OpenVas

OpenVAS es un sistema de analisis de vulnerabilidades y un escáner de seguridad de red.

Posee una interfaz gráfica a modo de cliente y el corazón de openVAS es un servidor con un conjunto de pruebas de vulnerabilidades para detectar problemas de seguridad en sistema remotos y aplicaciones

Para instalarlo en Linux-BackTrack se necesitan los siguientes pasos...

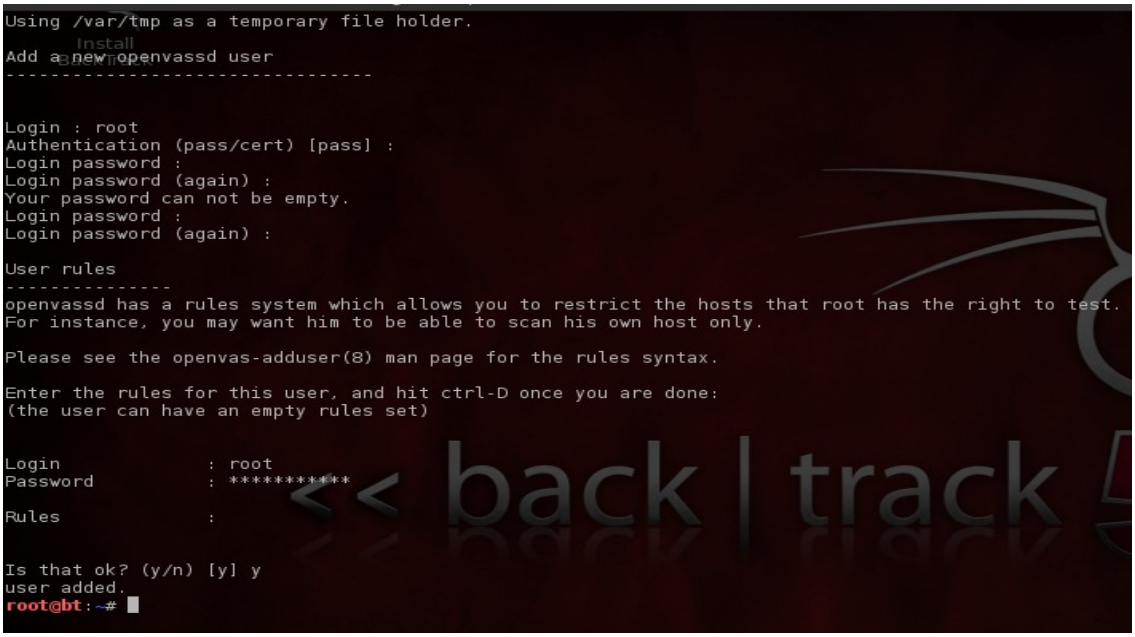
1. La manera más sencilla para instalar todos los componentes necesarios de OpenVas es mediante comandos en consola de la siguiente manera:

#apt-get update
#apt-get install openvas

2. Una vez instalado, todas la entradas se encontraran localizadas en el menú de Backtrack->Vulnerability Assessment->Vulnerability Sacanners->OpenVas.

3. Luego se debe realizar una configuración del OpenVas.

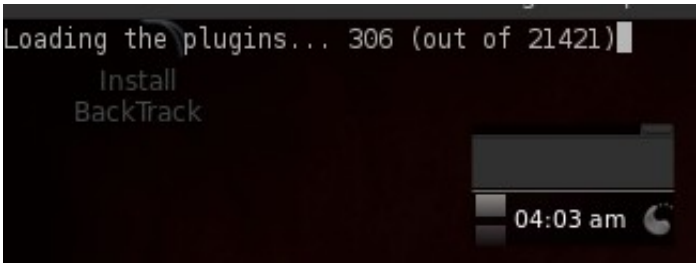
4. En el menú, seleccione OpenVAS Adduser y siga las instrucciones. Ingrese su login y pass para añadir su nuevo usuario.

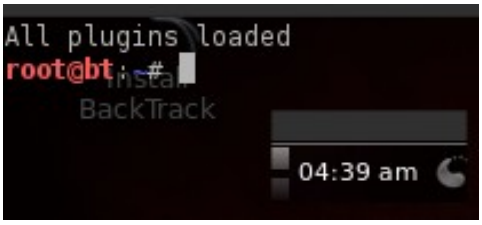


5. Luego se debe crear el certificado, en el menú, seleccione OpenVAS mkcert y siga las instrucciones; aquí se creará el certificado SSL autofirmado.

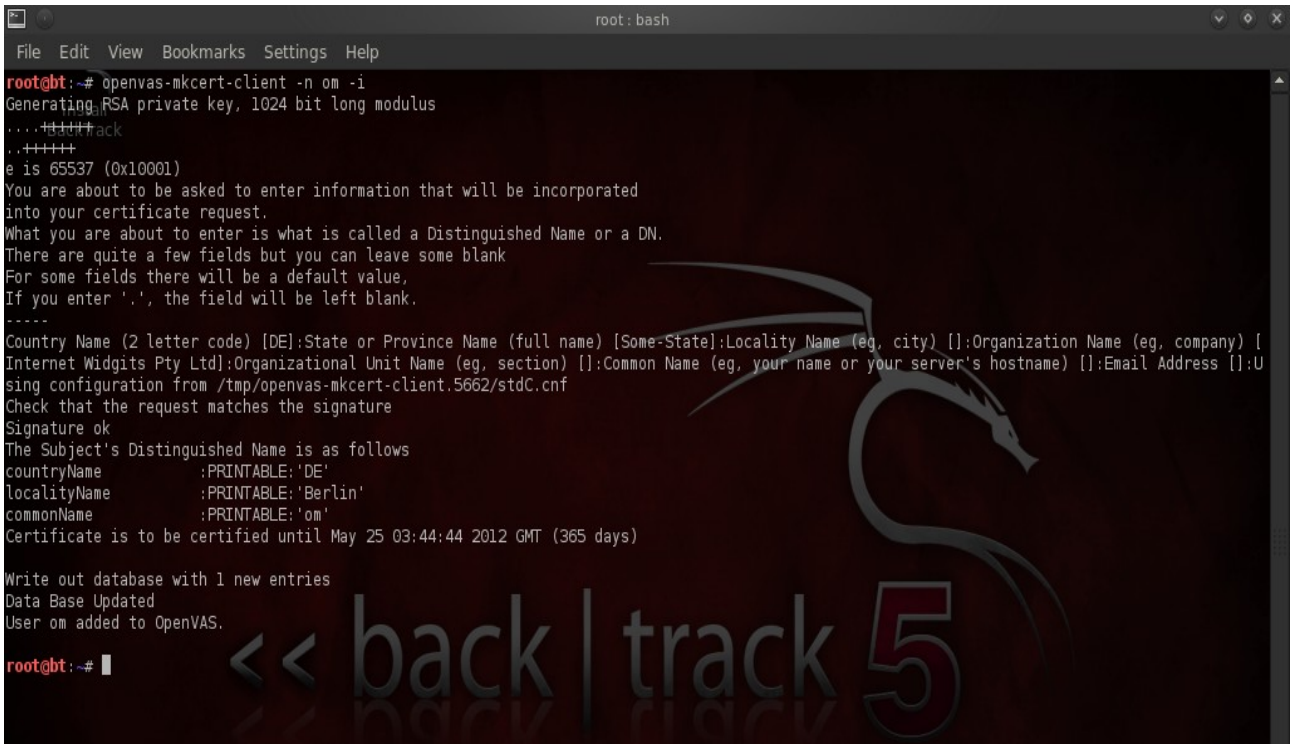
6.Selecciones OpenVas NVT Sync en donde se buscarán las series más recientes, estos son los que el analizador usa para detectar las vulnerabilidades en lo que va a escanear, por lo tanto, se deben actualizar regularmente.

7. Se debe colocar el escáner en marcha, por lo que ingresamos a Start OpenVas Scanner, puede que la primera vez tome su tiempo para comprobar y cargar el nuevo NVT que descargo en el paso anterior.





8. Creamos la configuración del gerente, y el primer paso es un certificado de cliente para el gestor OpenVas que se crea mediante el comando: openvas-mkcert-client -n om -i

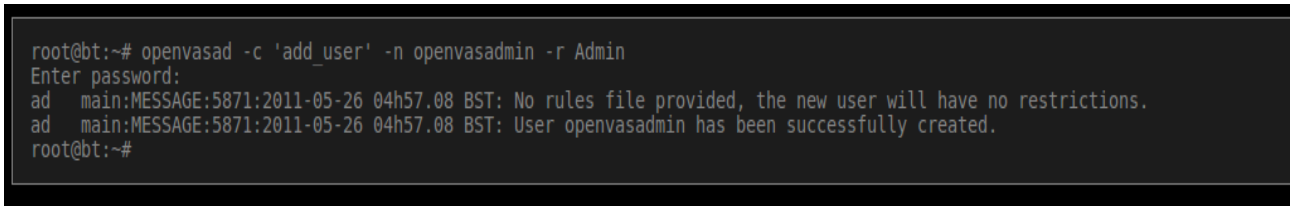


9. Ahora tenemos que reconstruir la base de datos, ya que ahora está fuera de fecha con el agregado de nvt y que de otra manera sería obtener errores sobre la base de datos. Usted debe hacer esto cada vez que actualice el de NVT. Utilizando el comando.

openvasmd --rebuild

10. Ahora debemos crear un usuario de administrador qu se utilizará para realizar todas las evaluaciones, esto se realiza mediante el siguiente comando:

openvas -c 'add_user' -n NOMBRE -r Admin.



Asegúrese de que puede recordar este nombre de usuario y la contraseña asociada, ya que lo necesitará cuando ejecute openvas.

11. Ahora debes iniciar el Administrador de OpenVAS. Como se está corriendo desde mi máquina local que va a utilizar para ejecutar en localhost y, en este caso, el puerto por defecto. Utilizando el siguiente comando.

openvasmd -p 9390 -a 127.0.0.1

12. Se debe iniciar el Administrador de OpenVAS. Esto se hace mediante la ejecución del siguiente comando.

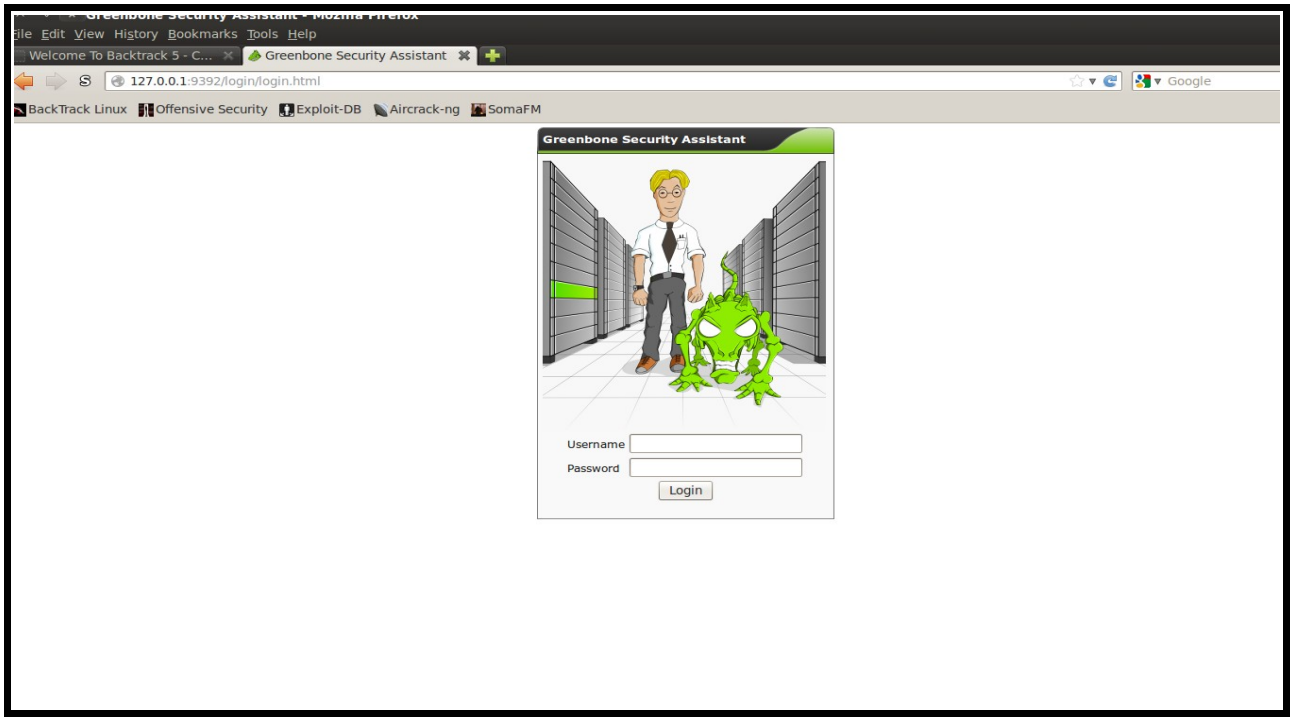
openvasad -a 127.0.0.1 -p 9393

13. A partir de Greenbone Asistente de Seguridad se ejecutará mediante el siguiente comando.

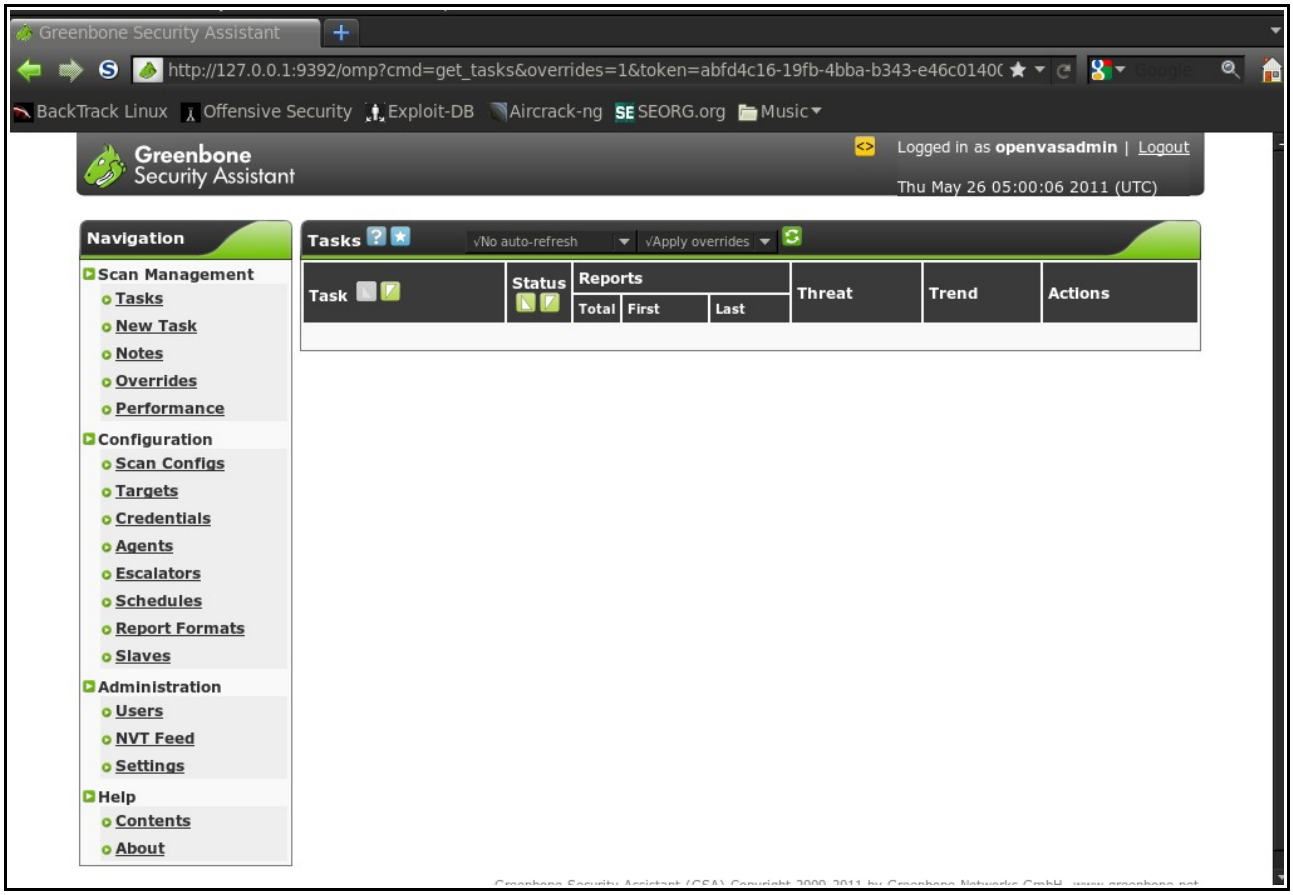
gsad --http-only --listen=127.0.0.1 -p 9392

En este punto de la instalación está prácticamente completa, ahora sólo queda utilizar y manejar nuestro sistema de análisis.

14. Ahora tenemos que iniciar una aplicación para que pueda comunicarse con el escáner mediante el Greenbone seguridad de escritorio. Inicie esto desde la opción de menú y rellenar los datos y detalles que hemos creado anteriormente, a continuación, haga clic en el botón de inicio de sesión.



De esta manera hemos iniciado la sesión y está listo para trabajar.



FUENTE:
http://www.backtrack-linux.org/wiki/index.php/OpenVas