SPAWAR
Systems Center
ATLANTIC

Automated Checking Of Windows User Configuration Settings

Jack Vander Pol

SPAWAR Systems Center ATLANTIC

Topics

- The Automation Gap
- Current Capability
- Our Method
- Proposal
- Example Results
- Discussion
- Implications

The Automation Gap – User Account Configuration

- The number of items currently not automatable in most SCAP validated applications is significant:
  - Any setting defined as part of a User Configuration GPO
    - Microsoft Office
    - Internet Explorer
    - 1453 of 3102 settings in the WindowsServer2008R2andWindows7GroupPolicySettings.xlsx are listed as “User”
    - https://www.microsoft.com/en-us/download/details.aspx?id=25250

SPAWAR Systems Center ATLANTIC

Current Capability

- The current method for checking user settings is via the registry_test, HKEY_CURRENT_USER hive
  - Unfortunately this only reviews the currently logged in user and User Policies can be different for each user.
  - HKCU is not available remotely.

- Due to these issues, much content, such as USGCB has disabled any HKCU tests

SPAWAR Systems Center ATLANTIC

Our Method

- We chose to implement the HKCU method a bit differently
  - HKCU is a pointer to HKUS\<SID> of the user running the software.
  - HKUS\<SID> corresponds to each users NTUser.dat file loaded to the registry when they login.

- Our solution?
  - Read both the logged in user(s) data via HKUS\<SID> and all other previously logged on users via their NTUSER.dat file.
  - This allows current SCAP content to review the user configuration settings for all users who have logged onto the computer.
  - Implemented in SCC 1.1 in 2009

SPAWAR Systems Center ATLANTIC

Proposal: Simplified Overview

1. Determine if any users are currently logged on via HKUS\<SID>
   a) Review any logged in user from the registry
2. Determine the location of User Profiles Directory
3. Read the contents of each ‘real’ user’s NTUser.dat file, excluding any locked files, as they are logged in, and reviewed in step 1a
4. Fail checks for each user profile found to be non-compliant, including the following information
   a) Username
   b) Last Logon
   c) Profile Directory

Example Results – Outlook 2007 (test)

Test ID:oval:mil.ssclant:tst:2501

Result:false

Title:MS Outlook 2007 SP2: Check if HKCU\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail\UnblockSafeZone is set to disabled

Object ID:oval:mil.ssclant:obj:2500

Object Requirements:

- hive must be equal to 'HKEY_CURRENT_USER'
- key must be equal to 'Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail'
- name must be equal to 'UnblockSafeZone'

State ID:oval:mil.ssclant:ste:1

State Requirements:

- type must be equal to 'reg_dword'
- value must be equal to '1'

Example Results – Outlook 2007

Collected Item Properties:

- Info Msg - 'Logon Name: testuser1, Last Logon: Currently Logged On, Profile Directory: C:\Users\testuser1'
- hive equals 'HKEY_CURRENT_USER'
- key equals 'Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail'
- name equals 'UnblockSafeZone'
- type equals 'reg_dword'
- value equals '1'

Collected Item Properties:

- Info Msg - 'Logon Name: TestUser2, Last Logon: 90 days ago, Profile Directory: C:\Users\TestUser2\ntuser.dat'
- hive equals 'HKEY_CURRENT_USER'
- key does not exist

SPAWAR Systems Center ATLANTIC

Discussion: OVAL Updates?

- Update the existing registry_test documentation
  - Explain that HKEY_CURRENT_USER means HKUS\<SID> and all unlocked NTUser.dat files from normal user accounts.
- Update registry_test specification
  - Does not seem to make sense to add specific attributes for HKCU which do not apply to HKLM etc..
- Create a new oval test for NTUser.dat file checking
  - Allows for several additional content driven attributes, such as
    - Local vs domain accounts
    - Last Login
    - Username pattern matching etc…

SPAWAR Systems Center ATLANTIC

Pros and cons: Reuse registry_test

- Pros
  - Existing OVAL 5.3-5.10 content can be used
    - Content from Microsoft Security Compliance Manager
  - Some tools may already support this method along with SCC

- Cons
  - Not nearly as flexible if a subset of profiles is desired
  - Tools will provide differing results until all are updated to support reading NTUser.dat files

SPAWAR Systems Center ATLANTIC

Pros and cons: New Ntuser.dat test

- Pros
  - More granular tests
    - Domain/Local accounts
    - Last Login
  - Consistent results
    - Tools will either support the new oval test or not
- Cons
  - Not available for current OVAL content, likely OVAL 5.11?
  - Any existing HKCU content remains worthless

Discussion Questions

- Is OVAL automation for Windows User Configuration critical?
- If so, which method is preferred?
  - Documentation updates to registry_test in OVAL 5.11?
  - Create new OVAL test in OVAL 5.11?
- Can Info Messages be recommended or required in OVAL results?
  - <oval-sc:message level="info">Logon Name: testuser1, Last Logon: Currently Logged On, Profile Directory: C:\Users\testuser1</oval-sc:message>

SPAWAR Systems Center ATLANTIC

Other Implications

XCCDF

- As with any other oval test which can have multiple results, the details will be lost when rolling up to XCCDF

Multiple Cached Profiles

- A user may have cached profiles on 1-N computers, meaning a potential duplication of results or different results depending on GPO's applied at login.
  - User1 logs into computer1 90 days ago with GPO1 applied to his user.
  - User1 logs into computer2 45 days ago with GPO2 applied to his user.

SPAWAR Systems Center ATLANTIC

Implications Continued

- Do not load each NTUser.dat as a registry hive
  - This can cause locked profiles, preventing users from logging in
  - Instead decode and directly read the NTUser.dat file
- Checks to not pass until ALL accounts are compliant
  - Old and orphaned cached profiles can cause user headaches
    - Recommend that users purge old cached profiles after a fixed number of days
  - Local user cannot be secured with Domain User profiles
    - Example: The local built in administrator account will need to be configured via local GPO's

Thanks

Special Thanks

- National Security Agency
  - Michael Kinney
  - Edward Wienholt
  - Jim Ronayne
- Internal Revenue Service
  - Janice Harrison
  - Denise Crisco
- SPAWAR Systems Center Atlantic
  - Kyle Stone
  - Bryan Wilson

Links

- http://www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx