LEAD WITH CONFIDENCE

ISC2™ | SECURITY CONGRESS 2023

isc2.org/Congress | #ISC2Congress

How to Get the Penetration Testing Experience You Need

Phillip Wylie, phillip.wylie@gmail.com

$whoami

Phillip Wylie, CISSP, OSCP, GWAPT

- Offensive Security Professional
- 19 plus years cybersecurity including 10 plus years of offensive security
- Former Adjunct Instructor @ Dallas College
- DEF CON 940 Founder
- Concept creator & coauthor of “The Pentester Blueprint: Starting a Career as an Ethical Hacker”
- Featured in “Tribe of Hackers Red Team”
- Podcaster and host of “The Phillip Wylie Show” and previously “The Hacker Factory Podcast”

My Offensive Security Career Path

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

What is pentesting?

What is Pentesting?

- Assessing security from an adversarial perspective using hacking tools and techniques.
- Pentesting is also referred to as ethical hacking.
- Pentesting is an offensive security assessment type.

Offensive Security Types

- Vulnerability Assessment
- Pentesting
- Adversary Emulation aka Red Teaming

Offensive Security Types Comparison

- Vulnerability Assessment – vulnerability discovery and validation
- Pentesting – vulnerability discovery and validation, exploitation and post exploitation
- Adversary Emulation aka Red Teaming – emulating a threat actor, testing defenses technology, response, and ability to stop

Pentesting Experience

Pentesting Tools

Network Vulnerability Scanners - Nessus, Nexpose, OpenVas, Nuclei

Operating Systems

- Linux - Kali, Parrot OS,
- Windows Commando VM, Flare VM

Pentesting Tools

- Port and service scanners – Nmap, Masscan
- Exploit tools - Metasploit, Core Impact, Exploit Pack
- Password and hash cracking – Hashcat, John the Ripper, CrackMapExec, Responder

Web App Pentesting Tools

- Interception proxies - Burp Suite, OWASP ZAP
- Web App Vulnerability Scanners - Web Inspect, AppScan, Acunetix, Invicti, Nikto, Nuclei
- Fuzzers – Ffuf, Wfuz, GoBuster, Feroxbuster

Pentesting Skills

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

Hands-on Experience: Labs

- CTFs (capture the flags)
- HackTheBox
- TryHackMe
- Home Lab using Vulnerable VMs

Hands-on Experience: Real World

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

Hands-on Experience: CVEs

- 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 Experience: CVEs

- 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 Skills

Demonstrating Skills

- Write ups, articles, blog posts on GitHub, Medium, or Blog
- 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

Building Your Brand

Building Your Brand

Content Creation

- Streaming
- Video - YouTube, Instagram
- Writing

Speaking

- Conferences
- Cybersecurity Meetings

Professional Networking

Professional Networking

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

Let’s connect!

LinkedIn: PhillipWylie

X (formerly Twitter): @PhillipWylie

Instagram: @PhillipWylie

YouTube: @PhillipWylie

Podcast: phillipwylieshow.com

Website: thehackermaker.com

LEAD WITH

ISC2™ | SECURITY CONGRESS **2023**

CONFIDENCE

isc2.org/Congress | #ISC2Congress

Thank You!

Phillip Wylie