

# Openvas 漏洞扫描器 配置和使用

何伊圣

[Akast@ngsst.com](mailto:Akast@ngsst.com)

NEURON

# 关于

- **OpenVAS** : 免费, 命令行界面、图形界面、WEB界面。
- **Nessus**、**Nexpose** : 商业, 命令行界面、web界面。
- apt-get install nexpose
- SAINT: saintexploit
- magicbox ubuntu debian



# 安装

- magicbox里面已经安装好openvas了，其他ubuntu系统要使用magicbox的源来安装OpenVAS，或者手动下载来安装。
- 直接安装openvas，不用更新系统。
- apt-get install openvas
- 重新启动magicbox系统

# 其他系统里面手动安装

- **Step 1: Configure OBS Repository**
- `sudo apt-get -y install python-software-properties`
- `sudo add-apt-repository "deb  
http://download.opensuse.org/repositories/security:/OpenVAS:/STABLE:/v4/xUbuntu\_10.04/ ./"`
- `sudo apt-key adv --keyserver hkp://keys.gnupg.net --recv-keys BED1E87979EAFD54`
- `sudo apt-get update` 先要删除或注释掉deb-src的一行，否则更新会出错。
- `wget  
http://download.opensuse.org/repositories/security:/OpenVAS:/STABLE:/v4/Debian\_5.0/Release.key`
- `apt-key adv --import Release.key`

魔方渗透系统

```
root@magicbox:~# apt-key adv --keyserver hkp://keys.gnupg.net --recv-keys BED1E87979EAFD54
Executing: gpg --ignore-time-conflict --no-options --no-default-keyring --secret-keyring /etc/
primary-keyring /etc/apt/trusted.gpg --keyserver hkp://keys.gnupg.net --recv-keys BED1E87979E
gpg: 下载密钥'79EAFD54', 从 hkp 服务器 keys.gnupg.net
gpg: 密钥 79EAFD54: 公钥"security OBS Project <security@build.opensuse.org>"已导入
gpg: 没有找到任何绝对信任的密钥
gpg: 合计被处理的数量: 1
gpg: 已导入: 1
root@magicbox:~#
```



root@magicbox: ~



[OpenVAS - Install Op...



```
root@magicbox:~# apt-get -y install greenbone-security-assistant gsd openvas-cli openvas-manager openvas-scanner openvas-administrator s
```

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

greenbone-security-assistant 已经是最新的版本了。

openvas-cli 已经是最新的版本了。

openvas-manager 已经是最新的版本了。

openvas-scanner 已经是最新的版本了。

openvas-administrator 已经是最新的版本了。

sqlite3 已经是最新的版本了。

xsltproc 已经是最新的版本了。

将安装下列额外的软件包：

libopenvas4 libqt4-webkit

下列【新】软件包将被安装：

gsd libopenvas4 libqt4-webkit

升级了 0 个软件包，新安装了 3 个软件包，要卸载 0 个软件包，有 1 个软件包未被升级。

需要下载 1,845kB 的软件包。

解压缩后会消耗掉 5,243kB 的额外空间。

获取：1 [http://32.repository.backtrack-linux.org/revolution/main/libqt4-webkit\\_4:4.7.0-0ubuntu2~lucid1~ppa2](http://32.repository.backtrack-linux.org/revolution/main/libqt4-webkit_4:4.7.0-0ubuntu2~lucid1~ppa2) [46.2kB]

获取：2 [http://download.opensuse.org/repositories/security:/OpenVAS:/STABLE:/v4/xUbuntu\\_10.04/](http://download.opensuse.org/repositories/security:/OpenVAS:/STABLE:/v4/xUbuntu_10.04/) ./ gsd 1.2.2-1 [1,104kB]

获取：3 [http://download.opensuse.org/repositories/security:/OpenVAS:/STABLE:/v4/xUbuntu\\_10.04/](http://download.opensuse.org/repositories/security:/OpenVAS:/STABLE:/v4/xUbuntu_10.04/) ./ libopenvas4 4.0.6-1 [695kB]

下载 1,845kB，耗时 12秒 (148kB/s)

选中了曾被取消选择的软件包 libopenvas4。

(正在读取数据库 ... 系统当前总共安装有 239074 个文件和目录。)

正在解压缩 libopenvas4 (从 .../libopenvas4\_4.0.6-1\_i386.deb) ...

选中了曾被取消选择的软件包 libqt4-webkit。

正在解压缩 libqt4-webkit (从 .../libqt4-webkit\_4%3a4.7.0-0ubuntu2~lucid1~ppa2\_i386.deb) ...

选中了曾被取消选择的软件包 gsd。

正在解压缩 gsd (从 .../archives/gsd\_1.2.2-1\_i386.deb) ...

正在处理用于 man-db 的触发器...

正在设置 libopenvas4 (4.0.6-1) ...

正在设置 libqt4-webkit (4:4.7.0-0ubuntu2~lucid1~ppa2) ...

正在设置 gsd (1.2.2-1) ...

正在处理用于 libc-bin 的触发器...

ldconfig deferred processing now taking place

```
root@magicbox:~#
```



魔方渗透系统

# NEURON

# Openvas路径

应用程序 位置 系统 1月10日星期四 上午

MagicBox 信息搜集工具 root@magicbox: /pentest/misc/openvas

Wine 漏洞扫描工具 漏洞扫描工具 Nessus

附件 漏洞利用工具 网络安全评估 OpenVAS漏洞扫描工具 OpenVAS Adduser

互联网 权限提升工具 WEB应用评估 lynis Openvas check setup

其它 维持访问工具 mantra OpenVAS Mkcert

greenbone-security-a 数据库安全工具 OpenVAS NVT Sync

openvas-cli 已经是最新 无线安全工具 Start Greenbone Security Assistant

openvas-manager 已经是最新 报告编写工具 Start Greenbone Security Desktop

openvas-scanner 已经是最新 启动常用服务 Start Openvas Administrator

openvas-administrator 已经是最新 杂项工具 Start Openvas Cli

sqlite3 已经是最新的 下列【新】软件包将被安装： Start OpenVAS Manager

xsltproc 已经是最新的 gsd libopenvas4 libqt4-webkit Start OpenVAS Scanner

将会安装下列额外的软件包： Start OpenVAS Scanner

libopenvas4 libqt4-webkit 升级了 0 个软件包，新安装了 3 个软件包，要卸载需要下载 1,845kB 的软件包。 Stop Greenbone Security Assistant

解压后会消耗掉 5,243kB 的额外空间。 Stop Openvas Administrator

获取：1 http://32.repository.backtrack-linux.org/ Stop Openvas Cli

获取：2 http://download.opensuse.org/repositories/ OpenVAS feed server - http://openvas.org/ Stop OpenVAS Manager

获取：3 http://download.opensuse.org/repositories/ This service is hosted by Intevation GmbH - http://intevation.de Stop OpenVAS Scanner

下载 1,845kB，耗时 12秒 (148kB/s)

选中了曾被取消选择的软件包 libopenvas4。

(正在读取数据库 ... 系统当前总共安装有 239074 个软件包)

正在解压缩 libopenvas4 (从 .../libopenvas4\_4.0.0-1.i586.rpm.rpm)

```

zope_path_disclosure.nasl
zope_path_disclosure.nasl
zope_zclass.nasl
zope_zclass.nasl.asc
zyxel_http_pwd.nasl
zyxel_http_pwd.nasl.asc
zyxel_pwd.nasl
zyxel_pwd.nasl.asc
[i] Download complete
[i] Checking dir: ok
[i] Checking MD5 checksum: ok
root@magicbox:/pentest/misc/openvas# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'
[i] Online information about this feed: 'http://www.openvas.org'
[i] NVT dir: /usr/local/var/lib/openvas/plugins
[i] Will use rsync
[i] Using rsync: /usr/bin/rsync
[i] Configured NVT rsync feed: rsync://feed.openvas.org/openvas.nvt
OpenVAS feed server - http://openvas.org/
This service is hosted by Intevation GmbH - http://intevation.de
All transactions are logged.
Please report problems to admin@intevation.de
  
```

# Openvas 配置

- 跟着下面的步骤，一步一步配置即可。
- `openvas-check-setup` 安装检查工具是非常有用的工具，它能帮助诊断问题并提供有关如何解决这些问题的建议。





# Openvas-配置检查

- `cd /pentest/misc/openvas`
- `./openvas-check-setup`

```
root@magicbox: /pentest/misc/openvas
```

```
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
```

```
sh: /pentest/misc/openvas/openvas-check-setup.sh: 没有那个文件或目录
```

```
root@magicbox:~# cd /pentest/misc/openvas/
```

```
root@magicbox:/pentest/misc/openvas# ls
```

```
openvas-check-setup
```

```
root@magicbox:/pentest/misc/openvas# mv openvas-check-setup openvas-check-setup.sh
```

```
sh
```

```
root@magicbox:/pentest/misc/openvas# ls
```

```
openvas-check-setup.sh
```

```
root@magicbox:/pentest/misc/openvas# ./openvas-check-setup.sh
```

```
openvas-check-setup 2.1.5
```

```
Test completeness and readiness of OpenVAS-4  
(add '--v5' if you want to check for OpenVAS-5)
```

```
Please report us any non-detected problems and  
help us to improve this check routine:  
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
```

```
Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.
```

```
Use the parameter --server to skip checks for client tools  
like GSD and OpenVAS-CLI.
```

```
Step 1: Checking OpenVAS Scanner ...
```

```
OK: OpenVAS Scanner is present in version 3.2.5.
```

```
ERROR: No CA certificate file of OpenVAS Scanner found.
```

```
FIX: Run 'openvas-mkcert'.
```

```
ERROR: Your OpenVAS-4 installation is not yet complete!
```

```
Please follow the instructions marked with FIX above and run this  
script again.
```

```
If you think this result is wrong, 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@magicbox:/pentest/misc/openvas#
```



# Openvas证书配置

CA certificate life time in days [1460]:

CA证书的使用寿命（默认是1460天）

Server certificate life time in days [365]:

服务器证书的使用寿命（默认是365天）

Your country (two letter code) [DE]:

您所在国家（两个字母代码）

Your state or province name [none]:

您所在的州或省的名称

Your location (e.g. town) [Berlin]:

您所在的位置（例如镇）

Your organization [OpenVAS Users United]:

您所在组织

# Openvas证书配置

```
root@magicbox: /pentest/misc/openvas
```

文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

```
root@magicbox:/pentest/misc/openvas# openvas-mkcert
```

```
/usr/local/var/lib/openvas/private/CA created
```

```
/usr/local/var/lib/openvas/CA created
```

-----  
Creation of the OpenVAS SSL Certificate  
-----

This script will now ask you the relevant information to create the SSL certificate of OpenVAS.

Note that this information will *\*NOT\** be sent to anybody (everything stays local), but anyone with the ability to connect to your OpenVAS daemon will be able to 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]: NEURON

Your organization [OpenVAS Users United]: NEURON

# Openvas证书配置

```
root@magicbox: /pentest/misc/openvas
```

文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

## Creation of the OpenVAS SSL Certificate

Congratulations. Your server certificate was properly created.

The following files were created:

. Certification authority:

Certificate = /usr/local/var/lib/openvas/CA/cacert.pem

Private key = /usr/local/var/lib/openvas/private/CA/cakey.pem

. OpenVAS Server :

Certificate = /usr/local/var/lib/openvas/CA/servercert.pem

Private key = /usr/local/var/lib/openvas/private/CA/serverkey.pem

Press [ENTER] to exit



```
root@magicbox:/pentest/misc/openvas# ./openvas-check-setup.sh
openvas-check-setup 2.1.5
Test completeness and readiness of OpenVAS-4
(add '--v5' if you want to check for OpenVAS-5)

Please report us any non-detected problems and
help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.

Use the parameter --server to skip checks for client tools
like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
OK: OpenVAS Scanner is present in version 3.2.5.
OK: OpenVAS Scanner CA Certificate is present as /usr/local/var/lib/openvas/CA/cacert.pem.
ERROR: The NVT collection is very small.
FIX: Run a synchronization script like openvas-nvt-sync or greenbone-nvt-sync.

ERROR: Your OpenVAS-4 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.

If you think this result is wrong, 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@magicbox:/pentest/misc/openvas#
```



# openvas-nvt-sync升级漏洞库

- 使用命令openvas-nvt-sync更新NVTs (Network Vulnerability Tests) 文件，是一些.nasl和.inc文件，用于测试漏洞的。NVT同步脚本，更新扫描规则库。

```
root@magicbox:/pentest/misc/openvas# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[i] NVT dir: /usr/local/var/lib/openvas/plugins
[i] Will use rsync
[i] Using rsync: /usr/bin/rsync
[i] Configured NVT rsync feed: rsync://feed.openvas.org:/nvt-feed
OpenVAS feed server - http://openvas.org/
This service is hosted by Intevation GmbH - http://intevation.de/
All transactions are logged.
Please report problems to admin@intevation.de
```

```
receiving incremental file list
```

魔方渗透系统

```
./
GSHB/
nmap_nse/
```

# NEURON

```
sent 52 bytes  received 980270 bytes  12814.67 bytes/sec
total size is 146379807  speedup is 149.32
```

```
[i] Checking dir: ok
[i] Checking MD5 checksum: ok
```

IRC: root@magicbox:/pentest/misc/openvas#

```
root@magicbox:/pentest/misc/openvas# ./openvas-check-setup.sh
openvas-check-setup 2.1.5
Test completeness and readiness of OpenVAS-4
(add '--v5' if you want to check for OpenVAS-5)

Please report us any non-detected problems and
help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.

Use the parameter --server to skip checks for client tools
like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
OK: OpenVAS Scanner is present in version 3.2.5.
OK: OpenVAS Scanner CA Certificate is present as /usr/local/var/lib/openvas/CA/cacert.pem.
OK: NVT collection in /usr/local/var/lib/openvas/plugins contains 29247 NVTs.
WARNING: Signature checking of NVTs is not enabled in OpenVAS Scanner.
SUGGEST: Enable signature checking (see http://www.openvas.org/trusted-nvts.html).
Step 2: Checking OpenVAS Manager ...
OK: OpenVAS Manager is present in version 2.0.4.
ERROR: No client certificate file of OpenVAS Manager found.
FIX: Run 'openvas-mkcert-client -n om -i'

ERROR: Your OpenVAS-4 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.

If you think this result is wrong, 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@magicbox:/pentest/misc/openvas#
```



# Openvas-创建客户端证书

- openvas-mkcert-client -n om -i

```
root@magicbox:/pentest/misc/openvas# 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]:Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizational Unit Name (eg, section) []:Common Na
me (eg, your name or your server's hostname) []:Email Address []:Using configuration from /tmp/openvas-mkcert-
client.8036/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 Jan 10 07:44:49 2014 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
User om added to OpenVAS.

root@magicbox:/pentest/misc/openvas#
```

```
root@magicbox: /pentest/misc/openvas
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

root@magicbox:/pentest/misc/openvas# ./openvas-check-setup.sh
openvas-check-setup 2.1.5
Test completeness and readiness of OpenVAS-4
(add '--v5' if you want to check for OpenVAS-5)

Please report us any non-detected problems and
help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.

Use the parameter --server to skip checks for client tools
like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
OK: OpenVAS Scanner is present in version 3.2.5.
OK: OpenVAS Scanner CA Certificate is present as /usr/local/var/lib/openvas/CA/cacert.pem.
OK: NVT collection in /usr/local/var/lib/openvas/plugins contains 29247 NVTs.
WARNING: Signature checking of NVTs is not enabled in OpenVAS Scanner.
SUGGEST: Enable signature checking (see http://www.openvas.org/trusted-nvts.html).

Step 2: Checking OpenVAS Manager ...
OK: OpenVAS Manager is present in version 2.0.4.
OK: OpenVAS Manager client certificate is present as /usr/local/var/lib/openvas/CA/clientcert.pem.
OK: OpenVAS Manager database found in /usr/local/var/lib/openvas/mgr/tasks.db.
OK: Access rights for the OpenVAS Manager database are correct.
OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.

Error: no such table: meta
ERROR: Could not determine database revision, database corrupt or in invalid format.
FIX: Delete database at /usr/local/var/lib/openvas/mgr/tasks.db and rebuild it.

ERROR: Your OpenVAS-4 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.

If you think this result is wrong, 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@magicbox: /pentest/misc/openvas
```

```
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
```

```
root@magicbox:/pentest/misc/openvas# ./openvas-check-setup.sh
```

```
openvas-check-setup 2.1.5
```

```
Test completeness and readiness of OpenVAS-4  
(add '--v5' if you want to check for OpenVAS-5)
```

```
Please report us any non-detected problems and  
help us to improve this check routine:  
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
```

```
Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.
```

```
Use the parameter --server to skip checks for client tools  
like GSD and OpenVAS-CLI.
```

```
Step 1: Checking OpenVAS Scanner ...
```

```
OK: OpenVAS Scanner is present in version 3.2.5.
```

```
OK: OpenVAS Scanner CA Certificate is present as /usr/local/var/lib/openvas/CA/cacert.pem.
```

```
OK: NVT collection in /usr/local/var/lib/openvas/plugins contains 29247 NVTs.
```

```
WARNING: Signature checking of NVTs is not enabled in OpenVAS Scanner.
```

```
SUGGEST: Enable signature checking (see http://www.openvas.org/trusted-nvts.html).
```

```
Step 2: Checking OpenVAS Manager ...
```

```
OK: OpenVAS Manager is present in version 2.0.4.
```

```
OK: OpenVAS Manager client certificate is present as /usr/local/var/lib/openvas/CA/clientcert.pem.
```

```
OK: OpenVAS Manager database found in /usr/local/var/lib/openvas/mgr/tasks.db.
```

```
OK: Access rights for the OpenVAS Manager database are correct.
```

```
OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
```

```
OK: OpenVAS Manager database is at revision 41.
```

```
OK: OpenVAS Manager expects database at revision 41.
```

```
OK: Database schema is up to date.
```

```
ERROR: The number of NVTs in the OpenVAS Manager database is too low.
```

```
FIX: Make sure OpenVAS Scanner is running with an up-to-date NVT collection and run 'openvasmd --rebuild'.
```

```
ERROR: Your OpenVAS-4 installation is not yet complete!
```

```
Please follow the instructions marked with FIX above and run this  
script again.
```

```
If you think this result is wrong, please report your observation  
and help us to improve this check routine:
```

```
2013/1/10
```

# Openvas

- root@magicbox:/pentest/misc/openvas# rm -rf /usr/local/var/lib/openvas/mgr/tasks.db
- root@magicbox:/pentest/misc/openvas# openvassd 载入漏洞库
- root@magicbox:/pentest/misc/openvas# openvasmd --rebuild 更新后需要重建数据库，这两个步骤要等待比较久！

```
root@magicbox:/pentest/misc/openvas# rm -rf /usr/local/var/lib/openvas/mgr/tasks.db
root@magicbox:/pentest/misc/openvas# openvassd
All plugins loaded
root@magicbox:/pentest/misc/openvas# openvasmd --rebuild
root@magicbox:/pentest/misc/openvas#
```

# Openvas-添加管理员用户

```
Step 1: Checking OpenVAS Scanner ...
OK: OpenVAS Scanner is present in version 3.2.5.
OK: OpenVAS Scanner CA Certificate is present as /usr/local/var/lib/openvas/CA/cacert.pem.
OK: NVT collection in /usr/local/var/lib/openvas/plugins contains 29247 NVTs.
WARNING: Signature checking of NVTs is not enabled in OpenVAS Scanner.
SUGGEST: Enable signature checking (see http://www.openvas.org/trusted-nvts.html).

Step 2: Checking OpenVAS Manager ...
OK: OpenVAS Manager is present in version 2.0.4.
OK: OpenVAS Manager client certificate is present as /usr/local/var/lib/openvas/CA/clientcert.pem.
OK: OpenVAS Manager database found in /usr/local/var/lib/openvas/mgr/tasks.db.
OK: Access rights for the OpenVAS Manager database are correct.
OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
OK: OpenVAS Manager database is at revision 41.
OK: OpenVAS Manager expects database at revision 41.
OK: Database schema is up to date.
OK: OpenVAS Manager database contains information about 29247 NVTs.
OK: xsltproc found.

Step 3: Checking OpenVAS Administrator ...
OK: OpenVAS Administrator is present in version 1.1.2.
ERROR: No users found. You need to create at least one user to log in.
It is recommended to have at least one user with role Admin.
FIX: Create a user using 'openvasad -c 'add_user' -n <name> --role=Admin'
```

```
root@magicbox:/pentest/misc/openvas# openvasad -c 'add_user' -n neuron --role=Admin
Enter password:
ad main:MESSAGE:28500:2013-01-10 03h06.40 EST: No rules file provided, the new user will have no restrictions.
ad main:MESSAGE:28500:2013-01-10 03h06.40 EST: User neuron has been successfully created.
root@magicbox:/pentest/misc/openvas#
```

# Openvas-添加管理员用户

- 创建一个管理员用户
- `openvasad -c 'add_user' -n akast -r Admin`
- Enter password:
- `ad main:MESSAGE:5871:2011-05-26 04h57.08 BST: No rules file provided, the new user will have no restrictions.`
- `ad main:MESSAGE:5871:2011-05-26 04h57.08 BST: User openvasadmin has been successfully created.`



```
Step 1: Checking OpenVAS Scanner ...
OK: OpenVAS Scanner is present in version 3.2.5.
OK: OpenVAS Scanner CA Certificate is present as /usr/local/var/lib/openvas/CA/cacert.pem.
OK: NVT collection in /usr/local/var/lib/openvas/plugins contains 29247 NVTs.
WARNING: Signature checking of NVTs is not enabled in OpenVAS Scanner.
SUGGEST: Enable signature checking (see http://www.openvas.org/trusted-nvts.html).

Step 2: Checking OpenVAS Manager ...
OK: OpenVAS Manager is present in version 2.0.4.
OK: OpenVAS Manager client certificate is present as /usr/local/var/lib/openvas/CA/clientcert.pem.
OK: OpenVAS Manager database found in /usr/local/var/lib/openvas/mgr/tasks.db.
OK: Access rights for the OpenVAS Manager database are correct.
OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
OK: OpenVAS Manager database is at revision 41.
OK: OpenVAS Manager expects database at revision 41.
OK: Database schema is up to date.
OK: OpenVAS Manager database contains information about 29247 NVTs.
OK: xsltproc found.

Step 3: Checking OpenVAS Administrator ...
OK: OpenVAS Administrator is present in version 1.1.2.
OK: At least one user exists.
OK: At least one admin user exists.

Step 4: Checking Greenbone Security Assistant (GSA) ...
OK: Greenbone Security Assistant is present in version 2.0.1.

Step 5: Checking OpenVAS CLI ...
OK: OpenVAS CLI version 1.1.4.SVN.r.

Step 6: Checking Greenbone Security Desktop (GSD) ...
OK: Greenbone Security Desktop is present in Version 1.2.1.

Step 7: Checking if OpenVAS services are up and running ...
OK: netstat found, extended checks of the OpenVAS services enabled.
OK: OpenVAS Scanner is running and listening on all interfaces.
OK: OpenVAS Scanner is listening on port 9391, which is the default port.
ERROR: OpenVAS Manager is NOT running!
FIX: Start OpenVAS Manager (openvasmd).
ERROR: OpenVAS Administrator is NOT running!
FIX: Start OpenVAS Administrator (openvasad).
ERROR: Greenbone Security Assistant is NOT running!
FIX: Start Greenbone Security Assistant (gsad).
```

魔方渗透系统  
NEURO

# Openvas启动服务

- `openvasmd -p 9390 -a 127.0.0.1` //Starting OpenVAS Manager
- `openvasad -a 127.0.0.1 -p 9393` //Starting OpenVAS Administrator
- `gsad --http-only --listen=127.0.0.1 -p 9392`
- //Starting Greenbone Security Assistant
- <http://127.0.0.1:9392>

魔方渗透系统

```
root@magicbox:/pentest/misc/openvas# openvasad -a 127.0.0.1 -p 9393
root@magicbox:/pentest/misc/openvas# openvasmd -p 9390 -a 127.0.0.1
root@magicbox:/pentest/misc/openvas# gsad --http-only --listen=127.0.0.1 -p 9392
root@magicbox:/pentest/misc/openvas#
```

root@magicbox: /pentest/misc/openvas

文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

OK: xsltproc found.

Step 3: Checking OpenVAS Administrator ...

OK: OpenVAS Administrator is present in version 1.1.2.

OK: At least one user exists.

OK: At least one admin user exists.

Step 4: Checking Greenbone Security Assistant (GSA) ...

OK: Greenbone Security Assistant is present in version 2.0.1.

Step 5: Checking OpenVAS CLI ...

OK: OpenVAS CLI version 1.1.4.SVN.r.

Step 6: Checking Greenbone Security Desktop (GSD) ...

OK: Greenbone Security Desktop is present in Version 1.2.1.

Step 7: Checking if OpenVAS services are up and running ...

OK: netstat found, extended checks of the OpenVAS services enabled.

OK: OpenVAS Scanner is running and listening on all interfaces.

OK: OpenVAS Scanner is listening on port 9391, which is the default port.

WARNING: OpenVAS Manager is running and listening only on the local interface. This means that you will not be able to access the  
or OpenVAS CLI.

SUGGEST: Ensure that OpenVAS Manager listens on all interfaces.

OK: OpenVAS Manager is listening on port 9390, which is the default port.

OK: OpenVAS Administrator is running and listening only on the local interface.

OK: OpenVAS Administrator is listening on port 9393, which is the default port.

WARNING: Greenbone Security Assistant is running and listening only on the local interface. This means that you will not be able  
from the outside using a web browser.

SUGGEST: Ensure that Greenbone Security Assistant listens on all interfaces.

OK: Greenbone Security Assistant is listening on port 9392, which is the default port.

Step 8: Checking nmap installation ...

WARNING: Your version of nmap is not fully supported: 6.25

SUGGEST: You should install nmap 5.51.

Step 9: Checking presence of optional tools ...

OK: pdflatex found.

WARNING: PDF generation failed, most likely due to missing LaTeX packages. The PDF report format will not work.

SUGGEST: Install required LaTeX packages.

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 for RPM and DEB based targets will not work.

SUGGEST: Install rpm.

WARNING: Could not find makensis binary, LSC credential package generation for Microsoft Windows targets will not work.

SUGGEST: Install nsis.

It seems like your OpenVAS-4 installation is OK.

魔方渗透系统

NEURON

# Greenbone security desktop

- 登录进去，New Task创建一个新任务。
- Scan Targets设置新任务的扫描目标。



**Log in**

Please enter address and user account for your scan engine.

If you select one of the profiles, you only need to enter the password.

Before you press the log in button you may store the access profile.

Note, that the scan engine must have OMP support enabled for the given port for a successful connection.

**Profile**

neuron

**Serveraddress** **Port**

127.0.0.1 9390  OMP 2.0

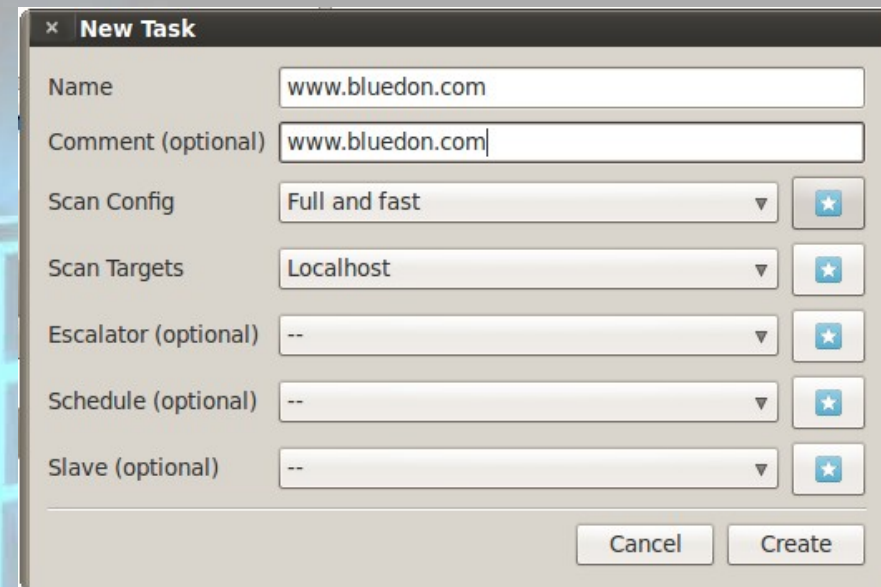
**Username**

akast

**Password**

\*\*\*\*\*


**Log in** **Cancel**





**New Task**


**Name** www.bluedon.com


**Comment (optional)** www.bluedon.com

**Scan Config** Full and fast 

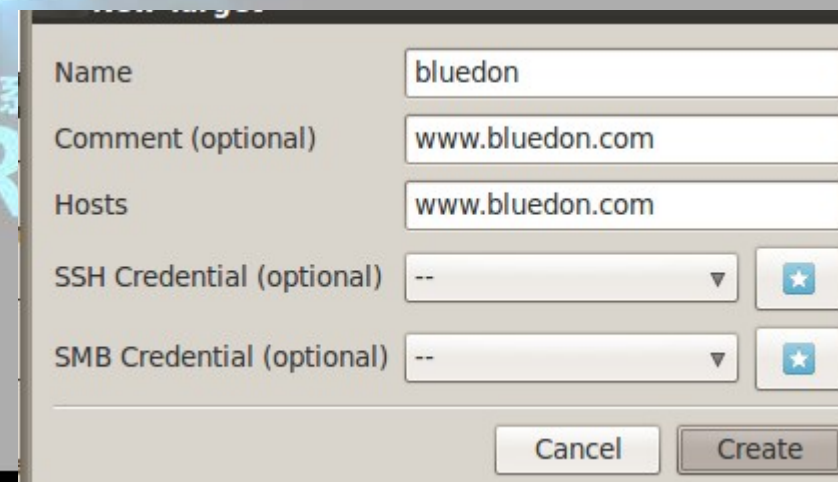
**Scan Targets** Localhost 

**Escalator (optional)** -- 

**Schedule (optional)** -- 

**Slave (optional)** -- 

**Cancel** **Create**





**New Target**

**Name** bluedon

**Comment (optional)** www.bluedon.com

**Hosts** www.bluedon.com

**SSH Credential (optional)** -- 

**SMB Credential (optional)** -- 

**Cancel** **Create**



Refresh Settings

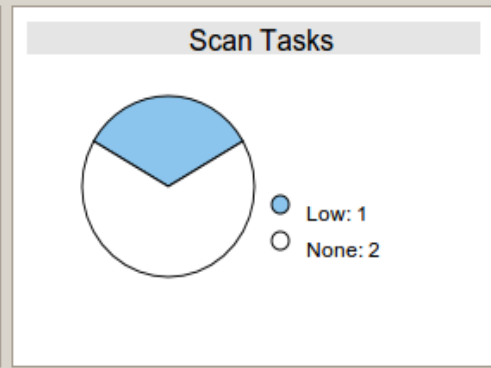
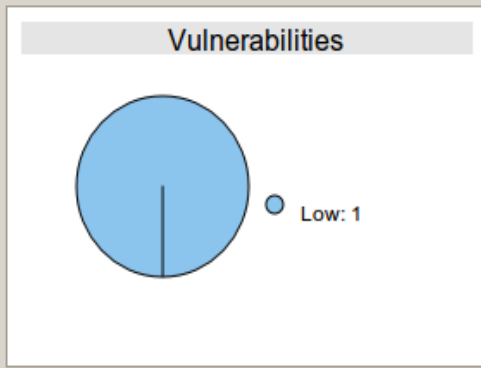


## Dashboard

Refresh Interval:  sec

Apply Interval

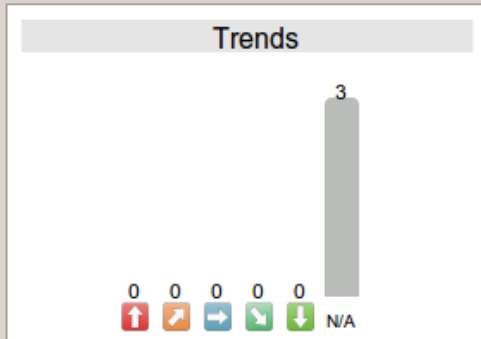
Stop Interval



### Top 5 Tasks

akast test

bluedon



### Task Overview

Total	3
Running	1
Progress	0
Done	1
New	1
Error	0

### Resources Overview

Targets	3
Scan Configs	5
Schedules	0
Escalators	0
Credentials	0
Agents	0
Overrides	0
Notes	0

Next Refresh:

## Tasks

Name	Status	Reports	First	Last	Threat	Trend
akast test	Done	1	Apr 9 2012	Apr 9 2012	Low	
bluedon	20%	0			None	
bluedon ip	New	0				

Task bluedon

Summary Reports Notes Overv

Name: bluedon

Comment: bluedon

Config: Full and fast

Escalator:

Schedule:

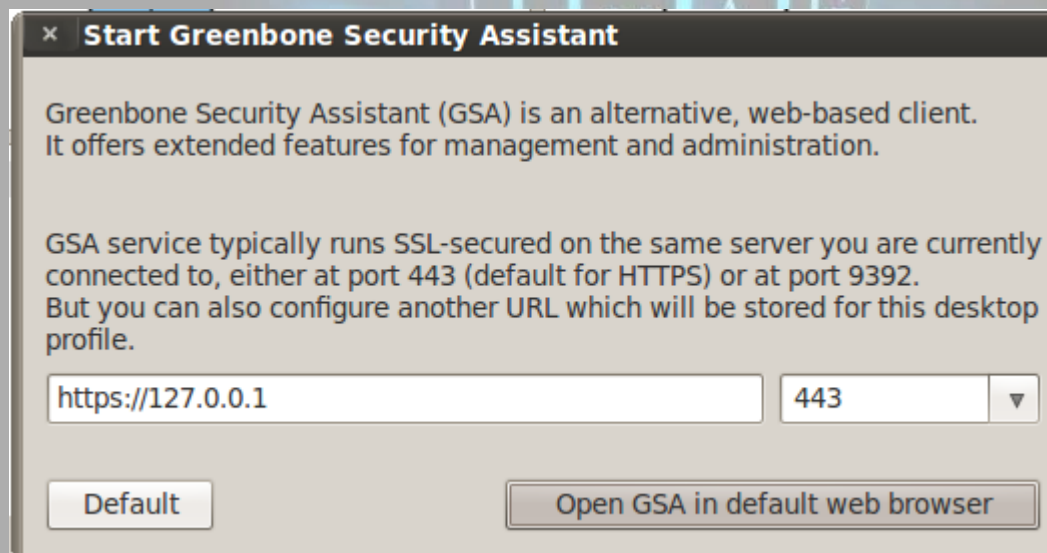
Target: bluedon

Slave:

Status: Running

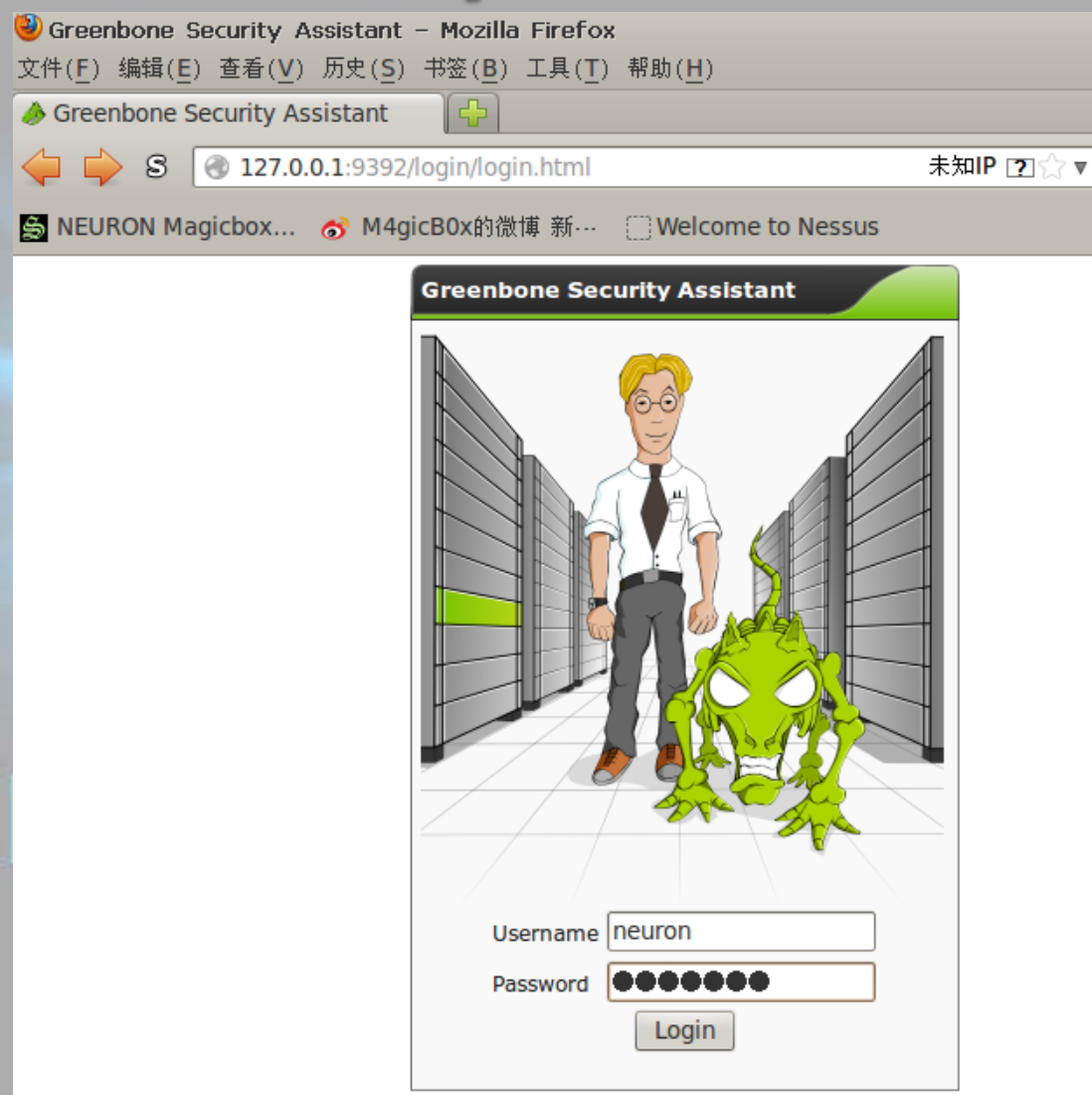
# Greenbone Security Assistant

- web访问界面，直接用浏览器访问 `http://127.0.0.1:9392` 也一样。



# Greenbone Security Assistant

- Web访问方式





**Navigation****Scan Management**

- [Tasks](#)
- [New Task](#)
- [Notes](#)
- [Overrides](#)
- [Performance](#)

**Configuration**

- [Scan Configs](#)
- [Targets](#)
- [Credentials](#)
- [Agents](#)
- [Escalators](#)
- [Schedules](#)
- [Report Formats](#)
- [Slaves](#)

**Administration**

- [Users](#)
- [NVT Feed](#)
- [Settings](#)

**Help**

- [Contents](#)

**Results of last operation**

Operation: Start Task  
Status code: 202  
Status message: OK, request submitted

**Tasks**

vNo auto-refresh

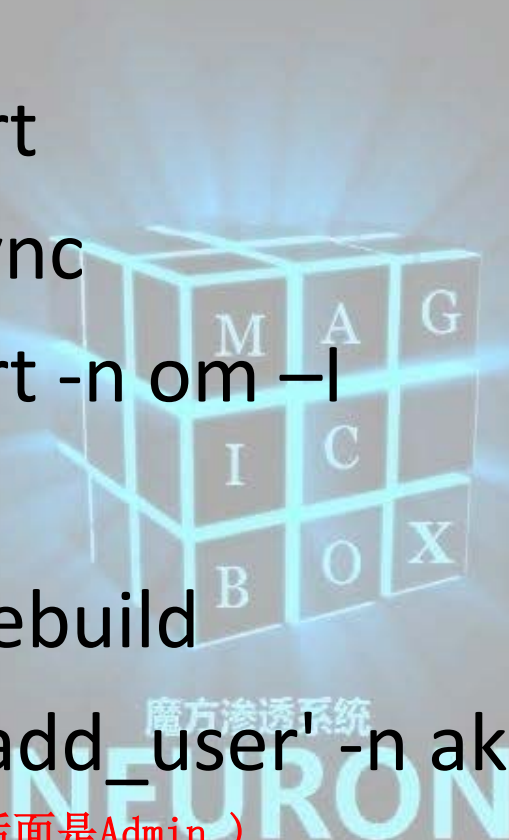
vApply overrides



Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
<b>NEURON</b> (www.ngsst.com)	Requested	0					

# 配置过程

- openvas-mkcert
- openvas-nvt-sync
- openvas-mkcert -n om -l
- openvassd
- openvasmd --rebuild
- openvasad -c 'add\_user' -n akast -r Admin  
(有引号, 区分大小写, -r 后面是Admin)
- openvas-adduser



# 联系

问题反馈、交流

Akast Saint H

QQ群: 74293375

QQ & Email & gtalk: [akast@ngsst.com](mailto:akast@ngsst.com)



魔方渗透系统

NEURON