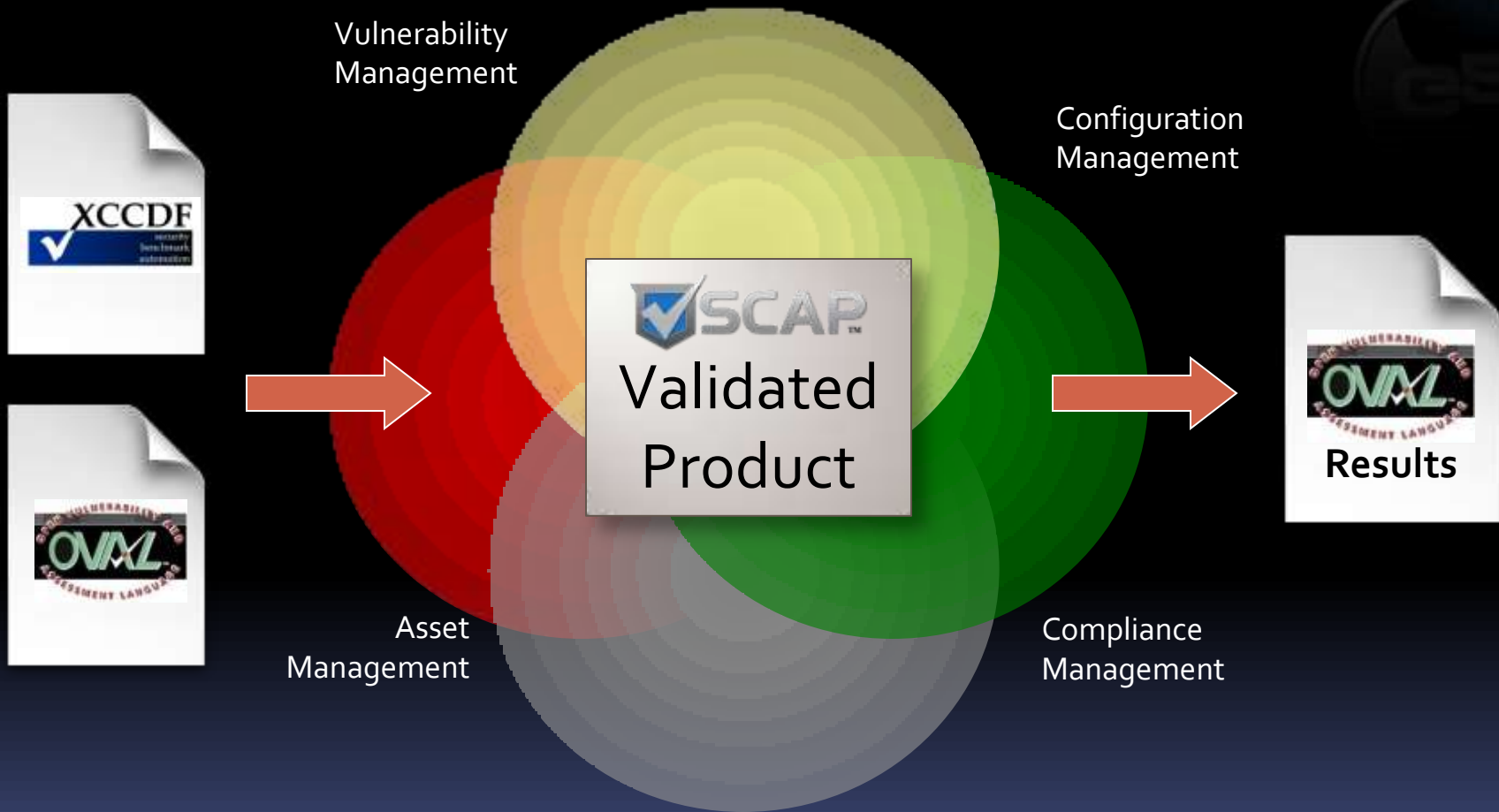


The Enhanced SCAP Editor (eSCAPe) and Libraries





It all depends on SCAP Content



See list of SCAP Validated tools at <http://nvd.nist.gov/scapproducts.cfm>



Manual SCAP Content Creation

- Requires significant understanding of SCAP
 - Protocols
 - Schemas
 - specifications
- Can be error prone
- Time consuming



XCCDF Document Structure

```
<Benchmark id="malware_testing_content">
  <status date="2010-06-09">draft</status>
  <title>Malware Testing Content</title>
  <description>File content for OVAL file malware_file_check-oval.xml
  <platform idref="cpe:/o:microsoft:windows_xp" />
  <version>vo.0</version>
  <Profile id="malware_content_2010">
    <title>Malware Content 2010</title>
    <description>Malware content 2010 description</description>
    <select idref="MAL-49" selected="true" />
  </Profile>
  <Group id="windows_malware_content">
    <title>Windows Malware Content</title>
    <description>Windows Malware Content description</description>
    <Rule id="MAL-49">
      <title>File test for malicious file 34564.exe</title>
      <description>File content that checks C:\WINDOW\temp for file
34564.exe</description>
      <check>
        <check-content-ref href="file_version_check-oval.xml"
name="oval:test.g2.com:def:1" />
      </check>
    </Rule>
  </Group>
</Benchmark>
```





OVAL Document Structure

<definitions>

```
<definition id="oval:test.g2.com:def:1" class="vulnerability">
  <metadata>
    <title>File test for malicious file 34564.exe</title>
    <description>Checking for malicious file named 34564.exe</description>
    <affected family="windows">
      <platform>Microsoft Windows XP</platform>
    </affected></metadata>
    <criteria operator="AND">
      <criterion comment="File test for 34564.exe" test_ref="oval:test.g2.com:tst:1"/></criteria>
    </definition></definitions>
```

<tests>

```
<file_test id="oval:test.g2.com:tst:1" comment="File test for files named 34564.exe">
  <object object_ref="oval:test.g2.com:obj:1"/>
  <state state_ref="oval:test.g2.com:ste:1"/>
</file_test></tests>
```

<objects>

```
<file_object id="oval:test.g2.com:obj:1" comment="Check C:\WINDOW\temp for file">
  <path datatype="string">C:\WINDOW\temp</path>
  <filename datatype="string">34564.exe</filename>
</file_object></objects>
```

<states>

```
<file_state id="oval:test.g2.com:ste:1" comment="Check for file size">
  <size datatype="int" operation="equals">89829</size>
</file_state></states>
```



The Enhanced SCAP Editor (eSCAPe)

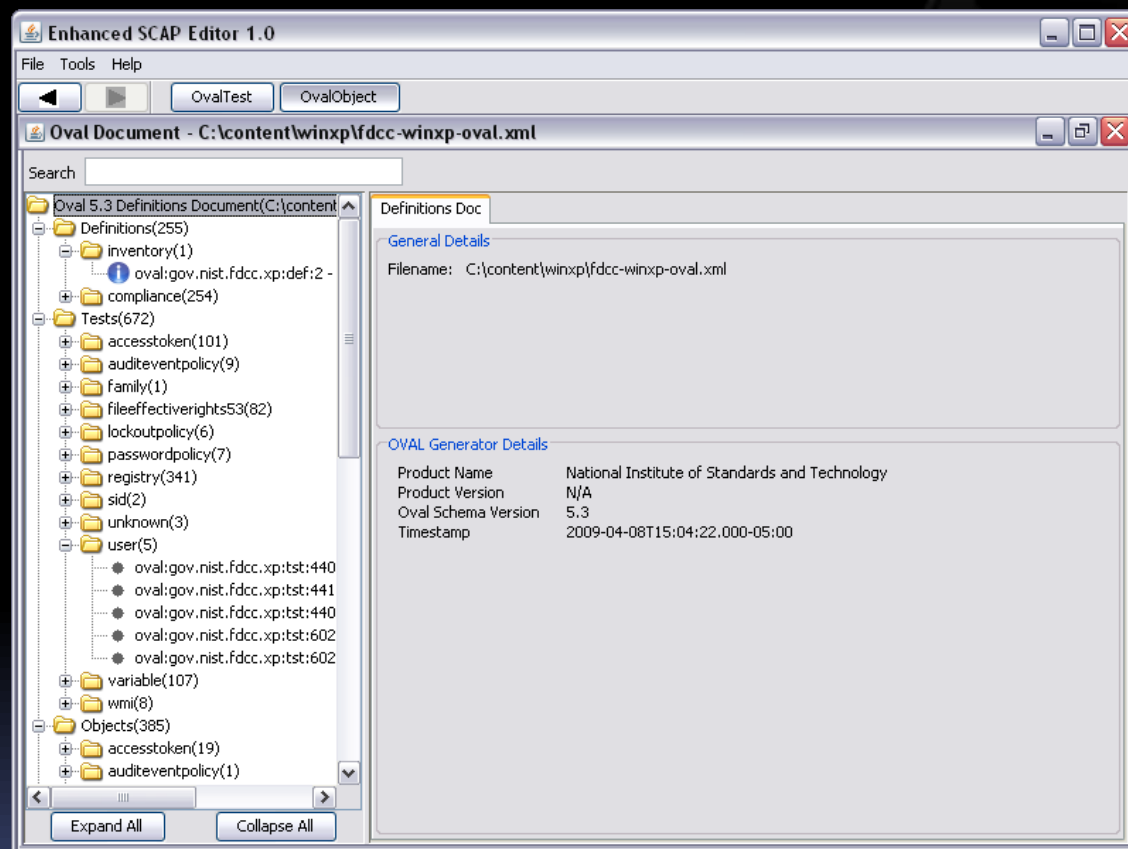


- Friendly interface for creating and editing SCAP documents
- Full OVAL file creation
 - Creation of definitions, tests, objects, states and variables
 - Support for OVAL versions 5.3 - 5.6
- Full OVAL file editing
 - Support for OVAL versions 5.3 - 5.6
- Searching inside OVAL documents
- Partial XCCDF file creation and editing
- Rapid OVAL and XCCDF creation with wizards
- CPE OVAL and CPE Dictionary viewing and creation
- Regular Expression Editor Tool and Validator Tool
- OVAL document merging
- Schema validation of OVAL and XCCDF documents
- SCAP Data Stream support and SCAP 1.0 validation



eSCAPe Editor - OVAL Editor

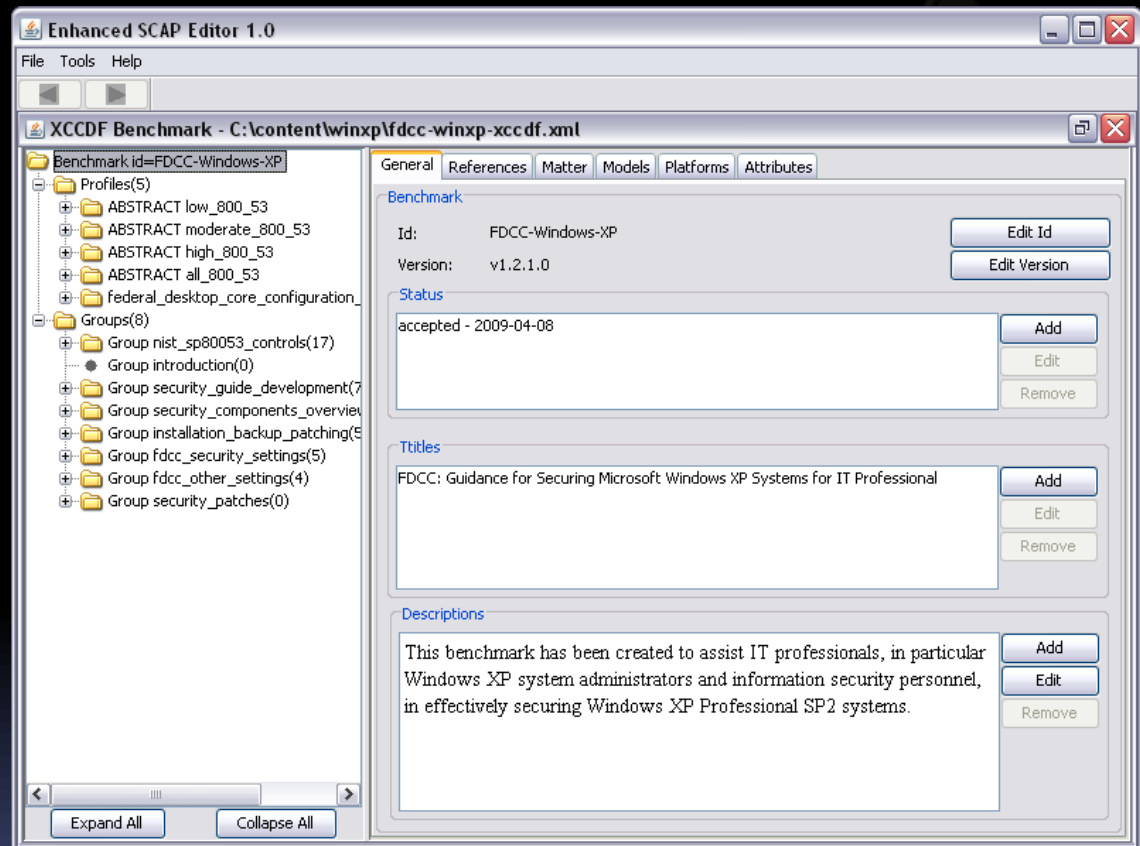
- Allows for viewing and editing of opened OVAL files. This is the standard editor and provides full editing of OVAL documents.
- Elements:
Breadcrumb
Toolbar,
Document Tree,
Information Area,
Search Bar





eSCAPe Editor - XCCDF Editor

- Allows for viewing and editing of opened XCCDF files
- XCCDF Documents can be created on the fly from open OVAL documents
- Elements: Document Tree, Information Area





W32/Conficker

“Conficker’s \$9.1 billion estimated economic cost”^[1]

“French fighter planes grounded by computer virus”^[2]



Heat map of W32/Conficker – 1 April 2009

1. Cyer Secure Institute, April 20th, 2009 (source <http://cybersecureinstitute.org/blog/?p=15>)

2. CNET News, February 8, 2009 (source http://news.cnet.com/8301-17852_3-10159186-71.html)



Example: Win32/Conficker.A

Looking to assess 2 things with SCAP:

- If we are ***vulnerable*** to the Microsoft Server Service Remote Code Execution Vulnerability, MS08-067, CVE-2008-4250
- If any of our assets have been ***infected*** with the Win32/Conficker.A worm



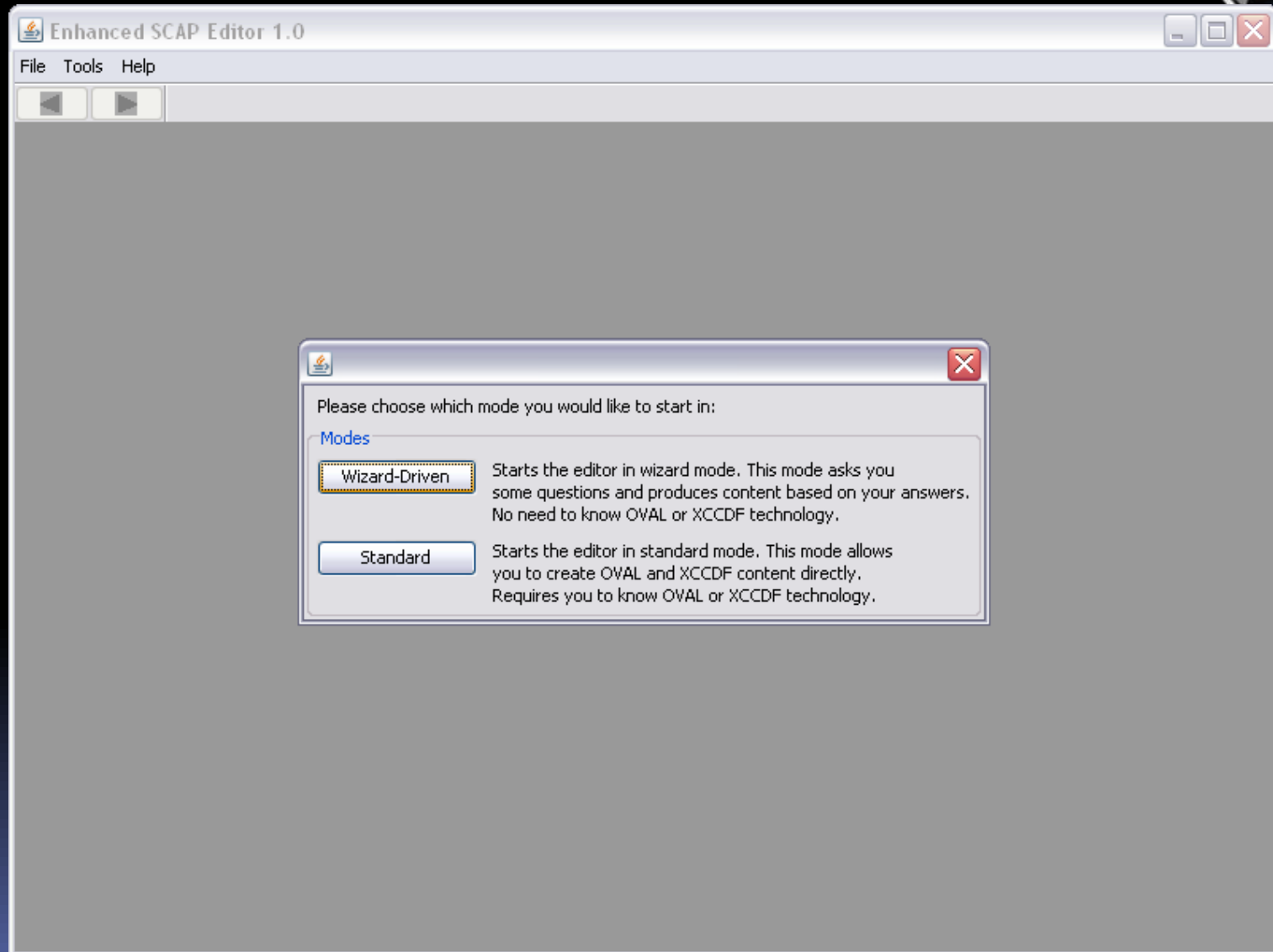
Checking Conficker.A Vulnerability

[CVE-2008-4250](#) - Microsoft Server Service Remote Code Execution Vulnerability

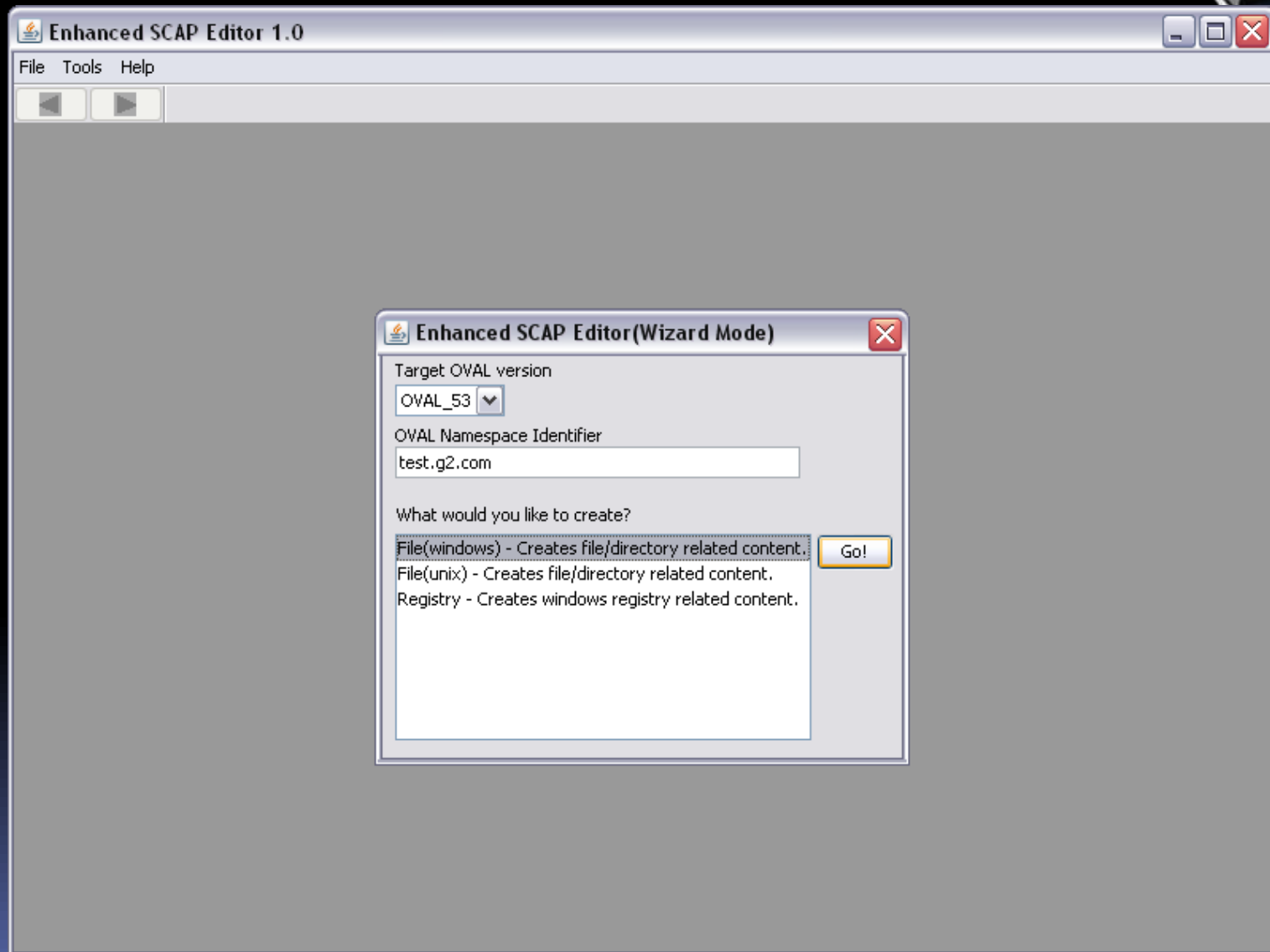
1. Microsoft Windows XP (x86) SP3 is installed
2. **%systemroot%\Netapi32.dll version is less than 5.1.2600.5694**

1. Common Vulnerabilities and Exposures (source <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>)

Start eSCAPe & Enter Wizard Mode



Select the File Test Wizard



Enter Test Information



Create New windows File Test [Close]

What to check about file [Save content](#)

Platform: windows

Title: Checking for vulnerability to Microsoft Server Service Remote Code Execution

Path:

- Regex [Edit](#)
- [Edit](#)

[File detail](#)

Must exist and meet the following criteria

- path(String)
- filename(String)
- owner(String)
- size(Int)
- a_time(Int)
- c_time(Int)
- m_time(Int)
- ms_checksum(String)
- version(Version)

Added

[Edit](#)

[Remove](#)

Page 1 of 2

[Back](#) [Next](#) [Cancel](#)

Enter Test Information (2)



The screenshot shows a 'Create New windows File Test' dialog box. The main window has a title bar with a close button. Below the title bar is a 'Save content' button. The main area is divided into several sections:

- Platform:** windows
- Title:** Checking for vulnerability to Microsoft Server Service Remote Code Execution
- Path:** %systemroot% (with a dropdown arrow, a 'Regex' checkbox, and an 'Edit' button)
- Filename:** Netapi32.dll (with a 'Regex' checkbox and an 'Edit' button)
- Recurse to find file(s)/directory(ies)
- File/Dir Existence:** Exists Doesn't Exist
- File detail:** Must exist and meet the following criteria
 - a_time(INT)
 - c_time(INT)
 - m_time(INT)
 - ms_checksum(String)
 - version(VERSION)
 - type(ENUMERATED)
 - development_class(String)
 - company(String)
 - internal_name(String)

An inset dialog box titled 'File detail' is open over the 'version(VERSION)' entry. It contains the following fields:

- Datatype:** VERSION
- Operation:** equals (with a dropdown arrow)
- Data:** 5.1.2600.5694
- Buttons:** Ok, Cancel

At the bottom of the main dialog box, there is a 'Page 1 of 2' indicator, 'Back' and 'Next' buttons, and a 'Cancel' button. On the right side of the main dialog, there are 'Edit' and 'Remove' buttons.

Enter Test Information (3)



Create New windows File Test [Close]

What to check about file:

Platform: windows

Title: Checking for vulnerability to Microsoft Server Service Remote Code Execution

Path: %systemroot% Regex

Filename: Netapi32.dll Regex

Recurse to find file(s)/directory(ies)

File/Dir Existence

Exists Doesn't Exist

File detail

Must exist and meet the following criteria

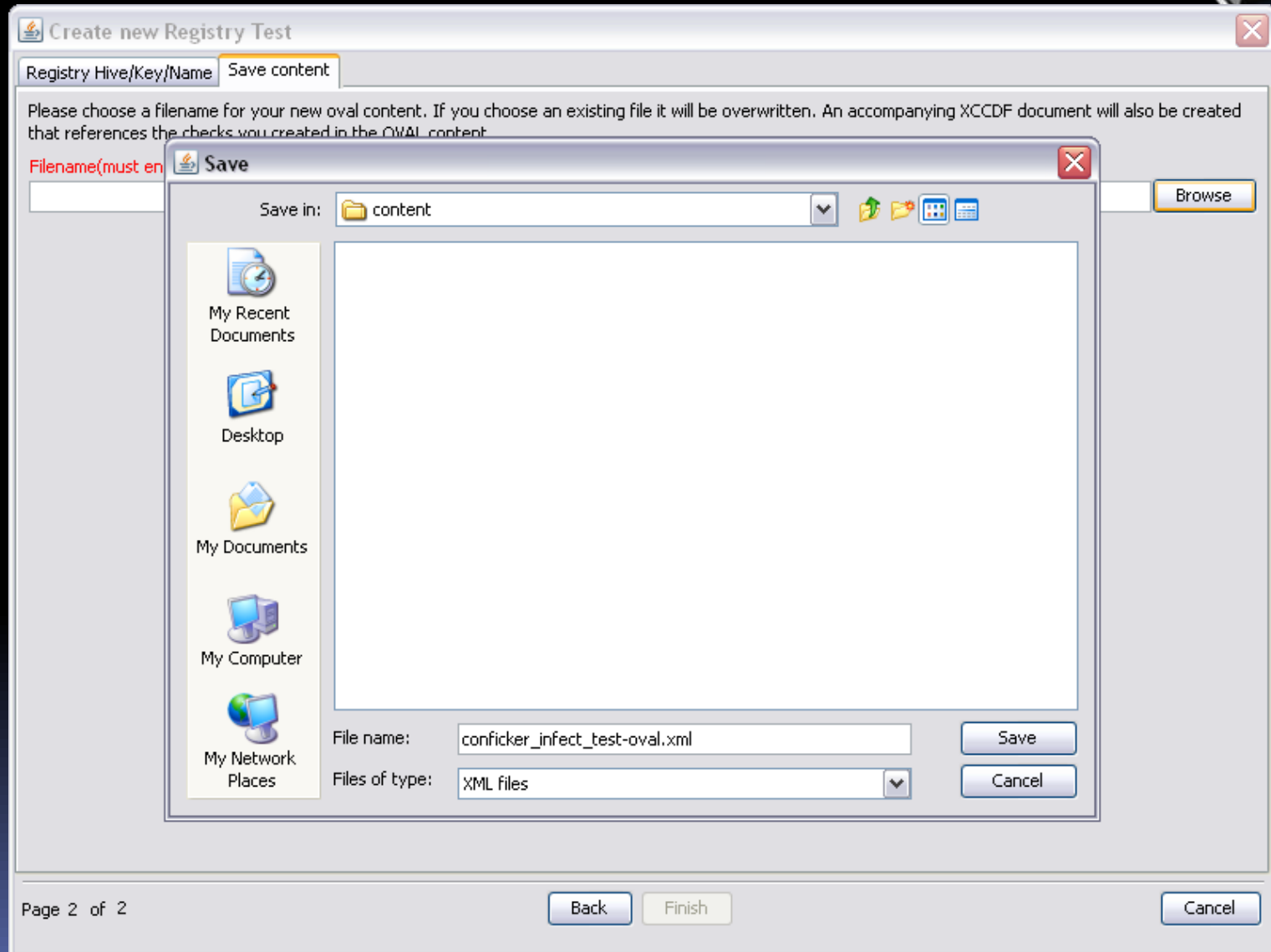
- path(String)
- filename(String)
- owner(String)
- size(Int)
- a_time(Int)
- c_time(Int)
- m_time(Int)
- ms_checksum(String)
- type(Enumerated)

Added

version(Version) less than 5.1.2600.5694

Page 1 of 2

Save OVAL File – Create XCCDF



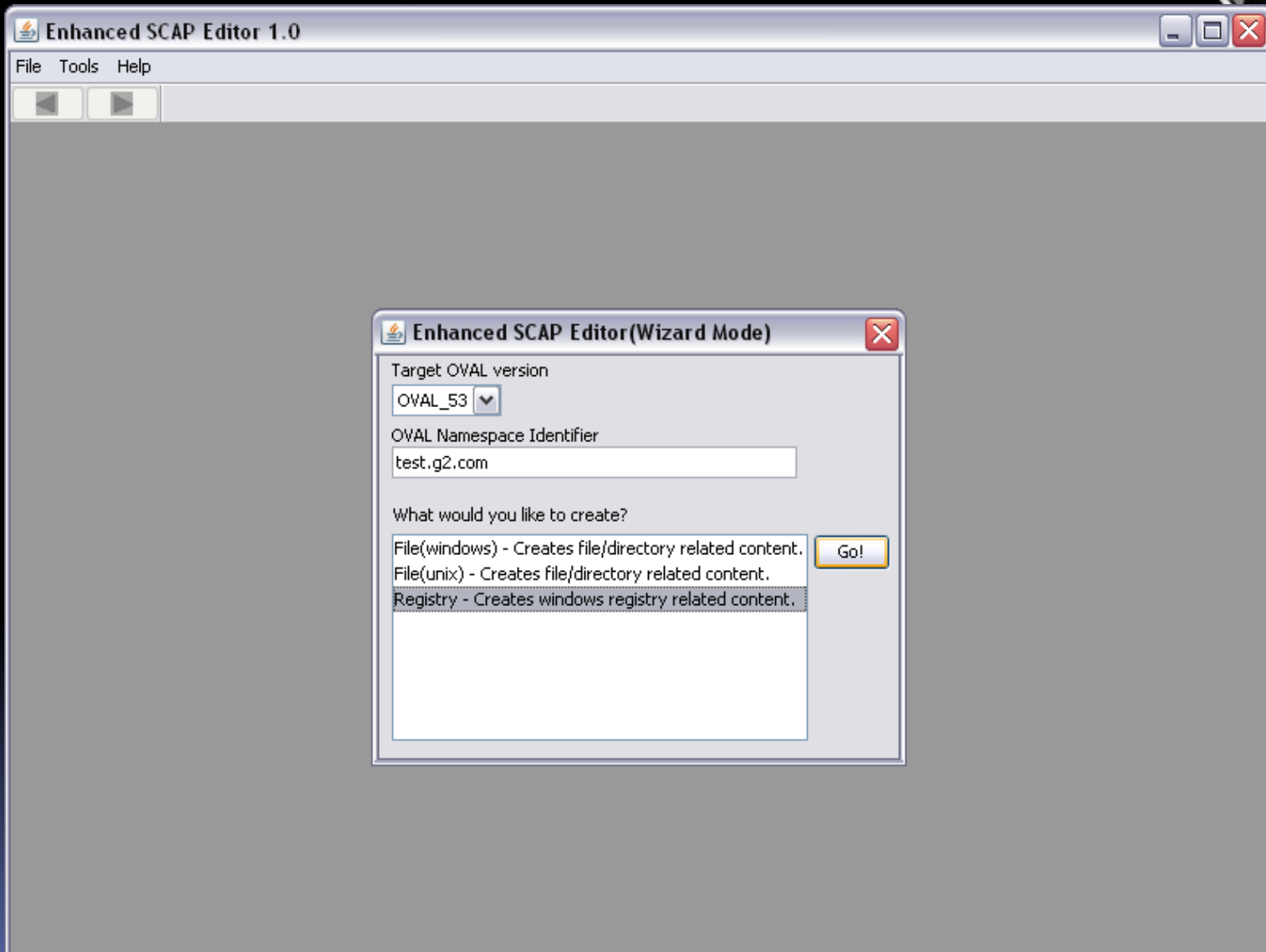


Checking Win32/Conficker.A Infection

1. *Hive\Key:* HKLM\SYSTEM\CurrentControlSet\Services\vcdrlxeu
Name: DisplayName
Value (data): 0
2. *Hive\Key:* HKLM\SYSTEM\ControlSet001\Services\vcdrlxeu\Parameters
Name: ServiceDll
Value (data): %systemroot%\nxyme.dll
 - where 'nxyme.dll' is <random>.dll, with <random> as a 5-8 character lowercase alphabetic name.

1. Microsoft (source <http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.A>)

Select the Registry Wizard



Enter Test Information



Create new Registry Test [X]

Registry Hive/Key/Name

Title
Checking for Win32/Conficker .A Infection

[What is to be tested](#)

- Hive\Key exists - ignore Name and Value
- Hive\Key does NOT exist - ignore Name and Value
- Hive\Key\Name exists - ignore Value
- Hive\Key\Name does NOT exist - ignore Value
- Value of hive\key\name

[Registry Hive](#)

HKEY_LOCAL_MACHINE [v]

[Registry Key](#)

SYSTEM\ControlSet001\Services\vcdr\xeu\Parameters Regex

[Registry Name](#)

ServiceDll Regex

[Registry Value](#)

[]

Datatype: string [v] Operation: pattern match [v]

Page 1 of 2

Enter Test Information (2)



The screenshot shows a 'Create new Registry Test' dialog box with a 'Regex pattern editor' sub-dialog box open over it. The main dialog box has the following fields and options:

- Registry Hive/Key/Name:** Save content
- Title:** Checking for Win32/Conficker.A Infection
- What is to be tested:**
 - Hive\Key exists - ignore Name and Value
 - Hive\Key does NOT exist - ignore Name and Value
 - Hive\Key\Name exists - ignore Value
 - Hive\Key\Name does NOT exist - ignore Value
 - Value of hive\key\name
- Registry Hive:** HKEY_LOCAL_MACHINE
- Registry Key:** SYSTEM\ControlSet001\Services\vcdr
- Registry Name:** ServiceDll
- Registry Value:** (empty)
- Datatype:** string

The 'Regex pattern editor' sub-dialog box contains:

- Regex Pattern:** Pattern: `^C:\\WINDOWS\\{[a-z]{5,8}\\.[Dd][L][L]}$`, Status: Pattern OK
- Test Area:** You can test that your pattern defined above will match text you supply.
Text to match: C:\WINDOWS\btuyup.dll (with a 'Match' button)
Number of groups matched: 0
Matched text: C:\WINDOWS\btuyup.dll
- Buttons:** Ok, Cancel

At the bottom of the main dialog box, there are 'Back', 'Next', and 'Cancel' buttons. The 'Page 1 of 2' indicator is also visible at the bottom left.

Enter Test Information (3)



Create new Registry Test [X]

Registry Hive/Key/Name

Title
Checking for Win32/Conficker .A Infection

What is to be tested

- Hive\Key exists - ignore Name and Value
- Hive\Key does NOT exist - ignore Name and Value
- Hive\Key\Name exists - ignore Value
- Hive\Key\Name does NOT exist - ignore Value
- Value of hive\key\name

Registry Hive

HKEY_LOCAL_MACHINE [v]

Registry Key

SYSTEM\ControlSet001\Services\vcdr\xeu\Parameters Regex

Registry Name

ServiceDll Regex

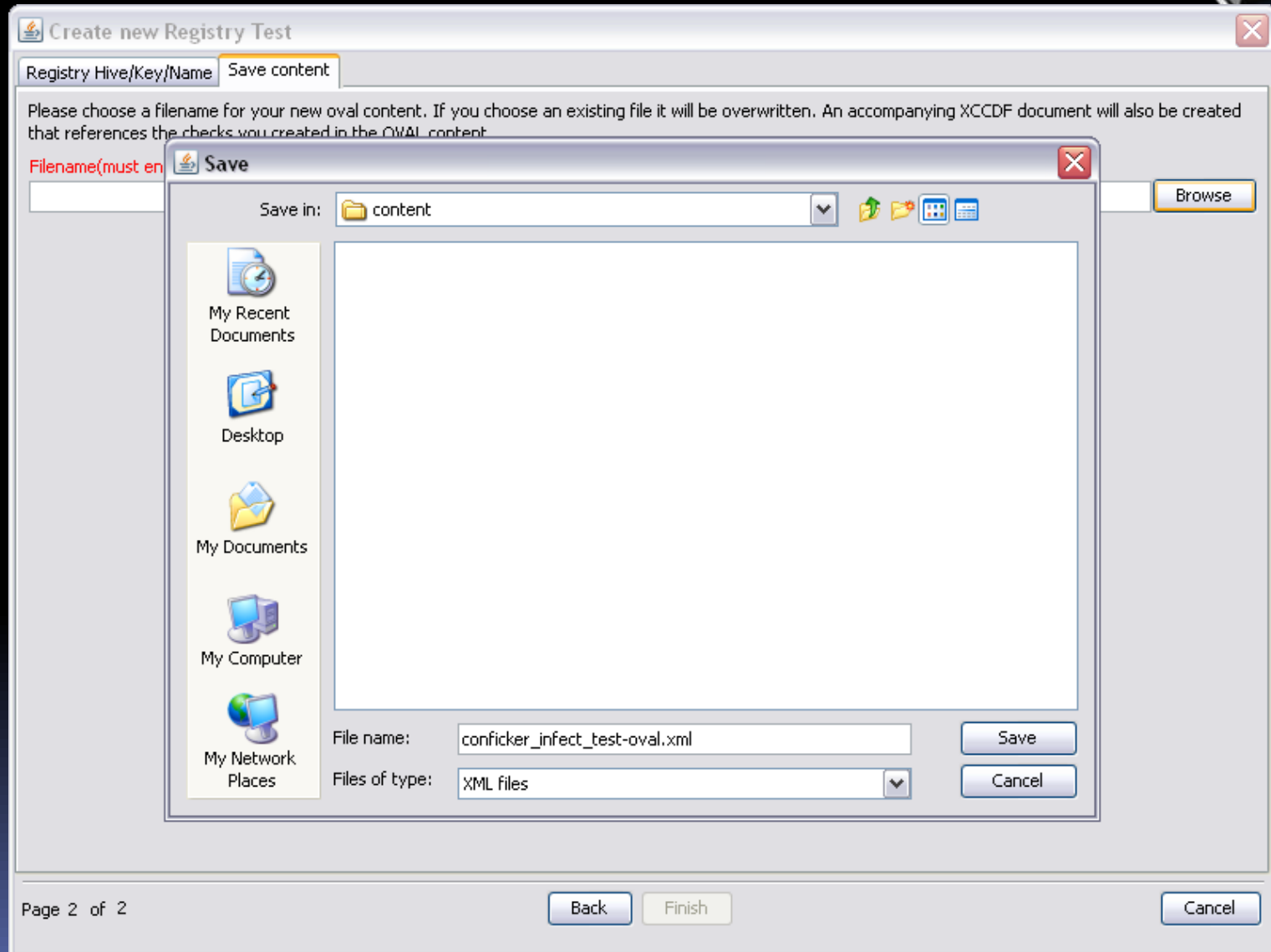
Registry Value

^C:\\WINDOWS\\{[a-z]{5,8}\\.[Dd][Ll][Ll]\$

Datatype: string [v] Operation: pattern match [v]

Page 1 of 2

Save OVAL File – Create XCCDF





Benchmark “Critical-controls” Tailoring using eSCAPE

- Need to tailor FDCC benchmark for our organization
 - Want to allow auto-run for all devices, except thumb drives (removal devices)
 - Will need to edit the FDCC OVAL file
 - We can use eSCAPE to make the needed changes

Open OVAL File in eSCAPE



The screenshot shows the 'Enhanced SCAP Editor 0.0.11-SNAPSHOT' application. The main window displays an OVAL document titled 'OVAL Document - C:\fdcc-winxp-oval.xml'. A search bar at the top left contains the text 'autorun'. The left pane shows a tree view of the document structure, with 'Tests(3)' expanded to show three items, the second of which is selected: 'oval:gov.nist.fdcc.xp:def:117 - Autorun Disabled for All Drives'. The right pane shows the 'General' tab for this selected test, with fields for 'Class' (COMPLIANCE), 'Id' (oval:gov.nist.fdcc.xp:def:117), and 'Title' (Autorun Disabled for All Drives). Below these fields is a 'Version' dropdown set to '1'. At the bottom of the right pane is a 'References Summary' table.

| Id | Source | Url |
|------------|-------------------------|-----|
| CCE-2710-2 | http://cce.mitre.org | |
| CCE-44 | cce.mitre.org/version/4 | |

Identify Test to be Adjusted



The screenshot shows the 'Enhanced SCAP Editor 0.0.11-SNAPSHOT' application. The main window displays an 'OVAL Document - C:\fdcc-winxp-oval.xml'. A search bar at the top left contains the text 'autorun'. The left pane shows a tree view of the document structure. Under 'Definitions(2)', there are two items: 'oval:gov.nist.fdcc.xp:def:612261224 - Do not automatically start Wind' and 'oval:gov.nist.fdcc.xp:def:117 - Autorun Disabled for All Drives'. Under 'Tests(3)', there are three items: 'oval:gov.nist.fdcc.xp:tst:171 - Registry key HKEY_LOCAL_MACHINE\Sc', 'oval:gov.nist.fdcc.xp:tst:172 - Registry key HKEY_LOCAL_MACHINE\Sc', and 'oval:gov.nist.fdcc.xp:tst:612261224 - Registry key HKLM\SOFTWARE\'. The right pane shows the 'Criteria' tab, which displays a list of criteria under 'Criteria<AND>'. The criteria are: 'Definition<oval:gov.nist.fdcc.xp:def:2> - Microsoft Windows XP is installed', 'Criterion<oval:gov.nist.fdcc.xp:tst:171> - Registry key HKEY_LOCAL_MACHINE\Softv', and 'Criterion<oval:gov.nist.fdcc.xp:tst:172> - Registry key HKEY_LOCAL_MACHINE\Softv'. The 'Status' field at the bottom is empty.

Select OVAL Test State to Edit



The screenshot shows the 'Enhanced SCAP Editor 0.0.11-SNAPSHOT' application. The main window displays an OVAL document titled 'OVAL Document - C:\fdcc-winxp-oval.xml'. On the left, a tree view shows the document's structure, including 'Definitions(2)', 'compliance(2)', and 'Tests(3)'. The 'Tests(3)' folder is expanded, showing several registry tests. One test, 'oval:gov.nist.fdcc.xp:tst:172 - Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=255', is selected. The right pane shows the configuration for this test. The 'General' tab is active, displaying the Test Id, Test Type (registry_test), Comment, Check (all), Check Existence (at_least_one_exists), and State Operator (AND). The 'Version' is set to 1. The 'Test Detail' section shows the Object Id (oval:gov.nist.fdcc.xp:obj:69) and a list of State(s). The state 'oval:gov.nist.fdcc.xp:ste:49 - No comment set' is selected, and a tooltip indicates it can be double-clicked to view.

Navigate to State and click 'Edit'



The screenshot displays the 'Enhanced SCAP Editor 0.0.11-SNAPSHOT' interface. The main window shows a tree view of OVAL states on the left and a detailed view of a selected state on the right. A 'String Editor' dialog box is open over the state details, showing a 'String Value' of '255'. The state details include a 'General' tab with 'State Id' set to 'oval:gov.nist.fdcc.xp:ste:49' and 'State Type' set to 'registry_state'. Below this, there is a 'Possible parameters' section with a text area containing the text: 'registry key belongs to. This is a specific set of values: HKEY_CURRENT_CONFIG, HKEY_LOCAL_MACHINE, and HKEY_USERS.' At the bottom of the state details, there is an 'Added parameters' table.

| Name | Operation | Datatype | Value |
|-------|-----------|----------|-------|
| value | equals | int | 255 |



Autoplay Setting Values

- Microsoft documentation of Autoplay registry value settings

| Value | Setting |
|------------|---|
| 0x1 | Disables AutoPlay on drives of unknown type. |
| 0x4 | Disables AutoPlay on removable drives. |
| 0x8 | Disables AutoPlay on fixed drives. |
| 0x10 | Disables AutoPlay on network drives. |
| 0x20 | Disables AutoPlay on CD-ROM drives. |
| 0x40 | Disables AutoPlay on RAM drives. |
| 0x80 | Disables AutoPlay on drives of unknown type. |
| 0x255 | Disables AutoPlay on all types of drives. |

Adjust Setting per Documetation



The screenshot shows the 'Enhanced SCAP Editor 0.0.11-SNAPSHOT' interface. The main window displays an 'OVAL Document - C:\fdcc-winxp-oval.xml'. On the left, a tree view shows a list of OVAL states, with a folder named 'registry(136)' expanded. The right pane shows the configuration for a selected state (State Id: oval:gov.nist.fdcc.xp:ste:49, State Type: registry_state). A 'String Editor' dialog box is open in the foreground, showing a 'String Value' of '4'. The background configuration includes a 'Comment' field and a 'Possible parameters' section with an 'Add' button. Below that, an 'Added parameters' table is visible.

| Name | Operation | Datatype | Value |
|-------|-----------|----------|-------|
| value | equals | int | 255 |

Save Customized Benchmark




The screenshot shows the 'Enhanced SCAP Editor 0.0.11-SNAPSHOT' interface. The 'File' menu is open, showing options like 'New', 'Open', 'Save', and 'Save As'. The 'Recent' list includes several benchmark entries, with 'oval:gov.nist.fdcc.xp:ste:49 - No Comment Set' selected. The main workspace displays a tree view of the benchmark structure, with a folder named 'registry(136)' expanded. The right-hand pane shows the configuration for the selected state, 'oval:gov.nist.fdcc.xp:ste:49'. The 'General' tab is active, showing the 'State Id' as 'oval:gov.nist.fdcc.xp:ste:49' and the 'State Type' as 'registry_state'. The 'Version' is set to '1'. The 'Possible parameters' section shows a parameter named 'hive' with a value of 'hive'. The 'Added parameters' table is as follows:

| Name | Operation | Datatype | Value |
|-------|-----------|----------|-------|
| value | equals | string | 4 |



The eSCAPe Libraries

- Can be used to script the creation and editing of SCAP content
- Used to build the eSCAPe Editor
- Coded in Java (1.6)
- Released as open source software under the GPLv3 license 



Using the eSCAPe Libraries

1. Download the libraries
(<http://www.g2-inc.com/escape>)
1. Choose a development environment
(Example: Eclipse)
2. Install the Java Development kit (JDK)
3. See the documentation. On the G2 eSCAPe page under 'Library Documentation'



eSCAPe Libraries in Action

“Automated Creation of SCAP Content”

Shane Shaffer and Peter Guerra , G2

- Tuesday, Sept. 24th, 2:30-3:15pm, Ballroom I
- Discussion on how the eSCAPe libraries have been used to create automated SCAP content for detecting malware



How to get eSCAPe

Released as FREE open source software under the GPLv3 license

The screenshot shows the eSCAPe website interface. At the top, there is a navigation bar with links: HOME, ABOUT G2, JOIN OUR TEAM, CONTACT G2, and G2. Below this is a banner with the text "TRUSTED INNOVATORS" and the G2 logo. The main content area is titled "Building SCAP Content Just Got Easy" and includes a paragraph describing the Enhanced SCAP Editor (eSCAPe) as a utility for building Security Content Automation Protocol (SCAP) content files. It also features two screenshots: one of the "Editor" interface and one of the "Library" interface. Below the screenshots, there are two columns of text explaining the editor's use and the library's contents. At the bottom, there is a "Download" section with a "Download" button and a "More" link.

<http://www.g2-inc.com/escape>

The screenshot shows the NIST Security Content Automation Protocol (SCAP) website. The header includes the NIST logo and the text "National Institute of Standards and Technology Information Technology Laboratory". The main title is "Security Content Automation Protocol". A navigation menu on the left includes links for Home, Publications, Release Cycle, SCAP Validation, SCAP Content, SCAP Specifications, SCAP 1.1 (Draft), SCAP 1.0, Events, Community, and Emerging Specifications. The "SCAP Specifications" section is highlighted. The main content area is titled "SCAP Specifications" and includes a paragraph explaining the need for a common revision cycle. It also features a "Protocol" section with details for "SCAP Security Content Automation Protocol" and "SCAP Security Content Automation Protocol".

<http://scap.nist.gov/revision/index.html>



Contact Information

Peter Parker

Security Engineer

410-290-9710 | Peter.Parker@G2-Inc.com

Shane Shaffer

Senior Security Architect

410-290-9710 | Shane.Shaffer@G2-Inc.com

Jeff Cockerill

Senior Software Developer

410-290-9710 | Jeff.Cockerill@G2-Inc.com

How to get eSCAPe

<http://www.g2-inc.com/escape>