

BackTrack5漏洞评估之OpenVAS(Open Vulnerability Assessment System)

2012-05-16

来源: 互联网

作者: 自学网

点击:

OpenVAS (Open Vulnerability Assessment System)是一个包含集成安全工具和服务的系统，为漏洞管理提供了强大的平台，其开发基于C/S架构，通过客户端向服务端请求对目标的具体网络漏洞执行测试集。模块化和稳定的设计使该平台支持并行安全测试的同时支持多操作系统(Linux/Win32)。

OpenVAS核心组件和功能。

1、OpenVAS Scanner可以有效地管理NVT (Network Vulnerability Tests, 网络漏洞测试)的执行。测试插件可以通过NVT种子()每日更新。

2、OpenVAS Client提供基于传统桌面方式访问和基于命令行访问。

该工具主要功能是通过OTP (OpenVAS Transfer Protocol, OpenVAS传输协议)控制扫描执行，该协议为OpenVAS Scanner的基础通信协议。

3、OpenVAS Manager为漏洞扫描提供核心服务，主要负责存储配置和扫描结果。

此外，提供基于XML的OMP (OpenVAS Management Protocol, OpenVAS管理协议)，以方便执行各种功能。例如，扫描调度、报告生成、扫描结果过滤和聚合等。

4、Greenbone Security Assistant是一个基于OMP运行的Web服务。

用户能够用其基于OMP的客户端提供的Web访问接口，配置、管理和控制扫描过程。

其桌面版称为GSA Desktop，提供了与之类似的功能。

除此之外，OpenVAS命令行也为OMP基础通信提了命令行接口。

5、OpenVAS Administrator 负责处理用户管理和种子更新管理。

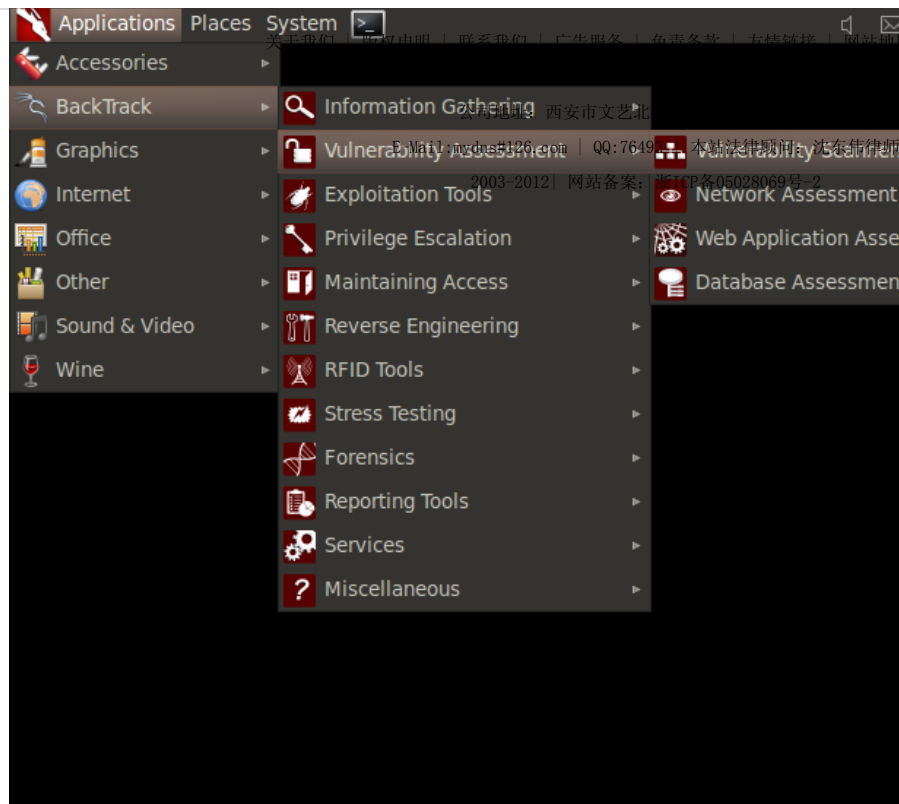
需要注意一点的是BT5中OpenVAS跟BT4中的不大一样了，在BT4中的OpenVAS不像BT5要敲那么多命令，而本文只讲BT5的OpenVAS。

首先创建一个证书，用于SSL加密的，因为是C/S架构：

排行 热门

- linux上NC的应用——蜜罐技术
- Auto pentesting. Nmap, SSLscans, screens
- 制作Backtrack USB启动盘
- 使用REAPER破解PIN到90.00%~99.99%问题的解
- SQL注入漏洞测试工具比较
- BackTrack5漏洞评估之OpenVAS(Open Vulnera
- BackTrack 5 R1 XSS研究之XSSer使用说明中
- Burp Suite工具使用之四-Sequencer模块介绍
- dnsenum的使用
- patator暴力破解工具使用教程
- BackTrack 5学习之SQLNinja
- Wireshark使用方法（学习笔记一）
- Metasploit攻击Oracle的环境搭建

- 彩虹表的原理简介
- 微软“影子系统” EWF让你运行不明程序不再
- BackTrack5漏洞评估之OpenVAS(Open Vulnera
- 强大的嗅探工具ettercap使用教程
- ettercap的几个不错的用法
- Nessus 5.0 使用指南
- john破解*nix密码
- 最受欢迎的十大WEB应用安全评估系统
- How to install Nessus 5.0 offline
- PHP Taint - 一个用来检测XSS漏洞的扩展
- backtrack5下注册nessus非商用版
- 利用PwDump7抓取系统hash为空白时候的解决
- Cain嗅探80端口时过滤垃圾信息



- backtrack5下注册nessus非商用版
- 制作Backtrack USB启动盘
- 使用IDA解密恶意软件
- Backtrack安装额外工具
- 虚拟机安装BackTrack-Linux全过程
- Burp Suite工具使用之一-Scanner模块介绍
- 向日葵远程控制软件全面评测 安全且强悍
- 三款免费渗透测试工具
- 使用REAPER破解PIN到90.00%~99.99%问题的解
- Linux常用的安全工具
- BackTrack 5 R1 XSS研究之XSSer使用说明中
- 最受欢迎的十大WEB应用安全评估系统
- PHP Taint - 一个用来检测XSS漏洞的扩展

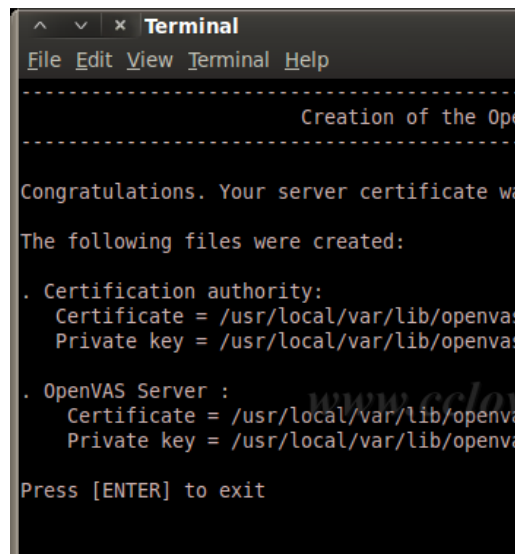
填入信息，随便填：

```
Terminal
File Edit View Terminal Help
/usr/local/var/lib/openvas/private/CA create
/usr/local/var/lib/openvas/CA created
-----
Creation of the OpenVAS CA
-----

This script will now ask you the relevant information to create the
state of OpenVAS.
Note that this information will *NOT* be sent to anyone, but anyone
with the ability to connect to the OpenVAS server can retrieve this
information.

CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [DE]: CN
Your state or province name [none]: GuangDong
Your location (e.g. town) [Berlin]: GuangZhou
Your organization [OpenVAS Users United]: w
```

生成成功了：



```
^ _ x Terminal
File Edit View Terminal Help

-----
Creation of the OpenVAS certificates
-----

Congratulations. Your server certificate was created.

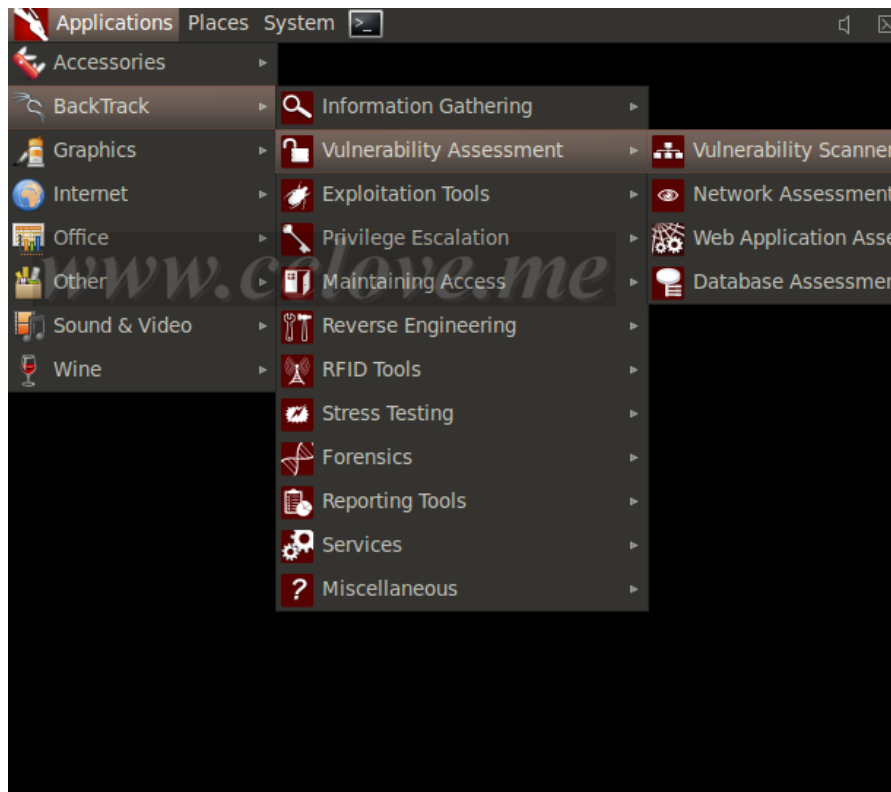
The following files were created:

. Certification authority:
  Certificate = /usr/local/var/lib/openvas/cacert.pem
  Private key = /usr/local/var/lib/openvas/cacert.pem

. OpenVAS Server :
  Certificate = /usr/local/var/lib/openvas/servercert.pem
  Private key = /usr/local/var/lib/openvas/serverkey.pem

Press [ENTER] to exit
```

再添加用户：



填入用户名和密码，这个用户的角色是openvassd user：

```
^ v x root@LK-BT5: ~
File Edit View Terminal Help
Using /var/tmp as a temporary file holder.

Add a new openvassd user
-----

Login : LK
Authentication (pass/cert) [pass] :
Login password :
Login password (again) :

User rules
-----
openvassd has a rules system which allows you to res
For instance, you may want him to be able to scan hi

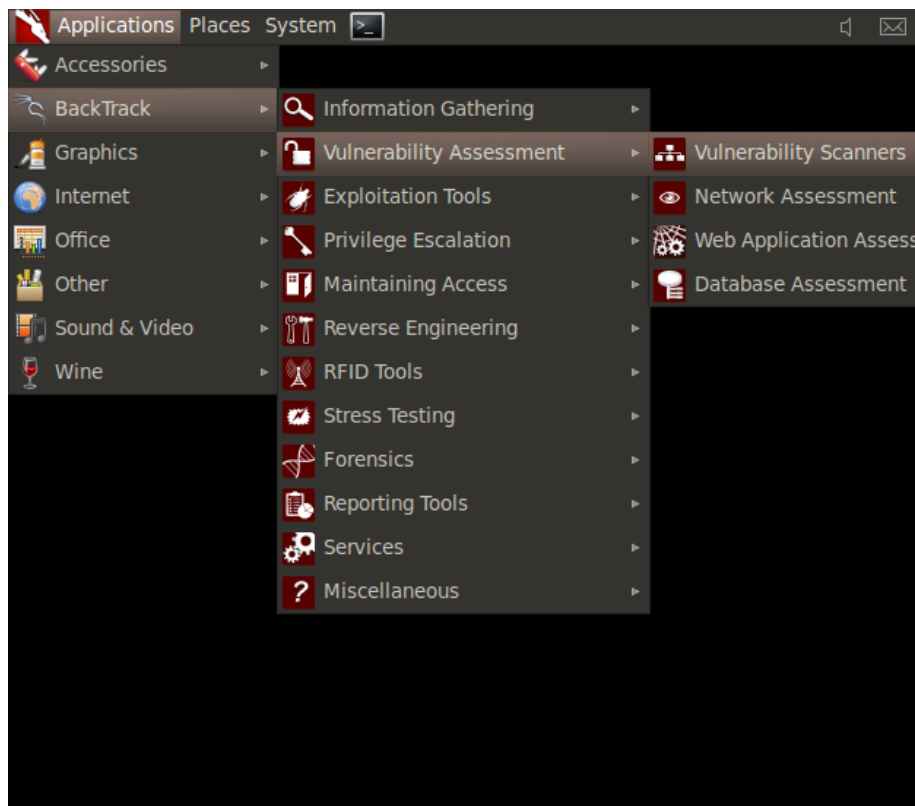
Please see the openvas-adduser(8) man page for the r

Enter the rules for this user, and hit ctrl-D once y
(the user can have an empty rules set)

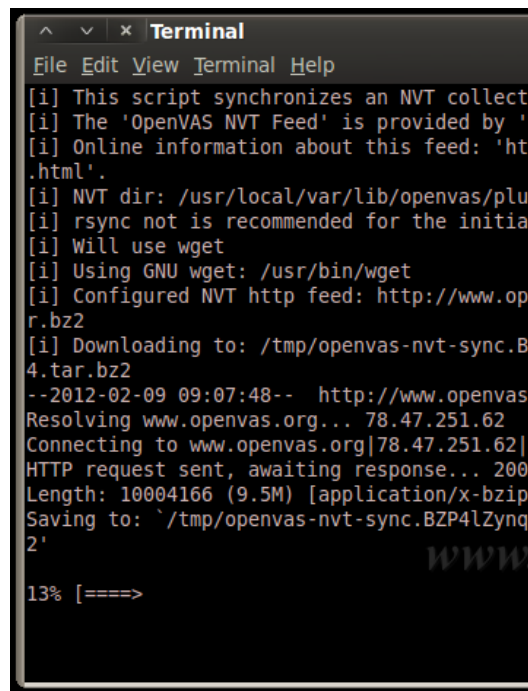
Login          : LK
Password       : *****
Rules          :

Is that ok? (y/n) [y] y
user added.
```

更新插件，通过NVT:



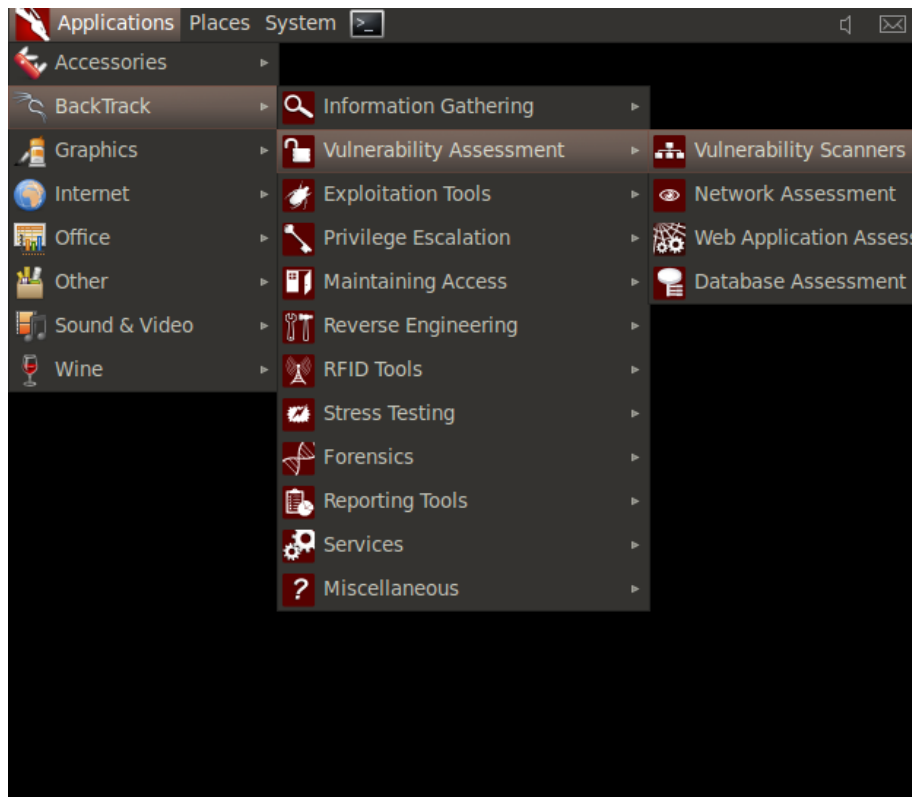
更新中:



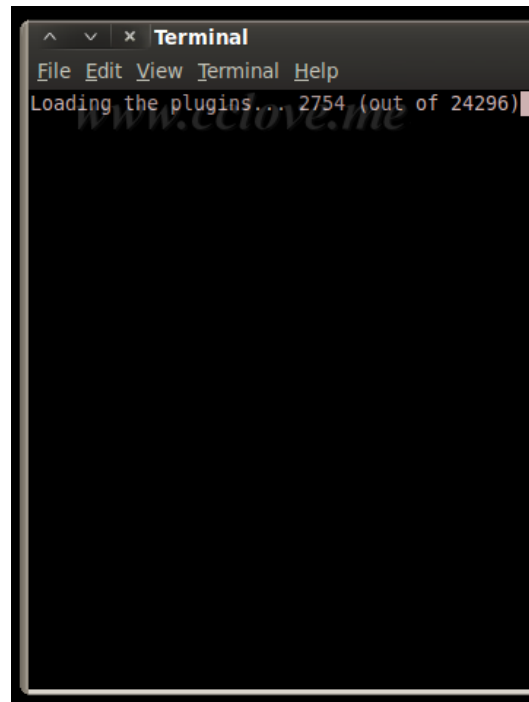
```
^ v x Terminal
File Edit View Terminal Help
[i] This script synchronizes an NVT collecti
[i] The 'OpenVAS NVT Feed' is provided by 'T
[i] Online information about this feed: 'htt
.html'.
[i] NVT dir: /usr/local/var/lib/openvas/plug
[i] rsync not is recommended for the initial
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.ope
r.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.BZ
4.tar.bz2
--2012-02-09 09:07:48-- http://www.openvas.
Resolving www.openvas.org... 78.47.251.62
Connecting to www.openvas.org[78.47.251.62]:
HTTP request sent, awaiting response... 200
Length: 10004166 (9.5M) [application/x-bzip2]
Saving to: `/tmp/openvas-nvt-sync.BZP4lZynq8
2'

13% [====>
```

开启openvas scanner 后台进程:



然后它开始加载的插件:



设置OpenVAS manager服务，先添加一个客户端的证书给openvas manager:

```
root@LK-BT5: ~  
File Edit View Terminal Help  
root@LK-BT5:~# openvas-mkcert-client -n om -i  
Generating RSA private key, 1024 bit long modulus  
.....++++++  
.....++++++  
e is 65537 (0x10001)  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State]  
ts Pty Ltd]:Organizational Unit Name (eg, section) []:Common Name (eg, your name  
/openvas-mkcert-client.2627/stdC.cnf  
Check that the request matches the signature  
Signature ok  
The Subject's Distinguished Name is as follows  
countryName          :PRINTABLE:'DE'  
localityName         :PRINTABLE:'Berlin'  
commonName           :PRINTABLE:'om'  
Certificate is to be certified until Feb  8 14:21:01 2013 GMT (365 days)  
  
Write out database with 1 new entries  
Data Base Updated  
User om added to OpenVAS.
```

然后重建数据库，这个在每次与NVT同步之后都要做:

再添加一个为管理员角色的用户:

开启OpenVAS Manager后台进程:

开启OpenVAS Administrator后台进程:

再开启Greenbone Security Assistant后台进程, 这个是为了web登陆的,
如果想用C/S架构而不想用B/S架构的话, 这个可以不用:

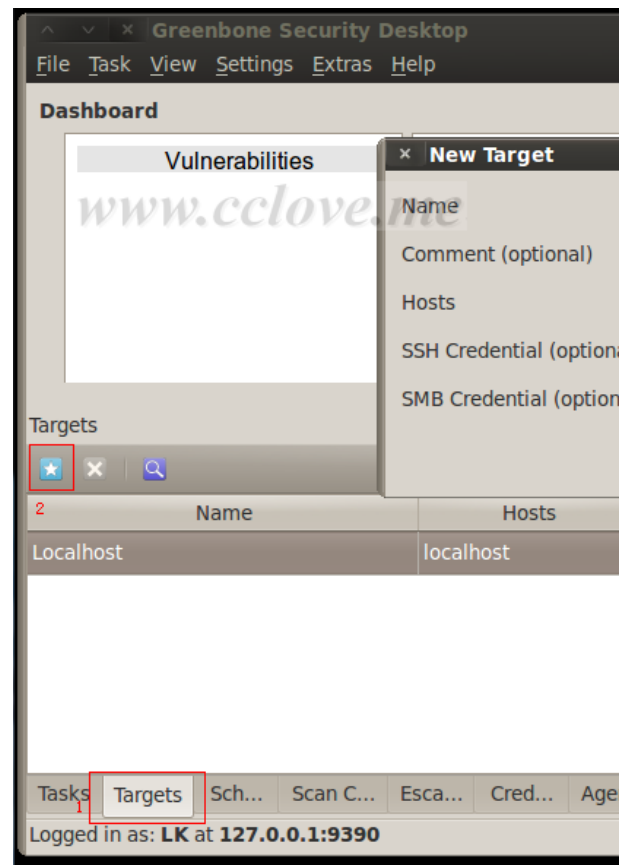
好了, 服务器方面就搞定了。

接下来就是要连接上去, 你可以使用客户端连接,
或者直接打开浏览器键入:9392 来访问。

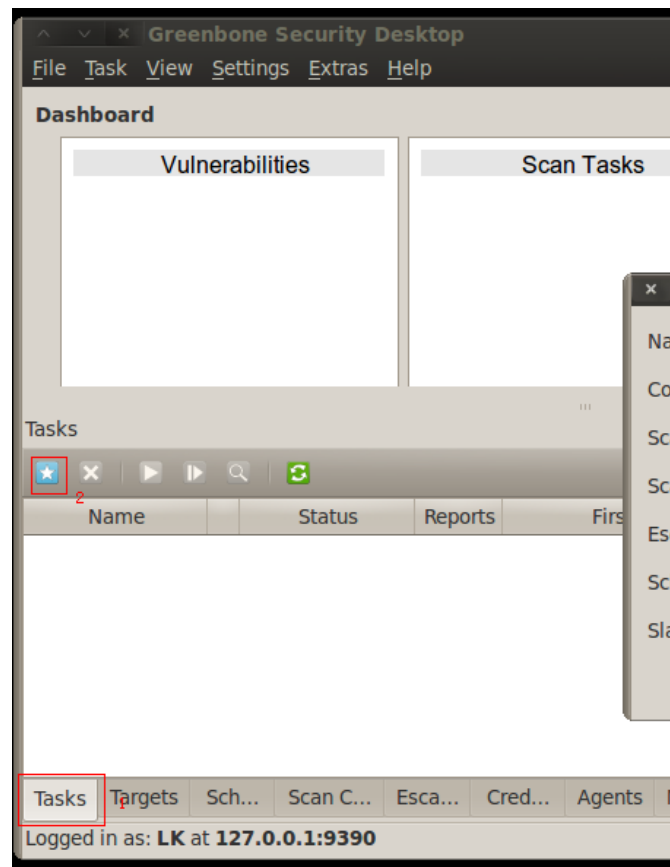
打开客户端, 输入用户名密码:



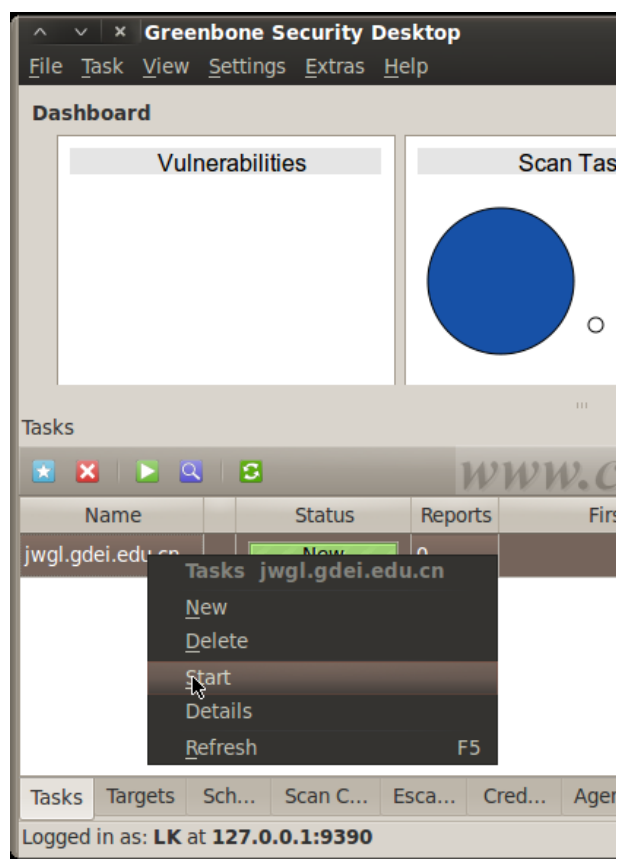
登陆进去之后先添加一个目标, 这跟BT4的不大一样, BT4的是直接输入的, 而在这里, 要分别输入,
刚开始我还以为要注册才可以扫描其它计算机:



然后再添加一个任务:



开始扫描:

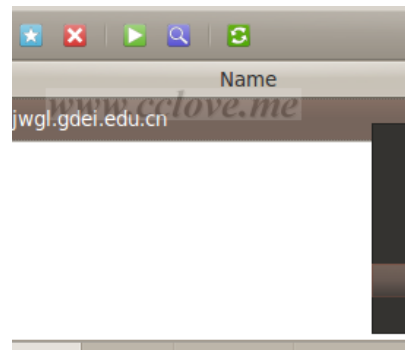


然后就可以看到正在扫描了，客户端不能实时显示进度，要自己去刷新，

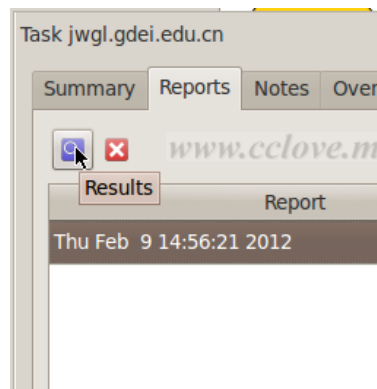
在菜单栏某选项有刷新的选项可以选择，于是我设置每10秒自动刷新一次：



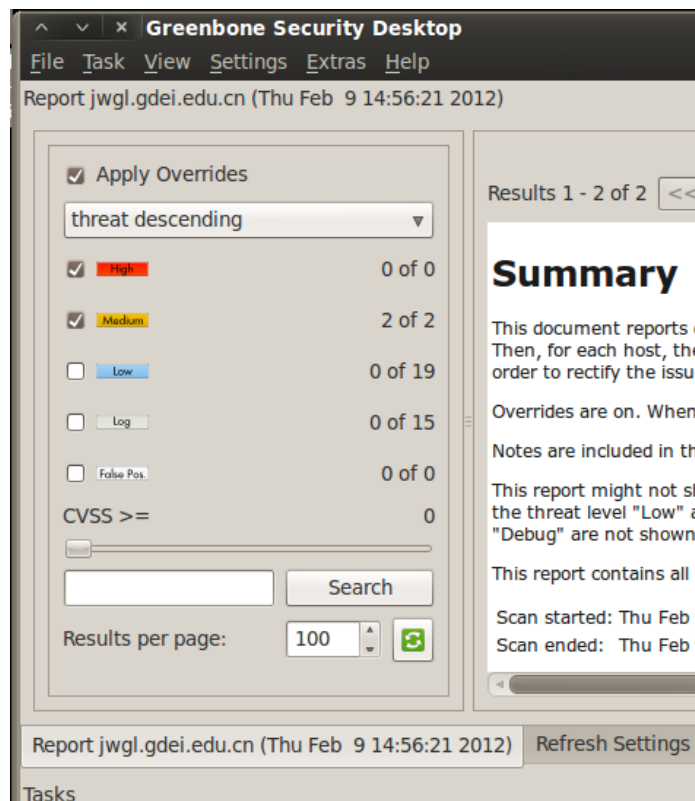
完成之后右键单击任务，选择Details:



选择查看结果:



可以在这里查看，也可以导出为其它格式，我就习惯导出为html：



参考资料#Installing_OpenVAS

上一篇：[metasploit常用渗透命令](#)

下一篇：[网络抓包工具wireshark常用封装过滤规则](#)

相关文章

[linux上NC的应用——蜜罐技术](#)

[制作Backtrack USB启动盘](#)

[SQL注入漏洞测试工具比较](#)

[BackTrack 5 R1 XSS研究之XSSer](#)

[Auto pentesting. Nmap, SSLscan](#)

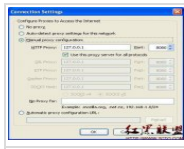
[使用REAPER破解PIN到90.00%~99.9](#)

[BackTrack5漏洞评估之OpenVAS \(Op](#)

[Burp Suite工具使用之四-Sequencer](#)

[dnsenum的使用](#)[patator暴力破解工具使用教程](#)

图文推荐

[linux上NC的应用——蜜](#)[BackTrack5漏洞评估之Op](#)[Burp Suite工具使用之四](#)[Burp Suite工具使用之一](#)

发表评论

验证码:

☐

匿名?

[发表评论](#)[最新评论](#) [进入详细评论页>>](#)