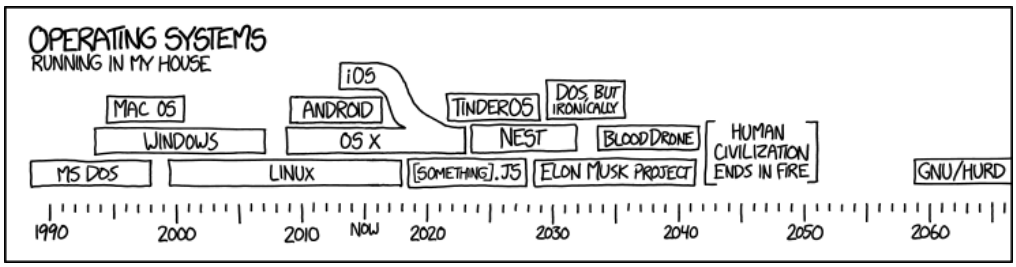
# SSH and web servers

Monday, April 20, 2015 8:34 AM




One of the survivors, poking around in the ruins with the point of a spear, uncovers a singed photo of Richard Stallman. They stare in silence. "This," one of them finally says, "This is a man who BELIEVED in something."

## Objectives

- Explain the need for encrypted services
- Log in remotely using ssh
- Copy files to and from a remote system securely
- Setup and configure SSH options
- Configure ssH to use key based authentication
- Remove host record from ~/.ssh/known_hosts

---

he openSSH suite of tools

- Created to replace insecure/plaintext tools and daemons
  - ↳ telnet / telnetd
  - ↳ rcp (remote copy)
  - ↳ rsh (remote shell)
  - ↳ ftp / ftpd (never install this anymore...)

Replaced under ssH suite

- ↳ scp (secure, remote copy)

↳ sftp (secure ftp)

↳ ssh / sshd (secure remote shell)
(also my wife's initials ...)

↳ ssh-keygen creates and manages RSA keys

---

Introduction to OpenSSH

↳ Came from OpenBSD Unix project - 1999
↳ Forked and brought to Linux
↳ Everyone is running OpenBSD OpenSSH
↳ only game in town
↳ If you learn it once you learn everywhere

↳ Uses public key encryption
↳ Client side + Server side
↳ non-secure protocols (rcp, rsh, ftp)

Will happily trust you and connect

↳ SSH suite uses site "finger printing"
to alert against M-I-T-M attacks

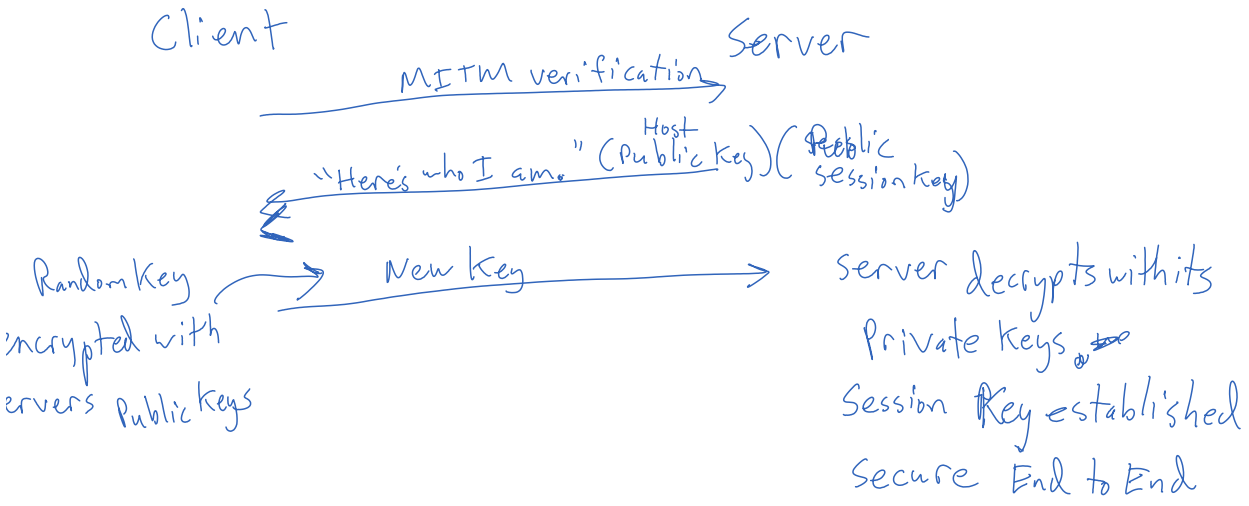
↳ After secure and encrypted connection established
↳ then data is transferred through a secure tunnel

↳ You will be using SSH protocol ALOT in your life
↳ Learn it now young Jedi....

---

it works

- Uses a host key pair and a session key pair
  - ↳ Host key generated at install both public + private keys




---

settings
/etc/ssh

ssh_config client global settings

sshd_config server global settings

~/.ssh local ssh client configuration

authorized_keys which system your server will accept connections from with out a password

id_rsa id_rsa.pub your public and private keys

Known_hosts Contains RSA public keys of systems you have connected to.

---

SSH

ng

Open one Fedora system to be the client

Open another Linux system

↳ if Fedora sudo yum install openssh-server

↳ sudo systemctl start sshd.service

↳ sudo systemctl enable sshd.service

↳ Ubuntu

↳ sudo apt-get install openssh-server

↳ auto starts

.tax

- ssh aplustudent@10.0.0.9
  username@IP

- scp thefile.txt aplustudent@10.0.0.9
  ↑ filename username ↑ IP

Go ahead and connect via SSH or SCP and then look at ~/.ssh/known_hosts file.

What do you see?

SSH can be used to execute "one off" commands.

ssh aplustudent@10.0.0.9 uptime

ls ~

There is a -v command to debug connection output

-p

scp aplusstudent@10.0.0.9:memos.txt memodir

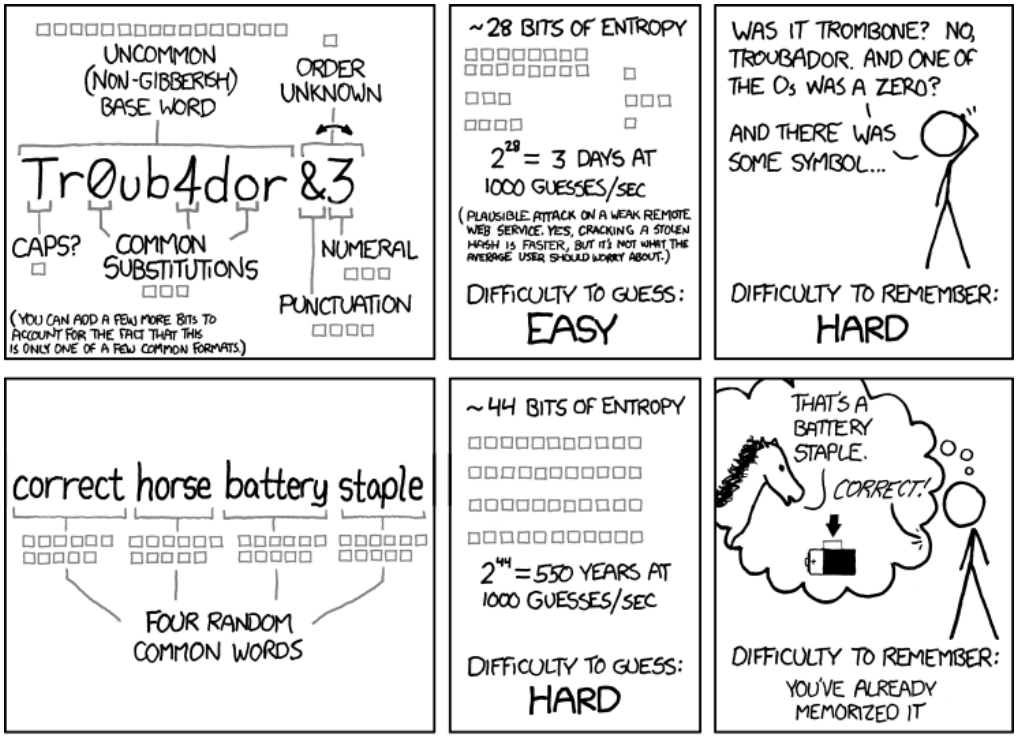
sync

Smarter than scp, as it won't copy unchanged files
only sync new data

rsync -av
aplusstudent@10.0.0.9:memos.txt memodir
↑ copy only files and dirs

Good use for backing up data as not all data changes

ased Authentication ... Passwords are the problem...




use ssh-keygen to generate a new public/private keypair
his will beused as our authentication mechanism

ssh-keygen -t rsa (default is 2048 bits - thats very large)
you can use -b 4096 or 8192 if paranoid

two files will be generated in ~/.ssh

↳ id_rsa ⇐ guard these keys (chmod 600)
↳ id_rsa.pub

y Your new ID to the server

- ssh-copy-id aplustudent@10.0.0.9
- use -i if you want to copy a different identity
- Now authenticate ssh aplustudent@10.0.0.9
  ↳ No password prompt
  ↳ Downside is you have to move private keys around
  ↳ or set up multiple key pairs (Home, office, Laptop)

bleshooting

↳ /var/log/messages /var/log/secure
↳ or a -v, -vv, -vvv for debug info

l forwarding

- See ch. 18

---

mary

→ OpenSSH suite of secure tools to replace insecure UNIX tools

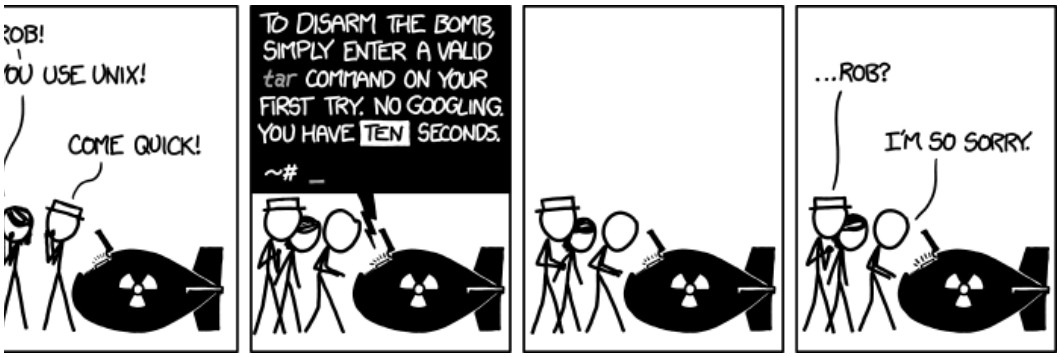
→ Uses public/private Key exchange

→ Allows for key based authentication

→ Installed by default on all linux/UNIX systems

---

## che (httpd) - Setting up a Web Server (ch. 26)




### jectives

- Explain purpose of Apache
- Configure Apache to provide simple content
- Customize Apache settings
- Set up redirects so users can publish content from home directory
- Configure virtual hosts

---

### ro to Apache

Is a module based web server

This expands Apache's base configuration

↳ enables it to render languages

- PHP
- Python

- PERL
  ↳ Called Mod-*  mod_perl  mod_python  mod_ssl

figuration

Sudo yum install system-config-httpd

eb

Documents

Apache

~~http.apache.org/docs/2.4~~

nes

Apache + httpd are used interchagibly in Fedora

- Apache server works by launching Apache processes to handle incoming requests
- By default web pages and content are served out of /var/www/html
- The problem is these files are owned by root
  ↳ You may not want to give everyone sudo permission
  ↳ Create a "second group", give that group access to /var/www/html
  ↳ add users to that group

ation

sudo yum groupinstall "Web Server" or sudo yum install httpd

- sudo systemctl enable httpd.service

httpd.

→ sudo systemctl s service

sudo yum install php

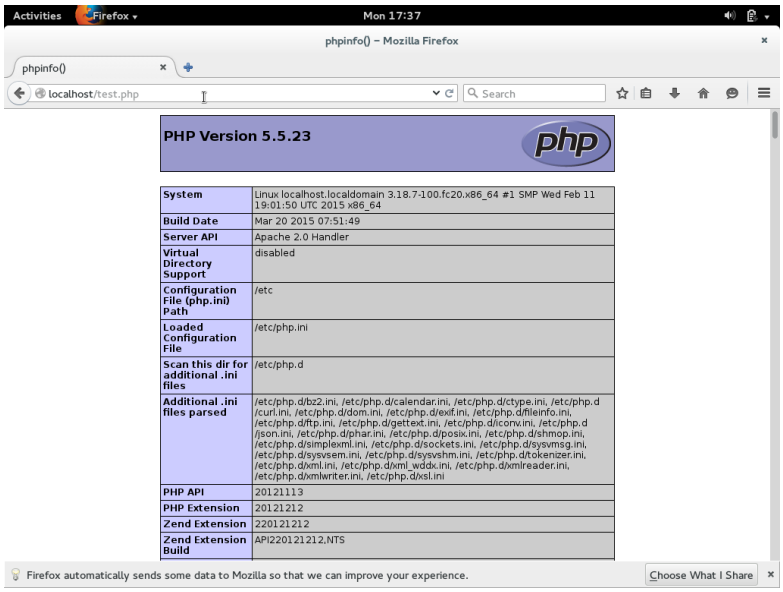
↳ restart web server service

use vi to create a file named test.php in the /var/www/html directory

↳ Add these contents...

```
<?php
phpinfo();
?>
```

↳ save the file and open a web browser in your virtual machine




ing - to see if it is working open a browser & point to http://localhost - what do you see?

conf files red in /etc/httpd/conf/httpd.conf

ctl can be used to start and stop apache too

/var/log/httpd/access_log
/var/log/httpd/error_log

---

---

404, 410, 502, 504, 200
these
to know values

---

is the most common webserver (IIS + Nginx coming)

modules for extending capabilities