实验环境

```
目标靶机：OWASP_Broken_Web_Apps_VM_1.2
测试渗透机：Windows10 /Kali
```

nmap

nmap简介

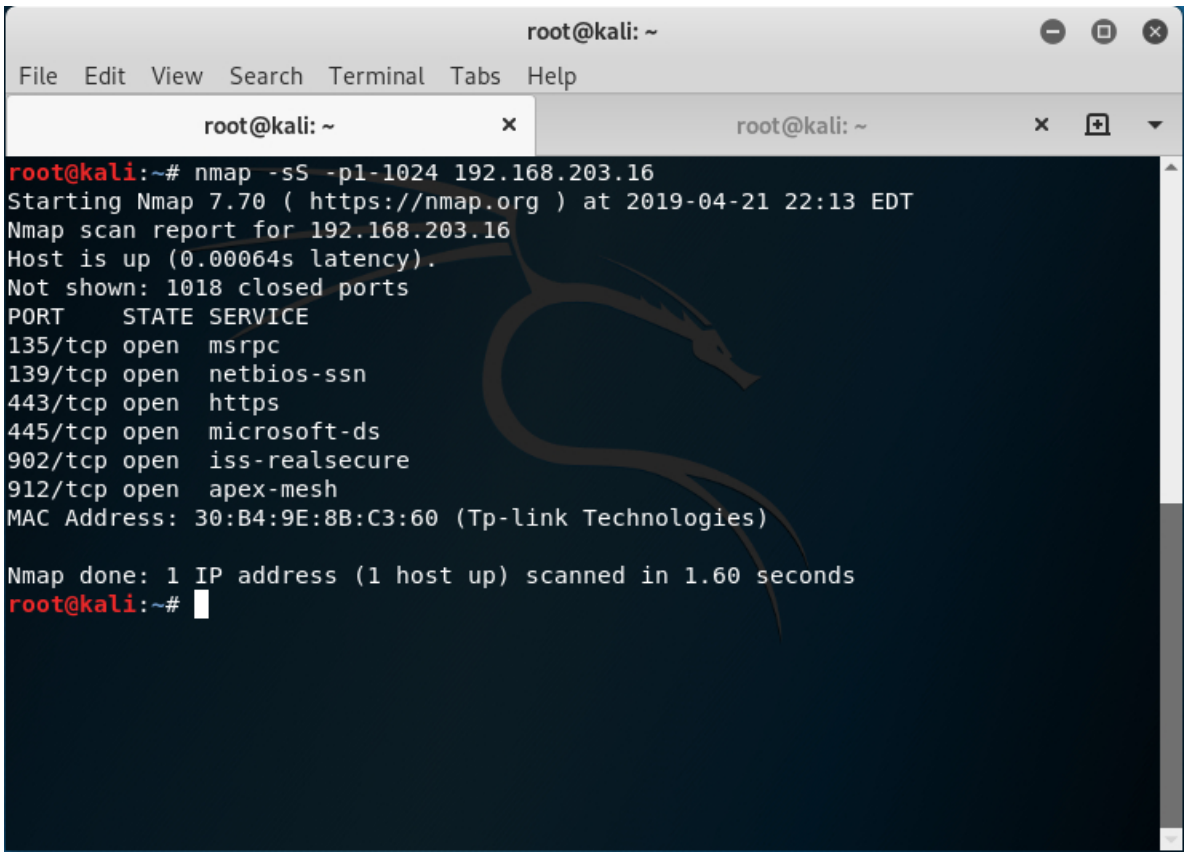
```
Nmap是安全渗透领域最强大的开源端口扫描器，能跨平台支持运行。
https://nmap.org/
http://sectools.org/
```

扫描示例

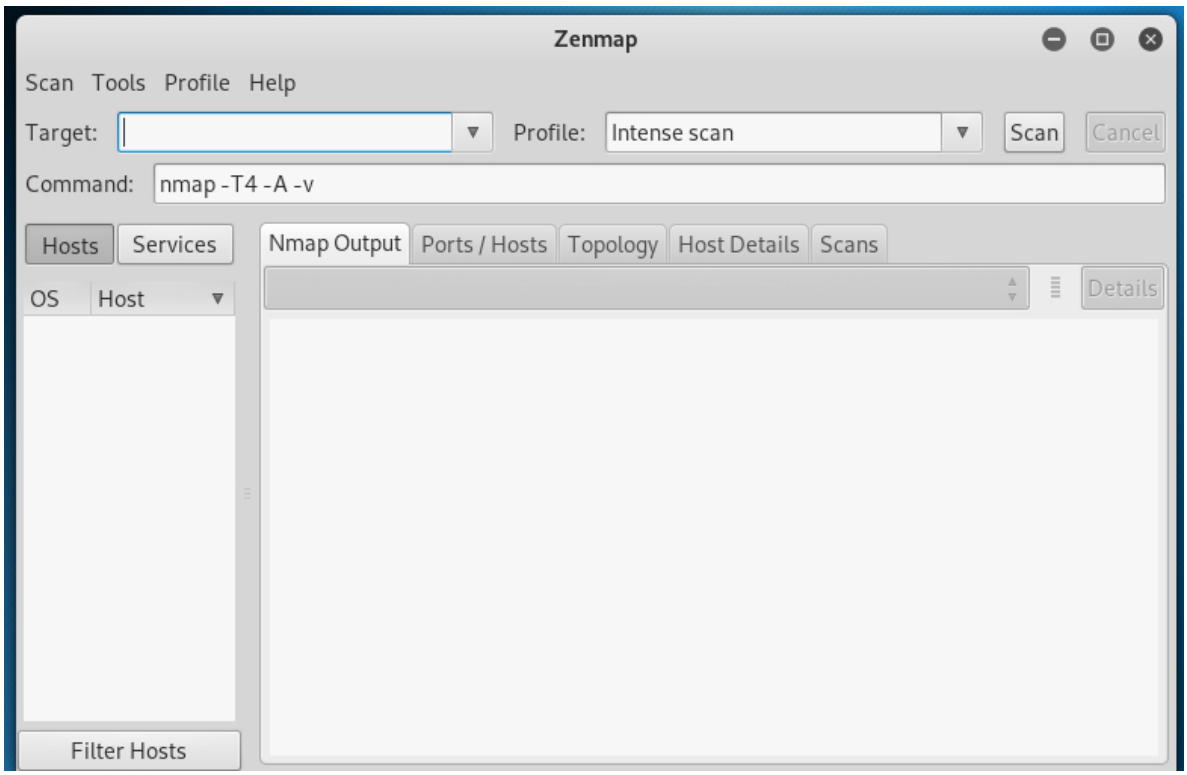
```
主机发现：  nmap -sn 192.168.203.16
端口扫描：  nmap -sS -p1-1024 192.168.203.16
系统扫描：  nmap -O 192.168.203.34
版本扫描：  nmap -sV 192.168.203.34
综合扫描：  nmap -A 192.168.203.34

脚本扫描：
            root@kali:/usr/share/nmap/scripts#
            nmap --script=default 192.168.203.34
            nmap --script=auth 192.168.203.34
            nmap --script=brute 192.168.203.34
```

```
nmap参考指南
https://nmap.org/man/zh/
```



zenmap



Intense scan

```
nmap -T4 -A -v 192.168.203.34
-T 设置速度等级，1到5级，数字越大，速度越快
-A 综合扫描
-v 输出扫描过程
```

Intense scan plus UDP

```
nmap -sS -sU -T4 -A -v 192.168.203.34
-sS TCP全连接扫描
-sU UDP扫描
```

Intense scan, all TCP ports

```
nmap -p 1-65535 -T4 -A -v 192.168.203.34
-p 指定端口范围
```

Intense scan, no ping

```
nmap -T4 -A -v -Pn 192.168.203.34
-Pn 不做ping扫描，例如针对防火墙等安全产品
```

Ping scan

```
nmap -sn 192.168.203.34
-sn 只做ping扫描，不做端口扫描
```

Quick scan

```
nmap -T4 -F 192.168.203.34
-F fast模式，只扫描常见的服务端口，比如默认端口(1000个)还少
```

Quick scan plus

```
nmap -sV -T4 -O -F --version-light 192.168.203.34
-sV 扫描系统和服务版本
-O 扫描操作系统版本
```

Quick traceroute

```
nmap -sn --traceroute www.baidu.com
```

Regular scan

```
nmap 192.168.203.34
```

Slow comprehensive scan

```
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script
"default or (discovery and safe)" 192.168.203.34
```

OpenVAS

OpenVAS(Open Vulnerability Assesment System),即开放式漏洞评估系统，是一个用于评估目标漏洞的杰出框架，开源且功能强大；

它与著名的Nessus“本是同根生”，在Nessus商业化之后仍然坚持开源，号称“当前最好用的开源漏洞扫描工具”。最新版的Kali Linux不再自带OpenVAS了，需要自己部署OpenVAS漏洞检测系统。其核心部件是一个服务器，包括一套网络漏洞测试程序，可以检测远程系统和应用程序中的安全问题。

但是它的最常用用途是检测目标网络或主机的安全性。它的评估能力来源于数万个漏洞测试程序，这些程序是以插件的形式存在。openvas是基于C/S（客户端/服务器），B/S（浏览器/服务器）架构进行工作，用户通过浏览器或者专用客户端程序来下达扫描任务，服务器端负责授权，执行扫描操作并提供扫描结果。
http://www.openvas.org
http://www.greenbone.net

部署OpenVAS

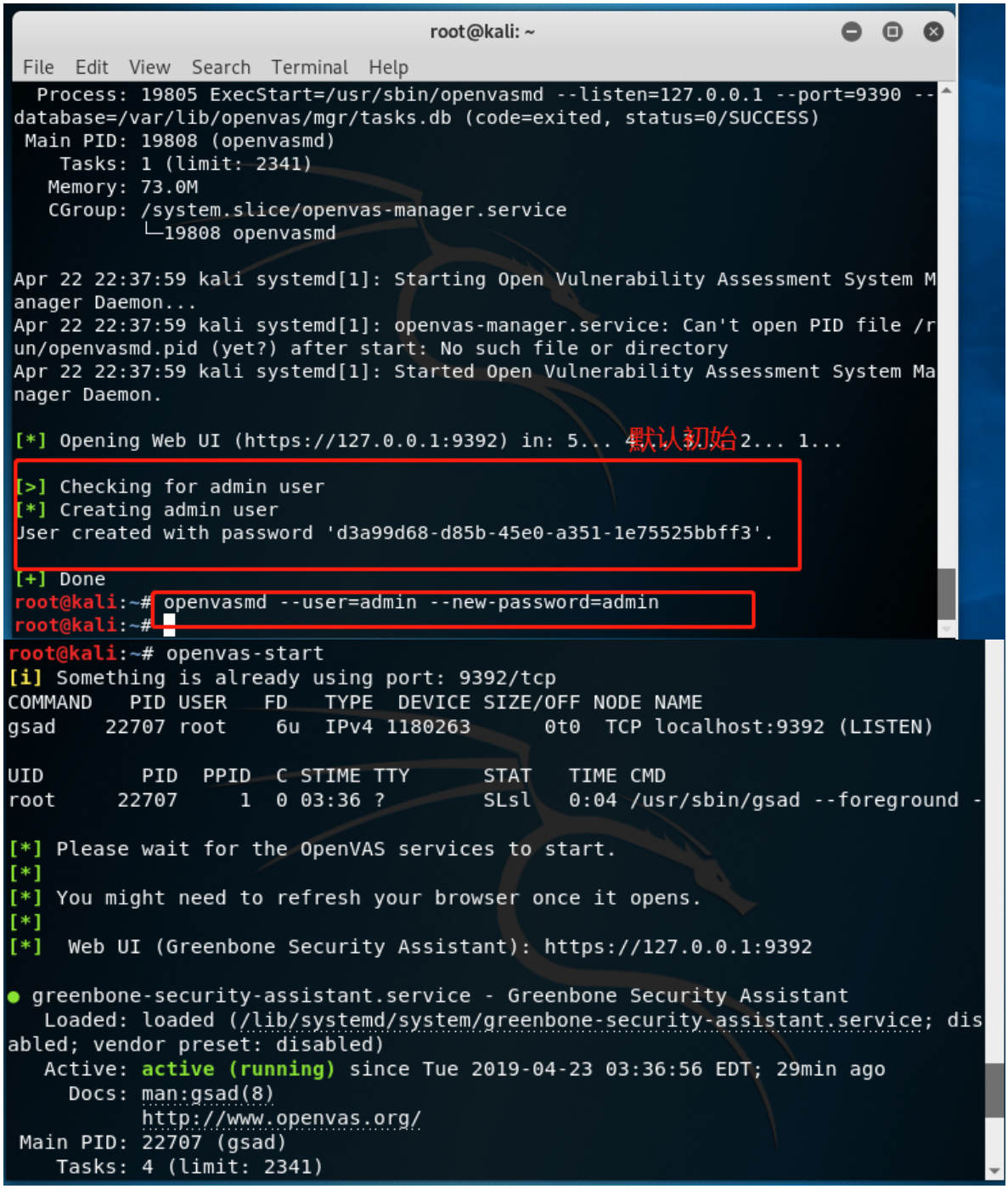
```
升级kali linux
root@kali:~# apt-get update
root@kali:~# apt-get dist-upgrade

安装OpenVAS
root@kali:~# apt-get install openvas
root@kali:~# openvas-setup

修改admin账户密码
root@kali:~# openvasmd --user=admin --new-password=admin

修改默认监听IP
root@kali:~# vim
```

```
root@kali:~# openvas-start
```

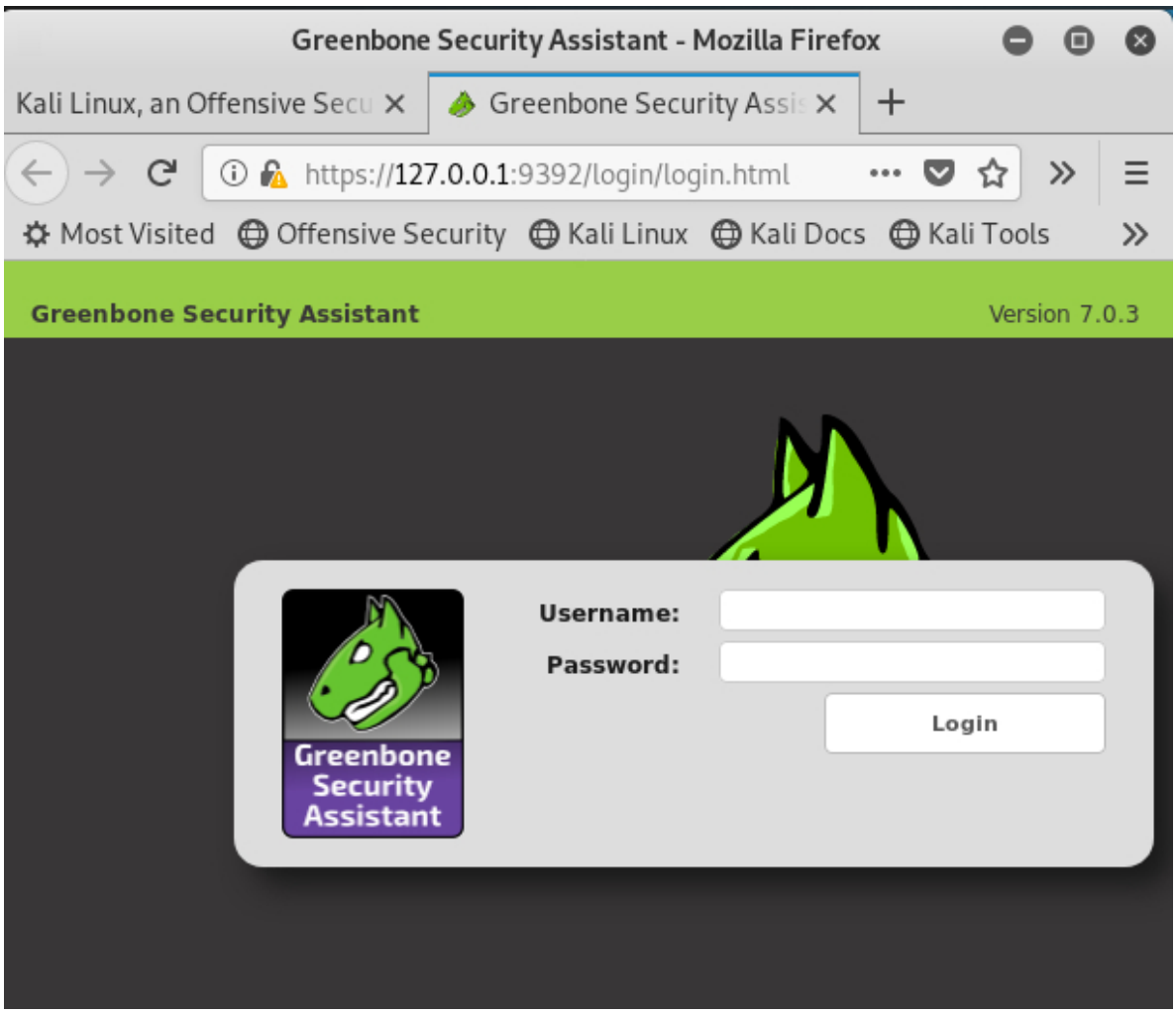


检查安装：

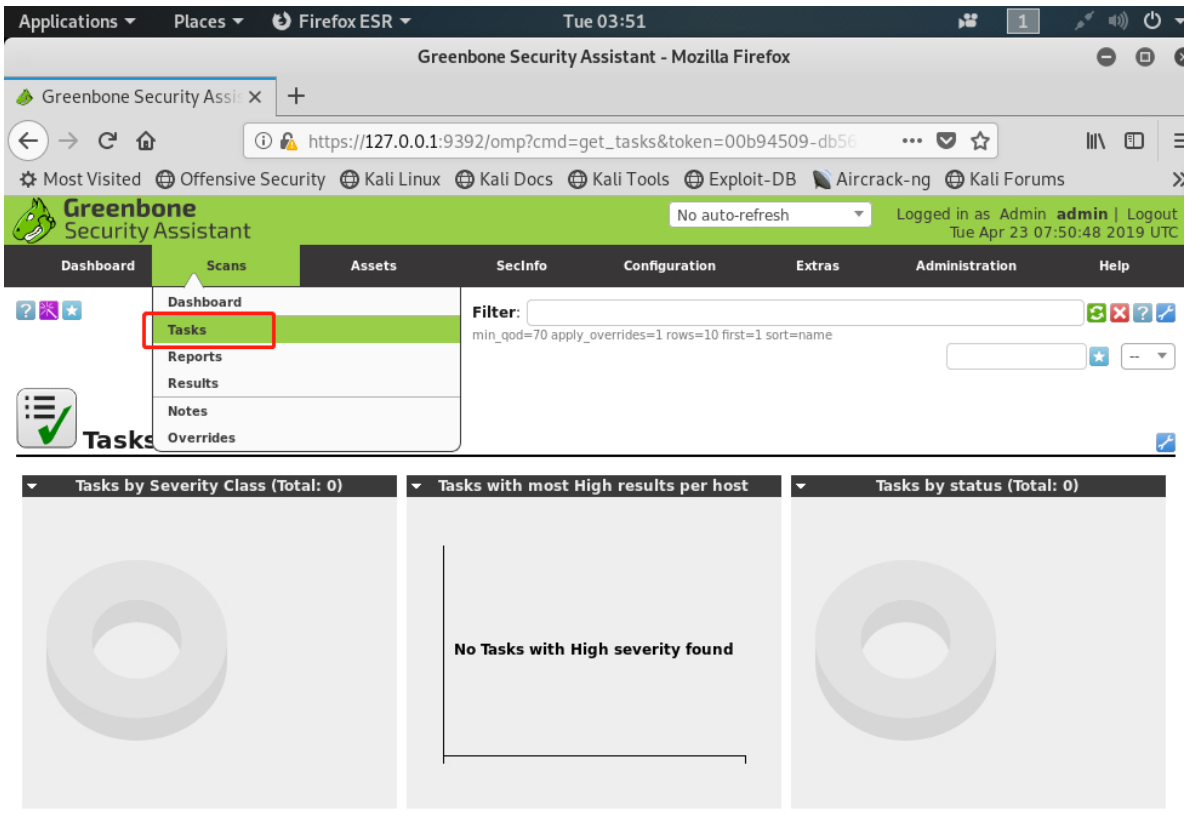
```
root@kali:~# ss -tnlp
root@kali:~# openvas-check-setup
```

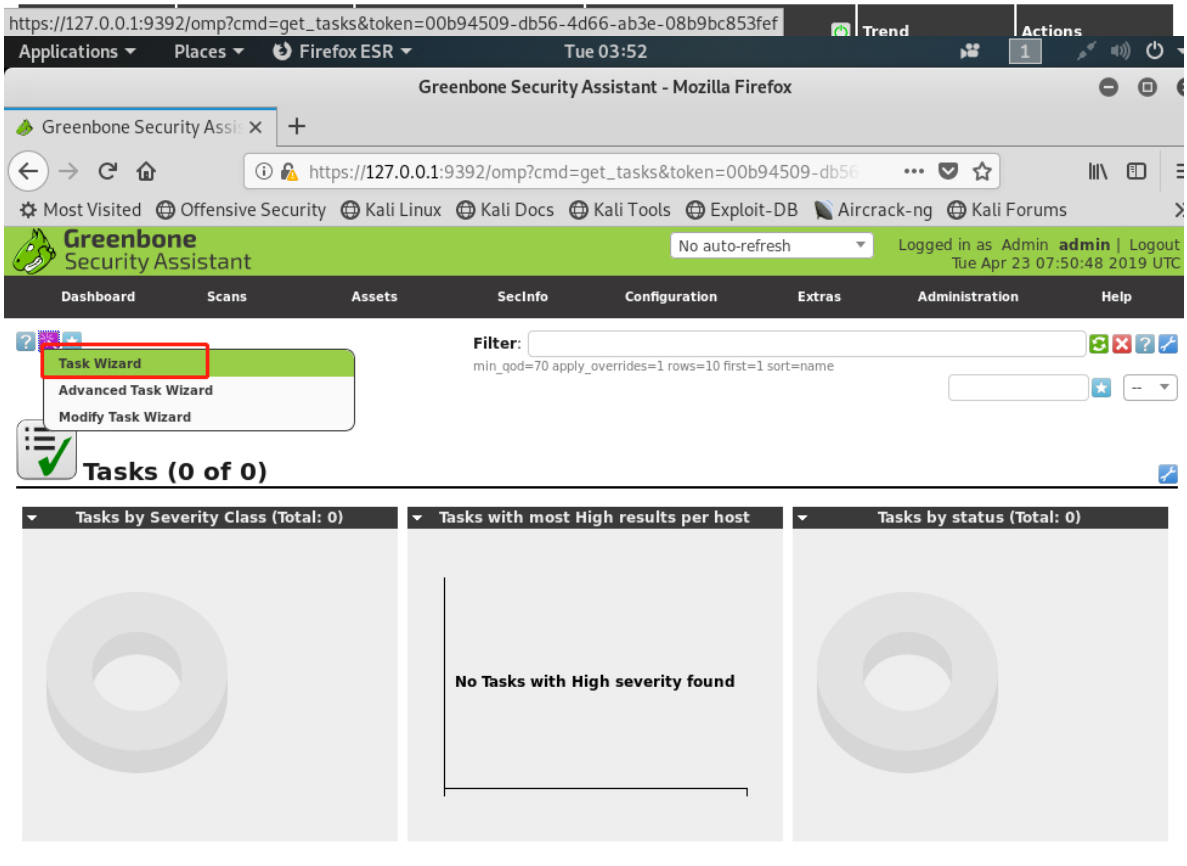
登录OpenVAS

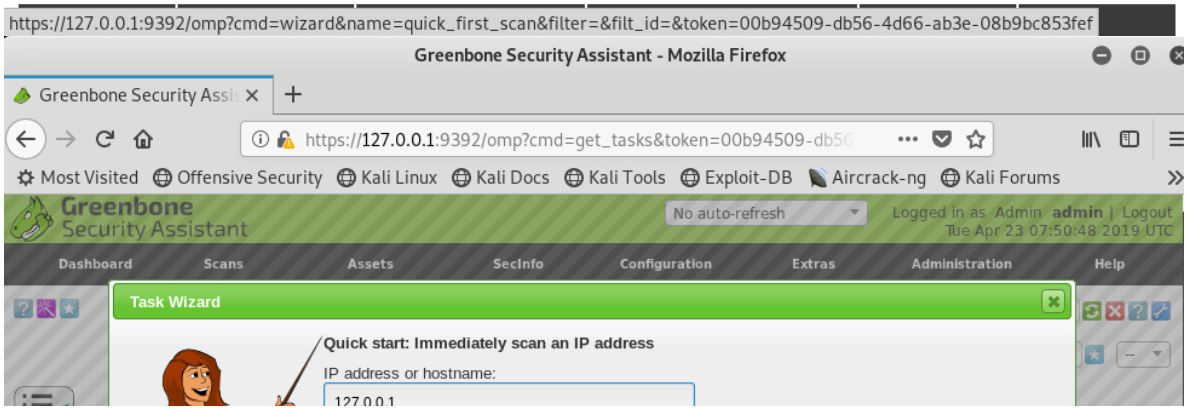
```
https://127.0.0.1:9392 #ip为kali的IP
注：https
```

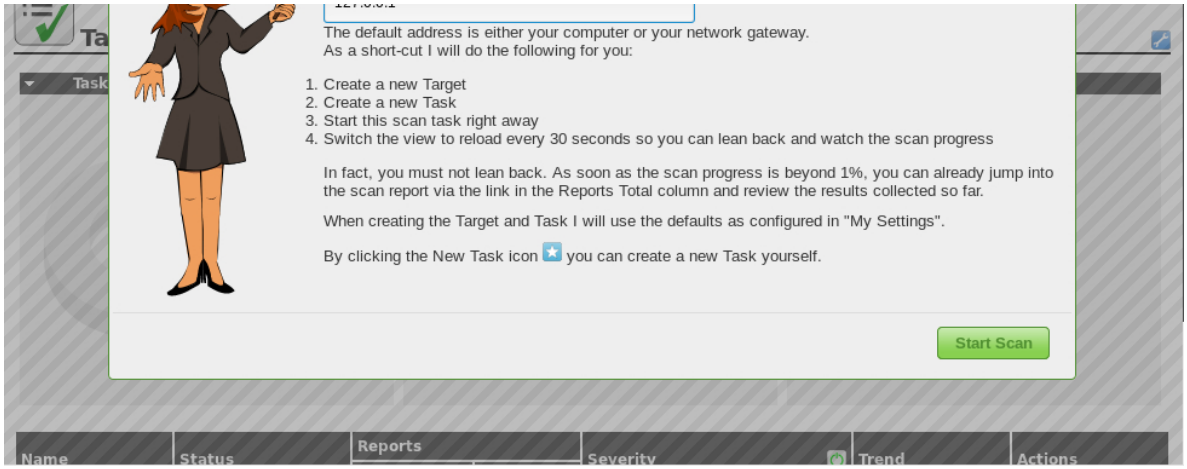

Greenbone Security Assistant - Mozilla Firefox
Kali Linux, an Offensive Secu
Greenbone Security Assis
https://127.0.0.1:9392/login/login.html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Greenbone Security Assistant
Version 7.0.3
Username:
Password:
Login
Greenbone Security Assistant

新建扫描task

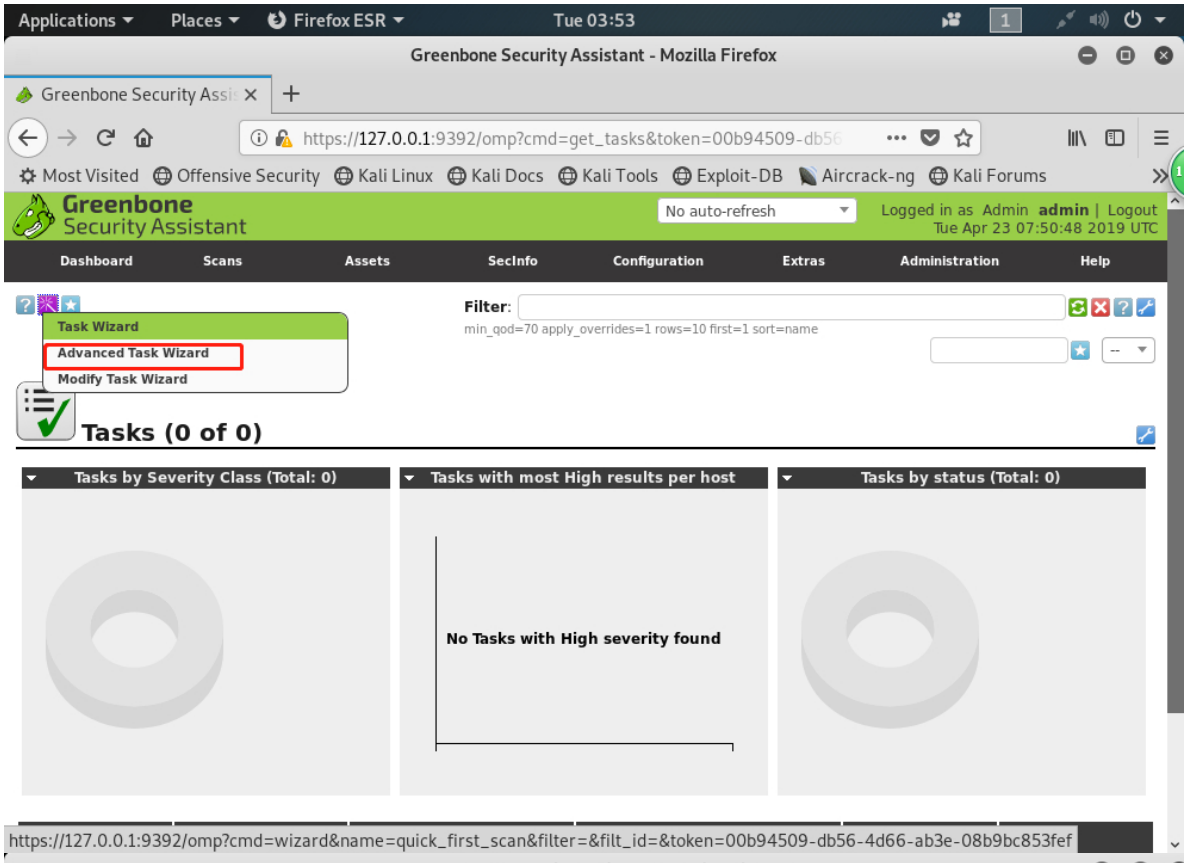

Applications
Places
Firefox ESR
Tue 03:51
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Apr 23 07:50:48 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Tasks
Reports
Results
Notes
Overrides
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks
Tasks by Severity Class (Total: 0)
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 0)


https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56-4d66-ab3e-08b9bc853fef
Trend
Actions
Applications
Places
Firefox ESR
Tue 03:52
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Apr 23 07:50:48 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Task Wizard
Advanced Task Wizard
Modify Task Wizard
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks (0 of 0)
Tasks by Severity Class (Total: 0)
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 0)


https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=00b94509-db56-4d66-ab3e-08b9bc853fef
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Apr 23 07:50:48 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Task Wizard
Quick start: Immediately scan an IP address
IP address or hostname:
127.0.0.1


The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.
When creating the Target and Task I will use the defaults as configured in "My Settings".
By clicking the New Task icon you can create a new Task yourself.
Start Scan
Name
Status
Reports
Severity
Trend
Actions

高级扫描task



https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=00b94509-db56-4d66-ab3e-08b9bc853fef