Segunda Edición del Curso Online de Especialización en Seguridad informática para la intrusión de sistemas. Metasploit en profundidad

Orientado a:

- Responsables de seguridad.
- Cuerpos y fuerzas de seguridad del Estado.
- Agencias militares.
- Ingenieros de sistemas o similar.
- Estudiantes de tecnologías de la información.

Organización y Directores del curso:

- Dr. Jorge Ramió (Criptored) @criptored
- Dr. Alfonso Muñoz (Criptored) @criptored

LinkedIn Criptored: https://www.linkedin.com/grp/home?gid=8387069

Impartición: online vía WebEx Duración: 12 horas Certificado CPE de 12 horas, válido para certificaciones profesionales Fecha: 2, 9 y 16 de octubre de 2015 Días/Horas: Viernes de 16:00 a 20:00 horas (España)

Instructor: D. Pablo González - @pablogonzalezpe (CV al final del documento)
https://www.linkedin.com/pub/pablo-gonz%C3%A1lez-p%C3%A9rez/22/71/463

La matrícula incluye como documentación y material de apoyo adicional el libro de la editorial 0xWORD: **Metasploit para Pentesters. 3ª Edición revisada y ampliada**. Este libro se proporciona al contratar un curso completo en formato individual. Gastos de envío en Península incluidos. Gastos de envío para fuera de España (véase los descuentos en función de su proveedor local).

TEMARIO

Módulo 1. Metasploit framework. Explotación y post-explotación

1. Introducción al framework
    i. Arquitectura. Binarios e interfaces
    ii. Estructura de archivos del framework: modules, data, external, scripts, tools, …
    iii. Adicción y modificación de módulos al framework
    iv. Automatización y configuración del entorno
    v. Comandos básicos
    vi. Github oficial: Metasploit-framework
2. Herramientas de pentesting con Metasploit
    a. Las auxiliary: un cajón
    b. Escáneres de puertos y fingerprinting (SSH, SMB, HTTP, …)
    c. Servidores DNS y DHCP
    d. Protocolo ARP
    e. DoS y módulos de Brute Force

3. Módulos de explotación con Metasploit
    i. Tipos de explotación y módulos: Explotación directa, client-Side, explotación local y fileformat
    b. Atributos y métodos de los módulos
        i. Payloads y configuraciones. Plataformas
        ii. Explotación en distintos sistemas: Windows (XP, 7, 8, 8.1), Linux y servicios multiplataforma
4. Post-Explotación
    i. Funcionalidades. Recolección de información y ámbito
    ii. Comandos y módulos de Meterpreter
    iii. Inclusión de módulos de Meterpreter
        1. Sessiondump
    iv. Más funcionalidades de Meterpreter en un pentesting

Módulo 2. Metasploit avanzado

5. Técnicas y usos en un pentesting
    a. VPN como MiTM
    b. ProxyChains & Socks4a
    c. Shellcodes personalizables
    d. Pivoting
6. Evasión de AVs
    a. Herramientas del framework (msfpayload, msfencode, msfvenom)
    b. Dynamic Stager
    c. DLL & EXE go to 0
        i. Scripts: Meterpreter en PS y Meterpreter binary to Base64
7. Desarrollo de módulos y scripts
    i. Componentes y conceptos básicos de los módulos. Mixins
    ii. Herramientas del framework: Pattern_create, Pattern_offset, Metasm
    iii. Explicación Stack Buffer Overflow
        1. Generación de un exploit en Ruby
        2. Generación del módulo en Metasploit
    iv. Generación de scripts en Meterpreter

REQUISITOS

Para poder realizar las prácticas propuestas en el curso y poder aprovechar los recursos de forma adecuada se recomienda que los alumnos dispongan diversas máquinas virtuales y software instalado. Esta información se proporcionará a los alumnos una vez formalizada la matrícula.

PRECIOS*:

- Importante: exento de IVA para residentes en Canarias o Latinoamérica
- Curso completo en formato individual: 300 euros + IVA
- Curso completo en formato grupo (máximo 5 asistentes): 700 euros + IVA

- Descuentos especiales: La organización podrá aplicar descuentos especiales y adicionales a los descritos en función de consideraciones particulares. Actualmente, se consideran los siguientes descuentos:
- Estudiantes (universidades, institutos y centros de educación, ...) y profesionales acreditados (ISACA, ANCITE, ...): 10% de descuento

* Precios detallados sin contemplar gastos derivados de las transferencias bancarias o transacciones por PayPal o tarjeta de crédito que irán por cuenta del alumno. Todos los gastos ocasionados y derivados del abono del curso irán a cargo del solicitante, en ningún caso la empresa abonará dichos gastos, de ser cargados en la cuenta bancaria de Eventos Creativos la transferencia será devuelta y la reserva del curso cancelada.

INSCRIPCIONES Y MÁS INFORMACIÓN EN EVENTOS CREATIVOS
Info@eventos-creativos.es