Linux Networking

...

DNS Resolution

/etc/hosts

- List of hosts/IPs

/etc/resolv.conf

- Name server settings

/etc/nsswitch.conf

- Determines DNS settings

/etc/hosts

```
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts

::1 ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

ff02::3 ip6-allhosts

127.0.0.1 ubuntu
```

/etc/resolv.conf

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)

#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN

nameserver 10.50.255.254

search openstacklocal
```

/etc/nsswitch.conf

passwd: compat

...entries...

hosts: files mdns4_minimal [NOTFOUND=return] dns

networks: files

protocols: db files

services: db files

ethers: db files

rpc: db files

netgroup: nis

Use for Netgroups (1)

```
# hosts.allow

portmap:ALL

ALL:192.168.2.,192.168.3.,.linuxlaboratory.org EXCEPT

badhost.linuxlaboratory.org, opus, willy


# hosts.deny

ALL:ALL
```

Use for Netgroups (2)

#/etc/netgroup > goodhosts (opus,-,)(willy,-,)(cartman,-,)(stan,-,)(chef,-,)

#

hosts.allow

ALL: @goodhosts,192.168.2.,192.168.3.

Packets

http://beej.us/guide/bgnet/html/multi/theory.html#twotypes

Sockets

“...a two-way communications pipe, which can be used to communicate in a wide variety of *domains*.”

-Act like two-way FIFOs

-Communication takes place through sockets interface instead of file interface

-Linux sockets are a special file in the file system

http://beej.us/guide/bgipc/html/multi/unixsock.html#unixsockover

Regular Sockets

Protocol stack processes its respective layer, performing address, checksum (if applicable) validation, removes its respective header and trailer (if applicable) and passes up the contents to its immediate upper layer

Raw Sockets

No layer checking done, it is up to the application using the raw socket to interpret the data. RAW sockets are often used as packet capture/sniffer programs as it captures the “raw” data from the network interface card and passes it directly to the application

Must have root privileges

Inter Process Communication

Processes use sockets to communicate between one another

-Server/Client

-Socket Pair

Network Sockets

A network socket is an internal endpoint for sending or receiving data at a single node in a computer network.

Sockets with BASH

Demo

Further reading:

https://techblog.sethleedy.name/?p=24280

Networked Services

ntpd – Network Time Protocol Daemon

httpd (apache) – Hyper Text Transfer Protocol Daemon

sshd – Secure SHell Daemon

postfix, sendmail – Mail Server Daemon

snmpd – Simple Network Management Protocol Daemon

iptables, nftables, ufw – Network Filtering Protocol Service

nfsd – Network File System Server Daemon

dnsmasq, nscd – Name Service Cache Daemon

named (bind)– Dynamic Naming Service Server Daemon

smbd (samba) – Server Message Block Server Daemon

Network Super Servers

Listen for network connection on behalf of another program

Hands off control of that connection to intended server

Help reduce memory load and improve security

Servers that normally use super server: telnet, FTP, TFTP, rlogin, finger, POP, IMAP

inetd/xinetd:

inetd - older super server w/o built-in security

xinetd - newer super server w/ built-in security

Further Reading:
http://unixadminschool.com/blog/2011/07/inetd-vs-xinetd-in-linux/

xinetd

Configuration file: /etc/xinetd.conf

Listen to only one network interface for the service:

bind = <IP Address>

Accept connections only from IP addresses:

only_from = <IP Addresses|Network>

Deny connections only from IP addresses:

no_access = <IP Addresses|Network>

Set times during which users may access the server:

access_times = hour:min-hour:min

If access is prohibited, send optional banner to client:

banner = /usr/local/etc/deny_banner

Pros and Cons of xinetd

Pros:

Conserves resources

Runs daemons only when needed

Provides an additional layer of security and can turn virtually any script or program into a service

Cons:

Can be used to create a backdoor listener

xinetd backdoor

Demo

Network Services

Demos:

- host
- dig
- nslookup

Gather Network Information

Demo:

- **netstat**
- **lsof**
- **ip**
- **ifconfig**
- **arp**

Enumerate Network Services

Demo:

- **telnet**
- **netcat**
- **nmap**

Samba

Allows Windows file and printer sharing on Linux

/etc/samba/smb.conf

Pros and Cons of Samba

Pros:

- Free

- Uses CIFS - public version of SMB protocol

Cons:

- Difficult to configure properly

- Generally seen as vulnerable due to complexities of Windows<>Linux sharing