

목차

1. 소개	3
2. oscap 기본 사용법	3
2.1. 설치	3
2.2. SCAP 콘텐츠에 대한 정보 표시	4
결과 파일에 대한 추가 정보 (XCCDF 및 ARF)	6
2.3. OSCAP로 스캔	7
OVAL	7
XCCDF	10
Source DataStream 원본 데이터스트림	11
Result DataStream (ARF) 결과 데이터 스트림	11
Result STIG Viewer	12
2.4. Remediate System 시스템 재조정(치료)	12
Online Remediation 온라인 재조정(치료)	13
Offline Remediation 오프라인 재조정(치료)	13
Remediation Review 재조정 검토	13
2.5. Check Engines 엔진 점검	14
CVE, CCE, CPE 및 기타 식별자	14
번들로 제공되는 CCE 데이터	15

OpenSCAP 1.2 매뉴얼

1. 소개

이 설명서는 호출되는 명령 줄 도구 **oscap**와 가장 일반적인 작업에 대한 정보를 제공 합니다. **oscap**으로 당신은 시스템의 보안 구성 설정을 확인할 수 있으며, 표준 및 사양을 기반으로 규칙을 사용하여 타협의 징후에 대한 시스템을 검사합니다. **oscap**은 **SCAP** 의해 유지 사양의 라인 **NIST** 시스템 보안을 관리하기 위한 표준화 된 방식을 제공하기 위해 만들어졌다. 새로운 사양은 일관되고 반복 가능한 수정 작업 흐름을 제공하기 위해 NIST의 SCAP 릴리스주기 에 의해 관리됩니다. **oscap**는 주로 XCCDF를 처리합니다. 이는 체크리스트 콘텐츠를 표현하는 표준 방식이며 보안 체크리스트를 정의합니다. 또한 CPE , CCE 및 OVAL 과 같은 다른 사양과 결합하여 SCAP 검증 제품으로 처리 할 수 있는 SCAP 표현 체크리스트를 작성합니다. SCAP에 대한 자세한 내용은 SCAP 표준을 참조하십시오 .

이 **oscap**도구는 **OpenSCAP** 프로젝트 의 일부입니다 . 이 도구에 대한 그래픽 대안에 관심이 있으시면 **SCAP Workbench** 페이지 를 방문 하십시오.

우리는 **scap-security-guide SSG** 프로젝트를 사용하여 SCAP 콘텐츠를 제공 할 것입니다. 이는 여러 가지 컴퓨터 보안 영역을 다루는 SCAP 문서 형식으로 작성된 보안 정책을 제공하며 존중 당국 (PCI DSS , STIG 및 USGCB)에서 권장하는 보안 지침을 구현 합니다.

최소한 XCCDF 또는 OVAL에 대해 잘 알고 있다면 자신 만의 SCAP 콘텐츠를 생성 할 수도 있습니다. XCCDF 콘텐츠는 오픈 소스 라이선스하에 온라인으로 자주 게시되기 때문에 필요에 맞게이 콘텐츠를 사용자 정의 할 수 있습니다. SCAP Workbench는 커스터마이제이션을 수행하는 훌륭한 도구입니다.

매뉴얼의 기본 **oscap** 사용법 섹션에서는 도구 및 SCAP 콘텐츠를 설치하는 방법과이를 사용하여 SCAP 콘텐츠를 검사하고, 구성 스캔을 수행하며, 자동으로 시스템을 교정하는 방법을 제시합니다.

세 번째 섹션에서는 SCAP 콘텐츠의 유효성 검사, 서명 및 변형, 보고서 및 가이드 생성 및 CPE 적용 가능성에 대한 몇 가지 정보와 같은 고급 주제를 다룹니다.

마지막 절에는 Linux 및 Windows에서 개발자에게 유용한 **oscap** 디버깅 및 컴파일에 대한 정보가 포함되어 있습니다.

2. oscap 기본 사용법

로컬 시스템의 구성 또는 취약점 검색을 수행하려면 다음을 사용할 수 있어야합니다.

- A tool (oscap or SCAP Workbench)
- SCAP content (XCCDF, OVAL...)

2.1. 설치

[소스](#) 에서 OpenSCAP 라이브러리와 **oscap** 도구를 빌드하거나 (자세한 내용은 컴파일 섹션 참조) Linux 배포판에 기존 빌드를 사용할 수 있습니다. Fedora 또는 Red Hat Enterprise Linux 배포판에 **oscap** 도구를 설치하려면 다음 yum 명령을 사용하십시오.

```
# yum install openscap-scanner
```

openscap-scanner가 없다면 openscap-utils 패키지를 설치하십시오

이 oscap도구를 사용하기 전에 시스템에 일부 SCAP 콘텐츠가 있어야합니다. 해당 웹 사이트에서 다운로드 할 수 있지만 다음 섹션에서 SSG 프로젝트를 사용합니다. 소스에서 빌드 하거나 패키지 관리 시스템을 사용하여 설치할 수 있습니다.

```
# yum install scap-security-guide
```

SCAP 콘텐츠는 /usr/share/xml/scap/ssg/content/ 디렉토리에 설치됩니다.

SCAP 콘텐츠를 시스템에 가져 오거나 설치 하면 oscap 콘텐츠에 대한 파일 경로를 지정하여 콘텐츠를 처리 할 수 있습니다. oscap은 SCAP 1.2 및 SCAP 역 호환성 1.1 및 SCAP 1.0 를 지원합니다. 이전 버전의 SCAP 콘텐츠를 가져오고 처리하려면 특별한 처리가 필요하지 않습니다.

oscap, 지원되는 사양, 기본 제공 CPE 이름 및 지원되는 OVAL 개체의 버전을 표시하려면 다음 명령을 입력하십시오.

```
$ oscap -V
```

2.2. SCAP 콘텐츠에 대한 정보 표시

oscap의 기능 중 하나는 파일 내의 SCAP 내용에 대한 정보를 표시하는 것입니다. 실행 중인 oscap info 명령은 같은 문서 유형, 사양 버전, 상태, 문서가 게시 된 날짜 (같은 SCAP 문서 및 디스플레이 정보의 내부 구조의 시험을 허용 생성) 및 문서 시스템을 파일에 복사 된 날짜 (수입). 일반적으로 XCCDF 문서 또는 SCAP 데이터 스트림을 검사 할 때 가장 유용한 정보는 프로필, 검사 목록 및 스트림에 대한 정보입니다.

다음 예제에서는 target이 SCAP 데이터 스트림 일 때 명령의 사용법과 샘플 출력을 보여줍니다.

```
$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Document type: Source Data Stream
Imported: 2016-08-10T20:49:16

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
Generated: (null)
Version: 1.2
Checklists:
    Ref-Id: scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml
    Status: draft
    Generated: 2016-08-10
    Resolved: true
    Profiles:
        xccdf_org.ssgproject.content_profile_standard
```

```

xccdf_org.ssgproject.content_profile_pci-dss
xccdf_org.ssgproject.content_profile_C2S
xccdf_org.ssgproject.content_profile_rht-ccp
xccdf_org.ssgproject.content_profile_common
xccdf_org.ssgproject.content_profile_stig-rhel7-
workstation-upstream
xccdf_org.ssgproject.content_profile_stig-rhel7-
server-gui-upstream
xccdf_org.ssgproject.content_profile_stig-rhel7-
server-upstream
xccdf_org.ssgproject.content_profile_ospp-rhel7-
server
xccdf_org.ssgproject.content_profile_nist-cl-il-al
xccdf_org.ssgproject.content_profile_cjis-rhel7-
server
    Referenced check files:
        ssg-rhel7-oval.xml
        system:
http://oval.mitre.org/XMLSchema/oval-definitions-5
        ssg-rhel7-ocil.xml
        system: http://scap.nist.gov/schema/ocil/2
http://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_7.xml
        system:
http://oval.mitre.org/XMLSchema/oval-definitions-5
Checks:
    Ref-Id: scap_org.open-scap_cref_ssg-rhel7-oval.xml
    Ref-Id: scap_org.open-scap_cref_ssg-rhel7-ocil.xml
    Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-cpe-oval.xml
    Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-oval.xml
Dictionaries:
    Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-cpe-dictionary.xml

```

XCCDF 문서를 검사 할 때 :

```

$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
Document type: XCCDF Checklist
Checklist version: 1.1
Imported: 2016-08-10T20:49:16
Status: draft
Generated: 2016-08-10
Resolved: true
Profiles:
    standard
    pci-dss
    C2S
    rht-ccp
    common
    stig-rhel7-workstation-upstream
    stig-rhel7-server-gui-upstream

```

```
stig-rhel7-server-upstream
ospp-rhel7-server
nist-cl-il-al
cjis-rhel7-server
Referenced check files:
ssg-rhel7-oval.xml
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
ssg-rhel7-ocil.xml
    system: http://scap.nist.gov/schema/ocil/2
http://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_7.xml
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
```

Document type : 파일의 형식을 설명합니다. 공통 유형에는 XCCDF, OVAL, 소스 데이터 스트림 W 결과 데이터 스트림이 포함됩니다. **Checklist version :** XCCDF 파일에 대해서만 표시된 XCCDF 버전입니다. 일반적인 값은 1.1과 1.2입니다. **Imported :** OpenSCAP에서 사용하기 위해 파일을 가져온 날짜입니다. OpenSCAP은 로컬 파일 시스템을 사용하고 독점 데이터베이스 형식이 없기 때문에 가져온 날짜는 파일 수정 날짜와 동일합니다. **Status :** XCCDF 벤치 마크 상태입니다. 일반적인 값에는 accepted, draft, deprecated, incomplete가 포함됩니다. 자세한 내용은 XCCDF 사양을 참조하십시오. 이것은 XCCDF 파일에만 표시됩니다. **Generated date :** 파일이 생성 / 생성 된 날짜입니다. 이 날짜는 XCCDF 파일 W 검사 목록에 표시되며 XCCDF 상태 요소에서 제공됩니다. **Checklists :** oscap xccdf eval 명령어에 --benchmark-id 옵션과 함께 사용하는 경우 데이터 스트림에 통합 된 사용 가능한 검사 목록이 나열 됩니다 . 또한 각 체크리스트에는 상세한 정보가 인쇄되어 있습니다. **Profiles :** oscap xccdf eval 명령어에 --profile 옵션과 함께 사용하는 경우 사용 가능한 프로필 ID가 나열 됩니다

결과 파일에 대한 추가 정보 (XCCDF 및 ARF)

oscap info는 XCCDF 결과 및 ARF 파일과 함께 사용시 약간 유용한 명령입니다. 일반적으로 요청되는 두 가지 중요한 날짜는 평가 시작일과 종료일입니다.

XCCDF 결과 파일에서 파일을 찾으려면 파일을 열고 TestResult 요소를 찾으십시오. 시작 시간 과 종료 시간 속성은 평가 시간과 날짜가 포함되어 있습니다.

```
<TestResult id="xccdf_org.open-scap_testresult_common" start-
time="2017-01-21T19:16:28" end-time="2017-01-21T19:17:35"
```

ARF 파일에서 날짜를 조회하려면 파일을 열고 다시 TestResult 요소를 찾으십시오. 요소는 arf : report 요소에 있습니다.

```
<arf:reports>
  <arf:report id="xccdf1">
    <arf:content>
      <TestResult xmlns="http://checklists.nist.gov/xccdf/1.2"
id="xccdf_org.open-
scap_testresult_xccdf_org.ssgproject.content_profile_stig-rhel7-server-
upstream" start-time="2017-01-20T14:30:18" end-time="2017-01-20T14:36:32"
```

HTML 보고서 인 표 평가 특성 에서 두 날짜를 모두 찾을 수도 있습니다 . XCCDF 결과 또는 ARF에서 HTML 보고서를 생성하려면 `oscap xccdf generate report` 명령을 사용하십시오 .

2.3. OSCAP로 스캔

`oscap` 도구 의 주요 목표 는 로컬 시스템의 구성 및 취약성 검색을 수행하는 것입니다. `Oscap`은 XCCDF 벤치 마크 및 OVAL 정의를 평가하고 적절한 결과를 생성 할 수 있습니다. SCAP 콘텐츠는 단일 파일 (OVAL 파일 또는 SCAP 데이터 스트림) 또는 여러 개의 별도 XML 파일로 제공 될 수 있습니다. 다음 예는 이러한 접근 방식을 구분합니다.

OVAL

SCAP 문서는 단일 OVAL 파일 (OVAL 정의 파일)의 형식을 가질 수 있습니다. `oscap` 도구는 OVAL 정의를 평가하는 동안 OVAL 정의 파일을 처리합니다. 시스템 정보를 수집하고 평가하며 OVAL 결과 파일을 생성 합니다. 각 OVAL 정의의 평가 결과는 표준 출력 스트림에 인쇄됩니다. 다음 예는 OVAL 정의 파일과 관련된 가장 일반적인 시나리오를 설명합니다.

주어진 OVAL 정의 파일 내의 모든 정의를 평가하려면 다음 명령을 실행하십시오.

```
$ oscap oval eval --results oval-results.xml scap-oval.xml
```

여기서 `scap-oval.xml` 은 OVAL 정의 파일이고 `oval-results.xml` 은 OVAL 결과 파일입니다.

다음은 주어진 OVAL 정의 파일 내에서 하나의 특정 정의를 평가하는 예입니다.

```
$ oscap oval eval --id oval:rhel:def:1000 --results oval-results.xml scap-oval.xml
```

평가되는 OVAL 정의가 `oval:rhel:def:1000` 문자열 로 정의되고 `scap-oval.xml` 은 OVAL 정의 파일이고 `oval-results.xml` 은 OVAL 결과 파일입니다.

SCAP 데이터 스트림 컬렉션 내의 특정 데이터 스트림의 일부인 OVAL 구성 요소의 모든 정의를 평가하려면 다음 명령을 실행하십시오.

```
$ oscap oval eval --datastream-id ds.xml --oval-id xccdf.xml --results oval-results.xml scap-ds.xml
```

여기서 `ds.xml`은 데이터 스트림이고, `xccdf.xml`는 OVAL 컴포넌트를 지정하는 XCCDF 파일이다. `oval-results.xml`는 OVAL 결과 파일, `scap-ds.xml`는 SCAP 데이터 스트림의 컬렉션을 나타내는 파일이다.

SCAP 콘텐츠가 여러 XML 파일로 표현되면 OVAL 정의 파일을 XCCDF 파일과 함께 배포 할 수 있습니다. 이러한 경우 OVAL 정의는 검사 중에 XCCDF 파일에서 내보내는 변수에 따라 달라질 수 있으며 OVAL 정

의를 별도로 평가하면 잘못된 결과가 발생할 수 있습니다. 따라서 외부 변수는 OVAL 정의 평가 중에 사용되는 특수 파일로 내보내 저장합니다. 다음 명령은 이 시나리오의 예입니다.

```
$ oscap xccdf export-oval-variables --profile
united_states_government_configuration_baseline usgcb-rhel5desktop-xccdf.xml
$ oscap oval eval --variables usgcb-rhel5desktop-oval.xml-0.variables-0.xml
--results usgcb-results-oval.xml usgcb-rhel5desktop-oval.xml
```

여기서 `united_states_government_configuration_baseline`가 XCCDF 문서의 프로파일을 나타내고, `usgcb-rhel5desktop-xccdf.xml`가 XCCDF 문서를 지정하는 파일이며, `usgcb-rhel5desktop-oval.xml`는 OVAL 정의 파일이다 `usgcb-rhel5desktop-oval.xml-0.variables-0.xml` 은 XCCDF 파일에서 내보낸 변수가 들어있는 파일이고, `usgcb-results-oval.xml` 은 OVAL 결과 파일입니다.

OVAL 지시문 파일을 사용하여 결과를 “thin” 또는 “full” 여부를 제어 할 수 있습니다. 이 파일은 `--directives <file>` 옵션을 사용하여 OpenSCAP에서 로드 할 수 있습니다.

full 대신 thin 결과를 가능하게하는 OVAL 지시문 파일의 예 :

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_directives xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-
res="http://oval.mitre.org/XMLSchema/oval-results-5"
xmlns="http://oval.mitre.org/XMLSchema/oval-directives-5"
xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-results-5 oval-
results-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-5 oval-
common-schema.xsd http://oval.mitre.org/XMLSchema/oval-directives-5 oval-
directives-schema.xsd">
  <generator>
    <oval:product_name>OpenSCAP</oval:product_name>
    <oval:schema_version>5.8</oval:schema_version> <!-- make sure the OVAL
version matches your input -->
    <oval:timestamp>2017-02-04T00:00:00</oval:timestamp>
  </generator>
  <directives include_source_definitions="true">
    <oval-res:definition_true reported="true" content="thin"/>
    <oval-res:definition_false reported="true" content="thin"/>
    <oval-res:definition_unknown reported="true" content="thin"/>
    <oval-res:definition_error reported="true" content="thin"/>
    <oval-res:definition_not_evaluated reported="true" content="thin"/>
    <oval-res:definition_not_applicable reported="true" content="thin"/>
  </directives>
</oval_directives>
```

유스 케이스에 thin OVAL 결과가 필요한 경우 시스템 특성을 생략 할 가능성이 높습니다. 해당 효과에 `--without-syschar` 옵션을 사용할 수 있습니다 .

일반 OVAL 파일을 검사 할 때 OVAL 지시문 파일 사용 :

```
$ oscap oval eval --directives directives.xml --without-syschar --results oval-results.xml oval.xml
```

원본 DataStream에서 OVAL 구성 요소를 검색 할 때 OVAL 지시문 파일 사용 :

```
$ oscap oval eval --directives directives.xml --without-syschar --datastream-id ds.xml --oval-id oval.xml --results oval-results.xml scap-ds.xml
```

여러 파일이 배포 될 때 어떤 OVAL 파일이 사용될 지 항상 명확하지는 않습니다. XCCDF 파일을 평가하는 경우 다음을 사용할 수 있습니다.

```
$ oscap info ssg-rhel7-xccdf.xml
Document type: XCCDF Checklist
Checklist version: 1.1
Imported: 2017-01-20T14:20:43
Status: draft
Generated: 2017-01-19
Resolved: true
Profiles:
    standard
    pci-dss
    C2S
    rht-ccp
    common
    stig-rhel7-workstation-upstream
    stig-rhel7-server-gui-upstream
    stig-rhel7-server-upstream
    stig-rhevh-upstream
    ospp-rhel7-server
    nist-cl-il-al
    cjis-rhel7-server
    docker-host
    nist-800-171-cui
Referenced check files:
    ssg-rhel7-oval.xml
        system: http://oval.mitre.org/XMLSchema/oval-definitions-5
    ssg-rhel7-ocil.xml
        system: http://scap.nist.gov/schema/ocil/2
https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml.bz2
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
```

출력에서 참조 된 모든 점검 파일을 볼 수 있습니다. 이 경우에는 ssg-rhel7-oval.xml이 참조 된 것으로 간주됩니다. 이 파일의 내용을 보려면 텍스트 편집기에서 열 수 있습니다.

`oscap info` 원본 데이터 스트림 파일에서도 사용할 수 있습니다. Source DataStream은 종종 번들로 제공되는 OVAL 파일을 참조합니다. 소스 데이터 스트림에서 `oscap ds sds-split` 명령을 사용하여

OVAL 파일을 추출 할 수도 있습니다.

```
$ oscap ds sds-split ssg-rhel7-ds.xml extracted/  
$ ls -l extracted/  
scap_org.open-scap_cref_output--ssg-rhel7-cpe-dictionary.xml  
scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml  
ssg-rhel7-cpe-oval.xml  
ssg-rhel7-ocil.xml  
ssg-rhel7-oval.xml
```

원본 데이터 스트림을 분할 한 후 텍스트 편집기를 사용하여 OVAL 및 XCCDF 파일을 개별적으로 검사 할 수 있습니다. 이것은 예제 일 뿐이며 파일 이름은 분리하려는 DataStream의 내용에 따라 다르며 Source DataStream 또는 Result DataStream에서 직접 XCCDF 및 OVAL 내용을 검사 할 수도 있습니다.

XCCDF

XCCDF 벤치 마크를 평가할 때 **oscap**은 보통 XCCDF 파일, OVAL 파일 및 CPE 사전을 처리합니다. 시스템 분석을 수행하고 이 분석을 기반으로 XCCDF 결과를 산출합니다. 스캔 결과를 별도의 파일에 저장할 필요는 없지만 XCCDF 파일에 첨부 할 수는 있습니다. XCCDF 체크리스트 내의 각 XCCDF 규칙의 평가 결과는 표준 출력 스트림에 인쇄됩니다. 규칙과 관련된 CVE 및 CCE 식별자도 함께 인쇄됩니다. 다음은 단일 XCCDF 규칙에 대한 샘플 출력입니다.

Title	Verify permissions on 'group' file
Rule	usgcb-rhel5desktop-rule-2.2.3.1.j
Ident	CCE-3967-7
Result	pass

CPE dictionary는 콘텐츠가 대상 플랫폼에 적용 가능한지 여부를 결정하는 데 사용됩니다. 적용 할 수없는 콘텐츠는 각 관련 XCCDF 규칙이 적용 할 수 없음 으로 평가되도록합니다.

다음 예제는 XCCDF 벤치 마크 평가의 가장 일반적인 시나리오를 보여줍니다.

XCCDF 파일에서 특정 프로필을 평가하려면 다음 명령을 실행합니다.

```
$ oscap xccdf eval --profile Desktop --results xccdf-results.xml --cpe cpe-dictionary.xml scap-xccdf.xml
```

scap-xccdf.xml 는 XCCDF 문서이고, Desktop은 XCCDF 문서에서 선택된 프로파일이다 xccdf-results.xml는 검사 결과를 저장하는 파일이며, cpe-dictionary.xml는 CPE dictionary이다.

위의 명령에 --rule 옵션을 추가 하여 특정 규칙을 평가할 수 있습니다 .

```
$ oscap xccdf eval --profile Desktop --rule  
ensure_gpgcheck_globally_activated --results xccdf-results.xml --cpe cpe-
```

```
dictionary.xml scap-xccdf.xml
```

여기서 `ensure_gpgcheck_globally_activated` 는 평가할 데스크톱 프로필 의 유일한 규칙입니다 .

Source DataStream 원본 데이터스트림

일반적으로 필요한 모든 입력 파일은 원본 데이터 스트림에 함께 묶입니다. Source DataStream을 사용한 스캐닝은 번들 된 벤치 마크 중 어떤 것을 수행해야 하는지를 결정하는 데 사용할 수있는 몇 가지 추가 매개 변수가있는 `oscap xccdf eval` 명령에 의해 처리됩니다 .

SCAP DataStream 컬렉션 내의 DataStream에 속한 특정 XCCDF 벤치 마크를 평가하려면 다음 명령을 실행하십시오.

```
$ oscap xccdf eval --datastream-id ds.xml --xccdf-id xccdf.xml --results xccdf-results.xml scap-ds.xml
```

여기서 `scap-ds.xml`은 SCAP 데이터 스트림의 컬렉션을 나타내는 파일이고, `ds.xml`는 특정 데이터 스트림이고, `xccdf.xml`가 원하는 XCCDF 문서에 `component-ref`를 가리키는 ID이며 `xccdf-results.xml`은 스캔 결과를 포함하는 파일이다.

명령 행에서 `--datastream-id` 옵션을 생략 하면 컬렉션의 첫 번째 데이터 스트림이 사용됩니다. `--xccdf-id` 옵션을 생략 하면 `checklists` 요소의 첫 번째 구성 요소가 사용됩니다. 둘 다 생략하면 `checklists` 요소의 첫 번째 DataStream이 사용됩니다. `checklists` 요소의 첫 번째 구성 요소가 사용됩니다.

(대안, 권장하지 않음) SCAP DataStream 컬렉션 내의 DataStream의 일부인 특정 XCCDF 벤치 마크를 평가하려면 다음 명령을 실행하십시오.

```
$ oscap xccdf eval --benchmark-id benchmark_id --results xccdf-results.xml scap-ds.xml
```

여기서 `scap-ds.xml`가 SCAP 데이터 스트림의 컬렉션을 나타내는 파일이고, `benchmark_id`는 컴포넌트 내의 `xccdf:Benchmark`를 포함하는 문자열과 일치하는 `id` 속성이다. `xccdf-results.xml`는 검사 결과를 포함하는 파일이다.

Result DataStream (ARF) 결과 데이터 스트림

위의 예제에서는 `--results` 명령 줄 인수를 사용하여 XCCDF 결과 파일을 생성합니다. 또한 Result DataStream (ARF - Asset Reporting Format이라고도 함) XML을 생성하는 데 `--results-arf` 옵션을 사용할 수도 있습니다.

```
$ oscap xccdf eval --benchmark-id benchmark_id --results-arf arf-results.xml scap-ds.xml
```

Result STIG Viewer

XCCDF 검사 결과를 DISA STIG Viewer로 가져올때 Rule ID가 DISA와 일치하지 않으면 규칙의 특수 참조와 함께 `--stig-viewer` 명령 행 인수를 사용하여 DISA STIG Viewer에서 가져올 수 있는 XCCDF 결과 파일을 생성 할 수 있습니다.

```
$ oscap xccdf eval --profile stig-rhel7-disa --stig-viewer results-stig.xml  
ssg-rhel7-ds.xml
```

입력 XCCDF의 각 규칙은 STIG 규칙 ID에 대한 참조를 포함해야하며 해당 href 속성은 정확히 <http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx> 이어야합니다.

예:

```
<Rule id="rpm_verify_permissions">  
  ...  
  <reference  
href="http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx">SV-86473r  
2_rule</reference>  
  ...  
</Rule>
```

DISA STIG Viewer에 대한 자세한 내용을 보려면 [여기](#)를 클릭 하십시오 .

2.4. Remediate System 시스템 재조정(치료)

OpenSCAP은 호환되지 않는 상태에서 발견 된 시스템을 자동으로 수정합니다. 시스템 재조정의 경우 지침이있는 XCCDF 파일이 필요합니다. `scap-security-guide` 패키지에는 특정 수정 지침이 포함되어 있습니다.

시스템 재조정은 다음 단계로 구성됩니다.

- `oscap`은 정기적 인 XCCDF 평가를 수행합니다.
- 결과 평가는 OVAL 정의를 평가하여 수행됩니다. 실패한 각 규칙은 재조정 후보로 표시됩니다.
- `oscap`은 적절한 수정 요소를 검색하여 해결하고 환경을 준비하며 수정 스크립트를 실행합니다.
- 수정 스크립트의 출력은 `oscap`에 캡처되어 `rule-result` 요소 내에 저장됩니다. 수정 스크립트의 리턴 값도 저장됩니다.
- `oscap`은 수정 스크립트를 실행할 때마다 수정 스크립트가 올바르게 적용되었는지 확인하기 위해 즉시 OVAL 정의를 다시 평가합니다. 이 두 번째 실행 중에 OVAL 평가가 성공으로 돌아 오면 규칙 결과가 고정되고 그렇지 않으면 오류가 발생합니다.
- 재조정의 자세한 결과는 출력 XCCDF 파일에 저장됩니다. 두 개의 `TestResult` 요소를 포함합니다. 첫 번째 `TestResult` 요소는 재조정 이전의 검사를 나타냅니다. 두 번째 `TestResult`는 첫 번째 `TestResult`에서 파생되었으며 치료 결과를 포함합니다.

교정과 관련하여 `oscap`에는 `online`, `offline` 및 `review`의 세 가지 작동 모드가 있습니다.

Online Remediation 온라인 재조정(치료)

온라인 재조정은 검색시 수정 요소를 실행합니다. 평가 및 재조정은 단일 명령의 일부로 수행됩니다.

온라인 치료를 사용하려면 `--remediate` 명령 줄 옵션을 사용하십시오. 예를 들어, `scap-security-guide` 패키지를 사용하여 온라인 치료를 실행하려면 다음을 실행하십시오.

```
$ oscap xccdf eval --remediate --profile
xccdf_org.ssgproject.content_profile_rht-ccp --results scan-xccdf-
results.xml /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

이 명령의 출력은 두 개의 섹션으로 구성됩니다. 첫 번째 섹션은 재조정 이전 스캔 결과를 표시하고 두 번째 섹션은 재조정을 적용한 후 스캔 결과를 보여줍니다. 두 번째 부분은 고정 및 오류 결과 만 포함 할 수 있습니다. 수정 결과는 수정 이후에 수행 주사 통과 것을 나타낸다. 오류 결과도 개선을 적용한 후, 평가는 여전히 통과하지 않음을 나타냅니다.

Offline Remediation 오프라인 재조정(치료)

오프라인 재조정을 통해 픽스 실행을 연기 할 수 있습니다. 첫 번째 단계에서는 시스템이 평가되고 결과는 XCCDF 파일 의 `TestResult` 요소에 저장 됩니다.

두 번째 단계에서는 `oscap` 수정 스크립트를 실행하고 결과를 확인합니다. 결과를 입력 파일에 저장하면 데이터가 손실되지 않습니다. 오프라인 치료 중에는 입력 된 값을 기반으로 모든 데이터를 상속 하는 새 `TestResult` 요소가 만들어집니다. 새로 작성된 `TestResult` 는 실패한 룰 - 결과 요소 에서만 다릅니다. 이를 위해 치료가 실행됩니다.

`scap-security-guide` 패키지를 사용하여 오프라인 치료를 수행하려면 다음을 실행하십시오.

```
$ oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_rht-ccp --
results scan-xccdf-results.xml /usr/share/xml/scap/ssg/content/ssg-rhel7-
ds.xml

$ oscap xccdf remediate --results scan-xccdf-results.xml scan-xccdf-
results.xml
```

Remediation Review 재조정 검토

검토 모드를 사용하면 사용자가 추가 검토를 위해 파일에 수정 지침을 저장할 수 있습니다. 이 작업 중에는 재조정 내용이 실행되지 않습니다. 셸 스크립트 형식으로 재조정 지침을 생성하려면 다음을 실행하십시오.

```
$ oscap xccdf generate fix --template urn:xccdf:fix:script:sh --profile
xccdf_org.ssgproject.content_profile_rht-ccp --output my-remediation-
script.sh /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

2.5. Check Engines 엔진 점검

대부분의 XCCDF 콘텐츠는 OVAL 검사 엔진을 사용합니다. 이것은 OVAL 정의가 시스템을 평가하기 위해 평가 될 때입니다. 평가에 대한 완벽한 정보는 OVAL 사양에 정의 된대로 OVAL 결과 파일에 기록됩니다. 이 파일을 검토하여 평가에 사용 된 정의와 결과가 그대로 나타나는 이유를 확인할 수 있습니다. -- oval-results 를 사용 하지 않으면 이러한 파일이 생성되지 않습니다 .

일부 콘텐츠는 대체 체크 엔진 (예 : SCE 체크 엔진) 을 사용할 수 있습니다 .

OpenSCAP에서 지원하지 않는 검사 엔진이 필요한 검사 결과는 검사되지 않은 것으로보고됩니다. 체크 시스템이 알려져 있고 지원되지 않는 한, 체크 내용은 읽히거나 해석되지 않습니다. 다음은 알 수 없는 검사 시스템이있는 XCCDF의 평가 결과입니다.

```
$ oscap xccdf eval sds-datastream.xml
```

```
Title    Check group file contents
Rule     xccdf_org.example_rule_system_authcontent-group
Result   notchecked

Title    Check password file contents
Rule     xccdf_org.example_rule_system_authcontent-passwd
Result   notchecked

Title    Check shadow file contents
Rule     xccdf_org.example_rule_system_authcontent-shadow
Result   notchecked

...
```

검사가 수행되지 않은 규칙에 대해서도 검사되지 않은 결과가보고됩니다. notchecked는 평가할 수 있는 특정 규칙에 체크가 없다는 것을 의미합니다.

CVE, CCE, CPE 및 기타 식별자

각 XCCDF 규칙은 xccdf:ident 요소를 내부에 가질 수 있습니다. 이러한 요소를 통해 콘텐츠 작성자는 CVE, CCE, CPE 및 기타와 같은 다양한 외부 식별자를 참조 할 수 있습니다.

검사 할 때 oscap은 결과에 관계없이 검사 된 규칙의 식별자를 출력합니다. 예 :

```
Title    Ensure Repodata Signature Checking is Not Disabled For Any Repos
Rule     rule-2.1.2.3.6.a
Result   pass

Title    Verify user who owns 'shadow' file
Rule     rule-2.2.3.1.a
Ident    CCE-3918-0
Result   pass
```

Title	Verify group who owns 'shadow' file
Rule	rule-2.2.3.1.b
Ident	CCE-3988-3
Result	pass

모든 식별자 (있는 경우)는 각 규칙에 대해 표준 출력에 인쇄됩니다. 표준 출력은 소형 식별자 메타 데이터를 표시 할 수 없으므로 식별자 자체 만 표시됩니다.

식별자는 HTML 보고서 출력의 일부이기도 합니다. 식별자가 CVE 인 경우이를 클릭하여 공식 NVD 데이터 베이스에서 메타 데이터를 표시 할 수 있습니다 (인터넷 연결 필요). OpenSCAP은 다른 유형의 식별자에 대한 메타 데이터를 제공하지 않습니다.

이러한 ID를 찾을 수있는 또 다른 위치는 기계가 읽을 수있는 **Result Datastream** 파일입니다. 이 파일은 `--results-arf` 옵션을 추가하여 스캔 중에 생성 될 수 있습니다.

```
$ oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_common --
fetch-remote-resources --results-arf results.xml
/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
```

결과 데이터 스트림 파일 `results.xml`에는 `<rule-result>` 요소에 이러한 식별자가 포함됩니다.

```
<rule-result idref="xccdf_org.ssgproject.content_rule_partition_for_tmp"
time="2017-01-20T14:30:18" severity="low" weight="1.000000">
  <result>pass</result>
  <ident system="https://nvd.nist.gov/cce/index.cfm">CCE-27173-4</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg-partition_for_tmp:def:1"
href="#oval0"/>
  </check>
</rule-result>
```

OpenSCAP 1.2.9부터 HTML의 Group-By 기능을 사용하여 식별자 및 참조를 기반으로 결과를 간략하게 볼 수 있습니다.

HTML 보고서를 사용하여 식별자로 규칙을 조회 할 수도 있습니다. HTML 보고서의 검색 상자에 식별자 (예 : CCE-27173-4)를 입력 할 수 있으며 식별자가있는 규칙 만 표시됩니다. 이것은 모든 유형의 XCCDF ID 또는 참조에 사용될 수 있습니다. 규칙 제목을 클릭하면 세부 정보가 표시되고 찾은 식별자를 비롯한 모든 식별자가 표시됩니다. 이는 SCAP 콘텐츠 품질에 크게 의존합니다. 식별자가 소스 콘텐츠에 없으면 HTML 보고서에서 사용할 수 없습니다.

두 개의 식별자 (예 : CCE 식별자를 NIST 800-53 식별자에 매핑)를 매핑하려면 첫 번째 식별자를 사용하여 검색 상자를 통해 HTML 보고서에서 CCE ID를 조회해야 합니다. 그런 다음 NIST SP 800-53 ID로 그룹화하면 검색된 CCE ID와 관련된 모든 NIST 800-53 ID를 볼 수 있습니다.

번들로 제공되는 CCE 데이터

OpenSCAP은 정적 또는 제품 번들 CCE 데이터를 제공하지 않습니다. 따라서 날짜가 정의되어 있지 않기 때문에 정적 또는 제품 번들 CCE 데이터의 마지막 생성, 업데이트 및 공식 게시 날짜를 표시 할 방법이 없습니다.

From:

<https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link:

https://atl.kr/dokuwiki/doku.php/openscap_%EB%A7%A4%EB%89%B4%EC%96%BC_v1.2

Last update: **2021/05/26 13:38**

