Real World Intrusion Detection: First Steps

Mark K. Mellis, *Consultant*

SystemExperts Corporation

What We'll Talk About

- Small to Medium Sized Sites
- Freeware Tools
- Philosophy

What We'll Talk About

- Where to Deploy
- What 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

- Have you automated your log processing?

Small to Medium Size Sites

- Big sites have big problems:
  - they start at thousands of authentications per hour
  - and hundreds of megabytes (or more) of network traffic per hour
- Although principles are the same, tools are different
- The budget is probably different, too
- We'll address smaller sites here today

Philosophy

- **Why ID?**
  - More Sophisticated Opponents
  - More Complex Systems
  - More Protocols Through the Firewall
  - More Connected Business Partners
  - Defense in Depth

Philosophy

- You're cheap
  - You'd like to do things economically
- You're talented
  - You can use FTP and can type `'make'`
- You're busy
  - You don't have a dedicated security group; ID is a part time job
  - No time for software development projects

Philosophy

- Freeware tools where it makes sense
- Preference for Open Source
- Log and Ignore door-knob rattling (but…)
- When a real threat occurs, you want to know!

Philosophy

- **Speaking of wanting to know...**
  - Config changes on systems
  - Authentication failures
  - Attempts to learn about your site
  - Attempts to access your services

What to Deploy

- Central Logging
- syslog
  - UDP
  - ubiquitous
- nsyslogd
  - `http://coombs.anu.edu.au/~avalon/nsyslog.html`
  - TCP connections and encryption

What to Deploy

- SHARP
  - `http://www.csis.gvsu.edu/sharp`
  - paper presented at LISA 2000
  - modular, extensible architecture
  - normalized log format
  - uses nsyslogd
  - I haven't used it but it looks promising

What to Deploy

- log_analysis
  - `http://linux.umbc.edu/~mabzug1/log_analysis.html`
  - provides daily reporting
  - many default patterns - major time saver
  - extensible

What to Deploy

- logsurfer
  - `http://www.cert.dfn.de/eng/logsurf/home.html`
  - provides close-to-real-time notification
  - matches regexp patterns across multiple lines, with timeouts
  - can invoke external programs
  - nasty config language - but worth it
  - can only read one file at a time

What to Deploy

- **xtail**
  - `http://www.unicom.com/sw/xtail/`
  - tail -f of several files, multiplexed onto STDOUT
  - venerable
    - 1989 version available
    - author's favorite use is following uucp logs :-)
  - stick it in front of logsurfer

What to Deploy

- Aide
  - `http//www.cs.tut.fi/~rammer/aide.html`
  - detects configuration changes on Unix hosts
  - open source Tripwire work-alike
  - No cryptographically-signed database
    - run with database on CDROM
- You may prefer commercial Tripwire
  - `http://www.tripwire.com`

What to Deploy

- klaxon
  - `http://www.eng.auburn.edu/users/doug/second.html#Security`
  - monitors for connection attempts on otherwise unused ports

What to Deploy

- scanlogd
  - `http://www.openwall.com/scanlogd/`
  - monitors for TCP port scans
  - no UDP
  - works for both overt and “stealth” scans
  - won’t catch “low and slow”
  - may not identify source of spoofed scans
  - worth it regardless

What to Deploy

- snort
  - `http://www.snort.org/`
  - lightweight network IDS
  - identifies network based exploits
  - promiscuous mode sniffer
  - paper presented at LISA 1999 in Seattle
  - very active ongoing development
  - current version doesn't do packet reassembly
  - set it up to syslog

What to Deploy

- What about Honeypots?

How to Deploy

- **Routers are Hosts, Too**
  - They can syslog
  - authentication events
    - if using TACACS on Cisco gear
  - configuration changes
  - access list “hits”
  - reboots

How to Deploy

- Make sure you capture all authentication events
  - brute force works, and won't you be embarrassed?
  - may need replacements for system utilities, or non-default configs
    - For Solaris, see `http://csclub.stthomas.edu/~bugtraq/1998/msg00700.html`
    - Linux - PAM modules

How to Deploy

- Don’t forget your applications!
- Scan your database and web server logs

How to Deploy

- **Event Correlation**
  - clocks must be synchronized - use NTP
- **Big Log Server**
  - 100 Gig RAID is cheap now

Where to Deploy

- all exposed machines should have host Intrusion Detection installed (or integrated)
  - external web server, firewall, mail server, DNS server
  - routers and switches should syslog
- all infrastructure machines should have host ID installed (or integrated)
  - internal mail servers, DNS servers, authentication servers, log servers, network management stations
  - routers and switches should syslog

Where to Deploy

- **Network IDS - Snort**
  - 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

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

Wrapping Up

- 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

More Freeware Resources

- The COAST Archive
  - `ftp://coast.cs.purdue.edu/pub/tools/unix`
  - home of swatch, klaxon, Tripwire, tcp_wrappers, and a host of other tools
- The SHADOW Project
  - `http://www.nswc.navy.mil/ISSEC/CID`
  - bit-level analysis, for when you have too much time on your hands

Many Thanks To...

- **My Customers**
  - for all those different “learning experiences”
- **My SystemExperts colleagues**
  - for showing me how to do systematic log analysis and the usefulness of application logging

Mark K. Mellis
Consultant

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

1392 E. Elmgrove Drive
Glendora, California 91741
+1 626 852 8639 (direct)