ETHICAL HACKING

JUAN CARLOS VELARDE ALVAREZ MANSILLA

INTRODUCCION

CONCEPTOS BASICOS

HACKER

Se llama así a las personas con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionadas con las operaciones de computadora, redes, seguridad, etc.

Un hacker, es una persona apasionada, curiosa, dedicada, libre, comprometida con el aprendizaje y con enormes deseos de mejorar sus habilidades y conocimientos.

Es un programador experto de computadoras

TIPOS DE HACKERS

WHITEHAT

Hace referencia a un hacker de sombrero blanco, el cual se rige por su ética, esta se centra en analizar, testear, proteger y corregir vulnerabilidades (bugs) en los sistemas de información y comunicación

Estos suelen trabajar en empresas de seguridad informática. De donde proviene la definición de hackers éticos o pentesters (test de penetracion)

BLACK HATS

Es una clase de hacker dedicado a la obtención y explotación de vulnerabilidades en sistemas de información, bases de datos, redes informáticas, sistemas operativos, etc. Para su propio beneficio, por ello, desarrollan programas como malware, virus, troyanos, crack`s, etc. que les ayuden a lograr sus objetivos.

GRAYHAT

Son hackers que están en el límite de lo que se puede considerar bueno y lo malo. Usualmente se infiltran en un sistema o servidor (que va en contra de la ley) para poner sus nombres o cambiar los nombres de las empresas. También pueden avisar a los administradores que su sistema ha sido ganado por ellos para que en un futuro puedan cubrir esos huecos y fallas y los arreglen para que otros hackers maliciosos no puedan entrar.

ETHICAL HACKING

DEFINICION

Es el proceso por el cual, se utilizan las mismas técnicas y herramientas que un black hat para atacar a una organización y descubrir las vulnerabilidades de la misma.

Para tal finalidad los ethical hackers han desarrollado las denominadas pruebas de penetración, (PEN-TEST por sus siglas en inglés).

"para atrapar a un ladrón debes pensar como un ladrón".

PEN TESTING

Conjunto de métodos y técnicas para la realización y simulación de un ataque en un escenario controlado, al cual se le practica un test de intrusión, para evaluar la seguridad de un sistema o de una red informática, y así encontrar los puntos débiles y vulnerables en dichos sistemas o redes.

PORQUE REALIZAR PRUEBAS DE PENETRACION

La seguridad de una organización es un aspecto cambiante. Una empresa puede alcanzar un nivel de protección óptimo en un momento determinado y ser totalmente sensible poco después, luego de realizar cambios en la configuración de un servidor o realizarse la instalación de nuevos dispositivos de red.

Asi mismo, continuamente aparecen nuevos fallos de seguridad en software existentes, que previamente se creían seguros.

TIPOS DE ATAQUES

ACTIVOS: Estos alteran y comprometen la disponibilidad, integridad, autenticidad de la información, afectando a los sistemas, redes y aplicaciones informáticas objetivo. Ejemplo: Sql injection/ alteración de la aplicación web, robo de información.

PASIVOS: Estos no alteran, ni modifican al sistema o red objetivo, solo se obtiene y compromete la confidencialidad de la información. Ejemplo: un sniffing de red.

MODALIDADES DE ATAQUES

ATAQUE INTERNO: es realizado desde el interior de la organización, por lo general suelen ser perpetrados por personal propio de la empresa, empleados inconformes o clientes que tienen accesos. Colaborados por malas configuraciones. Ejemplo, robo de información, instalación de software malicioso, etc

ATAQUE EXTERNO: es el que se realiza desde una fuente externa a la organización. Ejemplo internet o conexiones remotas, etc

TÉCNICAS PARA UTILIZAR EN UN ATAQUE

Denegación de servicio DoS
Crackeo de contraseña por fuerza bruta
Explotacion de vulnerabilidades
Phising/ scam
Secuestro de secciones en redes wifi
Hijacking (secuestro), dominio, seccion, ip, entre otras
Spoofing (suplantación), ip, DNS etc.
Ingeniería social

TIPOS DE PRUEBAS PENTESTING

- **Pruebas de penetración con objetivo:** se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- **Pruebas de penetración sin objetivo**: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización.
- **Pruebas de penetración a ciegas**: en estas pruebas sólo se emplea la información pública disponible sobre la organización.

- **Pruebas de penetración informadas:** Se utiliza información privada, otorgada por la organización acerca de sus sistemas informáticos. Se trata de simular ataques realizados por individuos internos de la organización que tienen acceso a información privilegiada.

- **Pruebas de penetración externas**: son realizadas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos de seguridad perimetrales de la organización.

- **Pruebas de penetración internas**: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

MODALIDADES DE LAS PRUEBAS

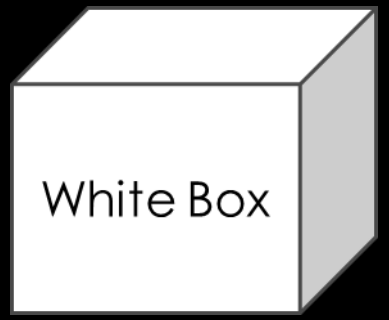
Red teaming: Prueba encubierta, es donde sólo un grupo selecto de directivos sabe de ella. En esta Modalidad son válidas las técnicas de "ingeniería social" para obtener información que permita realizar Ataque. Ésta prueba es la más real y evita se realicen cambios de última hora que hagan pensar que hay un Mayor nivel de seguridad en la organización.

Blue teaming: El personal de informática conoce sobre las pruebas. Se aplica cuando las Medidas tomadas por el personal de seguridad de las organizaciones ante un Incidente, repercuten en la continuidad de las operaciones críticas de la organización, por ello es necesario alertar al personal para evitar situaciones de pánico y fallas en la continuidad de la actividad.

FASES DE LAS PRUEBAS DE PENETRACION

- Recopilación de información
- Descripción de la red
- Exploración de los sistemas
- Extracción de información
- Acceso no autorizado a información sensible o crítica
- Auditoría de las aplicaciones web
- Elaboración de informes
- Informe final

TIPOS DE PRUEBAS DE PENETRACIÓN



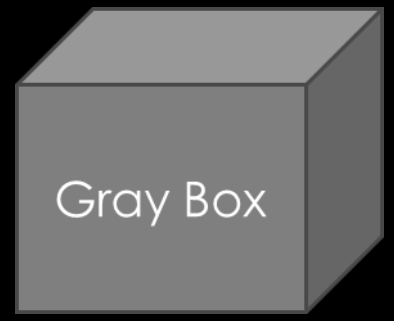
CAJA BLANCA

Se cuenta con el código fuente de la aplicación y la documentación. Se simula el ataque y el daño que podría ocasionar un trabajador interno enojado o desleal. En éste tipo de prueba, se encuentran cuestiones relacionadas a fallas lógicas, caminos mal estructurados en el código, el flujo de entradas específicas a través del código, funcionalidad de ciclos y condiciones, hoyos de seguridad interna y permite probar cada objeto y función de manera individual.

Caja Negra

Aquí, el tester no tiene acceso al código, ni a la documentación. Lo único con lo que cuenta para trabajar es con la versión descargable de manera pública de la aplicación. Se simula un ataque lanzado por un hacker; el vector de ataque más común, es la intercepción de tráfico y la inyección de contenido malicioso para obtener información. Éste tipo de pruebas, trata de explotar vulnerabilidad de tipo Cross Site Scripting(XSS), inyección de link e inyección de comandos SQL.

CAJA GRIS



Es una combinación de ambas, se realiza un análisis con la ventaja que se cuenta con el código y documentación, que sirven como guía.

BENEFICIOS DE UN ETHICAL HACKING

- Ofrecer un panorama acerca de las vulnerabilidades halladas en los sistemas de información.
- Deja al descubierto configuraciones no adecuadas en las aplicaciones instaladas en los sistemas que pudieran desencadenar problemas de seguridad en las organizaciones.
- Identificar sistemas que son vulnerables a causa de la falta de actualizaciones.
- Disminuir tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización.

HABILIDADES QUE DEBE TENER UN HACKER ÉTICO PENTESTER

- Tener conocimientos avanzados en programación (php, python, ruby, C, C++, .Net, java, etc.)
- Poseer conocimientos profundos de diversas plataformas como Linux, Windows, Unix, etc.
- Manejo de redes y protocolos, arquitecturas, etc.
- Dominio de hardware y software
- Ser experto en técnicas, metodos y herramientas de hacking
- Capacidad de análisis e investigación para proveer soluciones

HERRAMIENTAS PENTESTING

SAMURÁI PENTEST

Samurai Web Testing Framework es un entorno de trabajo basado en GNU/Linux Ubuntu, que ha sido pre-configurado para llevar a cabo test de penetración a aplicativos Web.

BACK TRACK

es una distribución GNU/Linux en formato Live CD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

WIFISLAX

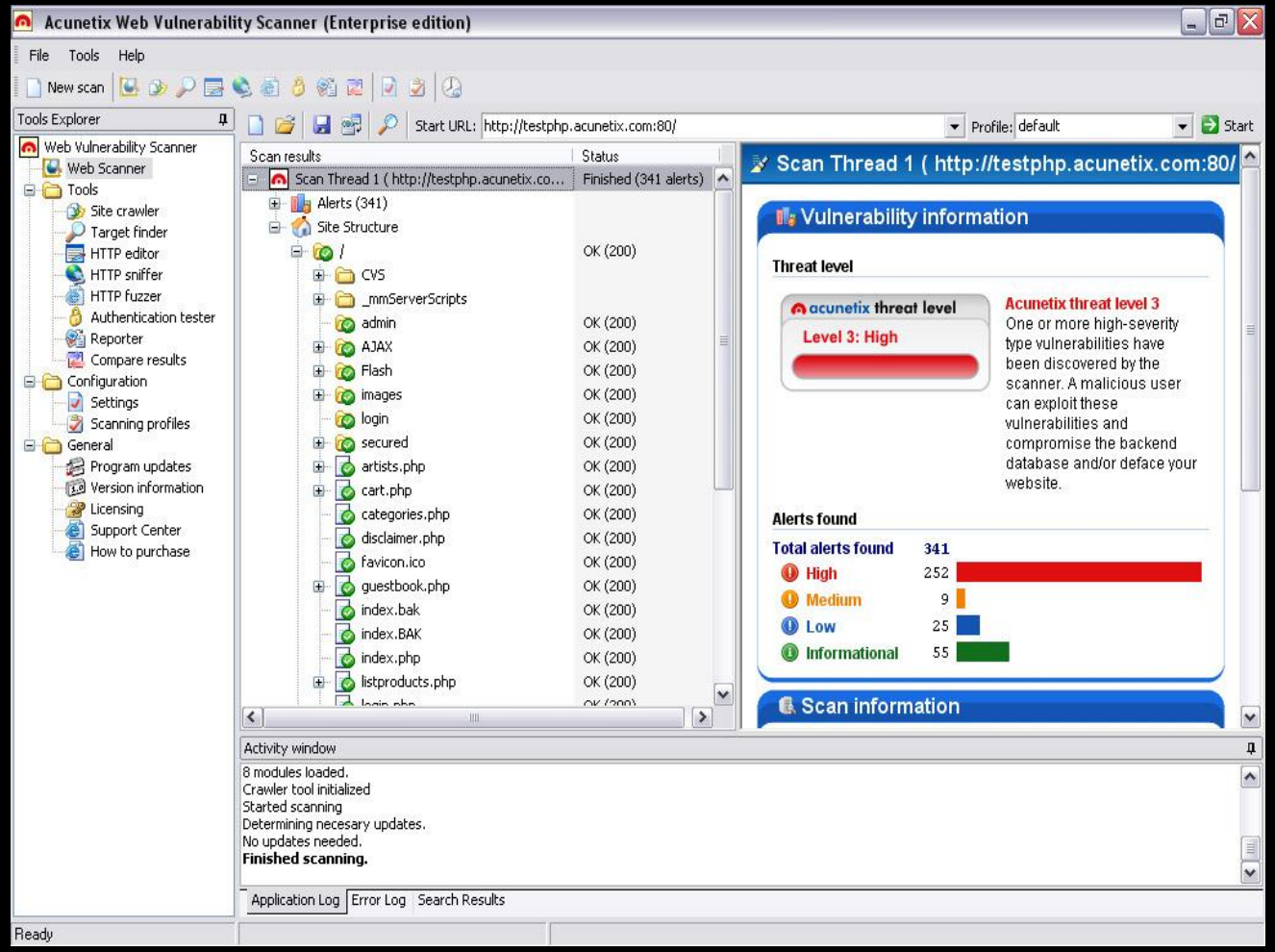
Incluye una larga lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan numerosos escáner de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría wireless, además de añadir una serie de útiles lanzadores.

MATRIUX

Es una distribución de seguridad que consiste en un poderoso conjunto, de herramientas libres y de código abierto que pueden ser utilizadas para varios propósitos incluyendo, pero no limitado a penetration testing, hacking ético, administración de sistemas y redes, investigaciones forenses, pruebas de seguridad, análisis de seguridad, y mucho más.

ACUNETIX

Potente herramienta para MS Windows que detecta un gran número de vulnerabilidades, entre ellas Cross-Site Scripting, SQL Injection, CRLF injection, Code execution, Directory Traversal, File inclusion, busca vulnerabilidades en formularios de subida de archivos (file upload) y muchísimas mas.



BIBLIOGRAFIA

- http://www.seguridad.unam.mx/descarga.dsc?arch=2776
- http://www.taringa.net/posts/ciencia-educacion/13129306/Hackers-Que-son-los-hackers.html
- http://thehackerway.com/about/
- http://www.slideshare.net/YulderBermeo/introduccion-hacking-etico
- http://securityec.com/herramientas-enfocadas-a-las-seguridad-informatica-pen-testing-seguridadinformatica/
- http://seguridadetica.wordpress.com/2012/04/11/5-heramientas-utiles-en-penetration-testing-para-aplicaciones-web/

GRACIAS