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

De Miércoles 1 a Martes 14 de Julio de 2015

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

Impartición: online vía WebEx Duración: 20 horas Certificado CPE de 20 horas, válido para certificaciones profesionales Formato: 2 módulos con diez horas cada uno Fecha: del 1 de julio al 14 de julio de 2015 Días/Horas: Lunes, Martes, Miércoles y Jueves de 16:00 a 18:30 horas (España)

Instructor: D. Pablo González - @pablogonzalezpe (CV al final del documento)

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 (10 horas)

1. Introducción al framework
    a. Arquitectura. Binarios e interfaces
    b. Estructura de archivos del framework: modules, data, external, scripts, tools,…
    c. Adicción y modificación de módulos del framework.
    d. Automatización y configuración del entorno
    e. Comandos básicos
    f. 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
    a. Tipos de explotación y módulos: Explotación directa, Client-Side Explotación local y Fileformat
    b. Atributos y métodos de los módulos
    c. Payloads y configuraciones. Plataformas
        i. Explotación en distintos sistemas: Windows (XP, 7, 8, 8.1), Linux y Servicios multiplataforma
4. Post-Explotación
    a. Funcionalidades. Recolección de información y ámbito
    b. Comandos y módulos de Meterpreter
    c. Inclusión de módulos de Meterpreter
        i. Sessiondump
    d. Más funcionalidades de Meterpreter en un pentesting

Módulo 2. Metasploit Avanzado. (10 horas)

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

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: 350 euros + IVA
- Curso completo en formato grupo (máximo 5 asistentes): 900 euros + IVA
- Coste por módulos en formato individual:
    - Módulo de 10 horas: 200 euros + IVA
- Coste por módulos en formato en grupo:
    - Módulo de 10 horas: 450 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 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

AGENDA. 1 JULIO A 14 JULIO 2015 – 16:00 a 18:30

		Miércoles 1 *de Julio*	Jueves 2 *de Julio*
		Módulo 1	*Módulo 1*
Lunes 6 de Julio	*Martes 7*	*Miércoles 8 de Julio*	*Jueves 9 de Julio*
Módulo 1	*Módulo 1*	*Módulo 2*	*Módulo 2*
Lunes 13 de Julio	*Martes 14 de Julio*		
Módulo 2	*Módulo 2*		

En el caso de no realizarse la formación del módulo 1 es posible, siempre que los matriculados así lo decidan, adelantar el módulo 2 a la primera semana de Julio.

Breve Curriculum del Instructor:

Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja. Ingeniero en Informática por la Universidad Rey Juan Carlos. Ingeniero Técnico en Informática de Sistemas en la Universidad Rey Juan Carlos. Premio al mejor expediente de su promoción en la Universidad Rey Juan Carlos y Premio Extraordinario Fin de Carrera en Ingeniería Técnica en Informática de Sistemas. Trabaja en 11Paths – Telefónica Digital Identity & Privacy como Project Manager. Es docente en el Máster de Seguridad de Tecnologías de la Información y de las

Comunicaciones en la Universidad Europea de Madrid. Trabajó en Informática64 durante 4 años en Formación, Consultoría y Auditoría. Tiene diversas publicaciones en el ámbito de la Seguridad de la Información:

- Autor del libro Metasploit para Pentesters. Editorial 0xWord. 1ª ed. 2012, 2ª ed. 2013 y 3ª ed. 2014.
- Autor del libro Ethical Hacking: Teoría y práctica para la realización de un pentesting. Editorial 0xWord.
- Autor del libro Pentesting con Kali. Editorial 0xWord.
- Autor del libro Powershell: La navaja suiza de los administradores de Sistemas. Editorial 0xWord 2012.

Pablo ha impartido formación en Rooted CON 2013, 2014 y 2015 con Metasploit Labs y Hacking de dispositivos iOS. También ha sido docente en los Labs de No cON Name 2013 y 2014 con Metasploit para Pentesters. Ha sido ponente en Rooted CON 2013 y 2014, No cON Name 2011, Navaja Negra 2014 y otros congresos como Hackron, Sh3llCon, Qurtuba Security Congress, Cybercamp o Rooted Valencia, entre otros. Ponente en congresos internacionales como la 8dot8 celebrada en Chile en 2014 o el IEEE SBS Gold en 2012.