
ATTACK
DEFENSE
by PentesterAcademy

Name	OpenSCAP: Automating Compliance Checks
URL	https://attackdefense.com/challengedetails?cid=2258
Type	DevSecOps: Vulnerability Assessment

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Challenge Description

OpenSCAP is used to check for security configurations in compliance with NIST Certified SCAP 1.2

A Kali GUI machine (kali-gui) is provided to the user with OpenSCAP installed on it. OpenSCAP uses OVAL (Open Vulnerability and Assessment Language) XML files to read the list of vulnerabilities and then check for those on the local machine. Two example OVAL XML files are stored in the home directory of the root user. One file contains CVE (Common Vulnerabilities and Exposures) definitions and the other contains the USN (Ubuntu Security Notice).

Objective: Use Openscap to scan the Kali machine!

Instructions:

- The OVAL XML files are provided at /root/oval-files/
- The OpenSCAP can be invoked using ‘oscap’ command

Solution

Step 1: Open a terminal and Check the content of the oval-files directory.

Command: ls oval-files/

```
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# ls oval-files/
oci.com.ubuntu.bionic.cve.oval.xml  oci.com.ubuntu.bionic.usn.oval.xml
root@attackdefense:~#
```

These files are classified on the basis of CVE and USN (Ubuntu Security Notice).

Step 2: Check the available options in openscap

Command: oscap --help

```
root@attackdefense:~# oscap --help
oscap

OpenSCAP command-line tool

Usage: oscap [options] module operation [operation-options-and-arguments]

oscap options:
   -h --help                    - show this help
   -q --quiet                   - quiet mode
   -V --version                 - print info about supported SCAP versions

Commands:
    ds - DataStream utilities
    oval - Open Vulnerability and Assessment Language
    xccdf - eXtensible Configuration Checklist Description Format
    cvss - Common Vulnerability Scoring System
    cpe - Common Platform Enumeration
    cve - Common Vulnerabilities and Exposures
    cvrf - Common Vulnerability Reporting Framework
    info - info module
```

Example 1: Check the system for vulnerabilities on the basis of CVE.

Step 1: Check the content of the CVE OVAL file.

Command: vim oval-files/oci.com.ubuntu.bionic.cve.oval.xml

```
        <definition class="vulnerability" id="oval:com.ubuntu.bionic:def:201318310000000" version="1">
            <metadata>
                <title>CVE-2013-1831 on Ubuntu 18.04 LTS (bionic) - low.</title>
                <description>lib/setuplib.php in Moodle through 2.1.10, 2.2.x before 2.2.8, 2.3.x before 2.3
.5, and 2.4.x before 2.4.2 allows remote attackers to obtain sensitive information via an invalid request, w
hich reveals the absolute path in an exception message.</description>
                <affected family="unix">
                    <platform>Ubuntu 18.04 LTS</platform>
                </affected>
                <reference source="CVE" ref_id="CVE-2013-1831" ref_url="https://cve.mitre.org/cgi-bin/cvenam
e.cgi?name=CVE-2013-1831" />
                <advisory>
                    <severity>Low</severity>
                    <rights>Copyright (C) 2013 Canonical Ltd.</rights>
                    <public_date>2013-03-25 21:55:00 UTC</public_date>
                    <discovered_by>Mark Nielsen</discovered_by>
                    <crd>2013-03-11 04:00:00 UTC</crd>
                    <crd>2013-03-11 04:00:00 UTC</crd>
                    <ref>http://people.canonical.com/~ubuntu-security/cve/2013/CVE-2013-1831.html</ref>
                </advisory>
            </metadata>
            <oval:notes>
                <oval:note>sarnold&gt; MSA-13-0013</oval:note>
            </oval:notes>
            <criteria>

                <criterion test_ref="oval:com.ubuntu.bionic:tst:201137570000000" comment="moodle package in
bionic is affected and needs fixing." />
            </criteria>
        </definition>
```

There are different definitions mentioned e.g.moodle version 2.2.x to 2.4.2 is vulnerable.

Step 2: Run the oscap tool in oval mode and pass the CVE OVAL XML file. Generate the report in HTML format.

Command: oscap oval eval --report report.htm oval-files/oci.com.ubuntu.bionic.cve.oval.xml

Description:

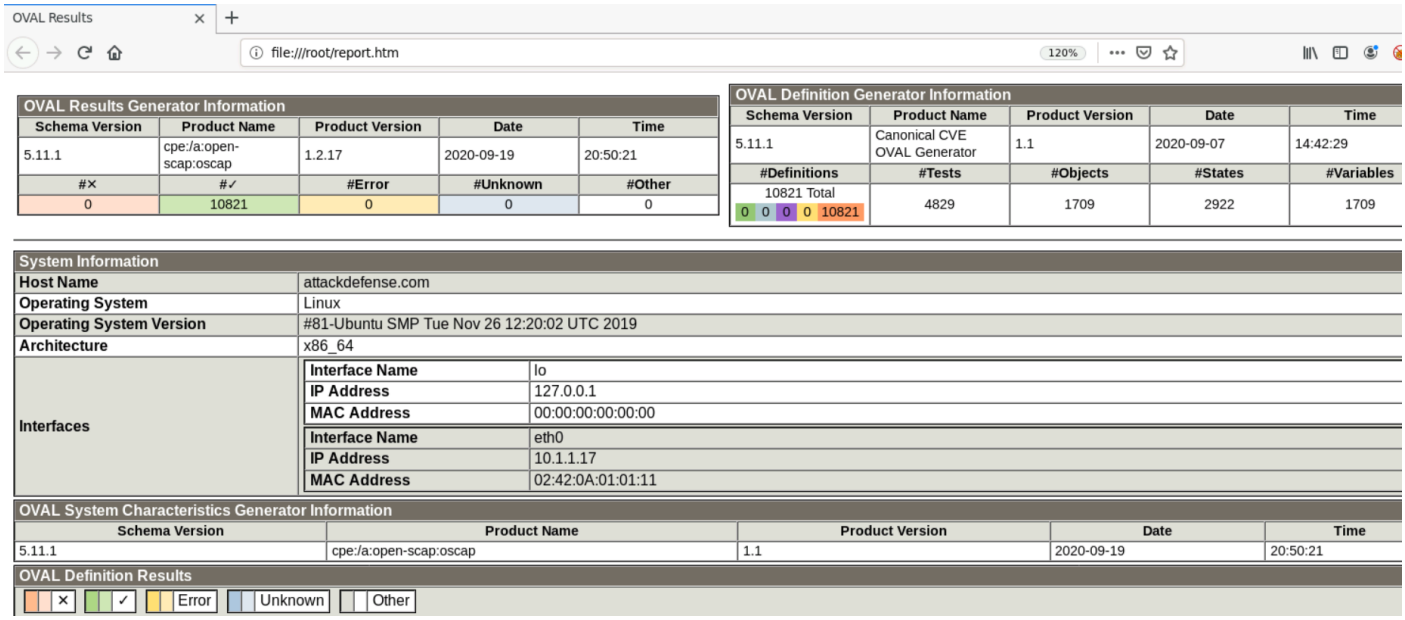
oval: Performing scan from Open Vulnerability and Assessment Language
eval: Probe the system and evaluate definitions from OVAL Definition file
report : Generate report with the name passed with flag
oval-files/oci.com.ubuntu.bionic.cve.oval.xml: File contains definitions for the scan

```
Definition oval:com.ubuntu.bionic:def:200851500000000: false
Definition oval:com.ubuntu.bionic:def:200851460000000: false
Definition oval:com.ubuntu.bionic:def:200851440000000: false
Definition oval:com.ubuntu.bionic:def:200767620000000: false
Definition oval:com.ubuntu.bionic:def:200751090000000: false
Definition oval:com.ubuntu.bionic:def:200747740000000: false
Definition oval:com.ubuntu.bionic:def:200702550000000: false
Definition oval:com.ubuntu.bionic:def:200224390000000: false
Evaluation done.
root@attackdefense:~#
```

The openscap scanned based on the information provided in the XML file to check for vulnerable packages in the system.

Step 3: Open the report in firefox.

Commands: firefox report.htm



ID	Result	Class	Reference ID	Title
oval:com.ubuntu.bionic:def:202099250000000	false	vulnerability	[CVE-2020-9925]	CVE-2020-9925 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202099150000000	false	vulnerability	[CVE-2020-9915]	CVE-2020-9915 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098950000000	false	vulnerability	[CVE-2020-9895]	CVE-2020-9895 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098940000000	false	vulnerability	[CVE-2020-9894]	CVE-2020-9894 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098930000000	false	vulnerability	[CVE-2020-9893]	CVE-2020-9893 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098620000000	false	vulnerability	[CVE-2020-9862]	CVE-2020-9862 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098500000000	false	vulnerability	[CVE-2020-9850]	CVE-2020-9850 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098430000000	false	vulnerability	[CVE-2020-9843]	CVE-2020-9843 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098070000000	false	vulnerability	[CVE-2020-9807]	CVE-2020-9807 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098060000000	false	vulnerability	[CVE-2020-9806]	CVE-2020-9806 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098050000000	false	vulnerability	[CVE-2020-9805]	CVE-2020-9805 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098030000000	false	vulnerability	[CVE-2020-9803]	CVE-2020-9803 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202098020000000	false	vulnerability	[CVE-2020-9802]	CVE-2020-9802 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202097940000000	false	vulnerability	[CVE-2020-9794]	CVE-2020-9794 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202097600000000	false	vulnerability	[CVE-2020-9760]	CVE-2020-9760 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202097590000000	false	vulnerability	[CVE-2020-9759]	CVE-2020-9759 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202096330000000	false	vulnerability	[CVE-2020-9633]	CVE-2020-9633 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202095490000000	false	vulnerability	[CVE-2020-9549]	CVE-2020-9549 on Ubuntu 18.04 LTS (bionic) - medium.
oval:com.ubuntu.bionic:def:202095480000000	false	vulnerability	[CVE-2020-9548]	CVE-2020-9548 on Ubuntu 18.04 LTS (bionic) - untriaged.

The openscap has scanned for all the given CVE's and found no vulnerabilities in the system.

Example 2: Check the system for vulnerabilities on the basis of USN

Step 1: Check the content of the USN OVAL file.

Command: vim oval-files/oci.com.ubuntu.bionic.usn.oval.xml

```
        </metadata>
        <criteria operator="OR">
           <criterion test_ref="oval:com.ubuntu.bionic:tst:379910000000" comment="?" />
        </criteria>
     </definition>
     <definition id="oval:com.ubuntu.bionic:def:38951000000" version="1" class="patch">
        <metadata>
           <title>3895-1 -- LDB vulnerability</title>
           <affected family="unix">
              <platform>Ubuntu 18.04 LTS</platform>
           </affected>
           <reference source="USN" ref_url="https://ubuntu.com/security/notices/USN-3895-1" ref_id="USN-3895-1"/>
           <reference source="CVE" ref_url="https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-3824.h
l" ref_id="CVE-2019-3824"/>
           <description>LDB could be made to crash if it received specially crafted network traffic.</description>
           <advisory from="security@ubuntu.com">
              <severity>Medium</severity>
              <issued date="2019-02-26"/>

           </advisory>
                                                                          131,21        0%
```

There are different definitions mentioned e.g. LDB in Ubuntu 18.04 LTS is vulnerable.

Step 2: Run the oscap tool in oval mode while passing the USN OVAL XML file and generate an HTML report

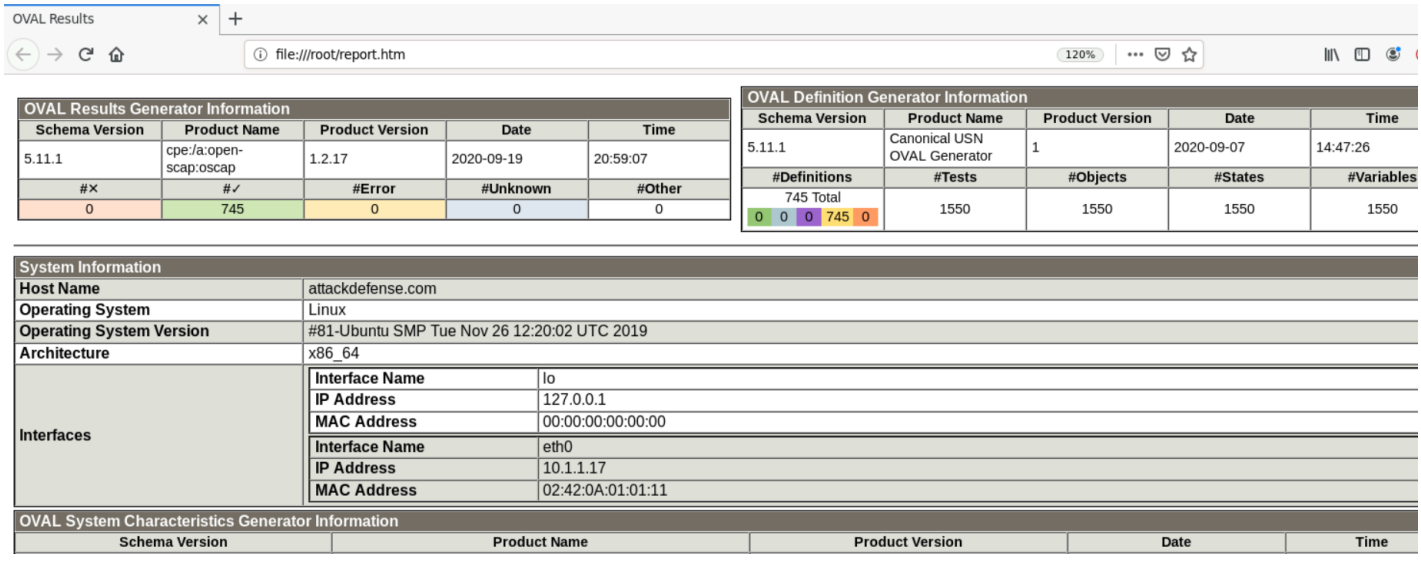
Command: oscap oval eval --report report.htm oval-files/oci.com.ubuntu.bionic.usn.oval.xml

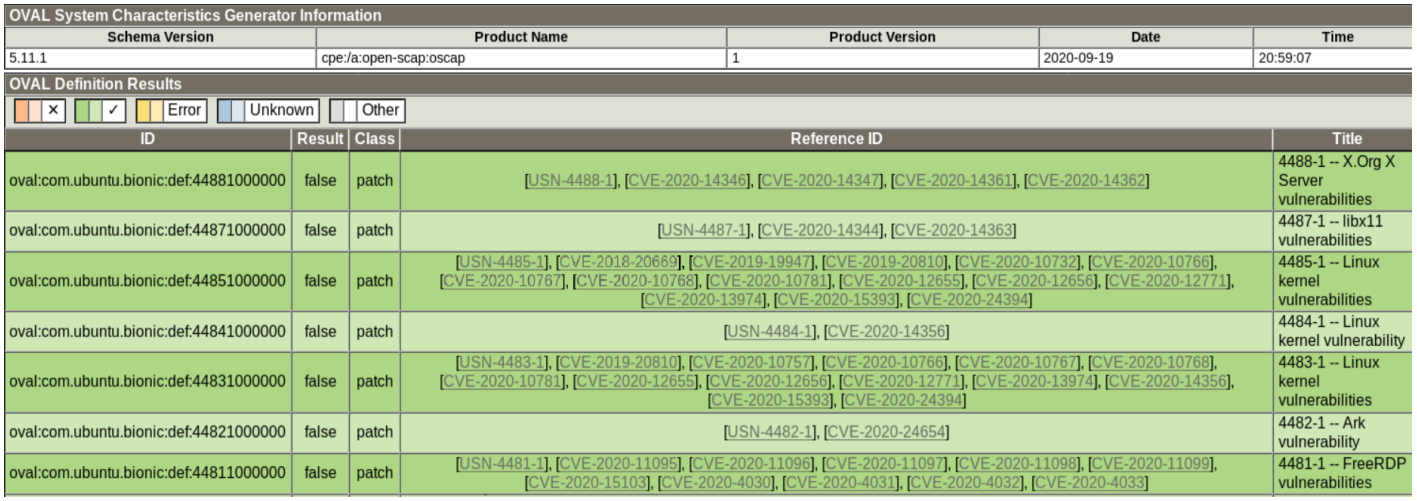
```
Definition oval:com.ubuntu.bionic:def:36452000000: false
Definition oval:com.ubuntu.bionic:def:36451000000: false
Definition oval:com.ubuntu.bionic:def:36431000000: false
Definition oval:com.ubuntu.bionic:def:36421000000: false
Definition oval:com.ubuntu.bionic:def:36401000000: false
Definition oval:com.ubuntu.bionic:def:36391000000: false
Definition oval:com.ubuntu.bionic:def:36371000000: false
Definition oval:com.ubuntu.bionic:def:36361000000: false
Definition oval:com.ubuntu.bionic:def:36293000000: false
Definition oval:com.ubuntu.bionic:def:36272000000: false
Evaluation done.
root@attackdefense:~#
```

The openscap scanned based on the information provided in the XML file to check for vulnerable packages in the system.

Step 3: Start firefox and open the report.htm file.

Command: firefox report.htm





OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11.1	cpe:/a:open-scap:oscap	1	2020-09-19	20:59:07

OVAL Definition Results

✕ ✓ Error Unknown Other

ID	Result	Class	Reference ID	Title
oval:com.ubuntu.bionic:def:44881000000	false	patch	[USN-4488-1], [CVE-2020-14346], [CVE-2020-14347], [CVE-2020-14361], [CVE-2020-14362]	4488-1 -- X.Org X Server vulnerabilities
oval:com.ubuntu.bionic:def:44871000000	false	patch	[USN-4487-1], [CVE-2020-14344], [CVE-2020-14363]	4487-1 -- libx11 vulnerabilities
oval:com.ubuntu.bionic:def:44851000000	false	patch	[USN-4485-1], [CVE-2018-20669], [CVE-2019-19947], [CVE-2019-20810], [CVE-2020-10732], [CVE-2020-10766], [CVE-2020-10767], [CVE-2020-10768], [CVE-2020-10781], [CVE-2020-12655], [CVE-2020-12656], [CVE-2020-12771], [CVE-2020-13974], [CVE-2020-15393], [CVE-2020-24394]	4485-1 -- Linux kernel vulnerabilities
oval:com.ubuntu.bionic:def:44841000000	false	patch	[USN-4484-1], [CVE-2020-14356]	4484-1 -- Linux kernel vulnerability
oval:com.ubuntu.bionic:def:44831000000	false	patch	[USN-4483-1], [CVE-2019-20810], [CVE-2020-10757], [CVE-2020-10766], [CVE-2020-10767], [CVE-2020-10768], [CVE-2020-10781], [CVE-2020-12655], [CVE-2020-12656], [CVE-2020-12771], [CVE-2020-13974], [CVE-2020-14356], [CVE-2020-15393], [CVE-2020-24394]	4483-1 -- Linux kernel vulnerabilities
oval:com.ubuntu.bionic:def:44821000000	false	patch	[USN-4482-1], [CVE-2020-24654]	4482-1 -- Ark vulnerability
oval:com.ubuntu.bionic:def:44811000000	false	patch	[USN-4481-1], [CVE-2020-11095], [CVE-2020-11096], [CVE-2020-11097], [CVE-2020-11098], [CVE-2020-11099], [CVE-2020-15103], [CVE-2020-4030], [CVE-2020-4031], [CVE-2020-4032], [CVE-2020-4033]	4481-1 -- FreeRDP vulnerabilities

The openscap has scanned for all the given USN's and found no vulnerabilities in the system.

Learnings

Check a system against NIST compliance using OpenScap.