Веб интерфейс

3. Знакомство с веб-интерфейсом

3.1 Вход в веб-интерфейс

Основной инструмент управления в составе **НАЙС.ОС Greenbone COMMUNITY EDITION** — веб-интерфейс (Greenbone Security Assistant, GSA). Для доступа:

1. Откройте браузер.
2. В адресной строке укажите IP-адрес веб-интерфейса устройства.
3. Авторизуйтесь учётной записью администратора веб-интерфейса, созданной при первичной настройке.

Подсказка

IP-адрес веб-интерфейса отображается в приглашении консоли входа или в меню администрирования (пункт *About*).

3.2 Рабочие панели (Dashboards)

На многих страницах в верхней части располагаются панели с наборами графиков и таблиц. Состав доступных виджетов зависит от текущего раздела. Для каждой страницы предусмотрен вариант по умолчанию; его можно восстановить кнопкой *Reset* над панелью.

3.2.1 Добавление отображения

1. Нажмите *Add* справа над панелью.
2. Выберите требуемый виджет из выпадающего списка (см. рис. 3.1).
3. Нажмите *Add*.

Подсказка

Поле ввода над списком фильтрует варианты.

Рис. 3.1 — Добавление виджета

3.2.2 Удаление отображения

Чтобы удалить виджет, нажмите значок удаления *Delete* в правом верхнем углу виджета (см. рис. 3.2).

Рис. 3.2 — Удаление виджета

3.2.3 Редактирование отображения

При наведении курсора на правую границу виджета доступен ряд действий (см. рис. 3.3):

- применить фильтр к графику или таблице (предварительно создайте и сохраните фильтр нужного типа ресурса);
- скачать график как SVG; скачать таблицу как CSV;
- показать/скрыть легенду (для графиков);
- переключить 2D/3D-режим (для графиков).

Рис. 3.3 — Дополнительные действия для виджета

3.2.4 Организация панелей

На странице *Dashboards* виджеты можно группировать и упорядочивать. Доступны предустановленные панели и произвольные наборы. Разрешено до 10 панелей. По умолчанию доступна панель *Overview* — сводка по заданиям, CVE и VT (см. рис. 3.4).

Рис. 3.4 — Панель *Overview*

3.2.4.1 Создание панели

1. Нажмите *New* на вкладках над панелью (см. рис. 3.5).

Рис. 3.5 — Создание новой панели

2. Укажите имя в поле *Dashboard Title*.
3. Выберите набор виджетов *Initial Displays* (см. рис. 3.6):
   - **Default** — как на Overview;
   - **Scan Displays** — задания, результаты, отчёты;
   - **Asset Displays** — хосты и ОС;
   - **SecInfo Displays** — VT, CVE, CERT-Bund Advisories;
   - **Empty** — пустая панель.

   Также можно выбрать уже существующую панель как шаблон.
4. Нажмите *Add* — панель появится на панели вкладок (см. рис. 3.7).

Рис. 3.6 — Параметры новой панели

Рис. 3.7 — Доступные панели во вкладках

3.2.4.2 Переименование и редактирование

Добавляйте/удаляйте виджеты согласно разд. 3.2.1 и 3.2.2; редактируйте — по разд. 3.2.3. Чтобы переименовать панель: нажмите *Rename* на вкладке панели (см. рис. 3.8), измените поле *Dashboard Title* и нажмите *Save*.

Рис. 3.8 — Переименование/удаление панели

3.2.4.3 Удаление панели

Нажмите *Delete* на вкладке панели (см. рис. 3.8).

3.3 Фильтрация содержимого страниц

Почти на каждой странице можно отфильтровать выводимые объекты. Фильтр — это выражения вида «ключ-оператор-значение», которые можно комбинировать. Контекст учитывается: доступные ключи зависят от открытой страницы. Регистронезависимо.

3.3.1 Панель фильтра

В правом верхнем углу размещена панель фильтра (см. рис. 3.9). Возможности:

- ввести выражение напрямую с учетом синтаксиса (см. разд. 3.3.3) и применить (*Update*);
- снять текущий фильтр (*Clear*);
- сбросить к значениям по умолчанию (*Reset*);
- открыть справку по фильтрам;
- открыть форму редактирования фильтра (*Edit*);
- выбрать и применить сохранённый фильтр из списка.

Рис. 3.9 — Панель фильтра

Чтобы изменить (и при необходимости сохранить) фильтр:

1. Нажмите *Edit* на панели фильтра.
2. Отредактируйте выражения (см. рис. 3.10). В поле *Filter* задайте условия.
3. Для сохранения отметьте *Store filter as* и укажите имя.
4. Нажмите *Update* — фильтр применится и, при выборе, сохранится (см. рис. 3.11).

Рис. 3.10 — Настройка фильтра

Рис. 3.11 — Выбор сохранённого фильтра

Подсказка

Для автоприменения конкретного фильтра на странице задайте «фильтр по умолчанию» в настройках пользователя (см. разд. 3.7).

3.3.2 Создание фильтра на странице «Filters»

1. Выберите *Configuration > Filters*.
2. Нажмите *New*.
3. Заполните поля (см. рис. 3.12):
   - **Name** — обязательное, выберите описательное имя;
   - **Comment** — необязательно, детали и контекст;
   - **Term** — выражения фильтра (см. разд. 3.3.3). Если пусто — используется базовый `first=1 rows=10 sort=name`;
   - **Type** — тип ресурса, к которому применим фильтр (работает только на соответствующей странице).
4. Нажмите *Save* — фильтр появится в списке выбора на панели фильтра (см. рис. 3.13).

Рис. 3.12 — Создание фильтра

Рис. 3.13 — Применение сохранённого фильтра

3.3.3 Синтаксис фильтров

Применённые выражения отображаются в левой нижней части страницы (см. рис. 3.14).

Рис. 3.14 — Пример применённых выражений

3.3.3.1 Глобальные ключи

Важно: глобальные ключи задаются один раз на запрос.

- `rows` — количество строк на страницу. По умолчанию `rows=10`. `-1` — все строки; `-2` — значение из настроек пользователя.
- `first` — номер первой строки в выдаче (например, `rows=10 first=11`).
- `sort` — сортировка по колонке по возрастанию (например, `sort=name`).
- `sort-reverse` — сортировка по убыванию.
- `tag` — выбор по тегу: `tag="server"` или `tag="server=mail"`; поддерживаются regexp.
- `tag_id` — выбор по UUID тега.

Примечание: `sort` и `sort-reverse` неприменимы на страницах деталей отчётов.

3.3.3.2 Операторы

```
=   — равно (rows=10)
~   — содержит (name~admin)
<   — меньше (created<-1w)
>   — больше (created>-1w)
regexp — регулярное выражение (regexp 192.168.[0-9]+.[0-9])
```

Не поддерживаются: `<=`, `>=`, скобки `( )`.

Особые случаи:

- Пустое значение после `=` — поиск ресурсов без значения: `comment=`.
- Если колонка не указана, поиск идёт по всем колонкам: `=192.168.15.5`.
- По умолчанию выражения объединяются через *or*. Для логического «И» используйте `and`.

  ```
  modified>2019-01-01 and name=services
  ```

  Приоритет: `and` выполняется раньше `or`.
- Отрицание — `not`: `not ~192.168.81.129`.

3.3.3.3 Текстовые фразы

```
overflow          — слова «overflow», «Overflow», «Bufferoverflow»
remote exploit    — «remote» или «exploit», или оба
```

```
remote and exploit — оба слова
"remote exploit"   — точная фраза
regexp 192.168.[0-9]+.[0-9] — по регулярному выражению
```

3.3.3.4 Временные выражения

Абсолютные: `YYYY-MM-DDTHHhMM`, например `2024-10-02T13h50`.

```
modified>2024-09-01T15h00 and modified<2024-09-30T15h00
```

Относительные: относительно текущего времени. Прошлое — с «-».

```
created>-5d   (за последние 5 дней)
Единицы: s, m, h, d, w, M(30 дней), y(365 дней)
```

Комбинации вида `5d1h` не допускаются — используйте суммарно в часах, например `121h`.

3.3.4 Примеры выражений

```
127.0.0.1
127.0.0.1 iana
127.0.0.1 and iana
=127.0.0.1
not ip:192.168.100.[0-9]{1,3}
regexp 192.168.[0-9]+.[0-9]
name=localhost
name~local
name:^local
port_list~tcp
modified>2023-04-03 and modified<2023-04-05
created>2023-04-03T13h00
rows=20 first=1 sort=name
created>-7d
tag="geo:long=52.2788
tag~geo
```

3.3.5 Управление фильтрами

Список

Выберите *Configuration > Filters* (см. рис. 3.15). Для каждого фильтра отображаются:

Name, *Term*, *Type*. Доступные действия: удалить в корзину, редактировать, клонировать, экспортировать в XML.

Массовые операции: под списком доступны *Bulk delete* и *Bulk export* по выборке из выпадающего списка.

Рис. 3.15 — Управление фильтрами

Страница деталей

Клик по имени открывает детали. Вкладки:

- **Information** — общие сведения (терм, тип, где используется);
- **User Tags** — назначенные теги (см. разд. 3.4);
- **Permissions** — права доступа.

Действия: справка, переход к списку, создание, клонирование, редактирование, удаление в корзину, экспорт.

3.4 Использование тегов (Tags)

Теги — метаданные, которые связываются с одним или несколькими ресурсами одного типа. Их можно применять в фильтрах (см. разд. 3.3 и 3.3.3.1).

3.4.1 Создание тега для одного ресурса

1. Откройте страницу деталей ресурса.
2. Перейдите на вкладку *User Tags* и нажмите *Add*.
3. Заполните поля:
    - **Name** (обязательно), **Comment** (необязательно), **Value** (значение для уточнения);
    - **Resource Type** и **Resources** — установлены для текущего ресурса;
    - **Active** — доступность тега.
4. Нажмите *Save*.

3.4.2 Создание тега для нескольких ресурсов

1. Откройте список нужного типа ресурсов и отфильтруйте выборку.
2. Внизу списка выберите область применения: *Apply to page contents* или *Apply to all filtered* (см. рис. 3.16), либо *Apply to selection* и отметьте чекбоксы нужных строк, затем нажмите *Add Tag*.
3. Выберите тег в *Choose Tag* или создайте новый (см. рис. 3.17).
4. Нажмите *Add Tag*.

Рис. 3.16 — Выбор ресурсов

Рис. 3.17 — Выбор тега для нескольких ресурсов

3.4.3 Создание тега на странице «Tags»

1. Выберите *Configuration > Tags*.
2. Нажмите *New*.
3. Заполните: *Name* (обязательно), *Comment*, *Value*, *Resource Type*, *Resources*, *Active* (см. рис. 3.18).
4. Нажмите *Save*.

Рис. 3.18 — Создание нового тега

3.4.4 Управление тегами

Список

Configuration > Tags — показывает *Name*, *Value*, *Active*, *Resource Type*, *Number of Resources*, *Modified*. Действия: включить/выключить, удалить в корзину, редактировать, клонировать, экспортировать XML.

Массовые операции доступны под списком (удаление/экспорт выбранных).

Детали

Вкладки: *Information* (значение, тип ресурса, активность), *Assigned Items* (список связанных ресурсов), *Permissions*. Действия: справка, к списку, создать, клонировать, редактировать, удалить в корзину, экспорт, включить/выключить.

3.5 Корзина (Trashcan)

Administration > Trashcan — список объектов в корзине по типам (см. рис. 3.19). Объекты в корзине ещё не удалены окончательно; полное удаление — вручную для объекта или при очистке корзины.

Empty Trash — очистить корзину целиком.

Рис. 3.19 — Содержимое корзины

В разделе типа ресурса (см. рис. 3.20): *Restore* — восстановить (доступно, если нет зависимостей в корзине), *Delete* — удалить окончательно (недоступно, если от объекта зависят другие).

Рис. 3.20 — Восстановление/удаление объекта

3.6 Статус обновлений (Feed Status)

Administration > Feed Status — состояние синхронизации SecInfo (см. рис. 3.21): *Type* (NVT, SCAP, CERT, GVMD_DATA), *Content*, *Origin*, *Version*, *Status*. Во время обновления отображается *Update in progress...* для всех типов.

Рис. 3.21 — Состояние фидов

3.7 Настройки пользователя

1. Наведите курсор на значок профиля в правом верхнем углу.
2. Выберите *Settings* (см. рис. 3.22).

Рис. 3.22 — Переход к настройкам

3. Выберите вкладку категории настроек.
4. Нажмите *Edit* рядом с нужной опцией и внесите изменения (см. рис. 3.23).

Рис. 3.23 — Изменение настроек

Ключевые параметры:

- **General**:
  - *Timezone* — часовой пояс отображения; система хранит данные в UTC.
  - *Password* — смена пароля.
  - *User Interface Language* — язык интерфейса (по умолчанию — из браузера).
  - *Rows Per Page* — количество строк на страницу (слишком большие значения замедляют загрузку; фильтры могут переопределять).
  - *Details/List/Report Export File Name* — шаблоны имён экспортируемых файлов. Подстановки: `%C`, `%c`, `%D`, `%F`, `%M`, `%m`, `%N`, `%T`, `%t`, `%U`, `%u`, `%%`.
  - *Auto Cache Rebuild* — авто-перестроение кэша; при массовых операциях можно временно отключать.
- **Severity**:
  - *Dynamic Severity* — изменять ли критичность существующих результатов при изменении VT.
  - *Default Severity* — критичность по умолчанию (если у VT не задана).
- **Defaults** — значения по умолчанию для различных настроек.
- **Filters** — назначение фильтров по умолчанию для страниц (применяются автоматически).

3.8 Открытие руководства

Руководство доступно по значку справки в правом верхнем углу. Также на каждой странице можно открыть релевантную главу, нажав значок справки в левом верхнем углу.

3.9 Выход из веб-интерфейса

Для выхода наведите курсор на значок профиля в правом верхнем углу и выберите *Log Out* (см. рис. 3.24). При бездействии выполняется авто-выход (значение тайм-аута по умолчанию — 15 минут). Наведите курсор на индикатор, чтобы увидеть оставшееся время; кликом его можно сбросить.