

# 1. Temario tentativo

- (1) Redes y protocolos
- (2) Sistemas operativos
- (3) Programación baja, vulnerabilidades y reversing
- (4) Pentesting
- (5) Hardeging, blue team y forensics
- (6) Criptografía

## 1.1. Algunos objetivos a mediano plazo

- Completar libros.
- Resolver máquinas o labs como Hack The Box, PicoCFT, Root-Me.
- Experimentar con laboratorios pequeños en casa: una red virtual con PfSense, Kali Linux, Window vulnerable, etc.
- Construir un portafolio de aprendizajes.
- Sacar las certificaciones eLearnSecurity Junior Penetration Tester v2 (eJPTv2), eLearnSecurity Certified Professional Penetration Tester v2 (eCPPTv2), eLearnSecurity Web Application Penetration Testing (eWPT), CompTIA Security +, Offensive Security Certified Professional (OSCP), CISM o CISSP.