

Nessus и OWASP ZAP

В KUMA можно импортировать сведения об активах из отчетов о результатах сканирования устройств с помощью Nessus, OWASPZAP, системы контроля защищенности и соответствия стандартам. Импорт происходит через API с помощью утилиты `import_asset_Nessus_OWASP.py`

(скрипт находится в Пресейл-Пак в папке Assets [ссылка доступна из [Дисклеймера](#)]).

Импортированные активы отображаются в веб-интерфейсе KUMA в разделе Активы. При необходимости вы можете редактировать параметры активов.

Предварительные настройки в KUMA

Создайте пользователя с ролью **главный администратор** со следующими **правами доступа для API**:

- GET /tenants
- GET /users/whoami
- POST /assets/import

Пользователь

☐ Выключен

*Имя

asset-api

*Логин

asset-api

*Адрес электронной почты

asset-api@lo.cal

☐ Получать уведомления по п

☐ Скрывать ресурсы из общег

☒ Может взаимодействовать

☐ Получать уведомления о со

☒ Группа главных администра

☒ Доступ к объектам КИИ

Взаимодействие с KUMA чере

Сгенерировать токен

Пр

Изменить пароль

Права доступа через API

GET /activeLists

☐

GET /alerts

☐

GET /assets

☐

GET /dictionaries

☐

GET /events/clusters

☐

GET /resources

☐

GET /resources/download/id

☐

GET /services

☐

GET /settings/id/id

☐

GET /system/backup

☐

GET /tenants

☒

GET /users/whoami

☒

POST /activeLists/import

☐

POST /alerts/close

☐

POST /assets/delete

☐

POST /assets/import

☒

POST /dictionaries/update

☐

POST /events

☐

POST /resources/export

☐

POST /resources/import

☐

POST /resources/toc

☐

POST /resources/upload

☐

POST /system/restore

☐

Сохранить

Сохраните настройки, **сгенерируйте токен** и отдельно сохраните его, например, в каком-либо текстовом редакторе. Нажмите **Сохранить**.

Добавьте **дополнительно поле** с названием «Description» в разделе **Параметры - Активы - Пользовательские атрибуты**.

Активы

Подробнее о пользовательских полях активов см. [в онлайн-справке](#).

При удалении настраиваемых полей также удаляются содержащиеся в них данные.

Пользовательские атрибуты

Название

Маска (регулярное выражение,
RE2)

Значение по умолчанию



Description



Сохраните изменения.

Импорт отчета от Nessus

Пример отчета от Nessus в формате CSV:

```
Plugin ID,CVE,CVSS v2.0 Base Score,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin
Output,STIG Severity,CVSS v3.0 Base Score,CVSS v2.0 Temporal Score,CVSS v3.0 Temporal Score,VPR
Score,Risk Factor,BID,XREF,MSKB,Plugin Publication Date,Plugin Modification Date,Metasploit,Core
Impact,CANVAS
"70658","CVE-2008-5161","2.6","Low","1.2.3.9","tcp","22","SSH Server CBC Mode Ciphers Enabled","The SSH
server is configured to use Cipher Block Chaining.","The SSH server is configured to support Cipher Block
Chaining (CBC)encryption. This may allow an attacker to recover the plaintext messagefrom the ciphertext.Note
that this plugin only checks for the options of the SSH server anddoes not check for vulnerable software
versions.","Contact the vendor or consult product documentation to disable CBC modecipher encryption, and
enable CTR or GCM cipher mode encryption.",,"The following client-to-server Cipher Block Chaining (CBC)
algorithmsare supported:3des-cbcaes128-cbcaes192-cbcaes256-cbcblowfish-cbcast128-cbcThe following
server-to-client Cipher Block Chaining (CBC) algorithmsare supported:3des-cbcaes128-cbcaes192-cbcaes256-
cbcbowfish-cbcast128-
cbc","","","1.9","","2.5","Low","32319","CERT:958563;CWE:200","","2013/10/28","2018/07/30","","",""
```

Далее необходимо хапустить скрипт `import_asset_Nessus_OWASP.py` по этому отчету указав необходимые параметры для его корректного запуска. Возможные опции скрипта:

```
# python import_asset.py --help
usage: import_asset.py [-h] --kuma KUMA --token TOKEN --tenant TENANT --vendor {Nessus,OWASPZAP} --
filepath FILEPATH
```

options:

-h, --help	show this help message and exit
--kuma KUMA	IP адрес сервера KUMA
--token TOKEN	Токен API
--tenant TENANT	Имя Тенанта
--vendor {Nessus,OWASPZAP}	Наименование вендора
--filepath FILEPATH	Путь до отчета

Пример запуска по отчету Nessus:

```
python3 import_asset_Nessus_OWASP.py --kuma 10.68.85.126 --token 98417b064c2a5cdfdf6bd011126c6453 --tenant Main --vendor Nessus --filepath C:\Users\ose\Downloads\nessus.csv
```

В KUMA актив будет выглядеть следующим образом:

Поиск...

☐

Название ↑

☐

12.3.11

☐

12.3.12

☐

12.3.4

☐

12.3.9

☐

10.68.85.1

☐

10.68.85.11

☐

10.68.85.13

☐

10.68.85.145

☐

10.68.85.2

☐

195.98.36.92

☐

Asset 1 Name

☐

Asset 2

☐

Asset 2 Name

☐

Asset 3 Name

☐

KSCNEW

☐

assets.name

☐

demo.lab

Информация об активе

Удалить

Изменить

Реагирование KEDR

Название

12.3.9

Тенант

Main

Источник актива

Создан вручную

Идентификатор

53dc3630-a855-4308-a5e8-92eed8faf0dc

Создано

12.12.2023 18:04:45

Последнее обновление

12.12.2023 18:18:09

IP-адрес

12.3.9

Владелец

asset-api

Категория КИИ

Информационный ресурс не является объектом КИИ

Настраиваемые поля

Description

Создано на основе отчета системы Nessus.

Категории

Другие уязвимости

SSH Server CBC Mode Ciphers Enabled

CVE 1 : CVE-2008-5161

Импорт отчета от OWASP ZAP

Пример отчета от Nessus в формате CSV:

```
{
  "@programName": "OWASP ZAP",
  "@version": "2.13.0",
  "@generated": "Mon, 25 Sep 2023 11:43:20",
  "site": [
    {
      "@name": "https://demo.lab",
      "@host": "demo.lab",
      "@port": "443",
      "@ssl": "true",
      "alerts": [
        {
          "pluginid": "10035",
          "alertRef": "10035",
          "alert": "Strict-Transport-Security Header Not Set",
          "name": "Strict-Transport-Security Header Not Set",
          "riskcode": "1",
          "confidence": "3",
          "riskdesc": "Low (High)",
          "reference": "https://ya.ru",
          "desc": "<p>HTTP Strict Transport Security (HSTS)</p>"
        }
      ]
    }
  ]
}
```

Далее необходимо хапустить скрипт `import_asset_Nessus_OWASP.py` по этому отчету указав необходимые параметры для его корректного запуска. Возможные опции скрипта:

```
# python import_asset.py --help
```

```
usage: import_asset.py [-h] --kuma KUMA --token TOKEN --tenant TENANT --vendor {Nessus,OWASPZAP} --
filepath FILEPATH
```

options:

-h, --help	show this help message and exit
--kuma KUMA	IP адрес сервера KUMA
--token TOKEN	Токен API
--tenant TENANT	Имя Тенанта
--vendor {Nessus,OWASPZAP}	Наименование вендора

--filepath FILEPATH Путь до отчета

Пример запуска по отчету OWASP ZAP:

```
python3 import_asset_Nessus_OWASP.py --kuma 10.68.85.126 --token 98417b064c2a5cdfdf6bd011126c6453 --tenant Main --vendor OWASPZAP --filepath C:\Users\ose\Downloads\owasp.json
```

В KUMA актив будет выглядеть следующим образом:

Поиск...

Название ↑

10.68.85.11

10.68.85.13

10.68.85.145

10.68.85.2

195.98.36.92

Asset 1 Name

Asset 2

Asset 2 Name

Asset 3 Name

KSCNEW

assets.name

demo.lab

lamoda.ru

localhost

test asset for comm

test_vuln

test_vuln

Информация об активе

Удалить

Изменить

Реагирование KEDR

Название

demo.lab

Тенант

Main

Источник актива

Создан вручную

Идентификатор

0f285395-8d26-4809-b33d-7857435d9dde

Создано

12.12.2023 18:10:59

Последнее обновление

12.12.2023 18:18:09

Владелец

asset-api

Полное доменное имя

demo.lab

Категория КИИ

Информационный ресурс не является объектом КИИ

Настраиваемые поля

Description

Создано на основе отчета системы OWASP ZAP.

Категории

Другие уязвимости

10035 в Strict-Transport-Security Header Not Set