
- ▼10-net
  - 10.0.0.0/8
- ▼192.168-net
  - 192.168.0.0/16
- ▶Supported machines
- ▶Admin



Edit Services for: Admin

○ Allow all traffic for "Admin"

● Allow only traffic for "Admin" on these ports:

All	Description	Ports	Protocol
□	Tomcat remote shutdown	8005	TCP
□	Remote web server access to an AJP port	9007	TCP
□	Distributed compiler	3632	TCP
□	iSync	3004	TCP
□	XGrid	4111	TCP
□	Remote RMI and RMI/IIOP access to JBoss	1099,8043	TCP
□	Dantz Retrospect	497	TCP UDP
□	ARD 2.0 – Apple Remote Desktop 2.0	3283,5900	TCP UDP
□	Timbuktu	407	TCP UDP
□	Apple File Service (AFP)	548	TCP
□	Server Admin SSL, also Web-ASIP	311	TCP
□	Remote Directory Access	625	TCP
☑	SSH – Secure Shell	22	TCP UDP

IPFW Manually

- Startup Script:

```
/sbin/ipfw -f flush
/sbin/ipfw add allow all from any to any via lo0
/sbin/ipfw add deny log ip from 192.168.0.0/16 to any in via en0
/sbin/ipfw add deny log ip from 172.16.0.0/12 to any in via en0
/sbin/ipfw add deny log ip from 10.0.0.0/8 to any in via en0
/sbin/ipfw add deny log ip from any to 192.168.0.0/16 in via en0
/sbin/ipfw add deny log ip from any to 172.16.0.0/12 in via en0
/sbin/ipfw add deny log ip from any to 10.0.0.0/8 in via en0
# allow admin subnet
/sbin/ipfw add allow ip from 123.123.123.0/24 to any
# block ssh
/sbin/ipfw add reset tcp from any to any 22 in    (fix if you changed port)
# mostly open rule
/sbin/ipfw add 65535 allow ip from any to any
```

Change the SSH port

- Edit /etc/sshd_config and change

```
#Port 22
```

To

```
Port 1234
```

(pick any port within reason)

- Edit /etc/services and change

```
ssh        22/udp    # SSH Remote Login Protocol
ssh        22/tcp    # SSH Remote Login Protocol
```

To

```
ssh        1234/udp    # SSH Remote Login Protocol
ssh        1234/tcp    # SSH Remote Login Protocol
```

Scan ports with NMAP

- See nmap presentation at earlier Mac Mgrs...
- http://www.macos.utah.edu/Documentation/macosx/security/nmap.html
- Don!t use nmap on < 10.4.2 (10.4.3?)
  - Lookupd bug hangs the server...

Autoscan /var/log/system.log

```
rm /path/to/system_log_alert_messages
/usr/bin/grep -i -f /path/to/system_log_watch_messages /var/log/system.log | /usr/bin/grep \
        -v -f /path/to/system_log_ignore_messages > /path/to/system_log_alert_messages
if [ -s /path/to/system_log_alert_messages ]; then
    /bin/cat /path/to/system_log_alert_messages | /usr/bin/mail -s "System.log report" root
fi
```

```
Feb 10 07:07:36 localhost sshd[1078]: Illegal user matt from 210.127.248.158
Feb 10 07:07:38 localhost sshd[1080]: Illegal user test from 210.127.248.158
Feb 10 07:07:40 sshd[1082]: Illegal user operator from 210.127.248.158
Feb 10 07:07:42 sshd[1084]: Illegal user wwwrun from 210.127.248.158
Feb 10 07:07:52 sshd[1096]: Illegal user apache from 210.127.248.158
Feb 10 07:07:59 sshd[1104]: Failed password for root from 210.127.248.158 port 58752 ssh2
Feb 10 07:08:01 sshd[1106]: Failed password for root from 210.127.248.158 port 59136 ssh2
Feb 10 07:08:03 sshd[1108]: Failed password for root from 210.127.248.158 port 59176 ssh2
Feb 10 07:08:15 sshd[1122]: Failed password for root from 210.127.248.158 port 60606 ssh2
```

Redirect root emails to yourself

- Edit /var/root/.forward and change

  /dev/null

  To

  yourname@yourserver.edu

Perhaps use certs & not passwds

- Good if you use one (secure) computer
- In Terminal, type:

  ```
  ssh-keygen -t rsa
  ```

- Type a passphrase (not the same as password)
  - You can leave it blank, but it is not recommended
- Copy contents of ~/.ssh/id_rsa.pub
- Add it to ~/.ssh/autorized_keys on server

Questions?