LIS-5364

Networking and the Shell

Telnet

- Talking to a computer online, typing.

  (in the clear)

SSH (Secure SHell)

- Encrypted (Keys, Passwords, or both)
- Now, the de facto standard, and applies to a lot of ideas (but mostly 2 and a half)
- 1) The actual shell
- 2) A “Tunnel” through which to pipe ANYTHING securely
- 2.5) FTP replacement

SSH (Secure SHell)

Standard way to connect from one computer to another.

```
ssh username@iporhostname.com
```

Important options:

-p Port (security through obscurity)

-X X forwarding

-L tunnel creation

Tunnel what?

- Anything that could go through the 'net.
  - File Transfers
- - VNC
- - “Skype”
- - Web connection/Proxy

SCP (Secure Copy)

Works very similarly to cp, you need only add the remote host (and other ssh type options)

```
scp username@host.com:/home/user/file
/home/username/stuff
```

Note: Nautilus and other filemanagers have this built in for GUI use.

SSH (Secure SHell)

You can set these to work

WITHOUT PASSWORDS.

And it’s SAFER. Whoa.

(you have to exchange keys..a quick detour)

Is that like a VPN?

<deep breath> yes. The phrase lately means two related, but different things:

1) Virtual Private Network.
Just as it sounds. Imagine a set of networked computers, but spread out across the internet. Traffic is encrypted and tunneled so it's as if all the computers are together in an enclosed place.

Is that like a VPN?

They could all access the net independently – or you could FORCE all traffic through a central location, for reasons.

..like monitoring – or

2) to OBSCURE the source for anonymity. This is usually what is meant by that service you buy. Really, they should just call these what they are: “proxies”

“ Servers” and such

- Ispace?

Shell Network Tools

Ifconfig (ip?) – display/modify network interfaces

- Find local ip
- Use local interfaces

iwconfig – display/modify WIRELESS interfaces

- turn wireless interfaces on/off
- change mode of card (Managed v Master, etc)

(use “sudo iwlist scan” to find local APs)

Other Network Tools

Ping – holler at an ip address/hostname

host – find out more host info

netstat – print most all network info

iptables – routing/firewall

traceroute – trace the route!

Netstat

nc

IP Addresses

IP address – unique 4 part number over the internet; but..

Subnets/Intranets (like the one you have at home with your wireless router) have special numbers:

127.0.0.1 – home

192.168.*.* - "local (possibly VPN)"

10.*.*.* – "local or VPN"

Also, for local - hostnames – less reliable, but useful if you do them right, once, and your network is closed.

less /etc/hostname

A little on ports

Ports are to IP addresses, roughly, what extensions are to telephone numbers.

Well known defaults (often not specified)

21 – FTP

22 – SSH

80 – Web/HTTP

443 – Web/HTTPS

8080 – other web stuff

5900 - VNC

6888+ - Bittorrent

655 – VPN

BUT – you can usually redefine these however you want, depending.

A little on ports

Ifconfig vs. whatismyip.com will give you different addresses.

The LATTER is the ip address to the “world”

Use NAT / Port Forwarding to get to the “right” computer.
(Remember, your router is just another computer, it ALSO has an IP)

Usually, have entries like the following:

SERVICE NAME	STARTPORT	ENDPORT	IP ADDRESS
HTTP	80	80	192.168.1.4
bittorrent	6888	6888	192.168.1.8
faceblaster7	7777	7777	192.168.1.20

Testing servers:

Curl

Wget

Links

w3m