



Webinar Gratuito

Reconocimiento Web

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 8 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/

Reconocimiento

El reconocimiento consiste en investigar todo lo relacionado a la estructura de un sitio web y el funcionamiento de sus aplicaciones. Este es un aspecto crítico, pero muchas veces no valorado.

Los ataques más efectivos son realizados haciendo un riguroso y profundo reconocimiento del objetivo, incluyendo todas las páginas webs, las aplicaciones y estructuras de comandos para la entrada y salida de un sitio web.

El reconocimiento se divide en dos áreas.

1. Reconocimiento de la Infraestructura.

Se orienta hacia los componentes “externos” de la aplicación web. Incluyendo Software freeware, open source y comercial.

2. Reconocimiento a la Aplicación.

Se orienta en la estructura, la lógica y características individuales de una aplicación web altamente personalizada.

Reconocimiento de la Infraestructura

Las Aplicaciones Web requieren una infraestructura de soporte; software o hardware del servidor web, entradas DNS, equipo de red, balanceadores de carga, etc.

El primer paso para la evaluación de seguridad de una aplicación web es la identificación y análisis de la infraestructura al más bajo nivel sobre la cual reside la aplicación.

Se utilizan diversas herramientas y técnicas para realizar esta tarea:

Huellas y Escaneo: Definir el Alcance

- Investigación en los registradores de Internet
- Consulta a los DNS
- Investigación general de la organización.
- Descubrimiento del servidor
- Identificación de los servicios de red

Reconocimiento de la Infraestructura (Cont.)

Captura Sencilla del banner

Huella Avanzada HTTP

- Métodos HTTP Inesperados
- Anomalías en la Cabeceras del Servidor
- SHODAN

Infraestructuras Intermedias

- Servidores Virtuales
- Detectar Balanceadores de Carga
- Detectar Proxys
- Detectar Firewalls de Aplicación Web

Reconocimiento de la Aplicación

El propósito de esta fase es inspeccionar la aplicación para generar una figura completa del contenido, los componentes, funciones, y flujo del sitio web, con el propósito de obtener pistas sobre donde podrían residir las vulnerabilidades.

Una adecuada inspección puede revelar problemas con aspectos de la aplicación más allá de la presencia o ausencia de ciertas firmas tradicionales de vulnerabilidades.

El reconocimiento de la aplicación es sencilla. Podría consistir en realizar un seguimiento o clics a través de la aplicación y poner atención en las URLs para ver como está estructurada el sitio web completo.

A continuación se detallan las tareas clave a realizar.

1. Inspección Manual
2. Herramientas automáticas de Reconocimiento
3. Web Crawling automático
4. Perfiles comunes de Aplicaciones Web

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/>



<http://www.reydes.com>



ReYDeS

Más Material

Videos de 22 Webinars Gratuitos que he dictado sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

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

Todas las diapositivas utilizadas en los Webinars Gratuitos las encuentran en la siguiente página.

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

Todos los artículos y documentos que he publicado.

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

Mi Blog sobre temas de mi interés.

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



¡Muchas Gracias!

Reconocimiento Web

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 8 de Noviembre del 2014