Security Automation

April 9, 2010
Security Automation: the challenge

- **“Tower of Babel”**
  - Too much proprietary, incompatible information
  - Costly
  - Error prone
  - Difficult to scale

- **Inefficient**
  - Resources spent on “security hygiene”
    - Vulnerability management
    - Configuration management
    - Patch management
    - Compliance management
Security Automation: the solution

- Standardization:
  - Same Object, Same Name
  - Reporting

- Automation:
  - Efficiency
  - Accuracy
  - Resources re-tasked to harder problems:
    - Incident response
    - Infrastructure enhancement
What are we achieving with Security Automation?

Minimize Effort
• Reducing the time and effort of manual assessment and remediation
• Providing a more comprehensive assessment of system state

Increase Standardization and Interoperability
• Enabling fast and accurate correlation within the enterprise and across organizations/agencies; Reporting
• Shortening decision cycles by rapidly communicating:
  • Requirements (What/How to check)
  • Results (What was found)
• Allowing diverse tool suites and repositories to share data
• Fostering shared situational awareness by enabling and facilitating data sharing, analysis, and aggregation
What are we achieving with Security Automation and Standardization?

Standard data, economy of scale, and reuse
- SCAP security content can be developed once and used by many
- Common definitions for vulnerabilities, software, and policy statements

Speed
- Rapidly identify vulnerabilities and improperly configured systems and communicate the degree of associated risk
  - Zero day malware detection
Partners

- **US Government**
  - National Institute of Standards and Technology (NIST)
  - National Security Agency (NSA)
  - Department of Homeland Security (DHS)
  - Defense Information Systems Agency (DISA)

- **Foreign Government**
  - Japan - **JVN/IPA** - Japan Vulnerability Notes / Information Technology Promotion Agency
  - Spain – **INTECO** - Instituto Nacional de Tecnologías de la Comunicación

- **Private Sector**
  - Apple, Microsoft, Red Hat, Sun Microsystems
  - Security product vendors
NIST SCAP Product Validation Program

http://nvd.nist.gov/scapproducts.cfm
Security Automation Resources
National Vulnerability Database

- NVD is the U.S. government repository of public vulnerability management information.
- Provides standardized reference for software vulnerabilities.
- Over 39,000 CVE entries with the NVD Analysis Team evaluating over 6,000 vulnerabilities a year
- Product dictionary containing 18,000 unique product names
- Used by government, industry and academia
- Machine-readable data feeds
- Spanish and Japanese language translation
- http://nvd.nist.gov
National Checklist Program

U.S. Government repository of publicly available security checklists

- Eases compliance management
- Checklists cover 178 products
  - SCAP content
- Checklist contributors include
  - Government organizations
  - Vendors
  - Non-profit organizations
- Part 39 of the Federal Acquisition Regulation (FAR)
- http://checklists.nist.gov
Content Tools

• eSCAPe
  • Creation of new and/or customized configuration policies
    • Puts the power of SCAP into the hands of existing staff; reduces cost/barrier of entry
    • Government wide, department level, or agency specific
    • Quickly generate specific assessment criteria for vulnerabilities or presence of malware
    • Pushed out to SCAP enabled products

• Content Validation
  • Ensures all content published to NCP is formatted correctly
Looking Ahead

• Remediation capabilities
  – Rapidly deploy corrective action
    • Shutting down services, locking out accounts, etc...

• Network Event Management
  – Event Management Automation Protocol (EMAP)

• Cloud Computing
SCAP Cloud Use Case

• SCAP in the IaaS, PaaS, and SaaS environment
  • Manage the asset inventory, e.g., compute, storage, services, etc.
  • Identify and manage the vulnerabilities and configurations
  • Express security policy and higher level framework compliance
  • Assess the components in the stack

• SCAP across diverse clouds
  • Express security level agreements for dynamic hosted environments
  • Encapsulate dynamic workloads
  • Assess and measure the hosted platforms according to the security requirements
Conclusion

Security Automation:

• Improves efficiency
• Promotes interoperability of data and security tools
• Enables standardized reporting across multiple views
• Provides enhanced situational awareness