Network Forensics

John Wills
Overview

- Network forensics
  - Proactive
  - Reactive
- Collection
- Tools
- Analysis
- Countermeasures
Reactive

- Preserving compromised machine
- Recovering from an intrusion
- Examine evidence
Proactive

- Prevent being compromised
- Examine data on the fly
- Gain information
- Employ means to stop an attacker
  - Countermeasures
Collection

- Network traffic
- System memory
- State table
- Log files
- Drive Image
Reactive Tools

- Ethereal and TCPDump
- Utility CD
- Memdump
- Netstat
- Netcat
Ethereal and TCPDump

- Ethereal and TEthereal
  - GTK interface
  - High packet format detection
  - TCP sequence reconstruction
- TCPDump
  - Command-line interface
  - Nearly identical features
- LibPCAP
Utility CD

- Preserving evidence is key
- Use memdump to copy state of system
  - Push it over the network using netcat

SystemA# nc -l -p 12000 > sysb-memdump

SystemB# memdump | nc SystemA 12000
Netstat

- Observe state table connections
- Capture information

SystemA# nc -l -p 12001 > sysb-netstat

SystemB# netstat -nt | nc SystemA 12001
Analysis

- Whois
- Abuse database
- Traceroute
Proactive Tools

- Network monitors
- Intrusion Detection Systems
  - Pattern matching
  - Anomaly-Based
- PortSentury
- State Defense
State Defense

- BSD TCP/UDP state table monitoring
  - Logs inbound connections
- Ncurses interface
- Ability to kill connections/logins
  - Correlates data with log files
- Logs traffic via LibPCAP
- Firewall related reactive measures
Countermeasures

- Contact provider to report abuse
- Reverse DoS
- Employ firewall rules to block/filter
  - Bandwidth consumption
  - Too many/false connections
  - Failed logins
  - Decoy scans