ZDResearch Training

This course will provide an enthusiastic student with many concepts of penetration testing, covering the range from infrastructure penetration testing to highest levels of web application testing. It has been taught over many years and the content have been published as a book, which makes the course very mature. Students will practice what they are taught on prepared virtual machines and try to get most out of the theories. Browse the course syllabus for a detailed outline of the concepts that will be covered.

ZDResearch

Penentration Test

ZDResearch

Course Material

- Interactive Slides
- Video Tutorials
- Downloadable Virtual Machines
- Staff Responding to Every Question

https://training.zdresearch.com/course/pentesting

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5 : Network Hacking

1. Introduction to Network Hacking
    - 1.1 Wireshark Analysis
    - 1.2 Generating TCP/IP Packets
        - 1.2.1 Scapy
        - 1.2.2 ARP Analysis
        - 1.2.3 UDP/DNS Analysis
        - 1.2.4 TCP Three-way Handshake Analysis
    - 1.3 network Structure Attacks
2. Read Network Information
    - 2.1 Sniffing with Scapy
    - 2.2 DPKT in Python
    - 2.3 Passive Address Gathering
    - 2.4 Cain&Able and Ettercap Sniffing
    - 2.5 Ettercap Filters Lab
3. Network Spoofing
    - 3.1 MAC Spoofing
    - 3.2 TCP Session Hijacking
    - 3.3 DHCP Spoofing
4. Network Manipulation
    - 4.1 Firewall Bypassing
        - 4.1.1 Firewall Categories
        - 4.1.2 Firewall and NAT Detection
        - 4.1.3 SSH Port Forwarding
    - 4.2 IDS Bypassing

Chapter 6: Web Application PenTesting

Chapter 7: Exploitation, Privilege Escalation

ZDResearch Training

ZDResearch

ZDResearch

Custom Research
Penetration Testing
Advanced training
BA/WA (PoC/Exploits)

https://training.zdresearch.com