



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 Penetration Test

Course Material

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

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



Chapter 1

1. Introducing Penetration Testing

1.1 What is penetration testing

1.2 Different types of test

1.2.1 External Tests

1.2.2 Internal Tests

1.2.3 Application Pen-Tests

1.3 Prerequisites

2. Introduction to Kali Pen-Testing Framework

2.1 Starting to work with Kali

2.2 Network setup in Kali

2.3 Service setup in Kali

2.4 Updating and Repositories

3. Concepts

3.1 Threats, Vulnerabilities, Exploits

3.2 Shell Classifications

3.2.1 Interactive & Non-Interactive

3.2.2 Reverse Shell & Bind Shell

3.2.3 Web Shells

3.3 TCP/IP Analysis

3.3.1 Wireshark

3.3.2 **Wireshark Lab**

3.4 Anonymity

3.4.1 Anonymity Methods

3.4.2 VPNs



3.4.3 SOCKS, Wide Proxy

3.4.4 Web Proxy

Chapter 2

1. Foot-printing, Reconnaissance, Social Engineering

1.1 Passive

1.2 Active

2. Web-Based Information Gathering

2.1 Google Hacking

2.2 Email Harvesting

2.3 whois

2.4 Firefox Recon

2.5 People Search

2.6 File Metadata

2.7 Image Header Metadata

3. DNS Information Gathering

3.1 DNS Protocol

3.2 Forward Lookup Brute-Forcing

3.3 Reverse Lookup Brute-Forcing

3.4 Zone Transfer

3.5 Load Balancers

4. Foca Tool

4.1 How to use Foca

4.2 Alternative Domains

4.3 DNS Prediction



4.4 IP Range Scan Tools

4.5 Network Discovery

4.6 DNS Cache Snooping

5. Maltego Tool

6. Social Engineering

6.1 Social Engineering Method

6.2 Remove Data Gathering

6.3 Local Data Gathering

6.4 Fake Emails

6.5 Phishing

Chapter 3

1. Data Gathering from Target Network

1.1 TCP Port Scanning

1.2 UDP Port Scanning

2. NMap Port Scanning

2.1 Three Step TCP Scan

2.2 TCP SYN Scan

2.3 Null Scan, Xmas Tree, Stealth FIN

2.4 Ping scanning

2.5 UDP Scanning

2.6 SYN/ACT Scanning

2.7 Addressing Methods for Scan

2.8 Port Defining for Scan

2.9 NMap Switch Tutorial



2.10 NMap Scripts

2.11 Anonymity with NMap

2.11.1 IP Spoofing

2.11.2 IP Fragmentation

2.11.3 Source Port Spoofing

2.11.4 Slow Scanning

2.11.5 IdleScanning

2.12 NMap Lab

3. Network Map

3.1 Topology using TTL

3.2 TraceRoute with UDP and TCP

3.3 Zenmap Topology Drawing

3.4 Passive Topology

3.5 Service Scanning for Topology

3.5.1 SNMP

3.5.2 NetBIOS, SMB

3.5.3 UPNP

4. Protocol-Based Information Gathering

4.1 ARP

4.2 SMTP

Chapter 4

1. Common Cryptography/Steganography

1.1 Encryption Algorithms

1.2 Hashing Algorithms



1.3 Reversible Encryptions

1.4 Digital Signature and Certificate

1.5 Breaking a Symmetric Cipher

2. Attacking Cryptography Systems

2.1 9 Strategies to Attack Cryptosystems

2.2 BruteForcing with Hydra

2.3 Dictionary Attacks and Improving Them

2.4 High Performance Cracking

2.5.1 GPU

2.5.2 Distributed Computing

2.5.3 Rainbow Tables

2.5 HashCat GPU Cracking

2.6 Zip, PDF, RAR, Office Password Cracking

2.7 Replay Attacks

2.8.1 Windows Authentication

2.8.2 Pass The Hash on NTLM

2.8 NT, LM hash extraction

2.9.1 Physical Login Bypass

2.9.2 SAM Database

2.9.3 Password History

2.9.4 Logon Sessions

2.9.5 Domain Controller

2.9.6 Windows 7 Password Lab



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



4.2.1 IDS & IPS

4.2.2 General IDS Bypassing

4.2.3 False Positive Bypasses

4.2.4 Packet Obfuscation

4.2.5 Session Splicing

4.2.6 TTL Expiry Attacks

5. Denial of Service & Flooding

5.1 HTTP POST DOS

5.2 SYN, ACK DOS

5.3 Switch MAC Flooding

5.4 Yersinia Tool

6. MITM Attacks

6.1 ARP Spoofing

6.2 SSLStrip

Chapter 6: Web Application PenTesting

1. Web Application Architecture

1.1 URL Structure

1.2 HTTP Protocol

1.2.1 Syntax

1.2.2 HTTP Requests

1.2.3 HTTP Response Codes

1.2.4 HTTP Cookies

1.2.5 Authentication

2. Web Application Testing

2.1 OWASP Framework



2.2 Simorgh Web Hacking Lab

3. SQL Injection

3.1 Detecting SQL injection

3.2 Authentication Bypass

3.3 Error Based Injection

3.4 File Operations

3.5 System Control

3.6 Blind Injection Detection

3.7 Blind Injection Exploitation

3.8 Injection Lab with Havij

4. Command Injection

5. XSS Injection

5.1 Reflected XSS

5.2 Stored/Persistent XSS

5.3 DOM Based XSS

6. Authentication and Session

6.1 Session Fixation

6.2 Authentication Flaw

7. Insecure Direct Object Reference

8. File Inclusion

9. CSRF

10. Weak Cryptography

11. URL Restriction

12. Malicious File Upload

13. Opeth Path Manipulation

14. Automatic Tools



14.1 Acunetix

14.2 Burp Suite

Chapter 7: Exploitation, Privilege Escalation

1. Introduction

1.1 Post Exploitation

1.2 Access Elevation

1.3 Metasploiting

2. Linux

2.1 Escalation

2.1.1 Linux Access Levels

2.1.2 ACLs

2.1.3 Architecture

2.1.4 Exploiting

2.1.5 Symlinking

3. Linux Post Exploitation

3.1 Metasploit

3.2 Linux Commands for Escalation

4. Windows

4.1 Escalation

4.1.1 Windows Access Levels

4.1.2 Windows Elevation

4.1.3 Exploiting

5. Windows Post Exploitation

5.1 Metasploit

5.2 Windows Commands for Escalation



ZDResearch

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

ZDResearch