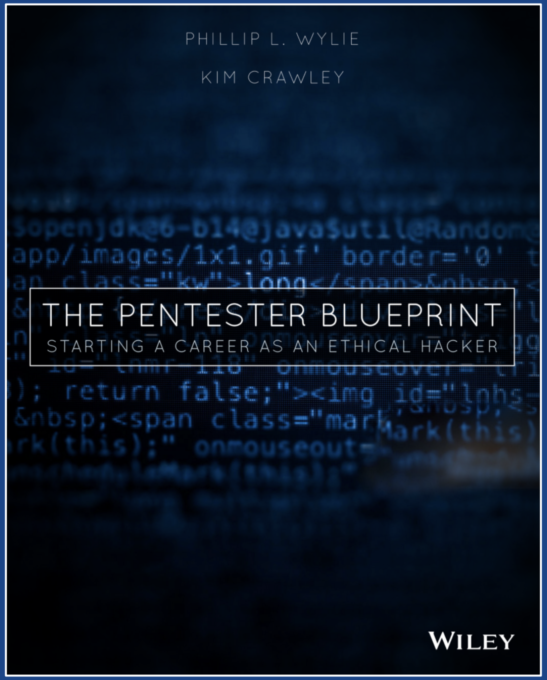
Jumpstarting your pentesting career with The Pentester Blueprint

Phillip Wylie, CISSP, OSCP, GWAPT

Phillip Wylie, CISSP, OSCP, GWAPT

- Security Solutions Specialist & Evangelist @ CYE
- Offensive Security Professional & Instructor
- Former Adjunct Instructor @ Dallas College
- DEF CON 940 & The Pwn School Project Founder
- Concept creator & coauthor of “The Pentester Blueprint: Starting a Career as an Ethical Hacker”
- Featured in “Tribe of Hackers Red Team”
- Host of “The Hacker Factory Podcast”



My Offensive Security Career Path

Pro Wrestler > CAD Drafter > Sysadmin > Infosec > AppSec > Pentester

"With great power comes great responsibility."
-Voltaire

Only hack if you have permission and even better written permission. Hacking <u>without</u> permission is illegal.

The What, Why, & How of Becoming a Pentester

What is Pentesting?

- Assessing security from an adversarial perspective using hacking tools and tactics, techniques, and procedures (TTPs)
- Also known as ethical hacking
- Security posture from an adversarial perspective
  - Better understanding of security risk severity
  - Exploitable vulnerabilities are higher risk and a higher priority for remediation as well as justification for budgeting.

Why Pentesting?

- Regulatory Compliance
  - Payment Card Industry Data Security Standard (PCI DSS) - Credit Card Processors
  - HIPPA - Medical Devices, Healthcare Providers
  - Service Organization Control (SOC2) - Technology Services
  - FINRA (Financial Industry Regulatory Authority)
- Fun job with a lot of job opportunities!

FINRA

SOC 2 TYPE 2

AICPA SOC

PCI DSS COMPLIANT

Pentesting Jobs, Synonymous Terms, & Departments

- Penetration Testers aka Pentesters
- Security Consultants, Analysts and Engineers
- Synonymous Terms
  - Ethical Hackers
  - Offensive Security
  - Adversarial Security
- Departments Pentesters Work in Roles
  - Threat and Vulnerability Management or Vulnerability Management

Pentesting Skills In Other Areas

- SOC (Security Operations Center) Analysts
- DFIR (Digital Forensics and Incident Response)
- Network Security Analysts and Engineers
- Purple Teams (where defensive and offensive security collaborate to improve defenses)
- Application Security

Types of Pentests: Targets

- Network – Internal, External, Wireless
- Application – Web App, API, Mobile, Cloud, Thick Client aka Binary
- Cloud
- Hardware – Network Hardware, IoT, ICS/OT, Medical Devices
- Transportation – Planes, Trains, and Automobiles (all types)
- People – Social Engineering
- Buildings – Physical Security

Types of Tests: Testing Depth

- Vulnerability Scans (not a pentest) – just running a vulnerability scanner.
- Vulnerability Assessments (not a pentest) – vulnerability scanning plus vulnerability validation.
- Pentest – Vulnerability Assessment plus exploitation (aka hacking)
- Red Team Ops/Adversarial Emulation – testing blue teams, attack simulation, less restrictive scope

Specializations

- Generalist – Network, WiFi, Light Web App
- Application – Web App, Mobile, Cloud, API, Thick Client
- Cloud - AWS, Azure, Google Cloud Platform (GCP)
- Social Engineering - People
- Physical - Buildings
- IoT & ICS/OT
- Hardware
- Transportation – Vehicles, Airplanes
- Red Team – Adversarial Simulation

Types of Pentests: Target Knowledge

- Black Box (aka Blind Pentest) – limited to target IP’s, more of an attacker approach
- White Box (aka Crystal Box) – detailed system info including accounts for app testing, documentation
- Gray Box – partial knowledge of target, a cross between the other two methods

Becoming a Pentester: Technology Skills

- Network
- Operating Systems (especially Windows and Linux)
- Security
- Application
- Hardware

Becoming a Pentester: Hacking Skills

- Pentesting Classes
- Conferences
- Cybersecurity Organizations or Club Meetings/Meetups
- Self-Study
  - Home Labs
  - Online Labs - Try Hack Me, Hack The Box
  - Videos
  - Tutorials
  - Blogs and Articles
  - Twitter

Hacker Mindset

The Hacker Mindset is the ability to think like a hacker and be able to find ways to exploit vulnerabilities. The Hacker Mindset is a culmination of creative and analytical thinking. Developing this mindset is similar to learning how to troubleshoot.

The Hacker Mindset takes time and repetition to develop and is best developed by hands on hacking experience.

Pentester Blueprint: Formula

Technology Knowledge

+

Security Knowledge

+

Hacker Knowledge & Mindset

Pentesting Education

Developing a Plan: Your Personal Pentester Blueprint

- Skills Inventory
- Skill Gap Analysis
- Create a Plan to Address Skills Gaps

Pentesting Education: Learning Resources

- SANS Institute: sans.org
- OffSec (formerly Offensive Security): offsec.com
- Antisyphon Training: antisyphontraining.com
- Virtual Hacking Labs: virtualhackinglabs.com
- Pentester Academy: pentesteracademy.com
- INE (formerly eLearn Security): INE.com
- Zeropoint Security: zeropointsecurity.co.uk
- Pentester Lab: pentesterlab.com
- TCM Security Academy: academy.tcm-sec.com
- Hack The Box Academy: HackTheBox.eu
- Try Hack Me: TryHackMe.com

Pentesting Education: Free Learning Resources

- Bugcrowd University: bugcrowd.com/university/
- HackerOne: hacker101.com
- HackingTutorials.org
- Web Security Academy: portswigger.net/web-security
- Try Hack Me: TryHackMe.com

Pentesting Education: Certifications

Entry Level

- CEH - EC-Council
- PenTest+ - CompTIA
- eJPT - INE

Intermediate

- PNPT – TCM Academy
- GPEN – SANS/GIAC (now includes Azure)
- OSCP – Offensive Security
- GWAPT – SANS/GIAC
- eCPPTv2 - INE

Advanced

- GxPN – SANS/GIAC
- OSCE – Offensive Security

Web App

- GWAPT – SANS/GIAC
- Burp Suite Certified Practitioner - Portswigger
- OSWA – Offensive Security
- OSWE – Offensive Security

Cloud

- GCPN - Cloud Pentesting

Pentesting Education: Certifications

Red Team

- CRTO - ZeroPoint Security
- SEC565: Red Team Operations and Adversary Emulation (no cert yet)

Pentesting Education: Certifications

Determining which certification to get

- Research job listings to see which certifications are more in demand.
- CEH and PenTest+ are DoD Directive 8570 certifications and can be helpful for government jobs, whether working directly for the government or through contracting and consulting.

Pentesting Education: Certifications

Certification Tips

- Learn the skills and not just prepare to pass the exam. This will help your probability of success and give you skills needed for pentesting roles. The better you know the content of the certification education content, and it will help during interviews.

Lab Environment: Home Lab

Lab Targets

- Virtual Systems - Purposely Vulnerable Systems
- Physical Hardware - Servers, Clients, Routers, Switches
- Vulnerable VMs
  - Metasploit 2 & 3
  - Vulnhub.com

Hacking System

- Virtual System
- Physical Hardware
- Hacking OS
  - Linux - Kali, Parrot OS
  - Windows - Commando VM, Flare VM (by Madiant)

Lab Environment: Online Lab

- Try Hack Me
- Hack The Box
- Proving Grounds Labs (OffSec): offsec.com
- Antisyphon Cyber Range: antisyphontraining.com/cyber-range/
- Over The Wire CTF: overthewire.org/wargames/ (Linux)
- Under The Wire CTF: underthewire.tech/index.htm (Windows)

Pentesting Education: Books

Penetration Testing:

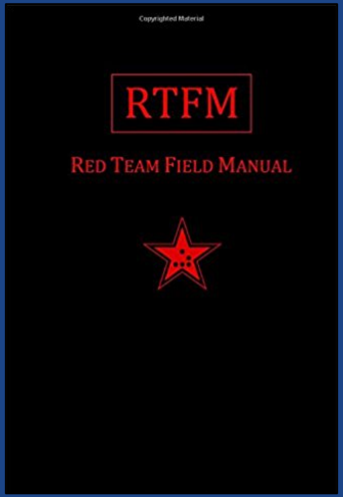
A Hands-On Introduction to Hacking

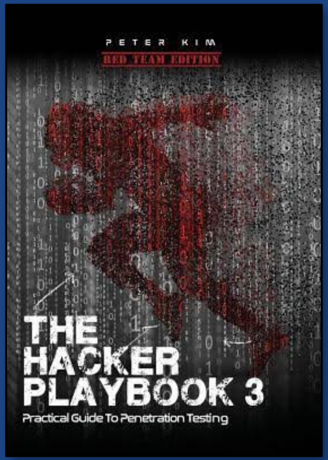
The Hackers Playbook 2 & 3

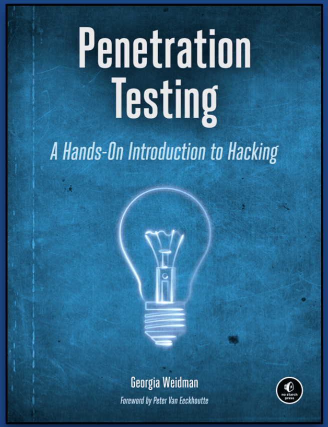
The Web Application Hacker's Handbook:
Discovering and Exploiting Security Flaws 2nd Edition

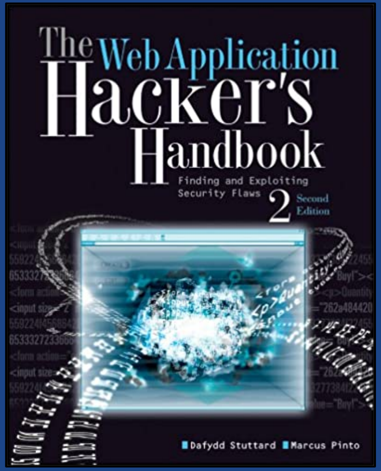
Operator Handbook

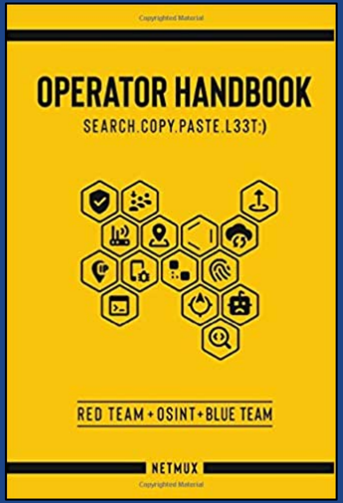
RTFM: Red Team Field Manual






Penetration Testing
A Hands-On Introduction to Hacking
Georgia Weidman
Foreword by Peter Van Eeckhoutte


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard
Marcus Pinto



Pentesting Experience & How to Get It

Pentesting Experience: Tools

- Vulnerability Scanners
  - Network - Nessus, Nexpose, OpenVas, Nuclei
  - Web App - Web Inspect, AppScan, Acunetix, Netsparker, Nikto, Nuclei
- Pentesting Operating Systems
  - Linux - Kali, Parrot OS,
  - Windows Commando VM, Flare VM
- Pentesting Tools - nmap, Metasploit
- Web App Pentesting Tools - Burp Suite, OWASP ZAP, Web App Scanners, Fuzzers

Pentesting Experience: Skills

- Networking
- Operating Systems – Windows & Linux
- Hacking/Pentesting
- Reverse Engineering

Hands-on Pentesting Experience: Educational/Lab Environments

- CTFs
- HACKTHEBOX
- TryHackMe
- Home Lab using Vulnerable VMs

Hands-on Pentesting Experience: Professional/Real World Environments

- Bug Bounties - Crowd Sourced Pentesting
  - Bugcrowd, HackerOne, Synack, Intigriti
- PaaS (Pentesting as a Service)
  - Cobalt, Synack
- Pro Bono & Low Cost Pentesting for Nonprofits, or Small Businesses
- CVEs (Common Vulnerabilities and Exposures)

Hands-on Pentesting Experience:
CVE Definition

The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures.[1] The United States' National Cybersecurity FFRDC, operated by The MITRE Corporation, maintains the system, with funding from the US National Cyber Security Division of the US Department of Homeland Security.[2] The system was officially launched for the public in September 1999.[3]

The Security Content Automation Protocol uses CVE, and CVE IDs are listed on Mitre's system as well as in the US National Vulnerability Database.[4]

ref: https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Hands-on Pentesting Experience: CVE Learning Resources

- Bobby Cooke aka Boku - Beginners Guide to 0day/CVE AppSec Research https://0xboku.com/2021/09/14/0dayappsecBeginnerGuide.html
- Joe Helle aka The Mayor - I Was Bored One Night and Found Two CVEs https://medium.themayor.tech/how-i-was-bored-one-night-and-found-two-cves-4233c3719194

Demonstrating & Documenting Skills

- Writing
  - CTF, HTB, and THM write ups
  - Articles and blog posts on GitHub, Medium, or other blog platforms
- CVE IDs - list under publications on LinkedIn (link to CVE) and resume
- Tool and technique demos and hacking walkthrough videos on YouTube
- Scripts or programs on GitHub

Build a Personal Brand

- Content Creation
  - Streaming
  - Video - YouTube, Vimeo, Instagram, TikTok, Facebook
  - Writing
- Public Speaking
  - Conferences
  - Cybersecurity Meetings
  - Webinars & Podcasts
- Social Media
  - LinkedIn
  - Twitter

Professional Networking

- LinkedIn
- Cybersecurity Group Meetings (ISSA, ISACA, (ISC)2, DEFCON Groups, OWASP Chapters, college clubs)
- Conferences
- Online Communities (Discord, Slack, etc.)
- Twitter

Job Hunting Tips

- Prepare for interviews
  - Know the OWASP Top 10
  - Be able to explain the basics like 3-way TCP handshake and OSI Model
- Infosec Job Hunting w/ BanjoCrashland https://youtube.com/playlist?list=PLqz80p7f6dFumNG0wU4Ql41PvhzamHO3_
- How to Create a Better Infosec Resume (with@jhaddix)! https://youtu.be/Zs28J_SDXYQ

Questions

?

Contact Me

/In/PhillipWylie

@PhillipWylie

thehackerfactory.simplecast.com

TheHackerMaker.com

youtube.com/@PhillipWylie