# Packet Inhaling with Tcpdump

Sniffing Network Traffic at
Lightning Speed

Jeff Muse
February 9, 2005

# Warning!

- Use tcpdump only if the owner of the network grants permission to do so!
- There may be legal consequences for using tcpdump or other sniffers without authorization.

# Uses of Tcpdump

- Watch or store network traffic
- Troubleshooting
- Study higher level protocols

# Getting Tcpdump

- Comes with most Linux/BSDs
- Compiles on most other versions of Unix
- http://www.tcpdump.org
- Libpcap is required to build from source.

# Parameters

- -i Interface
- -vv Verbose output
- -e Ethernet headers
- -s Size of capture
- -n Disable name resolution
- -r Read pcap file
- -X Ascii dump
- -w Write to pcap file

# Examples

- tcpdump -i eth0 -vv -n
- tcpdump -i eth0 -vv -lenX -s 1600
- tcpdump -i eth0 -vv -w dump.out
- tcpdump -r *file* -vv -lenX -s 1600 | less

# Berkeley Packet Filter (BPF)

- host
- net
- protocol
- and/or
- not

# BPF examples

- tcpdump *options* host 192.168.1.1
- tcpdump *options* icmp
- tcpdump *options* host 192.168.1.1 and icmp
- tcpdump *options* host 192.168.1.1 or 192.168.1.2 and port 22