It's Ten O'Clock; Do You Know Who's Connecting to Your Machine?

Dave Barr

barr@pop.psu.edu

Systems Administrator
Population Research Institute
The Pennsylvania State University

Agenda

- Overview
- The “tcp_wrapper”
- The RFC931 identification protocol
- The “Big Picture”
- Review and questions

Overview

- Basic services of TCP/IP

- Existing logging methods

  1. `last` — `/etc/wtmp`, login accounting

  2. process accounting — `lastcomm`

- The `inetd` service —
  `/etc/services` and `/etc/inetd.conf`

Overview, cont'd.

- Limitations of basic UNIX networking dæmons
  1. world–accessable
  2. not usually modifiable without source code

- Possible Solutions
  1. Individual modifications of every daemon
  2. `inetd`

The "tcp wrapper"

- Benefits of this approach

  1. Portability

  2. Flexibility

- Limitations

  - Only processes spawned from `inetd`

  - Notable exceptions:

    1. `sendmail`

    2. NIS services

    3. `portmap`

    4. NFS

Getting log_tcp

- Where?
  - ftp.win.tue.nl:/pub/security/log_tcp*.Z
  - ftp.uu.net:/pub/security/log_tcp*.Z
  - bug fix for multi-homed hosts:
    ftp.pop.psu.edu:/pub/log_tcp.4.2-psu.tar.Z

Installation

1. `log_tcp`
   - The `Makefile`
   - `log_tcp.h`
2. `/etc/inetd.conf`
3. `/etc/services`
4. `syslog` facility

Installation Cont'd

- Optional Features

  1. RFC931 support. "See below"
  2. hosts_access control. "See below"

- `hosts.deny` and `hosts.allow` files

  - additional logging
  - reverse fingering
  - unknown hosts

The RFC931 Identification protocol

- Where can I get it?

- Mechanism

  1. How the dæmon works

  2. The information it returns

  3. security issues

RFC931, cont'd.

- 931, IDENT, TAP

- Integration with existing clients and servers

  1. tcp_wrapper logs and hosts_access file

  2. wuarchive's `ftpd`

  3. IDA `sendmail`

The “Big Picture”

- What does this gain?

  1. collective security

  2. tracking of crackers

- What’s still out there?

  1. The “K” word

  2. common sense practices

Review and Questions