Taller Gratuito

Introducción al Pentesting

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Sábado 29 de Noviembre 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 (Master), Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General).
- Más de 11 años de experiencia en el área.
-  @Alonso_ReYDeS
-  pe.linkedin.com/in/alonsocaballeroquezada/

Agenda

- ¿Qué es una Prueba de Penetración?
- Algunos Conceptos
- Laboratorio de Pruebas
- Fases de una Prueba de Penetración
- Kali Linux
- Características de Kali Linux
- Reconocimiento
- Demostraciones

¿Qué es una Prueba de Penetración?

Una Prueba de Penetración puede ser definida como un intento legal y autorizado de encontrar y explotar satisfactoriamente sistemas de cómputo con el propósito de hacer estos sistemas más seguros.

Este proceso incluye probar vulnerabilidades como también proporcionar pruebas de concepto (PoC) de los ataques, para demostrar la existencia de las vulnerabilidades.

Una Prueba de Penetración adecuada siempre finaliza con recomendaciones específicas para remediar y solucionar lo encontrado durante el desarrollo de la prueba.

“Este proceso es utilizado para ayudar a asegurar las redes y computadoras contra futuros ataques.”

También se le conoce como Pen-Testing, Ethical Hacking, etc.

Algunos Conceptos

- Los Hackers Éticos realizan muchos de los procedimientos utilizando las mismas herramientas de los atacantes maliciosos.

- Es de suma utilidad para el Hacker Ético pensar como un atacante malicioso.

- Las Pruebas de Penetración simulan ataques reales, lo cual beneficia al cliente quién realiza el pago por estos servicios.

- Hay una palabra clave principal a considerar; Autorización.
  La autorización es el proceso de obtener la aprobación antes de realizar las pruebas o ataques. Cuando se obtiene la autorización, ambas partes acuerdan el alcance de la prueba, lo cual incluye los sistemas y recursos que se evaluarán. Es importante para ambas partes entender el alcance y la autorización.

- Otras formas de diferenciar a un Hacker Ético de un atacante malicioso son la Motivación y la Intención.

Laboratorio de Pruebas

Un buen Hacker Ético debe tener un lugar para practicar y explorar. Pues NO es “Ético” atacar sistemas o redes sin autorización.

Esto puede ser realizado mediante la creación de Laboratorios de Hacking, el cual es un entorno donde los ataques pueden ser realizados sin temor a quebrantar alguna ley o política. Aquí se es libre para explorar todas las herramientas y técnicas requeridas.

Como un paso extra de protección se puede crear un laboratorio aislado, donde no se permita ningún tipo de tráfico entrante o saliente desde/hacia el exterior.

Se recomienda la utilización de software de virtualización, los cuales son fáciles de configurar, además de permitir crear diferentes escenarios virtuales de prácticas con diferentes sistemas operativos.

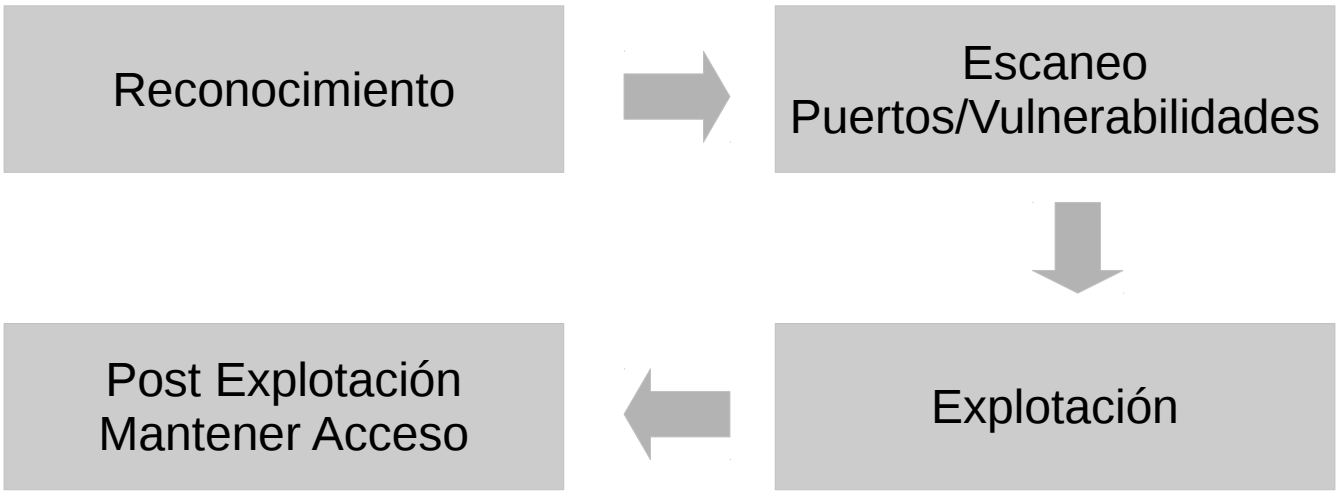
Las Pruebas de Penetración son un proceso destructivo, muchas herramientas y exploits puede generar mucho daño a los sistemas.

Fases de una Prueba de Penetración

Como la mayoría de procesos, existe un procedimiento para realizar una Prueba de Penetración. De esta manera puede ser dividida en una serie de pasos o fases.

Todas estas fases juntas forman una metodología completa de una Prueba de Penetración.

Su utilización es importante, porque no solo mantiene a la prueba enfocada y avanzando, sino porque permite la utilización de los resultados de cada fase en las fases posteriores.



Kali Linux

Kali Linux es la nueva generación de la Distribución Linux BackTrack para realizar Pruebas de Penetración y Auditorías de Seguridad.

Kali Linux es una completa reconstrucción de BackTrack desde las bases, adheriéndose completamente a los estándares de desarrollo de GNU/Linux Debian.

Se han realizado algunos cambios para cumplir ciertas necesidades.

- Acceso por diseño de un único usuario “root”.
- Servicios de Red deshabilitados por defecto.
- Kernel de Linux personalizado.

El inadecuado uso de las herramientas de seguridad dentro de la red, podrían causar daños irreparables y con resultados significativos.

* What is Kali Linux?: http://docs.kali.org/category/introduction

Características de Kali Linux

- Más de 300 herramientas para Pruebas de Penetración.
- Es libre y siempre lo será.
- Árbol Git Open Source.
- Cumplimiento con FHS (Filesystem Hierarchy Standard)
- Amplio soporte para dispositivos inalámbricos.
- Entorno de desarrollo seguro.
- Paquetes y repositorios firmados con GPG.
- Varios lenguajes.
- Completamente personalizable.

* What is Kali Linux?: http://docs.kali.org/introduction/what-is-kali-linux

Reconocimiento

El Reconocimiento también conocido como captura de información, es la más importante de las fases en una Prueba de Penetración. Pues mientras más tiempo se invierta recolectando información sobre el objetivo, se tienen más probabilidades de tener éxito en las fases posteriores.

Irónicamente el reconocimiento es también una de las fases más evitadas, menos utilizadas, y menos comprendidas en una metodología de Pruebas de Penetración.

- Reconocimiento Activo:

  Implica interactuar directamente con el objetivo. Existen altas probabilidades de ser detectados durante este procedimiento.

- Reconocimiento Pasivo:

  Utiliza una amplia cantidad de información disponible en la web. No se interactua directamente con el objetivo.

* What is Kali Linux?: http://docs.kali.org/introduction/what-is-kali-linux

Curso Virtuales

Todos los Cursos 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 Información:


caballero.alonso@gmail.com

@Alonso_ReYDeS 


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

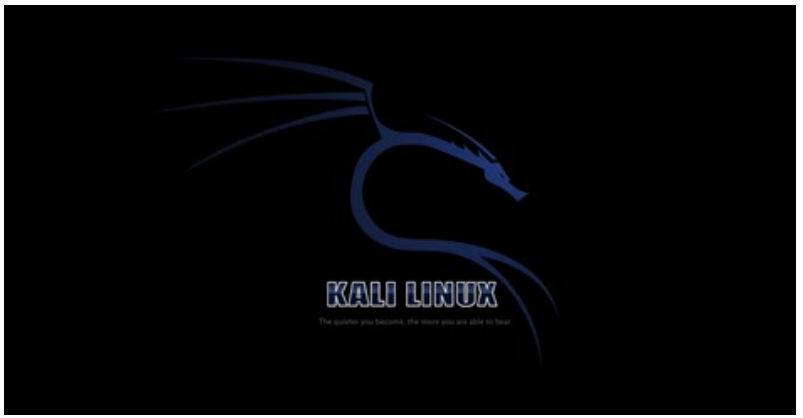

ReYDeS

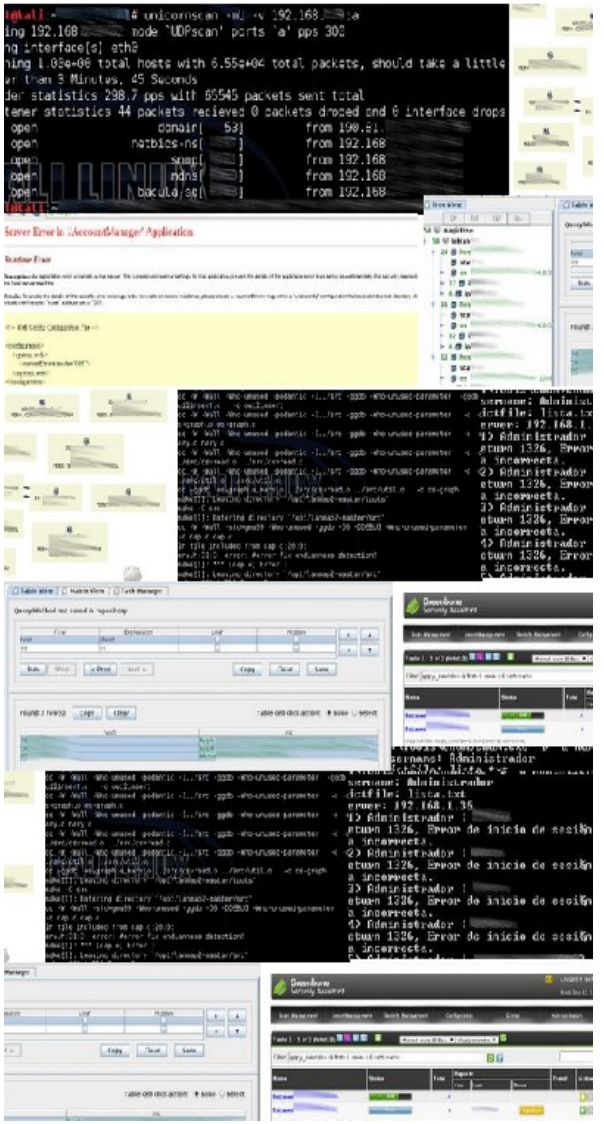

http://www.reydes.com

Demostraciones

A continuación se realizarán varias demostraciones utilizando las siguientes herramientas.

- Httrack
- Google
- The Harvester
- Whois
- Netcraft
- Host
- Nslookup
- Dig
- smtp-user-enum
- MetaGooFil
- SET





¡Muchas Gracias!

Introducción al Pentesting

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Sábado 29 de Noviembre del 2014