

Task: OVAL SC

Content

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

Introduction

The Open Vulnerability and Assessment Language (OVAL) is an approach for a standardized description of the (security) state of an IT system. OVAL files describe a vulnerability and define tests to identify the state in which a system is vulnerable. They usually refer to specific version of software products for which a known vulnerability exists.

This means that in order to check for vulnerabilities described in an OVAL definition, information about the current state of the system is needed. This information is collected in a standardized format as well — the OVAL System Characteristics (SC).

There are a number of solutions which perform checks based on OVAL definitions and SC files. OVAL definitions are provided by various vendors. MITRE provides the OVAL Repository with more than 10,000 entries.

OVAL Adoption Program



Greenbone is a official OVAL Adopter and Greenbone Security Manager registered as "Systems Characteristics Producer".

See also: [OVAL Adoption Program](#)

Supported are OVAL versions 5.3 to 5.9. Should any wrong, missing or incomplete OVAL element be found, users are encouraged to provide feedback to the Greenbone support team. The OVAL-SC implementation of the Greenbone solution allows to activate updates within a single day therefore provides timely improvements for the users.

Collecting Scan Results as OVAL SCs

During a scan the Greenbone Security Manager collects large amounts of data about the target system. This

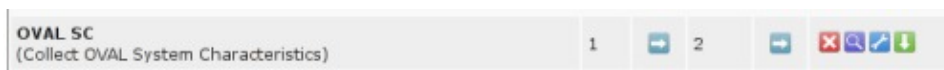
information is managed in an optimized data pool. Parts of this information are usable as a component of an OVAL System Characteristics.

The creation of OVAL SC files is not enabled by default but has to be explicitly enabled. The following scan configuration can be used to achieve this: [collect-oval-sc.xml](#)

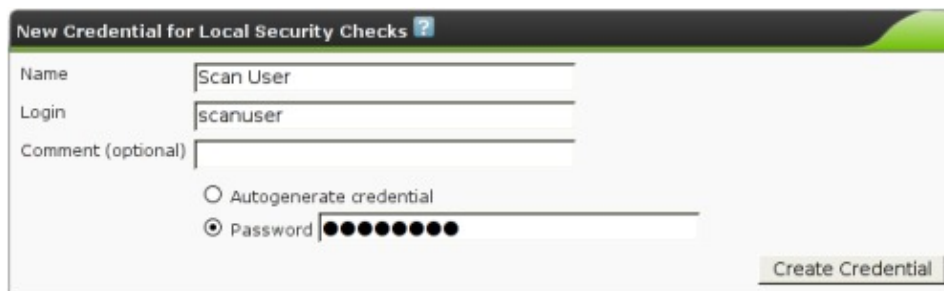
Import the scan configuration in the GSM:



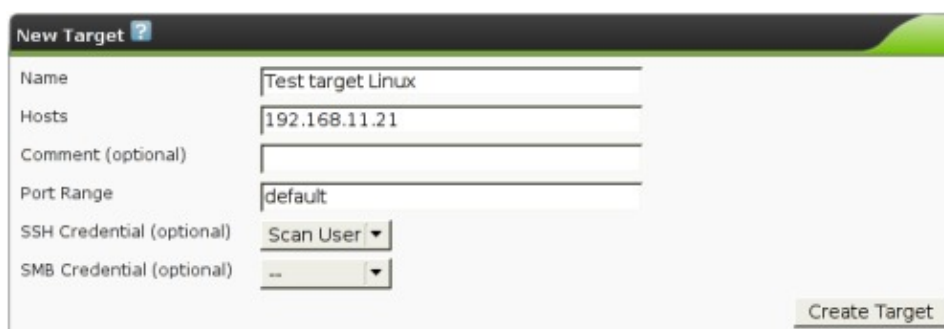
The new scan configuration is now shown in the list:



The most comprehensive results of a target system can be collected using authenticated scans. For this you need to create an account on the target system. Ensure that the account has the necessary privileges. For unixoid systems an account with low privileges is usually sufficient, for Windows system administrative privileges are required.



The following example shows the creation of a Linux target. For a Windows target the credential should be set in the SMB field instead of SSH.



Now create the task, which you can start immediately.

New Task ?

Name:

Comment (optional):

Scan Config:

Scan Targets:

Escalator (optional):

Schedule (optional):

Slave (optional):

The scan itself is very fast (in this example with a single target system 1 second) because the scan configuration is optimized to collect only the specific data need for generating the System Characteristics file.

The results are returned a log information. If you adjust your filter you can see the OVAL System Characteristics in XML formatted for easy readability:

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
192.168.11.21	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><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"> <generator> <oval:product_name>Greenbone Security Feed</oval:product_name> <oval:product_version>201103231409</oval:product_version> <oval:schema_version>5.9</oval:schema_version> <oval:timestamp>2011-03-24T14:21:46</oval:timestamp> <vendor>Greenbone Networks GmbH</vendor> </generator> <system info></pre>	

Please note: If you have collected data from a large number of target systems this view may become hard to read.

Exporting OVAL SCs

OVAL SC files are defined in a way that one file can contain only information about one system. **Using the Greenbone Security Manager you can collect a large number of System Characteristics from many different systems in one single step.**

Because of this we provide two Report Plugins:

- [OVAL-SC.xml](#) (requires GSM 1.4 or later): Produces a single SC file in the XML format.
- [OVAL-SC-archive.xml](#) (requires GSM 1.5 or later): Can be used for an arbitrary number of System Characteristics, which will be collected in a ZIP file. The names of the individual SC files will contain the IP address of the target system.

Import the report format plugins, verify the signature and activate them. For detailed information about this process, please refer to: [Feature: Report Formats](#)

You can now download the results in the format you require for further processing. Select the format "OVAL-SC" or "OVAL-SC archive" in the "Full report" line:

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

The ZIP archives look as follows:

Example: Using OVAL SCs with ovaldi

The MITRE organization not only provides the OVAL standard but also provides a reference implementation for local OVAL checks. The [OVAL Interpreter ovaldi](#) is available under an Open Source license.

By using the Greenbone Security Manager to provide OVAL System Characteristics it is easy to use ovaldi on Linux to check a Windows system — or the other way round.

For example, if the target system you tested above was a Debian Linux system, you can now download the official [Debian OVAL definitions 2010](#) and execute the test ("false" means that a condition was not met, i.e. a vulnerability does not exist on the target).

Ovaldi automatically creates a HTML and XML version of the plain text output as shown below:
[oval-sc-debian-lenny-sample-ovaldi-results.html](#) (110 KByte) and
[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.
```