
OffensiveResources V3
By: Zeyad Azima
Infrastructure
Books
The Hacker's Handbook
Advanced Infrastructure Penetration testing
Hacker playbook series
The Art of Network Penetration Testing
Mastering Kali Linux for Advanced Penetration Testing
Advanced Penetration Testing for Highly-Secured Environments
Advanced Penetration Testing
Hands-On Penetration Testing on Windows
Mastering Wireless Penetration Testing for Highly Secured Environments
Cybersecurity – Attack and Defense Strategies
RTFM: Red Team Field Manual
Penetration Testing: A Hands-on Introduction to Hacking
Hacking: Hacking Firewalls & Bypassing Honeypot
Red Team Development and Operations: A practical guide
Hands-On Red Team Tactics
Courses
OSCP
OSEP
eCPPT
eCPTX
SEC560
SEC660
SEC564
Practical Ethical Hacking
Windows Privilege Escalation for Beginners
Linux Privilege Escalation for Beginners
Movement, Pivoting, and Persistence
The External Pentest Playbook
CRTP
CRTE
PACES
CPRA
CRTE
Labs
Building Virtual Penetration Labs for Advanced Penetration Testing
Hack The Box: Pro Labs
Red Team Attack Lab
Capsulecorp Pentest
Building a Lab
Pentest Lab
Local PentestLab Management Script
Pentest-lab
Offensive Security Lab
Pentesteracademy Labs
Hack The Box
VulnHub
Offensive Security Proving Grounds
TryHackMe
Wireless
Books
BackTrack 5 Wireless Penetration Testing Beginner's Guide
Kali Linux Wireless Penetration Testing Cookbook
Mastering Wireless Penetration Testing for Highly Secured Environments
Courses
OSWP
Wi-Fi Security and Pentesting
Wi-Fi Hacking and Wireless Penetration Testing Course
SEC617: Wireless Penetration Testing and Ethical Hacking
Labs
Building a Pentesting Lab for Wireless Networks
The Courses and Books have explained how to build a lab
Social Engineering
Books
Social Engineering: The Science of Human Hacking
Social Engineering: The Art of Human Hacking
The Social Engineer's Playbook
Social Engineering: Hacking Systems, Nations, and Societies
Learn Social Engineering
Courses
Learn Social Engineering From Scratch
The Complete Social Engineering, Phishing & Malware
Advanced Social Engineering Training
Social Engineering (Cybrary)
Labs
Bro, it's about human hacking. Just hack yourself xD
IoT & Hardware
Books
Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things
The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things
IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your Smart Devices
The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks
Practical Hardware Pentesting: A Guide to Attacking Embedded Systems and Protecting Them Against the Most Common Hardware Attacks
Courses
SEC556: IoT Penetration Testing
Offensive IoT Exploitation
Securing IoT: From Security to Practical Pentesting on IoT
Applied Physical Attacks Series
Labs
The Courses and Books have explained how to build a lab
Offensive Programming
Books
Hands-On Penetration Testing with Python
Python Penetration Testing Cookbook
Python for Offensive PenTest
Black Hat Python
Gray Hat C#: A Hacker's Guide to Creating and Automating Security Tools
Black Hat Go: Go Programming For Hackers and Pentesters
Security with Go
Penetration Testing with Perl
Black Hat Ruby
Courses
I encourage you to read the books, cause there are a lot of courses for offensive programming but the most are using python.
Learn Python & Ethical Hacking From Scratch
The Complete Python Hacking Course: Beginner to Advanced
Offensive Bash Scripting
Powershell for Pentesters
Labs
First of all try to create automation tools for your tasks, also you can search for offensive tools and try to write one on your own way.
Tools:
Subdomain Enumeration
Directory Bruteforcing
Live Subdomain checker
Google Dorking
Extract javascript urls using page source
Reverse & Bind Shells
Protocol Enumeration
Port Scanner (TCP & UDP)
Hash & Password Cracking
Fuzzer
Malware (Keylogger, Spyware, CryptoMalware, etc.)
Packet Sniffer
Wifi Scanner or Bruteforcer
Vulnerability Scanner (Web, Network & System Vulnerabilities, etc.)
Exploitation Tool (Try to write an exploitation tool for known vulnerability [e.x: VsFtpd backdoor exploitation tool])
Network Sniffer
MAC address Changer
Network Scanner
ICS and SCADA
Books
Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions
Hacking SCADA/Industrial Control Systems: The Pentest Guide
Handbook of SCADA/Control Systems Security
Courses
ICS/SCADA Cybersecurity (Ec council)
ICS410: ICS/SCADA Security Essentials
Labs
The Courses and Books have explained how to build a lab
Exploit Development
Books
Penetration Testing with Shellcode
The Shellcoder's Handbook
Hacking: The Art of Exploitation
Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation
A Bug Hunter's Diary
Buffer Overflow Attacks: Detect, Exploit, Prevent
Linux Exploit Development for Beginners
Fuzzing: Brute Force Vulnerability Discovery
Fuzzing for Software Security Testing and Quality Assurance
The Fuzzing Book
Open Source Fuzzing Tools
A Guide to Kernel Exploitation
Courses
OSCE
OSED
eCXD
SEC760
Exploit Development Repo
x86 Assembly Language and Shellcoding on Linux
CNIT 127: Exploit Development
x86_64 Assembly Language and Shellcoding on Linux
Reverse Engineering Win32 Applications
Reverse Engineering Linux 32-bit Applications
Exploiting Simple Buffer Overflows on Win32
Reverse Engineering and Exploit Development
Exploit Development for Linux (x86)
Exploit Development for Linux x64
Introduction to Exploit/Zero-Day Discovery and Development
Exploit Development From Scratch
Hands-on Fuzzing and Exploit Development Part 1
Hands-on Fuzzing and Exploit Development Part 2
ZDResearch Exploit Development
Labs
Analyze previous and new zero-days vulnerabilities will give you deep into the real-world
PWN college
Phoenix
Vulnserver
BlazeDVD 5.1 Professional
DVD X Player
Easy CD DVD
Easy Chat Server 3.1
Easy File Sharing FTP Server 3.5
Easy File Management Web Server 5.3
Easy File Sharing Web Server 7.2
Easy RM to MP3 Converter 2.7.3.7
Eureka
FreeFTP 1.0.8
FreeFloat
Kolibri v2.0 HTTP Server
KNFTP Server 1.0.0
Kolibri v2.0 HTTP Server
Millenium MP3 Studio
Minishare
ProSysInfo TFTP Server TFTPDWIN 0.4.2
QuickZip 4.60
R 3.4.4
Ricoh DC Software DL-10 FTP Server
SolarFTP
Sorting MP3 Player 1.0
Xitami Webserver 2.5
VulnHub
Hack the box
Blockchain
Books
Bitcoin and Blockchain Security
Blockchain Technology And Hacking
Hands-On Cybersecurity with Blockchain
Courses
Certified Blockchain Security Professional (CBSP)
SEC554: Blockchain and Smart Contract Security
Blockchain Security Expert (CBSE)
Attack and Defence in Blockchain Technologies (W39)
Decentralized Application Security Project
smart contract security best practices
Labs
DDAPContracts
Ethernaut
Hacking Topic
Car Hacking
Books
The Car Hacker's Handbook
Hacking Connected Cars
Courses
CAR HACKING 101
Automotive hacking for Beginners
Car Hacking Training: Automotive Cybersecurity and In-Vehicle Networks for Beginners
Practical car hacking
Labs
Setup your lab from the courses & books
Game Hacking
Books
Exploiting Online Games
Game Hacking: Developing Autonomous Bots for Online Games
Hacking Video Game Consoles
Game Console Hacking: Xbox, PlayStation, Nintendo, Game Boy, Atari and Sega
Hacking the Xbox: An Introduction to Reverse Engineering
Courses
CS420 Game Hacking Course
Learn How To Code A Hack For ANY Game! - Game Hacking
Game Hacking: Cheat Engine Game Hacking Basics
Game Hacking Shenanigans – Game Hacking Tutorial Series
Game Hacking Tutorial
Labs
Setup your lab from the courses & books
Source Code Review
Books
SECURE COMPUTER SOFTWARE DEVELOPMENT: INTRODUCTION TO VULNERABILITY DETECTION TOOLS
Software Vulnerability Guide
secure Programming with Static Analysis: Getting Software Security Right with Static Analysis
The ultimate guide to code reviews – Edition 1
OWASP Code Review Guide v2
Courses
SAST
How to do Code Review – The Offensive Security Way
How to find vulnerabilities by source code review
Finding Security Vulnerabilities through Code Review – The OWASP way
OWASP DevSlop Show: Security Code Review 101 with Paul Ionescu
How to Analyze Code for Vulnerabilities
Labs
Pentesterlab Code Review
Damn Vulnerable Source Code
SVCP4CDetroit
Telecom
Books
Security for Telecommunications Networks
Courses
Mobile Network Hacking, IP Edition
New Era in Telecom Hacking by Ali Abdollahi at BSides Toronto 2020
Labs
Setup your lab from the courses & books
Malware Development
Books
You can read malware analysis books to get a deep understanding of malware
Courses
RED TEAM Operator: Malware Development Essentials Course
RED TEAM Operator: Malware Development Intermediate Course
Build Undetectable Malware Using C Language: Ethical Hacking
Practical Malware Development For Beginners
Coding Botnet & Backdoor In Python For Ethical Hacking
Ethical Hacking Foundations: Malware Development in Windows
Labs
No need for online labs you need to write a malicious code
VOIP
Books
Hacking VoIP: Protocols, Attacks, and Countermeasures
Hacking Exposed Voice Over IP: VoIP Security Secrets & Solutions
Hacking Exposed Unified Communications & VoIP Security Secrets & Solutions, Second Edition
Courses
VoIP Pentesting (NRT)
VoIP Hacking & Penetration Testing Training
VoIP pentest and SIP hacking
Labs
Setup your lab from the courses & books
Web Applications
Books
Web Application Hacker's Handbook
Portswigger learning materials
Owasp web Testing Guide
Real World Bug Hunting
Bug Bounty playbook part 1 & 2
Mastering Modern Web Penetration Testing
Mastering Kali Linux for Web Penetration Testing
Kali Linux Web Penetration Testing Cookbook
Courses
OSWE
eWAPT
eWAPTX
SEC542
SEC642
Offensive bug bounty hunter part 1 & 2 hackerverse
Web Application Attacks and API Hacking (WTC)
Labs
Portswigger
pentest
Portswigger labs
Hack me
OWASP Juice shop
Owasp Broken Web Apps
Pentesterlab
root-me
Mobile Applications
Books
OWASP Mobile Security Testing Guide
Mobile application penetration testing
Android hacker's handbook
Android hacker's handbook
iOS Hacker's Handbook
Courses
eMAPT
SEC575
Offensive AndroidHacker
ANDROID Hacking & Penetration Testing
Hacking and Pentesting iOS Applications
Labs
Damn Vulnerable iOS Application (DVIA)
List of intentionally vulnerable android apps
ExploitMe Mobile iPhone Labs
ExploitMe Mobile Android Labs
RFID & SDR
Books
RFID Security
Inside Radio: An Attack and Defense Guide
Courses
Ethical RFID Hacking
SDR Exploitation
SDR for Ethical Hackers and Security Researchers
Advance SDR for Ethical Hackers Security Researchers 2.0
SDR for Ethical Hackers and Security Researchers 3.0
Labs
Setup your lab from the courses & books
API
Books
OWASP API Security Project
Courses
OWASP Top 10: API Security Playbook
Offensive Api penetration testing
Web Application Attacks and API Hacking (WTC)
API Security: Offence and Defence (WTC)
Labs
Traceful API
vulnerable-api
vAPI
ecomclub
Cloud
Books
AWS Penetration Testing
Hands-On AWS Penetration Testing with Kali Linux
Pentesting Azure Applications
Mastering Cloud Penetration Testing
Courses
SEC588
Labs
AWS Pen-Testing Laboratory
Create Your own lab from the books
Reverse Engineering
Books
Reversing: Secrets of Reverse Engineering
Mastering Reverse Engineering
Reverse Engineering for Beginners
The Ghidra Book: The Definitive Guide
The IDA Pro Book, 2nd Edition
Practical Reverse Engineering
Courses
eCRE
FOR610: Reverse-Engineering Malware
Reverse Engineering Deep Dive
Reverse Engineering: IDA For Beginners
Expert Malware Analysis and Reverse Engineering
Reverse Engineering 1: x64dbg Debugger for Beginners
Reverse Engineering: Ghidra For Beginners
Reverse Engineering & Reversing .NET with dnSpy
Reverse Engineering for Beginners (Youtube)
Labs
CTF101: Reverse Engineering
CyberDefenders: Reverse Engineering CTF
Reverse Engineering CTF List