

Real World Intrusion Detection

Mark K. Mellis

Consultant

SystemExperts Corporation

What We'll Talk About

- ◆ Why Intrusion Detection?
- ◆ ID and the Organization
- ◆ Types of Intrusion Detection
- ◆ Where to Deploy
- ◆ How to Deploy
- ◆ Summary

Acronyms and Disclaimers

- ◆ **Intrusion Detection = ID**
- ◆ **Product Names are not Product Recommendations**
 - I've used a scant handful of the ID products available today
 - YMMV

Questions

- ◆ Do you use Intrusion Detection now?

Questions

- ◆ Do you have IP connectivity to business partners?

Questions

- ◆ Have you automated your log processing?

Why ID?

- ◆ More Sophisticated Opponents
- ◆ More Complex Systems
- ◆ More Protocols Through the Firewall
- ◆ More Connected Business Partners

Why ID?

- ◆ ID provides compensating controls, offsetting some of the risk of modern-day Internet connectivity
- ◆ ID helps sysadmins sleep at night

ID and the Organization

◆ Policy

- Management's way to communicate their will to those who carry out the organization's mission
- How may you protect the company?
 - how to evaluate and how to respond
- Who can assume the risk?
 - the level of management that can make the call to take down the site
- What are you protecting?
 - where to focus efforts

ID and the Organization

- Privacy Issues
 - network monitoring may require advance notification
 - especially sensitive in educational institutions

ID and the Organization

◆ Architecture

- Design for ID
 - liason with other groups and functions
 - ID infrastructure
- What's Next?
 - Tools
 - Attacks

ID and the Organization

◆ Implementation

- Firewalls
- IDS
- Host Security

ID and the Organization

◆ Operations

- Detection
- Classification
- Response
- Maintenance

ID and the Organization

◆ Training

- Knowledge
 - mailing lists
 - reading list
 - conferences
 - tutorials
- Practical Factors
 - using your tools
- Team Training
 - scenario based
 - include decision makers

Types of Intrusion Detection

- ◆ Network
- ◆ Host
- ◆ Application
- ◆ Analysis

Types of ID - Network

- ◆ "Smart Sniffers"
- ◆ Some record traffic for subsequent analysis
- ◆ Some analyze traffic in real time
- ◆ A few can dynamically reconfigure a firewall or filtering router to block an "attack"

Types of ID - Network

- ◆ These tools look for attack signatures
- ◆ The vendors of the commercial tools supply updated signatures on a more-or-less frequent basis
- ◆ Users may add signatures, too
 - Usually a proprietary language involved
- ◆ Most use a distributed model
 - sensor(s)
 - analysis console

Types of ID - Network

- ◆ They are non-trivial to set up and non-trivial to support
- ◆ You get what you pay for, whether the currency is cash, sweat or both
- ◆ NT is where most new commercial development is taking place

Types of ID - Host

◆ Instrumentation

- tripwire
- klaxon
- tcpwrappers
- commercial tools

◆ Authentication Events

- Successes
- Failures

◆ Reboots

Types of ID - Host

◆ Routers are Hosts, Too

- They can syslog
- Authentication events
- Access list "hits"
- Reboots

Types of ID - Host

- ◆ OS Auditing
 - AIX, HP/UX, NT, Solaris have it
 - Vary in tunability
- ◆ “Drowning in data”

Types of ID - Application

- ◆ Web application runs in DMZ
- ◆ Speaks SQL to database on the secure net
- ◆ Since DB queries are generated by (presumably) bug-free code, SQL errors may indicate “someone” performing ad hoc queries
- ◆ Probably not what you wanted
- ◆ Scan your database (and web server) logs

Types of ID - Analysis

- ◆ Many events are logged, but few events are “chosen”
- ◆ The shoemaker’s children go barefoot

Types of ID - Analysis

◆ Centralized Logging

- use syslog
 - block inbound traffic on udp port 514 on external router to thwart DOS
 - secure and reliable syslog replacements emerging
- use other protocols
 - NT event logging
 - SNMP events
- big log server
 - RAID
 - be careful with access
 - need offline storage - WORM is best

Types of ID - Analysis

- ◆ **Simple Reports (dust off your Camel book)**
 - top ten logins
 - logins on accounts idle more than three weeks
 - all su events
 - reboots
 - router reconfigs
 - SUID files added and deleted

Types of ID - Analysis

◆ Event Correlation

- clocks must be synchronized
 - NTP
- log normalization
 - syslogs tend to be free format
 - in order to correlate events, times, addresses, ports need to be represented in uniform manner
 - probably need a separate routine per data source
 - commercial tools may help
- databases for large sites

Where to Deploy

- ◆ In Areas Where Traffic is Concentrated
- ◆ In Areas Where Traffic is Particularly Sensitive
- ◆ Consistent with Hardware Constraints

Where to Deploy

- ◆ **In Areas Where Traffic is Concentrated**
 - choke points
 - adjacent to access routers
 - adjacent to firewalls

Where to Deploy

- ◆ **In Areas Where Traffic is Particularly Sensitive**
 - inside protected networks
 - in front of credit card processing systems
 - next to the HR database or the finance system
 - in business partner DMZs
 - all exposed machines should have host Intrusion Detection installed
 - all infrastructure machines should have host ID installed

Where to Deploy

◆ Consistent with Hardware Constraints

- today's higher bandwidth networks make our work harder
- switches and VLANs make it next to impossible
- SPAN ports on switches help
- some routers have ID agents built in
- you don't usually need to see all the traffic to match on a signature
- design your networks to be monitored

How to Deploy

- ◆ One step at a time
- ◆ Even the most humble beginnings will pay dividends
- ◆ Expect to spend at least a month fixing misconfigured systems
- ◆ Ultimately, it's not a project, it's a process

What We Talked About

- ◆ Why Intrusion Detection?
- ◆ ID and the Organization
- ◆ Types of Intrusion Detection
- ◆ Where to Deploy
- ◆ How to Deploy
- ◆ Summary

Freeware Resources

- ◆ **Bro**
 - <http://www.aciri.org/vern/bro-info.html>
- ◆ **The COAST Archive**
 - <ftp://coast.cs.purdue.edu/pub/tools/unix>
 - home of swatch, klaxon, Tripwire, tcp_wrappers, and a host of other tools

Freeware Resources

- ◆ **Logsurfer**
 - <http://www.cert.dfn.de/eng/logsurf>
- ◆ **The SHADOW Project**
 - <http://www.nswc.navy.mil/ISSEC/CID>

Commercial Resources

- ◆ **BackOfficer Friendly**
 - <http://www.nfr.com/products/bof>
- ◆ **Cisco Secure IDS (formerly NetRanger)**
 - <http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/index.shtml>

Commercial Resources

- ◆ **ISS RealSecure**
 - <http://solutions.iss.net/products/rsecure/rs.php>
- ◆ ***Network Intrusion Detection***
 - Subtitle: *An Analyst's Handbook*
 - by Stephen Northcutt
 - New Riders Publishing 1999

Commercial Resources

- ◆ **NAI CyberCop**
 - http://www.nai.com/asp_set/products/tns/cybercop_intrusion.asp
- ◆ **Network Flight Recorder**
 - <http://www.nfr.com/products/technology.html>
- ◆ **Tripwire (commercial version)**
 - <http://www.tripwiresecurity.com>

Many Thanks To...

- ◆ **Tina Darmohray**
 - for encouraging me to share what I learned
- ◆ **Christine Hogan**
 - for being the voice of sanity
- ◆ **Brad Johnson and Dick Mackey**
 - for showing me how to do systematic log analysis and the usefulness of application logging
- ◆ **Jason Reed**
 - for explaining how *really* big networks do ID

Mark K. Mellis
Consultant

Mark.Mellis@SystemExperts.com
<http://www.SystemExperts.com>

757 Londonderry Drive
Sunnyvale, California 94087
+1 408 733 6054 (direct)