Webinar Gratuito
OpenVAS

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 2 de Enero del 2014

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
- @Alonso_ReYDeS
- pe.linkedin.com/in/alonsocaballeroquezada/

Evaluación de Vulnerabilidades

Es el proceso de ubicar y reportar las vulnerabilidades. Esto proporcionar una manera de detectar y resolver los problemas de seguridad ante de que alguien o algo pueda explotarla.

La razón de realizar este procedimiento es debido a que es un componente crítico la infraestructura de seguridad de varias organizaciones; pues la habilidad de realizar una instantánea de la seguridad de toda la red que apoya a un número de procesos de seguridad y administrativos.

Cuando se descubre una nueva vulnerabilidad, se puede realizar una evaluación para descubrir los sistemas vulnerables, iniciar el proceso de la instalación de parches. Después de esto, se debe realizar otra evaluación para verificar que las vulnerabilidades se han solucionado.

Este ciclo de evaluar, parchar y verificar se ha convertido en un método estándar; para manejar los temas de seguridad; en varias organizaciones.

Tipos de Evaluaciones

1. Evaluaciones de Host

Estas herramientas requieren que el software sea instalado en cada sistema que se desea evaluar. Se evalúa vulnerabilidades a nivel del sistema como permisos de archivos inseguros, parches de software que faltan, políticas de seguridad que cumplen las normas, e instalaciones de puertas traseras o troyanos.

2. Evaluaciones de Red

Implica localizar a todos los sistemas funcionando en la red, determinar los servicios de red utilizados, y analizarlos por probables vulnerabilidades. Este tipo de evaluaciones pueden ser escalables y eficientes en términos de requerimientos administrativos, y son el único método factible para estimar la seguridad de grandes y complejas redes de sistemas heterogeneos.

El Proceso de Evaluación

Sin importar en gran medida cual es la solución utilizada para la evaluación de vulnerabilidades, es muy probable que se realice el mismo proceso de evaluación.

1. Detectar los Sistemas en Funcionamiento
2. Identificar los Sistemas en Funcionamiento
3. Enumerar los Servicios
4. Identificar los Servicios
5. Identificar las Aplicaciones
6. Identificar las Vulnerabilidades
7. Reportar las Vulnerabilidades

Dos Enfoques

1. Enfoque Administrativo

Realiza una evaluación desde la perspectiva de un administrador del sistema autenticado. Se debe proporcionar a la herramienta un usuario y contraseña con estos privilegios. Estas credenciales se utilizarán para detectar parches ausentes, configuraciones inseguras y probables vulnerabilidades en el software del cliente (Como un cliente de correo o un navegador web.)

2. Enfoque Externo

Toma la perspectiva de un intruso malicioso sin autenticación quien intenta irrumpir en la red. Este procedimiento es capaz de tomar decisiones sobre la seguridad del sistema únicamente mediante una combinación de huellas de la aplicación, identificación de versiones, e intentos de explotación. De esta manera se pueden detectar vulnerabilidades en un amplio rango de sistemas operativos y dispositivos.

¿Qué es OpenVAS?

OpenVAS (Sistema Abierto para la Evaluación de Vulnerabilidades) está constituido por varios servicios y herramientas que proporcionan un escaneo de vulnerabilidades muy completo y poderoso, además de una solución para la administración de vulnerabilidades.

El corazón de esta arquitectura asegurada con SSL orientada al servicio, es el Escaner OpenVAS. El muy eficiente escaner ejecuta los NVTs – Network Vulnerability Tests (Pruebas de Vulnerabilidad en Redes), los cuales son servidos con actualizaciones diarás mediante el OpenVAS NVT Feed o mediate el servicio comercial, con más de 30,000 en total.

Todos los productos OpenVAS son Software Libre. Y la mayoría de componentes tienen licencia GNU/GPL.

* OpenVAS: http://www.openvas.org/about.html

Características de OpenVAS

OpenVAS Scanner: Escano de varios objetivos concurrentemente, OpenVAS Transfer Protocol, Soporte SSL.

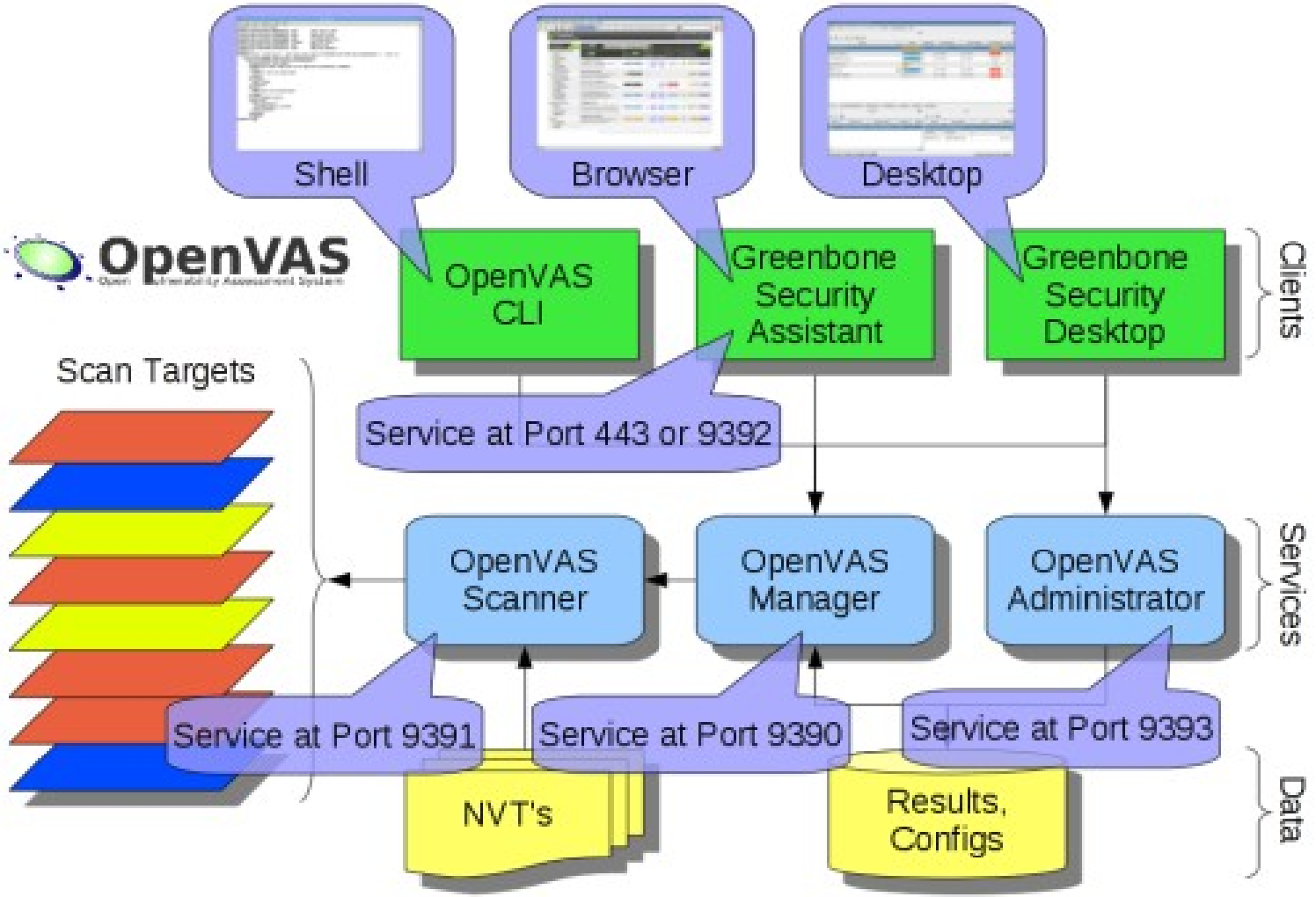
OpenVAS Manager: OpenVAS Management Protocol, Base de Datos SQL (sqlite) para las configuraciones y resultados, Tareas de escaneo concurrentes, Escaneos programados, Reportes en varios formatos (XML, HTML, etc.)

OpenVAS Administrator: OpenVAS Administration Protocol, Manejo de usuarios, Vista del estado del “feed”, sincronización del feed.

Greenbone Security Assistant: Cliente para OMP y OAP, HTTp y HTTPS, Servidor web propio (microhttpd), no se requiere un servidor web adicional, Sistema de ayuda integrado en línea.

* Features Overview: http://www.openvas.org/software.html#feature_overview

Resumen de la Arquitectura de OpenVAS



El Manejador de OpenVAS

Es el servicio central que consolida el escaneo de vulnerabilidades en una solución completa para la gestión de vulnerabilidades.

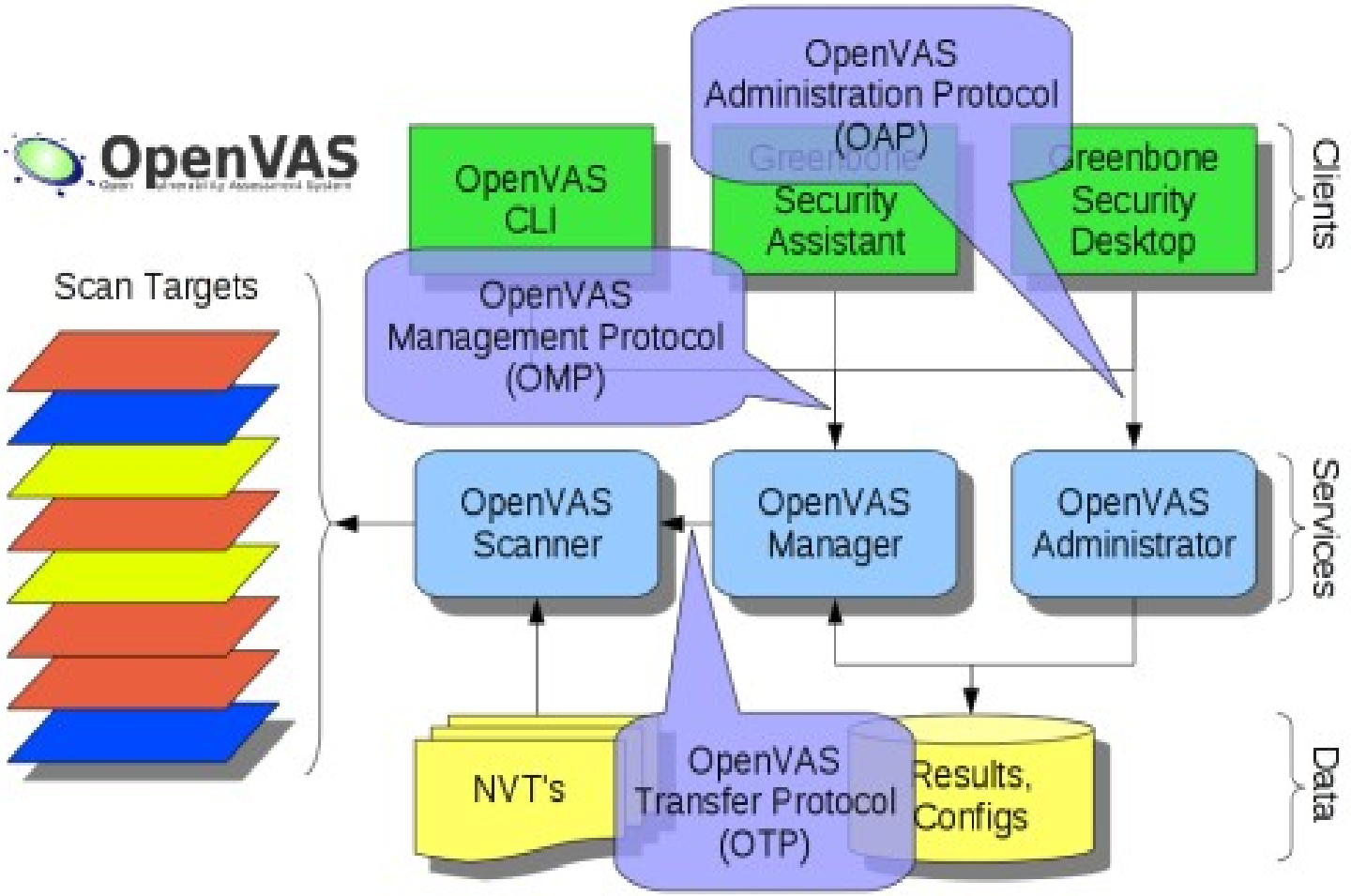
El Manejador controla el Escaner mediante OTP - OpenVAS Transfer Protocol (Protocolo OpenVAS de Transferencia) y ofrece por si mismo OMP - OpenVAS Management Protocol (Protocolo de Gestión OpenVAS) basado en XML.

Toda la inteligencia es implementada en el Manejador, así que es posible implementar varios tipos de clientes con un comportamiento similar, por ejemplo con relación al filtrado y ordenamiento de los resultados del escaneo.

El Manejador también controla una base de datos SQL (basada en sqlite) donde se almacenan centralizadamente toda la configuración y resultados del escaneo.

* http://www.openvas.org/software.html

El Manejador de OpenVAS (Cont.)



Clientes OpenVAS

OpenVAS dispone de diferentes clientes

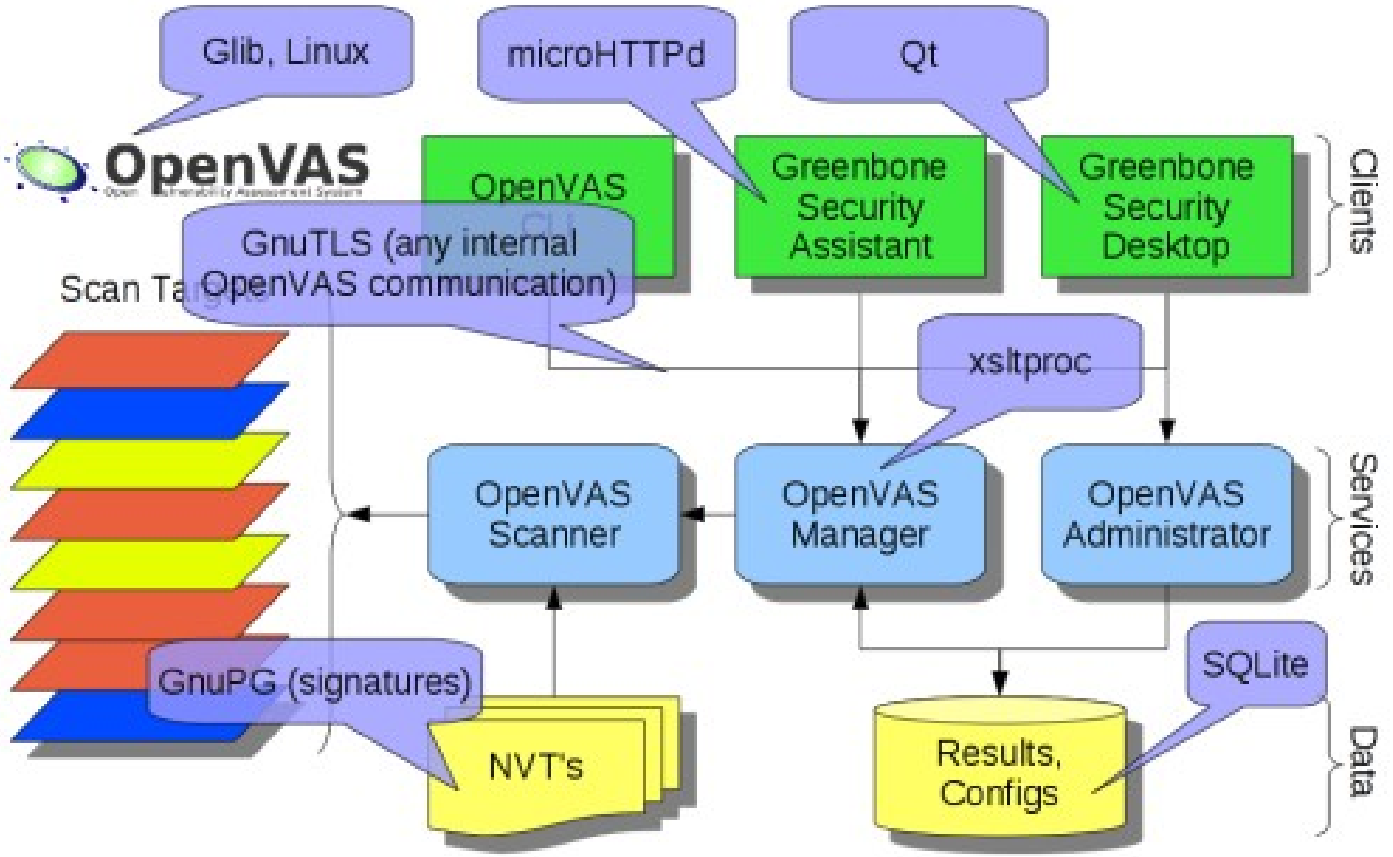
OMP. “Greenbone Security Assistant” (GSA) el cual es un servicio web que ofrece una interfaz de usuario para navegadores web. Este utiliza XSL (Extensible Stylesheet Language) el cual convierte las respuestas OMP en HTML.

The Greenbone Security Desktop (GSD) es un cliente OMP de escritorio basado en QT. Este funciona en diferentes versiones de Linux, Windows y otros sistemas operativos.

OpenVAS CLI (Command-line interface) contiene la herramienta en línea de comando “omp” el cual permite crear procesos batch para dirigir el Manejador de OpenVAS

Clientes OpenVAS (Cont.)

.



Más Sobre OpenVAS

El Administrador de OpenVAS actúa como una herramienta en línea de comando o como un demonio completo de servicio ofreciendo el protocolo OpenVAS de administración (OAP). Las tareas más importantes son el manejo de usuario y el manejo del ”feed”. GSA soporta OAP y los usuarios con el rol de “Admin” pueden acceder a la funcionalidad OAP.

La mayoría de las herramientas listadas anteriormente comparten la funcionalidad que es añadida en las Librerías OpenVAS.

El Escaner OpenVAS ofrece el protocolo de comunicación OTP el cual permite el control de la ejecución del escaneo. Tradicionalmente los clientes OpenVAS de Escritorio y CLI actúa como un cliente OTP directo.

OpenVAS oficialmente adopta OVAL (Open Vulnerability and Assessment Language), OVAL es un esfuerzo de la comunidad de seguridad de la información, para estandarizar la forma de valorar y reportar el estado de una máquina de los sistemas de cómputo.

* OVAL: http://oval.mitre.org/

Curso Virtual de Hacking Ético

Días:

Grupo 1: Sábados 4, 11, 18 y 25 de Enero del 2014
Grupo 2: Domingos 5, 12, 19 y 26 de Enero del 2014

Horario:

De 9:00am a 12:30m (UTC -05:00)

Más Información:

http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

caballero.alonso@gmail.com

@Alonso_ReYDeS

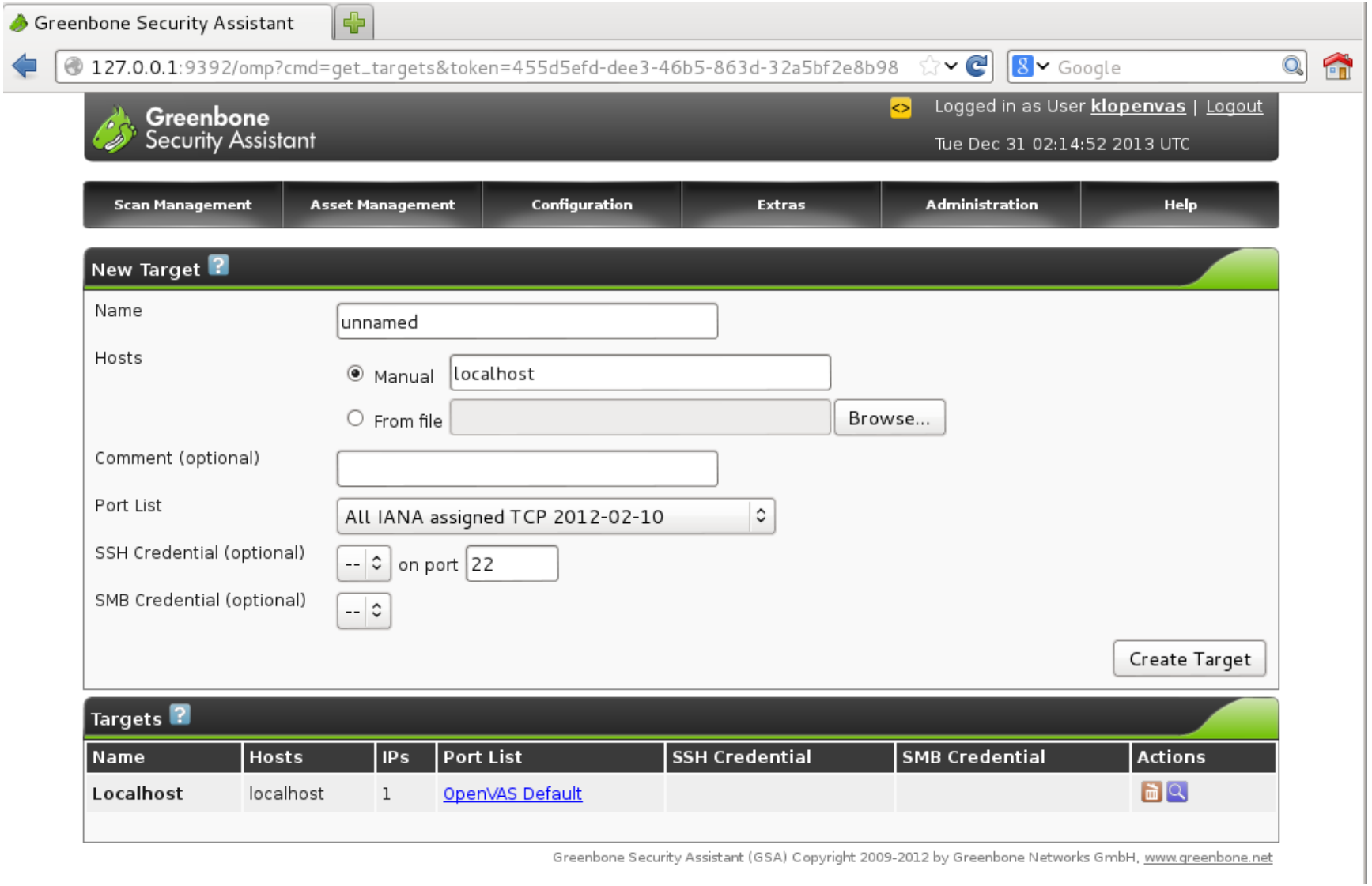
http://pe.linkedin.com/in/alonsocaballeroquezada/

ReYDeS

http://www.reydes.com

Demostraciones

A continuación se presentan algunas demostraciones prácticas utilizando OpenVAS en Kali Linux.



Más Material

Los invito a visualizar los 16 Webinars Gratuitos que he dictado durante todo el año 2013, sobre temas de Hacking Ético, Pruebas de Penetración, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Pueden obtener todas las diapositivas utilizadas en los Webinars Gratuitos desde la siguiente página:

http://www.reydes.com/d/?q=node/3

Pueden obtener todos los artículos y documentos que he publicado.

http://www.reydes.com/d/?q=node/2

Mi blog:

http://www.reydes.com/d/?q=blog/1

Webinar Gratuito

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 2 de Enero del 2014