Enhancing the FDCC Content

Andrew Buttner

January 24, 2008

MITRE

Origins

- vetted SCAP content published Spring 2007
  - a collection of disjoint content streams
  - available on the SCAP site
  - submitted by different groups
    - vendors
    - government
    - independent personnel
  - limited to no testing behind it
  - starting point for FDCC content
- work to finalize content started November 2007
  - bring cohesion to the content files
    - profile names
    - XCCDF format
    - documentation elements

Organize the Content

- first step was to organize the existing content
  - drop unnecessary rules
  - validate XCCDF -> OVAL mapping
  - references
  - group names
  - file names
- give a consistent feel to the content
  - easier to manage
  - easier to test

Organize the Content (cont.)

- wrote scripts to validate content
  - beyond XCCDF and OVAL validation
    - external variables correct
    - every rule is turned on by a profile
- developed stylesheet to produce spreadsheet
  - generated off content
    - means no “out-of-date” issues

Vendor Testing

- presented content to vendor community
  - to run through their tools
  - more eyes looking at the content
- issues identified and relayed to MITRE
  - fixes included in future drafts

Testing Exercise

- Gunter Air Force Base
  - December 10-12, 2007
  - Montgomery, AL
- Purpose: to exercise content against FDCC images
  - identify problems
  - determine necessary corrections
- Participants
  - government
  - commercial vendors
  - contractors
- Numerous improvements made

By the Numbers

- 729 Total Settings
  - XP = 253
  - XP Firewall = 26
  - Vista = 293
  - Vista Firewall = 35
  - IE 7 = 122

- 713 of these settings (98%) have automated checks
  - XP = 97% (246 of 253)
  - XP Firewall = 100% (26 of 26)
  - Vista = 98% (287 of 293)
  - Vista Firewall = 94% (33 of 35)
  - IE 7 = 99% (121 of 122)

Manual Settings

- some rules (16 total) can not be tested
  - don't know how
  - stated behavior cannot be observed
  - currently unsupported by OVAL
- marked as unknown tests
  - not included in scoring
- questions submitted to OS Vendors
  - vendors are the subject matter experts
  - MITRE and the Govt are looking for help
  - as of today, some questions still unanswered
    - working with Microsoft to address these

Manual Settings (list)

- Vista Firewall
  - IPv6 Block of Protocols 41
  - IPv6 Block of UDP 3544
- IE 7
  - Allow Install On Demand (Internet Explorer)
- XP/Vista
  - Kerberos: Enforce user logon restrictions
  - Kerberos: Maximum lifetime for service ticket
  - Kerberos: Maximum lifetime for user ticket
  - Kerberos: Maximum lifetime for user ticket renewal
  - Kerberos: Maximum tolerance for computer clock synchronization
  - Network access: Allow anonymous SID-Name translation
  - Internet Explorer Maintenance Policy Processing (XP only)

Problems with VHDs

- couple of issues with FDCC images
  - have been identified
    - appropriate people have been notified
  - content is correct
  - need setting on image to be adjusted

- Right To Create Global Objects
  - The OVAL Definition checks for Administrators, Service, Local Service and Network Service be given the rights to create global objects
  - The FDCC image the rights are given to - Administrators, Interactive, Service.
  - OVAL Definition is correct

Ongoing Questions

- still have some questions
  - need help from OS Vendors
  - OS documentation inconsistent
- example
  - disabled and not configured both result in missing reg key

Moving Forward

- version 1.0 was delivered on January 10, 2008
- content is not perfect
  - represents a huge step forward
  - was proved to result in >95% accuracy against FDCC images
  - continue to improve over time
- maintaining list of identified issues
- periodic release of new versions
  - as appropriate