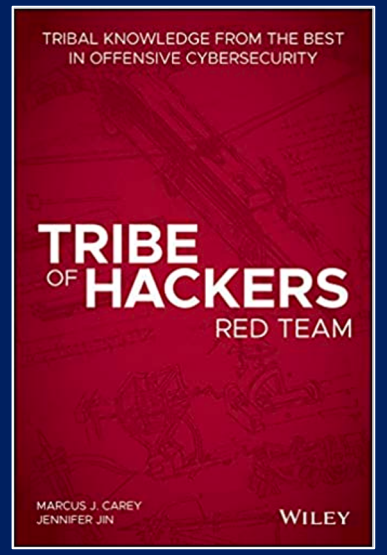
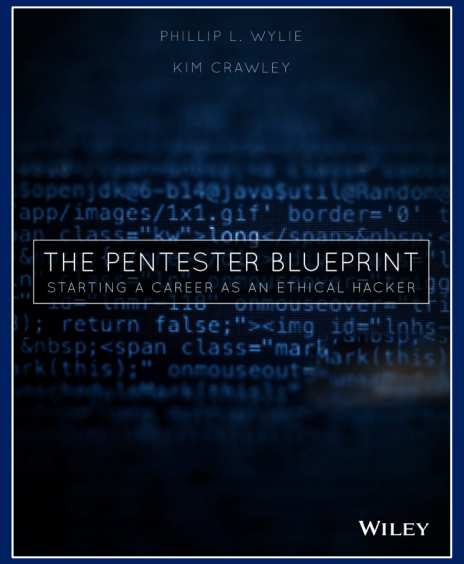
INSIDE THE MIND OF A THREAT ACTOR

Beyond Pentesting

whoami :
Phillip Wylie, CISSP, OSCP, GWAPT

- Penetration Tester
- Adjunct Professor @ Dallas College
- The Pwn School Project Founder
- Featured in the "Tribe of Hackers Red Team"
- Co-author of "The Pentester Blueprint: Starting a Career as an Ethical Hacker"
- "The Hacker Factory" podcast host
- **Innocent Lives Foundation** Ambassador & Champion
- **Hacking is NOT a Crime** Advocate & Board Member





My Offensive Security Career Path

Pro Wrestler > CAD Drafter > Sysadmin > Infosec > AppSec > **Pentester** > **Red Team** > **Cloud Pentester**

AGENDA

- My Offensive Security Career Path
- What is Offensive Security?
- Offensive Security Domains
- Red Team Intro
- Red Team Tools
- Red Team Blueprint
- Resources

HACKING IS NOT A CRIME

"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 OFFENSIVE SECURITY?

- Assessing the security of a target using adversarial tactics, techniques, and procedures (TTPs)
- Commonly known as ethical hacking

OFFENSIVE SECURITY DOMAINS

- Pentesting
  - Network
  - Application
  - Cloud
  - Social Engineering
  - Physical Security
  - Hardware
  - Vehicle
- Red Teaming

RED TEAM != PENTESTING

The terms **Red Team** and **Pentesting** have been used interchangeably. While there are similarities, there are distinct differences between true Red Teaming and Pentesting.

COMMONALITIES

Red Team

- Exploitation
- Social Engineering
- Phishing
- Physical Security Exploitation

Pentesting

- Exploitation
- Social Engineering
- Phishing
- Physical Security Exploitation

DIFFERENCES

Red Team

- Threat Actor Emulation
- Detection Avoidance
- Less Restrictive Scope

Pentesting

- No Threat Actor Emulation
- No Detection Avoidance
- More Restrictive Scope
- Vulnerability Focus

TOOL COMMONALITIES

Red Team

- Linux Attack Platforms
- Windows Attack Platforms
- Linux Based Tools
- Windows Based Tools
- Metasploit
- Malware & Exploits
- Command and Control (C2)

Pentesting

- Linux Attack Platforms
- Windows Attack Platforms
- Linux Based Tools
- Windows Based Tools
- Vulnerability Scanners
- Metasploit
- Malware & Exploits
- Command and Control (C2)

RED TEAM INTRO

- Scenario based security assessment emulating threat actors and even simulating specific APTs (Advance Persistent Threat). A goal of a Red Team operation is to simulate real-world breaches. Not only is the operator testing the security of the technology, they are testing the people, and processes.

“The Red Team tests the Blue Team”
– Wirefall (Dallas Hackers Association, Founder)

RED TEAM INTRO

- Red team operations take more time to plan and perform.
- Red team operations rely heavily on OSINT to enumerate information on target technologies and employees. Employees are leveraged through social engineering and phishing to gain an initial foothold in the target environment.
- Detection avoidance is very important to be successful in red team operations. We are impersonating a threat agent.

RED TEAM TTPS

- Red team operations rely on malware payloads to gain initial footholds.
- Evasion and obfuscation is very important for malware success.
- Command & Control (C2) is an important tool used to control compromised systems, deliver payloads, elevate privileges, lateral movement, and used for persistence.

RED TEAM OPS PLANNING

- Planning red team ops can very detailed and mapped to ATPs from the MITRE ATT&CK Framework and tools like VECTR.
- Red team ops can be less complicated and not mapped to specific APTs using common TTPs.

RED TEAM ADDITIONAL BENEFITS

- Tests people, process, and technology
- If activities are not detected the red team can work with security to tune the security defense systems to detect malicious activity.
- This can be extended to purple teaming to further enhance detection capabilities.

BECOMING A RED TEAM OPERATOR

Building the Base

- Technology Basics
  - Networking
  - Operating Systems
  - Active Directory
- Pentesting/Hacking
  - Techniques
  - Tools
- Programming & Scripting
  - Python
  - PowerShell
  - Go Lang
  - C#

BECOMING A RED TEAM OPERATOR

Red Team Focused Skills

- Malware & Exploit Development
  - Obfuscation & Evasion
- Active Directory Exploitation
- Command & Control (C2)
- Phishing
- Social Engineering
- Physical Security Exploitation

BECOMING A RED TEAM OPERATOR

Learning Path – Hacking Skills

- OSCP
- Hack The Box
- Social Engineering

Learning Path – Red Team Skills

- **Pentester Academy – Red Team Labs**
- **eLearn Security – Penetration Testing Extreme**
- **Hack The Box Pro – Rasta Labs**
- **Zero-Point Security –** Red Team Ops (Rastamouse)

RESOURCES: TOOLS

APT Planning

- attack.mitre.org
- vectr.io

Command and Control (C2)

- C2 Matrix - thec2matrix.com
- Cobalt Strike
- Silent Trinity
- Empire w/ Star Killer
- DeimosC2 – Critical Start/Team Ares

Operating Systems

- Slingshot Linux - sans.org/slingshot-vmware-linux/
- Kali Linux
- Parrot OS Linux
- Commando VM - Windows

RESOURCES: COURSES

- Hack The Box Pro Labs - RastaLabs (Rastamouse)
- Pentester Academy - Red Team Labs
- institute.sektor7.net
- Zero-Point Security - Red Team Ops (Rastamouse)
- eLearn Security Penetration (INE) - Testing Extreme
- SpecterOps - Adversary Tactics: Red Team Operations
- FortyNorth - Initial Access Operations & Intrusion Operations
- Silent Break Security - Dark Side Ops: Malware Dev & Dark Side Ops 2: Adversary Simulation
- SANS - SEC564: Red Team Exercises and Adversary Emulation
- cobaltstrike.com – Cobalt Strike videos and content (Training & Support)

RESOURCES: CERTIFICATIONS

Red Team Focused

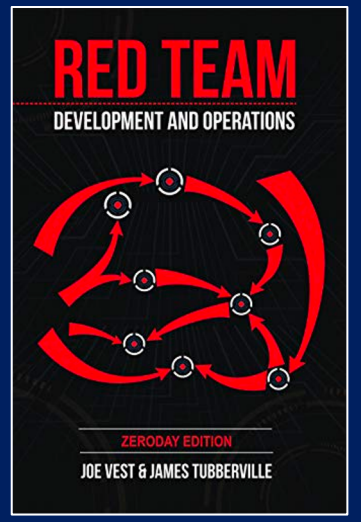
- Zero-Point Security - Certified Red Team Operator (CRTO)
- Pentester Academy - Certified Red Teaming Expert
- eLearn Security (INE) - Certified Penetration Tester eXtreme

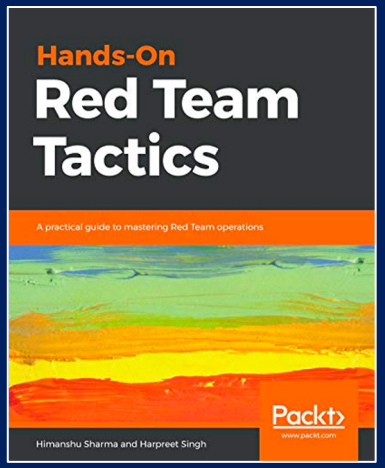
Pentesting Focused

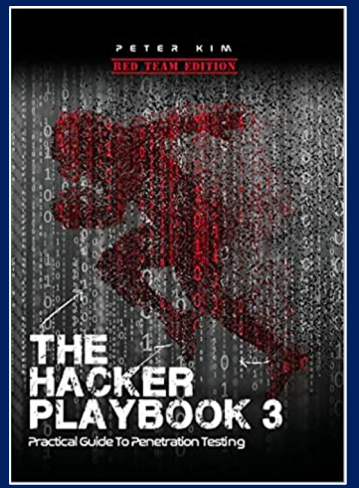
- Offensive Security – OSCP, OSCE, OSWE
- SANS/GIAC – GPEN, GXPN, GWAPT
- eLearn Security – eCPPT, eCXD, eWPT

RESOURCES: BOOKS

- Red Team Development and Operations: A practical guide
- Hands-On Red Team Tactics: A practical guide to mastering Red Team operations
- The Hacker Playbook 3: Practical Guide To Penetration Testing [Red Team edition]







RESOURCES: BLOGS

- redteamjournal.com/blog/
- redteam.guide/docs/
- threatexpress.com
- byt3bl33d3r.github.io
- blog.harmj0y.net
- bc-security.org/blog/
- posts.specterops.io
- rastamouse.me
- hausec.com
- silentbreaksecurity.com/blog/
- fortynorthsecurity.com/blog/
- ired.team
- vincentyiu.com

CONTACT

/In/PhillipWylie

Phillip.Wylie@gmail.com

@PhillipWylie

The Pwn School Project
PwnSchool.com

TheHackerMaker.com

The Hacker Factory Podcast
ITSPmagazine.com