The Pentester Blueprint:

A Guide to Becoming a Pentester

whoami:

Phillip Wylie, CISSP, OSCP, GWAPT

Principal Pentester @ US Bank

Adjunct Professor @ Richland College

Ambassador @ Bugcrowd

The Pwn School Project Founder

- 21+ years IT and InfoSec experience
- 6+ years system administration
- 8 years network security & AppSec
- 7 years pentesting (5 years consulting)

"With great power comes great responsibility."
-Voltaire

Only hack if you have permission and even better written permission. Hacking without permission is illegal.

What Is Pentesting?

- Assessing security from an adversarial perspective, attempting to exploit vulnerabilities to gain unauthorized access to systems and sensitive data (aka hacking).

Why Pentesting?

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 - Required for PCI DSS (Payment Card Industry Data Security Standard)
- Fun job
- A lot of job opportunities

Pentesting Jobs

- Penetration Testers aka Pentesters
- Security Consultants, Analysts and Engineers

Pentesting Synonyms

- Ethical Hackers
- Offensive Security
- Adversarial Security
- Threat and 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 is combined)
- Application Security

Types of Pentests: Targets

- Network – Internal, External, Wireless
- Application – Web App, Thick Client, Mobile, Cloud
- Hardware –Network Hardware (routers, switches, etc.),IoT (Internet of Things), Medical Devices (pacemakers, insulin pumps, etc.)
- Transportation – Vehicles of all types
- People – Social Engineering
- Buildings – Physical Security (often Included in Social Engineering

Types of Pentests: Target Knowledge

- Black Box – 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

Types of Tests: Testing Depth

- Vulnerability Scans – just running a vulnerability scanner.
- Vulnerability Assessments – vulnerability scanning plus vulnerability validation.
- Pentest – Vulnerability Test plus exploitation (aka hacking)
- Red Team/Adversarial Tests – testing blue teams, attack simulation, less restrictive scope

Specializations

- Generalist – Network, WiFi, Light Web App
- Application – Web App, Mobile, Thick Client
- Social Engineering - People
- Physical - Buildings
- Transportation – Vehicles, Airplanes
- Red Team – Adversarial Simulation

How Do I Become a Pentester?

Technological Knowledge

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

How Do I Become a Pentester?

Hacking Knowledge

- Classes
- Conferences
- Meetings/Meetups
- Self-Study
  - Home labs
  - Videos
  - Tutorials
  - Blogs and Articles
  - Twitter

How Do I Become a Pentester?

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 Mindset

Where to start?

?

Developing a Plan

Filling the Gaps

- No IT Experience: Start with the basics, Operating Systems, Hardware, Networking
- IT Experience: Learn Linux, security and Networking
- InfoSec Experience: Fill in the gaps of any basics you're missing, start learning pentesting/ethical hacking, participate in CTFs (capture The Flag) and bug bounties
- Everyone: Build a lab!

Lab

- Minimalist Lab – Virtualized Hosts (aka VMs) using VMWare, VirtualBox, Hypervisor, Etc.
- Dedicated Lab – Computer dedicated to lab purposes with VMs
- Advanced Lab – Servers, computers, routers and switches

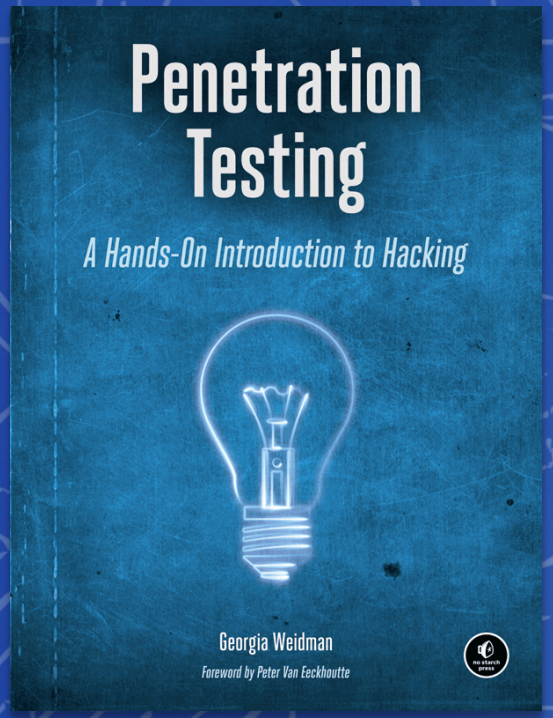
Home Lab: Attack Platform

- Kali Linux
- Parrot OS (Linux)
- Ubuntu w/ Pen Tester Framework (PTF)
- Windows 10 w/ Commando VM

Home Lab: Targets

- Create VM (Virtual Machine) Targets using VulnHub.com
- Metasploitable 2 & 3
- OWASP Webgoat
- Create your own VM Targets with vulnerable software from Exploit-DB.com

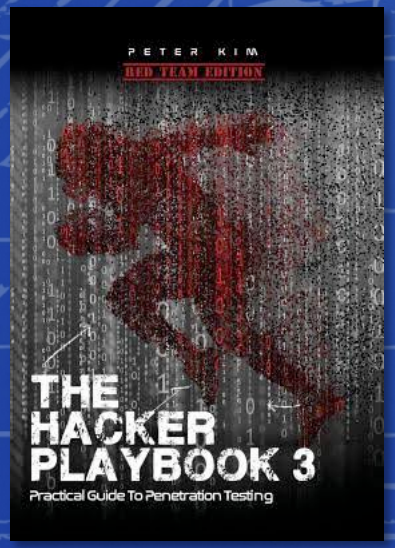
Recommended Reading



Penetration Testing

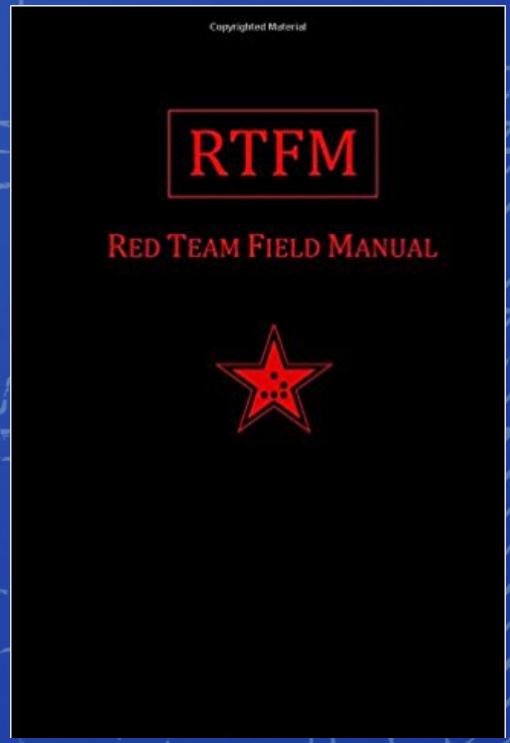
A Hands-On Introduction to Hacking

The Hackers Playbook 2 & 3



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

RTFM: Red Team Field Manual



Learning Resources

- SANS Institute: sans.org
- eLearn Security: eLearnSecurity.com
- Virtual Hacking Labs: virtualhackinglabs.com
- Pentester Academy: pentesteracademy.com
- Pentester Lab: pentesterlab.com
- Practical Pentest Labs: practicalpentestlabs.com

- Bugcrowd University: bugcrowd.com/university/
- SANS Pentesting Blog: pen-testing.sans.org/blog/
- HackingTutorials.org
- Cybrary.it
- Web Security Academy: https://portswigger.net/web-security
- owasp.org
- Hack The Box: hackthebox.eu
- Over The Wire CTF: overthewire.org/wargames/

https://thehackermaker.com/learning-resources/

Certifications

Entry Level

- CEH - eCCouncil
- PenTest+ - CompTIA

Intermediate

- GPEN – SANS/GIAC
- OSCP – Offensive Security

Advanced

- GxPN – SANS/GIAC
- OSCE – Offensive Security

Job Tips

- Professional Networking
  - Community: Clubs/groups and conferences
  - LinkedIn
- Interview Tips
  - Prepare for interviews
    - Know the OWASP Top 10
    - Be able to explain the basics like 3-way TCP handshake and OSI Model

Contact

/In/PhillipWylie

Phillip.Wylie@gmail.com

@PhillipWylie

The Pwn School Project
PwnSchool.com

Ethical Hacking Class & Web App Pentesting
@ Richland College
TheHackerMaker.com