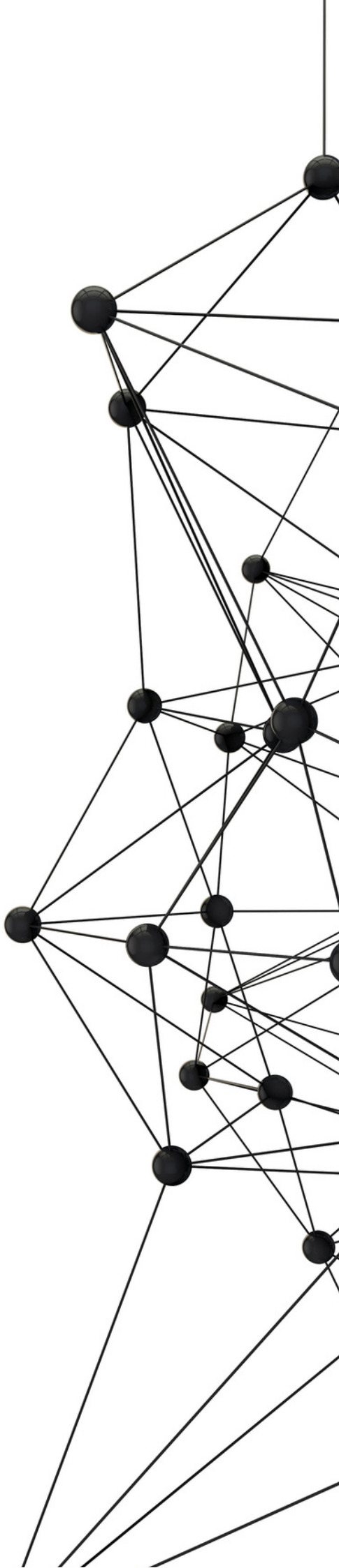
Curso Basico de Hacking

Temario del Curso



DSPWPCv3 IA

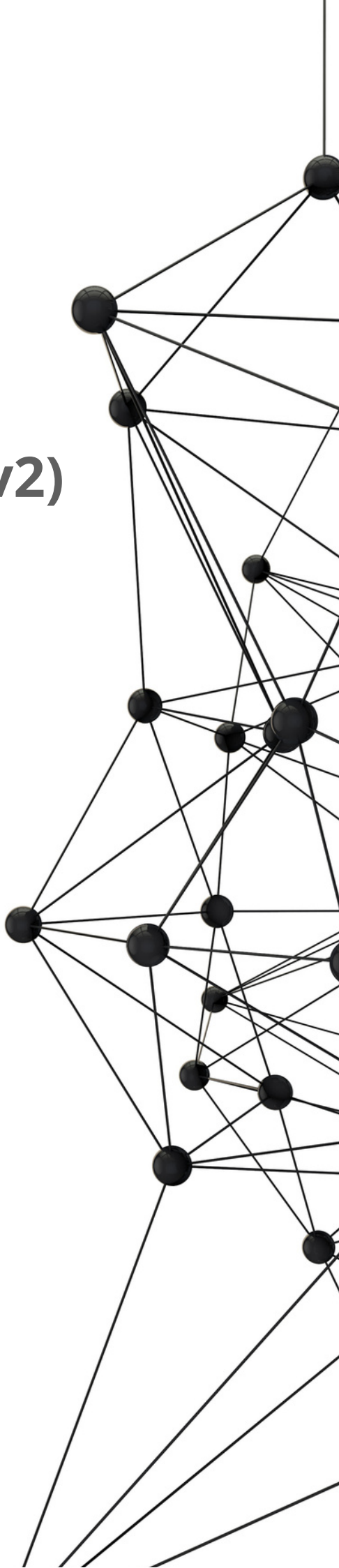
DeepSec Pentesting Web Python Course v3

INTRODUCCION

DeepSec Pentesting Web Python Course (DSPWPCv2)

En este curso se aprenderán las bases de Linux y el hacking ético, aprendiendo diversas técnicas en **RED TEAM** y **BLUE TEAM**.

El cursante aprenderá a aplicar los conocimientos de Python en una variedad de técnicas adentrándose en el área de la seguridad informática y programación de la manera correcta como también el manejo de IA para realizar pruebas de penetración. El cursante podrá observar y aplicar su conocimiento en laboratorios otorgados por el docente, lo cual permitirá que el cursante asimile lo que sucede por detrás al implementar una técnica.



DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

CARACTERISTICAS

¿A quien va dirigido el curso?

Este curso esta diseñado para aquellos que van introduciendose en la seguridad informatica y en Linux, y desean adquirir contenido de valor que no se encuentra en cualquier lado. El objetivo es hacerte ver otra perspectiva de la seguridad informatica la cual es no solamente implementar una tecnica con herramientas automatizadas, sino que tu desarrolles tus propias herramientas.

Duracion del Curso

La duración del curso "DeepSec Pentesting Web Python Course v3" es de veinte días los cuales cada día se darán dos horas de clase los dias martes, jueves y sabado

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

CARACTERISTICAS

Objetivos del Curso

- Manejo de IA para el pentesting
- Dominio de programación en Python
- Dominio de Python para hackers
- Dominio de técnicas de pentesting
- Conocimiento desarrollado de vulnerabilidades

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

CARACTERISTICAS

Requisitos

- Computadora con minimo 4gb de ram
- Computadora con acceso a Internet
- Intel i3 minimo o Ryzen 3 2200
- Ganas de aprender

¿Qué no tiene el curso?

- Restricción de Edad
- Restricción de País
- Necesidad de conocimientos previos al hacking
- Necesidad de conocimientos previos a Linux
- Necesidad de conocimientos en programacion

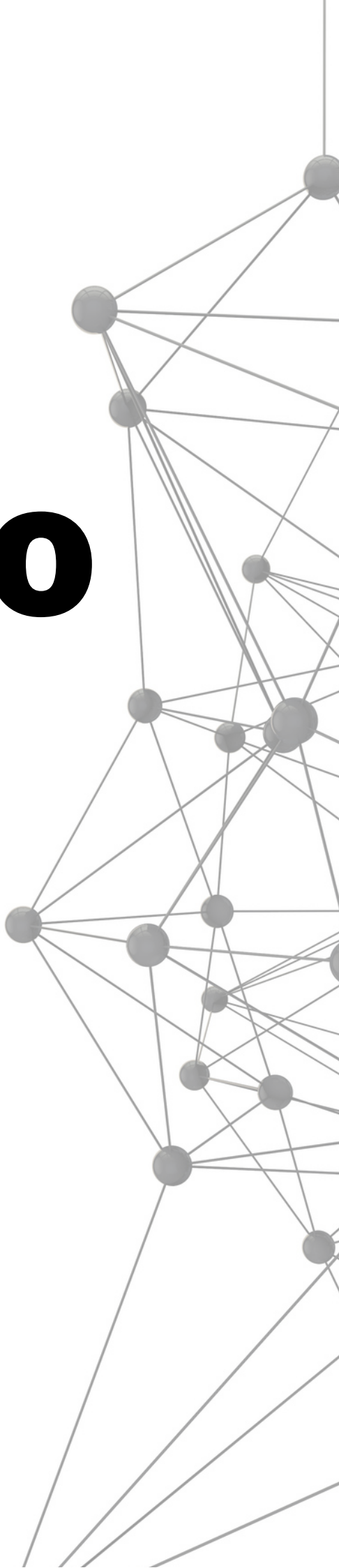
¿Qué incluye?

- Acceso al curso
- Acceso al temario completo
- Acceso al grupo privado del curso
- Constante seguimiento de material nuevo
- Atención personalizada con el instructor

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Temario

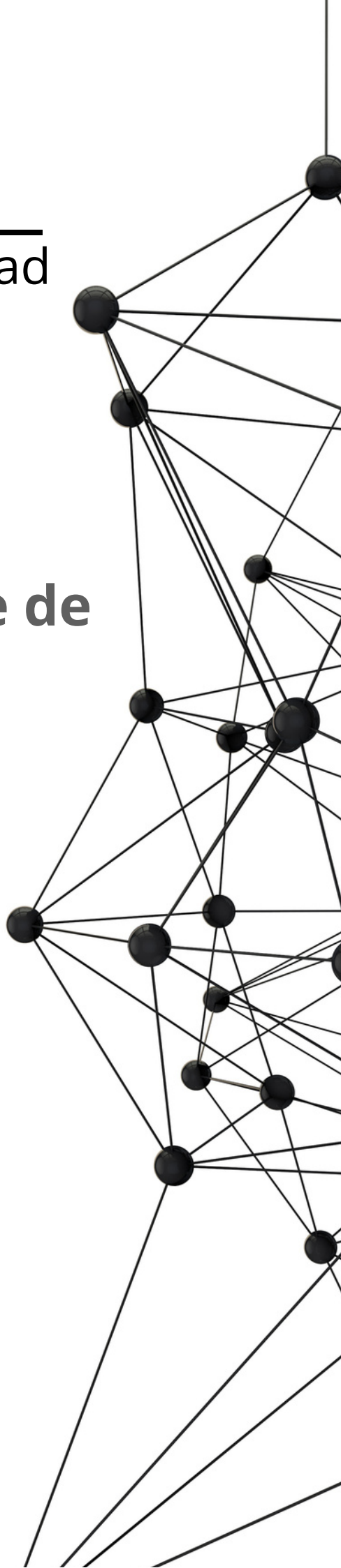


DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 1

Introduccion a la ciberseguridad



Presentacion

- Bienvenida al curso
- Conociendo al Profesor
- Establecimiento de normas de la clase

Introduccion y Despliegue de laboratorio

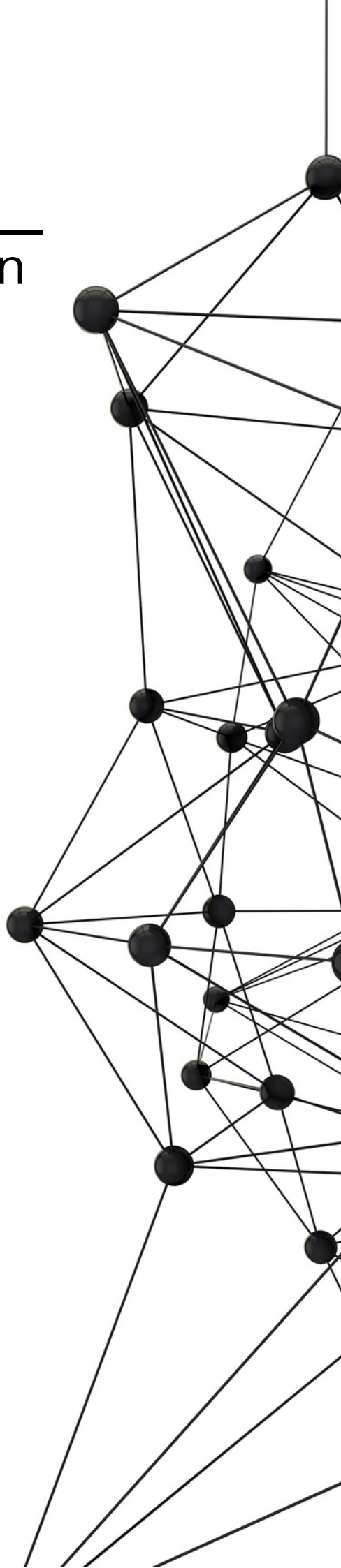
- ¿Por qué Python para hackers?
- Terminología de ciberseguridad
- Ramas de la seguridad informática
- Habilidades a desarrollar
- Fases del Pentesting
- Como usar la IA para hacer pentesting?
- Instalación de VMware/Virtual Box
- Instalación de Kali Linux/Parrot Os
- Instalación de Docker
- Instalación de Metasploitable 2
- Instalación Packet Tracer
- Instalación de vamAPI
- Creación cuenta en PortSwinger
- Instalacion Visual Code

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 2

Introduccion a la Programacion



Linux Basics

- Comandos básicos de la terminal
- Desplazamiento
- Creación de Ficheros
- Permisos
- Shebang
- Editores de Texto

Programacion en Python

- Tipos de Datos
- Estructuras condicionales
- Estructuras repetitivas
- Estructura de datos: Arrays
- Estructura de datos: Matrices
- Programacion Orientada a Objetos
- Estructura de datos diccionario
- Conociendo mas estructuras de datos
- Uso de la IA Codium

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 3

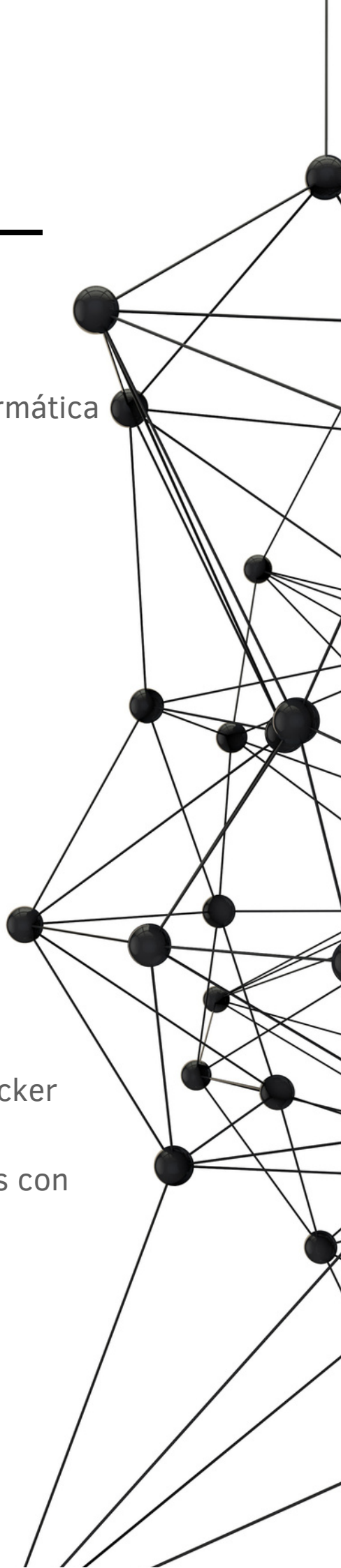
Python y Redes

Introduccion a Redes

- Importancia de las Redes en Seguridad Informática
- Redes un enfoque ascendente
- Modelo OSI y TCP
- ARP/NDP
- IPV4 y IPV6
- Subneting IPV4
- Direccionamiento IPV6
- Capa de Transporte
- TCP/UDP/QUICK
- Manejo de Wireshark
- Sniffing
- Arp Spoofing con Scapy

Docker

- Introducción a docker
- Despliegue de contenedores en Play with Docker
- Manejo de docker
- Automatizacion de creacion de contenedores con IA



DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 4

Reconocimiento y Explotacion

API Nmap

- Escaneo de puertos TCP
- Escaneo de puertos UDP
- Scripts de nmap
- Escaneo de vulnerabilidades
- Automatización de escaneo en toda la red
- Uso avanzado de Nmap

Busqueda de Exploits

- Modulos de busqueda de exploits
- Explotacion de servicios vulnerables

Ataques a Puertos Comunes

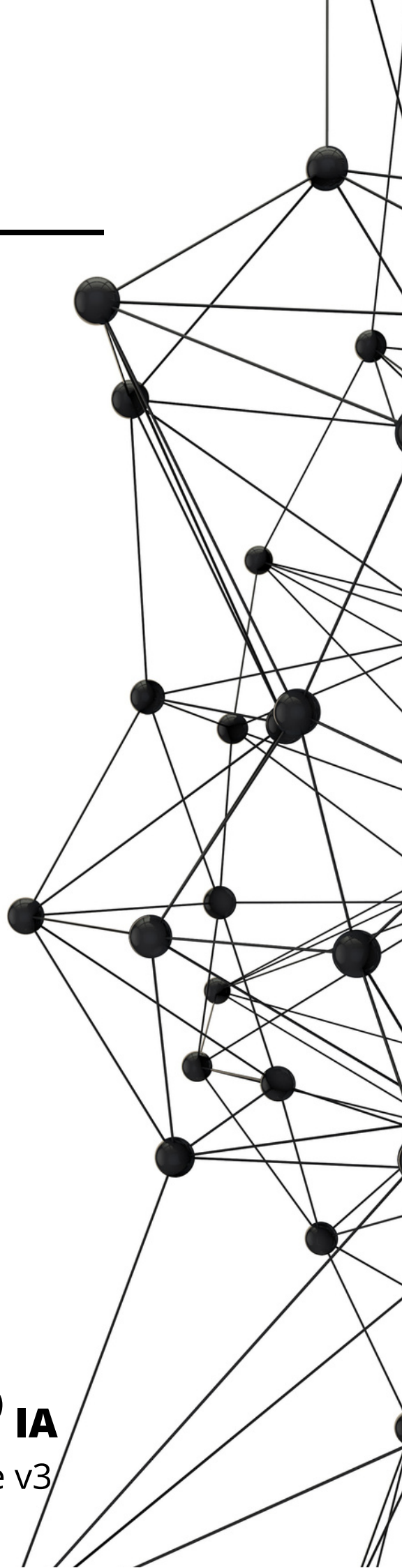
- Uso de la libreria ftplib
- Force Brute Attack FTP
- Explotacion de vulnerabilidades en FTP
- Uso de la libreria ssh2-python
- Force Brute Attack SSH
- Uso de la libreria paramiko
- Cifrado Asimetrico
- Evasion de Firewall desde IPV6 a SSH

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 5

Python y Redes 2 y Web



Basics Web 1

- Introducción a HTML
- Introduccion a CSS
- Introduccion a JS
- Uso del Framework Flask
- Creación de laboratorio
- Creacion Automatica de sitio web Frontend/Backend con IA

Basics Web 2

- Uso de la librería request en python
- Cabeceras HTTP
- Códigos de estado
- Envió de peticiones GET/POST
- Introducción a Fuzzing
- Creacion de Fuzzer
- Creacion automatica de herramientas de escaneo con IA

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 6

Pentesting Web 1

Cookie Hijacking

- Introducción a las cookies
- Set y Get de cookies en Flask
- CSRF
- Manejo de JWT en python
- Modificación del Laboratorio
- HTML Injection
- Cross Site Scripting Attack
- Cookie Hijacking
- Creación de Server en Python para extracción de cookies

Server Side Template Injection

- Introduccion a SSTI
- Modificacion de Laboratorio
- Local File Inclusion
- Aplicando ataque SSTI

DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 7

Pentesting Web 2

Reverse Shell's

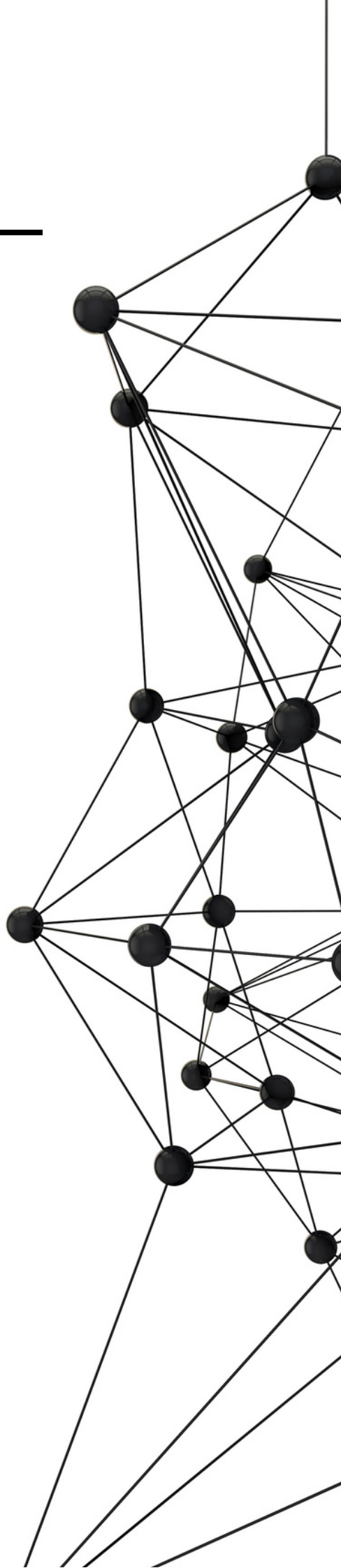
- Sockets en Python
- Creacion de listerner en Python
- Creacion de RevShell en Python
- Creacion de BindShell en Python
- ICMP Reverse Shell

Data Bases

- Introduccion a las base de datos
- Instalacion de sqlite3
- CRUD en sqlite3
- Python y Sqlite3
- SQL Injection
- Bypass Login con SQLi

Desearilization Attack

- Recapitulacion de POO
- Serializacion de Objetos
- Desearilizacion de Objetos
- Ataque de Desearilizacion



DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3

Modulo 8

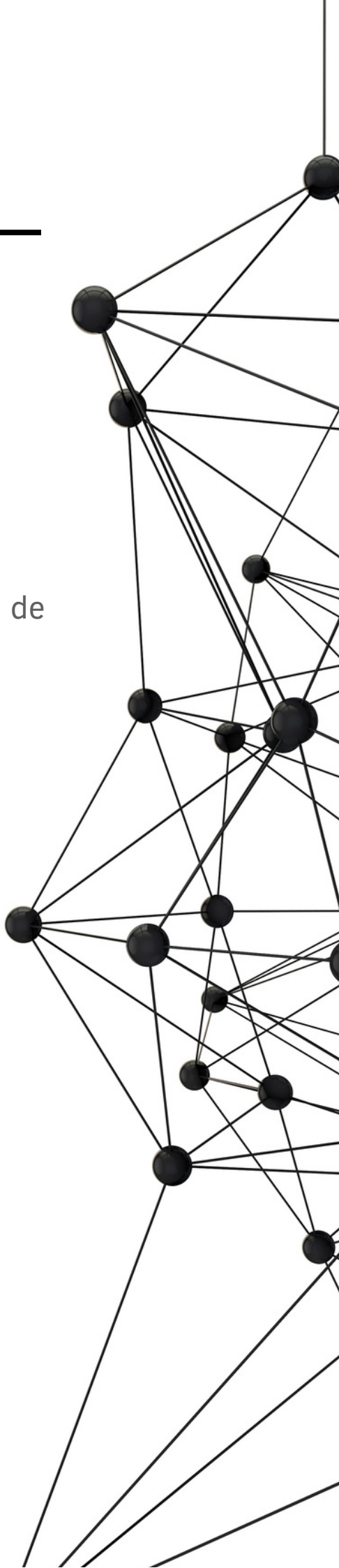
Pentesting Web 3

Pentesting en REST API

- SQLi Injection en un server con REST API
- Unauthorized Password Change
- Broken Object Level Authorization
- Mass Assignment
- Excessive Data Exposure mediante un Debug de un endpoint

Preparación para el Examen

- Automatizacion de explotacion con Python para maquinas de DeepSec Academy
- Automatizacion de explotacion con Python para maquinas de Vulnhub



DSPWPCv3 IA

DeepSec Pentesting Web Python Course v3