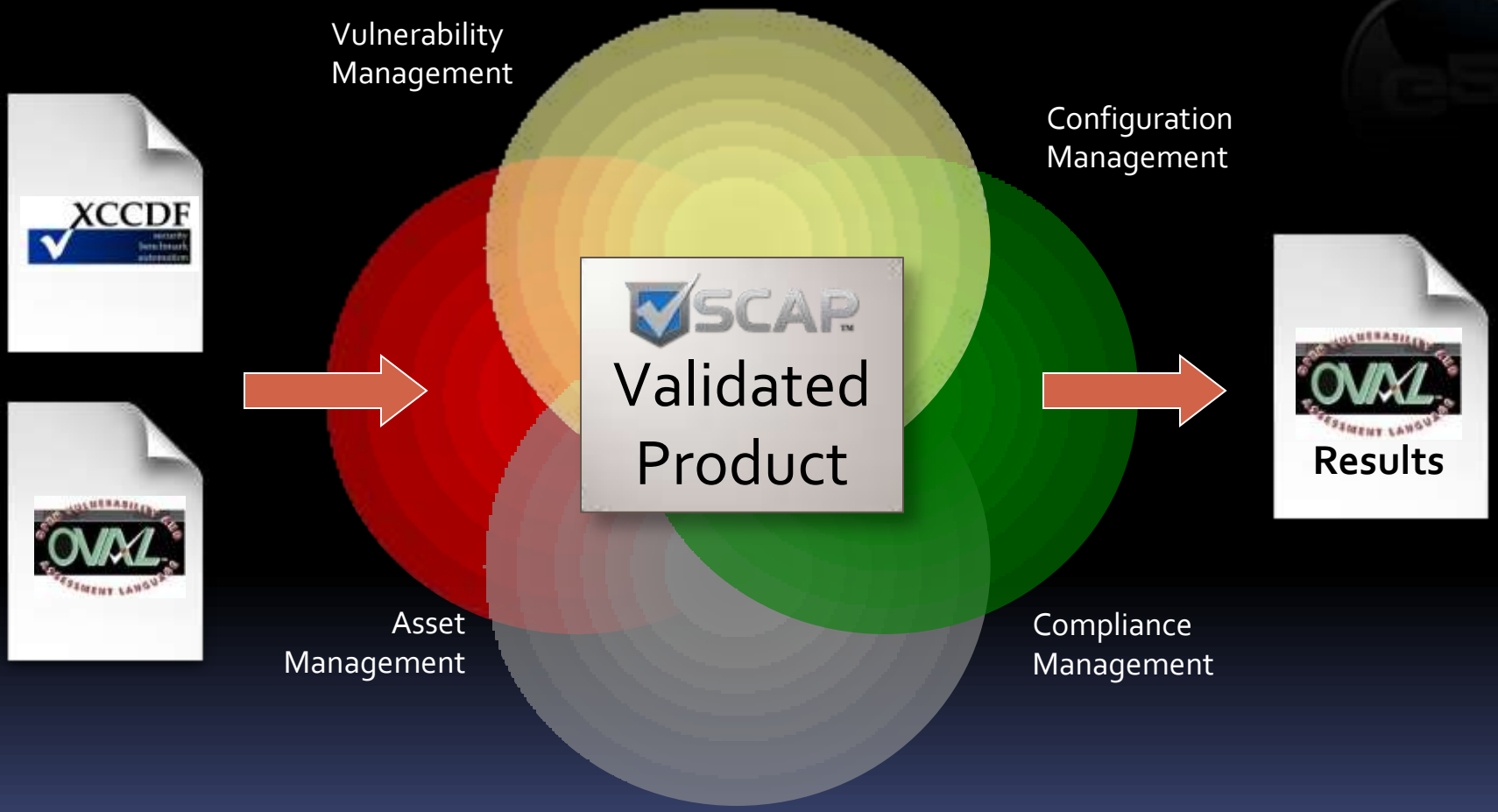
The Enhanced SCAP Editor (eSCAPe) and Libraries

It all depends on SCAP Content



See list of SCAP Validated tols 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.o</version>
    <Profile id="malware_content_2010">
        <title>Malware Content 2010</title>
        <description>Malware dontent 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

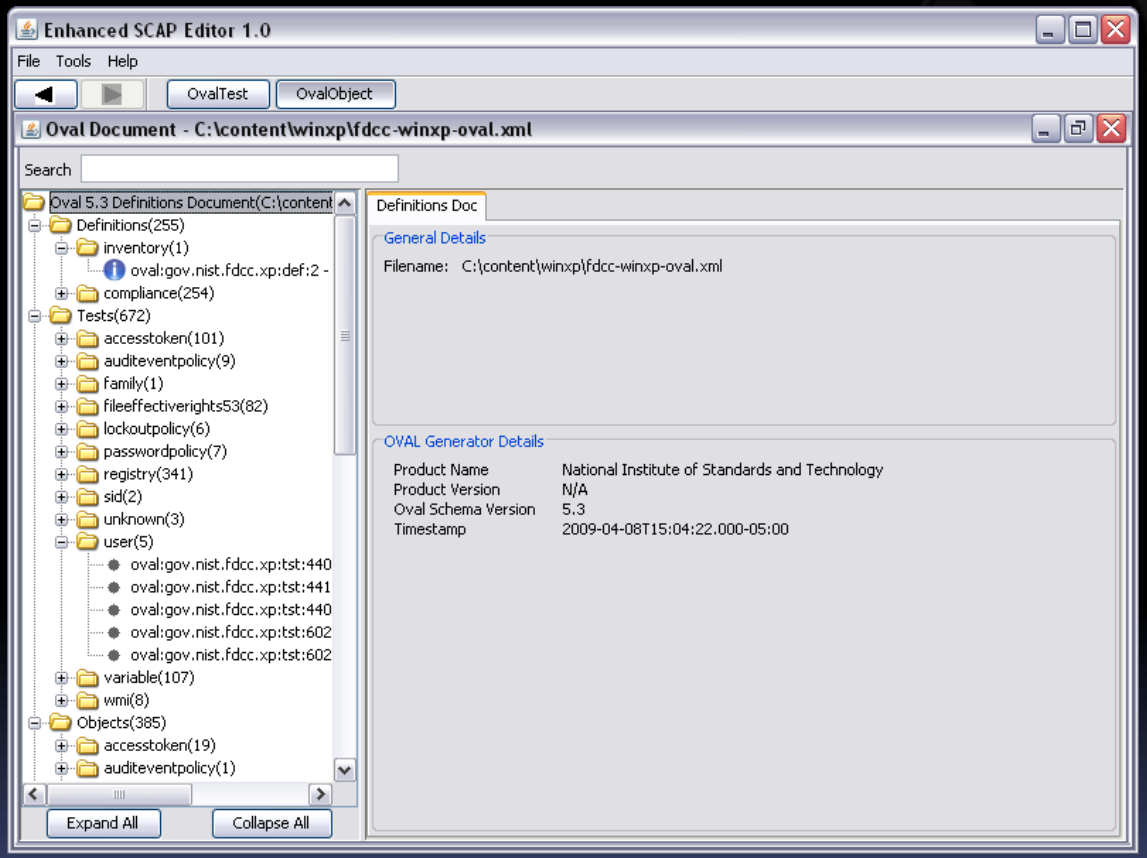
```
<definitions>
    <definition id="oval:test.g2.com:def:1" class="vulnerability">
        <metadata>
            <title>File test for malicious file 34564.exe</title>
            <description>Checking for malicious file named 34564.exe</description>
            <affected family="windows">
                <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

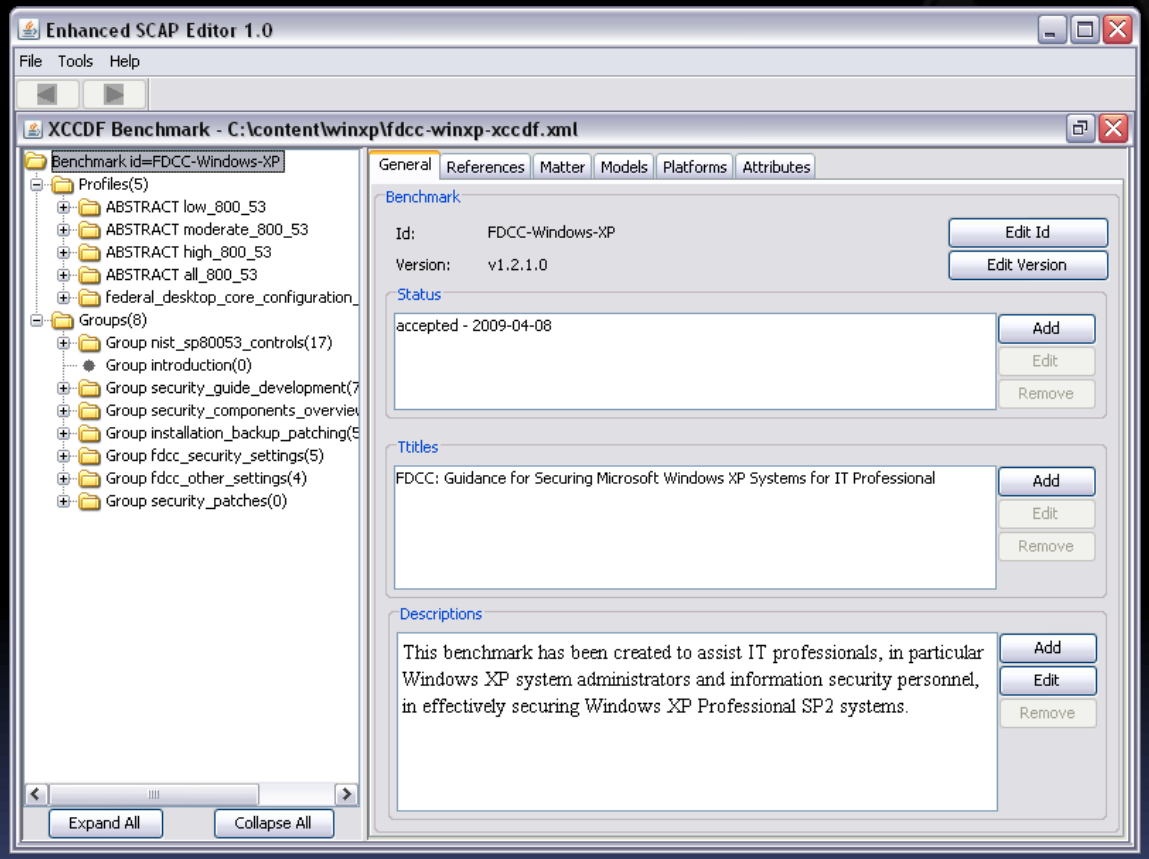
eSCAPe Editor - OVAL Editor

- 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 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

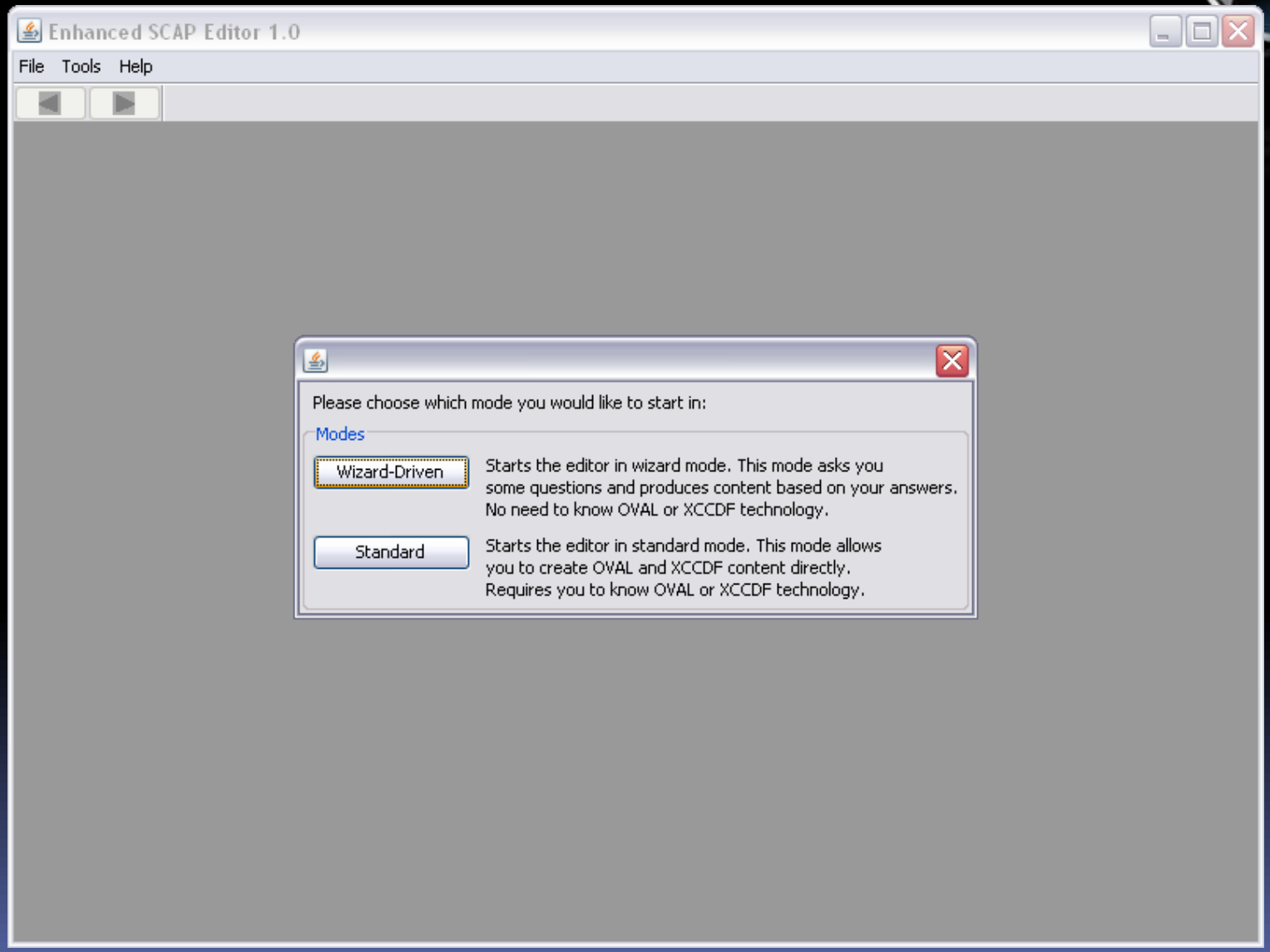
Checking Conficker.A Vulnerability

CVE-2008-4250 - Microsoft Server Service Remote Code Execution Vulnerability

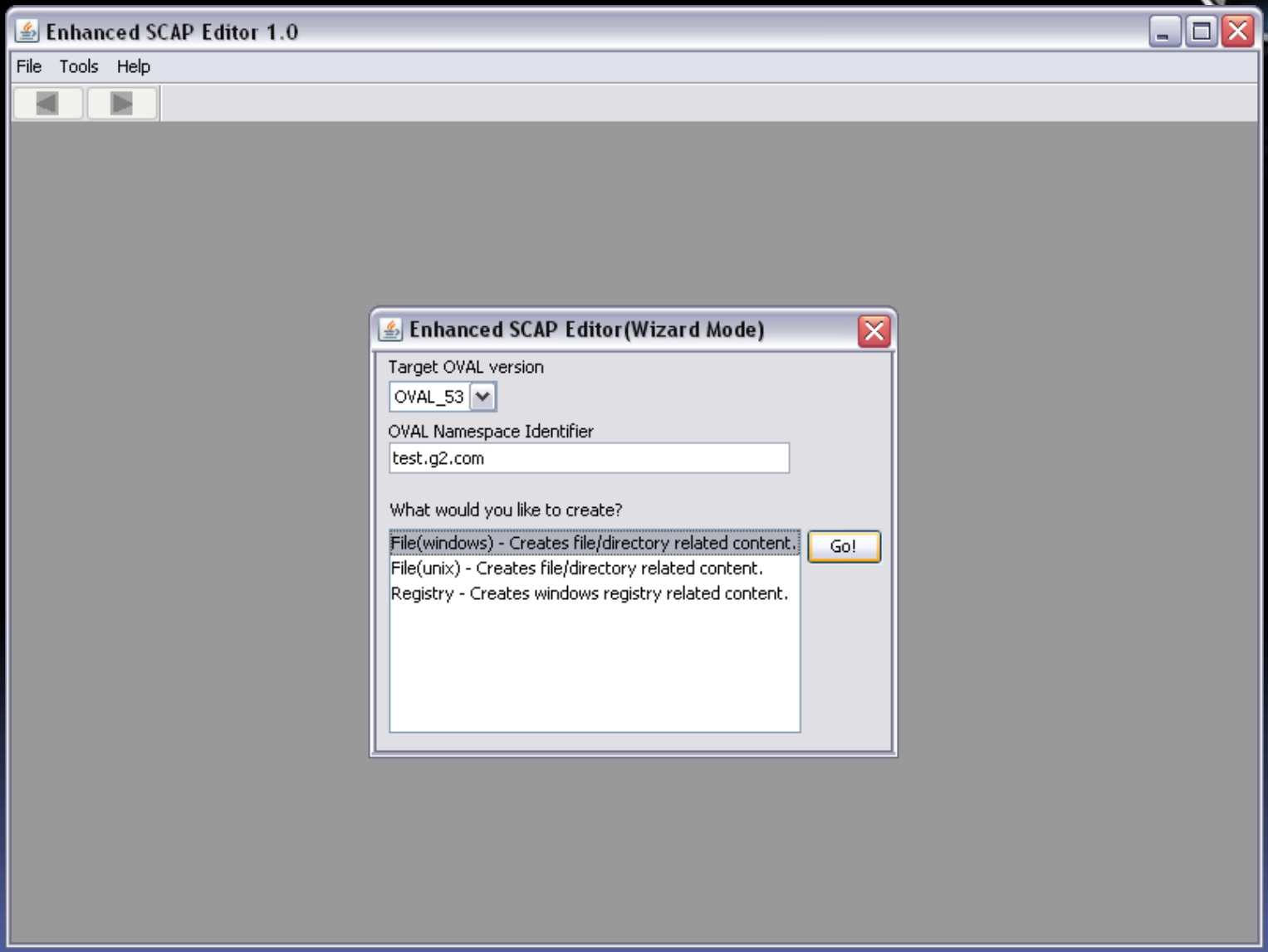
1. Microsoft Windows XP (x86) SP3 is installed
2. **%systemroot%\Netapi32.dll version is less than 5.1.2600.5694**

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

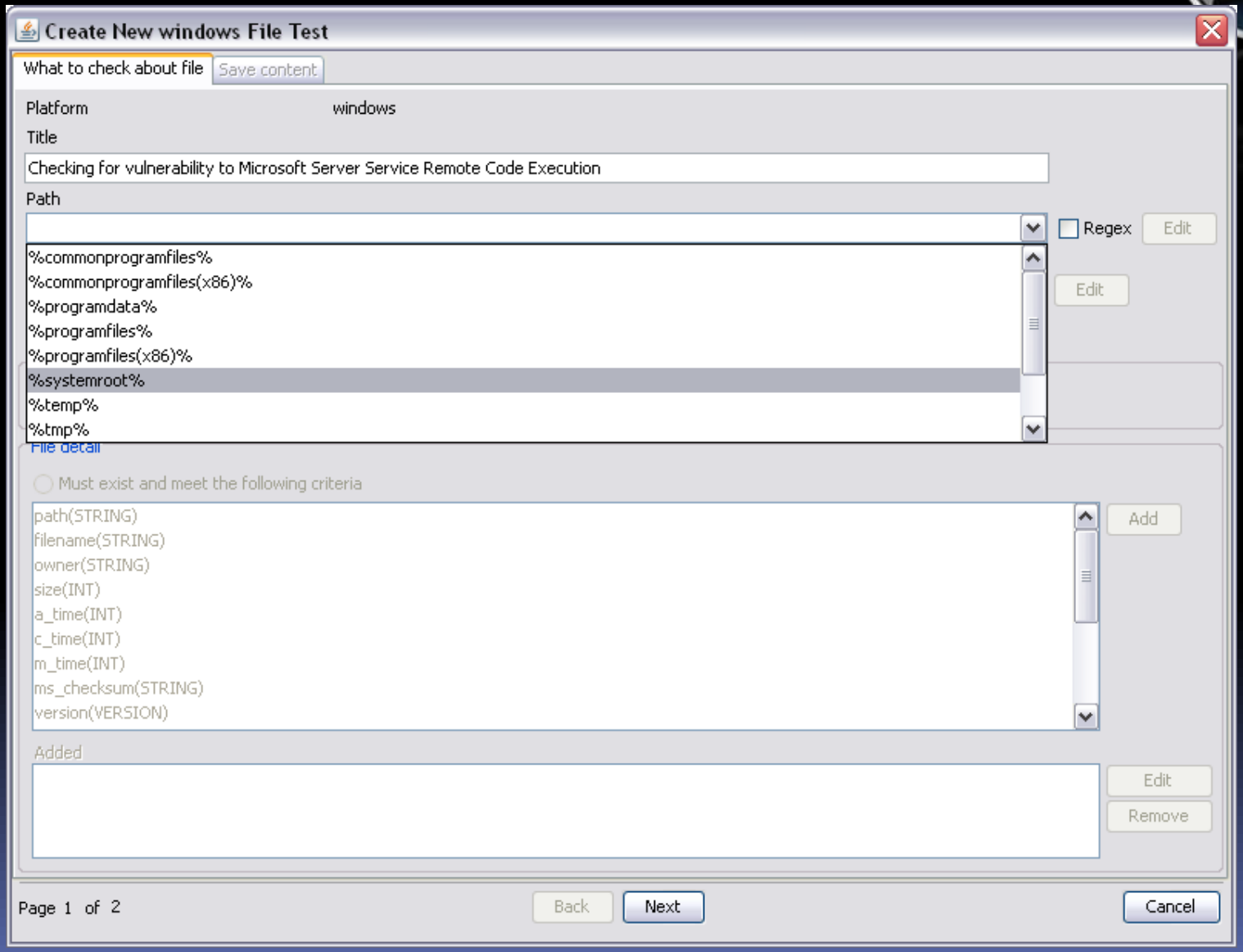
Start eSCAPe & Enter Wizard Mode



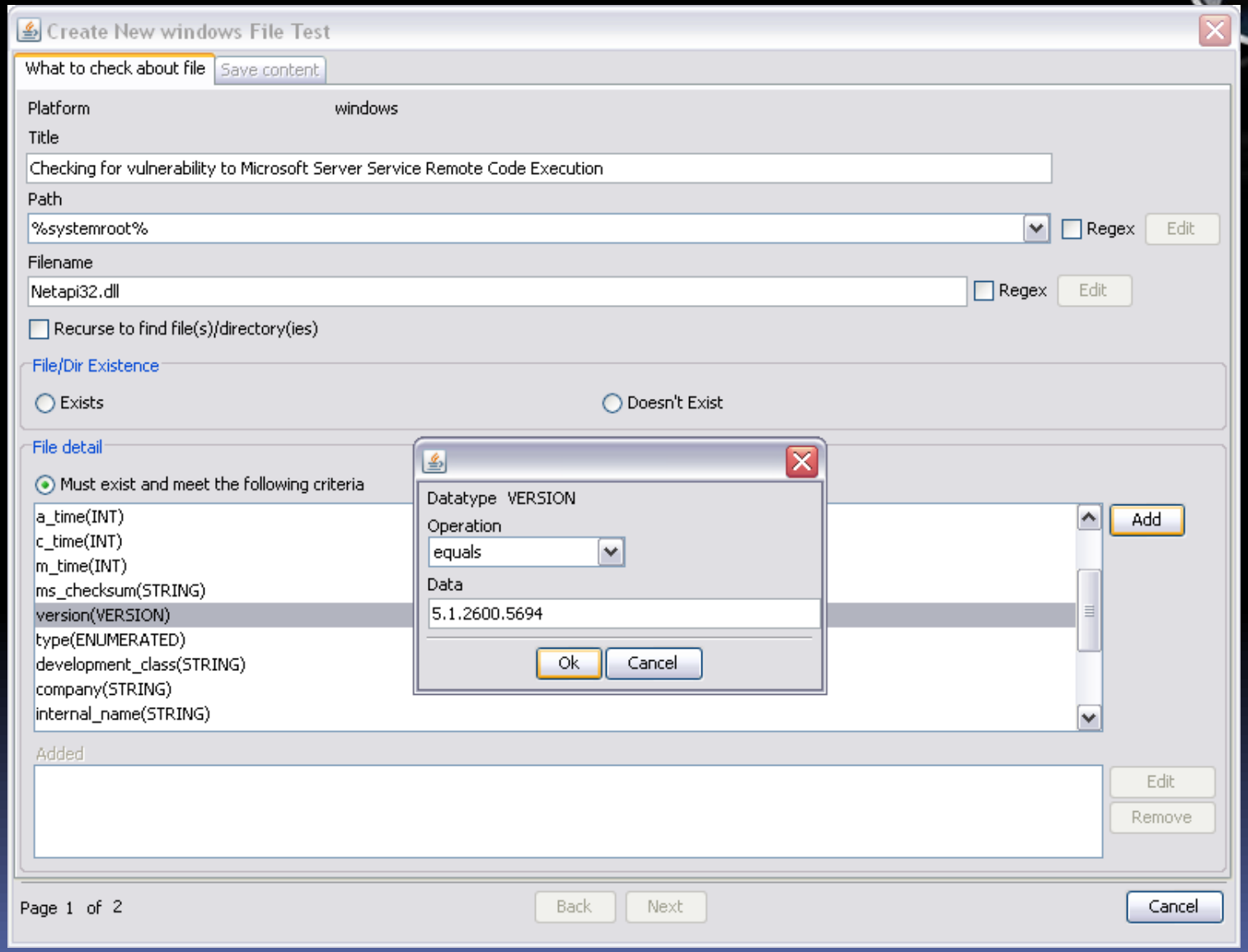
Select the File Test Wizard



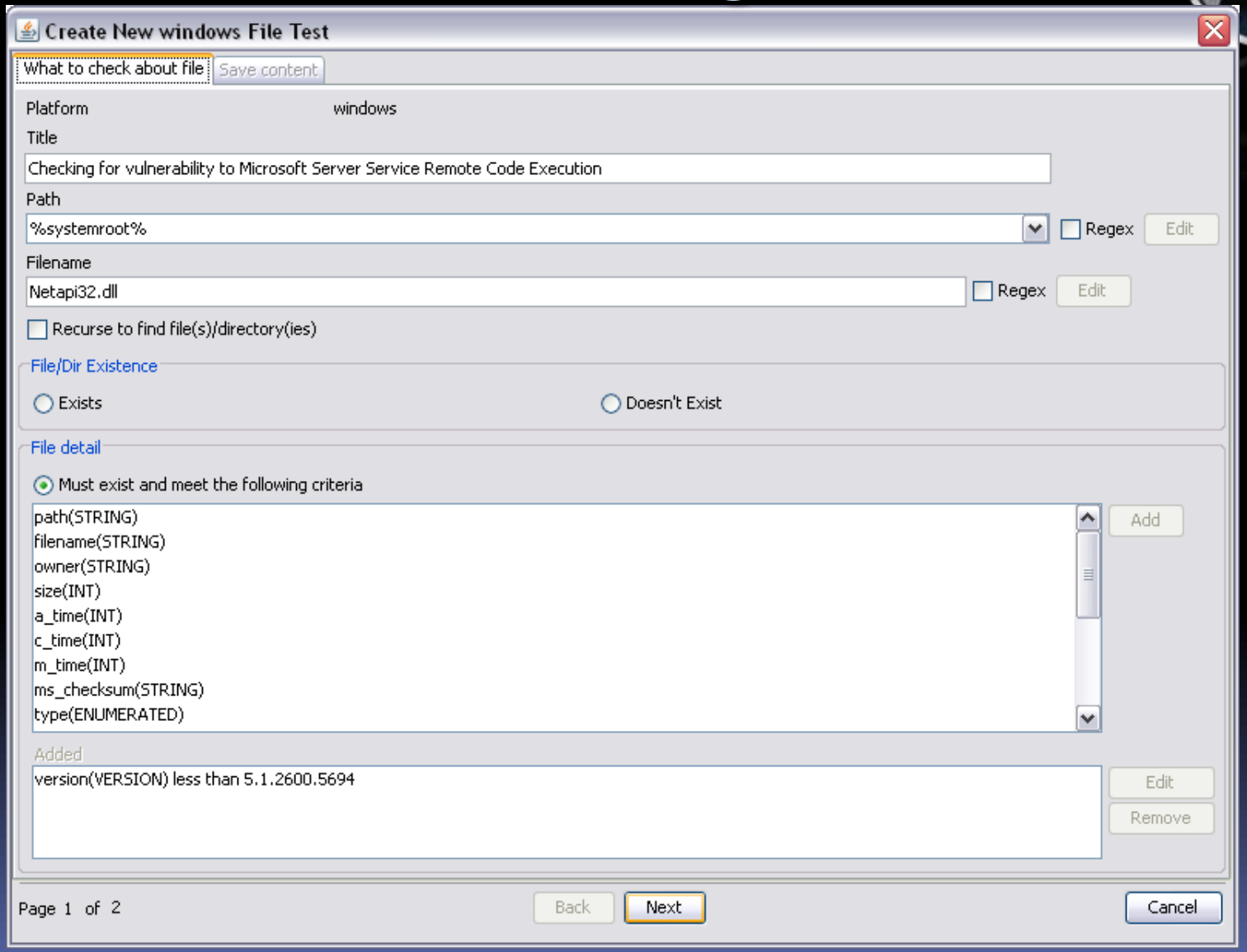
Enter Test Information



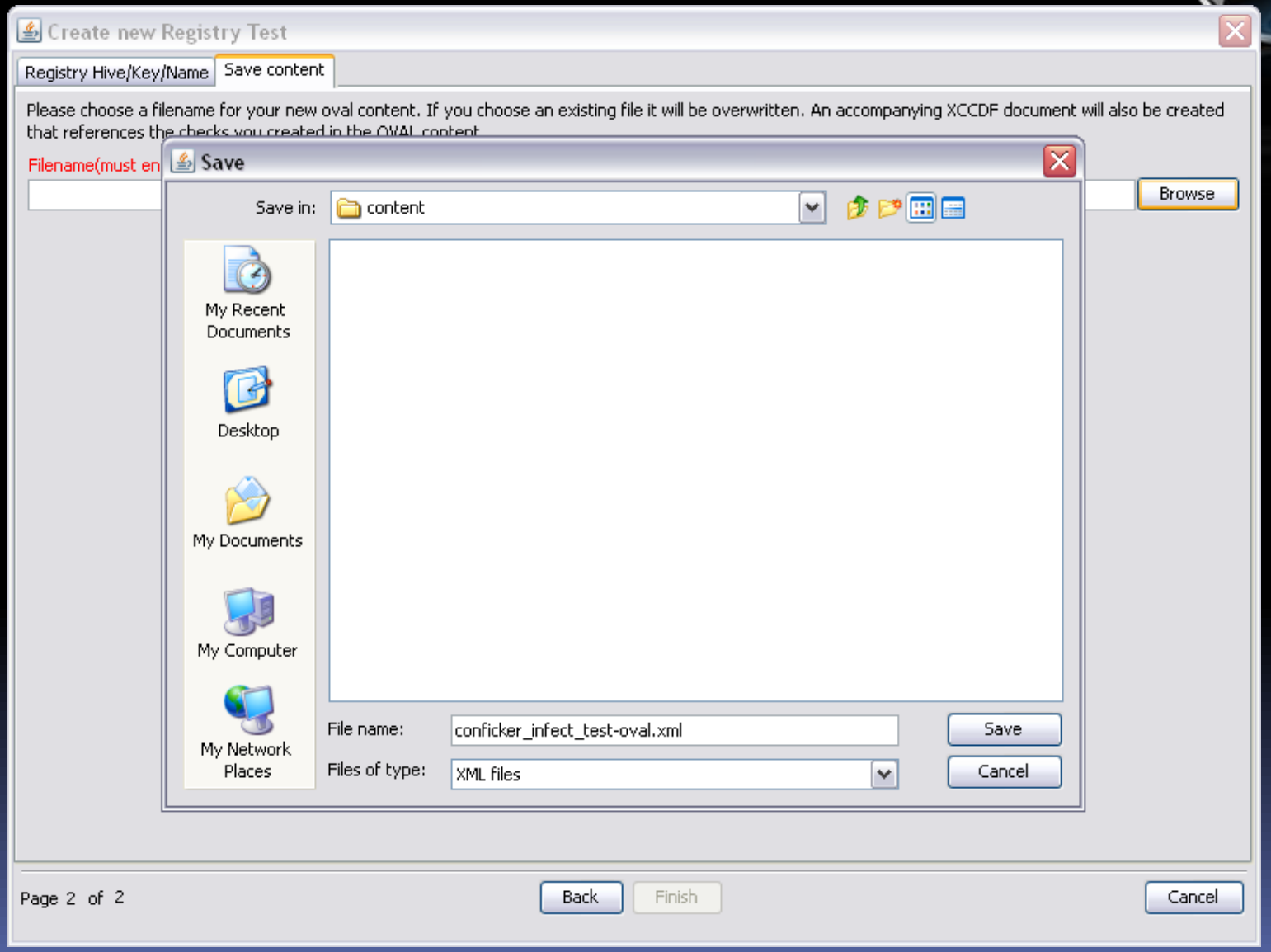
Enter Test Information (2)



Enter Test Information (3)



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**

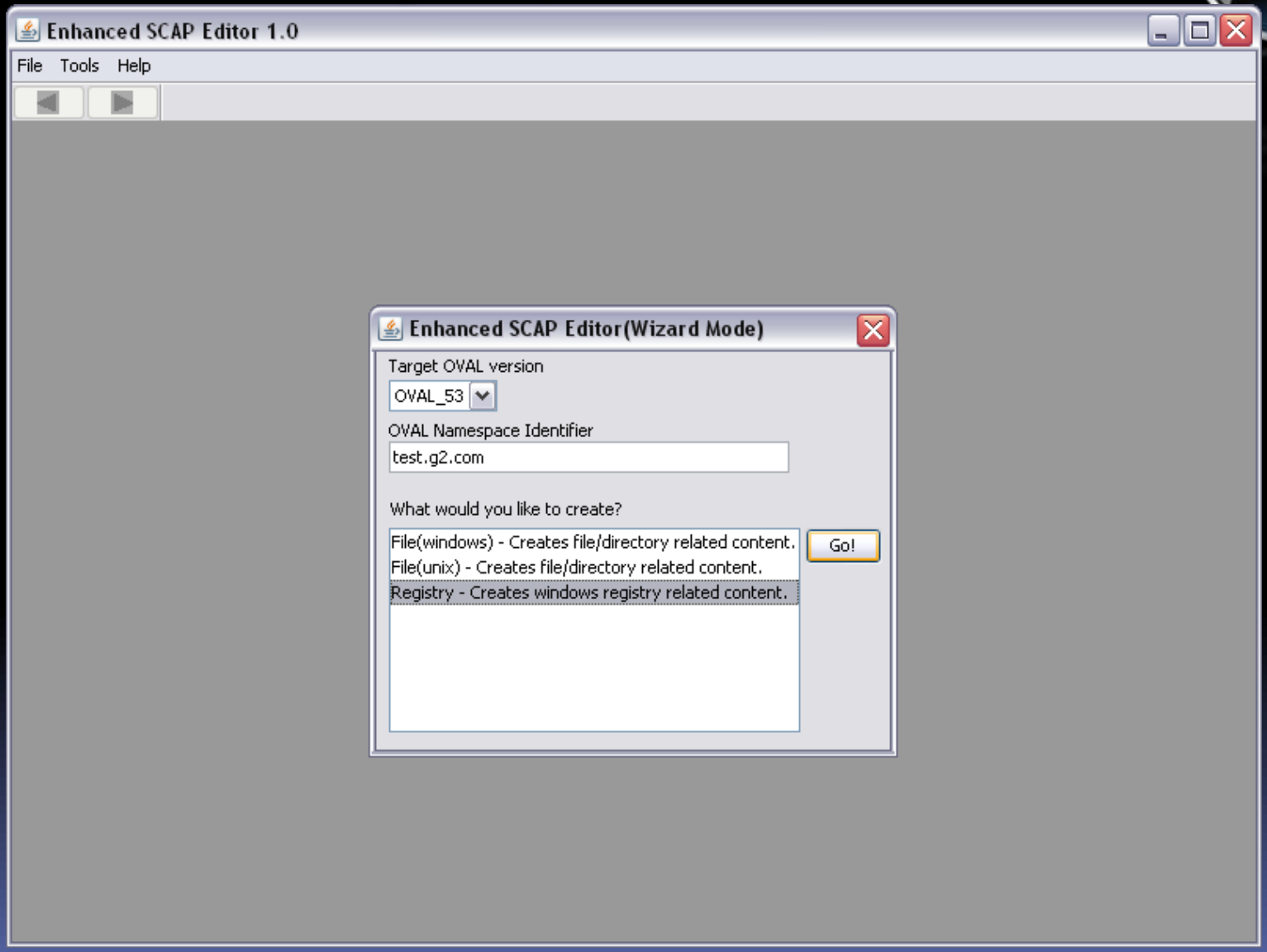
   ***Name*: ServiceDll**

   ***Value (data):* %systemroot%\nxyme.dll**

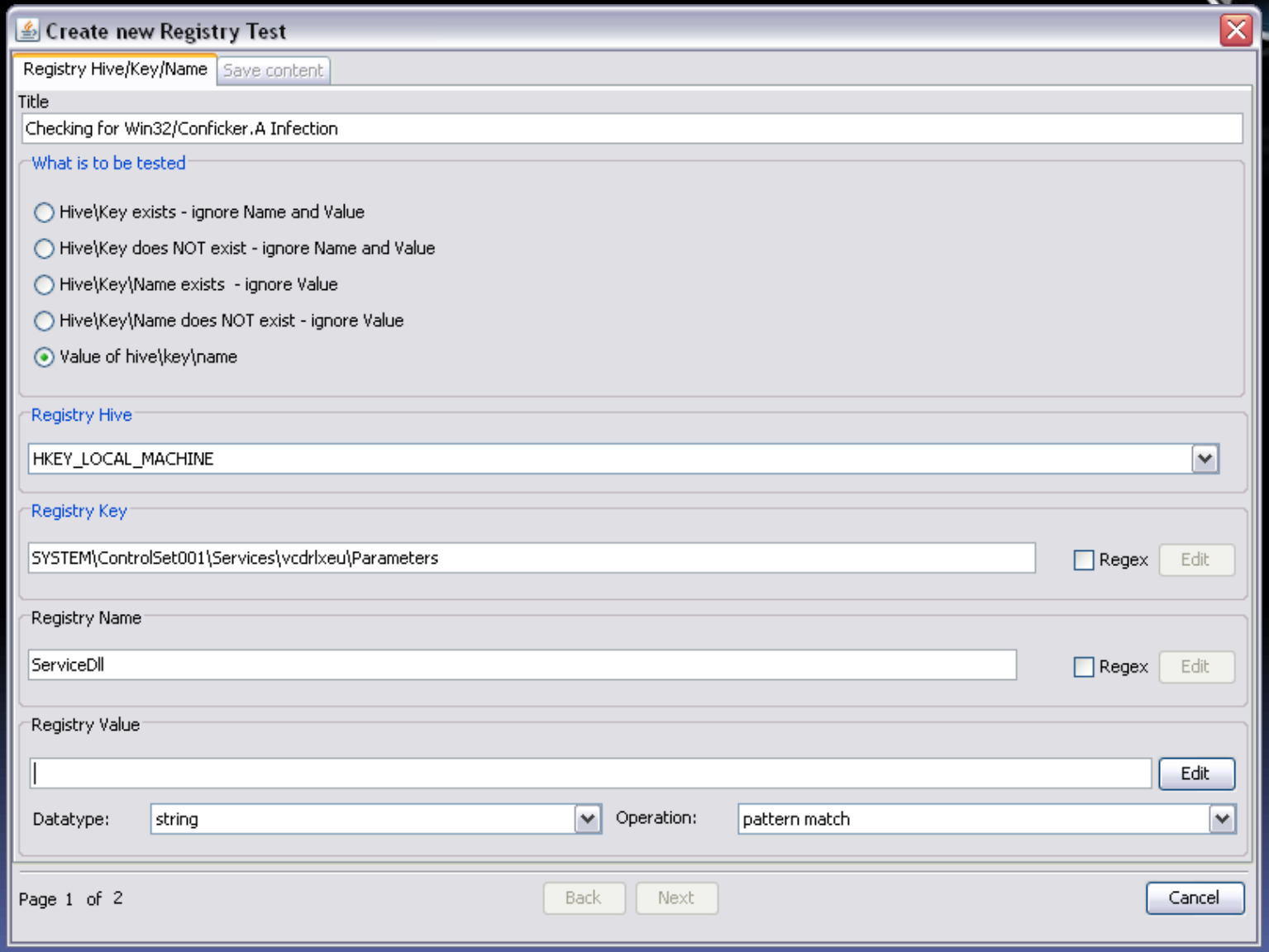
- **where 'nxyme.dll' is <*random*>.dll, with <*random*> as a 5-8 character lowercase alphabetic name.**

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

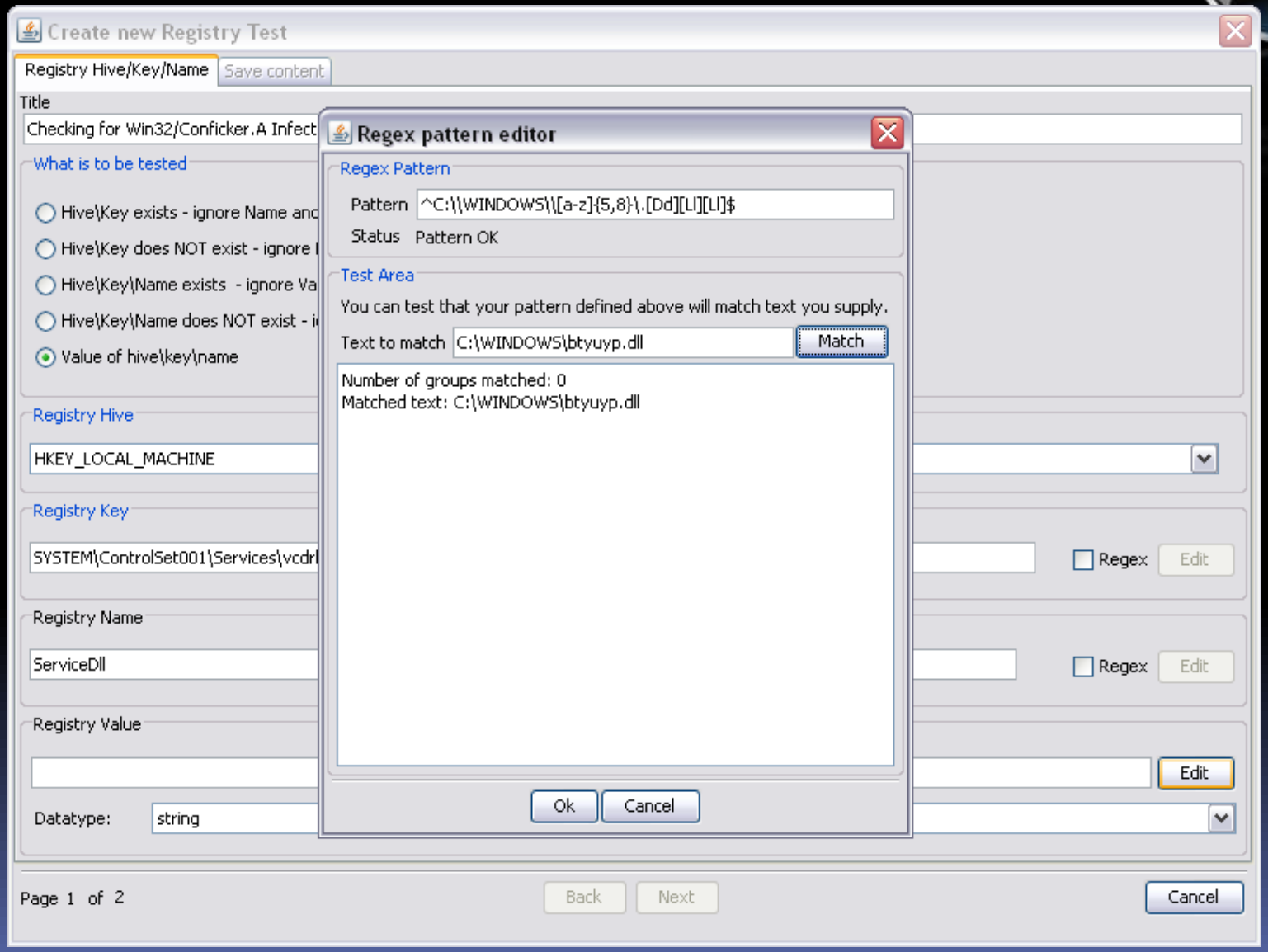
Select the Registry Wizard



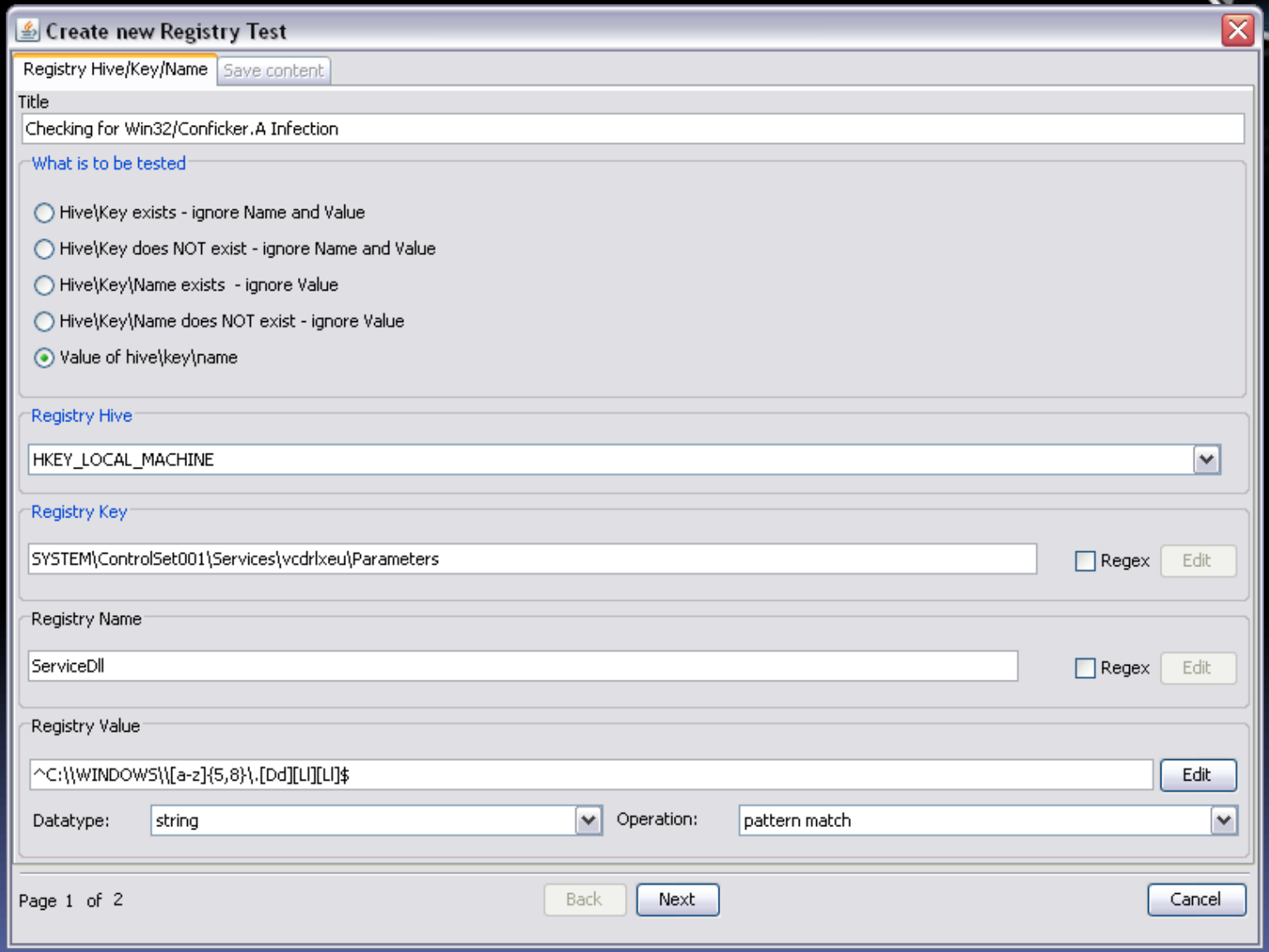
Enter Test Information



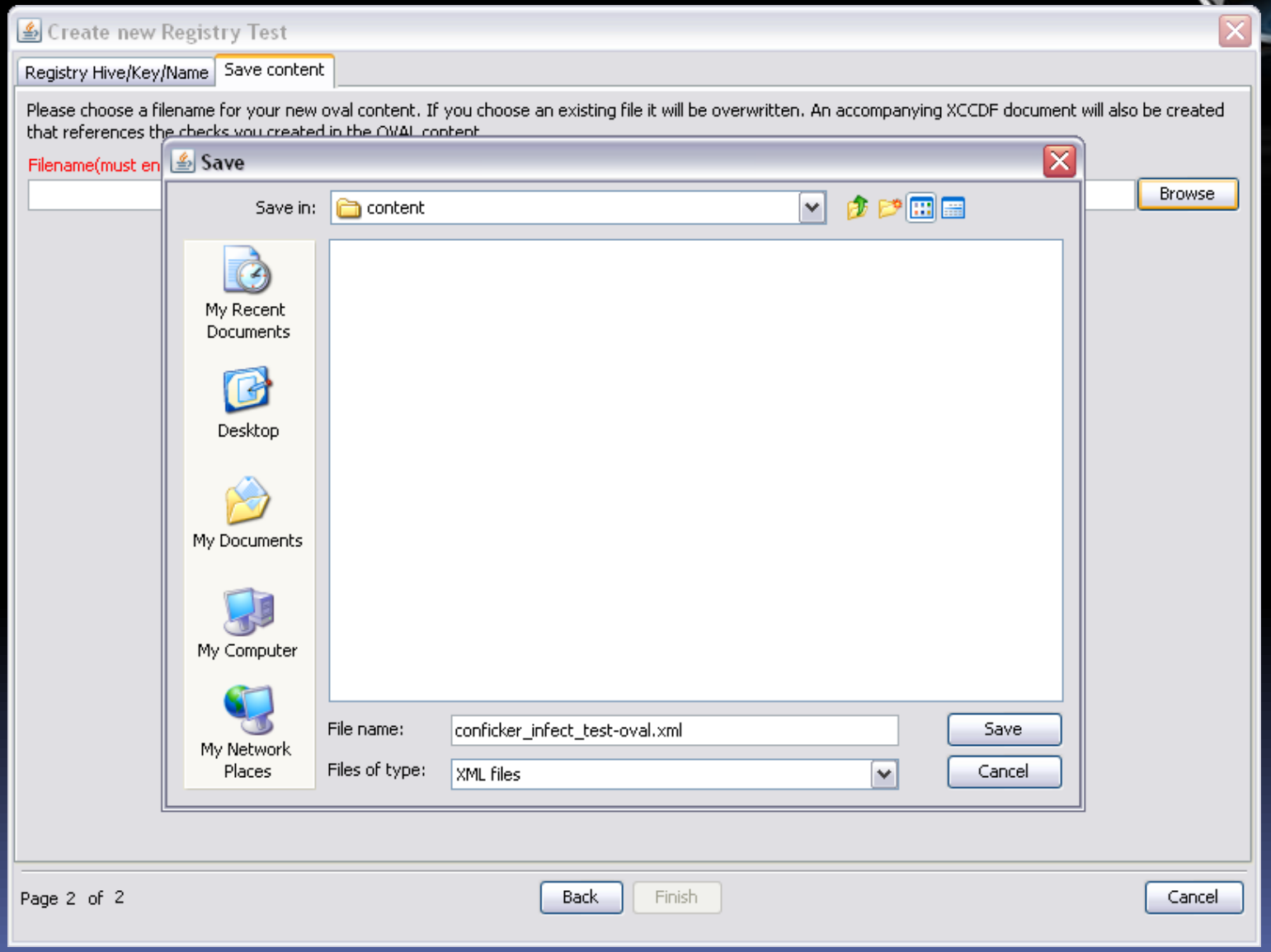
Enter Test Information (2)



Enter Test Information (3)



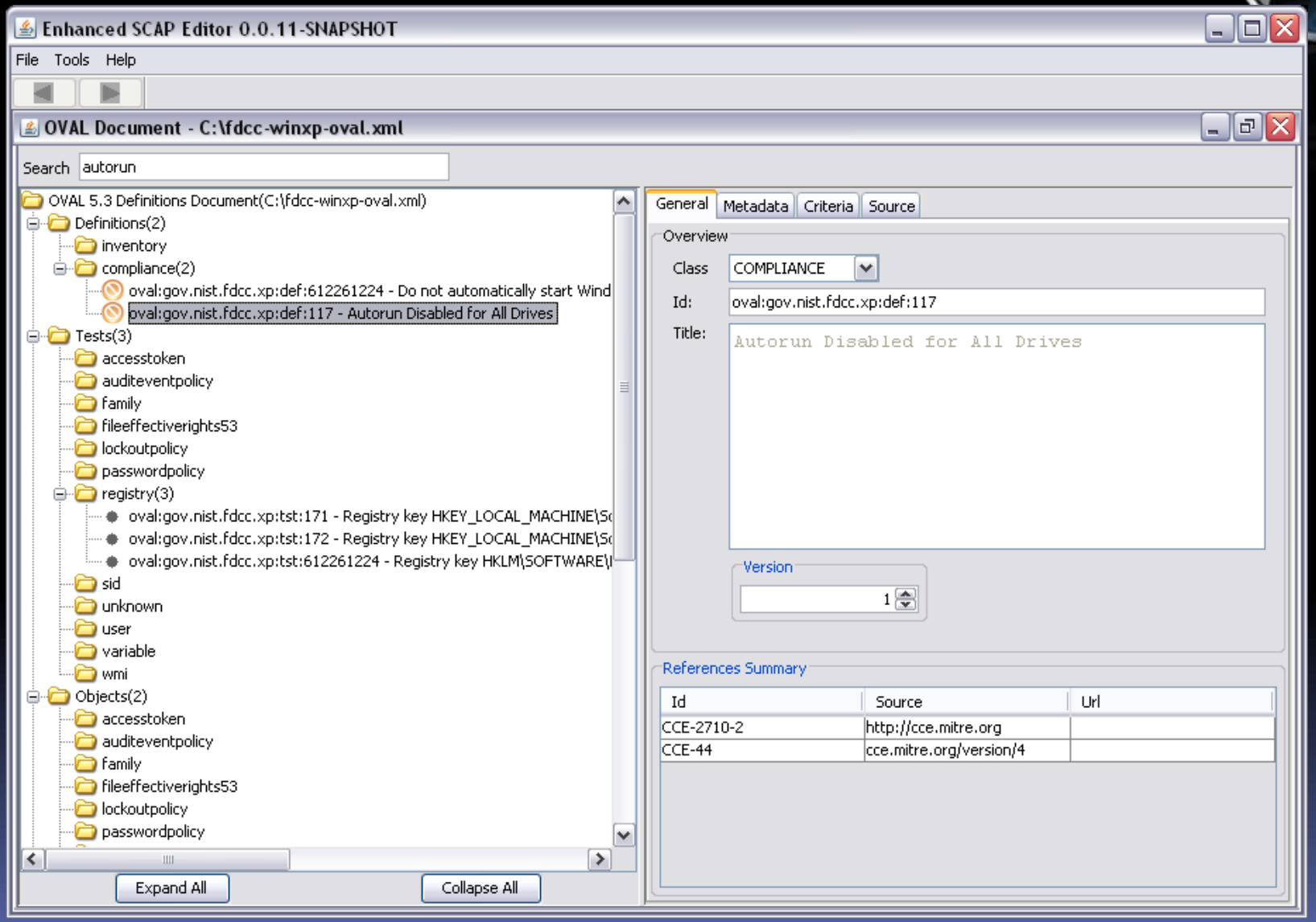
Save OVAL File – Create XCCDF



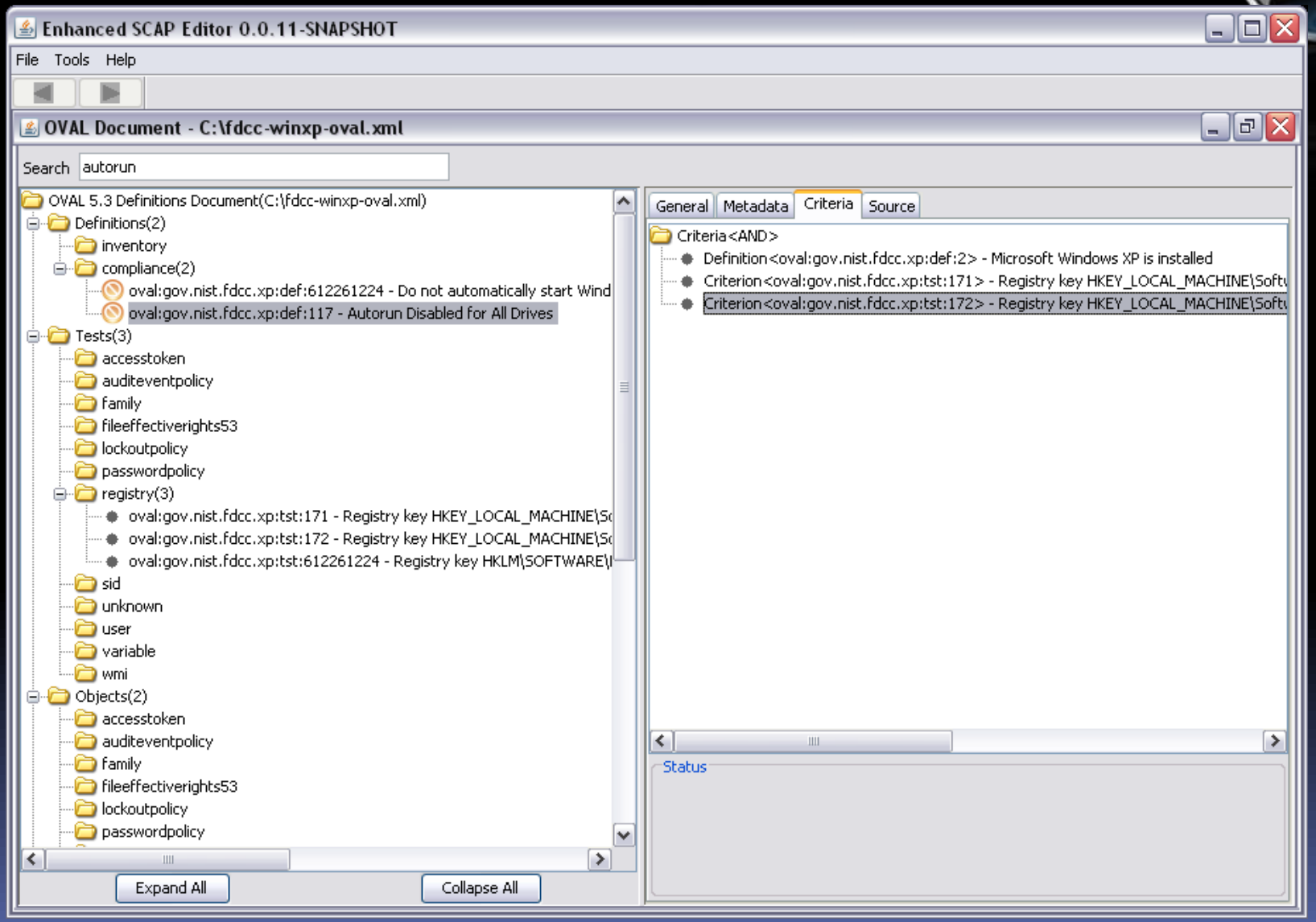
Benchmark "Critical-controls" Tailoring using eSCAPe

- 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

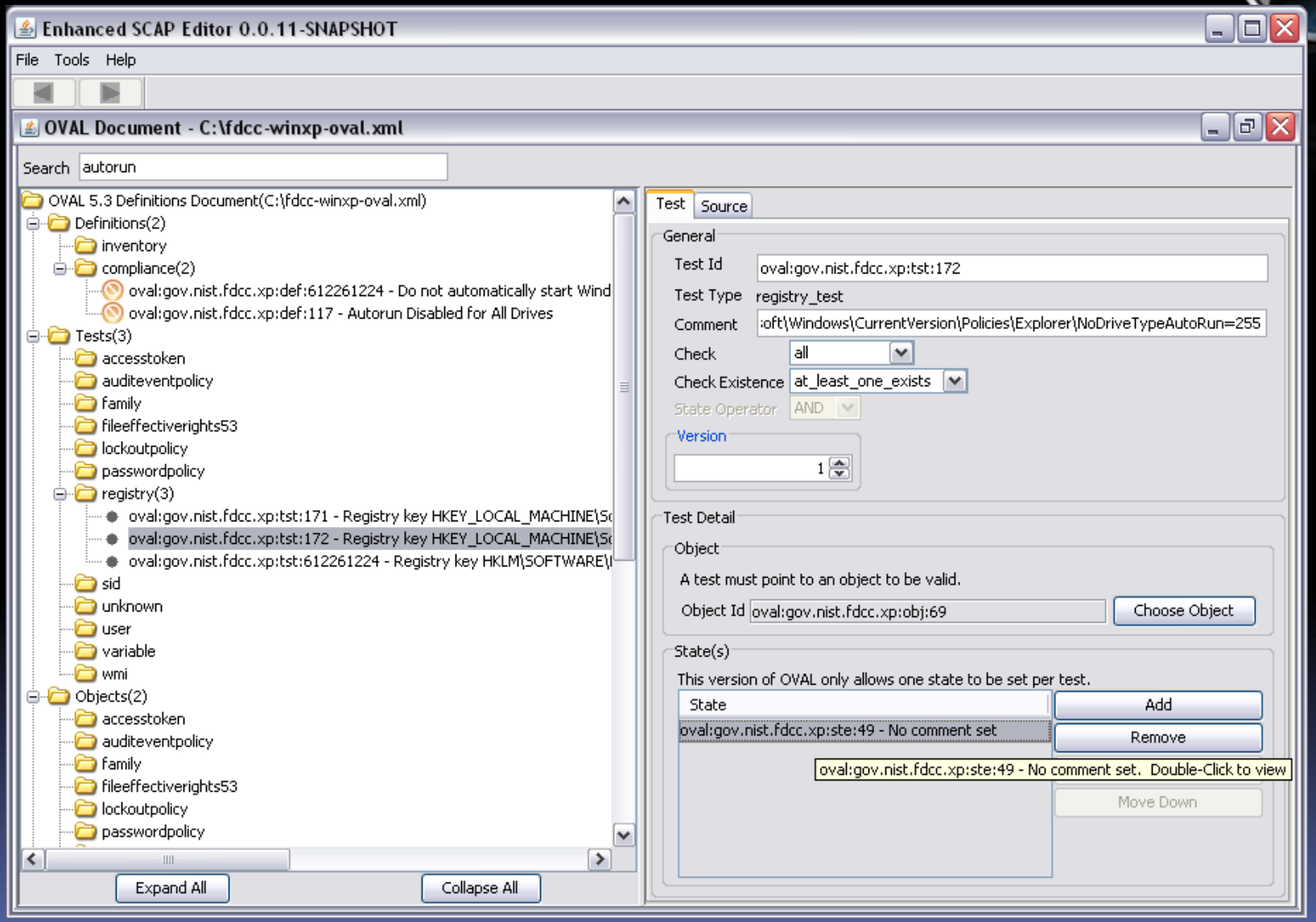
Open OVAL File in eSCAPe



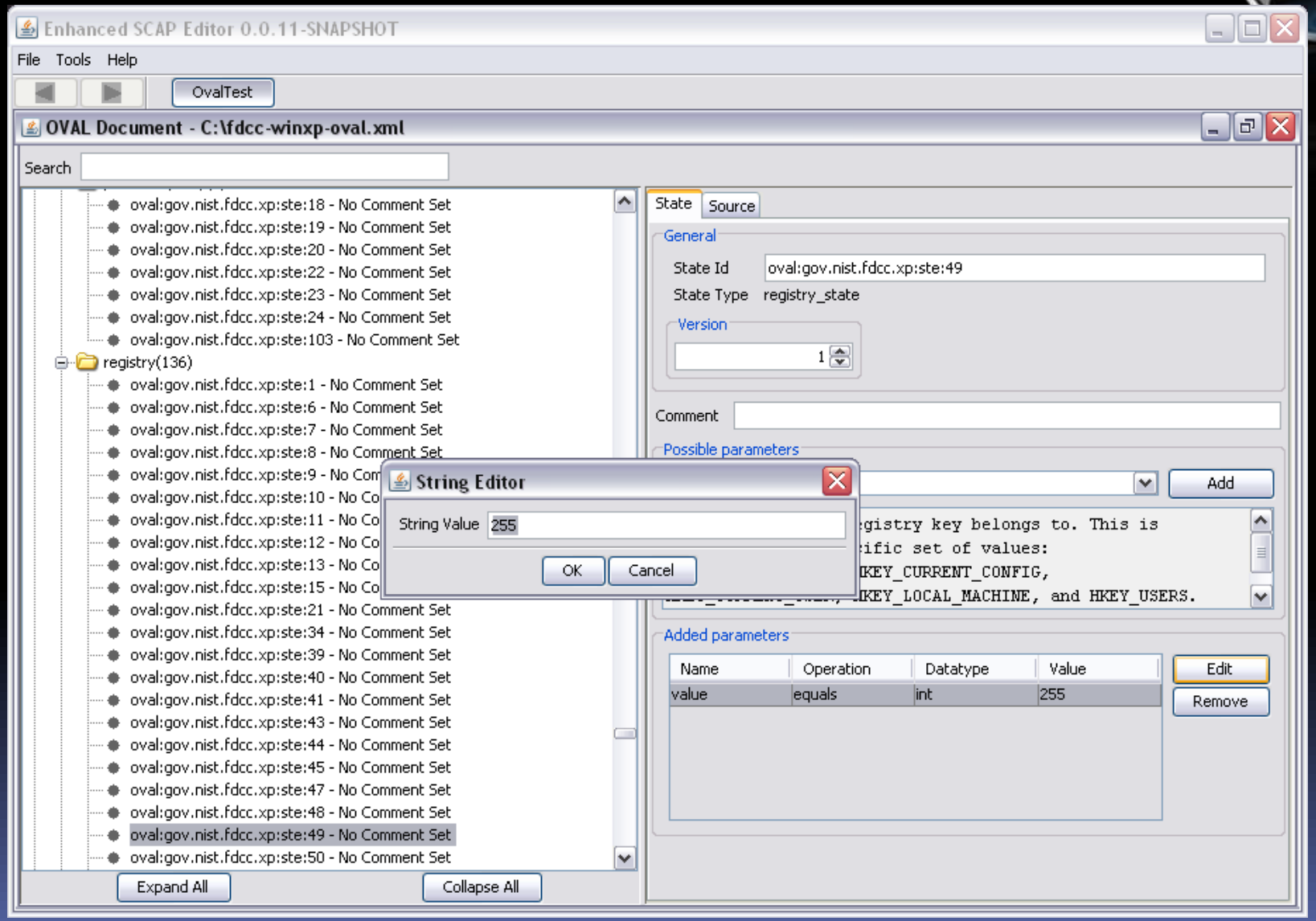
Identify Test to be Adjusted



Select OVAL Test State to Edit



Navigate to State and click 'Edit'

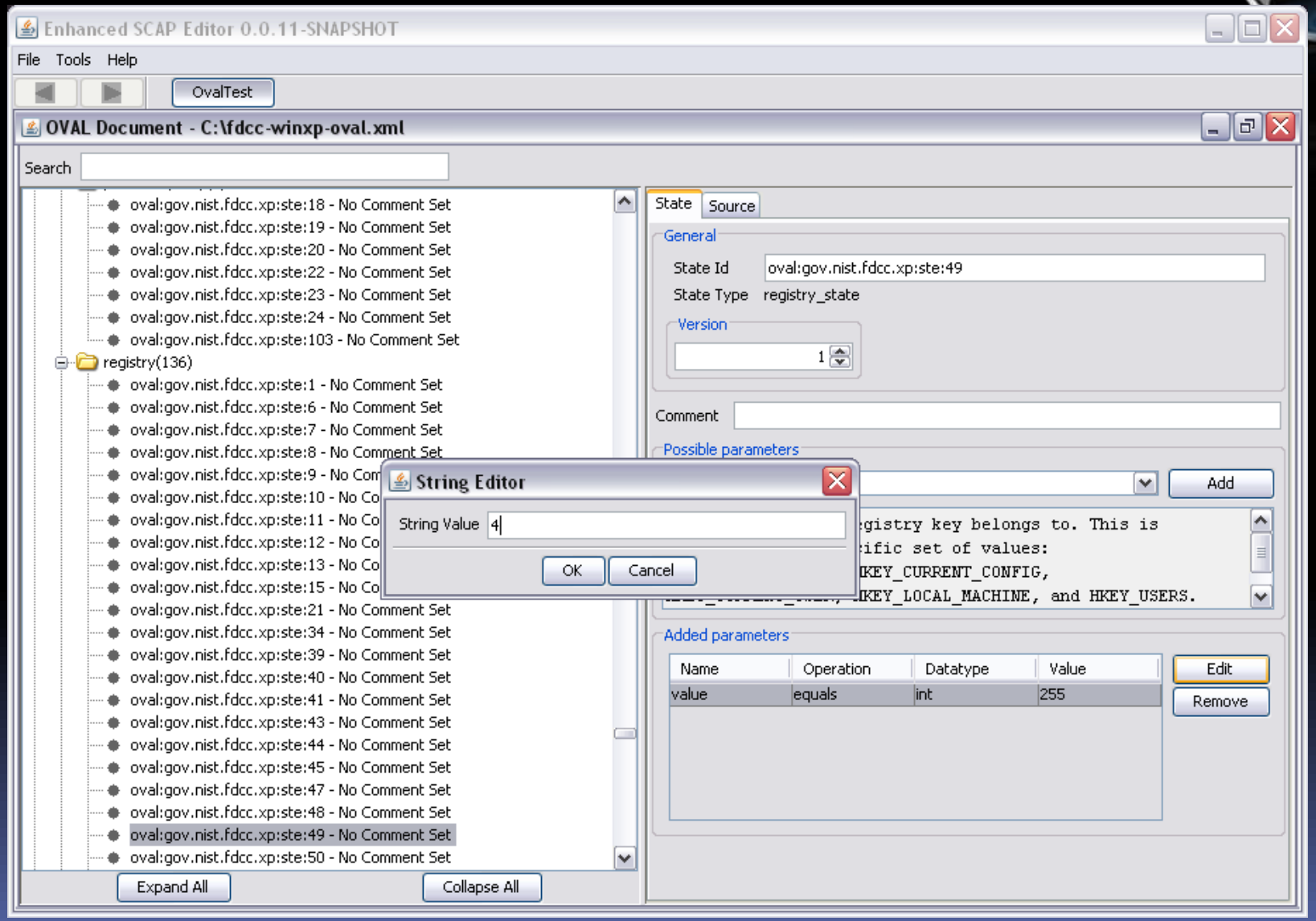


Autoplay Setting Values

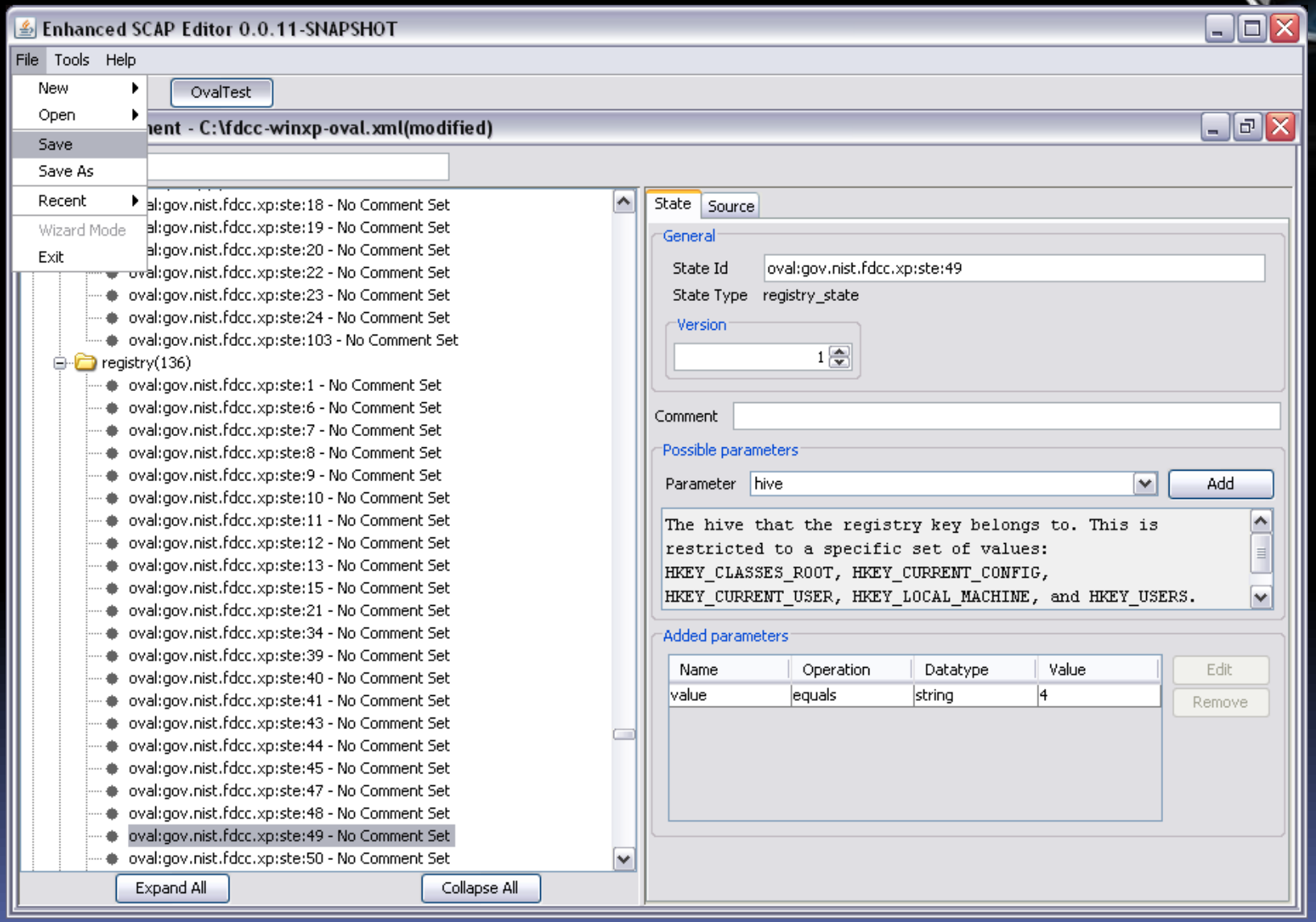
- Microsoft documentation of Autoplay registry value settings

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



Save Customized Benchmark



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

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

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