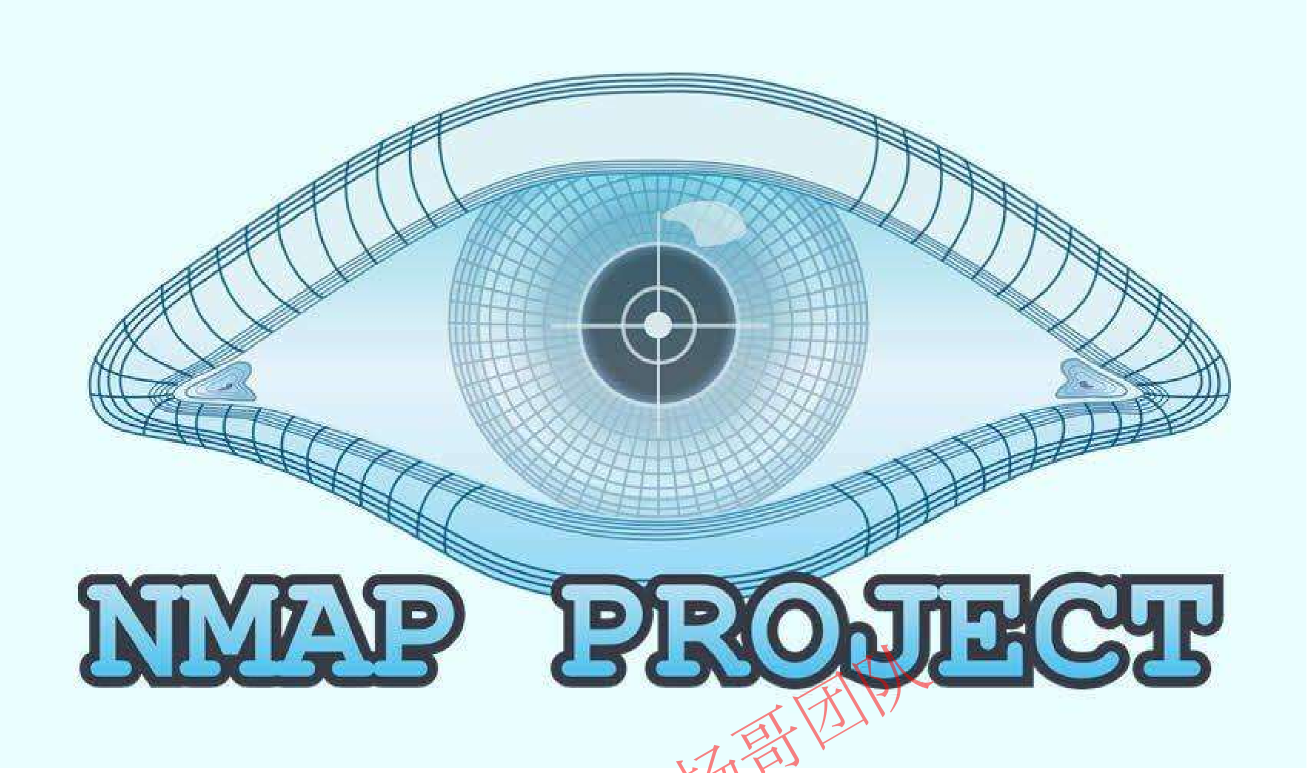
Web信息收集之目标扫描



1. 项目实验环境

```
目标靶机：OWASP_Broken_Web_Apps_VM_1.2
测试渗透机：win7/Kali
```

2. nmap

2.1 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/
```

2.1 扫描示例

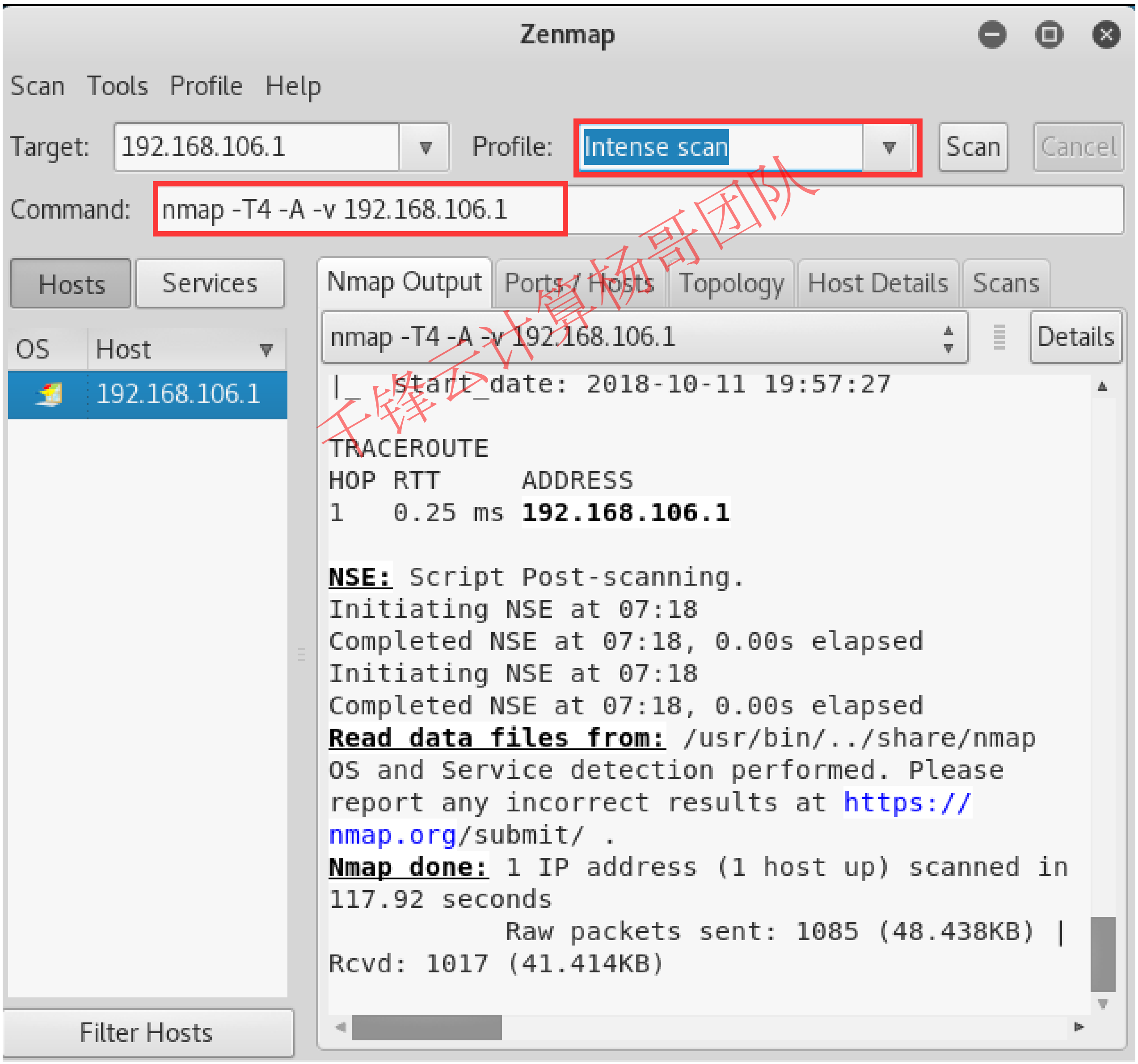
```
主机发现    nmap -sn 192.168.106/24
端口扫描    nmap -sS -p1-1000 192.168.106.134
系统扫描    nmap -O 192.168.106.134
版本扫描    nmap -sV 192.168.106.134
综合扫描    nmap -A 192.168.106.134

脚本扫描    root@kali:/usr/share/nmap/scripts#
           nmap --script=default 192.168.106.134
           nmap --script=auth 192.168.106.214
           nmap --script=brute 192.168.106.134
```

```
            nmap --script=vuln 192.168.106.134
            nmap --script=broadcast 192.168.106.134
            nmap  --script=smb-brute.nse 192.168.106.134
            map  --script=smb-check-vulns.nse --script-args=unsafe=1 192.168.106.134
            map  --script=smb-vuln-conficker.nse --script-args=unsafe=1 192.168.106.134
            nmap -p3306 --script=mysql-empty-password.nse 192.168.106.134
```

3. zenmap

3.1 Intense scan

```
nmap -T4 -A -v 192.168.106.1
-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
```



Target: 192.168.106.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.106.1

Host: 192.168.106.1

```
nmap -T4 -A -v 192.168.106.1
|_ start_date: 2018-10-11 19:57:27

TRACEROUTE
HOP RTT     ADDRESS
1   0.25 ms 192.168.106.1

NSE: Script Post-scanning.
Initiating NSE at 07:18
Completed NSE at 07:18, 0.00s elapsed
Initiating NSE at 07:18
Completed NSE at 07:18, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please
report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in
117.92 seconds
           Raw packets sent: 1085 (48.438KB) |
Rcvd: 1017 (41.414KB)
```

3.2 Intense scan plus UDP

```
nmap -sS -sU -T4 -A -v 192.168.106.134
-sS TCP全连接扫描
-sU UDP扫描
```

3.3 Intense scan, all TCP ports

```
nmap -p 1-65535 -T4 -A -v 192.168.106.134
-p 指定端口范围，默认扫描1000个端口
```

3.4 intense scan no ping

```
nmap -T4 -A -v -Pn 192.168.106.0/24
-Pn 不做ping扫描，例如针对防火墙等安全产品
```

3.5 ping scan

```
nmap -sn 192.168.106.0/24
nmap -sn -T4 -v 192.168.106.0/24
-sn 只做ping扫描，不做端口扫描
```

3.6 quick scan

```
nmap -T4 -F 192.168.106.134
-F fast模式，只扫描常见服务端口，比默认端口（1000个）还少
```

3.7 Quick scan plus

```
nmap -sV -T4 -O -F --version-light 192.168.106.134
-sV 扫描系统和服务版本
-O  扫描操作系统版本
```

3.8 Quick traceroute

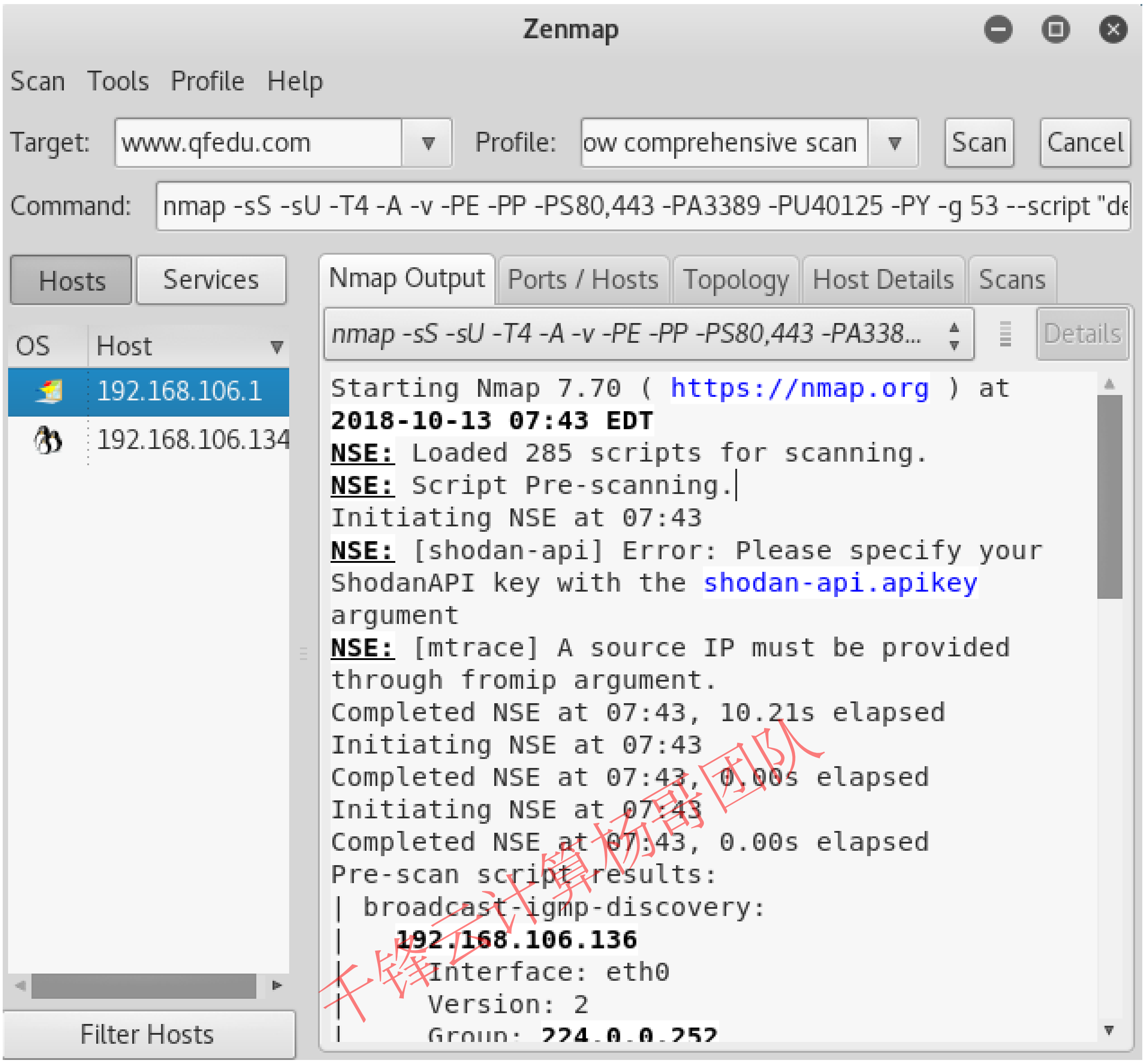
```
nmap -sn --traceroute www.qfedu.com
```

3.9 Regular scan

```
nmap www.qfedu.com
```

3.10 Slow comprehensive scan

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



Target: www.qfedu.com

Profile: ow comprehensive scan

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "de

```
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA338...
```

192.168.106.1
192.168.106.134

```
Starting Nmap 7.70 ( https://nmap.org ) at
2018-10-13 07:43 EDT
NSE: Loaded 285 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:43
NSE: [shodan-api] Error: Please specify your
ShodanAPI key with the shodan-api.apikey
argument
NSE: [mtrace] A source IP must be provided
through fromip argument.
Completed NSE at 07:43, 10.21s elapsed
Initiating NSE at 07:43
Completed NSE at 07:43, 0.00s elapsed
Initiating NSE at 07:43
Completed NSE at 07:43, 0.00s elapsed
Pre-scan script results:
| broadcast-igmp-discovery:
|   192.168.106.136
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.252
```

4. OpenVAS

Username: admin

Password: ●●●●●●●

Login

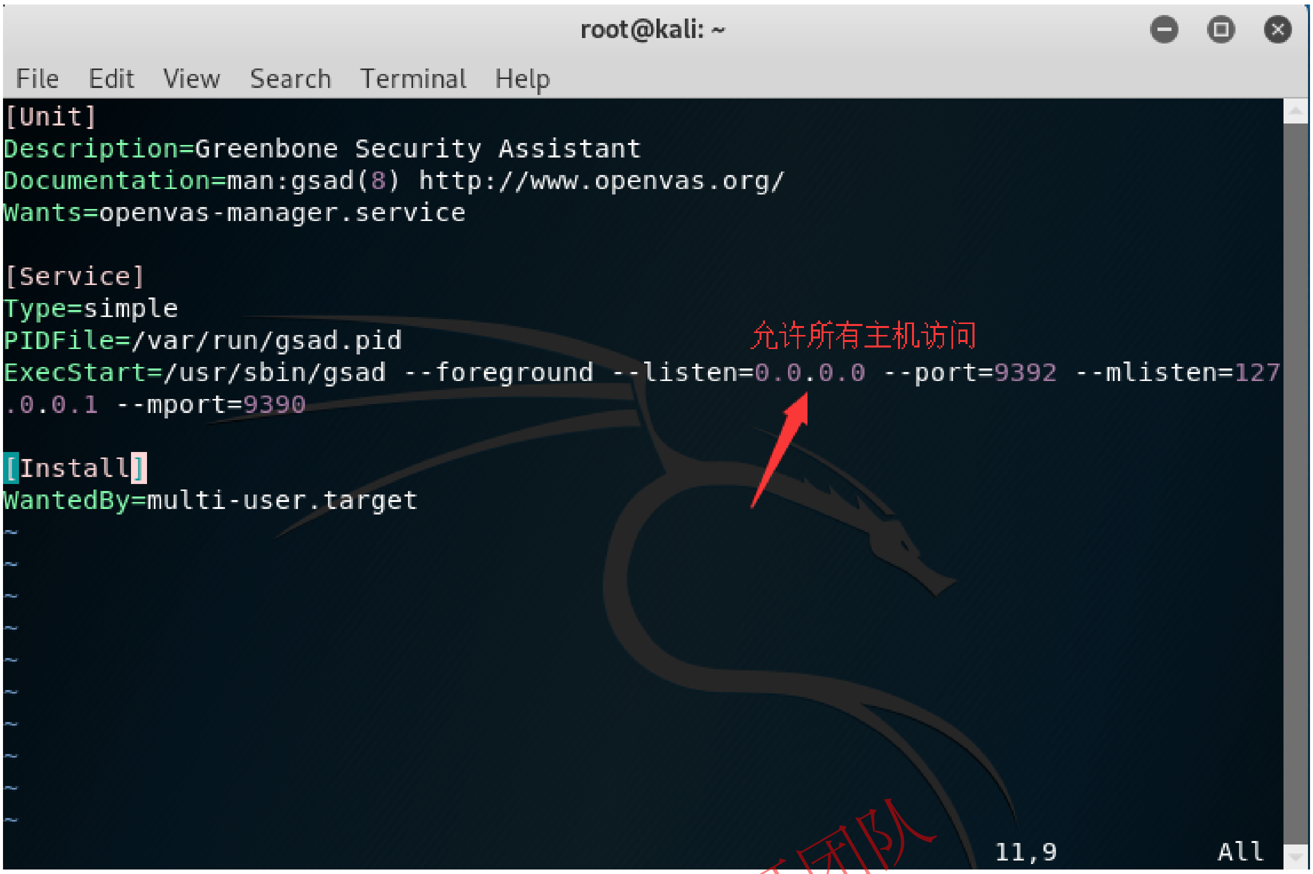
OpenVAS（Open Vulnerability Assessment System)，即开放式漏洞评估系统，是一个用于评估目标漏洞的杰出框架，开源且功能十分强大；

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，这些程序都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/

4.1 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=yangge

修改默认监听IP
root@kali:~# vim /lib/systemd/system/greenbone-security-assistant.service
```

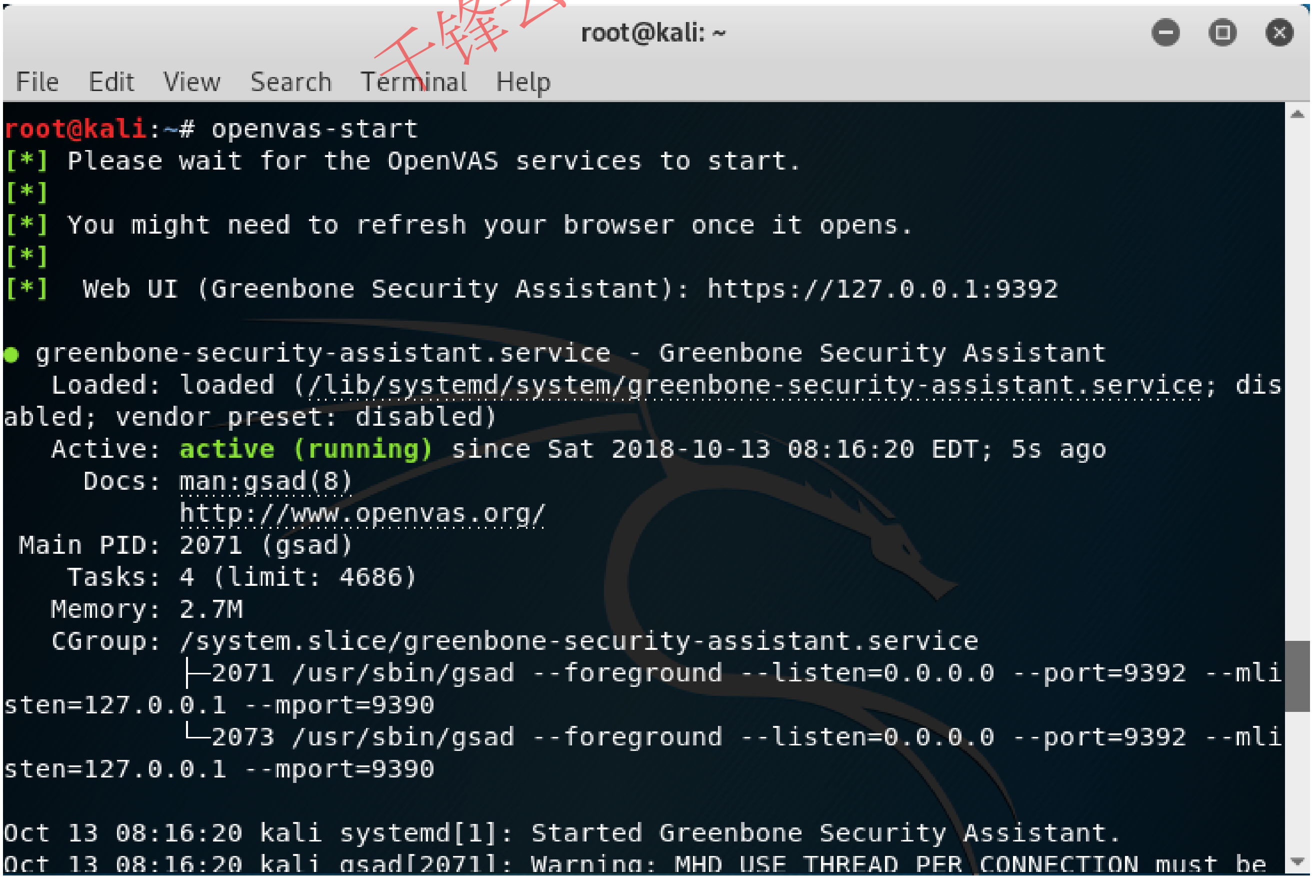


```
[Unit]
Description=Greenbone Security Assistant
Documentation=man:gsad(8) http://www.openvas.org/
Wants=openvas-manager.service

[Service]
Type=simple
PIDFile=/var/run/gsad.pid
ExecStart=/usr/sbin/gsad --foreground --listen=0.0.0.0 --port=9392 --mlisten=127
.0.0.1 --mport=9390

[Install]
WantedBy=multi-user.target
~
~
~
~
~
~
~
~
~
~
                                                               11,9          All
```

允许所有主机访问

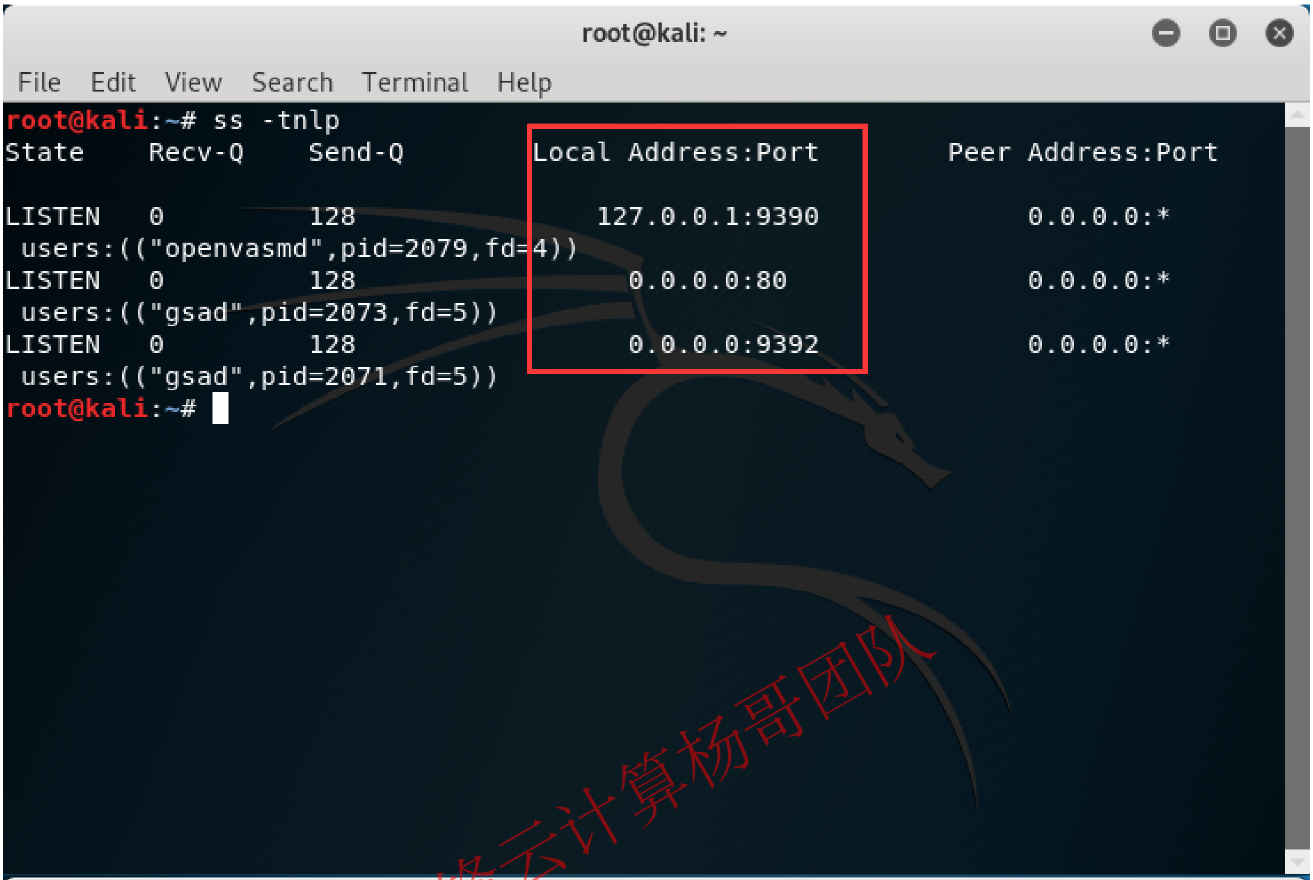
启动OpenVAS

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

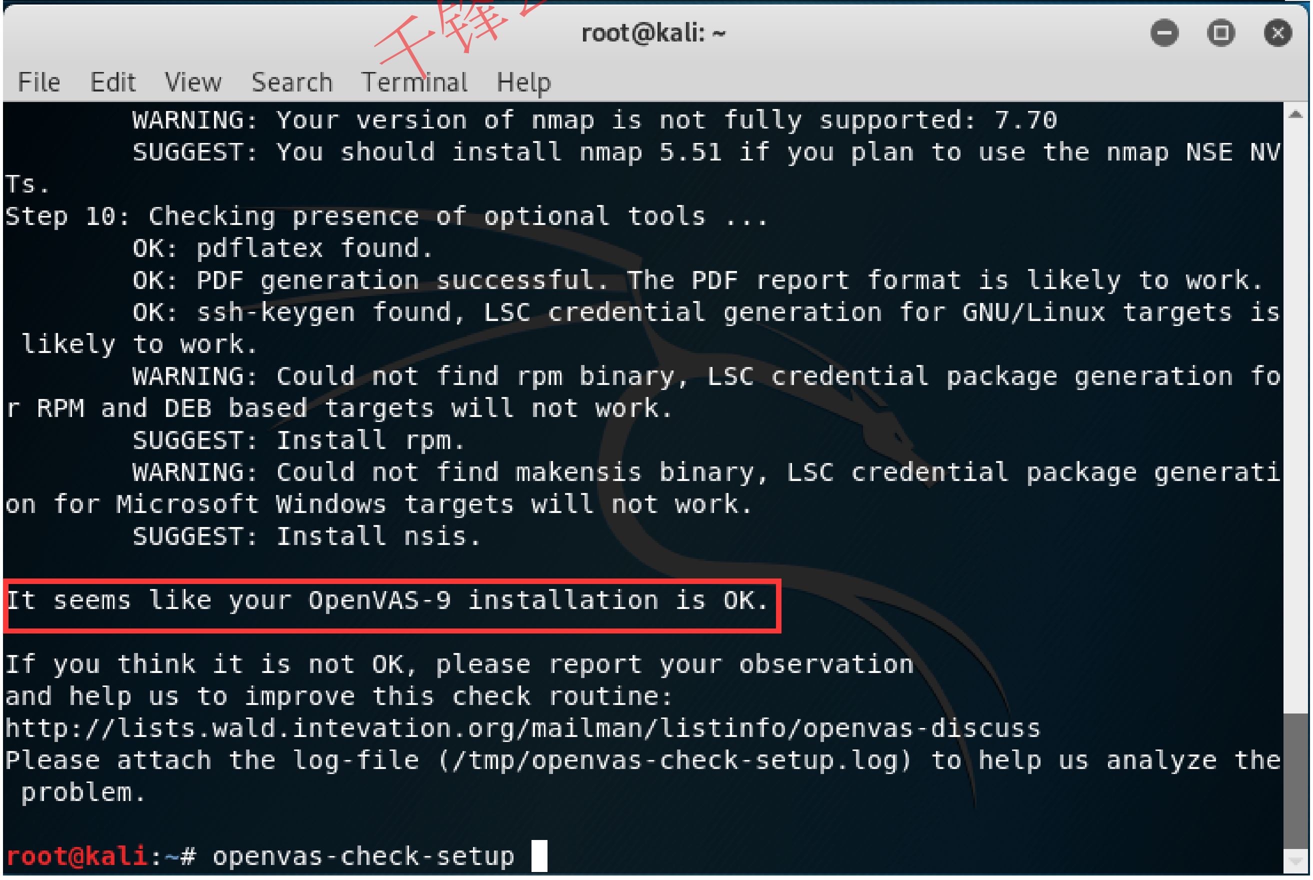


```
root@kali:~# openvas-start
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● greenbone-security-assistant.service - Greenbone Security Assistant
   Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; dis
abled; vendor preset: disabled)
   Active: active (running) since Sat 2018-10-13 08:16:20 EDT; 5s ago
     Docs: man:gsad(8)
           http://www.openvas.org/
 Main PID: 2071 (gsad)
    Tasks: 4 (limit: 4686)
   Memory: 2.7M
   CGroup: /system.slice/greenbone-security-assistant.service
           ├─2071 /usr/sbin/gsad --foreground --listen=0.0.0.0 --port=9392 --mli
sten=127.0.0.1 --mport=9390
           └─2073 /usr/sbin/gsad --foreground --listen=0.0.0.0 --port=9392 --mli
sten=127.0.0.1 --mport=9390

Oct 13 08:16:20 kali systemd[1]: Started Greenbone Security Assistant.
Oct 13 08:16:20 kali gsad[2071]: Warning: MHD USE THREAD PER CONNECTION must be
```

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



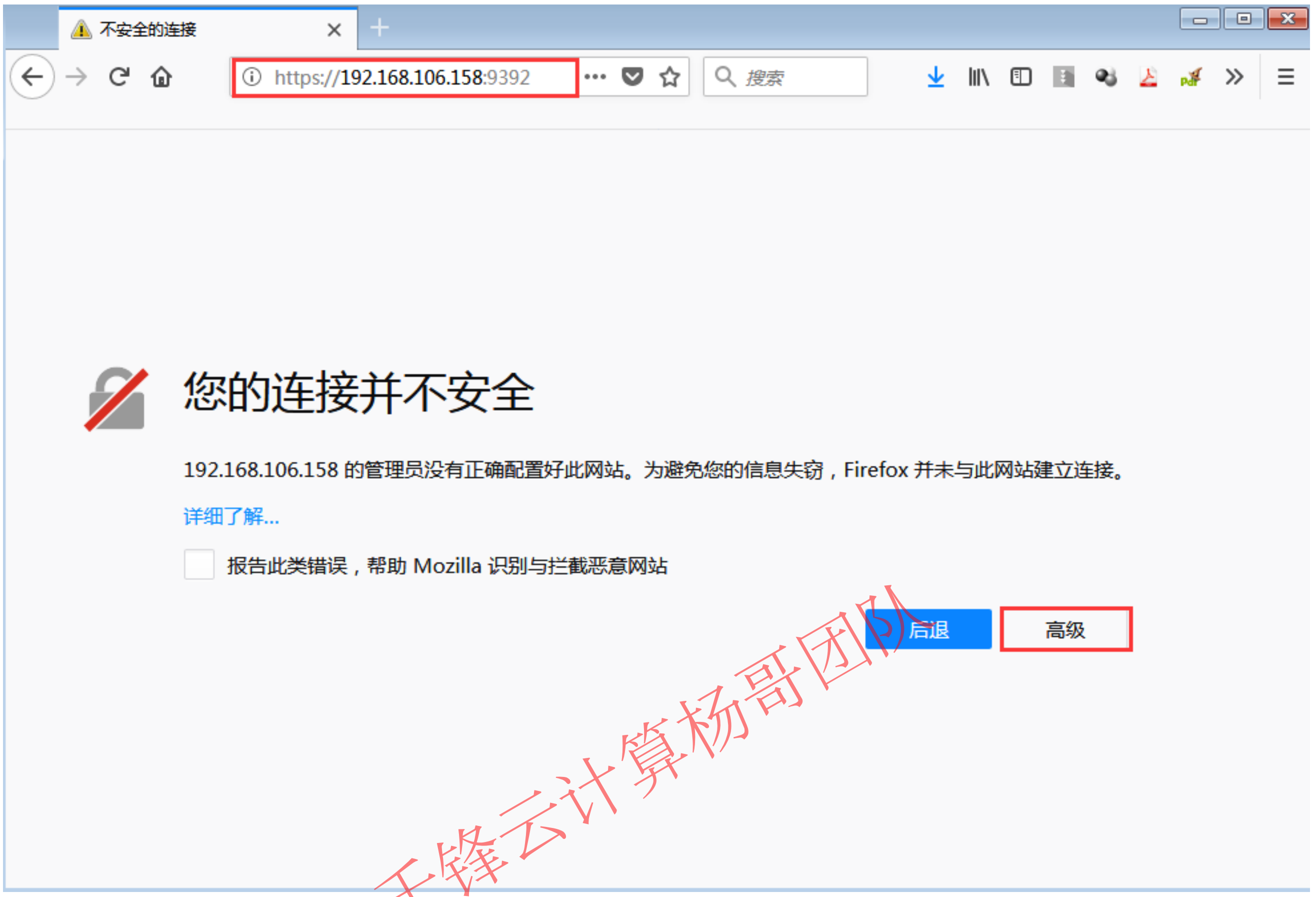
```
root@kali:~# ss -tnlp
State     Recv-Q     Send-Q          Local Address:Port          Peer Address:Port

LISTEN    0          128                 127.0.0.1:9390               0.0.0.0:*
 users:(("openvasmd",pid=2079,fd=4))
LISTEN    0          128                   0.0.0.0:80                 0.0.0.0:*
 users:(("gsad",pid=2073,fd=5))
LISTEN    0          128                   0.0.0.0:9392               0.0.0.0:*
 users:(("gsad",pid=2071,fd=5))
root@kali:~# 
```



```
        WARNING: Your version of nmap is not fully supported: 7.70
        SUGGEST: You should install nmap 5.51 if you plan to use the nmap NSE NV
Ts.
Step 10: Checking presence of optional tools ...
        OK: pdflatex found.
        OK: PDF generation successful. The PDF report format is likely to work.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is
 likely to work.
        WARNING: Could not find rpm binary, LSC credential package generation fo
r RPM and DEB based targets will not work.
        SUGGEST: Install rpm.
        WARNING: Could not find makensis binary, LSC credential package generati
on for Microsoft Windows targets will not work.
        SUGGEST: Install nsis.

It seems like your OpenVAS-9 installation is OK.

If you think it is not OK, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the
 problem.

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

4.2 登录OpenVAS

```
https://192.168.106.158:9392        #192.168.106.158为Kali IP
注：是https
```

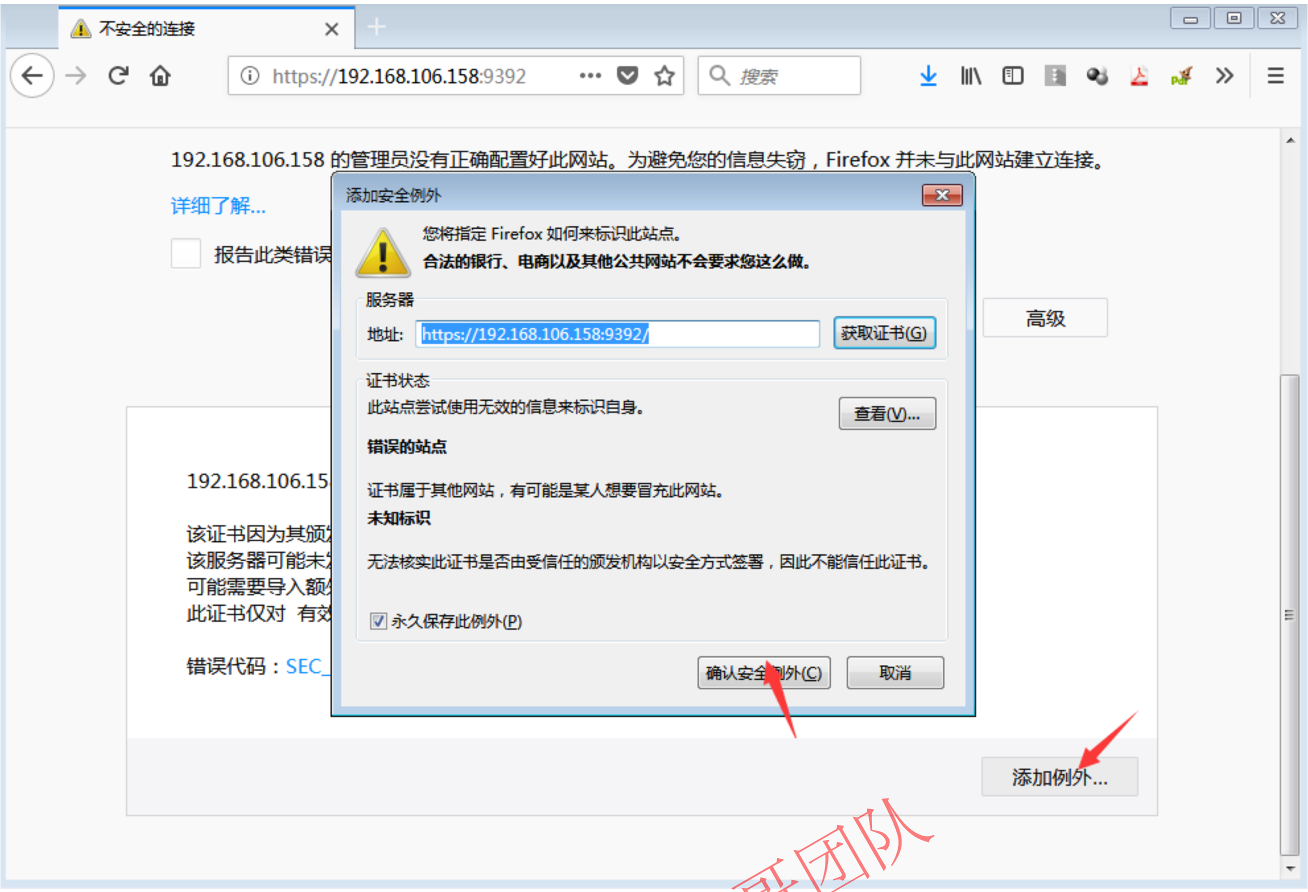


您的连接并不安全

192.168.106.158 的管理员没有正确配置好此网站。为避免您的信息失窃，Firefox 并未与此网站建立连接。

详细了解...

□ 报告此类错误，帮助 Mozilla 识别与拦截恶意网站



192.168.106.158 的管理员没有正确配置好此网站。为避免您的信息失窃，Firefox 并未与此网站建立连接。

添加安全例外

您将指定 Firefox 如何来标识此站点。
合法的银行、电商以及其他公共网站不会要求您这么做。

服务器

地址: https://192.168.106.158:9392/ 获取证书(G)

证书状态

此站点尝试使用无效的信息来标识自身。 查看(V)...

错误的站点

证书属于其他网站，有可能是某人想要冒充此网站。

未知标识

无法核实此证书是否由受信任的颁发机构以安全方式签署，因此不能信任此证书。

☑ 永久保存此例外(P)

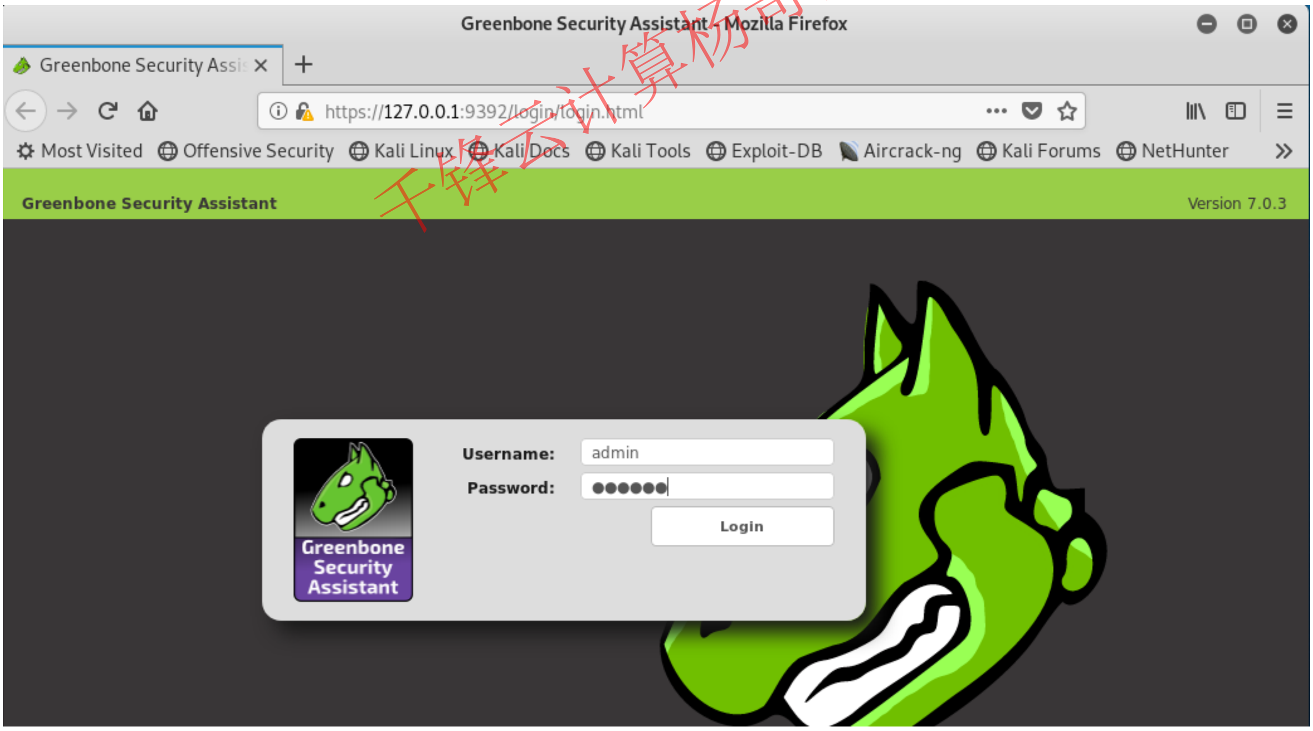
确认安全例外(C) 取消

192.168.106.15

该证书因为其颁
该服务器可能未
可能需要导入额
此证书仅对 有效

错误代码：SEC_

添加例外...

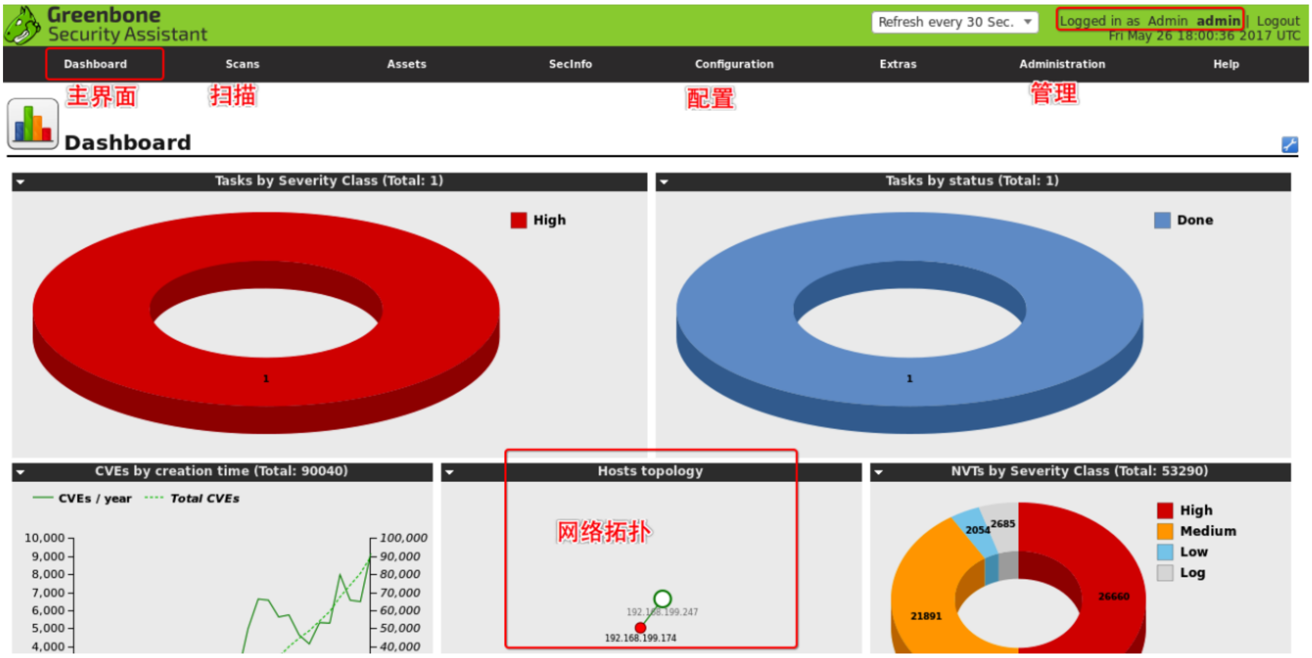


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/login/login.html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
Version 7.0.3
Greenbone Security Assistant

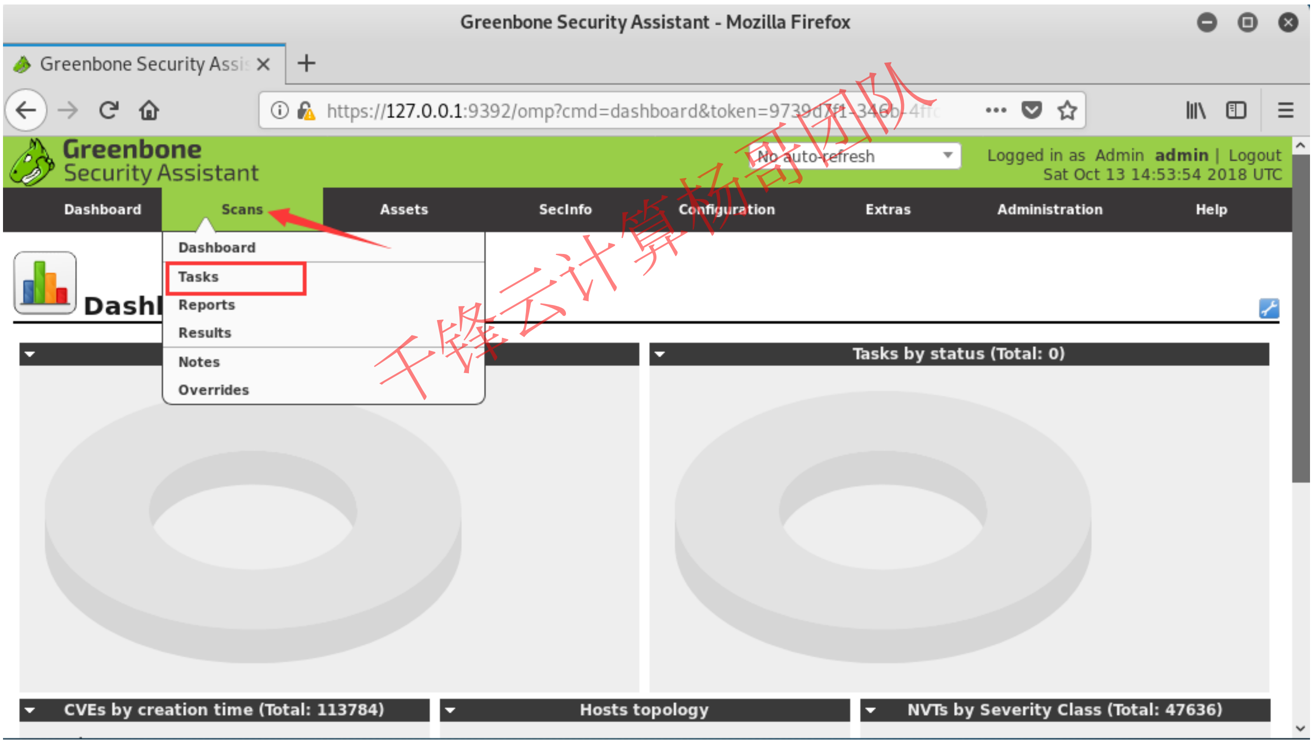
Username: admin

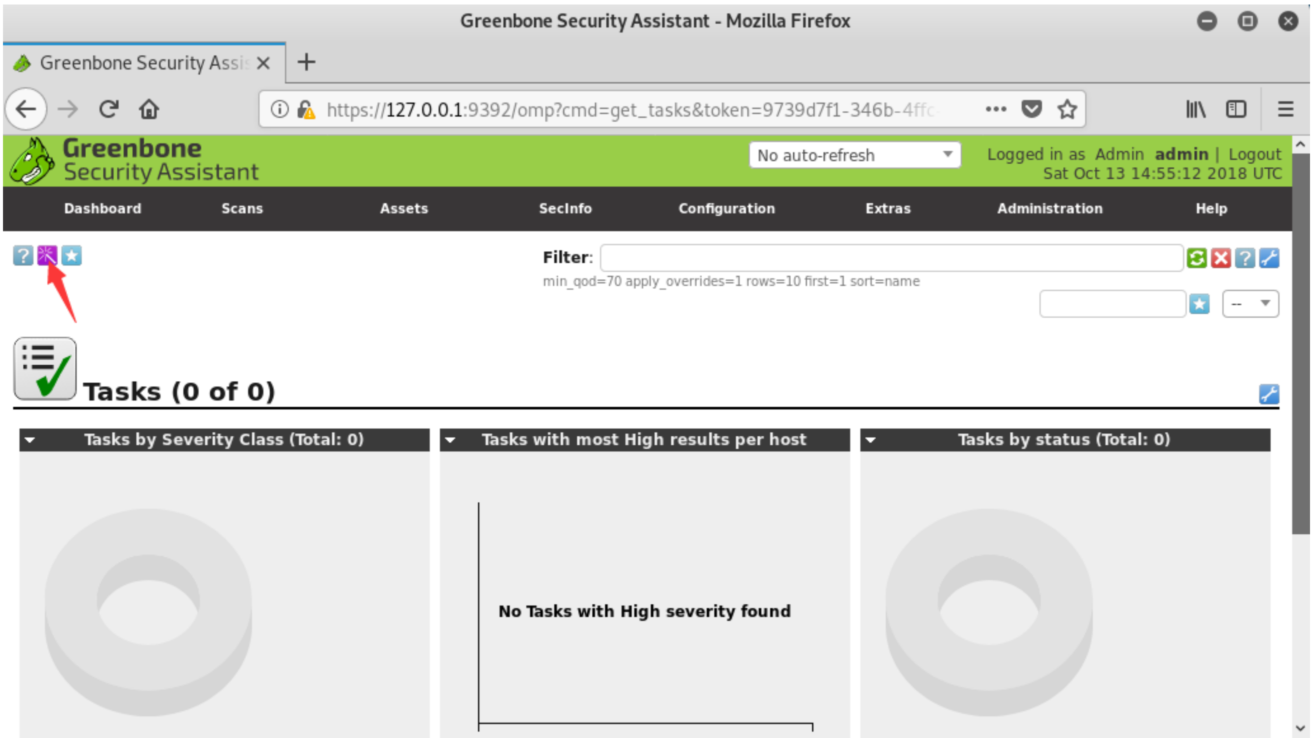
Password: ●●●●●●

Login


Greenbone Security Assistant
Refresh every 30 Sec.
Logged in as Admin admin | Logout
Fri May 26 18:00:36 2017 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
主界面
扫描
配置
管理
Dashboard
Tasks by Severity Class (Total: 1)
High
1
Tasks by status (Total: 1)
Done
1
CVEs by creation time (Total: 90040)
CVEs / year
Total CVEs
10,000
9,000
8,000
7,000
6,000
5,000
4,000
100,000
90,000
80,000
70,000
60,000
50,000
40,000
Hosts topology
网络拓扑
192.168.199.247
192.168.199.174
NVTs by Severity Class (Total: 53290)
2054
2685
26660
21891
High
Medium
Low
Log

4.3 新建扫描task

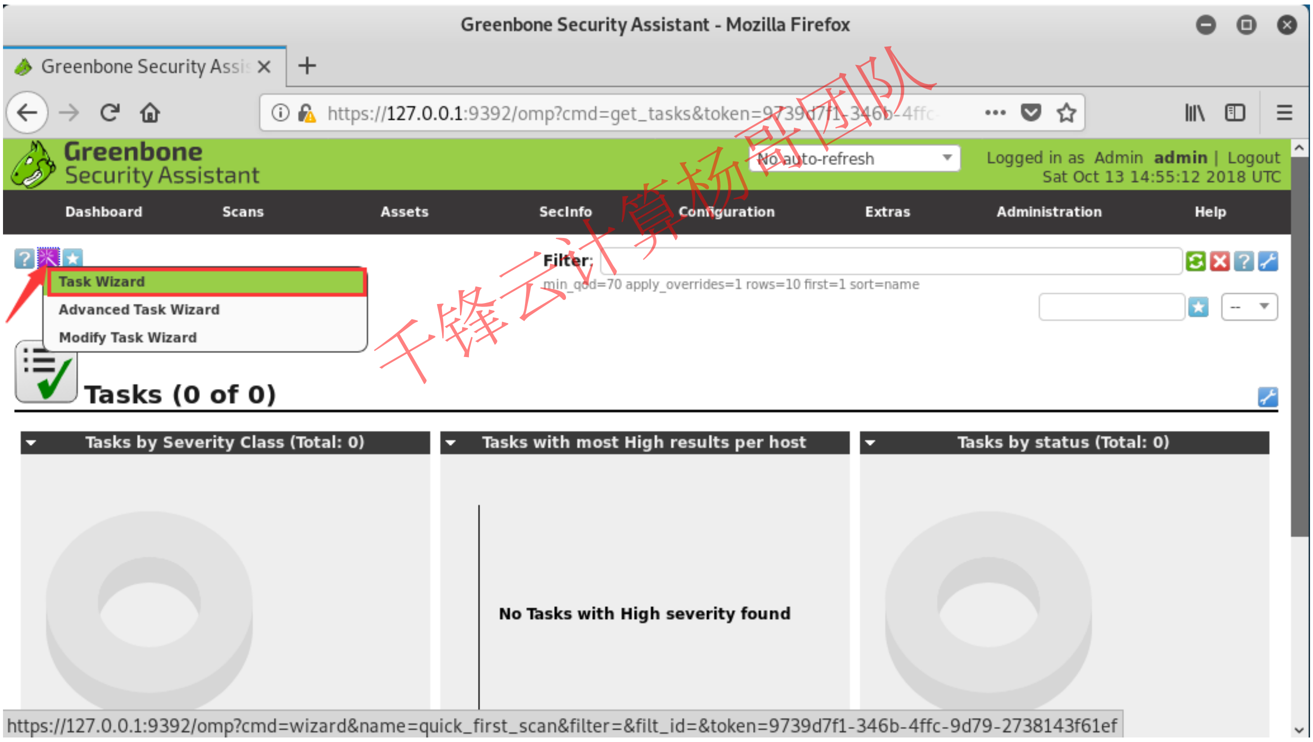

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=dashboard&token=9739d7f1-346b-4ffc
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sat Oct 13 14:53:54 2018 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Tasks
Reports
Results
Notes
Overrides
Dashb
Tasks by status (Total: 0)
CVEs by creation time (Total: 113784)
Hosts topology
NVTs by Severity Class (Total: 47636)


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sat Oct 13 14:55:12 2018 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Tasks (0 of 0)
Tasks by Severity Class (Total: 0)
Tasks with most High results per host
Tasks by status (Total: 0)
--

https://127.0.0.1:9392/omp?cmd=get_tasks&token=9739d7f1-346b-4ffc

Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

No Tasks with High severity found

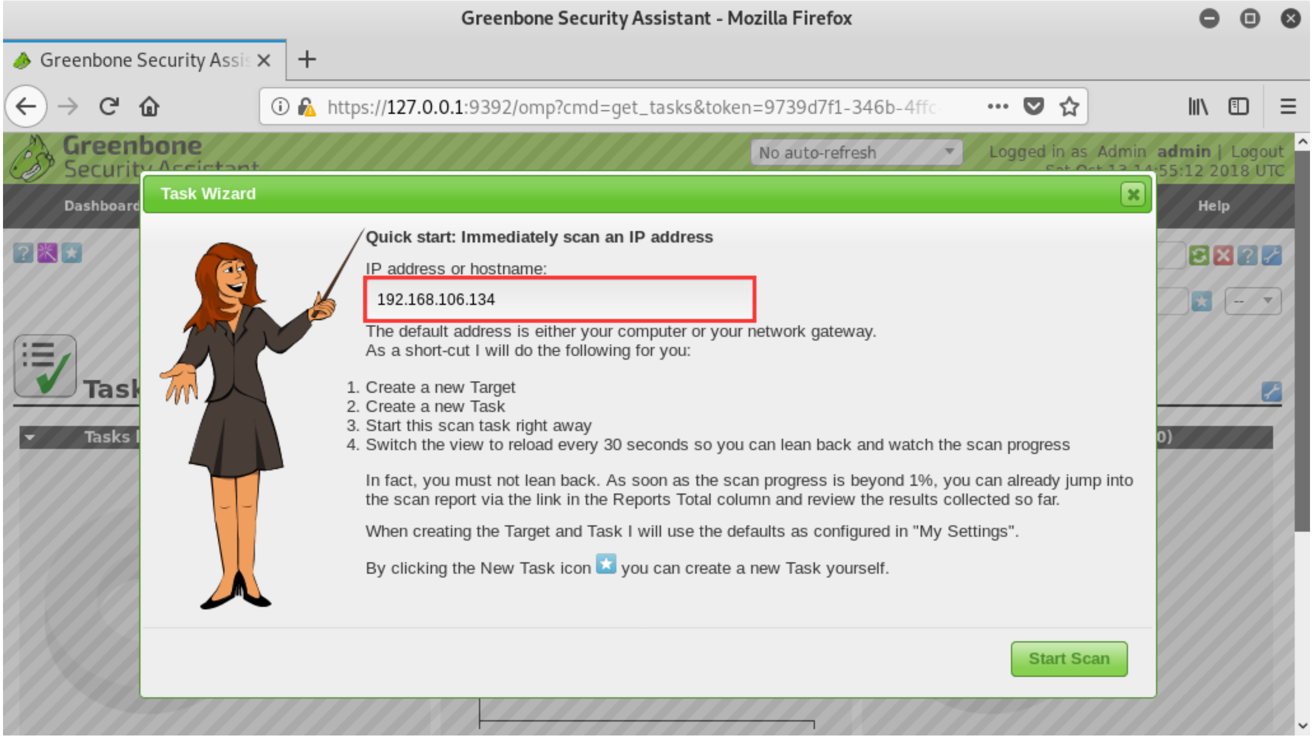

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sat Oct 13 14:55:12 2018 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Task Wizard
Advanced Task Wizard
Modify Task Wizard
Tasks (0 of 0)
Tasks by Severity Class (Total: 0)
Tasks with most High results per host
Tasks by status (Total: 0)
--

https://127.0.0.1:9392/omp?cmd=get_tasks&token=9739d7f1-346b-4ffc

Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

No Tasks with High severity found

https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=9739d7f1-346b-4ffc-9d79-2738143f61ef


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?cmd=get_tasks&token=9739d7f1-346b-4ffc
No auto-refresh
Logged in as Admin admin | Logout
Help
Task Wizard
Start Scan

Quick start: Immediately scan an IP address

IP address or hostname:

192.168.106.134

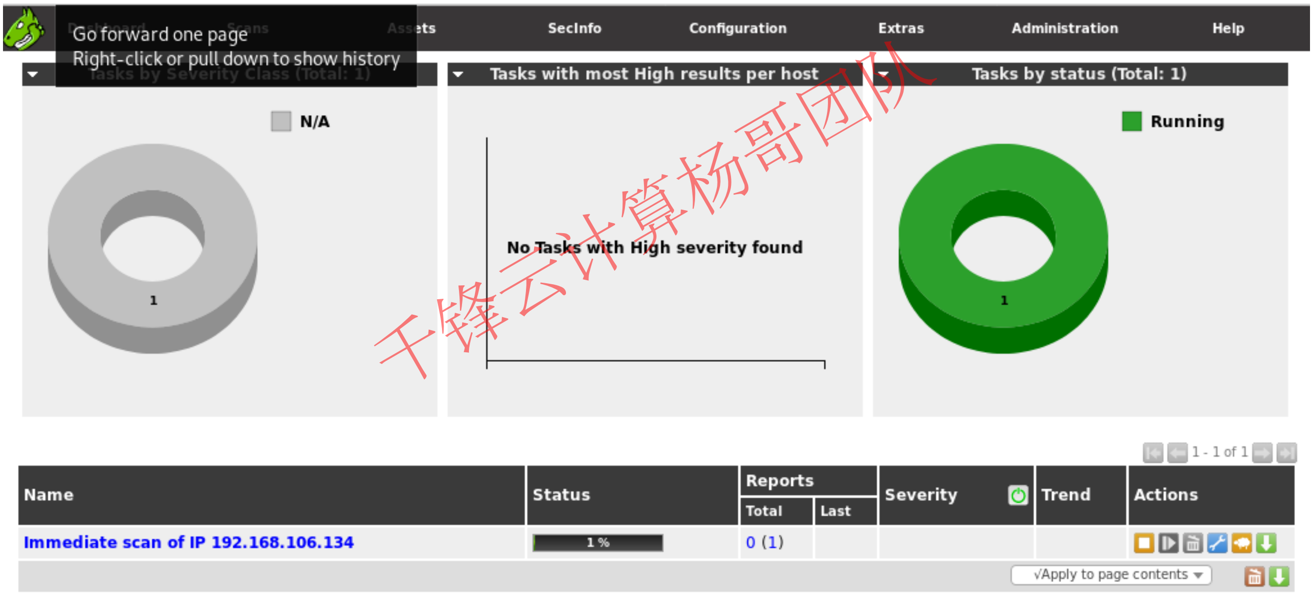
The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

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.

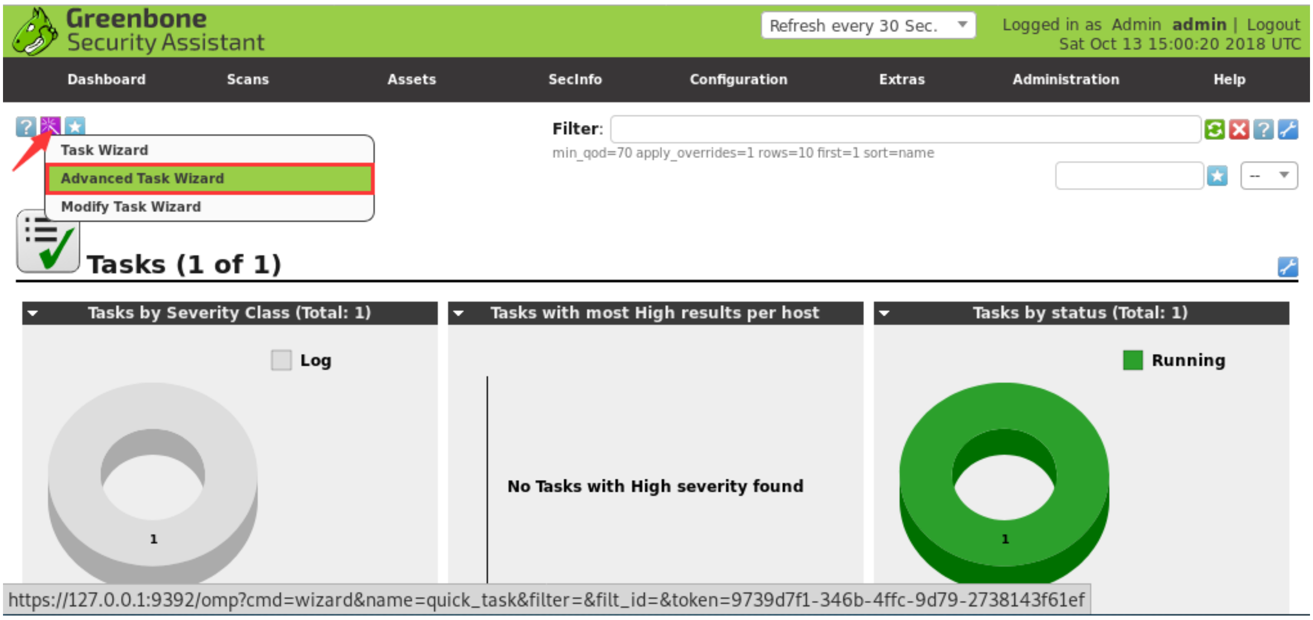
When creating the Target and Task I will use the defaults as configured in "My Settings".

By clicking the New Task icon ☆ you can create a new Task yourself.


Go forward one page
Right-click or pull down to show history
Assets
SecInfo
Configuration
Extras
Administration
Help
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 1)
Running
1
1 - 1 of 1
√Apply to page contents

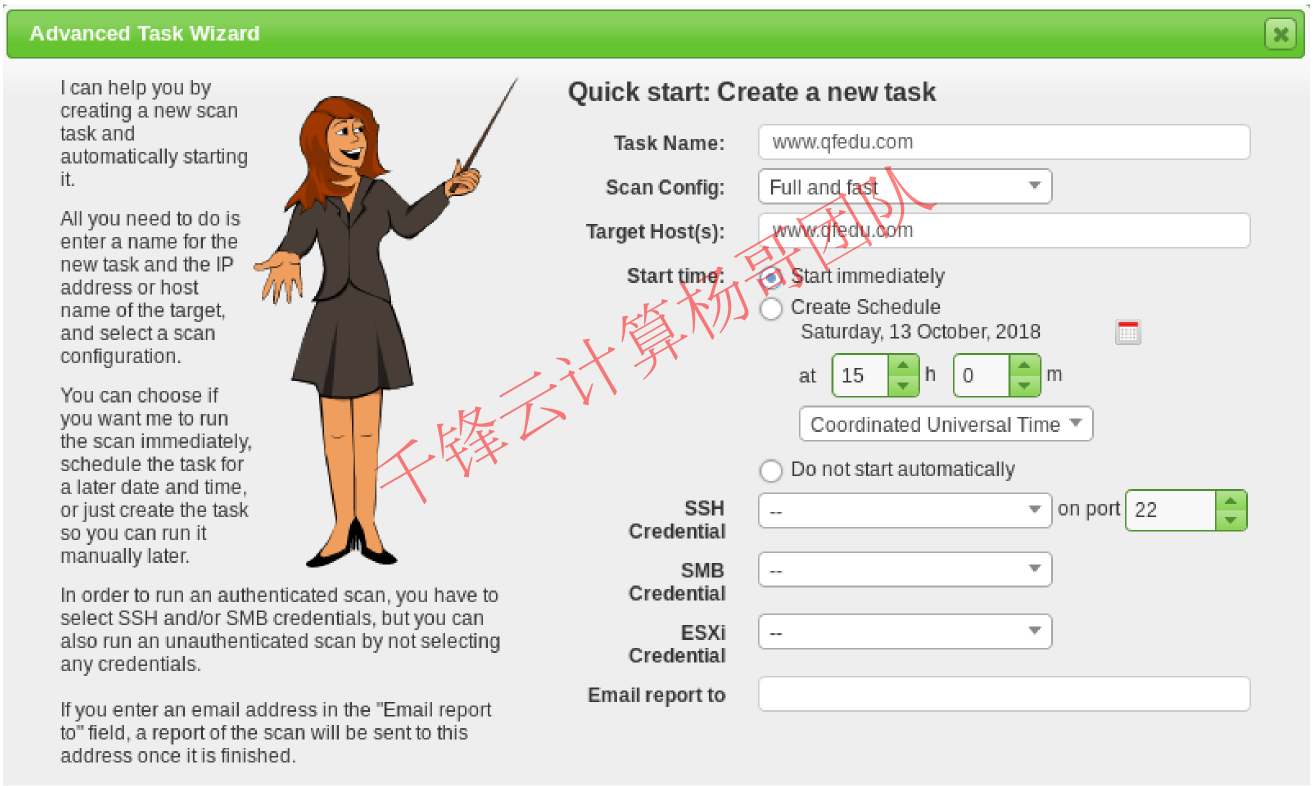
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.106.134	1 %	0 (1)				

4.4 高级扫描task



min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

https://127.0.0.1:9392/omp?cmd=wizard&name=quick_task&filter=&filt_id=&token=9739d7f1-346b-4ffc-9d79-2738143f61ef



I can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose if you want me to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.

Quick start: Create a new task

Task Name: www.qfedu.com

Scan Config: Full and fast

Target Host(s): www.qfedu.com

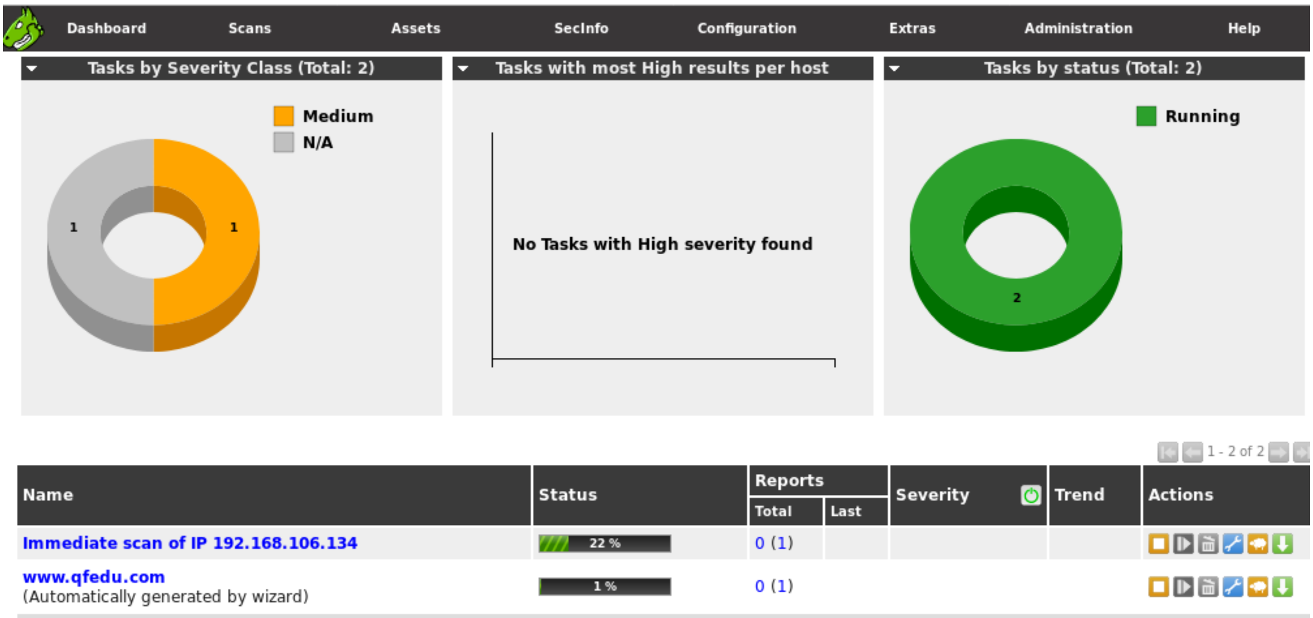
Start time: ● Start immediately
○ Create Schedule
Saturday, 13 October, 2018
at 15 h 0 m
Coordinated Universal Time
○ Do not start automatically

SSH Credential: -- on port 22

SMB Credential: --

ESXi Credential: --

Email report to


Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Tasks by Severity Class (Total: 2)
Medium
N/A
1
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 2)
Running
2
1 - 2 of 2

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.106.134	22 %	0 (1)				
www.qfedu.com (Automatically generated by wizard)	1 %	0 (1)				