Using tcpwrappers to save your system (and your bacon)

Dillon Pyron

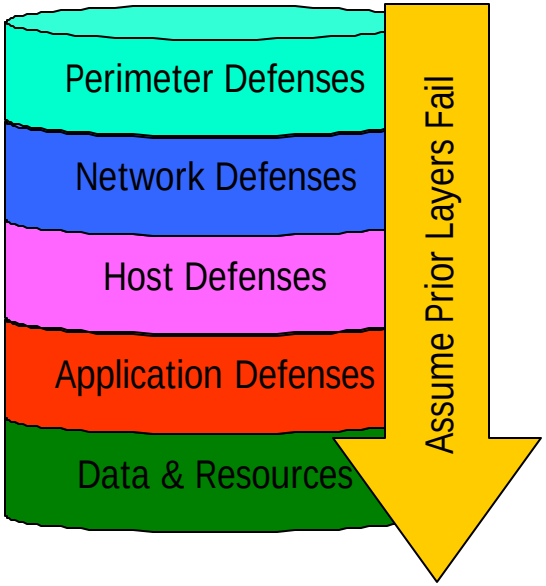
NETSerenity, Inc.

dillon@netserenity.net

InterWorks 2002
THE HP TECHNICAL TRAINING CONFERENCE

Intrusion Detection Basics

- Defense in depth



Perimeter

- Firewalls
- Routers (with ACL's)
- Perimeter IDS
  - Snort
  - ISS Real Secure
  - Network Flight Recorder
  - Cisco SecureIDS

Network

- Routers (with ACL's)
- Network IDS
  - Same players
- Effective subnetwork isolation

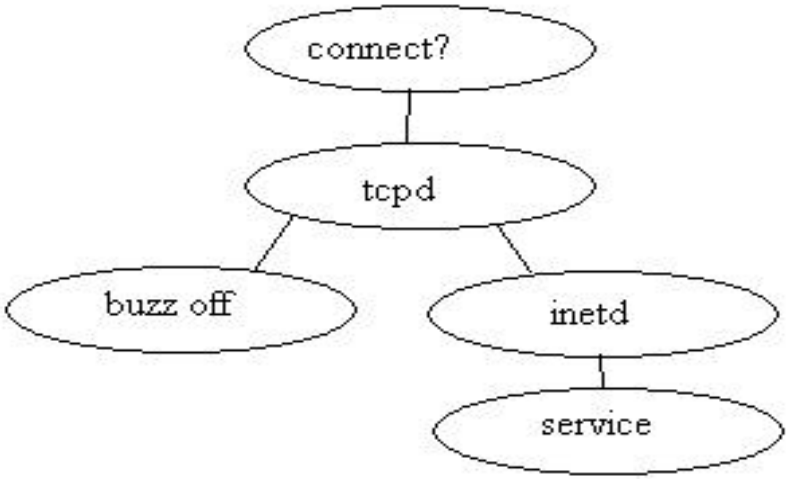
Host

- Tripwire
- IDS
  - ISS RealSecure
  - NFR
  - Cybercop
- Tcpwrappers

Tcpwrappers

- 10 years old!!!!
- Open Source!!!
- Already available with many *nix

How it works-the pictures



How it works

- Intercepts connection requests inside inetd
- Checks simple ruleset for permission/action
- Either starts the service or takes other actions

Mods to inetd.conf

- Replace service name with call to tcpd

```
ftp … /usr/sbin/tcpd ftpd
```

- tcpd replaces ftpd
- Determines who can use ftp
- Fires off the service when appropriate

hosts.allow & hosts.deny

- hosts.allow is read first and overrides hosts.deny
- Format is `service:hostname(s):action`
- The keyword ALL is used for both services and hostnames

Example files

- The hosts.allow file

```
in.telnetd: .pyron.org: ALLOW
```

- While the hosts.deny file is

```
in.telnetd: ALL: DENY
```

- This allows anyone in the pyron.org network to access telnet and blocks all others.

inetd.sec and HP-UX

- HP provides a simplified version with HP-UX
- Uses a single file /usr/adm/inetd.sec
- Format is `service action host(s)`
- In the example above

```
in.telnetd allow .pyron.org
```

Where do I use tcpwrappers?

- Any critical system
  - Firewalls
  - Web, ftp and mail servers
  - Your own machine!!!

Questions