Nmap

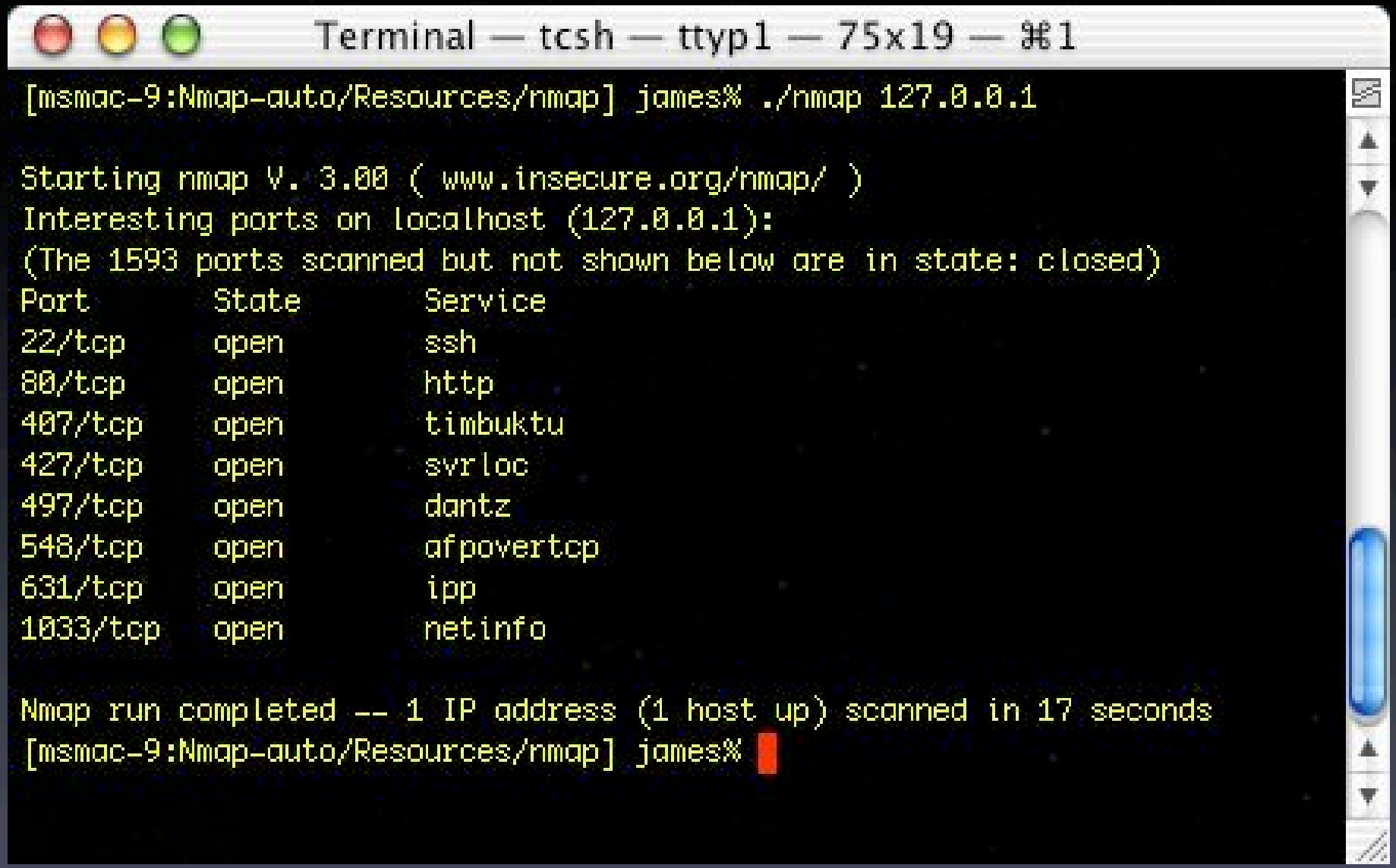
The University of Utah
Student Computing Labs
Macintosh Support
mac@scl.utah.edu

Nmap

- “Network Mapper”
- Free & Open source
- Command line utility
- Scans ports
- Lastest version 3.48
- Written by “Fyodor”

Nmap

- Nmap can determine
  - What hosts are on the network
  - Services running on host
    - Version too
  - The OS and version of the host
  - Type of packet filters/firewalls exist


Terminal — tcsh — ttyp1 — 75x19 — ⌘1
[msmac-9:Nmap-auto/Resources/nmap] james% ./nmap 127.0.0.1
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on localhost (127.0.0.1):
(The 1593 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
80/tcp open http
407/tcp open timbuktu
427/tcp open svrloc
497/tcp open dantz
548/tcp open afpovertcp
631/tcp open ipp
1033/tcp open netinfo
Nmap run completed -- 1 IP address (1 host up) scanned in 17 seconds
[msmac-9:Nmap-auto/Resources/nmap] james%

Nmap

- 3 states
  - Open
    - Port responds to requests
  - Closed
    - Port responds “closed”
  - Filtered
    - No response - firewalled

Nmap

- Some nmap scan options
  - -sS (TCP SYN steal port scan)
  - -sU (UDP port scan)
  - -p 1-65535 (all ports)
  - -v (Verbose, recommended)
  - -oN or -oX or -oG <*logfilename*>

Nmap

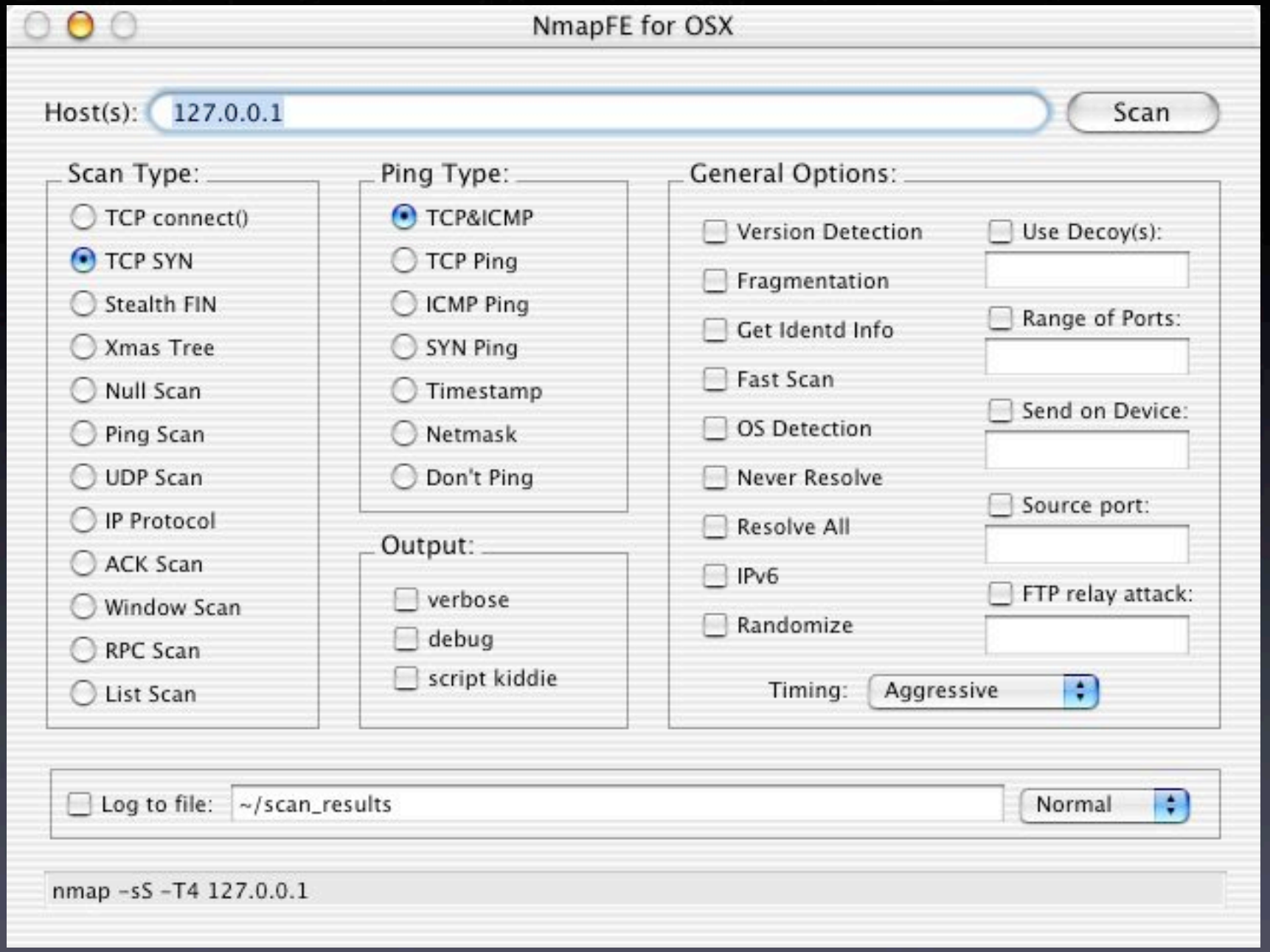
- What port is what?
  - There are several web pages that explain ports, notably:
    - Apple's Knowledge base #106439
    - macosxhints.com
    - www.iana.org (Internet Assigned Numbers Authority)

Nmap

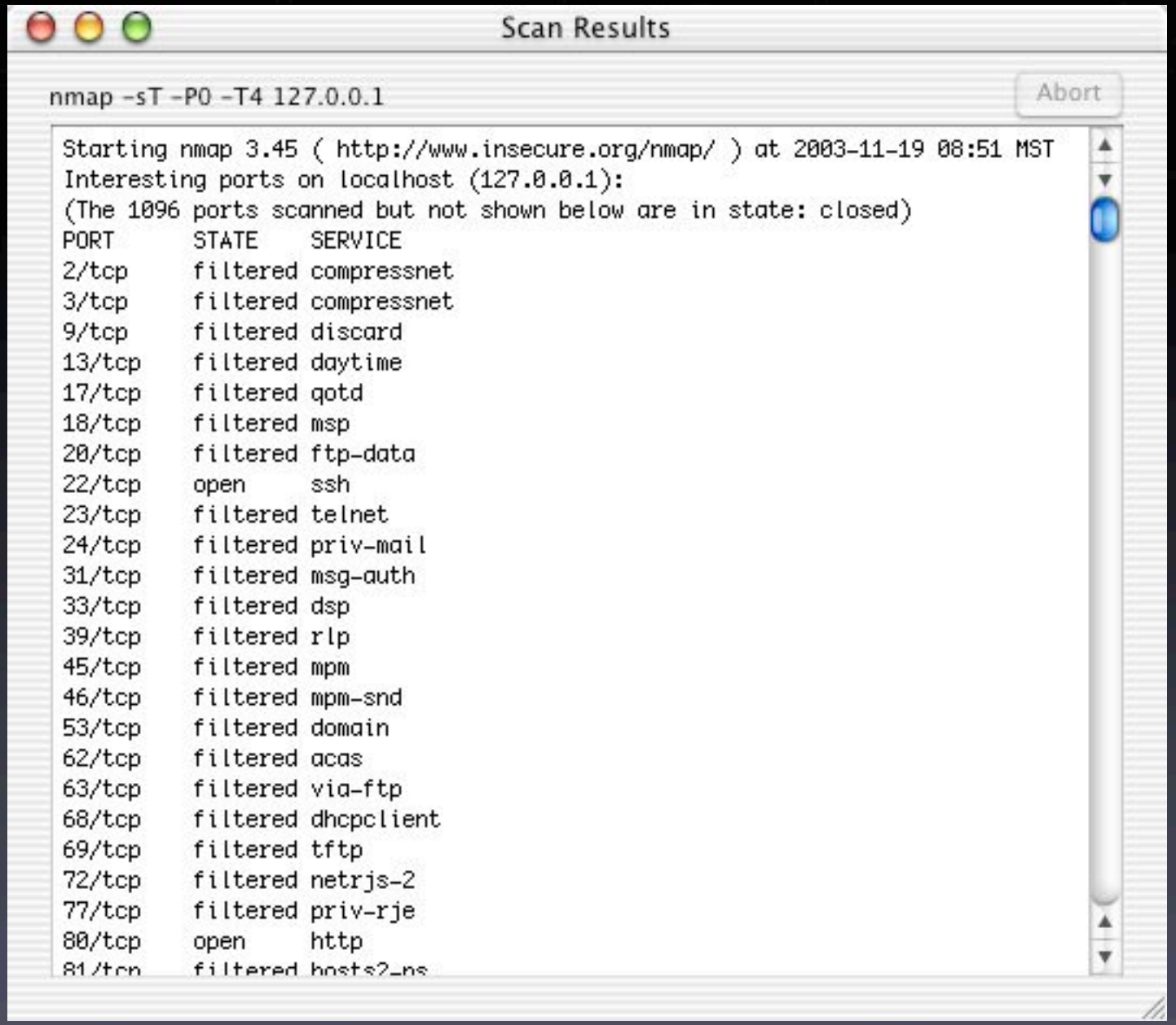
- Open ports that shouldn’t be there
  - Use common sense forensics
    - Double check that it isn’t legit
      - ps, tcpdump, & netstat
    - Turn off computer
    - Contact ISO ASAP

NmapFE

- Cocoa front end for Nmap
- Lastest version is .80
- Includes Nmap 3.45
- Written by Matthew Rothenberg
- Easiest way to get Nmap binary



The University of Utah Student Computing Labs


Scan Results
nmap -sT -P0 -T4 127.0.0.1
Abort
Starting nmap 3.45 (http://www.insecure.org/nmap/) at 2003-11-19 08:51 MST
Interesting ports on localhost (127.0.0.1):
(The 1096 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
2/tcp filtered compressnet
3/tcp filtered compressnet
9/tcp filtered discard
13/tcp filtered daytime
17/tcp filtered qotd
18/tcp filtered msp
20/tcp filtered ftp-data
22/tcp open ssh
23/tcp filtered telnet
24/tcp filtered priv-mail
31/tcp filtered msg-auth
33/tcp filtered dsp
39/tcp filtered rlp
45/tcp filtered mpm
46/tcp filtered mpm-snd
53/tcp filtered domain
62/tcp filtered acas
63/tcp filtered via-ftp
68/tcp filtered dhcpclient
69/tcp filtered tftp
72/tcp filtered netrjs-2
77/tcp filtered priv-rje
80/tcp open http

Automating Nmap

- Create a text file with all IP's to scan
- sudo ./nmap -iL <*filename*>
- This will get all IP's to scan from file

Automating Nmap

- Nmap-audit
  - Perl script
  - Written by Keith Resar
  - Version 1.66

Automating Nmap

- Nmap-auto
  - Our solution
    - A little simpler than nmap-audit
  - Perl script
  - Mac OS X StartupItem