

# Task: OVAL SC

## Inhalt

- [OVAL Adoption Program](#)
- [Scan-Daten als OVAL-SCs einsammeln](#)
- [OVAL-SC exportieren](#)
- [Beispiel: OVAL-SC für ovaldi verwenden](#)

## Einleitung

OVAL steht für Open Vulnerability and Assessment Language. Es ist ein Ansatz für standardisierte Beschreibung des (Sicherheits-)status eines IT-Systems. OVAL-Dateien beschreiben ein Sicherheitsproblem und definieren Tests um den verletzbaren Zustand eines Systems zu identifizieren. Sie wissen in welchem Zustand das Problem behoben ist. Oft bezieht sich das auf die Versionsnummern bestimmter Softwareprodukte.

Um gemäß einer OVAL-Beschreibung zu prüfen benötigt man also Informationen über den Systemzustand. Dieser wird in einer ebenfalls als XML standardisierten Form erhoben, der System Characteristics (SC).

Es gibt verschiedene Lösungen, die auf Basis von OVAL-Dateien und SC-Dateien Prüfungen durchführen. OVAL-Dateien werden von verschiedenen Herstellern zur Verfügung gestellt. MITRE pflegt das OVAL Repository mit über 10.000 Einträgen.

## OVAL Adoption Program



Greenbone ist offizieller OVAL Adopter und Greenbone Security Manager registriert als "Systems Characteristics Producer".

Siehe dazu: [OVAL Adoption Program](#)

Unterstützt werden die OVAL Versionen 5.3 bis 5.9. Sollten bei der Verwendung fehlerhafte, fehlende oder unvollständige OVAL-Elemente gefunden werden, so bitten wir um Rückmeldung über unseren Support. Die OVAL-SC Realisierung bei Greenbone erlaubt es, innerhalb eines Tages Updates für OVAL-SC zu aktivieren und damit zeitnah jegliche Verbesserungen für den Anwender bereitzustellen.

## Scan-Daten als OVAL-SCs einsammeln

Während eines Scans sichtet der Greenbone Security Manager zahlreiche Informationen über die angegebenen

Zielsysteme. Diese Informationen werden in einem eigenen, optimierten Daten-Pool verwaltet. Teile davon eignen sich aber auch direkt als Bestandteil von OVAL System Characteristics.

Die Erstellung von OVAL-SC Dateien ist nicht voreingestellt sondern muss in der Scan Configuration eingeschaltet werden. Die folgende Scan Configuration konzentriert sich genau auf diese Aufgabe:  
[collect-oval-sc.xml](#)

Importieren Sie diese in den GSM:

Die neue Scan Configuration wird anschliessend in der Liste angezeigt:

Die umfassendsten Ergebnisse zu den Zielsystemen werden über authentifizierte Scans ermittelt. Dafür muss zunächst ein Zugangskonto für das Zielsystem eingerichtet werden. Sorgen Sie dafür, dass das Konto auf dem Zielsystem entsprechend eingerichtet ist. Für unixoide Systeme reicht in der Regel ein niedrig privilegierter Zugang, bei Windows-Systemen sind zumeist Administrator-Rechte notwendig.

Das folgende Beispiel zeigt die Einrichtung eine Ziels mit Linux. Für ein Windows-System sollte das Credential bei SMB anstatt bei SSH gesetzt werden.

Nun wird der Task eingerichtet. Starten Sie ihn unmittelbar danach.

### New Task ?

Name:

Comment (optional):

Scan Config:

Scan Targets:

Escalator (optional):

Schedule (optional):

Slave (optional):

Der Scan-Vorgang ist sehr schnell (für dieses Beispiel mit nur einem Zielsystem 1 Sekunde), da mit der speziellen Scan Configuration zielgerichtet die Informationen eingesammelt werden.

Die Ergebnisse werden als Log-Information abgelegt. Stellen Sie den Filter entsprechend ein, so sehen die OVAL System Characteristics in für Lesbarkeit formatiertem XML:

### Report Summary ?

**Result of Task: OVAL SC test scan** [Back to Task](#)

Order of results: by host

Scan started: Thu Mar 24 14:21:45 2011

Scan ended: Thu Mar 24 14:21:46 2011

Scan status:

	High	Medium	Low	Log	False Pos.	Total	Download
Full report:	0	0	0	1	0	1	PDF <input type="button" value="Download"/>
All filtered results:	0	0	0	1	0	1	PDF <input type="button" value="Download"/>
Filtered results 1 - 1:	0	0	0	1	0	1	PDF <input type="button" value="Download"/>

### Result Filtering

Sorting: [port\\_ascending](#) | [port\\_descending](#) | [threat\\_ascending](#) | [threat\\_descending](#)

Show notes

Only show hosts that have results

CVSS >= 8.0

Text phrase:

Threat:  High  Medium  Low  Log  False Pos.

### Filtered Results 1 - 1 of 1

Host	Start	End	High	Medium	Low	Log	False Pos.	Total
<a href="#">192.168.11.21</a>	Mar 24, 14:21:45	Mar 24, 14:21:46	0	0	0	1	0	1
Total: 1			0	0	0	1	0	1

## Port summary for host "192.168.11.21"

Service (Port)	Threat
general/OVAL-SC	Log

## Security Issues reported for 192.168.11.21

Log	general/OVAL-SC
NVT: Show System Characteristics (OID: 1.3.6.1.4.1.25623.1.0.103999)	
<pre> &lt;oval_system_characteristics xmlns="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5" xmlns:linux-sc="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#linux" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-sc="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5 oval-system-characteristics-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#linux linux-system-characteristics-schema.xsd"&gt;   &lt;generator&gt;     &lt;oval:product_name&gt;Greenbone Security Feed&lt;/oval:product_name&gt;     &lt;oval:product_version&gt;201103231409&lt;/oval:product_version&gt;     &lt;oval:schema_version&gt;5.9&lt;/oval:schema_version&gt;     &lt;oval:timestamp&gt;2011-03-24T14:21:46&lt;/oval:timestamp&gt;     &lt;vendor&gt;Greenbone Networks GmbH&lt;/vendor&gt;   &lt;/generator&gt;   &lt;system info&gt; </pre>	

**Bitte beachten:** Haben Sie die Daten von vielen Zielsystemen gesammelt, so kann das den technischen Rahmen für die Ansicht sprengen.

## OVAL-SC exportieren

OVAL-SC's sind so definiert, dass sich eine Beschreibungs-Datei auch nur genau auf ein System bezieht. **Mit Greenbone können aber beliebig viele System Characteristics zu verschiedenen Systemen in einem einzelnen Schritt gesammelt werden.**

Wir stellen daher zwei Report Plugins zur Verfügung:

- [OVAL-SC.xml](#) (ab GSM 1.4 verwendbar): Für eine einzelne System Characteristics Datei die dann als XML geliefert wird.
- [OVAL-SC-archive.xml](#) (ab GSM 1.5 verwendbar): Für eine beliebige Anzahl von System Characteristics Dateien die in einer Zip-Datei zusammengefasst sind. Jede einzelne SC-Datei wird nach der IP-Adresse des jeweiligen Systems benannt.

Importieren Sie diese Report Format Plugins, prüfen Sie die Signaturen und aktivieren Sie sie schließlich. Wie das im Detail geht, kann man hier nachlesen: [Feature: Report Formats](#)

Nun können Sie die Ergebnisse in für die weitere Verwendung geeigneter Form direkt herunterladen. Wählen Sie dafür das Report Format "OVAL-SC" oder "OVAL-SC Archive" bei "Full report" aus:

**Report Summary** Apply overrides Back to Task

**Result of Task: OVAL SC test scan**

Order of results: by host

**Scan started:** Thu Mar 24 14:21:45 2011

**Scan ended:** Thu Mar 24 14:21:46 2011

Scan status: Done

	High	Medium	Low	Log	False Pos.	Total	Download
Full report:	0	0	0	1	0	1	PDF CPE HTML ITG LaTeX NBE OVAL-SC OVAL-SC Archive PDF TXT XML
All filtered results:	0	0	0	0	0	0	
Filtered results:	0	0	0	0	0	0	

**Result Filtering**

Sorting: [port\\_ascending](#) | [port\\_descending](#) | [threat\\_ascending](#) | threat\_descending

Show notes

Only show hosts that have results

CVSS >= 8.0

Text phrase:

Threat:  High  Medium  Low  Log  False Pos. Apply

**Filtered Results**

0 results

Die Zip-Archive sehen wir folgt aus:

**eport-577dd0d7-93d5-4ece-9cee-b7cf302e43aa.zip**

Archive Edit View Help

New Open Extract Add Files Add Folder

Back Location: /

Name	Size	Type	Date Modifi
192.168.11.21-oval-sc.xml	63.2 KB	XML doc...	25 March 2...

1 object (63.2 KB), 1 object selected (63.2 KB)

## Beispiel: OVAL-SC für ovaldi verwenden

Die Organisation MITRE stellt nicht nur OVAL zur Verfügung sondern auch eine Referenzimplementierung für die lokale Ausführung von OVAL-Tests. Der OVAL Interpreter ovaldi ist unter einer Open Source Lizenz verfügbar.

Greenbone macht es über die Bereitstellung von OVAL System Characteristics möglich, dass ein ovaldi-Aufruf beispielsweise auf einen Linux-System läuft, aber ein Windows-System prüft. Umgekehrt ist es

das natürlich genauso möglich.

War das im obigen Beispiel gescannte Zielsystem ein Debian Linux System, kann man nun die offiziellen [Debian OVAL definitions 2010](#) herunterladen und den Test ausführen ("false" bedeutet, dass ein Test keinen Befund hatte).

Ovaldi erstellt automatisch zur folgenden Ausgabe auch eine HTML- und eine XML-Version: [oval-sc-debian-lenny-sample-ovaldi-results.html](#) (110 KByte) und [oval-sc-debian-lenny-sample-ovaldi-results.xml](#) (4,4 MByte).

```
$ cd /tmp
$ ovaldi -m -o /tmp/oval-definitions-2010.xml \
  -i /tmp/oval-sc-debian-lenny-sample.xml \
  -a /usr/share/ovaldi/xml/
```

```
-----
OVAL Definition Interpreter
Version: 5.9 Build: 1
Build date: Mar 10 2011 15:21:36
Copyright (c) 2002-2011 - The MITRE Corporation
-----
```

```
Start Time: Tue Mar 22 11:50:00 2011
```

```
** parsing /tmp/oval-definitions-2010.xml file.
  - validating xml schema.
** checking schema version
  - Schema version - 5.3
** skipping Schematron validation
** parsing /tmp/oval-sc-debian-lenny-sample.xml for analysis.
  - validating xml schema.
** running the OVAL Definition analysis.
   Analyzing definition: FINISHED
** applying directives to OVAL results.
** OVAL definition results.
```

OVAL Id	Result
oval:org.debian:def:1965	false
oval:org.debian:def:1966	false
oval:org.debian:def:1967	false
oval:org.debian:def:1968	false
oval:org.debian:def:1969	false
oval:org.debian:def:1970	false
oval:org.debian:def:1971	false
oval:org.debian:def:1972	false
oval:org.debian:def:1973	false
oval:org.debian:def:1974	false
oval:org.debian:def:1976	false
oval:org.debian:def:1977	false
oval:org.debian:def:1978	false
oval:org.debian:def:1979	false
oval:org.debian:def:1980	false
oval:org.debian:def:1981	false
oval:org.debian:def:1982	false
oval:org.debian:def:1983	false
oval:org.debian:def:1984	false
oval:org.debian:def:1985	false
oval:org.debian:def:1986	false
oval:org.debian:def:1987	false
oval:org.debian:def:1988	false

oval:org.debian:def:1989	false
oval:org.debian:def:1990	false
oval:org.debian:def:1991	false
oval:org.debian:def:1992	false
oval:org.debian:def:1993	false
oval:org.debian:def:1994	false
oval:org.debian:def:1995	false
oval:org.debian:def:1996	false
oval:org.debian:def:1997	false
oval:org.debian:def:1998	false
oval:org.debian:def:1999	false
oval:org.debian:def:2000	false
oval:org.debian:def:2001	false
oval:org.debian:def:2002	false
oval:org.debian:def:2003	false
oval:org.debian:def:2004	false
oval:org.debian:def:2005	false
oval:org.debian:def:2007	false
oval:org.debian:def:2008	false
oval:org.debian:def:2009	false
oval:org.debian:def:2010	false
oval:org.debian:def:2011	false
oval:org.debian:def:2012	false
oval:org.debian:def:2013	false
oval:org.debian:def:2014	false
oval:org.debian:def:2015	false
oval:org.debian:def:2016	false
oval:org.debian:def:2017	false
oval:org.debian:def:2018	false
oval:org.debian:def:2019	false
oval:org.debian:def:2020	false
oval:org.debian:def:2021	false
oval:org.debian:def:2022	false
oval:org.debian:def:2023	false
oval:org.debian:def:2024	false
oval:org.debian:def:2025	false
oval:org.debian:def:2026	false
oval:org.debian:def:2027	false
oval:org.debian:def:2028	false
oval:org.debian:def:2029	false
oval:org.debian:def:2030	false
oval:org.debian:def:2031	false
oval:org.debian:def:2032	false
oval:org.debian:def:2033	false
oval:org.debian:def:2034	false
oval:org.debian:def:2035	false
oval:org.debian:def:2036	false
oval:org.debian:def:2037	false
oval:org.debian:def:2038	false
oval:org.debian:def:2039	false
oval:org.debian:def:2040	false
oval:org.debian:def:2041	false
oval:org.debian:def:2042	false
oval:org.debian:def:2043	false
oval:org.debian:def:2044	false
oval:org.debian:def:2045	false
oval:org.debian:def:2046	false
oval:org.debian:def:2047	false
oval:org.debian:def:2048	false
oval:org.debian:def:2049	false
oval:org.debian:def:2050	false
oval:org.debian:def:2051	false
oval:org.debian:def:2052	false

oval:org.debian:def:2053	false
oval:org.debian:def:2054	false
oval:org.debian:def:2055	false
oval:org.debian:def:2056	false
oval:org.debian:def:2057	false
oval:org.debian:def:2058	false
oval:org.debian:def:2059	false
oval:org.debian:def:2060	false
oval:org.debian:def:2061	false
oval:org.debian:def:2062	false
oval:org.debian:def:2063	false
oval:org.debian:def:2064	false
oval:org.debian:def:2065	false
oval:org.debian:def:2066	false
oval:org.debian:def:2067	false
oval:org.debian:def:2068	false
oval:org.debian:def:2069	false
oval:org.debian:def:2070	false
oval:org.debian:def:2071	false
oval:org.debian:def:2072	false
oval:org.debian:def:2073	false
oval:org.debian:def:2074	false
oval:org.debian:def:2075	false
oval:org.debian:def:2076	false
oval:org.debian:def:2077	false
oval:org.debian:def:2078	false
oval:org.debian:def:2079	false
oval:org.debian:def:2080	false
oval:org.debian:def:2081	false
oval:org.debian:def:2082	false
oval:org.debian:def:2083	false
oval:org.debian:def:2084	false
oval:org.debian:def:2085	false
oval:org.debian:def:2086	false
oval:org.debian:def:2087	false
oval:org.debian:def:2088	false
oval:org.debian:def:2089	false
oval:org.debian:def:2090	false
oval:org.debian:def:2091	false
oval:org.debian:def:2092	false
oval:org.debian:def:2093	false
oval:org.debian:def:2094	false
oval:org.debian:def:2095	false
oval:org.debian:def:2096	false
oval:org.debian:def:2097	false
oval:org.debian:def:2098	false
oval:org.debian:def:2099	false
oval:org.debian:def:2100	false
oval:org.debian:def:2101	false
oval:org.debian:def:2102	false
oval:org.debian:def:2103	false
oval:org.debian:def:2104	false
oval:org.debian:def:2105	false
oval:org.debian:def:2106	false
oval:org.debian:def:2107	false
oval:org.debian:def:2108	false
oval:org.debian:def:2109	false
oval:org.debian:def:2110	false
oval:org.debian:def:2111	false
oval:org.debian:def:2112	false
oval:org.debian:def:2113	false
oval:org.debian:def:2114	false
oval:org.debian:def:2115	false

```
oval:org.debian:def:2116           false
oval:org.debian:def:2117           false
oval:org.debian:def:2118           false
oval:org.debian:def:2119           false
oval:org.debian:def:2120           false
oval:org.debian:def:2121           false
oval:org.debian:def:2122           false
oval:org.debian:def:2123           false
oval:org.debian:def:2124           false
oval:org.debian:def:2125           false
oval:org.debian:def:2126           false
oval:org.debian:def:2127           false
oval:org.debian:def:2128           false
oval:org.debian:def:2129           false
oval:org.debian:def:2130           false
oval:org.debian:def:2131           false
oval:org.debian:def:2132           false
oval:org.debian:def:2133           false
```

-----

```
** finished evaluating OVAL definitions.
```

```
** saving OVAL results to results.xml.
```

```
** running OVAL Results xsl: /usr/share/ovaldi/xml//results_to_html.xsl.
```