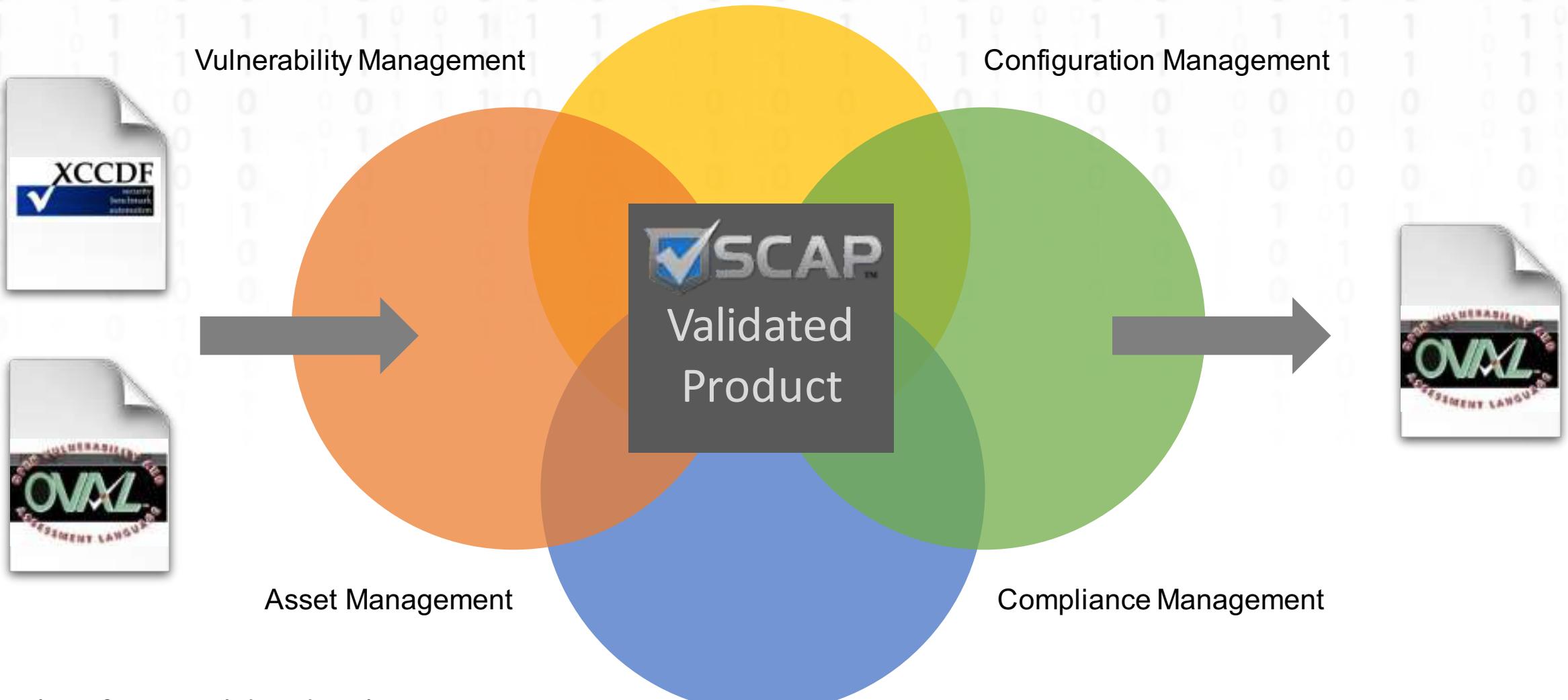


# The Enhanced SCAP Editor (eSCAPe) and Libraries



# It All Depends on SCAP Content



See list of SCAP Validated tools at:  
<http://nvd.nist.gov/scaproducts.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</description>
  <platform idref="cpe:/o:microsoft:windows_xp" />
  <version>v0.0</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)

---

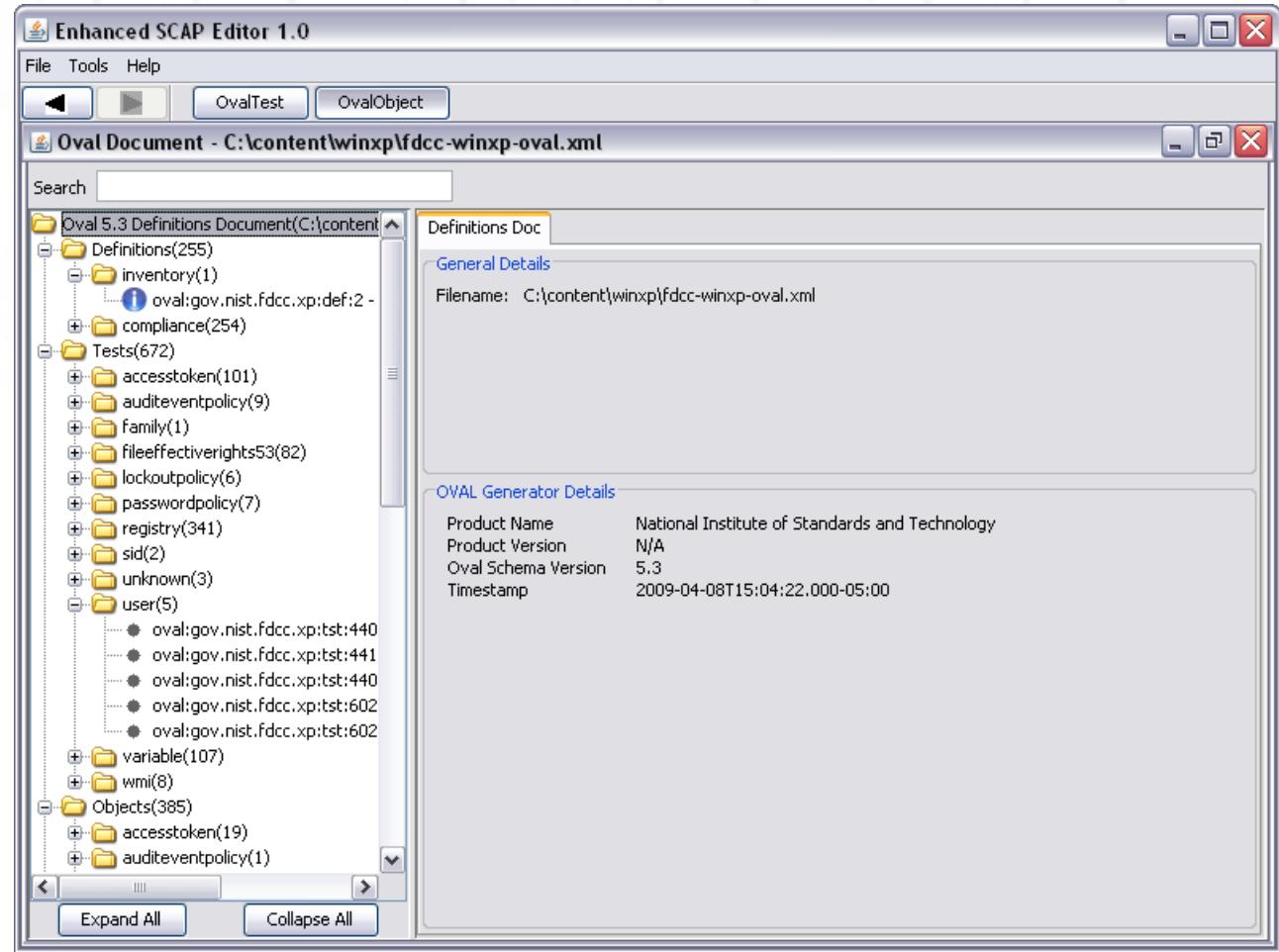


- Friendly interface for creating and editing SCAP documents
- Full OVAL file creation
  - Creation of definitions, tests, objects, states and variables
  - Support for OVAL versions 5.3 – 5.6
- Full OVAL file editing
  - Support for OVAL versions 5.3 – 5.6
- Searching inside OVAL documents
- Partial 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



# W32/Conficker



- “Conficker’s \$9.1 billion estimated economic cost”<sup>[1]</sup>
- “French fighter planes grounded by computer virus”<sup>[2]</sup>



*Heat Map of W32/Conficker – 1 April 2009*

1. Cyber 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](http://news.cnet.com/8301-17852_3-10159186-71.html))



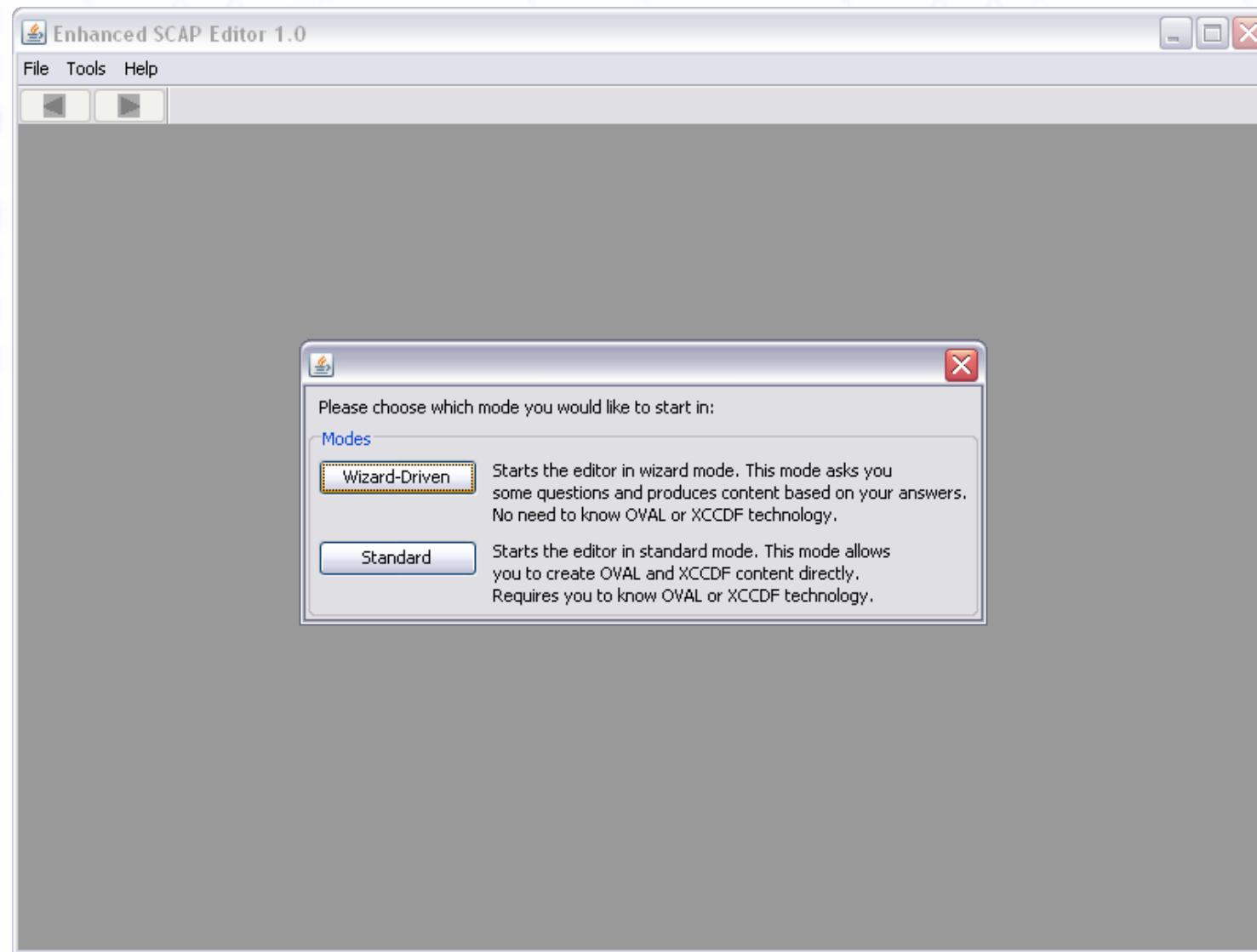
# Example: Win32/Conficker.A

---

**Looking to asses 2 things with SCAP:**

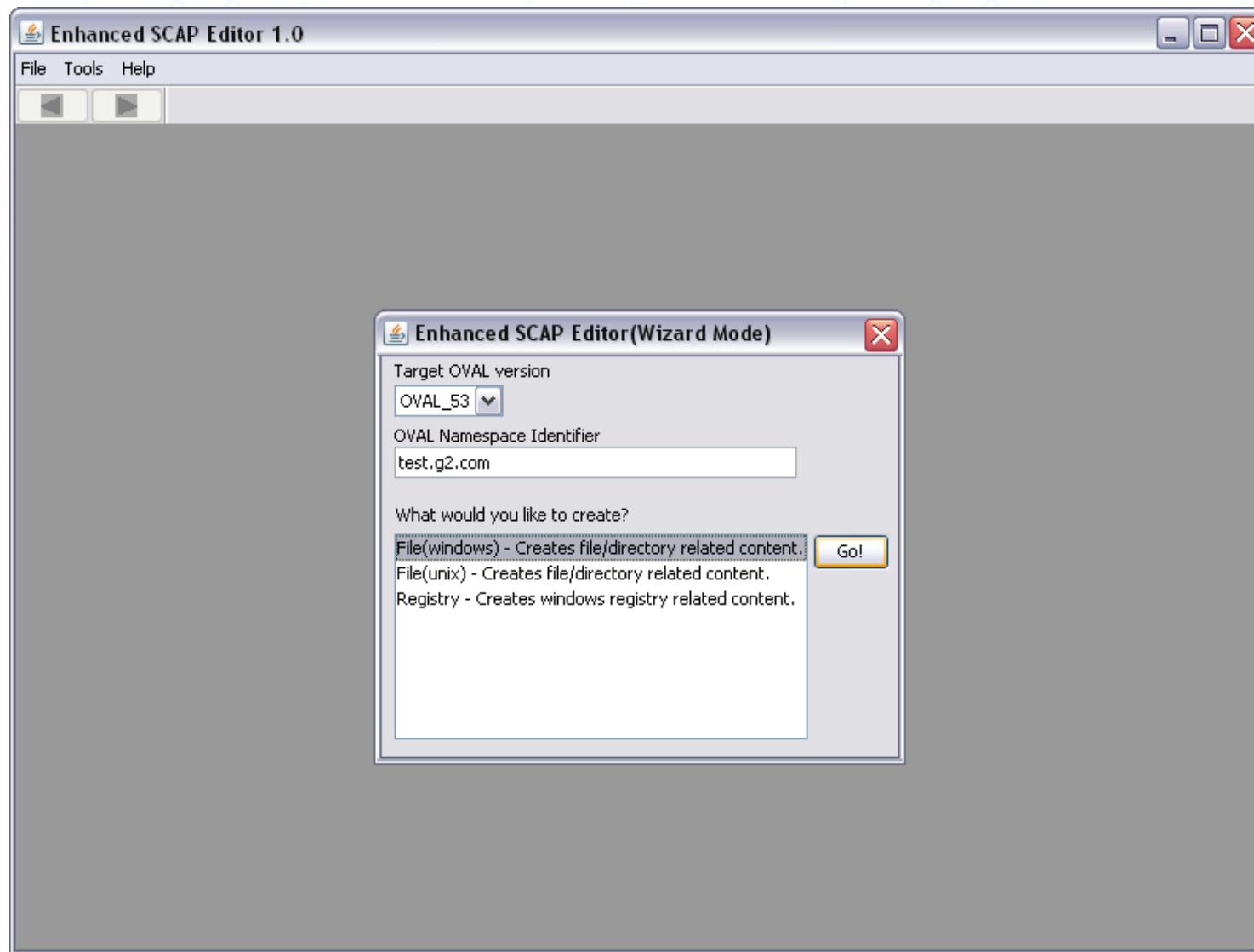
- If we are vulnerable to the Microsoft Server Service Remote Code Execution Vulnerability, MS08-067, CVE-2008-4250
- If any of our assets have been infected with the Win32/Conficker.A worm

# Start eSCAPE & Enter Wizard Mode





# Select the File Wizard





# Enter Test Information

Create New windows File Test

What to check about file

Platform: windows

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

Path:

- %commonprogramfiles%
- %commonprogramfiles(x86)%
- %programdata%
- %programfiles%
- %programfiles(x86)%
- %systemroot%
- %temp%
- %tmp%

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:

Page 1 of 2



# Enter Test Information (2)

Create New windows File Test

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

a\_time(INT)  
c\_time(INT)  
m\_time(INT)  
ms\_checksum(STRING)  
version(VERSION)  
type ENUMERATED  
development\_class(STRING)  
company(STRING)  
internal\_name(STRING)

Datatype VERSION

Operation: equals

Data: 5.1.2600.5694

Add

Added:

Page 1 of 2



# Enter Test Information (3)

**Create New windows File Test**

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

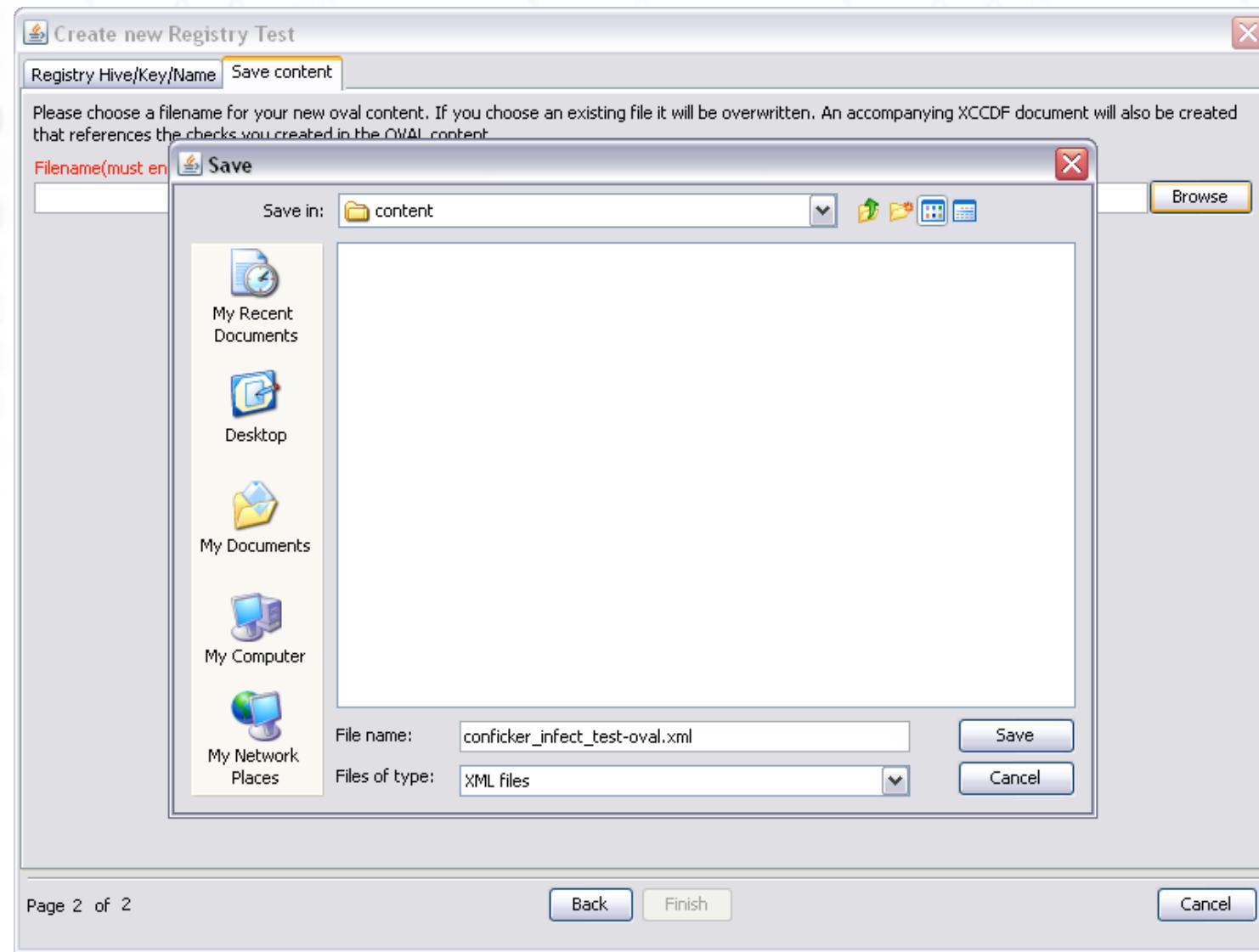
path(STRING)  
filename(STRING)  
owner(STRING)  
size(INT)  
a\_time(INT)  
c\_time(INT)  
m\_time(INT)  
ms\_checksum(STRING)  
type(ENUMERATED)

**Added**

version(VERSION) less than 5.1.2600.5694

Page 1 of 2

# Save OVAL File – Create XCCDF



# Checking Win32/Conficker.A Infection

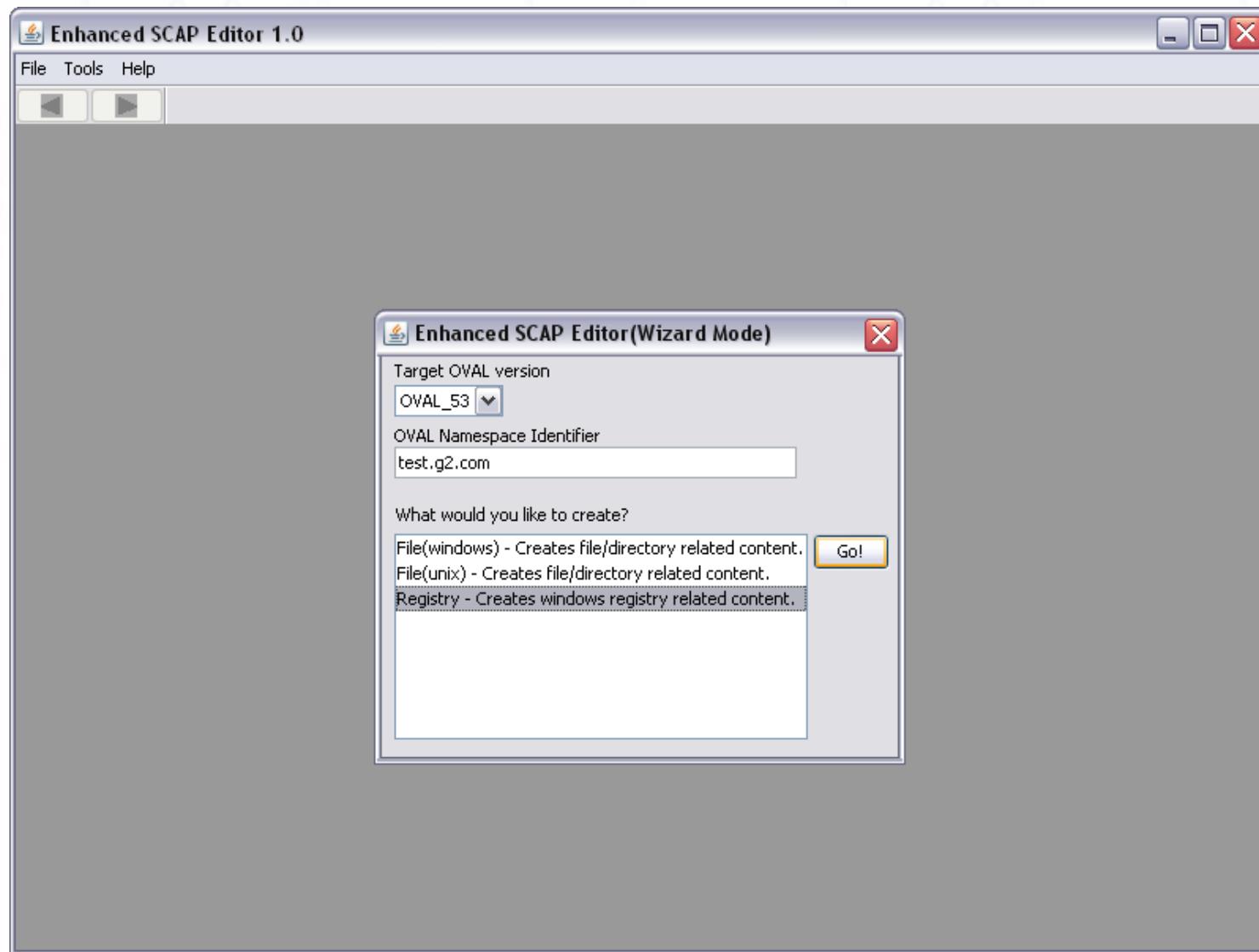
---



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
3. where 'nxyme.dll' is <random>.dll, with <random> as a 5-8 character lowercase alphabetic name.



# Select the Registry Wizard





# Enter Test Information

Create new Registry Test X

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\vcdrlxeu\Parameters  Regex Edit

Registry Name  
ServiceDll  Regex Edit

Registry Value  
| Edit

Datatype: string Operation: pattern match

Page 1 of 2 Back Next Cancel



# Enter Test Information (2)

Create new Registry Test

Registry Hive/Key/Name

Title: Checking for Win32/Conficker.A Infect

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 Name
- Value of hive\key\name

Registry Hive: HKEY\_LOCAL\_MACHINE

Registry Key: SYSTEM\ControlSet001\Services\vcdl

Registry Name: ServiceDll

Registry Value:

Datatype: string

**Regex pattern editor**

Regex Pattern

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

Status: Pattern OK

Test Area

You can test that your pattern defined above will match text you supply.

Text to match: C:\WINDOWS\btyuyp.dll

Number of groups matched: 0  
Matched text: C:\WINDOWS\btyuyp.dll

Regex

Regex

Page 1 of 2



# Enter Test Information (3)

**Create new Registry Test**

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\vcdrlxeu\Parameters  Regex [Edit](#)

Registry Name

ServiceDll  Regex [Edit](#)

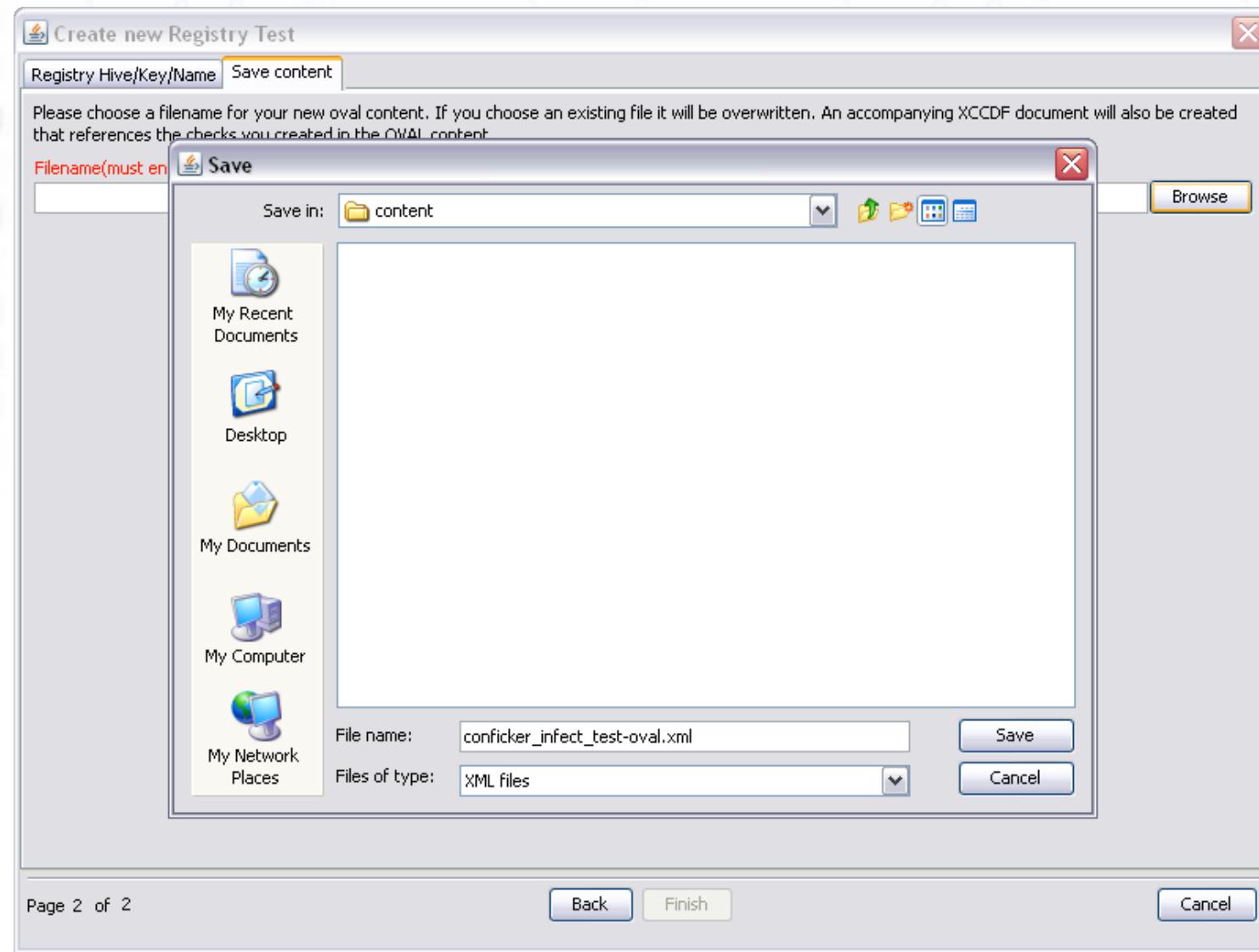
Registry Value

^C:\{WINDOWS\}\{[a-z]{5,8}\}\{[Dd][Ll][Uu]\}\$ [Edit](#)

Datatype: string Operation: pattern match

Page 1 of 2 [Back](#) [Next](#) [Cancel](#)

# 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 interface with the title bar "Enhanced SCAP Editor 0.0.11-SNAPSHOT". The menu bar includes "File", "Tools", and "Help". The toolbar has icons for New, Open, Save, and Print. The main window displays an "OVAL Document - C:\fdcc-winxp-oval.xml" tab. A search bar at the top left contains the text "autorun". The left pane is a tree view of the OVAL XML structure:

- OVAL 5.3 Definitions Document(C:\fdcc-winxp-oval.xml)
- Definitions(2)
  - inventory
  - compliance(2)
    - oval:gov.nist.fdcc.xp:def:612261224 - Do not automatically start Wind
    - oval:gov.nist.fdcc.xp:def:117 - Autorun Disabled for All Drives
- Tests(3)
  - accesstoken
  - auditeventpolicy
  - family
  - fileeffectiverights53
  - lockoutpolicy
  - passwordpolicy
  - registry(3)
    - oval:gov.nist.fdcc.xp:tst:171 - Registry key HKEY\_LOCAL\_MACHINE\Se
    - oval:gov.nist.fdcc.xp:tst:172 - Registry key HKEY\_LOCAL\_MACHINE\Se
    - oval:gov.nist.fdcc.xp:tst:612261224 - Registry key HKLM\SOFTWARE\|
  - sid
  - unknown
  - user
  - variable
  - wmi
- Objects(2)
  - accesstoken
  - auditeventpolicy
  - family
  - fileeffectiverights53
  - lockoutpolicy
  - passwordpolicy

The right pane shows the "General" tab of the selected "compliance" item. The "Class" is set to "COMPLIANCE". The "Id" is "oval:gov.nist.fdcc.xp:def:117" and the "Title" is "Autorun Disabled for All Drives". Below the title is a "Version" field with the value "1". The "References Summary" section lists two entries:

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

At the bottom of the interface are buttons for "Expand All" and "Collapse All".



# Identify Test to be Adjusted

The screenshot shows the Enhanced SCAP Editor interface with the title "Enhanced SCAP Editor 0.0.11-SNAPSHOT". The main window displays an "OVAL Document - C:\fdcc-winxp-oval.xml" file. The left pane contains a tree view of OVAL components:

- OVAL 5.3 Definitions Document(C:\fdcc-winxp-oval.xml)
  - Definitions(2)
    - inventory
    - compliance(2)
      - oval:gov.nist.fdcc.xp:def:612261224 - Do not automatically start Wind
      - oval:gov.nist.fdcc.xp:def:117 - Autorun Disabled for All Drives
  - Tests(3)
    - accesstoken
    - auditeventpolicy
    - Family
    - fileeffectiverights53
    - lockoutpolicy
    - passwordpolicy
    - registry(3)
      - oval:gov.nist.fdcc.xp:tst:171 - Registry key HKEY\_LOCAL\_MACHINE\So
      - oval:gov.nist.fdcc.xp:tst:172 - Registry key HKEY\_LOCAL\_MACHINE\So
      - oval:gov.nist.fdcc.xp:tst:612261224 - Registry key HKLM\SOFTWARE\I
    - sid
    - unknown
    - user
    - variable
    - wmi
  - Objects(2)
    - accesstoken
    - auditeventpolicy
    - Family
    - fileeffectiverights53
    - lockoutpolicy
    - passwordpolicy

The right pane shows the "Criteria" tab selected, displaying a list of criteria under "Criteria<AND>":

- 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\Software\Microsoft\Windows\CurrentVersion\Run
- Criterion<oval:gov.nist.fdcc.xp:tst:172> - Registry key HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

At the bottom of the editor, there are buttons for "Expand All" and "Collapse All".

# Select OVAL Test State to Edit



Enhanced SCAP Editor 0.0.11-SNAPSHOT

OVAL Document - C:\fdcc-winxp-oval.xml

Search autorun

OVAL 5.3 Definitions Document(C:\fdcc-winxp-oval.xml)

- Definitions(2)
  - inventory
  - compliance(2)
    - oval:gov.nist.fdcc.xp:def:612261224 - Do not automatically start Wind
    - oval:gov.nist.fdcc.xp:def:117 - Autorun Disabled for All Drives
- Tests(3)
  - accesstoken
  - auditeventpolicy
  - Family
  - fileeffectiverights53
  - lockoutpolicy
  - passwordpolicy
  - registry(3)
    - oval:gov.nist.fdcc.xp:tst:171 - Registry key HKEY\_LOCAL\_MACHINE\So
    - oval:gov.nist.fdcc.xp:tst:172 - Registry key HKEY\_LOCAL\_MACHINE\So
    - oval:gov.nist.fdcc.xp:tst:612261224 - Registry key HKLM\SOFTWARE\I
  - sid
  - unknown
  - user
  - variable
  - wmi
- Objects(2)
  - accesstoken
  - auditeventpolicy
  - Family
  - fileeffectiverights53
  - lockoutpolicy
  - passwordpolicy

Test Source

General

Test Id: oval:gov.nist.fdcc.xp:tst:172

Test Type: registry\_test

Comment: %soft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=255

Check: all

Check Existence: at\_least\_one\_exists

State Operator: AND

Version: 1

Test Detail

Object: A test must point to an object to be valid.

Object Id: oval:gov.nist.fdcc.xp:obj:69

Choose Object

State(s)

This version of OVAL only allows one state to be set per test.

State	Add
oval:gov.nist.fdcc.xp:ste:49 - No comment set	Remove

oval:gov.nist.fdcc.xp:ste:49 - No comment set. Double-Click to view

Move Down

Expand All

Collapse All



# Navigate to State and Click “Edit”

The screenshot shows the Enhanced SCAP Editor 0.0.11-SNAPSHOT interface. The main window title is "Enhanced SCAP Editor 0.0.11-SNAPSHOT" and the tab is "OVAL Document - C:\fdcc-winxp-oval.xml". The left pane displays a tree view of OVAL items, with a node "registry(136)" expanded, showing various sub-items. The right pane contains a "State" configuration panel and a "String Editor" dialog box. The "State" panel shows the following details:

- State Id: oval:gov.nist.fdcc.xp:ste:49
- State Type: registry\_state
- Version: 1
- Comment: (empty)
- Possible parameters: (empty)

The "String Editor" dialog box is open, showing "String Value: 255". The "OK" button is highlighted with a yellow border. A tooltip for the "String Value" field states: "This registry key belongs to. This is a specific set of values: HKEY\_CURRENT\_CONFIG, HKEY\_LOCAL\_MACHINE, and HKEY\_USERS." Below the editor, the "Added parameters" table is shown:

Name	Operation	Datatype	Value
value	equals	int	255

Buttons for "Edit" and "Remove" are visible next to the table.

# AutoPlay Setting Values



- Microsoft documentation of AutoPlay registry value settings

Value	Setting
0X1	Disables AutoPlay on drives of unknown type.
<b>0X4</b>	<b>Disables AutoPlay on removable drives.</b>
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.
0X55	Disables AutoPlay on all types of drives.



# Save Customized Benchmark

Enhanced SCAP Editor 0.0.11-SNAPSHOT

File Tools Help

OvalTest

Save As C:\fdcc\winxp-oval.xml(modified)

Recent oval:gov.nist.fdcc.xp:ste:18 - No Comment Set  
oval:gov.nist.fdcc.xp:ste:19 - No Comment Set  
oval:gov.nist.fdcc.xp:ste:20 - No Comment Set  
oval:gov.nist.fdcc.xp:ste:22 - No Comment Set  
oval:gov.nist.fdcc.xp:ste:23 - No Comment Set  
oval:gov.nist.fdcc.xp:ste:24 - No Comment Set  
oval:gov.nist.fdcc.xp:ste:103 - No Comment Set

registry(136)

- oval:gov.nist.fdcc.xp:ste:1 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:6 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:7 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:8 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:9 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:10 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:11 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:12 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:13 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:15 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:21 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:34 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:39 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:40 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:41 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:43 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:44 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:45 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:47 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:48 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:49 - No Comment Set
- oval:gov.nist.fdcc.xp:ste:50 - No Comment Set

State Source

General

State Id: oval:gov.nist.fdcc.xp:ste:49

State Type: registry\_state

Version: 1

Comment:

Possible parameters

Parameter: hive

The hive that the registry key belongs to. This is restricted to a specific set of values:  
HKEY\_CLASSES\_ROOT, HKEY\_CURRENT\_CONFIG, HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE, and HKEY\_USERS.

Added parameters

Name	Operation	Datatype	Value
value	equals	string	4

Expand All Collapse All

# 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

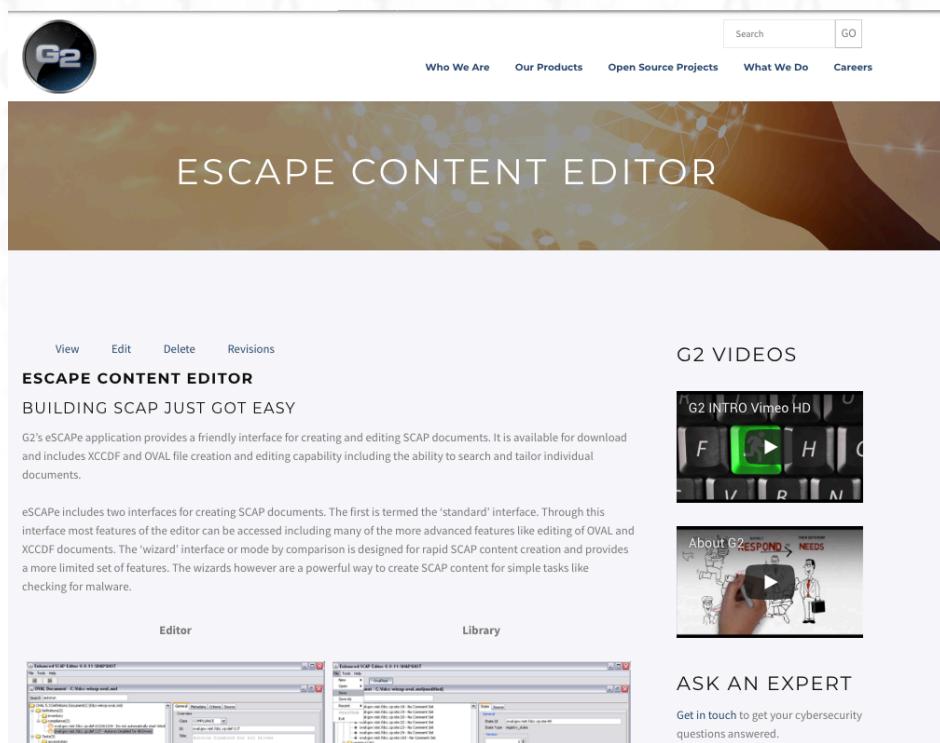
---

1. Download the libraries  
(<https://www.g2-inc.com/escape-content-editor>)
2. Choose a development environment (Example: Eclipse)
3. Install the Java Development kit (JDK)
4. See the documentation on the G2 eSCAPe page under  
'Library-Source' files



# How to get eSCAPe

Released as FREE open source software under the GPLv3 license



The screenshot shows the homepage of the eSCAPE Content Editor. At the top, there's a navigation bar with links for "Who We Are", "Our Products", "Open Source Projects", "What We Do", and "Careers". A search bar with a "GO" button is also present. Below the navigation is a large banner with the text "ESCAPE CONTENT EDITOR" and a background image of a network graph. Underneath the banner, there's a section titled "ESCAPE CONTENT EDITOR" with the sub-section "BUILDING SCAP JUST GOT EASY". It includes a paragraph about the application's features and two screenshots: one of the "Editor" interface showing a complex XML-based configuration window, and one of the "Library" interface showing a catalog of available SCAP content. To the right, there's a "G2 VIDEOS" section with two video thumbnails: "G2 INTRO Vimeo HD" and "About G2 RESPOND NEEDS". At the bottom, there's a "ASK AN EXPERT" section with the text "Get in touch to get your cybersecurity questions answered."

<https://www.g2-inc.com/escape-content-editor>



The screenshot shows the "SCAP Specifications" page from the National Institute of Standards and Technology (NIST). The header reads "National Institute of Standards and Technology" and "Security Content Automation Protocol". The left sidebar has a navigation menu with links for "Home", "Publications", "Balanced Cycle", "SCAP Validation", "SCAP Content", "SCAP Specifications", "SCAP 1.3 (Draft)", "SCAP 1.0", "Events", "Community", and "Emerging Specifications". The main content area is titled "SCAP Specifications" and contains information about the evolution of SCAP. It states: "SCAP must continually evolve to meet the ever changing needs of the community. The need for continued evolution results in multiple versions of SCAP being available at any given time. The [SCAP Release Cycle](#) defines a process for managing change relating to SCAP and the NIST SCAP Validation Program by providing a consistent and repeatable review work flow." Below this, it says: "The following list represents the currently available versions of SCAP. The current effective version of SCAP is [1.0](#)". There are sections for "Protocol" (listing SCAP 1.1, SCAP 1.0, and SCAP 0.9), "Content Development Tools" (listing the SCAP Content Validation Tool and Enhanced SCAP Editor (eSCAPe)), and "Community" (linking to the GitHub project site).

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

# Contact Information

**G2 Support**

[info@g2-inc.com](mailto:info@g2-inc.com)

**How to get eSCAPe**

<https://www.g2-inc.com/escape-content-editor>

