

Тәжірибелік сабақ – 3

Тақырыбы: OpenVAS – осалдықты анықтау қосымшасы

Сервис Canonical [Launchpad.net](https://launchpad.net) позволяет любому желающему создать репозиторий пакетов для Ubuntu (Personal Package Archive – PPA) и использовать его для распространения своих пакетов без лишних технических трудностей. А пользователи, прописавшие у себя такой репозиторий, смогут получать обновления пакетов из него автоматически.

Здесь мы рассмотрим процесс установки OpenVAS из PPA репозитория [Мохаммада Разави \(Mohammad Razavi\)](#). Этот репозиторий обновляется весьма оперативно, почти сразу после выхода новых версий. В том, что пакеты свежие можно убедиться сравнив версию софта [на официальном сайте](#) и в PPA [репозитории](#).

OpenVAS-8
Libraries 8.0.5
Scanner 5.0.4
Manager 6.0.6
Greenbone Security Assistant (GSA) 6.0.6
Commandline Interface (CLI) 1.4.3
openvas-smb 1.0.1

Package	Version	Uploaded by
 greenbone-security-assistant	6.0.6-3	 Mohammad Razavi (2015-10-19)
 greenbone-security-assistant9	6.1~beta2-1	 Mohammad Razavi (2015-11-03)
 openvas-cli	1.4.3-1	 Mohammad Razavi (2015-10-17)
 openvas-libraries	8.0.5-1	 Mohammad Razavi (2015-09-30)
 openvas-manager	6.0.6-2	 Mohammad Razavi (2015-10-17)
 openvas-scanner	5.0.4-3	 Mohammad Razavi (2015-10-17)
 openvas9-cli	1.4.3-1	 Mohammad Razavi (2015-10-17)
 openvas9-libraries	8.1~beta2-1	 Mohammad Razavi (2015-11-03)
 openvas9-manager	6.1~beta2-1	 Mohammad Razavi (2015-11-03)
 openvas9-scanner	5.1~beta2-1	 Mohammad Razavi (2015-11-03)

1 → 10 of 10 results First • Previous • Next ► • Last

Как видим, на текущий момент все свежее. Нет пакета для openvas-smb, что возможно может сказаться при сканировании windows-систем (а возможно и было учтено при сборке openvas-libraries). Также нет пакетов для OSPd-сканеров, их при необходимости придется устанавливать из исходников.

Для того, чтобы установить OpenVAS из стороннего репозитория Ubuntu необходимо:

1. Подготовить систему с Ubuntu. Мохаммад пишет, что работоспособность пакетов проверялась только для Ubuntu 14.04 LTS (Trusty Tahr). Эта версия Ubuntu будет поддерживаться до апреля 2019 года. Свободного места на жестком диске должно быть не меньше 10 Гб. Сам OpenVAS занимает не много, а security content значительно.

2. Добавить ppa репозиторий Мохаммада Разави
`sudo add-apt-repository ppa:mrazavi/openvas`

```
vmuser@vmuser-VirtualBox: ~
vmuser@vmuser-VirtualBox:~$ sudo add-apt-repository ppa:mrazavi/openvas
[sudo] password for vmuser:
OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Homepage: http://www.openvas.org/

* Openvas 9 (beta 2) is now available *

To install openvas 8, install the "openvas" package from this ppa. It is only tested on ubuntu 14.04 trusty.

You have to update openvas scripts/data after installation with the following commands:

sudo apt-get install sqlite3
sudo openvas-nvt-sync
sudo openvas-scapdata-sync
sudo openvas-certdata-sync

sudo service openvas-scanner restart
```

```
vmuser@vmuser-VirtualBox: ~
ninstall them, you just have to install "openvas9" package instead of "openvas". Then, update scripts/data just like the old packages.

Please note that the default port number of the web interface for the new packages are changed to 4000. So, to access the web interface for version 9, go to https://localhost:4000

You can change the web interface port number by modifying /etc/default/openvas-gsa. Then, restart its service by issuing "sudo service openvas-gsa restart".
More info: https://launchpad.net/~mrazavi/+archive/ubuntu/openvas
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keyring `/tmp/tmpuaip4o0b/secring.gpg' created
gpg: keyring `/tmp/tmpuaip4o0b/pubring.gpg' created
gpg: requesting key 4AA450E0 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpuaip4o0b/trustdb.gpg: trustdb created
gpg: key 4AA450E0: public key "Launchpad PPA for Mohammad Razavi" imported
gpg: Total number processed: 1
gpg:          imported: 1 (RSA: 1)
OK
vmuser@vmuser-VirtualBox:~$
```

1. Обновить информацию по пакетам
`sudo apt-get update`
2. Установить OpenVAS 8
`sudo apt-get install openvas`
udp. Для установки OpenVAS 9 выполните:
`sudo apt-get install openvas9`
Установка и настройка производится автоматически, но в одном месте нужно будет

подтвердить настройку Redis-a.

```
vmuser@vmuser-VirtualBox: ~
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  fonts-lmodern libhiredis0.10 libjemalloc1 libksba8 libmicrohttpd10
  libopenvas8 libptexenc1 libruby1.9.1 libyaml-0-2 lmodern luatex openvas-cli
  openvas-gsa openvas-manager openvas-scanner redis-server redis-tools ruby
  ruby1.9.1 sqlite3 tex-common texlive-base texlive-binaries
  texlive-latex-base texlive-latex-base-doc texlive-luatex xsltproc
Suggested packages:
  xmlstarlet ri ruby-dev ruby1.9.1-examples ri1.9.1 graphviz ruby1.9.1-dev
  ruby-switch sqlite3-doc debhelper perl-tk
The following NEW packages will be installed:
  fonts-lmodern libhiredis0.10 libjemalloc1 libksba8 libmicrohttpd10
  libopenvas8 libptexenc1 libruby1.9.1 libyaml-0-2 lmodern luatex openvas
  openvas-cli openvas-gsa openvas-manager openvas-scanner redis-server
  redis-tools ruby ruby1.9.1 sqlite3 tex-common texlive-base texlive-binaries
  texlive-latex-base texlive-latex-base-doc texlive-luatex xsltproc
0 upgraded, 28 newly installed, 0 to remove and 205 not upgraded.
Need to get 93,1 MB of archives.
After this operation, 207 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
vmuser@vmuser-VirtualBox: ~
Package configuration

Configuring openvas-scanner

Openvas scanner require redis database to store data. It will connect to
the database with a unix socket at /var/run/redis/redis.sock.

If you select yes, the installation process will enable redis unix
socket at this address automatically, by updateing
/etc/redis/redis.conf.

If you select no, you have to manually update your
/etc/redis/redis.conf.

Do you want to enable redis unix socket on /var/run/redis/redis.sock?

<Yes> <No>
```

1. Далее нужно будет обновить security content:
sudo openvas-nvt-sync
sudo openvas-scapdata-sync
sudo openvas-certdata-sync
2. И наконец перезапустить OpenVAS:
sudo service openvas-scanner restart
sudo service openvas-manager restart
sudo openvasmd -rebuild -progress

Все, можно пользоваться. Заходим на <https://localhost:443>, логин "admin", пароль "admin"

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant

Logged in as Admin admin | Logout
Sat Dec 5 23:59:52 2015 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Tasks (total: 0) No auto-refresh

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

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			

(Applied filter: apply_overrides=1 rows=10 first=1 sort=name) (total: 0)

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
I will appear automatically in areas where you have created no or only a few objects. And disappear when you have

Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration