Nmap basics

Maniac

Nmap Basics - Overview

- What is nmap?
  - Nmap, short for "network mapper", is an open source utility which can quickly scan broad ranges of devices and provide valuable information about the devices on your network. It can be used for IT auditing and asset discovery as well as for security profiling of the network.

Nmap Basics - Overview

- What does nmap do?
  - Nmap uses raw IP packets to determine what hosts are available on the network, the services that are enabled, the operating system and version of the host, what sort of firewall or packet filters are in place and many other aspects of the network. The information can be used both proactively to identify and correct security holes and by attackers to perform reconnaissance about the types and quantities of targets available and what weaknesses exist.

Nmap Basics - Overview

- Nmap runs on?
  - Nmap is available for a wide range of operating system platforms. The standard download is a compressed file containing the UNIX version (which runs on Linux, Solaris, Free/Net/OpenBSD, and Mac OS X) and the Windows version as well as NmapFE, the X-Windows front end for UNIX, and NmapWIN, the recommended Windows GUI for Nmap.

Nmap Basics - Overview

Nmap can perform a wide range of scans. Some are more aggressive and blatant, while some are designed to be stealthy and scan undetected. Depending on the type of scan performed, different information can be discovered as well.

Nmap Basics - Overview

Some of the scan types are:

Connect	SYN Stealth
FIN, Xmas, Null	Ping
UDP Scan	IP Protocol Scan
ACK Scan	Window Scan
RPC Scan	List Scan
FTP Bounce	

Nmap Basics - First Scan

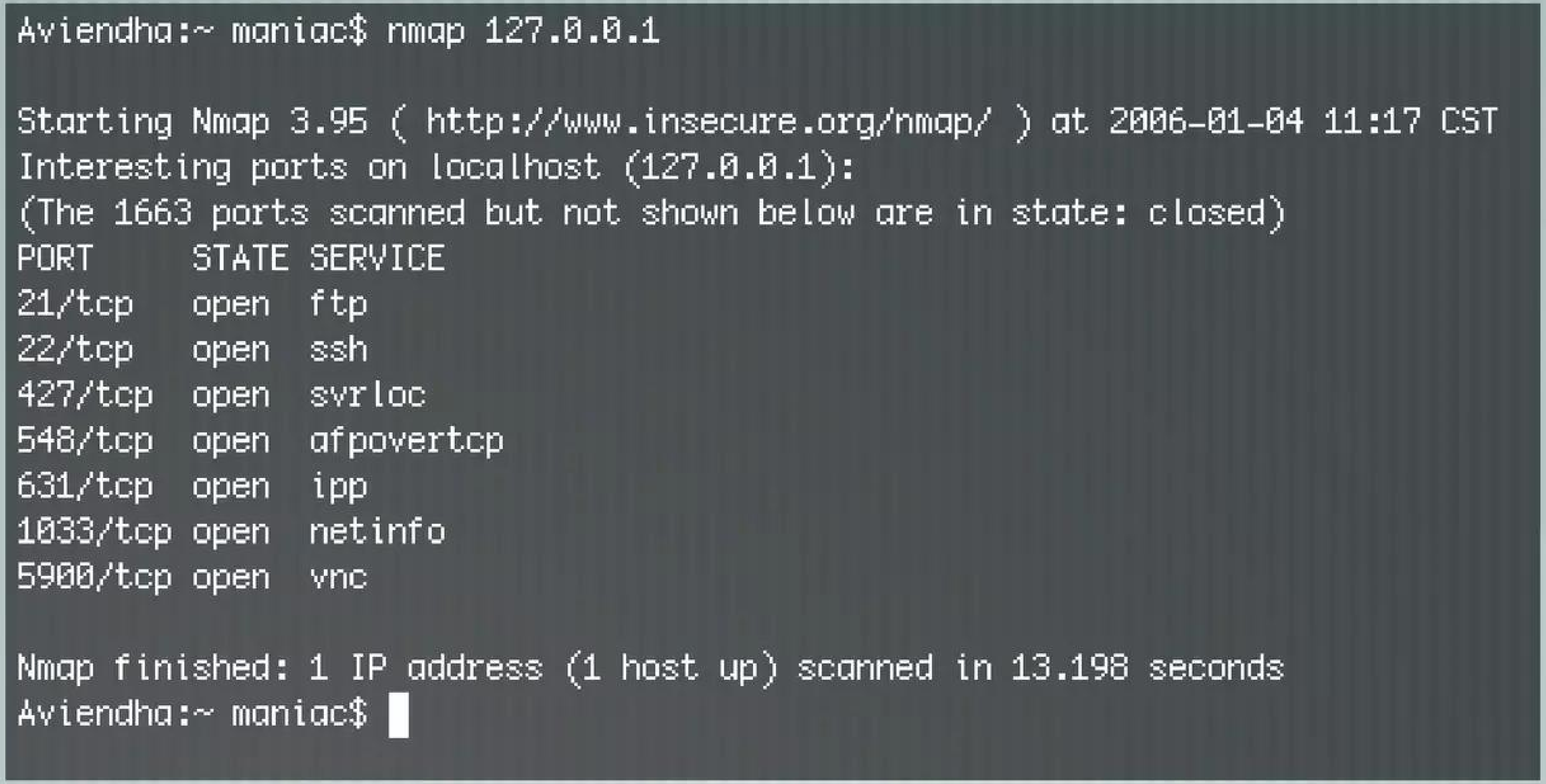
- How hard is nmap to use?
  - Nmap’s ability to be run from both the command line and from a GUI enable most people to get the tool up and running very quickly. Advanced features require more command line and technical expertise to use the tool effectively.

Nmap Basics - First Scan

- Windows users take heed:
  - Windows XP Service Pack 2 is shoddily supported due to the fact that Microsoft removed the socket layer from the Operating System. Furthermore, hacks and workarounds that have been discovered to get nmap to work results in Microsoft patching up this hole shortly thereafter. With this in note, your mileage may vary.

Nmap Basics - First Scan

- Basic nmap scan example.

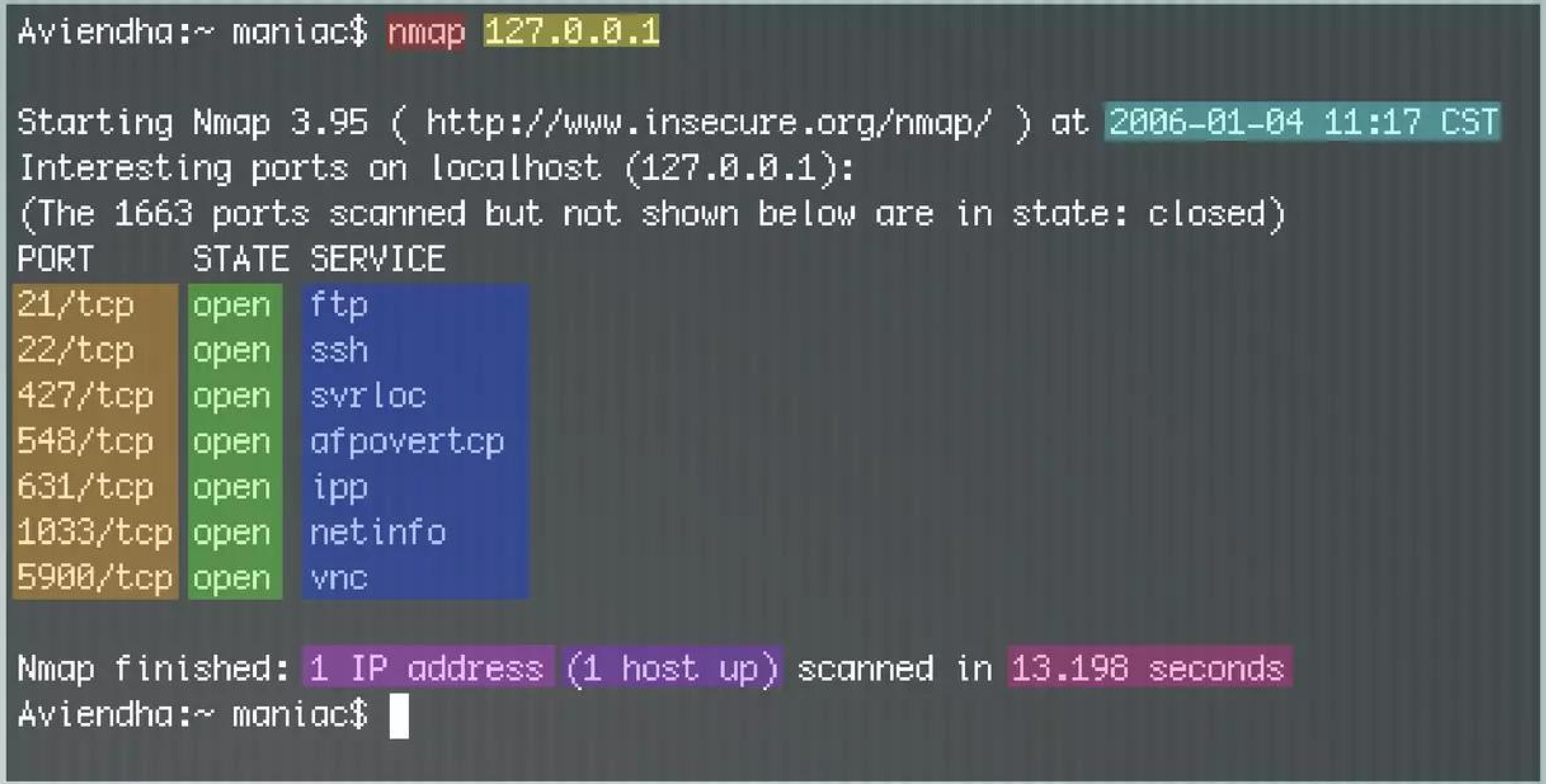


```
Aviendha:~ maniac$ nmap 127.0.0.1

Starting Nmap 3.95 ( http://www.insecure.org/nmap/ ) at 2006-01-04 11:17 CST
Interesting ports on localhost (127.0.0.1):
(The 1663 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
427/tcp  open  svrloc
548/tcp  open  afpovertcp
631/tcp  open  ipp
1033/tcp open  netinfo
5900/tcp open  vnc

Nmap finished: 1 IP address (1 host up) scanned in 13.198 seconds
Aviendha:~ maniac$ █
```

Nmap Basics - First Scan



```
Aviendha:~ maniac$ nmap 127.0.0.1

Starting Nmap 3.95 ( http://www.insecure.org/nmap/ ) at 2006-01-04 11:17 CST
Interesting ports on localhost (127.0.0.1):
(The 1663 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
427/tcp  open  svrloc
548/tcp  open  afpovertcp
631/tcp  open  ipp
1033/tcp open  netinfo
5900/tcp open  vnc

Nmap finished: 1 IP address (1 host up) scanned in 13.198 seconds
Aviendha:~ maniac$
```

- Application
- IP Addresses scanned
- Time and date of the scan
- Ports discovered
- State of the port
- The type of service this port typically is
- Total number of IP Addresses scanned
- IP addresses found to be active
- Number of seconds to complete the scan

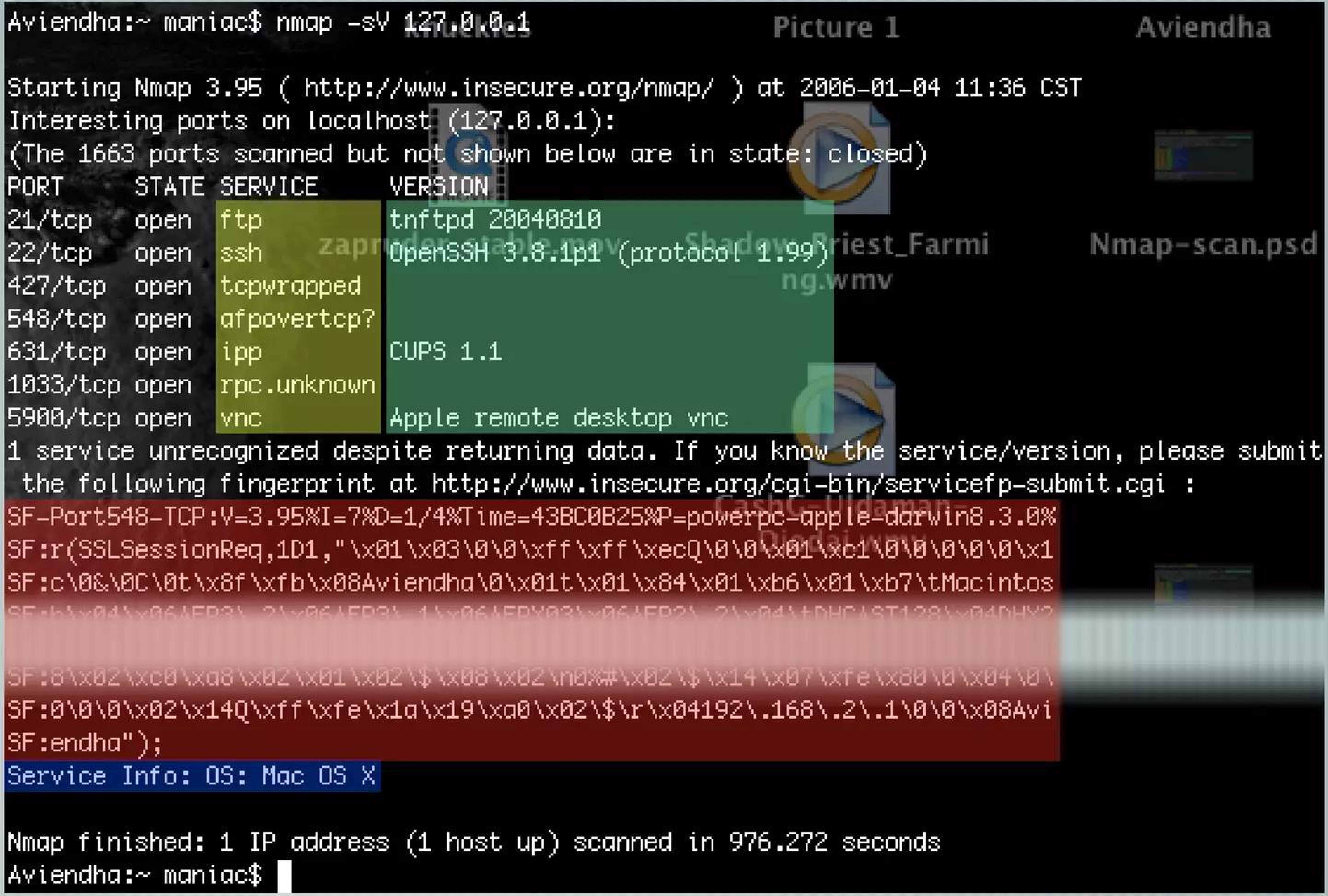
Nmap Basics - Version Detection

- What is host detection?
  - Host detection is a feature of nmap that tells it to further analyze what the packet behavior is, and assess what Operating System the target host is based on it's analysis.
- Ok, well what about version detection then?
  - Version detection expands on host detection by also querying the ports nmap finds open for what the service is.

Nmap Basics - Version Detection

- Example output from the version detection flag.

- Service Info
- Service Version
- Unknown Fingerprint
- Unknown Service Identifier



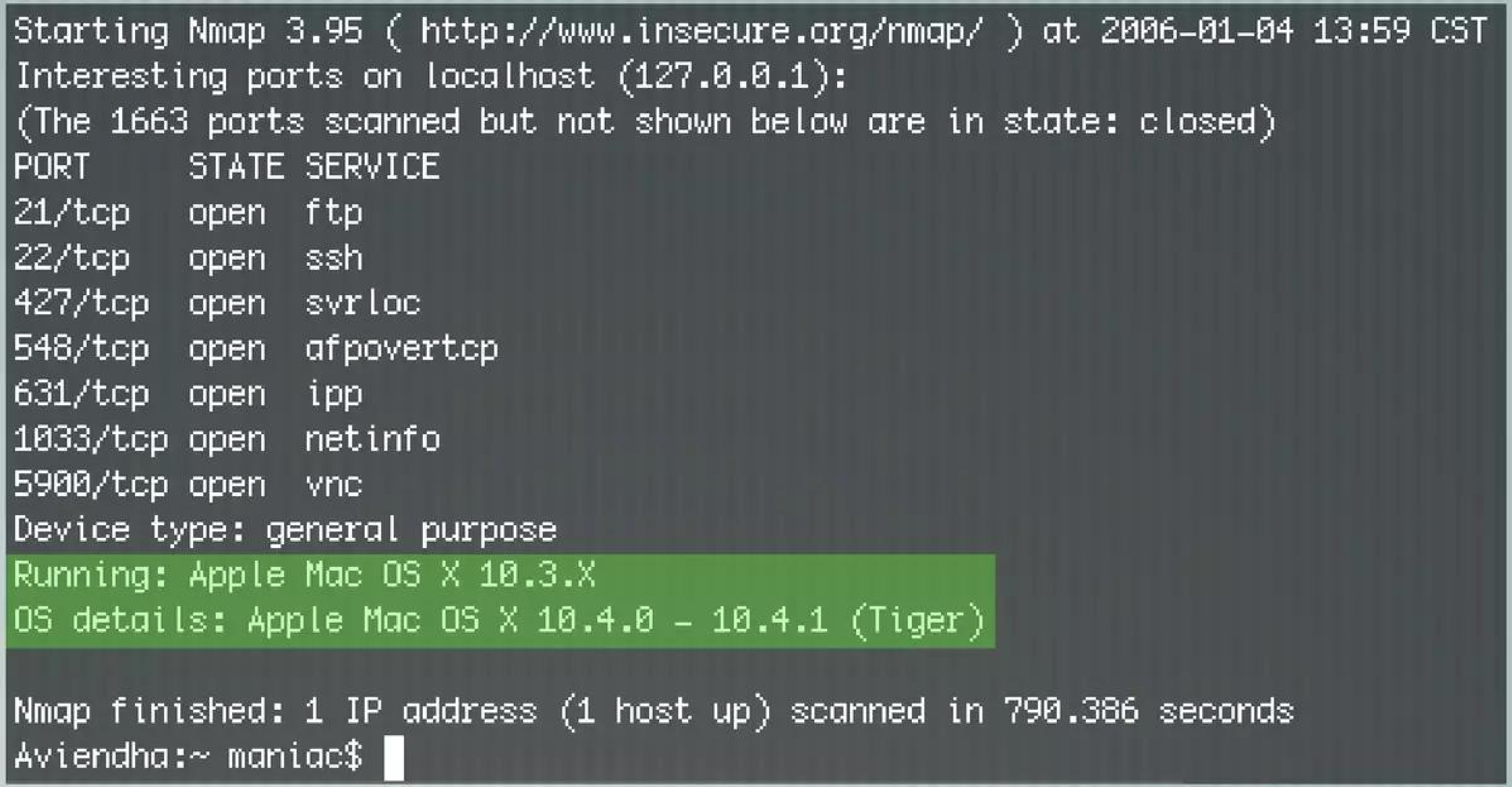
```
Aviendha:~ maniac$ nmap -sV 127.0.0.1

Starting Nmap 3.95 ( http://www.insecure.org/nmap/ ) at 2006-01-04 11:36 CST
Interesting ports on localhost (127.0.0.1):
(The 1663 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         tnftpd 20040810
22/tcp   open  ssh         OpenSSH 3.8.1p1 (protocol 1.99)
427/tcp  open  tcpwrapped
548/tcp  open  afpovertcp?
631/tcp  open  ipp         CUPS 1.1
1033/tcp open  rpc.unknown
5900/tcp open  vnc         Apple remote desktop vnc
1 service unrecognized despite returning data. If you know the service/version, please submit
 the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port548-TCP:V=3.95%I=7%D=1/4%Time=43BC0B25%P=powerpc-apple-darwin8.3.0%
SF:r(SSLSessionReq,1D1,"\x01\x03\0\0\xff\xff\xecQ\0\0\x01\xc1\0\0\0\0\0\x1
SF:c\0&\0C\0t\x8f\xfb\x08Aviendha\0\x01t\x01\x84\x01\xb6\x01\xb7\tMacintos
SF:h\x04\x06AFP3\.2\x06AFP3\.1\x06AFPX03\x06AFP2\.2\x04\tDHCAST128\x04DHX2
[illegible]
SF:8\x02\xc0\xa8\x02\x01\x02\$\x08\x02\n0%#\x02\$\x14\x07\xfe\x80\0\x04\0\
SF:0\0\0\x02\x14Q\xff\xfe\x1a\x19\xa0\x02\$\r\x04192\.168\.2\.1\0\0\x08Avi
SF:endha");
Service Info: OS: Mac OS X

Nmap finished: 1 IP address (1 host up) scanned in 976.272 seconds
Aviendha:~ maniac$
```

Nmap Basics - Version Detection

- Example of host detection.
  - Operating System Information



```
Starting Nmap 3.95 ( http://www.insecure.org/nmap/ ) at 2006-01-04 13:59 CST
Interesting ports on localhost (127.0.0.1):
(The 1663 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
427/tcp  open  svrloc
548/tcp  open  afpovertcp
631/tcp  open  ipp
1033/tcp open  netinfo
5900/tcp open  vnc
Device type: general purpose
Running: Apple Mac OS X 10.3.X
OS details: Apple Mac OS X 10.4.0 - 10.4.1 (Tiger)

Nmap finished: 1 IP address (1 host up) scanned in 790.386 seconds
Aviendha:~ maniac$
```

Nmap Basics - Pinging

- How does nmap identify hosts?
  - Nmap by default will perform either a TCP SYN or a TCP Connect ping to gather active hosts. In some cases nmap will even use ARP pinging to identify hosts as well.
- How can you turn off pinging?
  - The -P0 (P<zero>) switch will turn this feature off.

Nmap Basics

- This concludes “Hacking With Nmap, Part 1”

Nmap Basics

- Information Gathered from:
  - Insecurity.org - The home of Nmap
  - Netsecurity.about.com - Providers of the much of the Overview material.