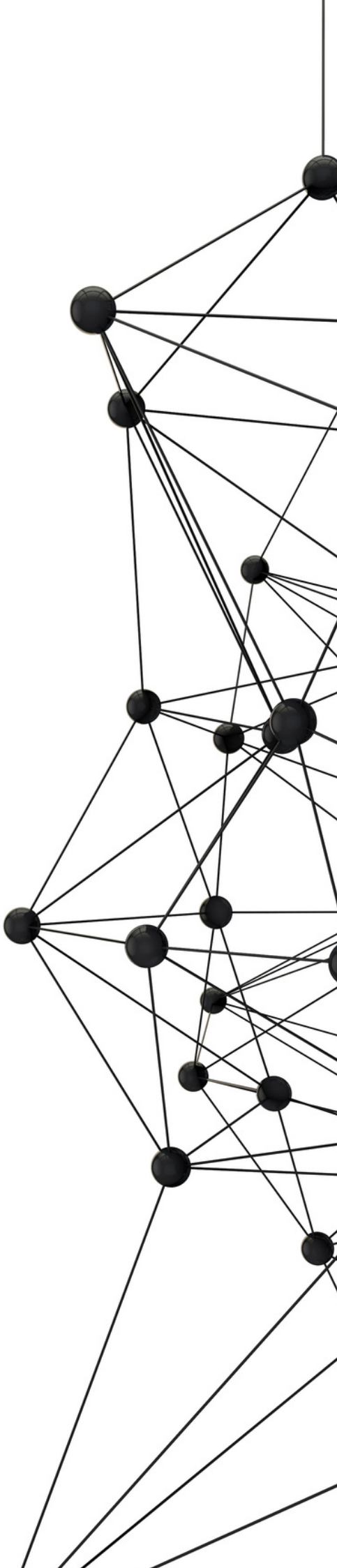
Curso Basico de Hacking

Temario del Curso



LOHPA

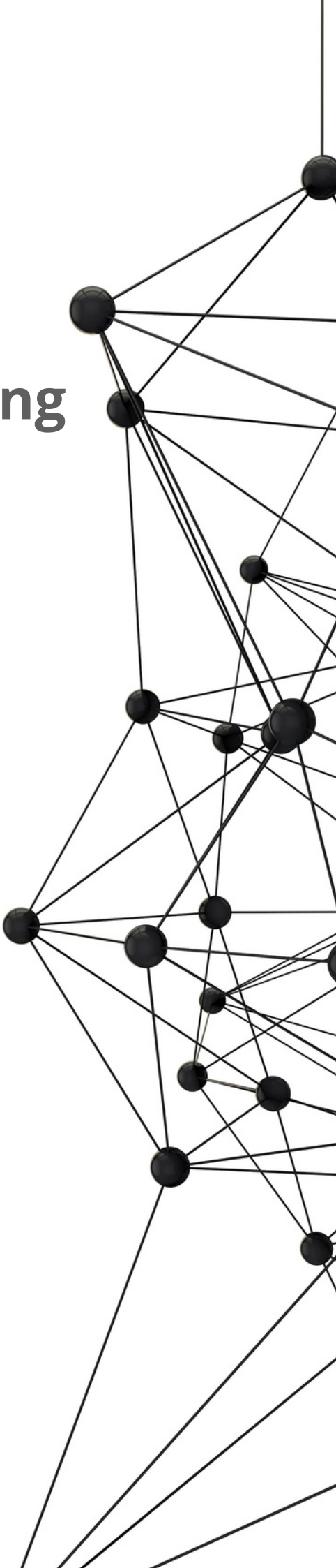
Linux Orientado al Hacking y Pentesting

INTRODUCCION

Linux Orientado al Hacking y Pentesting (LOHP)

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 Linux en una variedad de técnicas adentrándose en el área de la seguridad informática y programación de la manera correcta. El cursante podra observar y aplicar su conocimiento en laboratorios otorgados por el docente, lo cual permitira que el cursante asimile lo que sucede por detras al implementar una tecnica.



LOHP

Linux Orientado al Hacking y Pentesting

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 "Linux Orientado al Hacking y Pentesting" es de veinte y cinco días los cuales cada día se darán tres horas de clase consecutivas.

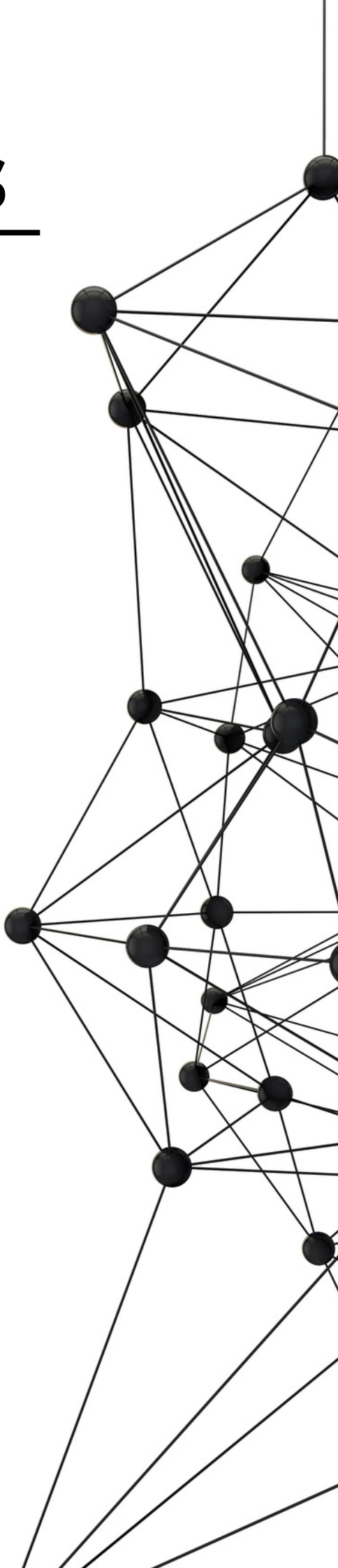
LOHPA

Linux Orientado al Hacking y Pentesting

CARACTERISTICAS

Objetivos del Curso

- Manejo de sistemas Linux
- Dominio de la terminal
- Dominio de programacion en Bash
- Comprension de la metodologia de Pentesting
- Comprensión de estructuras de Redes
- Dominio en Escalacion de Privilegios
- Comprension en implementacion de servidores
- Uso de la IA para la ciberseguridad



LOHPA

Linux Orientado al Hacking y Pentesting

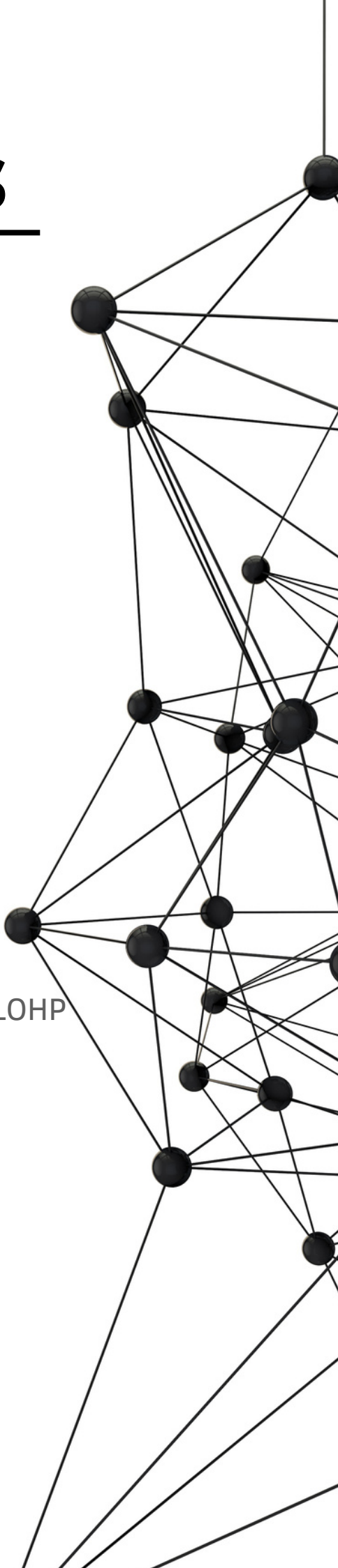
CARACTERISTICAS

Requisitos

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

¿Qué incluye?

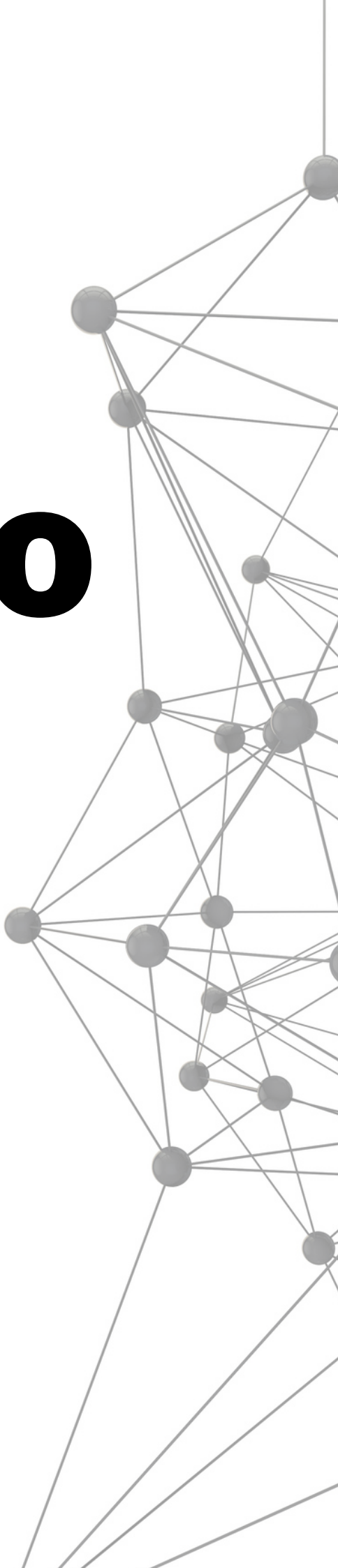
- Acceso al curso
- Acceso al temario completo
- Acceso a los laboratorios
- Acceso al grupo privado del curso
- Constante seguimiento de material nuevo
- Atención personalizada con el instructor
- 1 Voucher para el examen de certificacion LOHP



LOHP

Linux Orientado al Hacking y Pentesting

Temario



Modulo 1

Introduccion a la ciberseguridad

Presentacion y Introduccion

- Bienvenida al curso
- Conociendo al Profesor
- Establecimiento de normas de la clase
- Historia de Linux
- Entornos de Linux
- Funciones escenciales del sistema GNU/LINUX
- ¿Porque Linux es SO para hackers?
- Filosofia del software libre
- Inteligencia Artificial en Pentesting
- Etica en el uso de IA
- Habilidades a desarrollar
- OWASP Top 10 para LLM Apps
- LLM01: Prompt Injection
- LLM05: Supply Chain Vulnerabilities

Despliegue de laboratorio

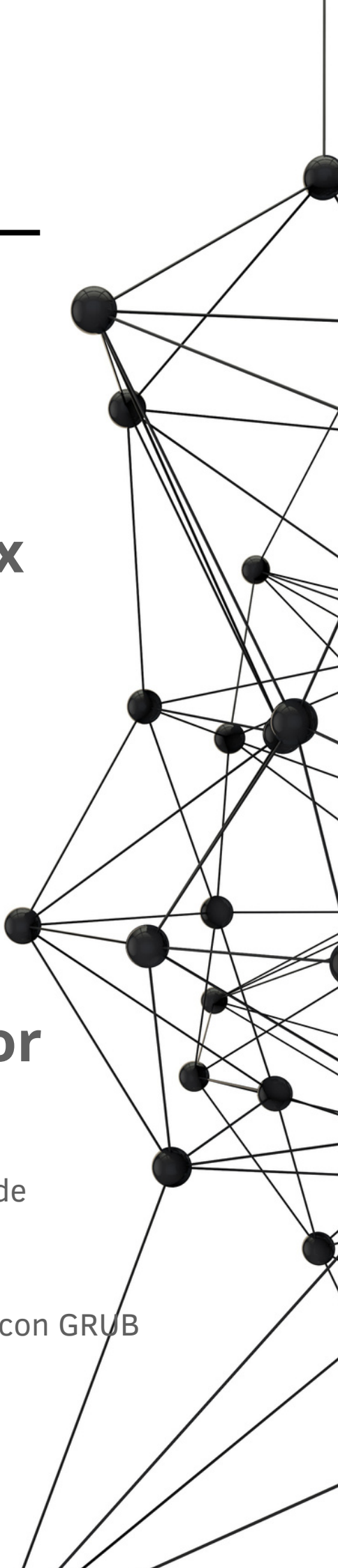
- Instalacion de Vmware/Virtual Box
- Instalacion de Kali Linux/Parrot Os
- Instalacion de Metasploitable 2

LOHPA

Linux Orientado al Hacking y Pentesting

Modulo 2

Fundamentos de Linux Parte 1



Configuracion Basica

- Proceso de Instalacion (overview)
- Primeros pasos y configuraciones esenciales

Particionamiento en Linux

- Tipos de particiones (ext4, swap, etc)
- Herramientas de particionamiento

Gestion de Paquetes y Software

- Sistemas de gestion de paquetes (apt, yum, pacman)
- Instalacion y actualizacion de software

Configuracion del Cargador de Arranque GRUB

- Que es GRUB y su importancia en el arranque de sistemas operativos
- Instalacion y configuracion basica de GRUB
- Solucion de problemas comunes relacionados con GRUB

LOHP

Linux Orientado al Hacking y Pentesting

Modulo 3

Conociendo al Sistema Parte 2

Customización

- Instalacion y uso de bspwm
- Instalacion y uso de polybar
- Cambiando la polybar
- Instalacion y uso de sxhkd
- Configurando atajos en sxhkd
- Instalacion y uso de Rofi
- Tipos de terminales (Alacritty, Gnome-Terminal, etc)

Usuarios y Grupos

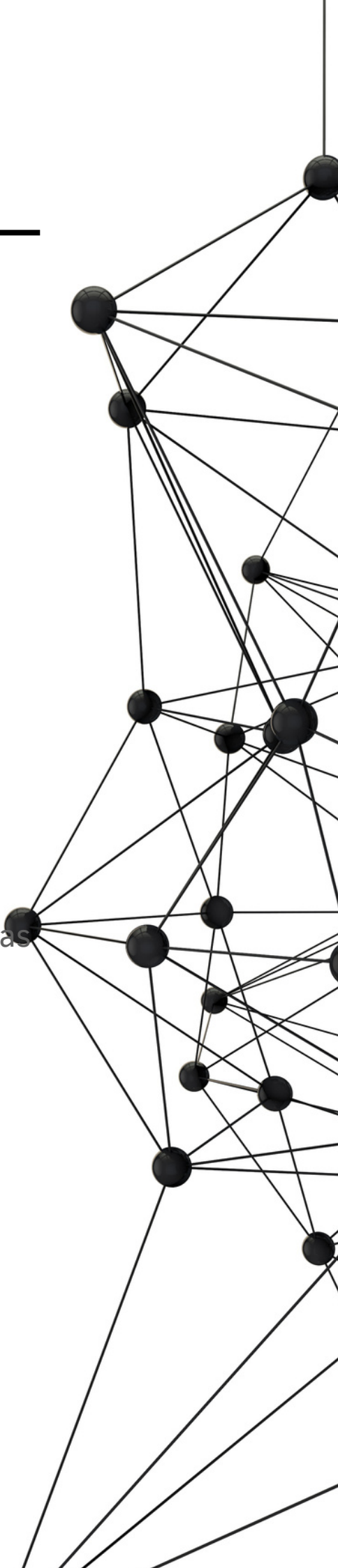
- Creacion de usuarios con herramientas
- Creacion de grupos con herramientas
- Estructura de /etc/passwd y /etc/shadow
- Desencriptacion de shadow con John y Hashcat
- Extraccion de credenciales de firefox
- Creando y modificando un usuario desde 0 sin herramientas
- Administracion de Permisos

LOHP

Linux Orientado al Hacking y Pentesting

Modulo 4

Conociendo al Sistema Parte 2



Sudoers

- Uso de sudoers
- Estructura del fichero /etc/sudoers
- Abuso de sudoers
- Buenas practicas para el uso de sudoers

SUID

- Permisos SUID, GUID y Sticky Byte
- SUID Explotation

Ficheros y enlaces

- Creacion y modificacion de ficheros y carpetas
- Copiar y Mover
- Creacion de Hard Links y Soft Links
- Compresion y decompresion de ficheros

LOHP

Linux Orientado al Hacking y Pentesting

Modulo 5

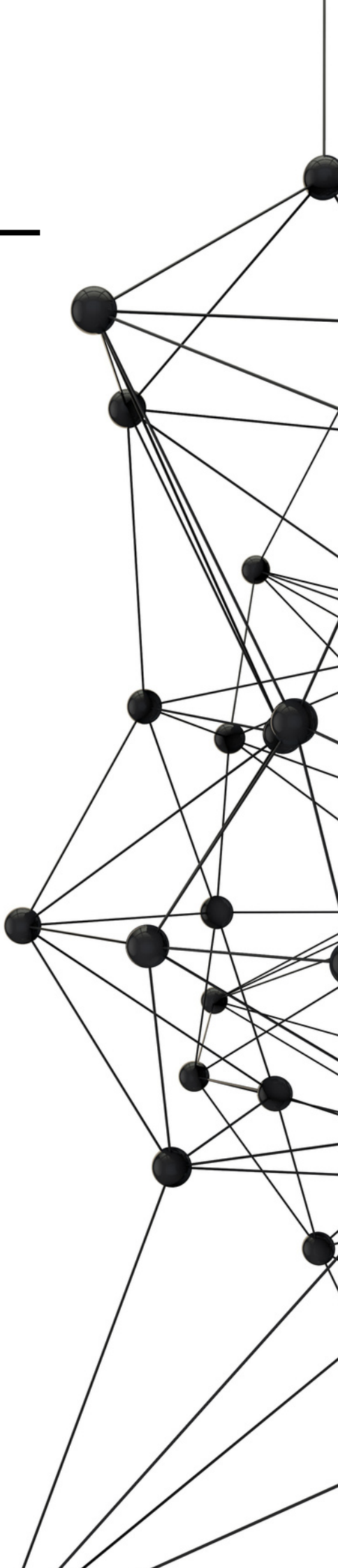
La vida de un programa

Programación básica en C

- Variables
- Condicionales
- Ciclos For y While
- Funciones propias de C
- Análisis de librerias dinamicas y estaticas
- Observando el funcionamiento de programa siendo ejecutado
- Mi primer modulo para el Kernel Linux

Buffer Overflow y Suplantacion de Librerias

- SUID explotation segunda parte
- Path Hijacking
- Debugeando con gdb
- Buffer Overflow Stack Based
- Hijacking Dynamically Linked Shared Object Library



LOHP

Linux Orientado al Hacking y Pentesting

Modulo 6

Redes y Conexiones

Modelo TCP/IP

- Redes al día de hoy
- Modelo Referencial OSI
- ¿Como funciona Internet?

Capa de Enlace de Datos

- Direccionamiento MAC
- Protocolo ARP

Capa de Red

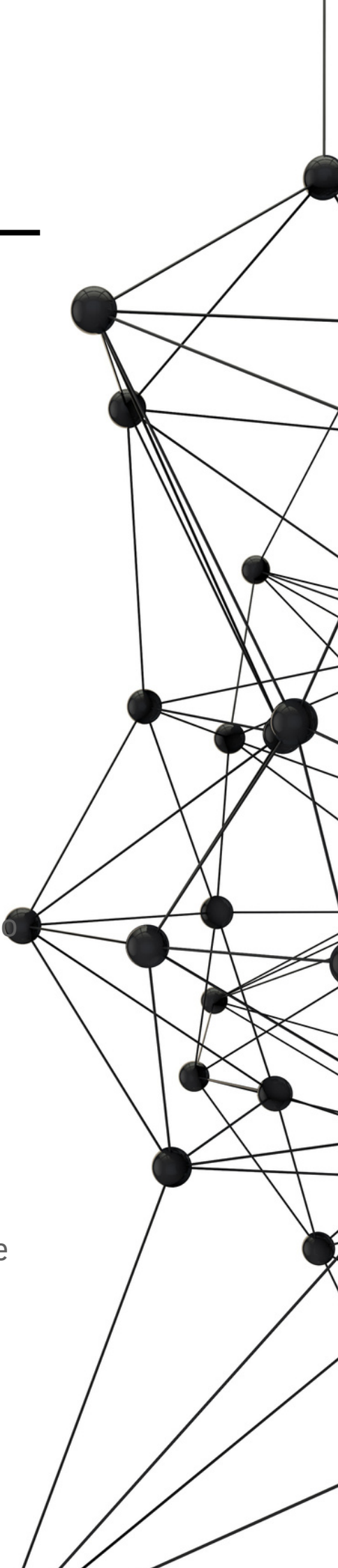
- Direccionamiento IPV4, IPV6
- Protocolo ICMP
- Asignacion de direccionamiento IPV4 estatico y dinamico

Capa de Transporte

- Protocolo TCP, UDP
- Manejo de netcat para TCP y UDP

Capa de Aplicacion

- Nociones básicas de un protocolo en capa de aplicación



LOHP

Linux Orientado al Hacking y Pentesting

Modulo 7

Programacion en Bash

Fase de Reconocimiento

- Reconocimiento de host desde ICMP y ARP
- Introduccion a Nmap
- Conociendo la herramienta Nmap
- Nmap avanzado
- Uso de scripts de Nmap

Programacion Shell

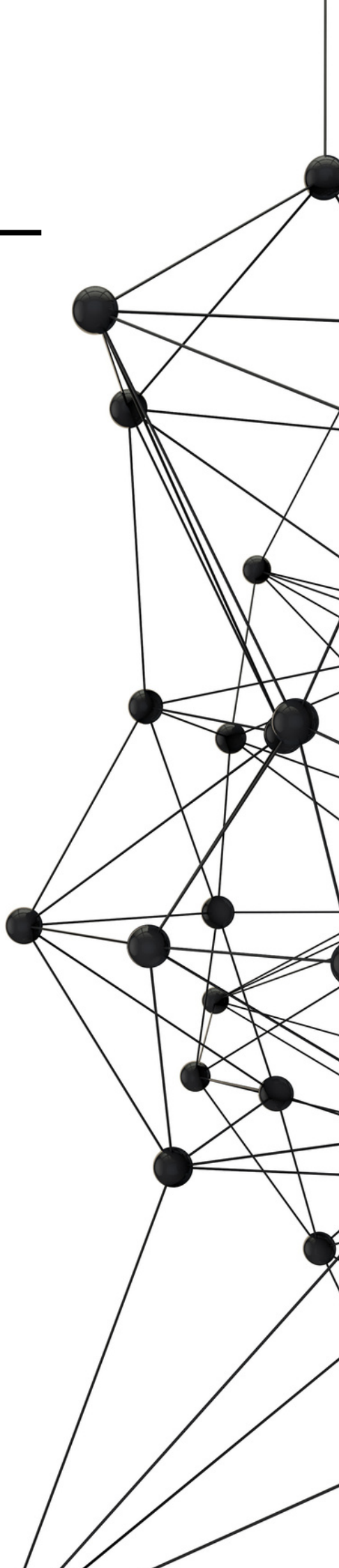
- Declaración de variables
- Condicionales
- Ciclos while - for
- Estructura de datos: vector
- Funciones
- Multi-Threading
- Interrupciones
- Automatizaciones con IA

Cronjobs

- Configuracion de crontab
- Creando el primer Cronjob en crontab
- Uso de pspy para escalacion de privilegios
- Escalada de privilegios desde crontab

LOHP

Linux Orientado al Hacking y Pentesting



Modulo 8

Implementación de Servidores y Pentesting Parte 1

Servidor FTP

- Introduccion al protocolo FTP
- Implementacion de vsftpd
- Configuracion de ficheros
- Cliente FTP

Pentesting FTP

- Anonymous login
- Ataques de Fuerza Bruta
- Post Explotacion en ficheros de configuracion

Servidor SSH

- Introduccion al protococolo SSH y criptografia asimetrica
- Implementacion de OpenSSH para un usuario
- Cliente SSH

Pentesting SSH

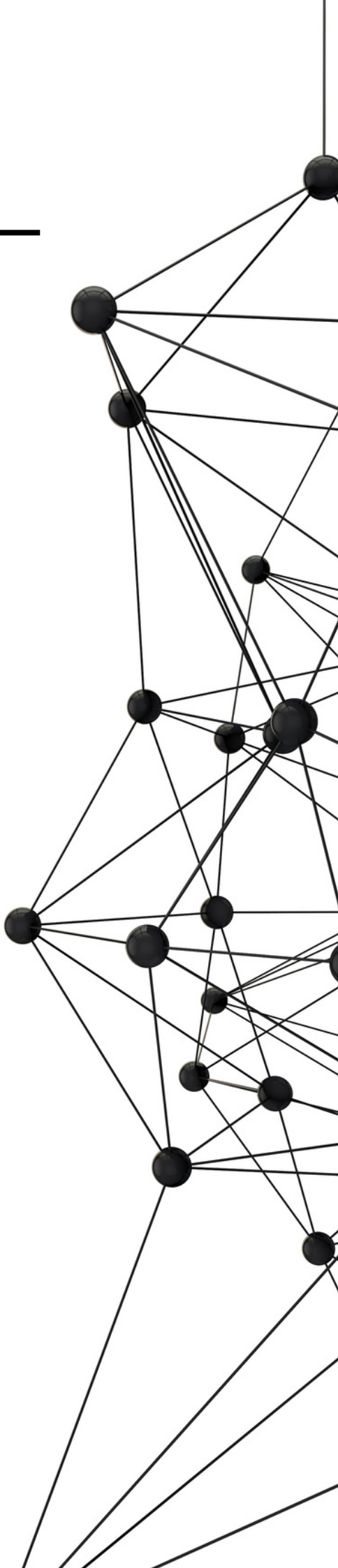
- Manipulacion de claves para acceder al servidor
- IPV6 Firewall Bypass

LOHP

Linux Orientado al Hacking y Pentesting

Modulo 9

Implementación de Servidores y Pentesting Parte 2



Servidores Web

- Introduccion al protocolo HTTP
- Implementacion de Apache2
- Implementacion de Nginx
- Creacion de servidor web auxiliar con Python
- Creando tu primera pagina web Estatica
- Implementacion de Php
- Manejo de metodos GET, POST, PUT, etc.
- Modulo para subir archivos en Php
- Visualizacion de los Logs

Pentesting Web 1

- Fuzzing de Directorios con herramientas automatizadas
- Explotacion de la Inclusion Local de Archivos (Local File Inclusion)
- Explotacion de Inclusion Remota de Archivos (Remote File Inclusion)
- Implementacion de Reverse Shell's
- Envenenamiento de los Logs

LOHP

Linux Orientado al Hacking y Pentesting

Modulo 10

Implementación de Servidores y Pentesting Parte 3

DBMS's

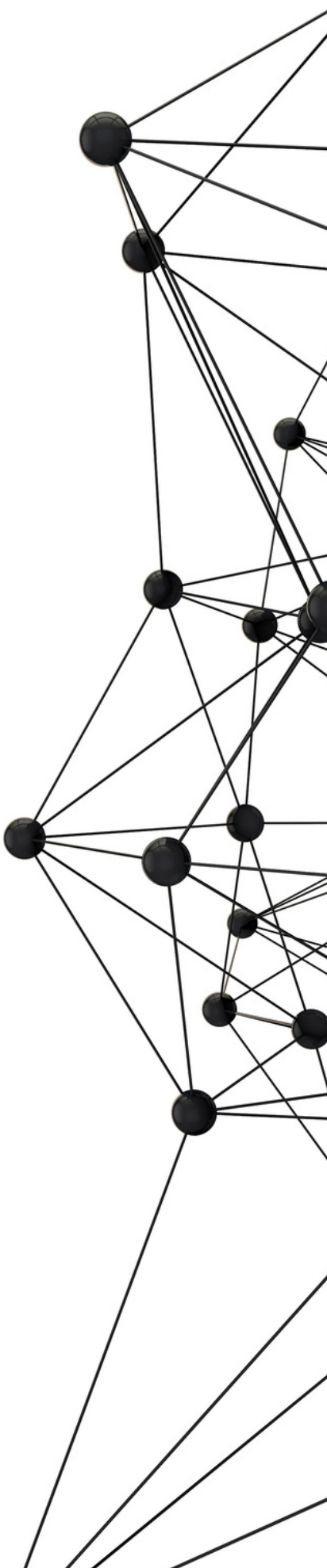
- Introducción a base de datos relacionales
- Modelo Relacional
- Modelo Físico
- Implementacion de MySql
- Creando mi primera base de datos en MySql
- Estudiando el Schema de MySql

SQL Injection

- Enlazando el Servidor Web con el DBMS
- Sql Injection Login Bypass
- Sql Injection Error Based
- Dump Database
- Securizacion con IA
- LLM03: Training Data Poissoning

Securizando con IA

- Securizacion con IA
- LLM03: Training Data Poissoning



LOHP

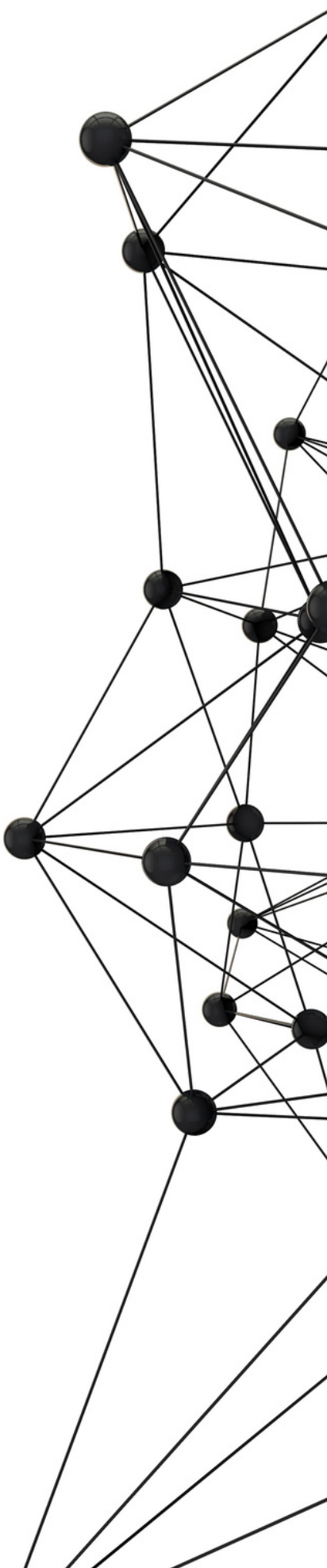
Linux Orientado al Hacking y Pentesting

Modulo 11

Content Manage System (CMS)

CMS: Wordpress

- Introduccion a Wordpress
- Enumeracion de usuarios
- Fuerza Bruta
- Remote Code Execution Autenticado
- Analisis y Busqueda de pluggins
- Explotacion de Pluggins
- Remote Command Execution desde Plugin Malicioso
- Dumping Users DataBases
- Desencriptacion de Hashes con John o Hashcat para contraseñas cifradas en base de datos



LOHP

Linux Orientado al Hacking y Pentesting

Modulo 12

Manejo de Exploits y Pivoting

Manejo de Exploits

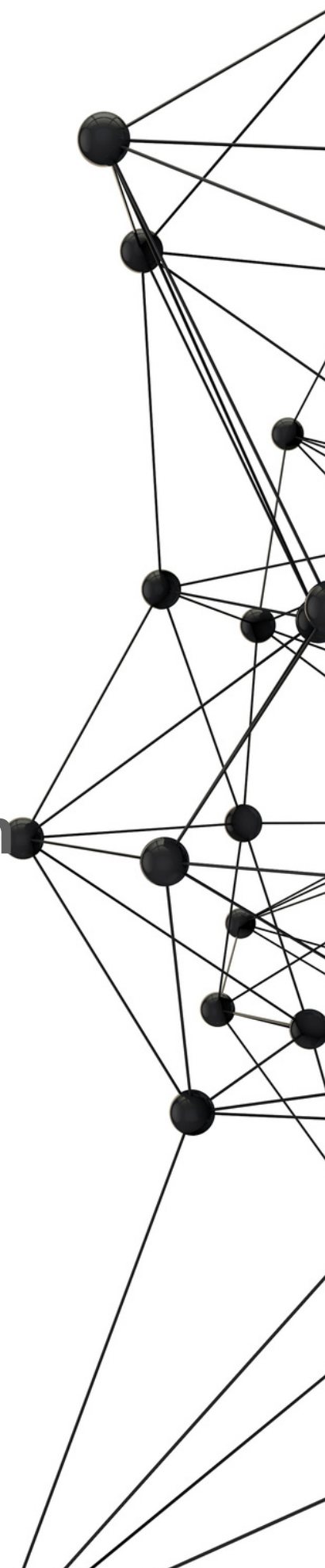
- Uso de Searchsploit para cualquier servicio
- Explotacion de Kernel Linux

Pivoting

- Subnetting
- Manejo de Proxychains
- Manejo de Chisel
- Tecnicas de Pivoting con Metasploit
- Persistencia

Preparacion para el Examen

- Resolucion de maquinas DeepSec Machines de forma manual
- Resolucion de maquinas DeepSec Machines con IA



LOHP

Linux Orientado al Hacking y Pentesting