

Network Tool Lab

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 2 September 19th, 2005

ifconfig

- network setup
- MAC address
- IP Address
- Network Address
- ipconfig in Windows

ping

- Internet **C**ontrol **M**essage **P**rotocol (**ICMP**) - Layer 1
- Ping - Packet Internet Groper
- ICMP echo request and echo reply
- Tests: packet dropping, latency, DNS
- ping -f — flood
- ping -n — no dns
- ping -s (packet size) — large packets used in Denial Of Service

traceroute

- Pings host with loop 1 to n ping TTL n
- Get information about where servers are physically located and ISP
- tracert in Windows

dig

- DNS lookup
- `dig -x` — reverse lookup
- `dig (domain name) AXFR` — domain transfer

whois

- Contact information for website from registrars
- When want to contact about some security problem
- keep information limited in your own whois

finger

- individual information
- usually not available

ps

- Shows processes running on a system
- Check if something is running that shouldn't be
- `ps A` — all user processes
- `ps -aux` — with username
- `ps -aux | grep (searchterm)` — search for a particular program

Sam Spade

- Windows equivalent of the basic Unix network tools