Open Vulnerability Assessment System (OpenVAS)

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 31 de Marzo del 2016

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Digital Forensics.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS www.facebook.com/alonsoreydes

pe.linkedin.com/in/alonsocaballeroquezada/

Evaluación de Vulnerabilidades

Es el proceso de ubicar y reportar las vulnerabilidades. Esto proporciona una manera de detectar y resolver los problemas de seguridad antes de la explotación de alguien o algo.

La razón de realizar este procedimiento es debido a ser un componente crítico en la infraestructura de seguridad de varias organizaciones, pues la habilidad de tener una instantánea de la seguridad de toda la red, apoya a diversos procesos de seguridad y administrativos.

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

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

* OpenVAS: http://openvas.org/

Tipos de Evaluaciones

1. Evaluaciones de Host

Estas herramientas requieren instalar el software en cada sistema requerido a ser evaluado. Se evalúan vulnerabilidades a nivel del sistema como permisos de archivos inseguros, parches ausentes de software, políticas de seguridad para el cumplimiento de 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 redes grandes y complejas sobre sistemas heterogeneos.

El Proceso de Evaluación

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

- Detectar los Sistemas en Funcionamiento
- Identificar los Sistemas en Funcionamiento
- Enumerar los Servicios
- Identificar los Servicios
- Identificar las Aplicaciones
- Identificar las Vulnerabilidades
- Reportar las Vulnerabilidades

OpenVAS

OpenVAS (Open Vulnerability Assessment System) o Sistema Abierto para la Evaluación de Vulnerabilidades; está constituido por varios servicios y herramientas los cuales proporcionan la capacidad para realizar un escaneo de vulnerabilidades muy completo y poderoso, además de ser una solución para la administración de vulnerabilidades.

El corazón de esta arquitectura es el Escaner OpenVAS orientada al servicio, asegurado utilizando SSL. Este muy eficiente escaner ejecuta los NVTs - Network Vulnerability Tests (Pruebas de Vulnerabilidad en Redes), los cuales son servidos con actualizaciones diarias mediante el OpenVAS NVT Feed o mediante el servicio comercial, con más de 30,000 de ellos 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

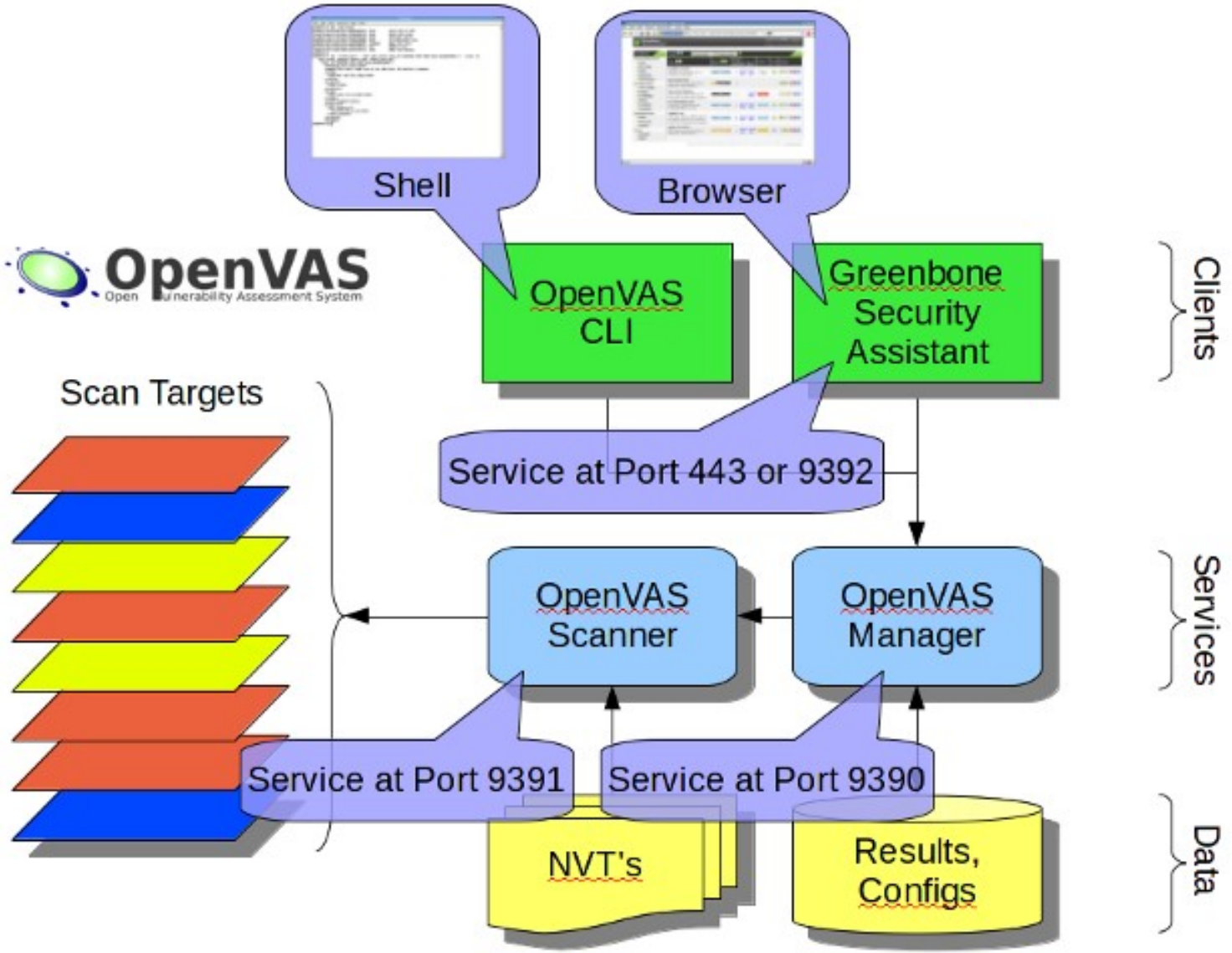
- **OpenVAS Scanner:** Escaneo de varios objetivos de manera concurrente. OpenVAS Transfer Protocol (OTP), Soporte SSL.

- **OpenVAS Manager:** OpenVAS Management Protocol (OMP), Base de Datos SQL (sqlite) para las configuraciones y resultados del escaneo, Soporte SSL para OMP (siempre), Varias tareas de escaneo concurrentes (Varios escaners OpenVAS), Gestor de notas para los resultados del escaneo, Gestor de falsos positivos para los resultados del escaneo. Escaneos programados, Detener, pausar y reiniciar tareas de escaneo. Modo Maestro-Esclabo para controlar varias instancias desde un nodo central, Reportes en varios formatos (XML, HTML, etc.), Gestor de usuarios, etc.

- **Greenbone Security Assistant (GSA):** 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



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

El Gestor de OpenVAS

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

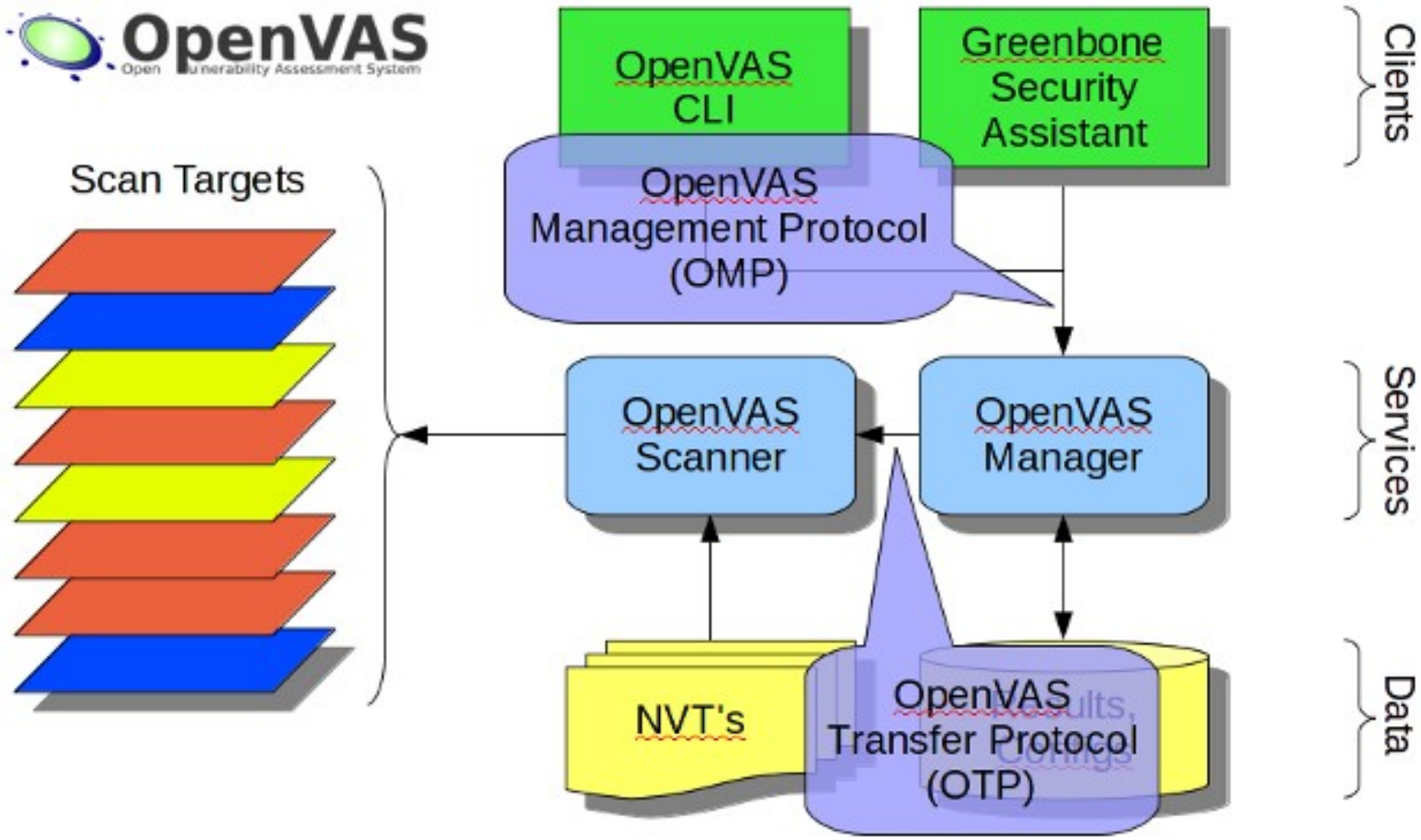
El Manejador controla el Escaner mediante OTP - OpenVAS Transfer Protocol (Protocolo OpenVAS de Transferencia) y ofrece por si mismo OMP - OpenVAS Management Protocol (Protocolo de Gestión OpenVAS) basado en XML.

Toda la inteligencia es implementada en el Gestor, así 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 Gestor también controla una base de datos SQL (basada en sqlite) donde se almacenan de manera centralizada toda la configuración y resultados del escaneo. Finalmente el gestor también controla la gestión de los usuarios incluyendo controles de acceso con grupos y roles.

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

El Gestor de OpenVAS (Cont.)



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

Clientes de OpenVAS

Están disponibles diferentes clientes OMP.

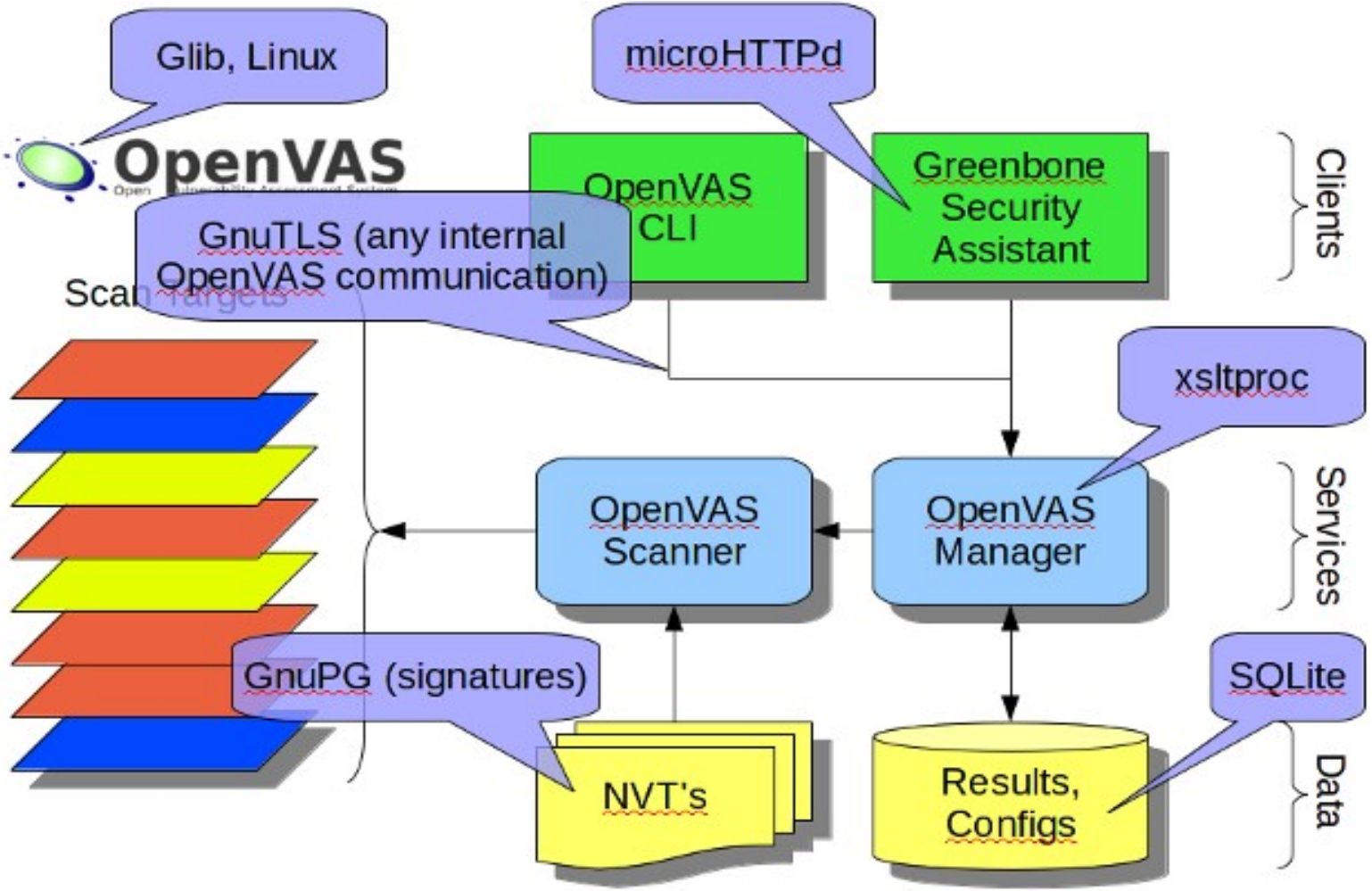
- **Greenbone Security Assistant (GSA)**: Es un servicio web el cual ofrece una interfaz de usuario para navegadores web. Este utiliza XSL (Extensible Stylesheet Language) el cual convierte las respuestas OMP en HTML.

- **OpenVAS CLI (Command-line Interface):** Contiene la herramienta en línea de comando “omp” el cual permite crear procesos batch (por lotes) para dirigir el Gestor de OpenVAS

La mayoría de las herramientas listadas comparten funcionalidad la cual esta añadida en las librerías OpenVAS.

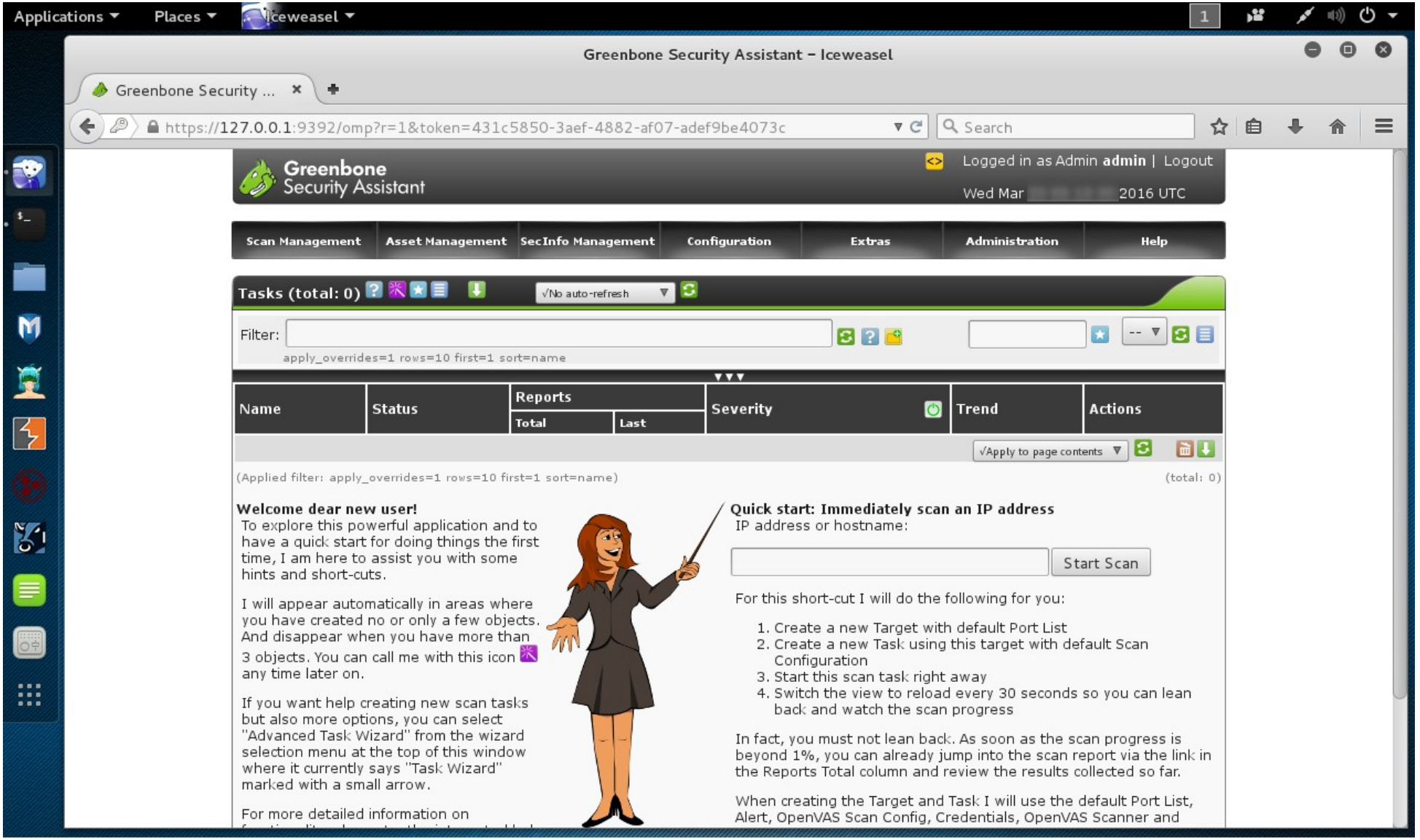
El escaner OpenVAS ofrecen un protocolo de comunicación OTP (OpenVAS Transfer Protocol) el cual permite controlar la ejecución del escaneo.

Clientes OpenVAS (Cont.)



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

Demostraciones



Curso Virtual de Hacking Ético

Curso Virtual de Hacking Ético 2016

Domingos 3, 10, 17, 24 de Abril y 1 de Mayo del 2016. De 9:00 am a 12:00 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación:

En la actualidad se requieren profesionales quienes sean responsables de encontrar y entender las vulnerabilidades en las organizaciones, además de trabajar diligentemente para mitigarlas antes de ser aprovechadas por los atacantes maliciosos. Este curso abarca las herramientas, técnicas y metodologías fundamentales para realizar adecuadamente proyectos de pruebas de penetración de inicio a fin. Todas las organizaciones necesitan personal experimentado quienes puedan encontrar vulnerabilidades, y este curso proporciona los conocimientos ideales.

Objetivos:

Este curso enseña a los participantes a realizar un reconocimiento detallado, aprendiendo sobre la infraestructura del objetivo mediante búsquedas en blogs, motores de búsqueda, redes sociales y otros sitios de Internet. Se escanean las redes objetivo utilizando las mejores herramientas disponibles, proporcionando las mejores opciones y configuraciones para realizar los escaneos. Luego se exploran diversos métodos de explotación para ganar acceso hacia los sistemas objetivo y medir el riesgo real para la organización. Después se realizan acciones de post-explotación y ataques de contraseñas, redes inalámbricas y aplicaciones web. Todo realizado en un laboratorio de pruebas controlado, donde se desarrollan los ataques.

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management. Ha sido Instructor en el OWASP LATAM Tour Lima, Perú y Conferencista en PERUHACK. Cuenta con más de trece años de experiencia en el área y desde hace nueve años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.

Más Información: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico
E-mail: **caballero.alonso@gmail.com** / Sitio Web: http://www.reydes.com

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

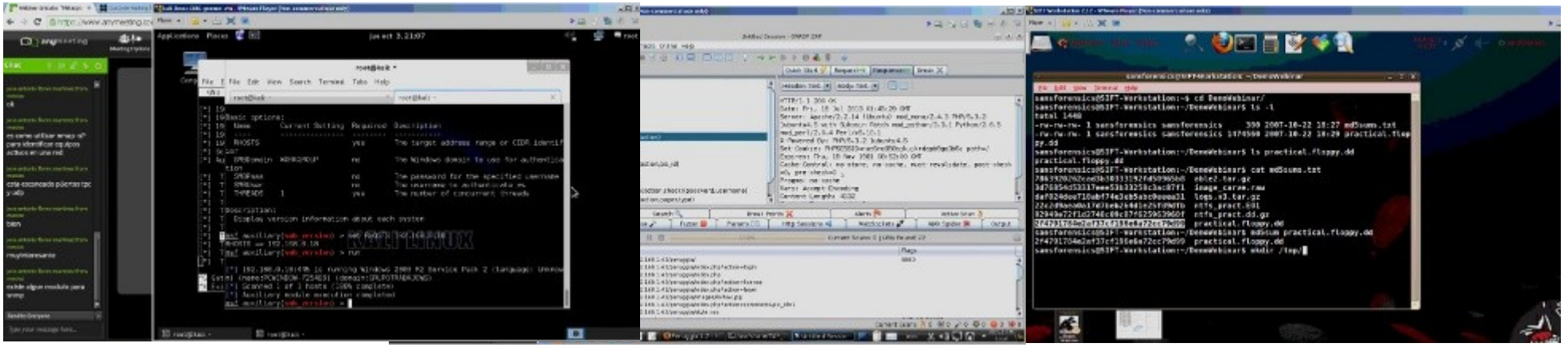
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

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

Curso Virtual de Informática Forense

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



Más Contenidos

Videos de 30 Webinars Gratuitos sobre temas de Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

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

Diapositivas utilizadas en los Webinars Gratuitos.

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

Artículos y documentos publicados

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

Mi Blog sobre temas de mi interés.

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

Open Vulnerability Assessment System (OpenVAS)

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 31 de Marzo del 2016