

kali linux 2017.2 OpenVAS9.0安装和使用



林鸿风采 关注

2017-11-16 16:42:36 12595人阅读 3人评论

OpenVAS是开放式漏洞评估系统，也可以说它是一个包含着相关工具的网络扫描器。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，可以临时替代nessus使用。

1、安装openvas

Kali linux 2017.2默认未安装openvas，需要手动安装：

安装步骤：

1) 更新

#apt-get update

```
root@kali:~# apt-get update
命中:1 http://mirror.hust.edu.cn/kali kali-rolling InRelease
正在读取软件包列表... 完成
root@kali:~# apt-get upgrade
```

#apt-get dist-upgrade

```
root@kali:~# apt-get upgrade
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
正在计算更新... 完成
```

2) apt-get 安装openvas

#apt-get install openvas* //安装所有的openvas安装包

```
root@kali: ~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
root@kali:~# apt-get install openvas*  
正在读取软件包列表... 完成  
正在分析软件包的依赖关系树  
正在读取状态信息... 完成  
注意, 根据Glob 'openvas*' 选中了 'openvas-cli-dbgsym'  
注意, 根据Glob 'openvas*' 选中了 'openvas-administrator'  
注意, 根据Glob 'openvas*' 选中了 'openvas-plugins'  
注意, 根据Glob 'openvas*' 选中了 'openvas'  
注意, 根据Glob 'openvas*' 选中了 'openvas-scanner-dbgsym'  
注意, 根据Glob 'openvas*' 选中了 'openvas-manager-common'  
注意, 根据Glob 'openvas*' 选中了 'openvas-server'  
注意, 根据Glob 'openvas*' 选中了 'openvas-client'  
注意, 根据Glob 'openvas*' 选中了 'openvas-cli'  
注意, 根据Glob 'openvas*' 选中了 'openvas-manager-dbgsym'  
注意, 根据Glob 'openvas*' 选中了 'openvas-scanner'  
注意, 根据Glob 'openvas*' 选中了 'openvas-manager'  
将会同时安装下列软件:  
doc-base fonts-texgyre gnutls-bin greenbone-security-assistant  
greenbone-security-assistant-common libfile-homedir-perl libfile-which-perl  
libgnutls-dane0 libhiredis0.13 libmicrohttpd12 libopenvas9 libunbound2  
libuuid-perl libyaml-tiny-perl preview-latex-style prosper ps2eps  
redis-server redis-tools tex-gyre texlive-extra-utils texlive-font-utils  
texlive-fonts-recommended texlive-fonts-recommended-doc  
texlive-generic-extra texlive-generic-recommended texlive-latex-extra
```

这是一个漫长的等待。。。。。

安装完成:

```
root@kali: ~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
update-rc.d: It looks like a non-network service, we enable it.  
正在设置 openvas-scanner-dbgsym (5.1.1-0kali2) ...  
正在设置 openvas-manager (7.0.1-0kali2) ...  
update-rc.d: We have no instructions for the openvas-manager init script.  
update-rc.d: It looks like a non-network service, we enable it.  
正在设置 openvas-manager-dbgsym (7.0.1-0kali2) ...  
正在处理用于 tex-common (6.06) 的触发器 ...  
Running updmap-sys. This may take some time... done.  
Running mktexlsr /var/lib/texmf ... done.  
正在设置 texlive-pstricks (2016.20170123-5) ...  
正在设置 texlive-latex-extra (2016.20170123-5) ...  
正在设置 prosper (1.00.4+cvs.2007.05.01-4.1) ...  
正在处理用于 tex-common (6.06) 的触发器 ...  
Running updmap-sys. This may take some time... done.  
Running mktexlsr /var/lib/texmf ... done.  
正在设置 greenbone-security-assistant-common (7.0.2-0kali1) ...  
正在设置 greenbone-security-assistant (7.0.2-0kali1) ...  
update-rc.d: We have no instructions for the greenbone-security-assistant init script.  
update-rc.d: It looks like a non-network service, we enable it.  
正在设置 openvas (9-kali2) ...  
正在处理用于 libc-bin (2.24-10) 的触发器 ...  
正在处理用于 systemd (232-22) 的触发器 ...  
root@kali:~#
```

3) 初始化openvas

#openvas-setup

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
正在处理用于 libc-bin (2.24-10) 的触发器 ...
正在处理用于 systemd (232-22) 的触发器 ...
root@kali:~# openvas-setup
ERROR: Directory for keys (/var/lib/openvas/private/CA) not found!
ERROR: Directory for certificates (/var/lib/openvas/CA) not found!
ERROR: CA key not found in /var/lib/openvas/private/CA/cakey.pem
ERROR: CA certificate not found in /var/lib/openvas/CA/cacert.pem
ERROR: CA certificate failed verification, see /tmp/tmp.oJJAzr2Wa6/openvas-manage-certs.log for details. Aborting.

ERROR: Your OpenVAS certificate infrastructure did NOT pass validation.
See messages above for details.
Generated private key in /tmp/tmp.JRw3ONZDNY/cakey.pem.
Generated self signed certificate in /tmp/tmp.JRw3ONZDNY/cacert.pem.
Installed private key to /var/lib/openvas/private/CA/cakey.pem.
Installed certificate to /var/lib/openvas/CA/cacert.pem.
Generated private key in /tmp/tmp.JRw3ONZDNY/serverkey.pem.
Generated certificate request in /tmp/tmp.JRw3ONZDNY/serverrequest.pem.
Signed certificate request in /tmp/tmp.JRw3ONZDNY/serverrequest.pem with CA certificate in /var/lib/openvas/CA/cacert.pem to generate certificate in /tmp/tmp.JRw3ONZDNY/servercert.pem
Installed private key to /var/lib/openvas/private/CA/serverkey.pem.
Installed certificate to /var/lib/openvas/CA/servercert.pem.
Generated private key in /tmp/tmp.JRw3ONZDNY/clientkey.pem.
```

这是一个漫长的等待。。。。。

初始化完成后，会自动生成默认账号密码，默认账号是：admin，密码如图：

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
dfn-cert-2017.xml.asc
181 100% 1.02kB/s 0:00:00 (xfr#32, to-chk=3/36)
shasums
2,002 100% 10.98kB/s 0:00:00 (xfr#33, to-chk=2/36)
timestamp
13 100% 0.07kB/s 0:00:00 (xfr#34, to-chk=1/36)
timestamp.asc
181 100% 0.99kB/s 0:00:00 (xfr#35, to-chk=0/36)

sent 719 bytes received 35,467,176 bytes 424,765.21 bytes/sec
total size is 35,456,172 speedup is 1.00
/usr/sbin/openvasmd

(openvassd:2545): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory
(openvassd:2545): lib kb_redis-CRITICAL **: redis_new: cannot access redis at '/var/run/redis/redis.sock'
(openvassd:2545): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory
openvassd: no process found
User created with password '5e15b818-280c-4d34-8e31-fe4854c89307'.
root@kali:~#
```

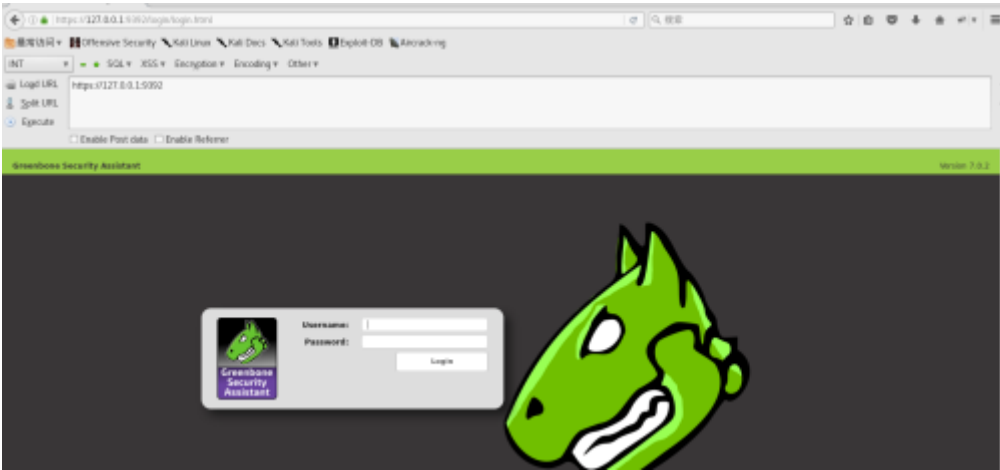
4) 安装完整性检测

#openvas-check-setup

```
root@kali: ~# opnvas-check-setup
User created with password '3e15b818-209c-4d34-b631-fc
root@kali:~# opnvas-check-setup
opnvas-check-setup 2.3.7
Test completeness and readiness of OpenVAS-9
Please report us any non-detected problems and
help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/opn
Send us the log-file (/tmp/opnvas-check-setup.log)
Use the parameter --server to skip checks for client
like GSD and OpenVAS-CLI.
Step 1: Checking OpenVAS Scanner ...
OK: OpenVAS Scanner is present in version 5.1.1
OK: redis-server is present in version v3.2.6
OK: scanner (kb location setting) is configured
socket: /var/run/redis/redis.sock
OK: redis-server is running and listening on sock
OK: redis-server configuration is OK and redis-
OK: NVT collection in /var/lib/openvas/plugins
WARNING: Signature checking of NVTs is not enab
SUGGEST: Enable signature checking (see http://
Step 2: Checking OpenVAS Manager ...
OK: The NVT cache in /var/cache/openvas contain
OK: OpenVAS Manager is present in version 7.0.
OK: OpenVAS Manager database found in /var/lib/
OK: Access rights for the OpenVAS Manager datab
OK: ssl3 found, extended checks of the Open
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/opnvas-check-setup.log) to help us analyze the problem.
root@kali:~#
```

安装完整性检测完成，安装ok。

到此，openvas已经安装完成，在本机中登录：<https://127.0.0.1:9392>，如下图：



5) 设置外部访问

Openvas自7.0起，默认不支持外部访问，为了使用方便，我们需要手动配置外部访问，Openvas9.0修改以下四个配置文件中的监听ip，由127.0.0.1改为0.0.0.0（表示任意IP），保存之后，重新加载systemctl，重启openvas即可。

具体操作如下：

```
#leafpad /lib/systemd/system/greenbone-security-assistant.service
```

本文件下修改两处：--listen和--mlisten



#leafpad /lib/systemd/system/openvas-manager.service



#leafpad /etc/default/openvas-manager //管理器：与接口通信，分配扫描任务，并根据扫描结果生成评估报告，默认端口为9390


```
openvas-manager
文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)
# NOTE: This file is not used if you are using systemd. The options are
# hardcoded in the openvas-manager.service file. If you want to change
# them you should override the service file by creating a file
# /etc/systemd/system/openvas-manager.service.d/local.conf like this:
# [Service]
# ExecStart=
# ExecStart=/usr/sbin/openvasmd <your desired options>

# The file the OpenVAS Manager will use as database.
DATABASE_FILE=/var/lib/openvas/mgr/tasks.db

# The address the OpenVAS Manager will listen on.
MANAGER_ADDRESS=127.0.0.1

# The port the OpenVAS Manager will listen on.
MANAGER_PORT=9390
```

#leafpad/etc/default/greenbone-security-assistant //访问web 端接口(gsad):访问opebvas 服务层的web 接口，默认监听地址为127.0.0.1，端口为9392。

此文件也是修改两处：GSA_ADDRESS和MANAGER_ADDRESS

```
greenbone
文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)
# NOTE: This file is not used if you are using systemd. The options are
# hardcoded in the greenbone-security-assistant.service file. If you want to change
# them you should override the service file by creating a file
# /etc/systemd/system/greenbone-security-assistant.service.d/local.conf like this:
# [Service]
# ExecStart=
# ExecStart=/usr/sbin/gsad --foreground

# The address the Greenbone Security Assistant will listen on.
GSA_ADDRESS=127.0.0.1

# The port the Greenbone Security Assistant will listen on.
GSA_PORT=9392

# The file to use as private key for HTTPS
#GSA_SSL_PRIVATE_KEY=

# The file to use as certificate for HTTPS
#GSA_SSL_CERTIFICATE=

# Should HTTP get redirected to HTTPS
# If $GSA_REDIRECT_PORT is not set it will redirect port 80.
#GSA_REDIRECT=1

# Redirect HTTP from this port to $GSA_PORT
# For this being effective $GSA_REDIRECT has to be set to 1.
#GSA_REDIRECT_PORT=9394

# The address the OpenVAS Manager is listening on.
MANAGER_ADDRESS=127.0.0.1

# The port the OpenVAS Manager is listening on.
MANAGER_PORT=9390
```

重新加载systemctl

```
#systemctl daemon-reload
```

重新启动openvas:

```
#openvas-stop
```

```
#openvas-start
```

重新检测安装完整性

```
# openvas-check-setup
```

OK, 搞定。


输入<https://ip:9392>，从本机意外的地方即可访问。

6) 修改密码

Openvas自动生成的默认密码太长，不容易记，我们可以修改成符合我们记忆习惯的密码。修改密码有两种方式，一种为命令行修改，另外一种GSM修改。此处介绍第一种修改方式。

通过命令行修改

```
# openvasmd --user=admin--new-password=admin
```



7) 升级插件和漏洞库

```
# openvas-feed-update //第一次安装，可以不用更新
```

```
# greenbone-nvt-sync // openvas-feed-update和greenbone-nvt-sync都可以升级插件和漏洞库，建议使用openvas-feed-update进行升级。
```

8) 其他命令：

```
#openvas-start //启动openvas
```

```
#openvas-stop //停止openvas
```

```
#openvasmd--help //帮助
```

2、Openvas的使用

1) 登录openvas

登录地址：<https://IP:9392>，我测试机的地址是：<https://192.168.3.126:9392>，输入登录账号密码：admin/admin

2) 新建任务

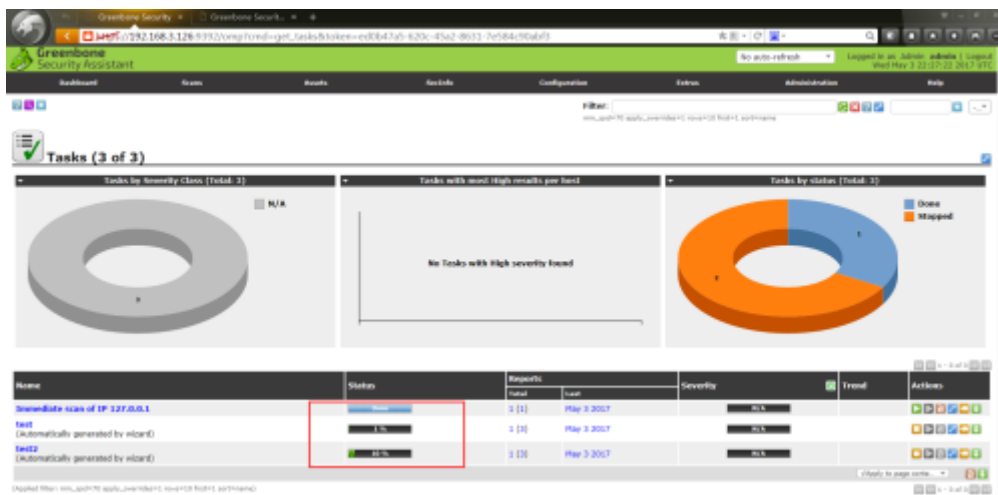
新建任务有两种方式：快速扫描和高级扫描

(1) 快速扫描

点击Scans-》Tasks打开扫描任务管理界面，如下图：

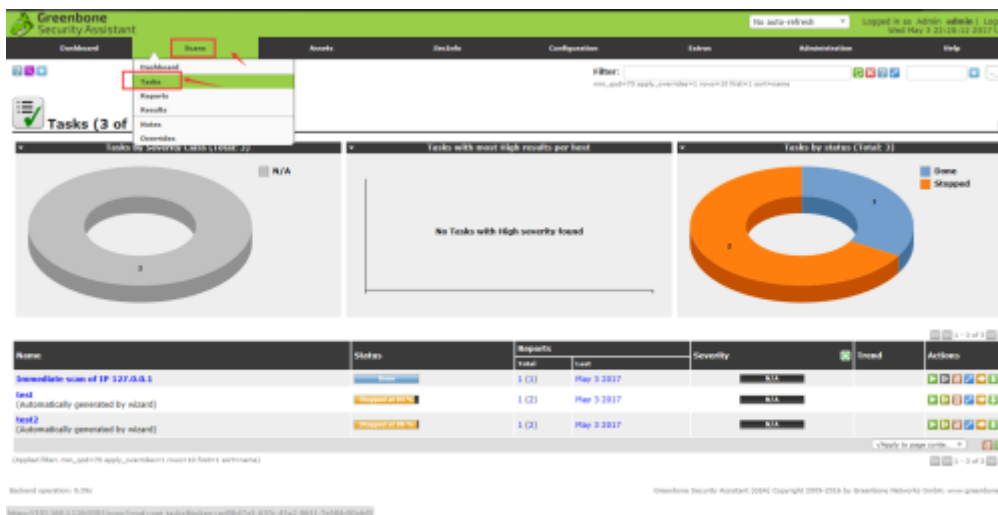


可以查看扫描进度，如下图：

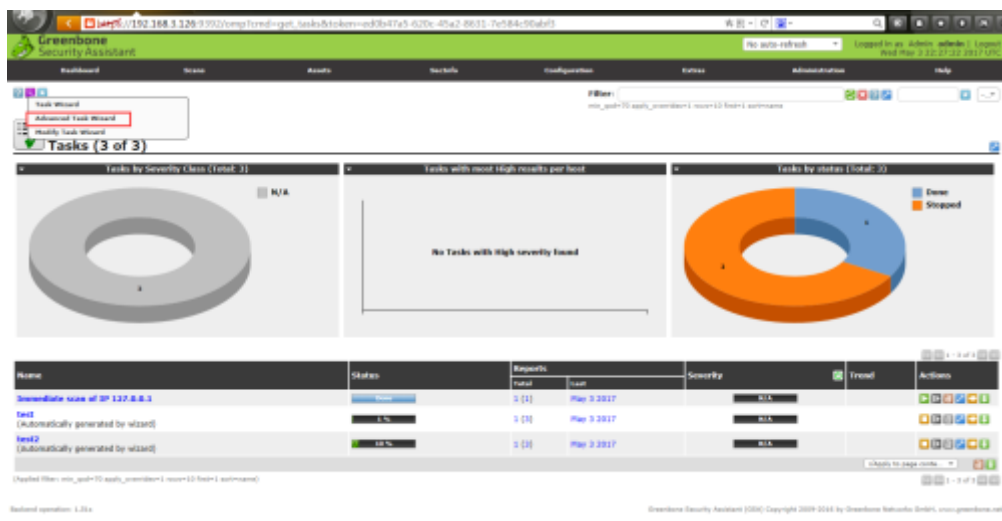


(2) 高级扫描

点击Scans-》Tasks打开扫描任务管理界面，如下图：



任务管理图标-》Advanced Task Wizard（高级任务向导），如下图：



打开高级任务向导页面，如下图：

任务名称

扫描配置

扫描主机

开始时间

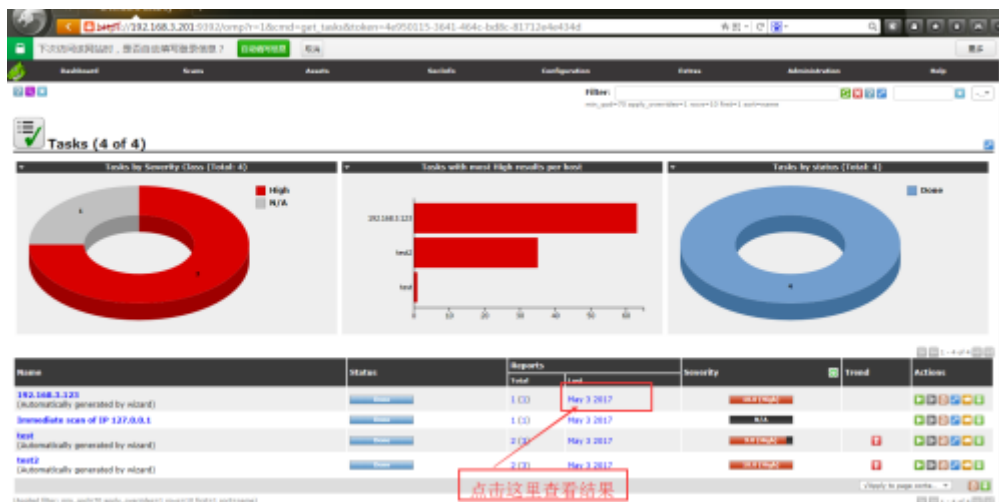
认证方式: ssh, smb等

报告发送邮件

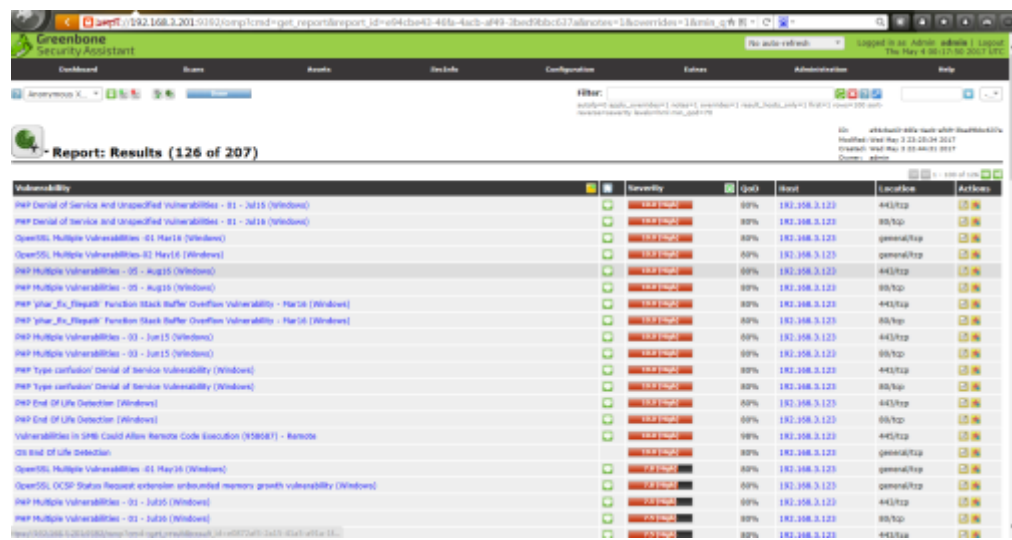
填写任务名称、扫描配置、扫描主机、开始时间等，点击“Create”，即可开始扫描。

3) 查看扫描结果

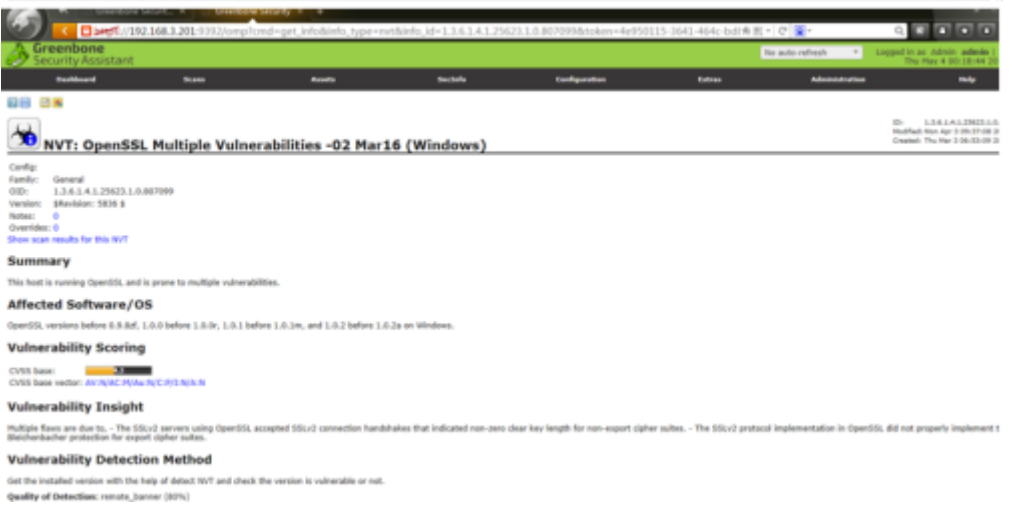
扫描结束后，查看扫描结果



查看漏洞列表

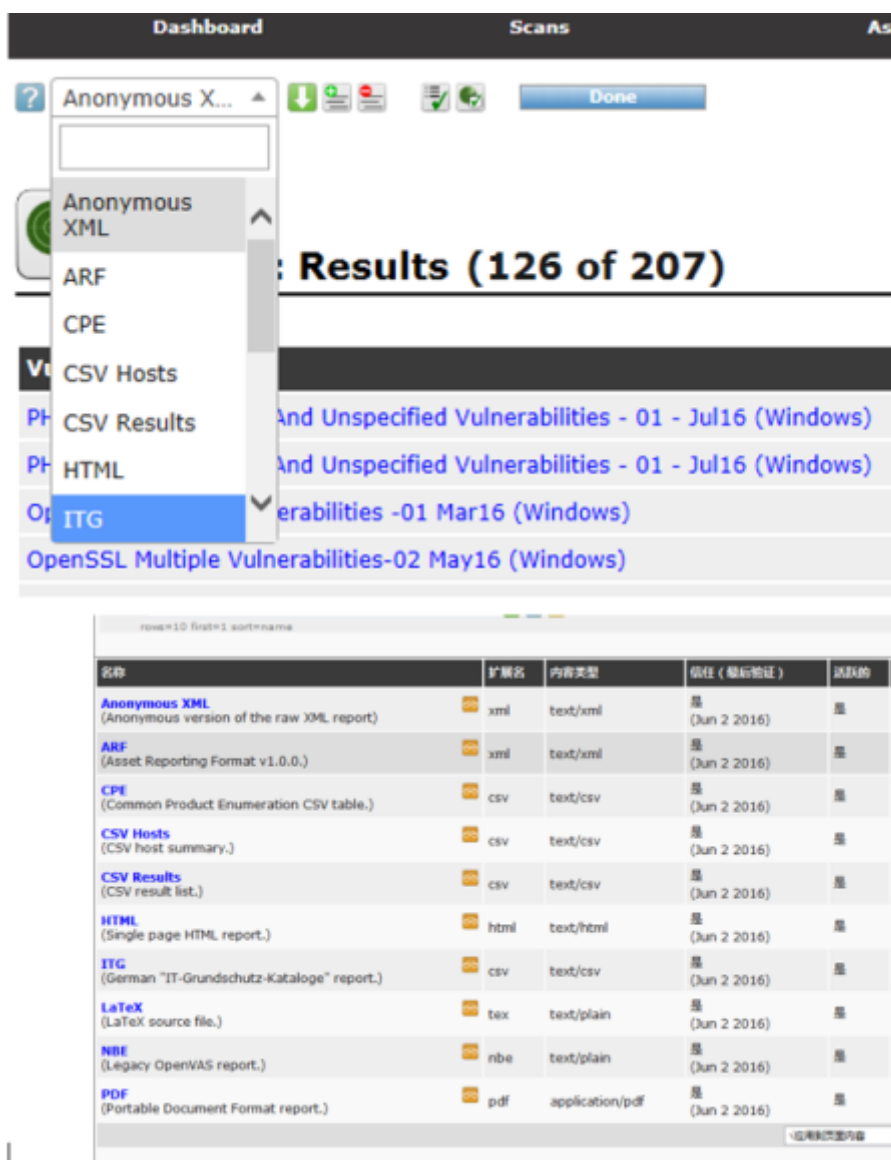


查看漏洞详情

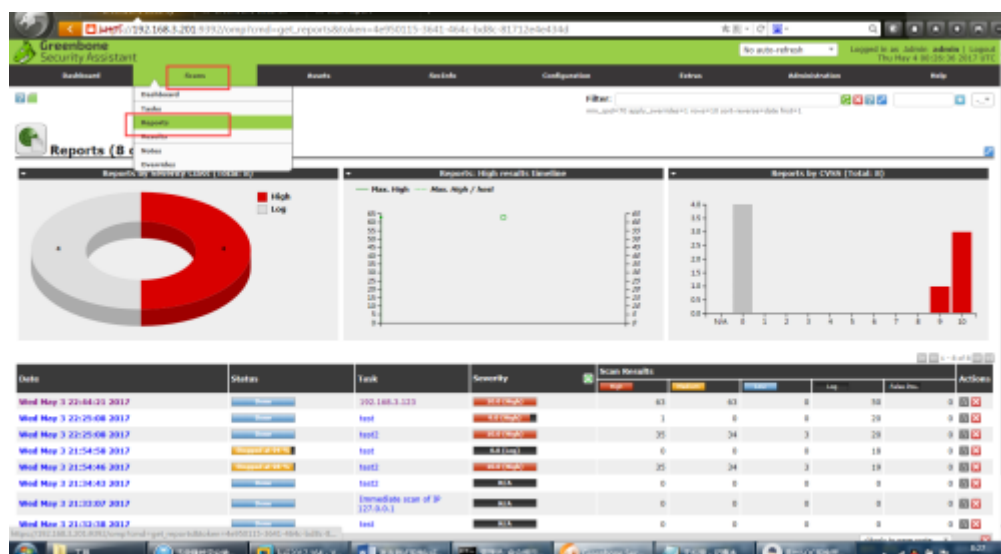


4) 导出扫描报告

扫描报告支持多种格式输出，如下图所示：



选择“Scans (扫描管理)”-“Reports (报告)”，如下图：



打开要导出报告的任务，进入漏洞列表，如图：

