**Типы объектов, которые присутствуют в файлах формата OVAL:**

* Определения уязвимостей (Vulnerability Definitions): Описания конкретных уязвимостей в программном обеспечении или операционной системе. Это может включать номера CVE (Common Vulnerabilities and Exposures), описания уязвимости, условия, при которых она проявляется, и другие подробности;
* Информация об уязвимостях CVE (Common Vulnerabilities and Exposures): это информация, взятая из базы данных общеизвестных уязвимостей информационной безопасности, которая показывает на какие общеизвестные уязвимости направлена найденная уязвимость (прошу прощения за тавтологию);
* Критерии (Criteria): Определения для проверки наличия или отсутствия уязвимостей на системе. Они могут включать в себя набор условий, которые должны быть выполнены для определения состояния безопасности, например, версии программного обеспечения, наличие определенных файлов и т.д;
* Патчи (Patches): Описания патчей безопасности, необходимых для исправления уязвимостей или обеспечения безопасности системы. Это может включать информацию о версиях исправлений, ссылки на загрузку патчей и прочее;
* Объекты системы (System Objects): Описания системных характеристик, таких как файлы, реестр, настройки системы и т.д. Эти объекты могут использоваться для проверки конфигураций системы на предмет соответствия безопасным стандартам.

**Лишние критерии в определениях уязвимостей:**

Подчеркну, что ЛИШНИХ критериев по моему мнению не бывает, все зависит от конкретного контекста безопасности и целей проверки ОС. Таких параметров в задании не задано. Видно, что критериев проверки этих уязвимостей чрезвычайно много. Из-за этих аспектов это задание вызывает трудности. Поэтому список лишних критериев скромен:

* Так как проявляется нагромождение критериев формата *"comment": "Red Hat Enterprise Linux 8 is installed"*, *"comment": "Red Hat CoreOS 4 is installed"* и т.д., которые указывают на наличие ПО Red Hat, в котором и проводился скан уязвимостей, информацию об установке этих ОС можно исключить. Эта информация содержится в генераторе в имени продукта;
* По 3-ей уязвимости можно заметить, что происходит скан пакетов Ruby. Я считаю, что достаточно указать только модули этого пакета которые должны быть проверены на реализацию уязвимости.
* Также видно нагромождение похожих test\_ref и много другого. Честно сказать я не понял, что с ними делать и стоит ли их убирать. Хотел бы задать этот вопрос вам.

**Вариант упрощения формата файла OVAL:**

Упрощение формата, в моем понимании, – это избавление от тех объектов, которые могут давать второстепенную информацию и нагромождают этот формат.

Больше всего места в файле занимают критерии уязвимостей, но повторюсь, по моему мнению их фильтрация может происходить только когда известна точная цель и контекст тестирования.

Для упрощения формата я решил оставить следующие данные, которые считаю самыми необходимыми:

* Definition id;
* Title;
* Информацию об уязвимости Cve;
* Description;
* Criteria (и все подразделы).

Пример, который получается при помощи моего кода:

[{'id': 'oval:com.redhat.rhba:def:20191992',

'title': 'RHBA-2019:1992: cloud-init bug fix and enhancement update (Moderate)',

'cve': ['CVE-2019-0816'],

'description': 'The cloud-init packages provide a set of init scripts for cloud instances. Cloud instances need special scripts to run during initialization to retrieve and install SSH keys, and to let the user run various scripts. Users of cloud-init are advised to upgrade to these updated packages.',

'criteria': [{'operator': 'OR',

'criteria': [{'comment': 'Red Hat Enterprise Linux must be installed',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992005'},

{'comment': 'cloud-init is earlier than 0:18.5-1.el8.4',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992001'},

{'comment': 'cloud-init is signed with Red Hat redhatrelease2 key',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992002'},

{'comment': 'Red Hat Enterprise Linux 8 is installed',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992003'},

{'comment': 'Red Hat CoreOS 4 is installed',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992004'},

{'operator': 'AND',

'criteria': [{'comment': 'cloud-init is earlier than 0:18.5-1.el8.4',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992001'},

{'comment': 'cloud-init is signed with Red Hat redhatrelease2 key',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992002'},

{'comment': 'Red Hat Enterprise Linux 8 is installed',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992003'},

{'comment': 'Red Hat CoreOS 4 is installed',

'test\_ref': 'oval:com.redhat.rhba:tst:20191992004'},

………………………>продолжение при тестировании кода.