



## Requirements

- Modern Linux distribution
- *finger* package installed

## To Do

1. When your neighbor is finished with ssh, block your neighbor's IP address from using ssh with the `/etc/hosts.allow` and/or `hosts.deny`. Test the results.

You may also block a Windows host from using `putty.exe` (the ssh-client).

2. Create your own fake finger daemon:

- Checkout the `finger` command:

```
finger user@127.0.0.1
```

- Create a script file called `/usr/local/sbin/fingerd` with the following content:

```
#!/bin/bash
echo "Finger is disabled for privacy reasons ..."
```

- Make the new file executable:

```
chmod +x fingerd
```

- Copy an existing snippet to a file called *finger* and use the following options in the file:

```
wait = no
user = nobody
protocol = tcp
server = /usr/local/sbin/fingerd
```

- Activate the changes by restarting the super daemon or by using:

```
killall -SIGHUP xinetd
```

- Checkout the `finger` command again.

3. Make your syslogger available for remote logging (add `-r` in `/etc/sysconfig/syslog`). Others may redirect to your host by addressing you with `@hostname` in the `syslog.conf` file.
4. Create a group called *loggroup*. Add your user as a member. Change the default group owner of the `/var/log/messages` file to *loggroup* in the `/etc/logrotate.conf`.

## Quick Reference Objectives to learn

### TCP wrapper

#Check order and examples:

```
vi /etc/hosts.allow
```

#See: `man 5 hosts_access`

```
in.telnetd : ALL : spawn echo "login from %c to %s ! mail -s warn root
```

```
vi /etc/hosts.deny
```

```
sshd : ALL EXCEPT 172.28.24.
```

### Super daemon xinetd

#Tip: Use `snippetname` from `/etc/services`

```
vi /etc/xinetd.conf
```

#Edit general settings

```
vi /etc/xinetd.d/snippet
```

#Change settings per `snippet`

```
only_from
```

= `172.28.0.0/16 172.27.200.1`

```
no_access
```

= `172.28.24.1`

```
access_times
```

= `9:00-18:00`

```
per_source
```

= `2`

```
/etc/init.d/xinetd restart
```

#Activate changes

### Logging

```
vi /etc/syslog.conf
```

#Edit syslog logger configuration

#See: `man syslog.conf` for *facilities* and *priorities*

```
vi /etc/sysconfig/syslog
```

#Edit `syslogd` daemon `-r` for remote logging

```
SYSLOGD_PARAMS="-r -s my.domain"
```



```
SYSLOGD_OPTIONS="-r -m 0"
```

#Generate message for syslogger:

```
logger -i -p kern.emerg -t yourname "Text"
```

```
vi /etc/logrotate.conf
```

#Edit `maxlog` files, `logrotate` is in `crontab`

## Theory Modules

LPIC 1 Certification Bible, isbn 0-7645-4772-0

- p. 413-420 System Logging
- p. 602-604 Using the Internet Super Server
- p. 697-701 Configuring TCP wrappers

## Extra References

- [www.tldp.org](http://www.tldp.org)