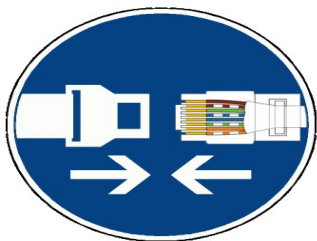


[www.seguridadpyme.es](http://www.seguridadpyme.es)

*ASISTENCIA TÉCNICA A LA SEGURIDAD INFORMÁTICA EN PYMES*

# *MANUAL OPEN VAS*

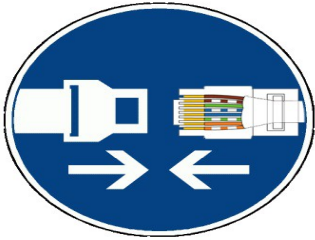


www.seguridadpyme.es

## Manual de Usuario para Open Vas

*OpenVAS es el acrónimo de Open Vulnerability Assessment System, un subsistema que opera dentro de la red para evaluar los riesgos de seguridad de los equipos en la organización y permitir cerrar sus vulnerabilidades anticipadamente. Posee una interfaz gráfica modo de cliente y el corazón de openVAS es un server con un set de pruebas de vulnerabilidades para detectar problemas de seguridad en sistema remotos y aplicaciones.*

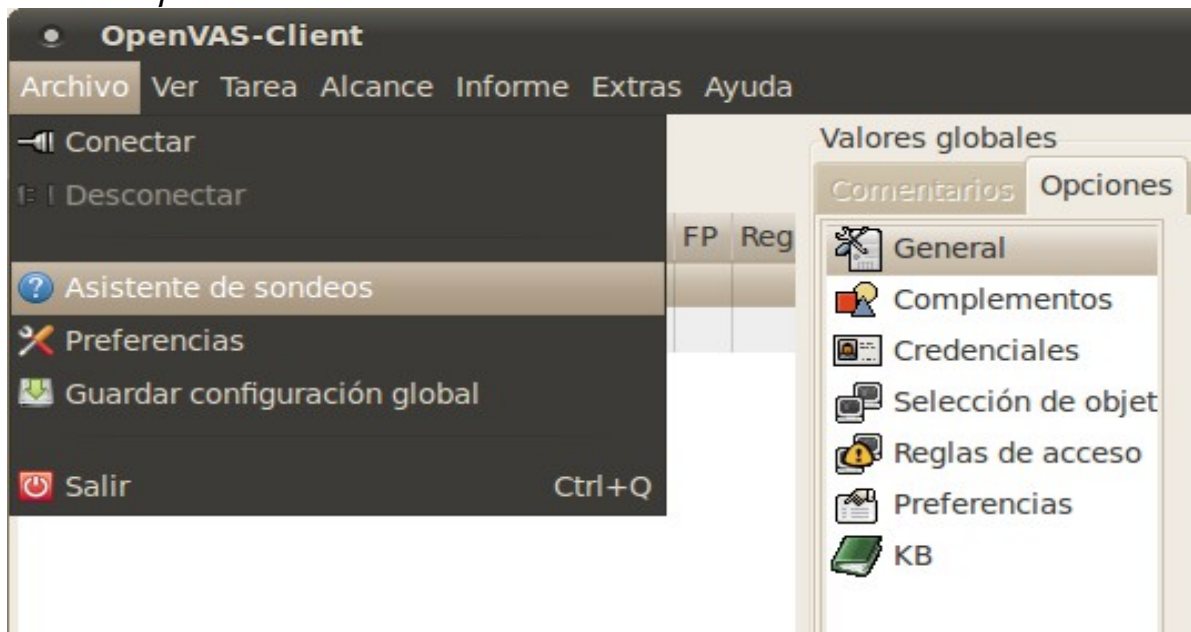
- 1. Algunas de las herramientas que utiliza durante sus revisiones se derivan de John-the-Ripper, Chkrootkit, LSOE, ClamAV, Tripwire y otras más. Esta basado en una arquitectura Cliente-Servidor. La parte de servidor tendrá que ser implementada en un sistema Linux, mientras que la parte del cliente podrá ser descargada para algunas versiones de Linux así como también para Windows XP.*
- 2. Para instalarlo desde la consola en un sistema Ubuntu/Melinux usaremos los siguientes comandos:*
  - `sudo apt-get install openvas-server openvas-client`*
  - `sudo /etc/init.d/openvas-server start`*
- 3. Creamos un usuario usando:*
  - `sudo openvas-adduser`*
- 4. Entraremos en el proceso interactivo para crear un usuario que nos preguntara el nombre de usuario, tipo de autenticación, password y finalmente las reglas de permisos (introduciremos CTRL+D)*
  - `Using /var/tmp as a temporary file holder.Add a new openvasd user`*  
-----
  - `Login : prueba`*
  - `Authentication (pass/cert) [pass] : pass`*
  - `Login password :`*
  - `Login password (again) :`*
  - `Add rules:`*

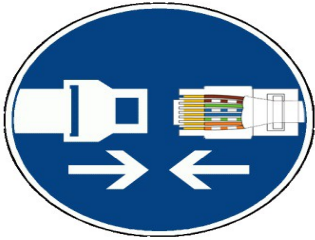


[www.seguridadpyme.es](http://www.seguridadpyme.es)

- *openvasd has a rules system which allows you to restrict the hosts that prueba has the right.*
- *For instance, you may want him to be able to scan his own host only.*
- *Please see the openvas-adduser man page for the rules syntax.*
- *Enter the rules for this user, and hit ctrl-D once you are done:*
- *(the user can have an empty rules set)*
- *Login : prueba*
- *Password : \*\*\*\*\**
- *Rules :*
- *Is that ok? (y/n) [y] y*
- *user added.*

5. *Cuando la instalación finalice iremos al menú Aplicaciones / Internet / OpenVAS-Cliente y cuando la aplicación se abra iremos al menú Archivo / Asistente de Sondeos .*





www.seguridadpyme.es

6. *Introducimos el nombre para la tarea de escaneo.*

**Asistente de sondeos**

Paso 1: Tarea Paso 2: Ámbito Paso 3: Objetivos Paso 4: Ejecutar

Las tareas describen lo que desea hacer. Puede utilizarlas para agrupar de forma lógica su trabajo por asunto, frecuencia, ubicación o cualquier otra cosa.  
Algunos nombres posibles de tareas serían:  
- Pruebas semanales  
- Cliente XYZ  
- Sistemas del proyecto ABC  
También debería introducir un comentario que describa mejor la tarea.

Introduzca un nombre para su tarea:

Comentario:

Atrás Cancelar Adelante

7. *Introducimos un nombre para el ámbito.*

**Asistente de sondeos**

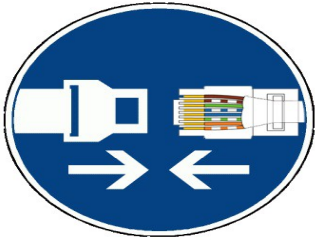
Paso 1: Tarea Paso 2: Ámbito Paso 3: Objetivos Paso 4: Ejecutar

Los ámbitos son parte de una tarea. Cada ámbito define una conexión a un servidor OpenVAS y una lista de sistemas a probar.  
Algunos nombres de posibles ámbitos son:  
- Servidores de Internet (p.ej. dentro de «Pruebas semanales») - Servidores de aplicación (p.ej. dentro de «Cliente XYZ») - Estaciones de trabajo (p.ej. dentro de «Sistemas del proyecto ABC») Debería también introducir un comentario que describa mejor el ámbito.

Introduzca un nombre para el ámbito:

Comentario:

Atrás Cancelar Adelante



www.seguridadpyme.es

8. *Introducimos la IP o la red que queremos analizar.*

**Asistente de sondeos**

Paso 1: Tarea Paso 2: Ámbito Paso 3: Objetivos Paso 4: Ejecutar

Los objetivos son los equipos y redes que desea analizar dentro de un ámbito. Pueden introducirse en los siguientes formatos:

- nombre simple de equipo (para sistemas en su LAN)
- nombre totalmente cualificado (p.ej. www.ejemplo.com)
- dirección IP (p.ej. 192.168.0.1)
- red IP (p.ej. 192.168.0.0/24 o 192.168.0.0/255.255.255.0)

Puede introducir más de un objetivo separándolos con comas.

Introduzca los objetivos a analizar:

localhost

Aviso: ¡Asegúrese de que está autorizado a analizar estos sistemas! Las pruebas dañinas se deshabilitan por omisión, pero algunos equipos y especialmente los servidores de impresoras tienen errores que hará que se desconecten. Piense en obtener un permiso por escrito antes de analizar servidores importantes que estén en producción.

Atrás Cancelar Adelante

9. *Pulsamos "Ejecutar".*

- *Nos pedirá usuario y contraseña para conectarnos al openVAS Server. Introducimos el usuario y contraseña que creamos al comienzo y Pulsamos "Aceptar".*

**Conectado al servidor OpenVAS**

Servidor OpenVAS

Sistema: localhost Puerto: 9390 Omisión

Autenticación

Usuario: prueba

Contraseña: ●●●●●●●●

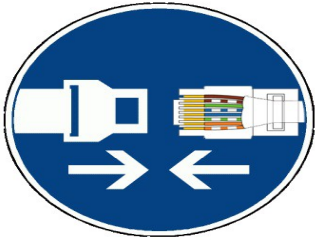
Autenticación por certificado

CA de confianza: cacert.pem Seleccionando...

Utilizar fichero de certificado: Seleccionando...

Utilizar clave en fichero: Seleccionando...

Cancelar Aceptar



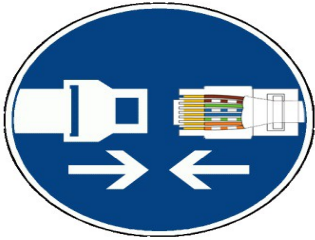
www.seguridadpyme.es

10. Pulsamos OK dejando el "checkbox default".



11. Finalmente comienza el escaneo.





www.seguridadpyme.es

## 12. Una vez que termine el escaneo podremos analizar el informe generado.

OpenVAS-Client  
Informe para el ámbito: localhost (Tarea: Red Local)

Nombre	Alto	Medio	Baja
Valores globales			
Red Local			
localhost			

Report 20100517-000128 0 3

Sistema/Puerto/Criticidad

- localhost
- http (80/tcp)
- Security Warning
- Security Note
- ntp (9390/tcp)
- ndmp (10000/tcp)
- mysql (3306/tcp)
- ipp (631/tcp)
- general/tcp
- ssh (22/tcp)
- general/SMBClient

Reportado por NVT "/doc directory browsable?" (1.3.6.1.4.1.25623.1.0.10056):

The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important -

Solution : Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:

```
<Directory /usr/doc>
AllowOverride None
order deny,allow
deny from all
allow from localhost
</Directory>
```

Risk factor : High  
CVE : CVE-1999-0678  
BID : 318

Reportado por NVT "Apache /server-status accessible" (1.3.6.1.4.1.25623.1.0.10677):

Requesting the URI /server-status gives information about the currently running Apache.

Risk factor : Low  
Solution : If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine.

Reportado por NVT "phpinfo.php" (1.3.6.1.4.1.25623.1.0.11229):

The following files are calling the function phpinfo() which disclose potentially sensitive information to the remote attacker :

```
/info.php
/info/phpinfo.php
/info/info.php
```

Solution : Delete them or restrict access to them  
Risk factor : Low

El análisis tuvo lugar de Sun May 16 23:46:13 2010 a Mon May 17 00:01:28 2010

no conectado

Enlace: <http://www.technoblog.com.ar/>