Python para Hackers

CloudLamb
E-Learning

Yunuen Lucatero

Experiencia

- Bug Bounty (HackerOne)
- Consultor de seguridad (México)
  - Minsait (Indra)
  - Scitum (Telmex)

Certificaciones

- GPEN | GWAPT | CHFI

Hobbies

- CTF (Ex Mayas Team Member | CyberWomen Challenge Chile - 3er lugar)
- Blogger (ocasional)

yunniscan

enigmagirl.com

CloudLamb E-Learning

¡Cuéntenme sobre ustedes!

¿Cuál es tu nombre?

¿Porqué quieres aprender Python?

¿De dónde eres?

¿Tienes alguna experiencia programando?

¿Cuáles son tus expectativas de este curso?

¿Cuál es el tema que más te interesa aprender?

CloudLamb E-Learning

Python para Hackers

Contenido del curso

Capítulo 1. Introducción

Python para Hackers | Ethical Hacking | Conceptos básicos

Capítulo 2. Primeros pasos

Instalación de Python | PyCharm | PyPI | Pip

Capítulo 3. Python

Tipos de datos y variables | Operadores | Cadenas | Condicionales | Bucles | Funciones | Clases y Objetos | Módulos | Archivos | Sockets

Capítulo 4. Hands-On

Ataques de diccionario | Web Server | Web Scraping | Fuerza bruta de Directorios Web | Fuerza bruta a formularios de autenticación (web) | Servidor/Cliente TCP | Banner Grabbing | Reconocimiento de máquinas | Nmap con Python | Packet Sniffing con Scapy | Paramiko (Cliente SSH)

Python para Hackers

Game Rules

Clases

- Cada martes/jueves
- 8:00 – 10:00 P.M. (Hora Chile)

- Teoría / Práctica

Grupo de WhatsApp

- Notificaciones
- Recordatorios de clases/exámenes
- Resolución de dudas

Plataforma Cloud-Lamb

- Diapositivas
- Material de apoyo
- Calificaciones

Evaluaciones

- 4 exámenes en total
  - 3 exámenes teóricos (en línea)
  - 1 examen práctico

Laboratorio

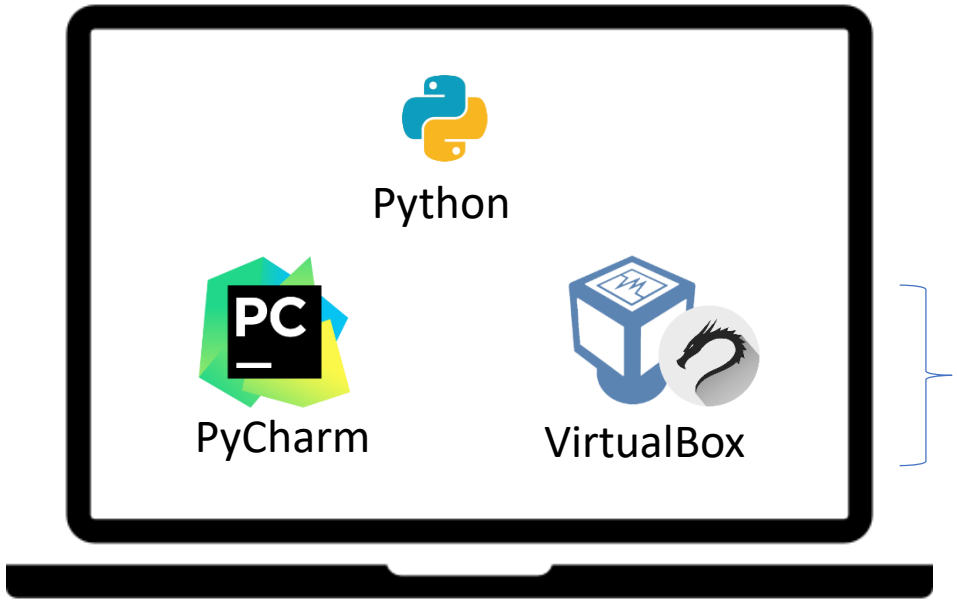
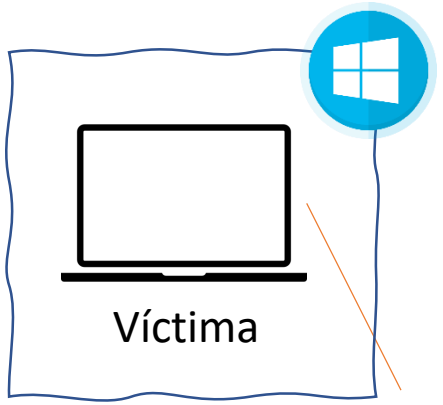


Imagen de Kali Linux para VirtualBox



Internet

Herramientas

VirtualBox (108 MB)
https://www.virtualbox.org/wiki/Downloads

Python para Windows (25.3 MB)
https://www.python.org/downloads/

PyCharm para Windows (295 MB)
https://www.jetbrains.com/es-es/pycharm/download/#section=windows

Kali Linux (1.8-2.1 GB)
https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

CloudLamb E-Learning

Python para Hackers

Contenido del curso

Capítulo 1. Introducción *Tema de hoy*

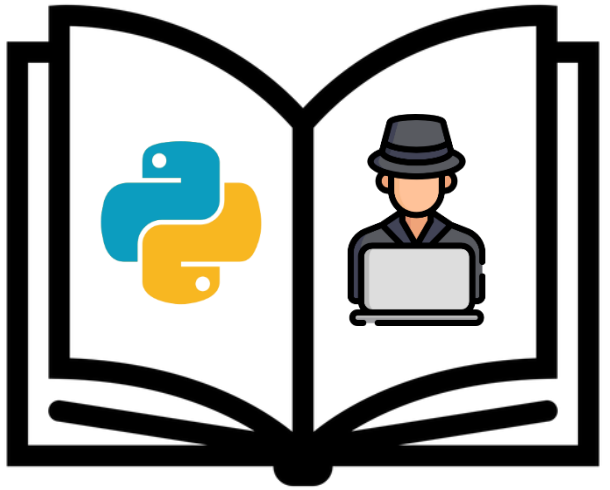
Python para Hackers | Ethical Hacking | Conceptos básicos

Capítulo 2. Primeros pasos

Capítulo 3. Python

Capítulo 4. Hands-On

Capítulo 1. Introducción



CloudLamb E-Learning

¿Qué es Python?

Es un **lenguaje de programación interpretado** que soporta programación orientada a objetos, imperativa y funcional.

Python se puede utilizar para programar aplicaciones de escritorio, aplicaciones web o para tareas de automatización.

CloudLamb E-Learning

Lenguaje interpretado

Al ser un lenguaje interpretado significa que es el código es **convertido a lenguaje máquina a medida que este se ejecuta**.

```
package main

import "fmt"

func main() {
  fmt.Printf("hello, world")
}
```

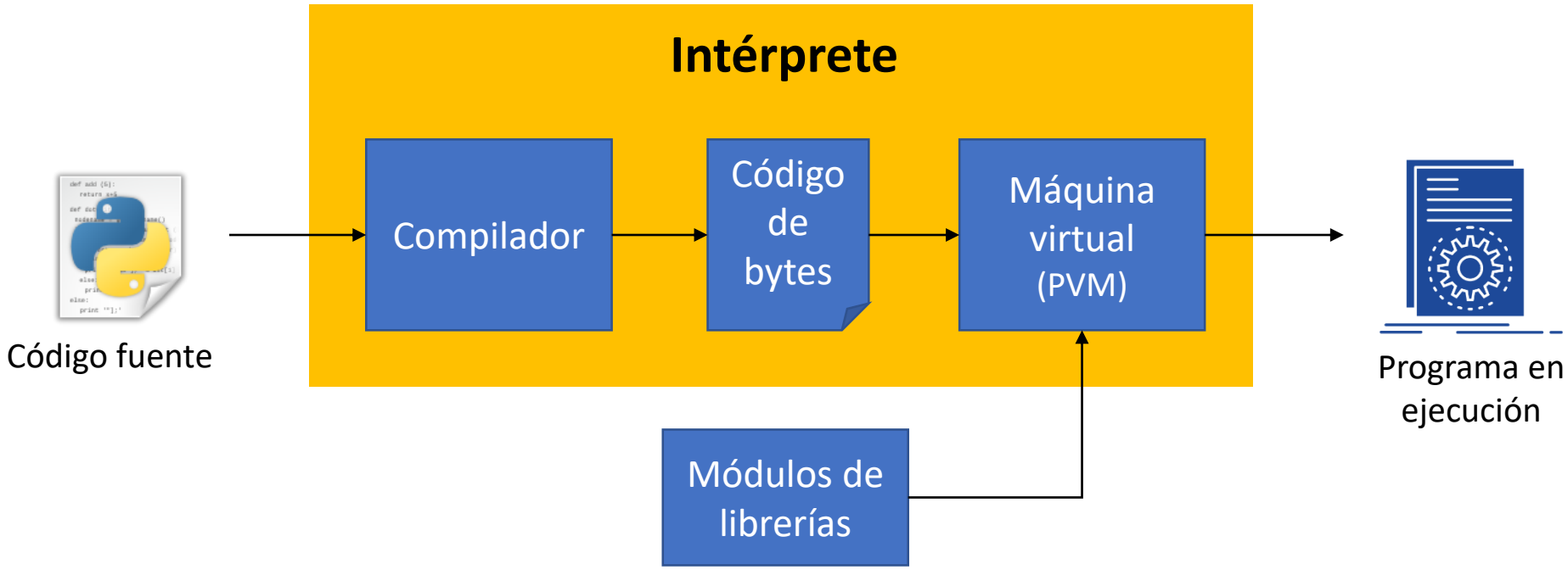
```
01010101111011100011010
01000101000101010010100
01010100101010100001010
00110100010101000111100
01100101001010101010010
11100011010100100100010
```

Lenguaje de alto nivel que entiende un programador

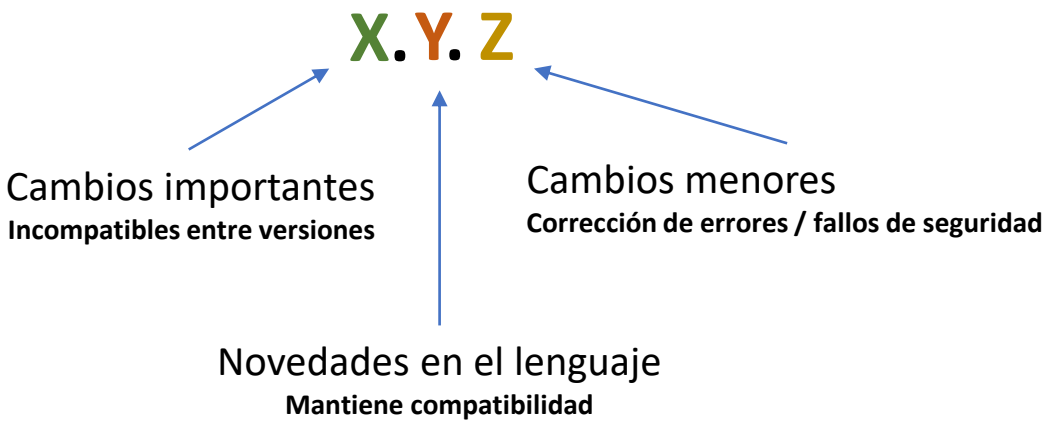
Lenguaje de máquina que entiende el procesador

Lenguaje interpretado

Al ser un lenguaje interpretado significa que es el código es **convertido a lenguaje máquina a medida que este se ejecuta**.



Versiones



Versión 2.0
2000

Versión 3.0
2008

Cambios en el lenguaje

- Incompatibilidad con versiones 2.X
- Poca disponibilidad de librerías (PyPI)

Versión 2.7
2010

Incorpora algunas características de Python 3

Versión 3.8.2
2020

Versión 2.7.18
2020

Características del lenguaje

Multiplataforma

- Mac OS X
- Windows
- Linux
- Unix

Orientado a objetos

- Clases
- Métodos y atributos

Software libre

- Descarga gratuita

Librerías estándar que permiten:

- Conectarse a servidores
- Realizar búsquedas en archivos con expresiones regulares
- Manipulación de archivos (lectura o escritura)
- …

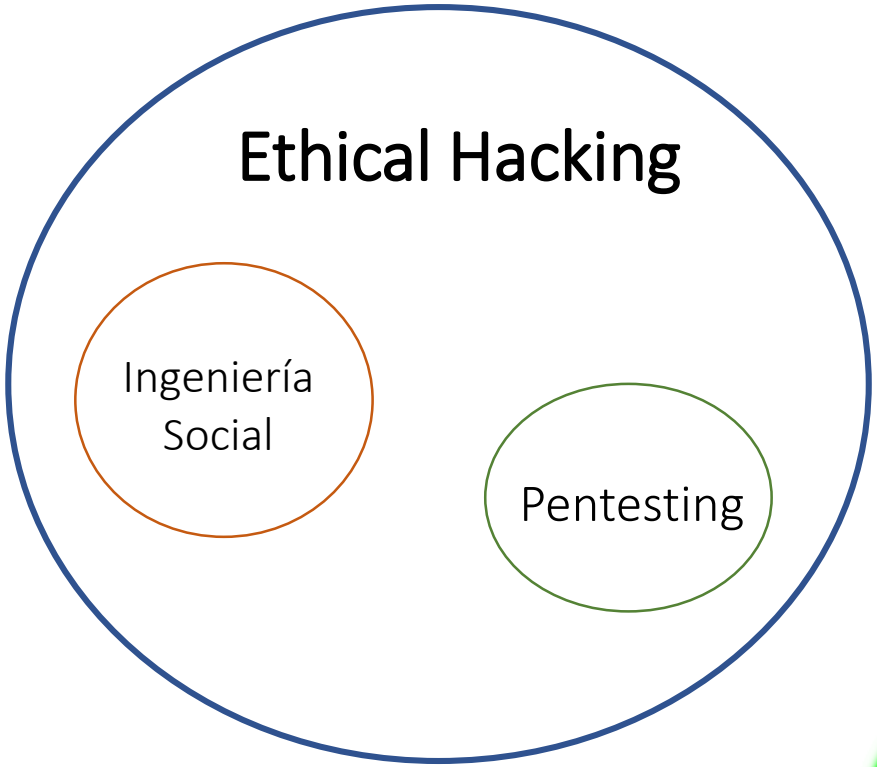
Fácil de aprender y usar!

¿Qué es Ethical Hacking?

Son técnicas que se emplean para **evaluar** dispositivos, sistemas informáticos o personas con el objetivo de **identificar vulnerabilidades, explotarlas** y determinar el riesgo/impacto que tiene para una organización.

CloudLamb E-Learning

Ethical Hacking



Metodología de Pentesting

Identificación de activos. Recopilación de información de aspectos técnicos (puertos, servicios, dominio, rangos de red, etc.).

Validación de vulnerabilidades identificadas para descartar falsos positivos, ponderación de riesgos y obtener mayor información del activo y entorno de red.

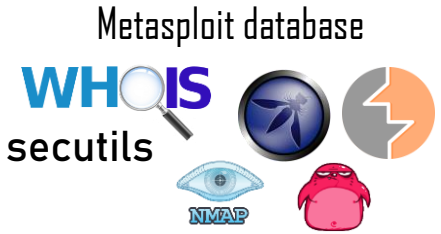
Reconocimiento

Descubrimiento & Enumeración

Análisis de vulnerabilidades

Explotación

Búsquedas pasivas para identificar información de la organización en fuentes públicas.



Identificar vulnerabilidades que afectan a los activos.

Conceptos básicos

Ataque / Explotación

Aprovecharse de alguna vulnerabilidad o debilidad para obtener acceso sin autorización o extraer información de un sistema informático.

Amenaza

Es un **actor o agente** que puede causar daño.

Vulnerabilidad

Es una **falla** que tiene un sistema informático la cual puede ser aprovechada para extraer información, causar algún daño, etc.

Riesgo

Es la **probabilidad** de que una amenaza aproveche una vulnerabilidad.

Conceptos básicos

Triada de la seguridad (CIA)

Son los **principios básicos** de la seguridad de la información los cuales utilizan diversos mecanismos de seguridad para protegerlos.

Confidencialidad: Es la propiedad de mantener segura la información ante *accesos no autorizados* y que sólo sea accesible por las personas o sistemas que tengan autorización.

Integridad: Propiedad cuyo objetivo es conservar la exactitud y completitud de la información, protegiéndola de cambios, eliminación o creación no autorizados.

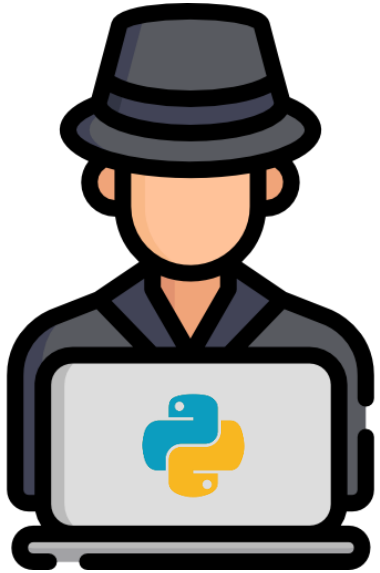
Disponibilidad: Propiedad que establece que un activo debe de ser accesible para las personas autorizadas cuando sea requerido.

Confidencialidad
Cifrado / Descifrado

Integridad
Hash
MAC
Firmas digitales

Disponibilidad
No usa criptografía

Uso de Python en Ethical Hacking



Una de las características principales de Python es la facilidad que tiene para usar librerías que permiten el **desarrollo de scripts especializados** para las actividades de Ethical Hacking.

Próxima clase...

- **Capítulo 2:** Primeros pasos

CloudLamb
E-Learning

CloudLamb E-Learning

CloudLamb

¡Muchas gracias por su atención!