

Sonar

Ryan Du Bois

What is Sonar, Potential Applications, Basic Networking, Plugin Framework, Bugs, ToDo List

Summary

- History
- Basic Network Primer
- Plugins and Plugin API
- Bugs / ToDo
- Contact Info

What is Sonar?

- Security Scanner
- Plugin Based
- Extendable

History

- Original Version
 - Windows Version
 - Replacement for Ping
 - Automated Program Execution
 - 469 Lines
- Current Version
 - Linux/POSIX Version
 - Replacement for nmap
 - Plugin Based
 - Automated Program Execution
 - 3907 Lines (sonar)
 - 3540 Lines (plugins)
 - 7447 Lines Total

History

- Student by day
- Hacker by night
 - Not enough sleep
- Wrote sonar to hack during the day while at school
 - Automated Execution
 - Delay time



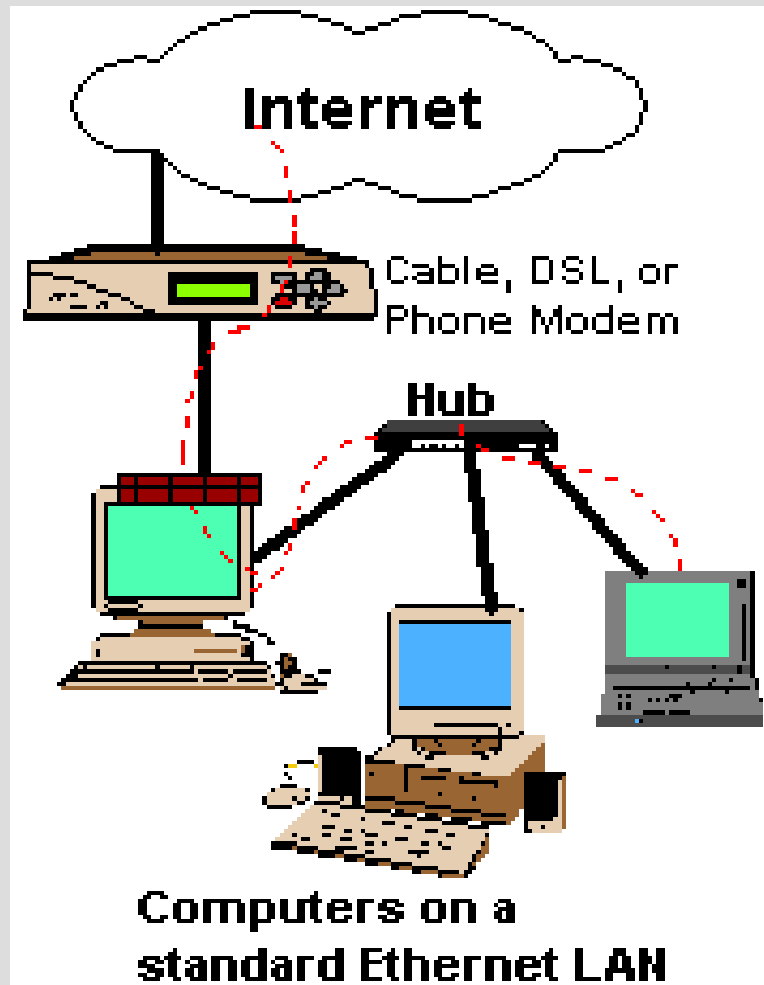
Long-term Goals

- Provide a pluggable replacement to nmap
 - Automated Program Execution
 - Plugins for Input, Output, and Scan-types
 - Continued, Regular Development

Strengths and Advantages

- Completely Customizable
 - Input format
 - Output format
 - Scan types
- Extendable
 - Any one can write plugins
- Open Source

Networks



- TCP/IP Protocols
- Interconnected
- Clients/Servers
- Hostnames mapped to an IP Address
- Shared Packets

TCP/IP Protocol

- IP Protocol Header <netinet/ip.h>
 - Stores source and destination
 - Total Packet Length, Version
 - Protocol Number for next header
 - Checksum
 - TCP Protocol Header <netinet/tcp.h>
 - Source and Destination Port Number
 - Sequence and ACK numbers
 - Flags (SYN, ACK, PUSH, etc.)
 - Checksum
 - Data Offset

Who's Who?

- How do you know who you are connected to?
- Reconnaissance
 - Services
 - OS Fingerprinting
 - DNS Names
 - Geographical Location
 - Round Trip Time
 - Route

Potential Applications

- Port-scanning
 - Services
 - Type of computer (Client, server, or both?)
- OS Fingerprinting
 - What operating system
 - Vulnerabilities
- Automated Penetration Testing
 - Corporate Networks
 - Universities
 - Home LANs

Why Plugins?

- Advantages
 - Updates
 - Easier
 - Specific
 - Functionality
 - Ease of Extension
 - Development
 - Focused
 - Bug Hunting
 - Narrows the search

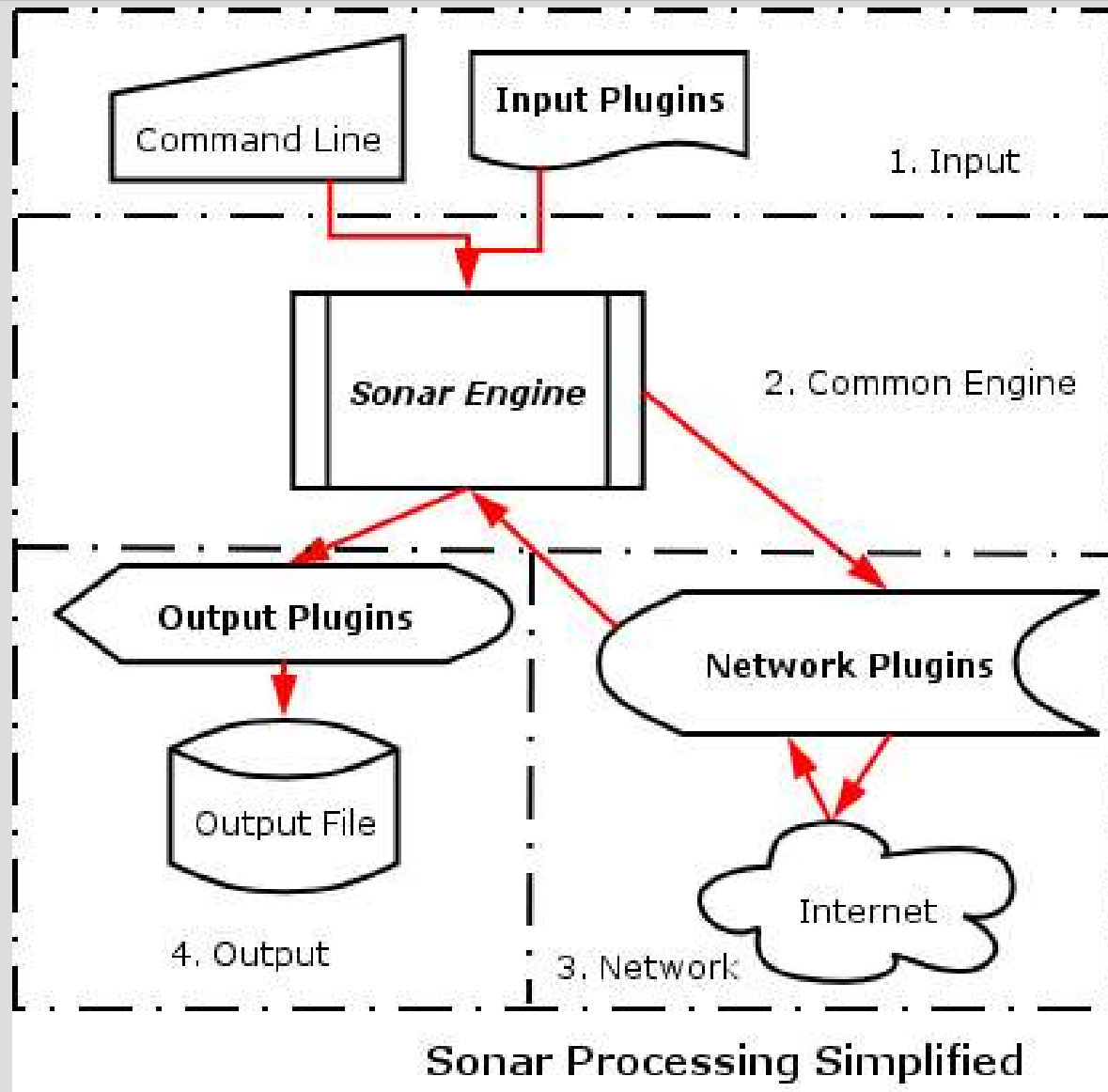
Why Plugins?

- Disadvantages
 - Complexity
 - Plugin API
 - Engine
 - Bugs
 - Engine bugs propagate to plugins
 - Extending the API
 - Backwards Compatibility
 - Forwards Compatibility

Plugin API

- Early versions
 - Network plugins only
 - Based on Xine code (yes, the movie player)
 - Weak Error Handling
 - Non-Parallel
- Later Versions
 - Support for Input and Output Plugins
 - Parallelized

Plugin API



Plugin API

- Input Plugins
 - Problems
 - Buffer Size
 - Number of Hosts
 - Return Hostname to Sonar

Plugin API

- Sonar Engine
 - Targeting
 - Addresses
 - Ports
 - DNS Resolution
 - Repetition
 - Command Line Options
 - Timing

Plugin API

- Network Plugins
 - Problems
 - IPv4/IPv6 Interoperability
 - Parallelism
 - Targeting
 - Outputting Results
 - Targeting
 - Handled by Sonar Engine
 - Threads

Plugin API

- Output Plugins
 - Problems
 - Results
 - Each Network scan has different result formats
 - Output File Selection
 - Results Output
 - Two Functions
 - Regular Output
 - Standard Result Format

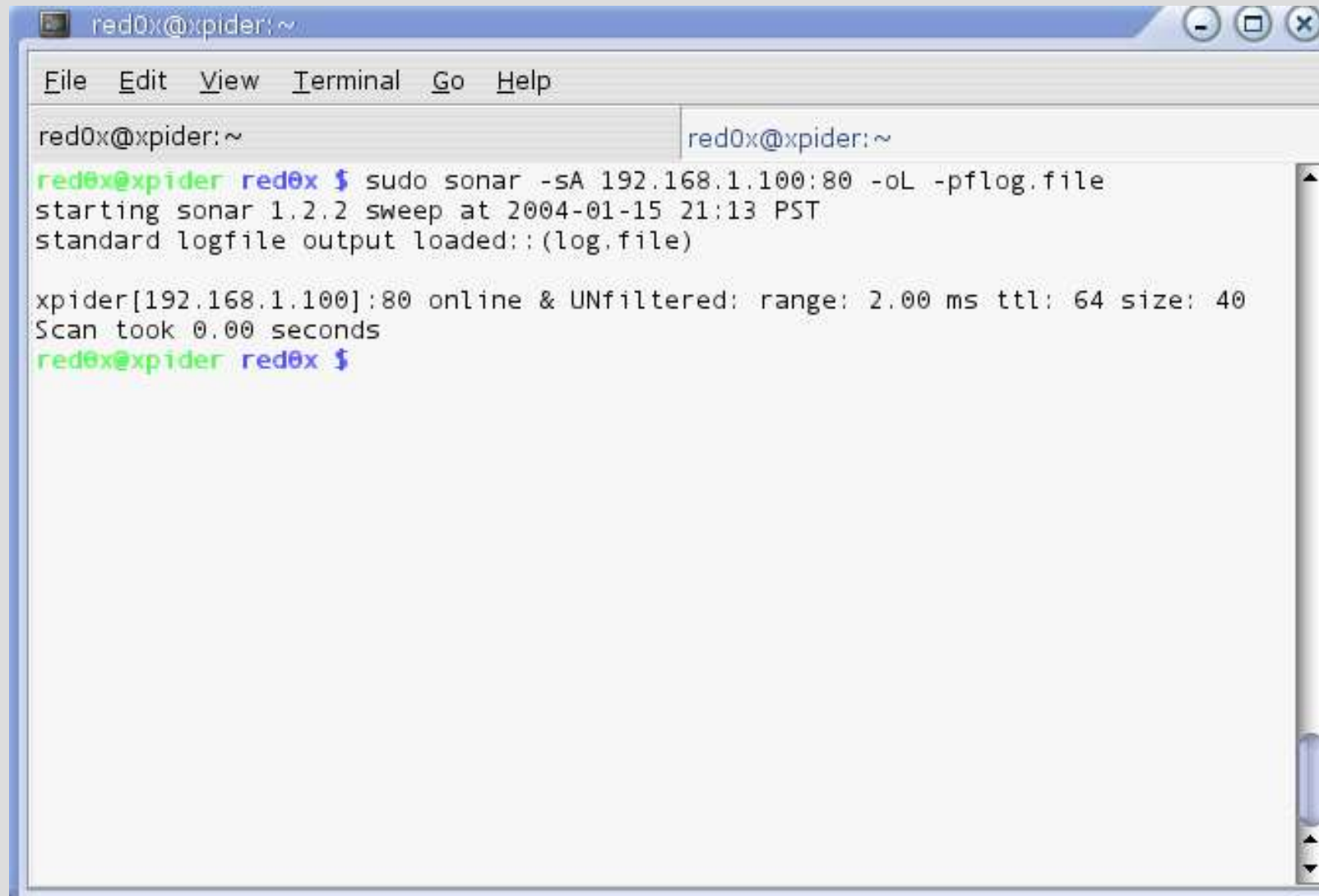
Bugs

- Parallelism
 - Running Multiple Scan Types
- Program Execution
- Statistics
 - Counting Sent Packets
- Only Two Network Plugins

ToDo List

- Fix Parallelism
- Implement More Scan Type
- Fix Statistics
- Error Handling and Reporting
- OS X Testing
- GUI

Example



```
red0x@xpider:~  
File Edit View Terminal Go Help  
red0x@xpider:~ red0x@xpider:~  
red0x@xpider red0x $ sudo sonar -sA 192.168.1.100:80 -oL -pflog.file  
starting sonar 1.2.2 sweep at 2004-01-15 21:13 PST  
standard logfile output loaded:;(log.file)  
  
xpider[192.168.1.100]:80 online & UNfiltered: range: 2.00 ms ttl: 64 size: 40  
Scan took 0.00 seconds  
red0x@xpider red0x $
```

Conclusion

- Lessons Learned
 - Plan for the Long Haul
 - Application Extensions
 - Backwards Compatibility
 - Start with Clean Code
 - Starting from Windows Code == BAD!
 - Plugins
 - Very Complex
 - Hard to get right on the first try
 - This was my first try ;-)

Conclusion

- Development
 - CVS is key!
 - Allows you to backtrack
 - Allows multiple people to edit the same code
 - Open Source
 - Anyone may contribute
 - Finding Help is Difficult

Links And Info

- <http://autosec.sourceforge.net>
- Bugs:
<http://autosec.sourceforge.net/helpDesk/index.htm>
- Ryan Du Bois
 - red0x@users.sourceforge.net
 - IRC: irc.freenode.net, #cplug, #autosec
- Project Status and Gnatt Chart
 - <http://ryand.hopto.org/~red0x/proj.html>