Configuration Management of Unix/Linux/OS X

Rich Casella/Brett Viren

Why

- November 2004
  - OA cyber security audit cites BNL for not having a configuration management program
- August 2005
  - System I consultants advise BNL that configuration management be addressed for all systems on site
- Late 2005/early 2006
  - System I consultants team with Office of Science as advisors how to fix security at DOE facilities
- April 2006 (?)
  - Configuration management is linked to DOE site office granting BNL authority to operate
- May 2006
  - Letter from Ray Orbach (Director, Office of Science) elevates cyber security to same level/effort as safety at all DOE facilities

How

- Center for Internet Security (CIS) based benchmarks
  - http://www.cisecurity.org/
  - BNL configuration baseline settings documented at http://intranet.bnl.gov/cybersecurity/configMgt/CISBenchmarks.asp
- Auditing via Ordo
- Compliance via (TBD)

BNL Configuration Baseline Settings

- Based on CIS benchmarks
- Mostly best-practices
- Some settings depend on class of machine (what service does it provide)
- Exceptions to CIS benchmarks documented

Auditing

- Configuration Management WG discussed possible solutions
  - Freeware/shareware: not much available
  - SLAC Ranger: a bit unwieldy, wasn't a good fit as a framework
  - Best solution for us is to write our own
    - Fit's into our framework
    - Integrates with our databases
    - Easy to maintain/update
    - Large (hopefully), free (except for time) developer base

Ordo

- Novus Ordo Seclorum (Ordo, for short)
  - Latin translation: “New Order of the Ages”
- Collaborative effort
- Perl-based
- Runs as non-root (unprivileged)
- Capable of running on all systems (mostly)
- Self-updating
- Secure (GPG encrypted communications)

Ordo

- Autoloading configuration test functions
  - Provides ability to override default tests for platform/OS dependent code
    - OS fingerprinting
    - Ifconfig data
- Client/Server model
  - Hosts collect data, email results to master
- Independent database back-end
- Lots of work to do

Compliance

- Ordo is not a compliance tool
  - Will never change anything on a machine, only read data
- What will we do for compliance?
  - Redhat Enterprise Network
  - CFEngine
  - Suggestions?
- CFG Mgmt WG

When

- We need to be compliant across the Unix/Linux/OSX domain by 09/01/2006
- This is an aggressive timeline
  - We need to start now
- Next Cyber audit - Nov 2006

Near Future Issues

- BNL Certification & Accreditation documents are being finalized
- Sysadmins need to ensure that their systems are covered by C&A documentation:
  - Baseline configurations in place, audited by Ordo
  - Security controls acceptable and implemented
    Risk assessments and contingency plan docs apply
- Any significant deviations and necessary mitigations must be described in supplementary documentation
- System Owner is responsible for doing this

Links

- http://intranet.bnl.gov/cybersecurity/configMgt/
- http://www.cisecurity.org/
- http://www.nist.gov