Hacking con Python

FOLLETO INFORMATIVO DEL CURSO

OBJETIVOS

- Explicar los conceptos básicos de programación estructurada y orientada a objetos con el fin de que los estudiantes sepan en qué momento conviene más utilizar cualquiera de los dos enfoques.

- Explicar los principales elementos que es necesario conocer para poder crear herramientas plenamente funcionales con Python.

- Enseñar cómo se pueden crear scripts en Python para automatización de tareas enfocadas a tareas de pentesting.

- Dar a conocer las principales librerías disponibles en Python a la hora de desarrollar herramientas enfocadas a la seguridad informática.

- Enseñar buenas prácticas sobre el desarrollo de programas con Python.

PERFIL ALUMNO

Estudiantes y profesionales que deseen aprender o mejorar sus conocimientos en programación y pentesting utilizando lenguaje Python.

CONTENIDOS

1. Recolección de información y aplicación de técnicas OSINT.

- Procesos de recolección de información básicos con Python.

- Utilizando Python para el acceso programático a los servicios de Google.

- Utilizando Python para el acceso programático a los servicios de Twitter.

- Utilizando Python para el acceso programático a Shodan.

- Consultas a servicios DNS y WHOIS.

- Geolocalización con Python y GoogleMaps.

- Geolocalización con PyGEOIP.

- Análisis de metadatos en imágenes.

- Análisis de metadatos en documentos PDF.

2. Escaneo, enumeración y actividades de pentesting.

- Tipos de escaneos en redes.

- Análisis de paquetes y escaneos con Scapy.

- Uso avanzado de Scapy para manipulación y reinyección de paquetes.

- Uso de Scapy para realizar ataques de ARP Spoofing.

- Uso de Scapy para realizar ataques de DNS Spoofing

- Enumeración con Python-nmap.

- Librerías comunes en Python para la creación de clientes HTTP.

- Parseo y extracción de contenidos de aplicaciones web con BeautifulSoup.

- Scraping de aplicaciones web con Scrapy.

- Detección de vulnerabilidades en aplicaciones web con Python.

- Pentesting sobre servicios FTP utilizando FTPLib

- Pentesting sobre servicios SSH/SFTP utilizando Paramiko

- Creación de túneles cifrados y redirección de puertos con Paramiko.

- Pentesting de servicios SMTP.

- Pentesting de servicios SMB con PySMB.

- Integración de Python con Metasploit Framework.

DATOS DE IMPARTICIÓN DEL CURSO

Nº horas: 8

Material y recursos didácticos a utilizar:

El alumno recibirá el material fungible necesario para el correcto desarrollo del curso, incluyendo un manual teórico y ejercicios prácticos de cada módulo.

DIPLOMA / CERTIFICADO: Certificado de carácter privado no oficial. Aquellos participantes cuyo expediente se tramite a través del sistema de formación continua bonificada podrán descontar el importe correspondiente en las aportaciones a la seguridad de la empresa y

recibirán un certificado expedido por la Fundación Tripartita.

PROFESORADO

Profesorado titulado y especializado en la materia. Cuenta asimismo con formación metodológica y experiencia docente

OTROS DATOS

Este curso forma parte de la oferta formativa permanente de Instituto Alcántara prevista para el curso 2016-2017.

INSTITUTO ALCÁNTARA, S.L.
C/ CRUZ CONDE, 19, 1ª PLANTA
14001 – CÓRDOBA
TELÉFONO: 957 48 14 34