

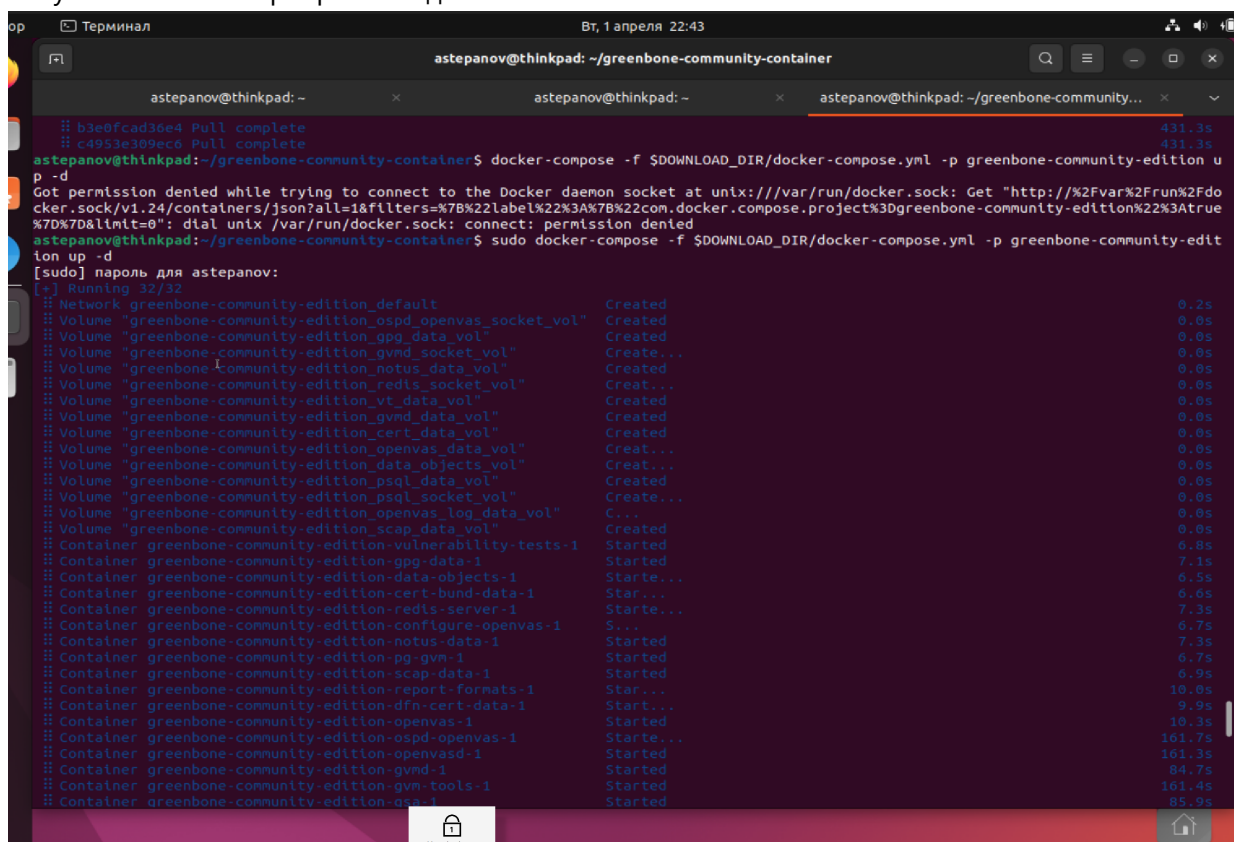
Модуль 2. Сканирование на уязвимости. Сетевые сканирования (vo_HW)

Задание №2. Сканирование с помощью OpenVAS

Шаг 1. Установка OpenVAS.

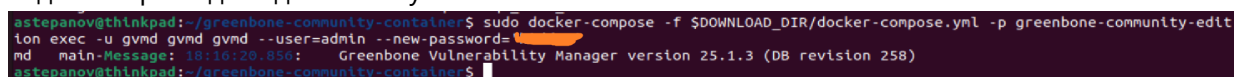
Устанавливаем OpenVas на виртуальной машине Ubuntu, следуя инструкции из урока по OpenVas в данном модуле

1. Устанавливаем **docker**, **docker-compose**, скачиваем нужный docker-контейнер (**greenbone-community-edition**)
2. Запускаем контейнер в режиме демона



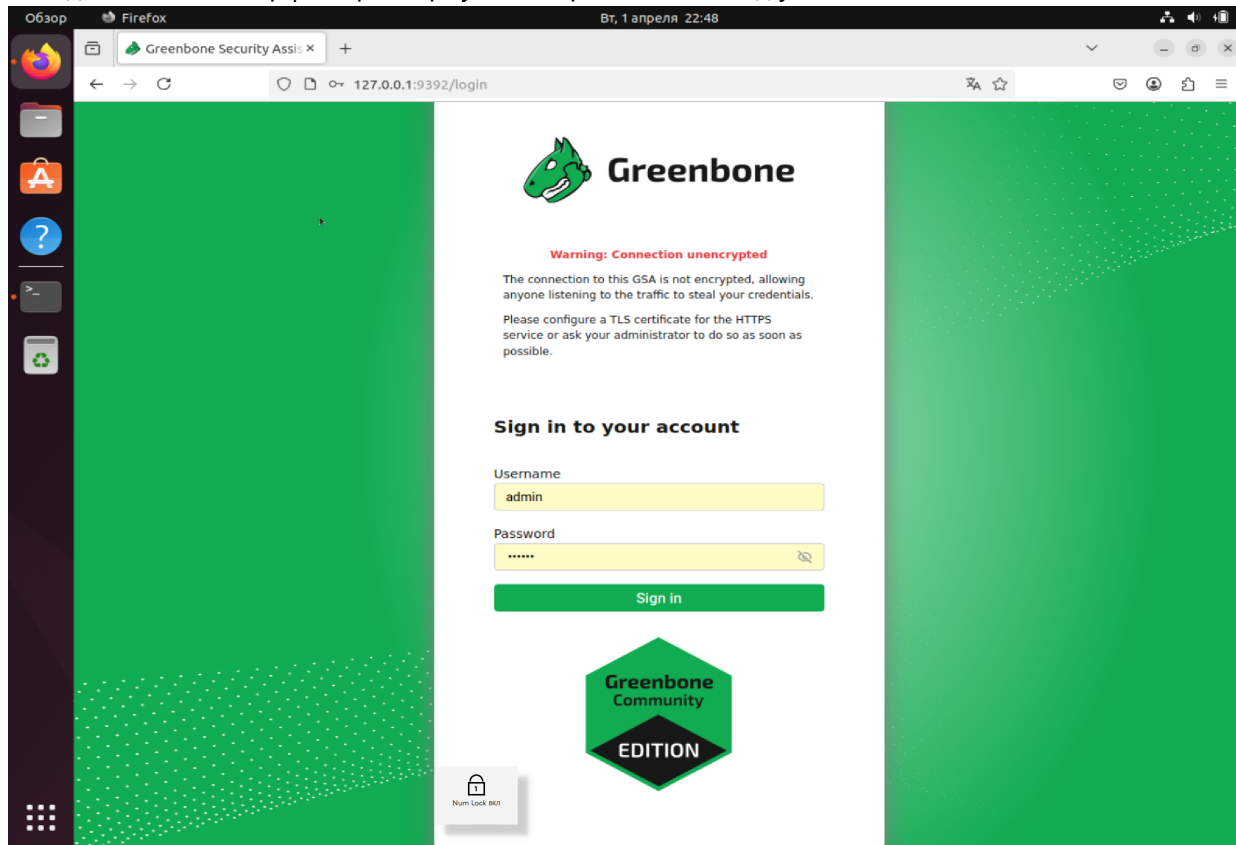
```
astepanov@thinkpad: ~/greenbone-community-container
astepanov@thinkpad: ~
astepanov@thinkpad: ~/greenbone-community-container$ docker-compose -f $DOWNLOAD_DIR/docker-compose.yml -p greenbone-community-edition up -d
Got permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json?all=1&filters=%7B%22label%22%3A%7B%22com.docker.compose.project%3Dgreenbone-community-edition%22%3Atrue%7D%7D&limit=0": dial unix /var/run/docker.sock: connect: permission denied
astepanov@thinkpad: ~/greenbone-community-container$ sudo docker-compose -f $DOWNLOAD_DIR/docker-compose.yml -p greenbone-community-edition up -d
[sudo] пароль для аstepanov:
Running 32/32
Network greenbone-community-edition_default Created 0.2s
Volume "greenbone-community-edition-ospd-openvas-socket-vol" Created 0.0s
Volume "greenbone-community-edition-gpg-data-vol" Created 0.0s
Volume "greenbone-community-edition-gvmd-socket-vol" Created 0.0s
Volume "greenbone-community-edition-notus-data-vol" Created 0.0s
Volume "greenbone-community-edition-redis-socket-vol" Created 0.0s
Volume "greenbone-community-edition-vt-data-vol" Created 0.0s
Volume "greenbone-community-edition-gvmd-data-vol" Created 0.0s
Volume "greenbone-community-edition-cert-data-vol" Created 0.0s
Volume "greenbone-community-edition-openvas-data-vol" Created 0.0s
Volume "greenbone-community-edition-data-objects-vol" Created 0.0s
Volume "greenbone-community-edition-psql-data-vol" Created 0.0s
Volume "greenbone-community-edition-psql-socket-vol" Created 0.0s
Volume "greenbone-community-edition-openvas-log-data-vol" Created 0.0s
Volume "greenbone-community-edition-scrap-data-vol" Created 0.0s
Container greenbone-community-edition-vulnerability-tests-1 Started 6.8s
Container greenbone-community-edition-gpg-data-1 Started 7.1s
Container greenbone-community-edition-data-objects-1 Started 6.5s
Container greenbone-community-edition-cert-bund-data-1 Started 6.6s
Container greenbone-community-edition-redis-server-1 Started 7.3s
Container greenbone-community-edition-configure-openvas-1 Started 6.7s
Container greenbone-community-edition-notus-data-1 Started 7.3s
Container greenbone-community-edition-pg-gvm-1 Started 6.7s
Container greenbone-community-edition-report-formats-1 Started 6.9s
Container greenbone-community-edition-dfn-cert-data-1 Started 10.0s
Container greenbone-community-edition-openvas-1 Started 9.9s
Container greenbone-community-edition-ospd-openvas-1 Started 10.3s
Container greenbone-community-edition-openvasd-1 Started 161.7s
Container greenbone-community-edition-gvmd-1 Started 161.3s
Container greenbone-community-edition-gvm-tools-1 Started 84.7s
Container greenbone-community-edition-gvm-1 Started 161.4s
Container greenbone-community-edition-gsa-1 Started 85.9s
```

3. Задаем пароль для админской учетной записи



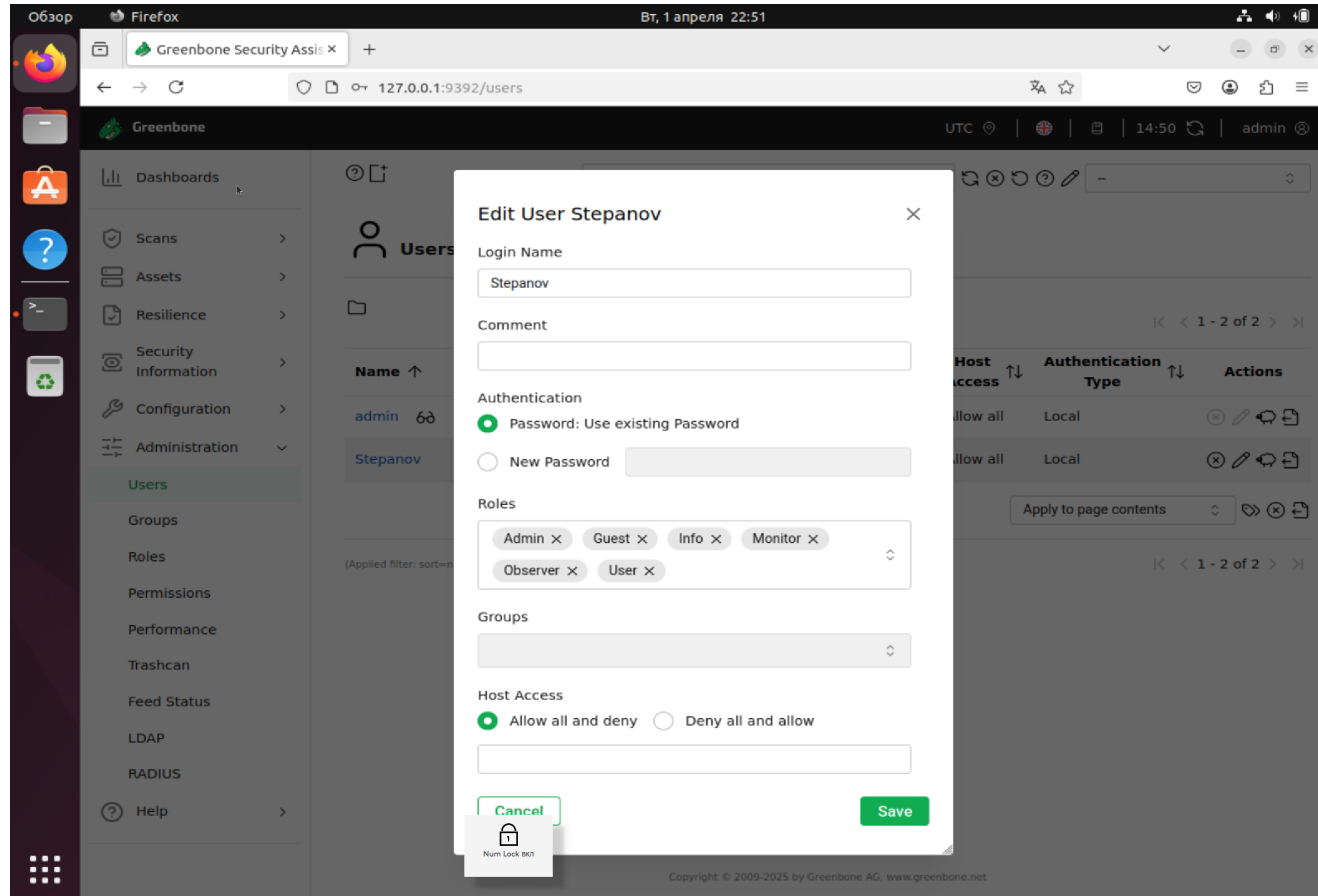
```
astepanov@thinkpad: ~/greenbone-community-container$ sudo docker-compose -f $DOWNLOAD_DIR/docker-compose.yml -p greenbone-community-edition exec -u gvm gvm gvm --user=admin --new-password=
md main-Message: 19:10:29.850: Greenbone Vulnerability Manager version 25.1.3 (DB revision 258)
astepanov@thinkpad: ~/greenbone-community-container$
```

4. Заходим в web-интерфейс развернутого приложения под учеткой **admin**



Шаг 2. Создать пользователя

Создаем пользователя Stepanov



Шаг 3. Настроить новый список для сканирования

Создаем новый список для сканирования согласно требованию в задании

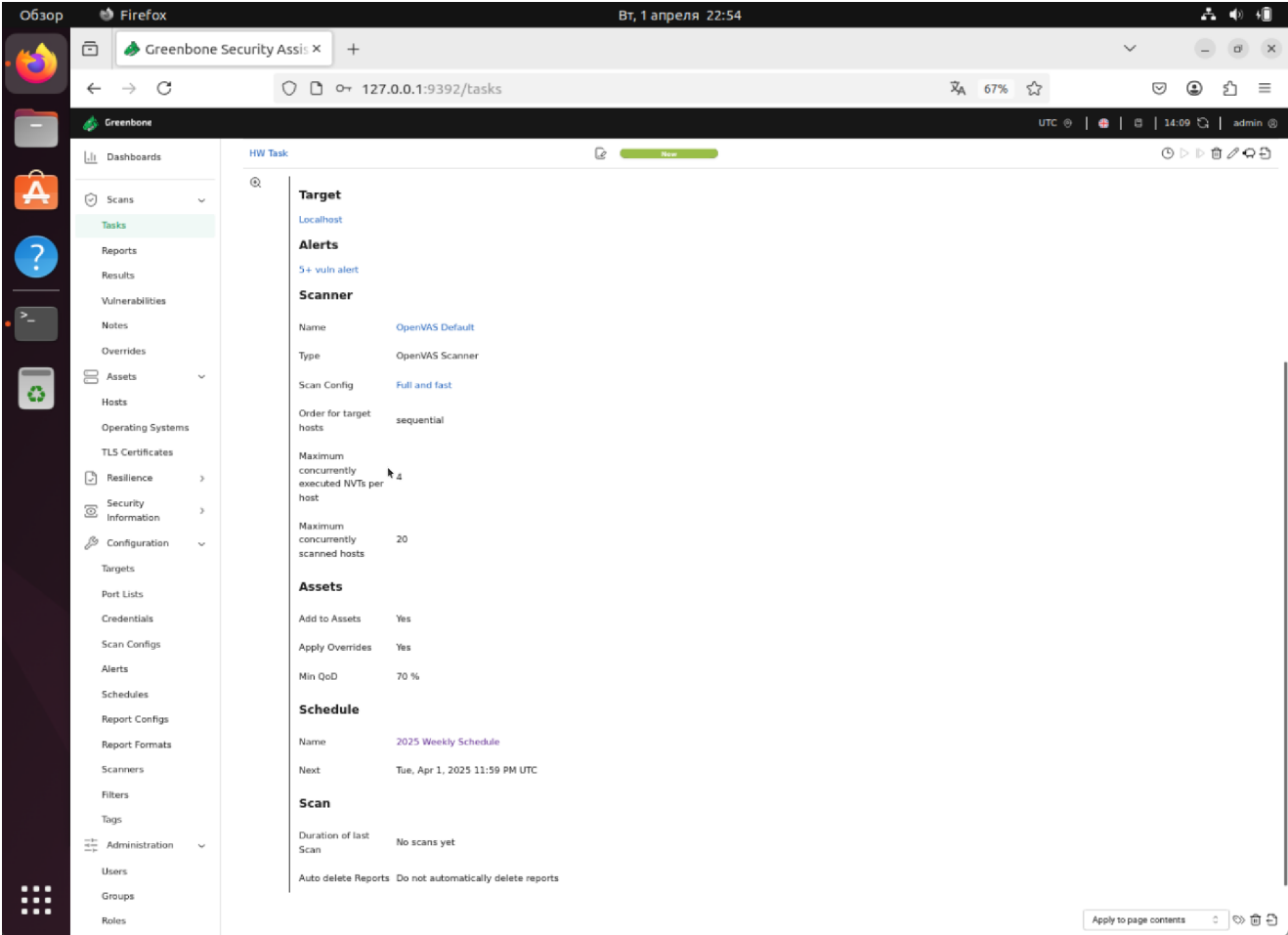
The screenshot displays the Greenbone Security Assistant (GSA) web interface. The browser is Firefox, and the URL is `127.0.0.1:9392/targets`. The interface is in Russian, with the top bar showing the date and time (Вр, 1 апреля 22:52) and the user (admin). The left sidebar contains a navigation menu with options like Results, Vulnerabilities, Notes, Overrides, Assets, Hosts, Operating Systems, TLS Certificates, Resilience, Security Information, Configuration, Targets, Port Lists, Credentials, Scan Configs, Alerts, Schedules, Report Configs, Report Formats, and Scanners. The 'Targets' section is currently selected. The main content area shows a table with one target, 'Localhost', and its configuration details. The configuration includes a list of hosts (192.168.1.0/24), a maximum of 253 hosts, and various scan options. A 'Num Lock On' notification is visible at the bottom left.

Name ↑	Hosts ↑↓	IPs ↑↓	Port List ↑↓	Credentials	Actions
Localhost	192.168.1.0/24	253	All TCP and Nmap top 100 UDP		

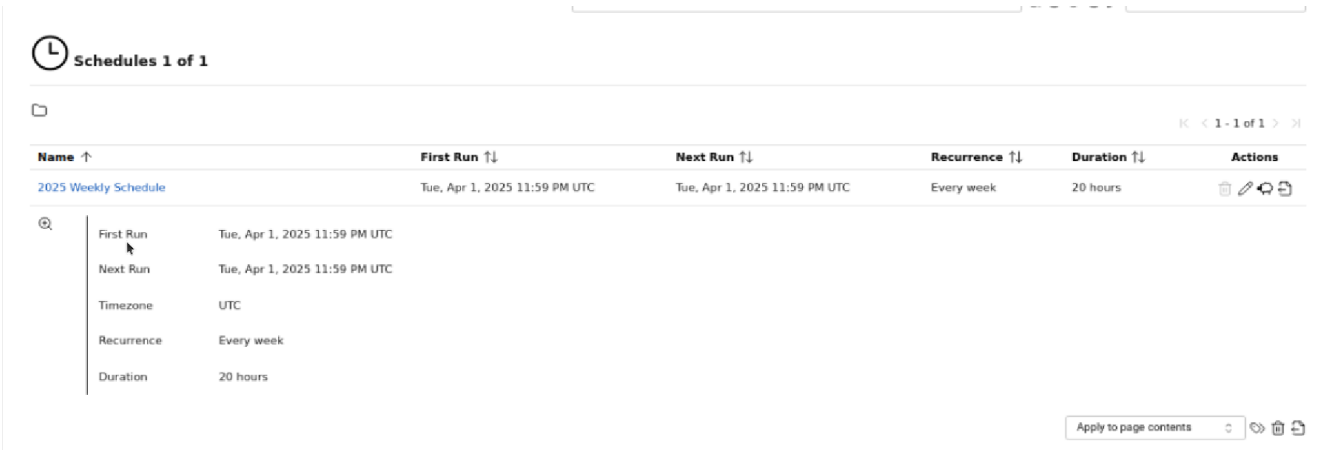
Hosts	
Included	192.168.1.0/24
Excluded	192.168.1.100
Maximum Number of Hosts	253
Allow simultaneous scanning via multiple IPs	Yes
Reverse Lookup Only	No
Reverse Lookup Unify	No
Alive Test	Scan Config Default
Port List	All TCP and Nmap top 100 UDP

Шаг 4. Создать новый таск на сканирование

Создаем новую задачу на сканирование под названием **HW Task**



Внутри задачи создаем новое расписание по которому будем производить проверку на уязвимости в течение следующего года под названием **2025 Weekly Schedule**



Шаг 5. Создать алерт, который будет обращаться с помощью метода HTTP Get на `http://127.0.0.1:8000/alert` при появлении уязвимости с уровнем критичности `>5.0`

Создаем алерт "5+ vuln alert" согласно заданию и устанавливаем его в нашей задаче.

Edit Alert 5+ vuln alert ✕

5+ vuln alert

Comment

алерт, который будет обращаться с помощью метода HTTP Get на http://127.0.0.1:8000/alert n

Event

☒ Task run status changed to

New

☐ New

NVTs

☐ Ticket Received

☐ Assigned Ticket Changed

☐ Owned Ticket Changed

Condition

☐ Always

☒ Severity at least

5

☐ Severity Level

changed

☐ Filter

matches at least

1

result(s) NVT(s)

☐ Filter

matches at least

1

result(s) more than previous scan

Report Content

Compose

Delta Report

☒ None

☐ Previous completed report of the same task

☐ Report with ID

Method

HTTP Get

HTTP Get URL

http://127.0.0.1:8000/alert

Active

☒ Yes

☐ No

Cancel

Save

Шаг 6. Сохранить задачу

Страница с сохраненным заданием

Обзор Firefox Вр, 1 апреля 23:00

Greenbone Security Assi: x 127.0.0.1:9392/tasks 67%

Greenbone UTC 14:56 admin

Filter

Tasks 1 of 1

Tasks by Severity Class (Total: 1)

Tasks with most High Results per Host

Tasks by Status (Total: 1)

HW Task

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

The screenshot displays the Greenbone Security Assistant (GSA) web interface in a Firefox browser. The address bar shows the URL '127.0.0.1:9392/tasks'. The left sidebar contains a navigation menu with categories like Dashboards, Scans, Tasks, Reports, Results, Vulnerabilities, Notes, Overrides, Assets, Hosts, Operating Systems, TLS Certificates, Resilience, Security Information, and Configuration. The main content area is titled 'Tasks 1 of 1' and features three summary charts: 'Tasks by Severity Class (Total: 1)' showing a single bar for 'N/A', 'Tasks with most High Results per Host' showing a line graph, and 'Tasks by Status (Total: 1)' showing a single bar for 'New'. Below these charts is a table with columns for Name, Status, Reports, Last Report, Severity, Trend, and Actions. The table contains one entry, 'HW Task', with a status of 'New'. The interface also includes a filter bar at the top, a sidebar with various icons, and a footer with the copyright notice 'Copyright © 2009-2025 by Greenbone AG, www.greenbone.net'.