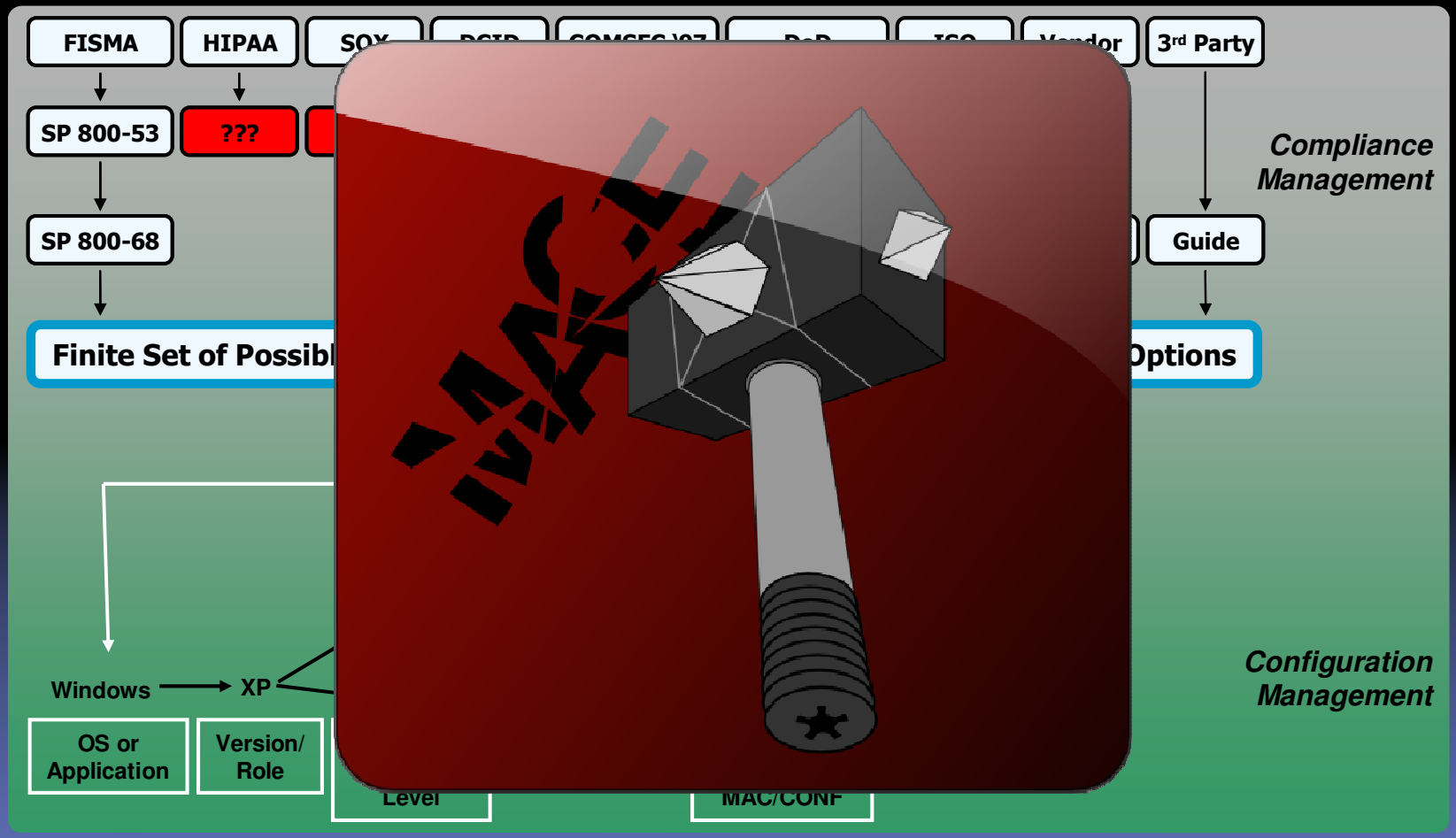
MAlware Content Editor

Acronyms

CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OVAL	Open Vulnerability Assessment Language
SCAP	Security Content Automation Protocol
XCCDF	eXtensible Checklist Configuration Description Format
XML	Extensible Markup Language

We're not talking about nothin' bad Compliance Management here.



XCCDF & OVAL for Maximum Compliance

XCCDF

OVAL

The OVAL language

- A collection of XML schema for representing system information, expressing specific machine states, and reporting the results of an assessment.[1]

[1] http://oval.mitre.org/

Malware Example

When executed, the worm copies itself as the following files:

%System%\jushed.exe

%System%\java2.exe

%Windir%\jvm.exe

It then creates the following files, which are copies of packed.Generic.238:

%System%\SKYNET[RANDOM LETTERS].dll

%System%\SKYNET[RANDOM LETTERS].dll

%System%\drivers\SKYNE[RANDOM LETTERS].sys

It creates the following clean files:

%Windir%\java.ini

%System%\SKYNET[RANDOM LETTERS].dat

%System%\SKYNETlog.dat

Malware Example

It then creates the following registry entries so that it runs every time Windows starts:

HKEY_CURRENT_USER\Software\Microsoft\Windows

\CurrentVersion\Policies\Explorer\Run

\"Windows Audio Services" = "%Windir%\jvm.exe"

HKEY_CURRENT_USER\Software\Microsoft\Windows

\CurrentVersion\Run\"SunJavaUpdateSched10" = "%System%\jushed.exe"

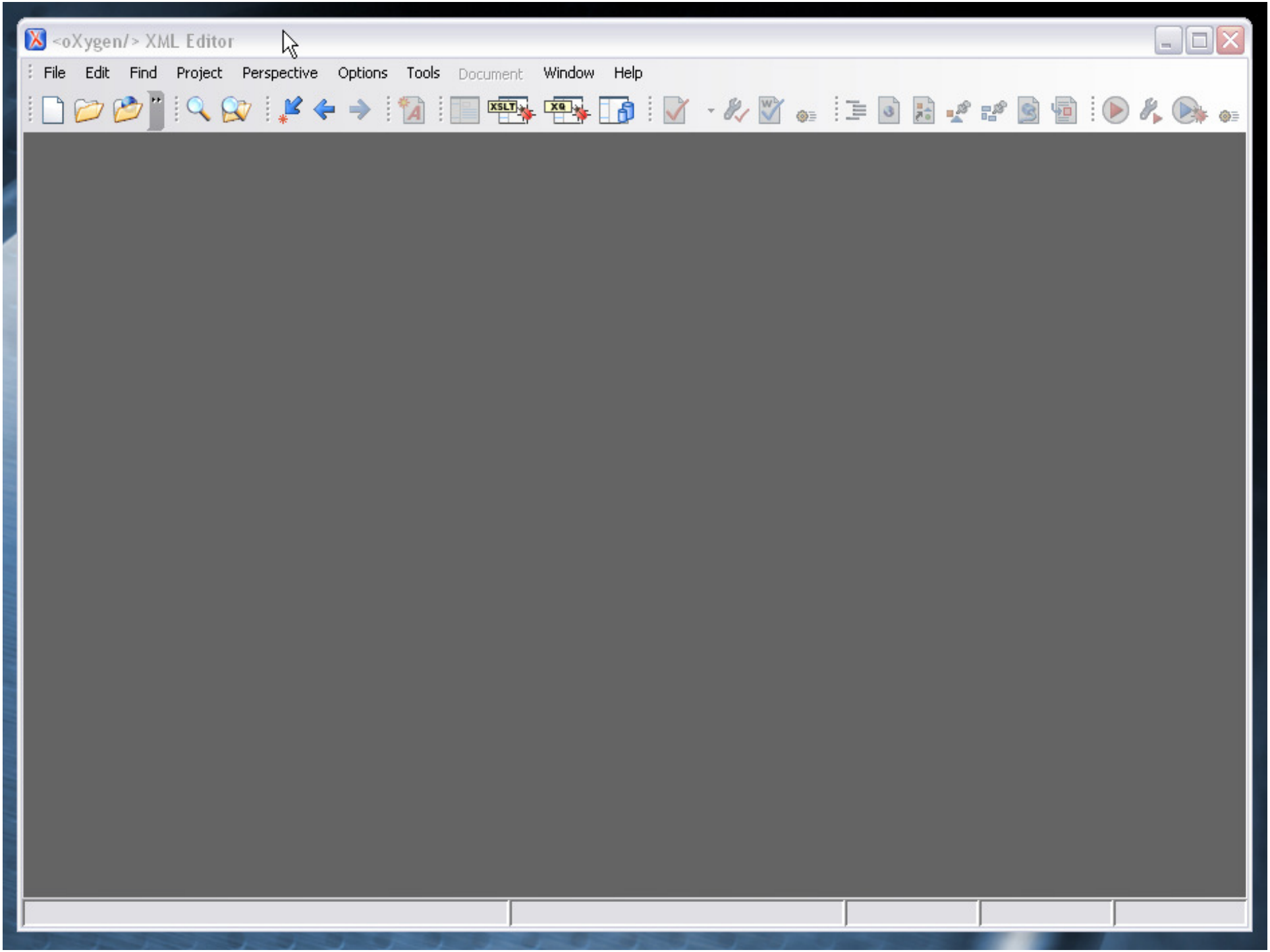
HKEY_CURRENT_USER\Software\Microsoft\Windows

\CurrentVersion\Run\"Windows Audio Services" = "%Windir%\jvm.exe"

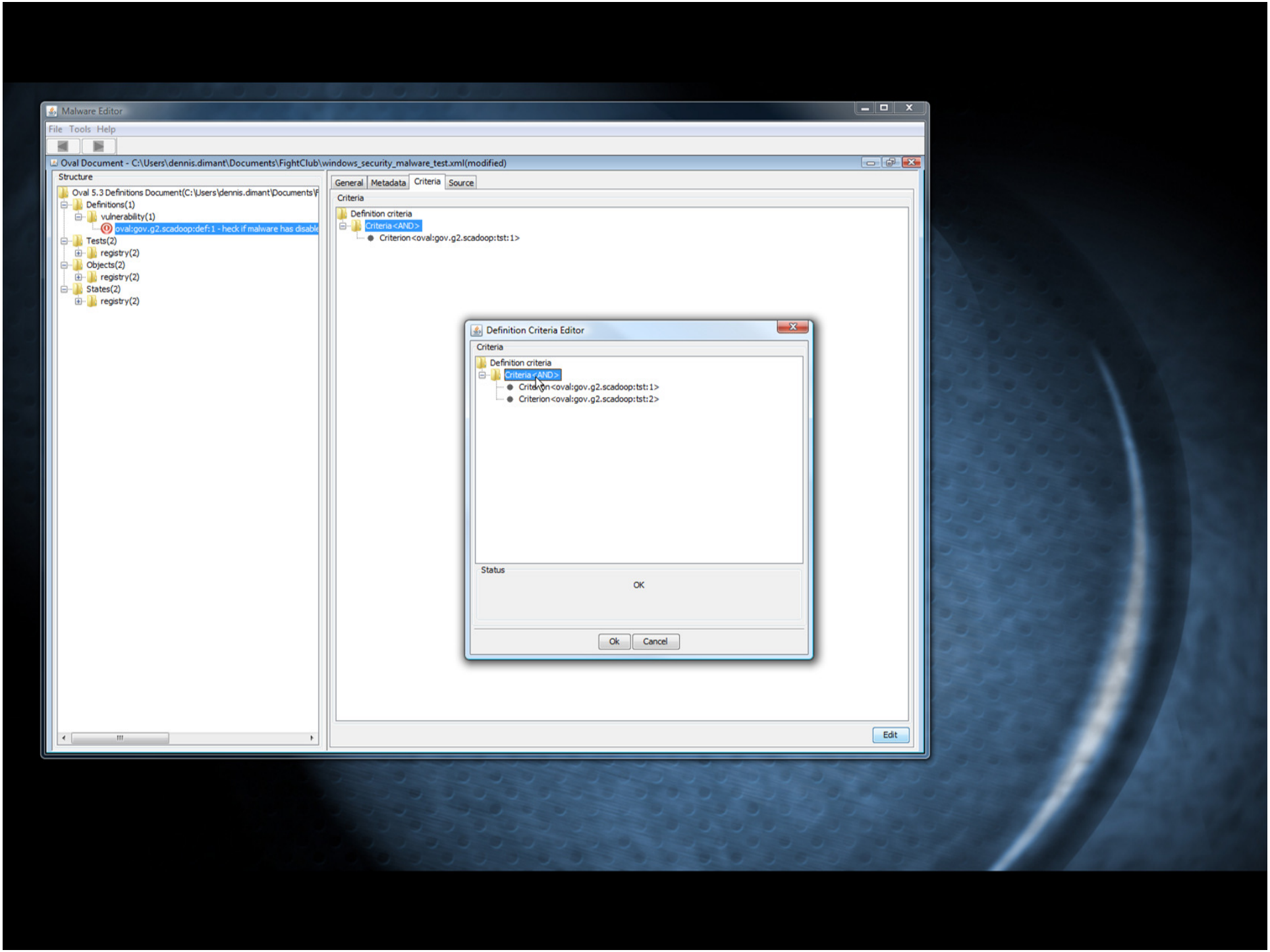
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

\{151B67MA-E28T-45KF-0O30-8801XS8WIF5J}\"StubPath" = "\"%Windir%\jvm.exe\""

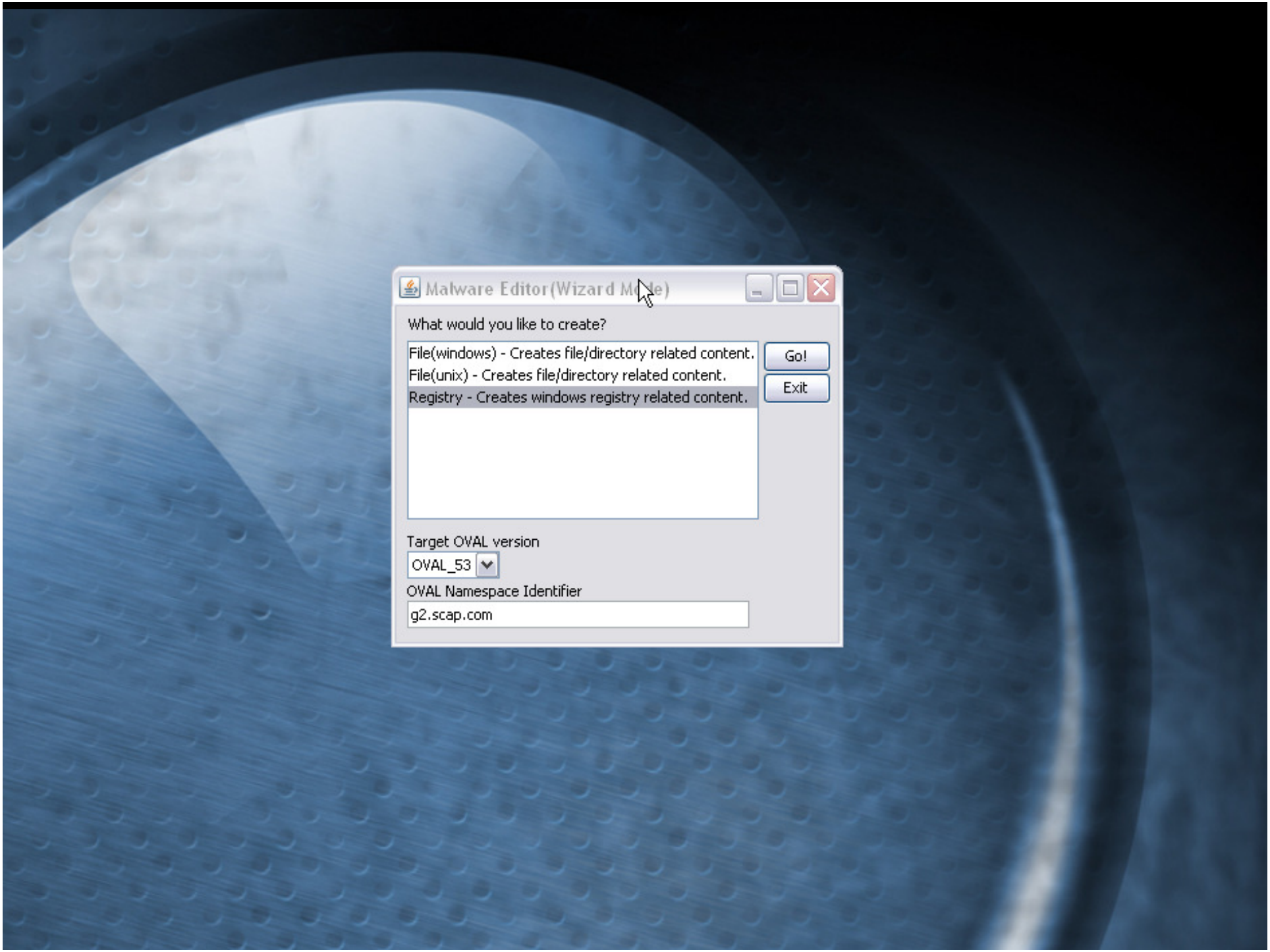
Using an XML editor to create content


<oXygen/> XML Editor
File
Edit
Find
Project
Perspective
Options
Tools
Document
Window
Help
XSLT
XQ

Using the advanced MACE editor to create content


Malware Editor
File Tools Help
Oval Document - C:\Users\dennis.dimant\Documents\FightClub\windows_security_malware_test.xml(modified)
Structure
Oval 5.3 Definitions Document(C:\Users\dennis.dimant\Documents\F
Definitions(1)
vulnerability(1)
oval:gov.g2.scadoop:def:1 - heck if malware has disable
Tests(2)
registry(2)
Objects(2)
registry(2)
States(2)
registry(2)
General
Metadata
Criteria
Source
Criteria
Definition criteria
Criteria <AND>
Criterion <oval:gov.g2.scadoop:tst:1>
Definition Criteria Editor
Criteria
Definition criteria
Criteria <AND>
Criterion <oval:gov.g2.scadoop:tst:1>
Criterion <oval:gov.g2.scadoop:tst:2>
Status
OK
Ok
Cancel
Edit

Using the MACE wizard to create content


Malware Editor(Wizard Mode)
What would you like to create?
File(windows) - Creates file/directory related content.
File(unix) - Creates file/directory related content.
Registry - Creates windows registry related content.
Go!
Exit
Target OVAL version
OVAL_53
OVAL Namespace Identifier
g2.scap.com

Contact Information

Paul Green
President, G2 Inc.
410-290-9710 | Paul.Green@G2-Inc.com

Shane Shaffer
Director, Security Automation
410-290-9710 | Shane.Shaffer@G2-Inc.com