Contenido Curso Hacking Ético

5770/ER/08/06

Departamento: I+D	**Proyecto:** Hacking	**Documento:** PW_IDU_CUR_070601_ContenidoCursohackingEtico 2007.odt	**Nº pags:** 6
Asunto: **Contenido de Curso de Hacking Ético 2007**			
Autor: Constantino Malagón		**Aprobado por:** José Luis Marina Manuel Guillermo Fraga	
Fecha de creación: 05-05-2007		**Fecha de aprobación:** 20-05-2007	
Lista de Distribución: Departamento de Seguridad Peopleware y de ISM Interesados en la Seguridad desde un punto de vista Técnico. Alumnos del Curso Peopleware: Hacking Ético 2007			

Índice

DESCRIPCIÓN DEL CURSO....3

OBJETIVO DEL CURSO....3

METODOLOGÍA....3

CONTENIDO....4

MÓDULO 1: INTRODUCCION AL HACKING ÉTICO....4
MÓDULO 2: METODOLOGÍA PARA LA OBTENCIÓN DE INFORMACIÓN PREVIA AL ATAQUE....4
MODULO 3: ACCESO AL SISTEMA....5
MODULO 5: MANTENIMIENTO DEL ACCESO....5
MODULO 4: BORRADO DE HUELLAS....6

PROYECTO DE FIN DE CURSO....6

Descripción del Curso

Un hacker ético es una persona a la que se contrata para simular los posibles ataques que se podrían llevar a cabo contra la red o los sistemas de una organización. Para llevar esto a cabo el hacker ético debe realizar toda clase de tests de penetración, estudios para la obtención de información del objetivo, simulacros de ataques tanto externos como internos,... En suma, debe pensar y actuar como lo haría un posible asaltante. Como muestra, es bien sabido por todos dónde acaban trabajando los crackers o hackers maliciosos.

Objetivo del Curso

El objetivo del curso es pues introducir las diferentes técnicas que se pueden llevar a cabo para conseguir el acceso no autorizado en un sistema o en una red. Con ello se podrán diseñar con más efectividad las medidas necesarias para evitar dichos ataques.

En el curso haremos una introducción a las técnicas de hacking/cracking, haciendo énfasis en un carácter metodológico para la consecución del posible ataque.

Metodología

El curso está basado en Linux y siempre que sea posible se utilizarán herramientas de código abierto. Es recomendable pues estar familiarizado con sistemas GNU/Linux, aunque no es un requisito indispensable para el correcto seguimiento del curso.

El curso es intensivo y de un enfoque totalmente práctico. La duración es de 16 horas sin incluir el tiempo de realización del proyecto fin de curso, que lo realizará el alumno durante las 2 siguientes semanas en horario fuera del curso pero con la ayuda del profesor.

Para la obtención del diploma acreditativo de aprovechamiento del curso es necesaria la realización en el plazo previsto del proyecto fin de curso.

Contenido

MÓDULO 1: INTRODUCCION AL HACKING ÉTICO

- ¿Qué es un hacker?
- Clases de hackers.
- ¿Puede el hacking ser ético?
- Funciones de un hacker ético
- Perfil de conocimientos de un hacker ético
- Fases en el ataque a un sistema:
  - Reconocimiento
  - Escaneo
  - Accesso al sistema
  - Mantenimiento del acceso
  - Borrado de huellas

MÓDULO 2: METODOLOGÍA PARA LA OBTENCIÓN DE INFORMACIÓN PREVIA AL ATAQUE

- Técnicas pasivas para la obtención de información.
  - Google hacking
- Técnicas pasivas para la obtención de información: Técnicas de escaneo
  - Definición de escaneo
  - Tipos de escaneo
  - Escaneo de puertos
  - Escaneo de una red
  - Detección de vulnerabilidades

- Ingeniería social
- LAB 1: Uso de Whois, Nslookup y Traceroute para obtención de información.
- LAB 2: Detección de puertos abiertos : Nmap
- LAB 3: Detección de vulnerabilidades: Nessus

MODULO 3: ACCESO AL SISTEMA

- Obtención de contraseñas (Cracking Passwords)
- ARP Spoofing: ataques man-in-the-middle.
- DNS Spoofing.
- Exploits.
- LAB 4: Obtención de una password mediante un sniffer (ethereal y telnet)
- LAB 5: Obtención de una password y descifrado posterior: Uso de Cain&Abel
- LAB 6: Spywares y Keyloggers: Uso de un keylogger basado en software y de un spyware.

MODULO 4: MANTENIMIENTO DEL ACCESO

- Troyanos y puertas traseras.
- Shell remotos.
- Evadir los firewalls. Reverse shell.
- Sistemas de detección de intrusos (IDS)
- LAB 7: Obtención de un shell remoto.
- LAB 8: Spywares y Keyloggers: Uso de un keylogger basado en software y de un spyware.
- LAB 9: Uso de un IDS: snort.

MODULO 5: BORRADO DE HUELLAS

- Uso de proxies anónimos.
- Encadenamiento de proxies.
- Ocultación de ficheros y procesos.
- Borrado de los logs del sistema.
- Análisis forense.
- LAB 10: Ocultar ficheros y procesos. Alternate Data Streams (ADS)

Proyecto de Fin de Curso

El proyecto fin de curso tiene como objetivo realizar un simulacro de ataque a un sistema. En concreto se construirá un troyano y se introducirá este troyano en un sistema aprovechándose de una vulnerabilidad conocida.

Esta práctica de desarrollará durante dos semanas posteriores al curso. De esta forma habrá tiempo suficiente para poder desarrollarla sin prisas y de forma que los alumnos puedan coordinarla con otras actividades.

El curso dispone de un foro atendido por el profesor para ayuda y seguimiento.

Se entregarán diplomas acreditativos a la entrega y evaluación del proyecto.