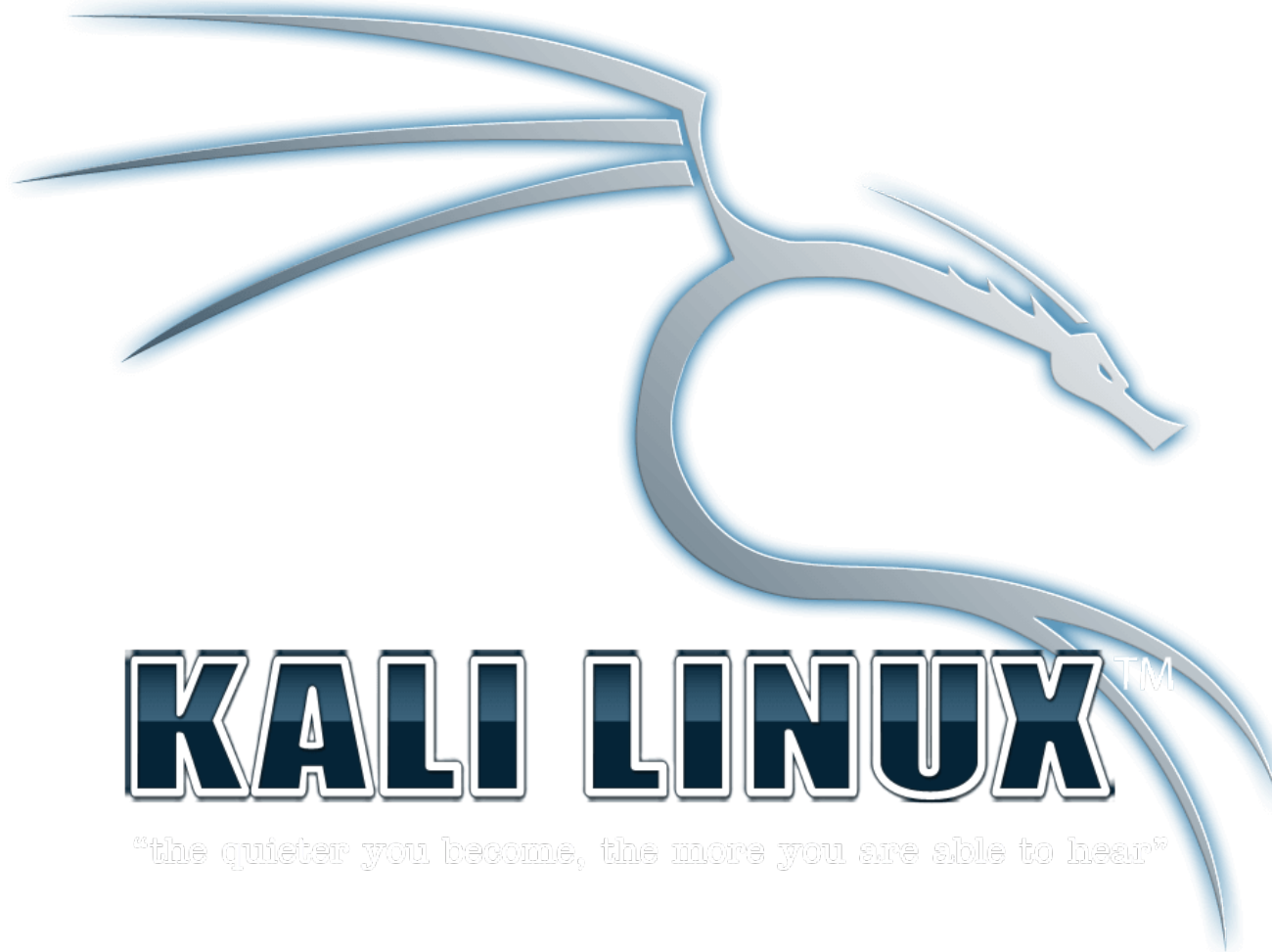


# Pentest com Kali Linux





**Instrutor: Vitor Mazuco**

**<http://facebook.com/vitormazuco>**

**Email: [vitor.mazuco@gmail.com](mailto:vitor.mazuco@gmail.com)**

**WebSite: <http://vmzsolutions.com.br>**



## Instalando e configurando um OpenVas

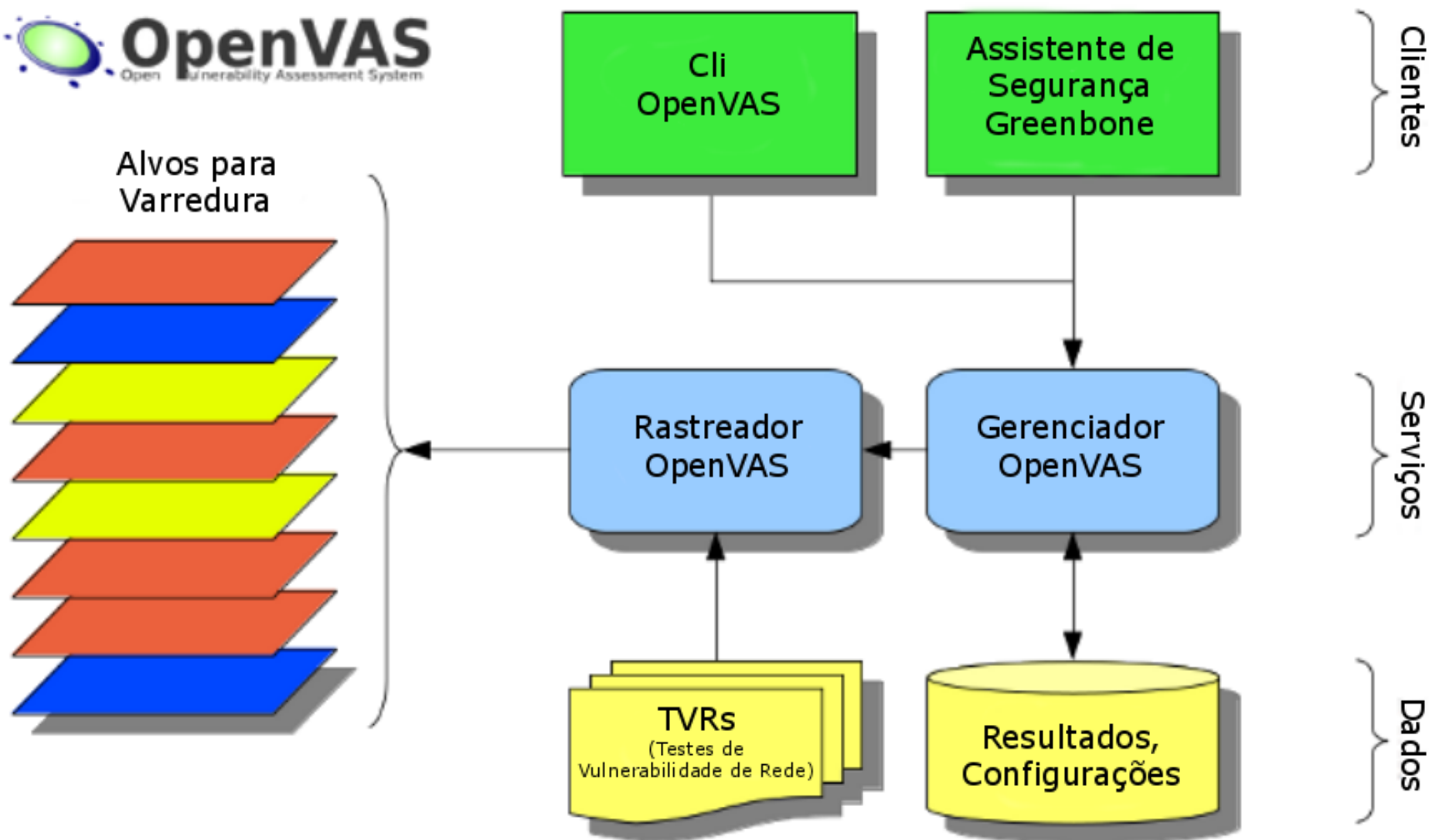
O OpenVAS, o Sistema de Avaliação de Vulnerabilidade, é um excelente estrutura que pode ser usada para avaliar as vulnerabilidades de nosso alvo. É um *fork* do projeto Nessus. Ao contrário de Nessus, o OpenVAS oferece aos seus usuários recursos totalmente gratuitos. Vamos instalar e configurar ele, mas antes vamos ver um pouco como ele roda.



## Instalando e configurando um OpenVas

O núcleo de sua arquitetura orientada a serviços com segurança SSL é o **Rastreador OpenVAS** (OpenVAS Scanner). O rastreador executa os Testes de Vulnerabilidade de Rede (TVRs) reais que são servidos com atualizações diárias, fornecidas pelo Feed NVT(Network Vulnerability Tests) OpenVAS ou através de um serviço de feed comercial.

# Instalando e configurando um OpenVas





## Instalando e configurando um OpenVas

O **Gerenciador OpenVAS** é o serviço central que consolida a varredura de vulnerabilidade em uma solução completa de gerenciamento de vulnerabilidade. O gerenciador controla o Rastreador através do OTP (OpenVAS Transfer Protocol ou Protocolo de Transferência OpenVAS) e por si só oferece o OMP (OpenaVAS Management Protocol ou Protocolo de Gerenciamento OpenVAS), um protocolo sem estado baseado em XML.



## Instalando e configurando um OpenVas

Toda a inteligência é implementada no Gerenciador, desta forma é possível implementar vários "pequenos clientes" que irão comportar-se consistentemente, como por exemplo, no que diz respeito à filtragem ou a classificação de resultados da verificação.



## Instalando e configurando um OpenVas

Vamos fazer a instalação do OpenVas com comando:

**\*(processos extremamente longos)\***

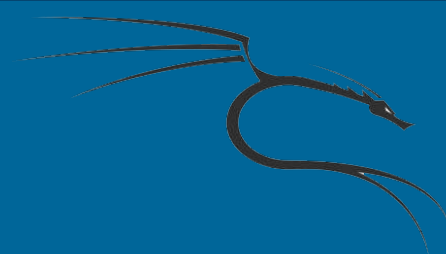
```
# apt-get install openvas
```

E depois faça a configuração e receba ao final a senha de admin

```
# openvas-setup
```



# Instalando e configurando um OpenVas



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# openvas-setup
/var/lib/openvas/private/CA created
/var/lib/openvas/CA created

[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: /var/lib/openvas/plugins
[w] Could not determine feed version.
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.V3pYxSaYIL/openvas-feed-2016-04-28-22922.tar.bz2
--2016-04-28 16:31:41-- http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org)... 5.9.98.186
Connecting to www.openvas.org (www.openvas.org)|5.9.98.186|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25475644 (24M) [application/x-bzip2]
Saving to: '/tmp/openvas-nvt-sync.V3pYxSaYIL/openvas-feed-2016-04-28-22922.tar.bz2'

s-nvt-sync.V3pYxSaYIL/openv  10%[==>]      2.46M   557KB/s   eta 47s
vt-sync.V3pYxSaYIL/openvas  11%[==>]      2.75M   574KB/s   eta 47s
feed-2016-04-28-22922.tar.  34%[=====>]    8.32M   821KB/s   eta 25s
```



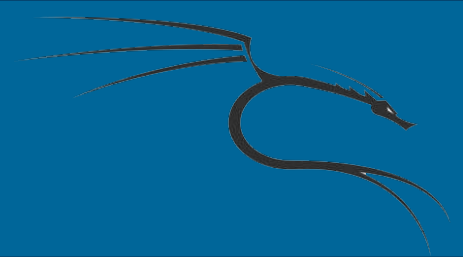
## Instalando e configurando um OpenVas

Os últimos comandos é a configuração do OpenVAS e a sincronização com a NVT. Dependendo da sua velocidade de conexão isso pode demorar um pouco para terminar.

Quando o processo de instalação estiver concluído, você será apresentada uma senha longa na última linha do terminal. Esta senha é usada para acessar a interface web OpenVAS então você precisa salvá-lo em algum lugar e alterá-lo após o primeiro login.



# Instalando e configurando um OpenVas



```
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) []:Com
mon Name (eg, your name or your server's hostname) []:Email Address []:Using configuration from /tmp/openvas-
s-mkcert-client.16383/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'DE'
localityName            :ASN.1 12:'Berlin'
commonName              :ASN.1 12:'om'
Certificate is to be certified until Apr 28 14:55:58 2017 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
Rebuilding NVT cache... done.
User created with password '33a48890-7250-449c-84f7-1ccea2ae14c'.
root@kali:~#
```



## Instalando e configurando um OpenVas

Quando o processo de configuração OpenVAS está finalizado, o OpenVAS gera, scaneia os serviços que estão escutando na porta 9390, 9391, 9392 e na porta 80 respectivamente. Você pode usar o seguinte comando do *netstat* para verificar se estes serviços estão ouvindo:

```
# netstat -antp
```



# Instalando e configurando um OpenVas

```
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:9390          0.0.0.0:*                LISTEN      16612/openvasmd
tcp        0      0 127.0.0.1:9391          0.0.0.0:*                LISTEN      16576/openvassd: Re
tcp        0      0 0.0.0.0:111             0.0.0.0:*                LISTEN      2627/rpcbind
tcp        0      0 127.0.0.1:80            0.0.0.0:*                LISTEN      16624/gsad
tcp        0      0 127.0.0.1:9392          0.0.0.0:*                LISTEN      16618/gsad
tcp        0      0 127.0.0.1:5432          0.0.0.0:*                LISTEN      3389/postgres
tcp6       0      0 :::111                  :::*                    LISTEN      2627/rpcbind
tcp6       0      0 :::1:5432               :::*                    LISTEN      3389/postgres
root@kali:~# openvas-start
Starting OpenVas Services
```



## Instalando e configurando um OpenVas


Caso contrário, execute o OpenVas com o comando:

```
# openvas-start
```

Conecte-se ao navegador com o endereço abaixo:

<http://127.0.0.1:9392>

# Instalando e configurando um OpenVas

 **Greenbone**  
Security Assistant

Logged in as Admin **admin** | Logout  
Mon Sep 26 14:51:12 2016 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks (total: 0) ? ✖ ⭐ ⌵ ⬇ vNo auto-refresh ↻

Filter:

apply\_overrides=1 rows=10 first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			

vApply to page contents ↻


(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 more than 3 objects. You can call me with this icon ✖ any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.



**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
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 default Port List, Alert,