

Laboratorio COMPTIA PENTEST+









LABORATORIO COMPTIA PENTEST+

- 01: Exploring the Lab Environment
- 02: Exploring the Domain Tools: Nslookup, Dig, and Whois
- 03: Navigating Open-Source Intelligence Tools
- 04: Understanding Social Engineering Toolkit (SET)
- 05: Understanding Spear Phishing and Credentials Attack
- 06: Exploring OpenVAS
- 07: Using Web Scanners
- 08: Understanding Nmap Common Usage
- 09: Scanning a Vulnerable System
- 10: Understanding Scan Output
- 11: Navigating Steganography Tools
- 12: Demonstrating Enumeration Techniques
- 13: Exploring the Basics of Metasploit
- 14: Using VSFTP Manual and Metasploit
- 15: Monitoring with Aircrack-ng
- 16: Discovering IoT devices with Shodan
- 17: Using SQL Injection
- 18: Using Reverse and Bind Shells
- 19: Analyzing Exploit Code
- 20: Exploring Programming Shells
- 21: Applying PenTest Automation
- 22: Exploring Password Attacks with John the Ripper and Hydra





