

Развертывание и использование инфраструктурного сканера

--

Для начала работ вам понадобится:

- *docker*

Подробная установка docker рассматривалась в методических материалах к предыдущим урокам

--

Запустим контейнер с инструментом openvas, используя image пользователя mikesplain:

```
$ docker run -d -p 443:443 -p 9390:9390 --name openvas mikesplain/openvas
```

```
filipp@filipp-notebook:~$ docker run -d -p 443:443 -p 9390:9390 --name openvas mikesplain/openvas
836206ff1c3a9e5f31e14dec458a34fdb098ea6c6fda7e85a0b2b332b12c875c
```

Убедимся в том, что контейнер успешно запущен:

```
$ docker ps
```

```
filipp@filipp-notebook:~$ docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
836206ff1c3a	mikesplain/openvas	"/bin/sh -c /start"	7 seconds ago	Up 6 seconds	0.0.0.0:443->443/tcp, :::443->443/tcp, 0.0.0.0:9390->9390/tcp, :::9390->9390/tcp

openvas

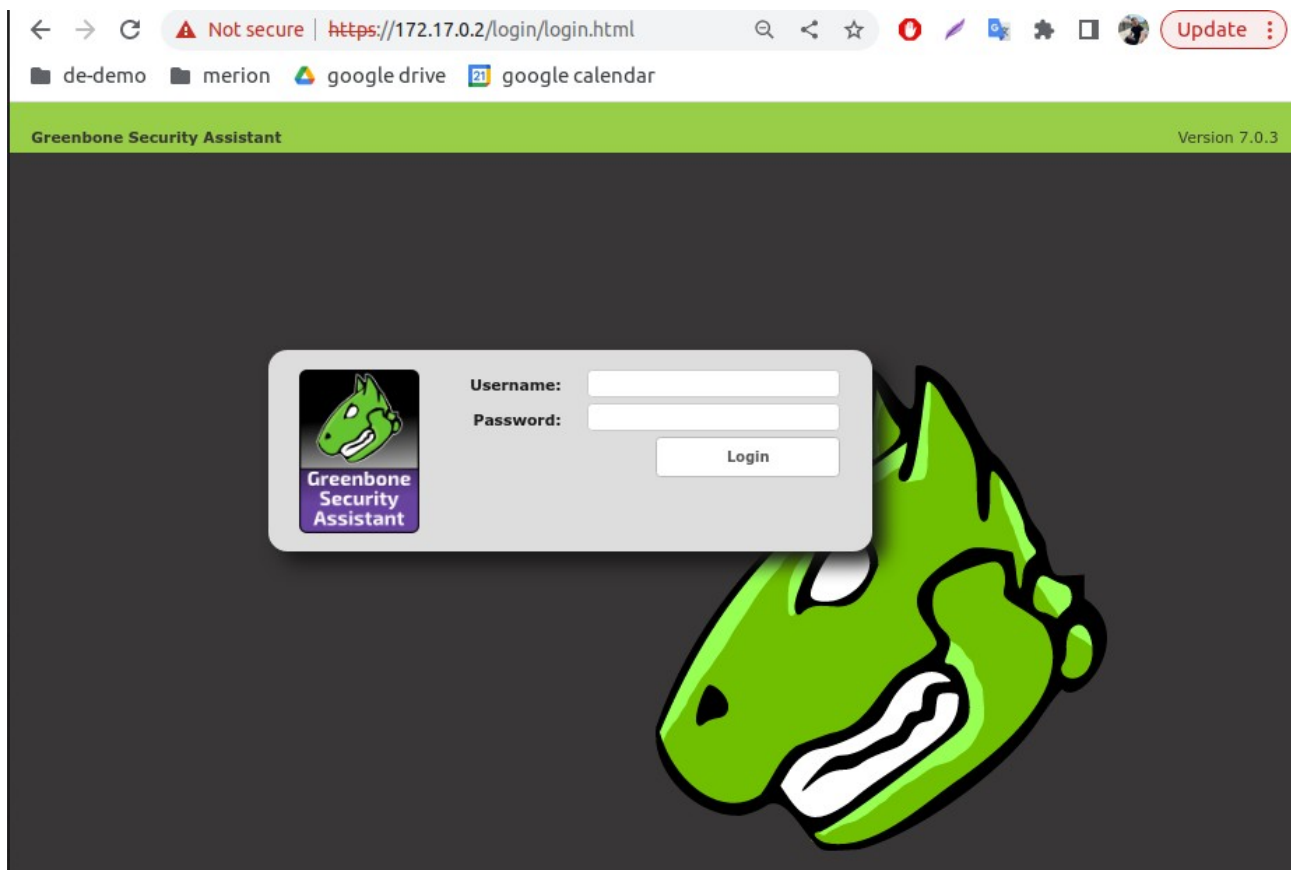
Контейнер запущен успешно, вызовем команду просмотра ip-адреса контейнера:

```
$ docker network inspect bridge
```

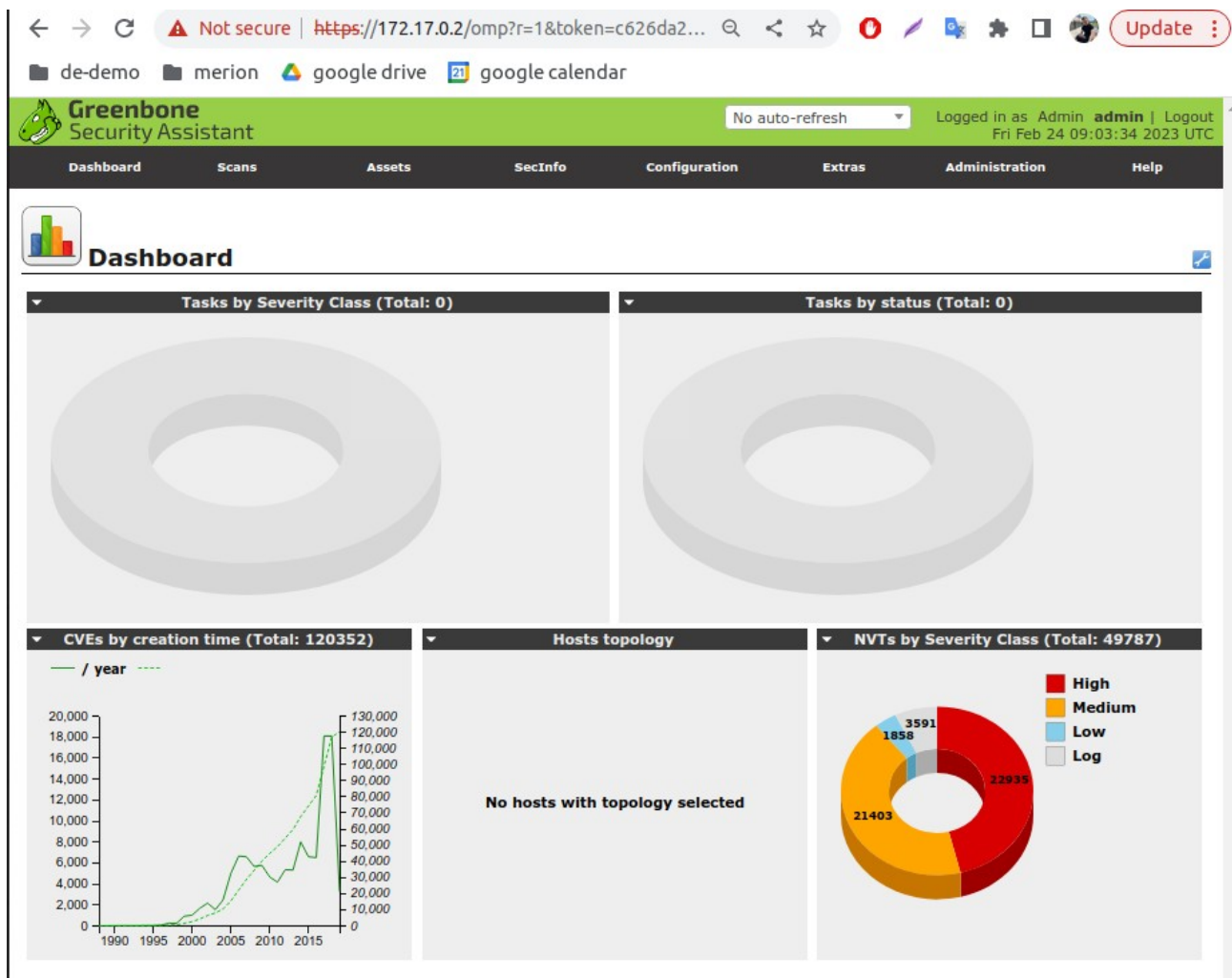
```
Display detailed information on one or more networks
filipp@filipp-notebook:~$ docker network inspect bridge
[
  {
    "Name": "bridge",
    "Id": "1008bccb2889abe091af1c674362551ff015c49e2f64195965e459ef78c65ce9",
    "Created": "2023-02-19T15:47:21.54871149+03:00",
    "Scope": "local",
    "Driver": "bridge",
    "EnableIPv6": false,
    "IPAM": {
      "Driver": "default",
      "Options": null,
      "Config": [
        {
          "Subnet": "172.17.0.0/16",
          "Gateway": "172.17.0.1"
        }
      ]
    },
    "Internal": false,
    "Attachable": false,
    "Ingress": false,
    "ConfigFrom": {
      "Network": ""
    },
    "ConfigOnly": false,
    "Containers": {
      "836206ff1c3a9e5f31e14dec458a34fdb098ea6c6fda7e85a0b2b332b12c875c": {
        "Name": "openvas",
        "EndpointID": "069421945b3d2aeed9c683e2eadd829ee49eed72b29664d8454fff1f155a964a",
        "MacAddress": "02:42:ac:11:00:02",
        "IPv4Address": "172.17.0.2/16",
        "IPv6Address": ""
      }
    }
  }
]
```

Используя ip-адресс, в браузере выполним переход в веб-интерфейс инструмента openvas:

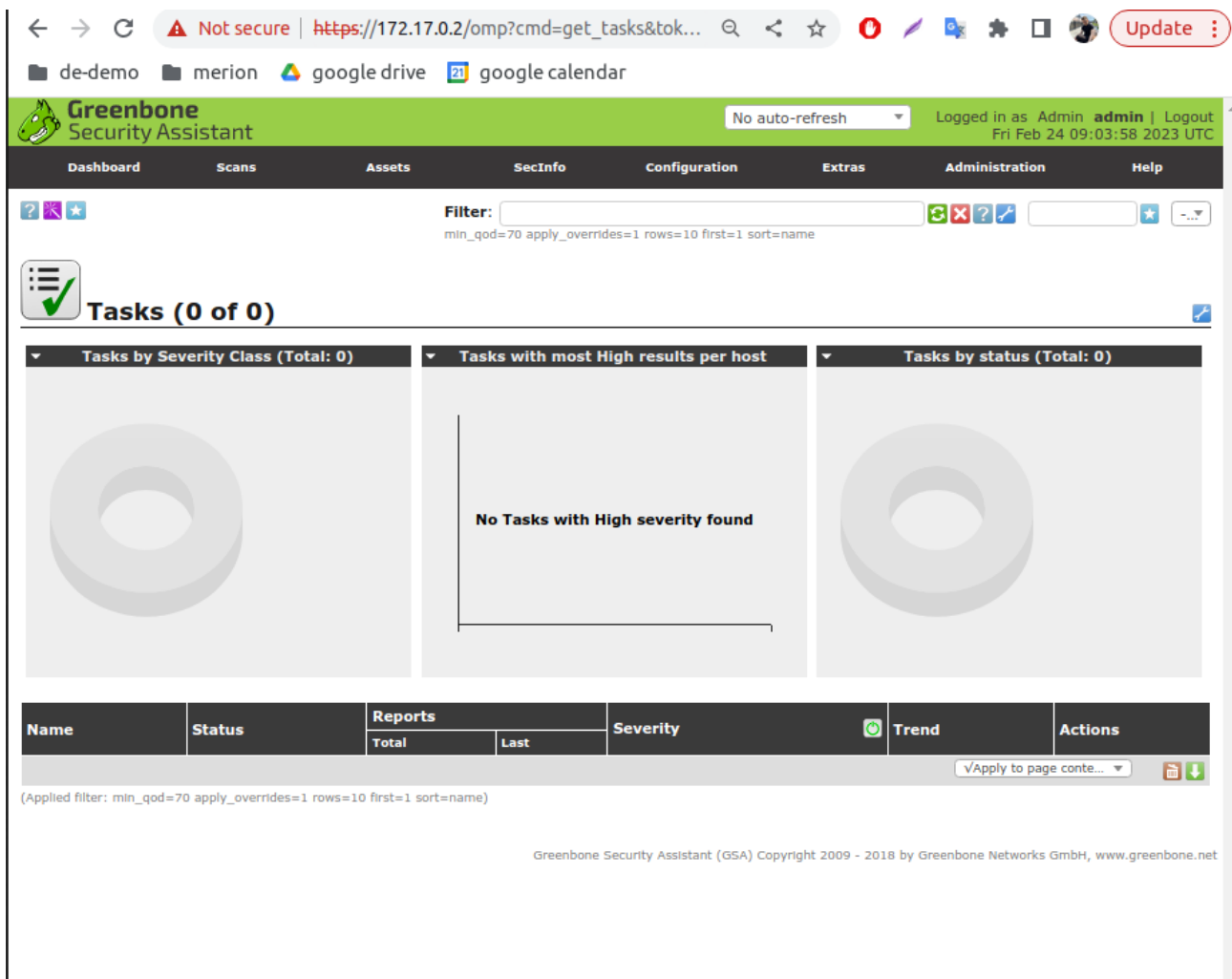
browser: <https://172.17.0.2/>



Авторизуемся, используя административные учетные данные по умолчанию (admin:admin):



Переходим в раздел "Scan", выбираем в выпадающем меню поле "Tasks":



В верхнем левом углу нажимаем на кнопку со звездочкой и выбираем "New Task":

Tasks (0 of 0)

New Task

Name: unnamed

Comment:

Scan Targets: ★

Alerts: ★

Schedule: -- ☐ Once ★

Add results to Assets: ☒ yes ☐ no

Apply Overrides: ☒ yes ☐ no

Min QoD: 70 %

Alterable Task: ☐ yes ☒ no

Auto Delete Reports: ☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest 5 reports

Scanner: OpenVAS Default

Scan Config: Full and fast

Network Source Interface:

Order for target hosts: Sequential

Maximum concurrently executed NVTs per host: 4

Maximum concurrently scanned hosts: 20

Create

Справа от поля "Scan Target" нажимаем на кнопку со звездочкой и переходим в интерфейс указания нового target для сканирования.

Далее указываем наименование target и ip-address (в моем случае это localhost, если вы сканируете инфраструктуру, убедитесь что обеспечен сетевой доступ по портам 22, 80, 443 для полноты возможностей сканирования):

Tasks (0 of 0)

New Task

Name

task1

New Target

Name

localhost

Comment

Hosts

☒ Manual

192.168.100.202

☐ From file

Choose File

No file chosen

☐ From host assets (0 hosts)

Exclude Hosts

Reverse Lookup Only

☐ Yes

☒ No

Reverse Lookup Unify

☐ Yes

☒ No

Port List

All IANA assigned TCP 2012...★

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

-- on port 22★

SMB

--★

ESXi

--★

SNMP

--★

Create

Сохраняем изменение, нажав кнопку "Create". Убедимся что в настройках Task подставился созданный target:

tasks (0 of 0)

New Task

Name

task1

Comment

Scan Targets

localhost

Alerts

Schedule

--

☐ Once

Add results to Assets

☒ yes
☐ no

Apply Overrides

☒ yes
☐ no

Min QoD

70

%

Alterable Task

☐ yes
☒ no

Auto Delete Reports

☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest

5

reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Network Source Interface

Order for target hosts

Sequential

Maximum concurrently executed NVTs per host

4

Maximum concurrently scanned hosts

20

Create

Нажимаем кнопку "Create". Созданный Task отображается в списке tasks, но еще не запущен

Name		Status		Reports		Severity	Trend	Actions
				Total	Last			
task1		New						

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Для запуска Task нажимаем кнопку начала сканирования ("Start") в разделе "Actions" нашего Task. Состояние Task изменилось на "Requested":



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
task1	Requested	0 (1)				

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Через некоторое время обновим страницу и убедимся, что строка состояния нашего Task изменяется на количество процентов от выполненного сканирования:



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
task1	28 %	0 (1)				

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

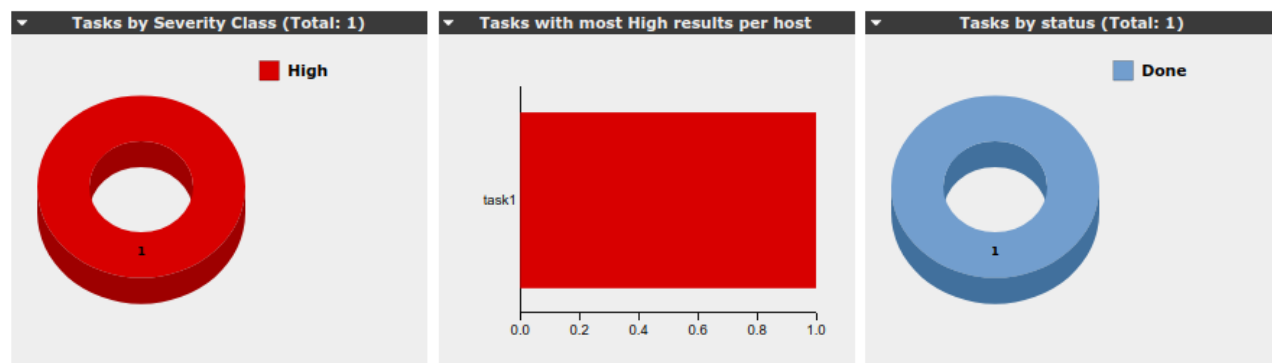
Сканирование может занять продолжительное время

--

Дождемся завершения сканирования, убедившись, что статус сканирования изменился на "Done":



Tasks (1 of 1)



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
task1	Done	1 (1)	Feb 24 2023	10.0 (High)		

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Перейдем к результатам сканирования, нажав на статус сканирования:

Greenbone Security Assistant

Logged in as Admin **admin** | Logout
Fri Feb 24 09:30:12 2023 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous X... Done

Filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70



Report: Results (4 of 29)

ID: d0406820-0db2-4258-a0d5-f63aea687b1e
Modified: Fri Feb 24 09:27:15 2023
Created: Fri Feb 24 09:11:51 2023
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
OpenVAS / Greenbone Vulnerability Manager Default Credentials	10.0 (High)	100%	192.168.100.202	9390/tcp	
SSL/TLS: Certificate Expired	5.0 (Medium)	99%	192.168.100.202	443/tcp	
SSL/TLS: Certificate Expired	5.0 (Medium)	99%	192.168.100.202	9390/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.100.202	general/tcp	

(Applied filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

Backend operation: 0.18s


Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

В открывшемся отчете можем ознакомиться со всеми результатами сканирования, нажав на них и перейдя в подробное описание:



Result: SSL/TLS: Certificate Expired

ID: 8b2db54f-a9fb-4751-a244-7b27214e11cc
Created: Fri Feb 24 09:12:47 2023
Modified: Fri Feb 24 09:12:47 2023
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
SSL/TLS: Certificate Expired	5.0 (Medium)	99%	192.168.100.202	9390/tcp	
Summary The remote server's SSL/TLS certificate has already expired.					
Vulnerability Detection Result The certificate of the remote service expired on 2020-08-20 19:18:24. Certificate details: subject ...: C=DE,L=Osnabrueck,O=openVAS Users,CN=218ffb30ff7a subject alternative names (SAN): None issued by ..: C=DE,L=Osnabrueck,O=openVAS Users,OU=Certificate Authority for 218ffb30ff7a serial: 5B7C65801F8422EBBDAD2299 valid from : 2018-08-21 19:18:24 UTC valid until: 2020-08-20 19:18:24 UTC fingerprint (SHA-1): 6B34D170BC2D0EAE4DB2D6122E2DA7E94F0ADF6F fingerprint (SHA-256): A672ACF698B0944271599E210BF04BF20736E3CCB5862FAF3EFAC987241BC4B9					
Solution Solution type:  Mitigation Replace the SSL/TLS certificate by a new one.					
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.					
Vulnerability Detection Method Details: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955) Version used: \$Revision: 11103 \$					

Подобным образом можем отработать все срабатывания, предприняв необходимые действия по их устранению. Полезно принимать в расчет рекомендации по митигации обнаруженных рисков (поле "Solution")

--