
THE ETHICAL
HACKER
NETWORK


EH-NET
Live!

Burp-less Hacking

Learning Web Application Pentesting on a Budget

Dec 19, 2019

PRESENTER:

Phillip Wylie

AGENDA

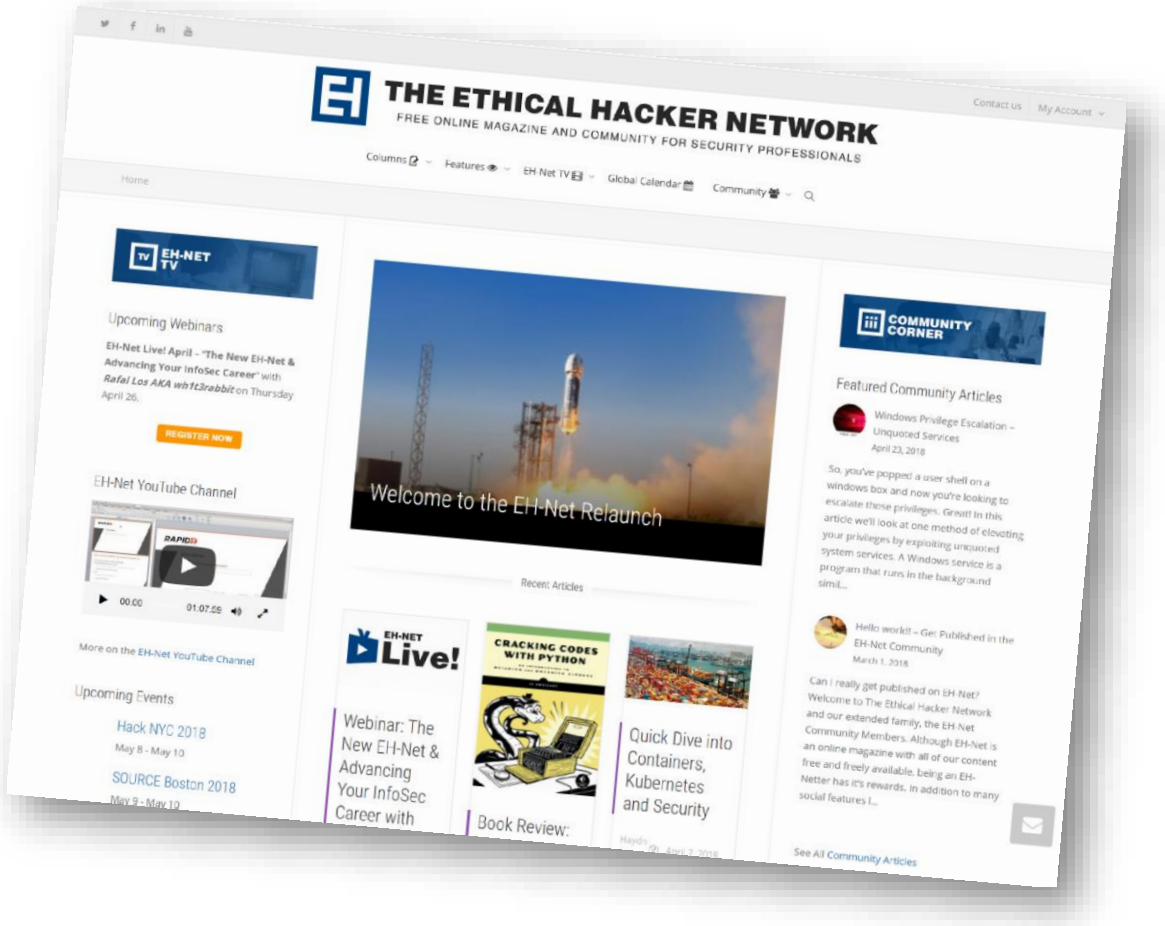
- Intro by Don Donzal, EH-Net Editor-in-Chief
- Bio – Phillip Wylie
  - What is WebApp Pentesting?
  - FOSS Tools of the Trade
  - The Setup – What is used for the demo
  - Live WebApp Pentest!
  - Career Advice
  - Study and Practice Resources
- Special Announcement from eLS!
- Q&A

INTRO

- Video will be made available on EH-Net
- Style = Interview!
  - Q&A in question tab in GTW
  - Twitter using #EHNet
- Post Game in EH-Net "**Web App Pen Testing**" Group: https://www.ethicalhacker.net/groups/web-app-pen-testing/
- Goal for today – Spark conversation. Advance your career!

OVERVIEW OF THE NEW EH-NET

- General Layout
  - Magazine side - Columnists, Features, Global Calendar
  - Community side – Members & Profiles, Activity, Forums, Groups, Community Articles
- Building your “Personal Ethical Hacker Network”
- Hello world! – Get Published in the EH-Net Community
- Limited Time – All new members get a free pen testing course from eLS!!



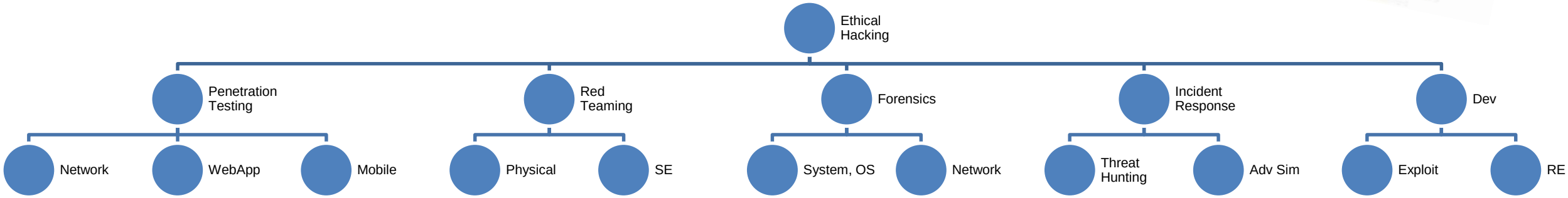
BIO – Phillip Wylie

Phillip Wylie is the Red Team Lead for a global conglomerate. Phillip is also an Adjunct Instructor at Richland College teaching Ethical Hacking and System Defense, a Bugcrowd Ambassador and the founder of The Pwn School Project. Phillip has over 21 years of experience in InfoSec and IT and has performed pentests on networks, wireless networks, applications including thick client, web application and mobile. Phillip has a passion for sharing, mentoring and educating. This passion was his motivation to start teaching and founding The Pwn School Project, a free monthly educational meetup with a focus on hacking. Phillip holds the following certifications; CISSP, NSA-IAM, OSCP, GWAPT. Follow him @PhillipWylie

DEF: ETHICAL HACKING

Performing computer security related activities with permission.

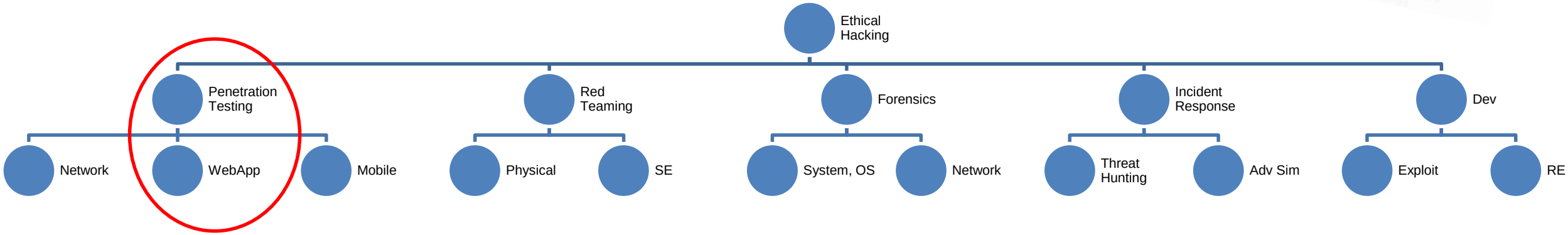
- Oxymoron? Nope
- Media focus on crime = negative association
- More specific term for clarification
- Good guys using bad guys' tools & techniques
- Umbrella term to include numerous specialties
- WebApp = Sub-Category of Pentesting



DEF: WEBAPP PENTESTING

What is Web Application Security Testing?

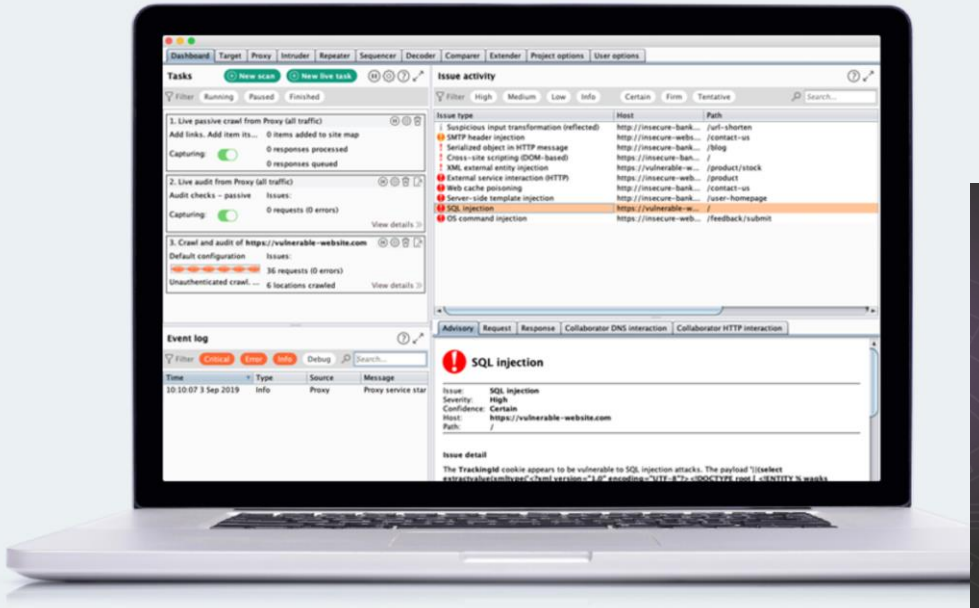
A security test is a method of evaluating the security of a computer system or network by methodically validating and verifying the effectiveness of application security controls. A web application security test focuses only on evaluating the security of a web application. The process involves an active analysis of the application for any weaknesses, technical flaws, or vulnerabilities. Any security issues that are found will be presented to the system owner, together with an assessment of the impact, a proposal for mitigation or a technical solution. -OWASP



Is Burp Really That Bad? Not at All!

Burp Suite Professional_

The go-to toolkit for penetration testing and bug bounty hunting



Enterprise

Automated protection for organizations and development teams

- ✓ Web vulnerability scanner
- ✓ Scheduled & repeat scans
- ✓ Unlimited scalability
- ✓ CI integration
- ✗ Advanced manual tools
- ✗ Essential manual tools

From $3,999 per year

Try for free | Buy now

Find out more »

Professional

#1 tool suite for penetration testers and bug bounty hunters

- ✓ Web vulnerability scanner
- ✗ Scheduled & repeat scans
- ✗ Unlimited scalability
- ✗ CI integration
- ✓ Advanced manual tools
- ✓ Essential manual tools

$399 per user, per year

Try for free | Buy now

Find out more »

Community

Feature-limited manual tools for researchers and hobbyists

- ✗ Web vulnerability scanner
- ✗ Scheduled & repeat scans
- ✗ Unlimited scalability
- ✗ CI integration
- ✗ Advanced manual tools
- ✓ Essential manual tools

Get Community

What is “FOSS”?

FOSS

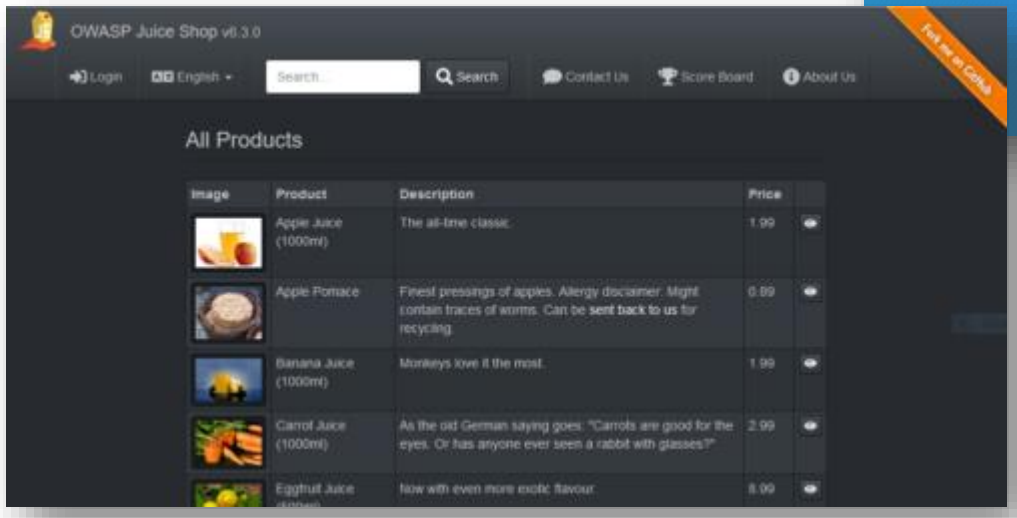
[ˈfäs]
NOUN

Free Open Source Software (FOSS) is code that is “freely licensed to use, copy, study, and change the software in any way, and the source code is openly shared so that people are encouraged to voluntarily improve the design of the software.”

Source: FOSS entry on Wikipedia

THE SETUP

- PTES
- Docker
- VMs
- Tools
- Hardware



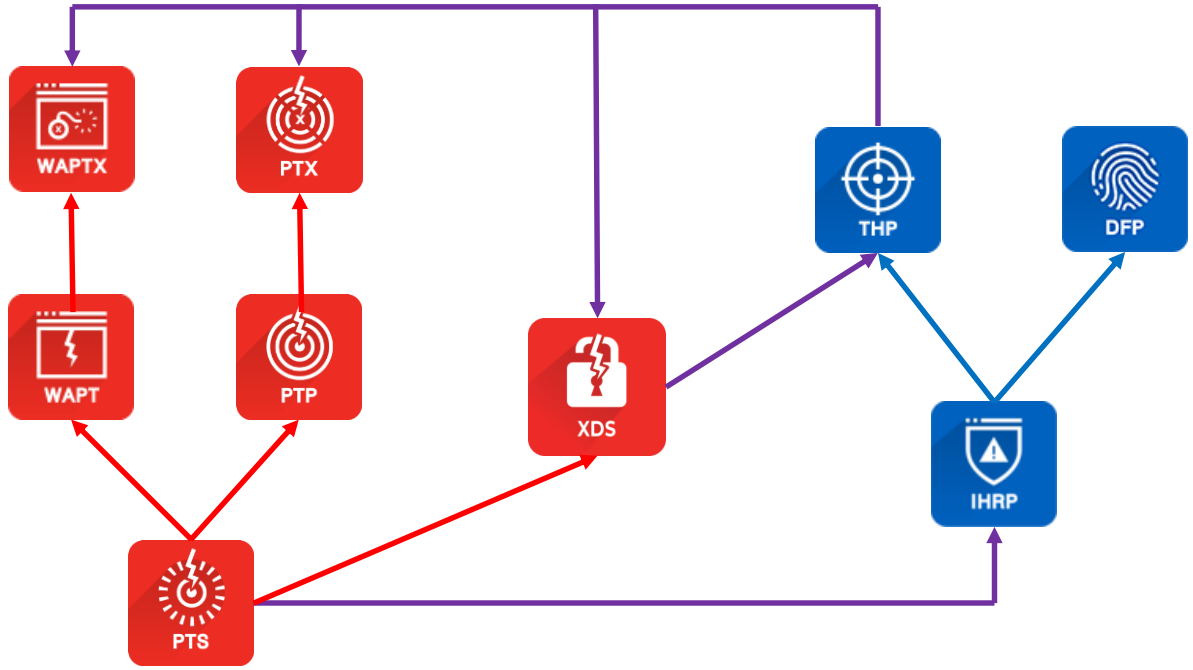
LIVE WEBAPP PENTEST!

CAREER OPPORTUNITIES

- Incident Responder
- SOC Analyst
- AppSec Analyst
- Project Manager
- Penetration Tester
- Red Team Member
- Bug Bounty Hunter

HOW DO I GET THERE?

- Experience – CTFs, Employment, Home lab, Non-profits, Open source projects, etc.
- Practical Training – eLearnSecurity Training Paths (NIST-NICE Role-based Training)
- Will playing CTFs get me a job?



https://www.elearnsecurity.com/course/

JOB INTERVIEW TIPS

- Methodology
- OWASP Top 10
- Soft Skills
- Extracurriculars
- Ability to Learn
- Be Resourceful
- Part of a Team
- Ability to Lead & Be Lead

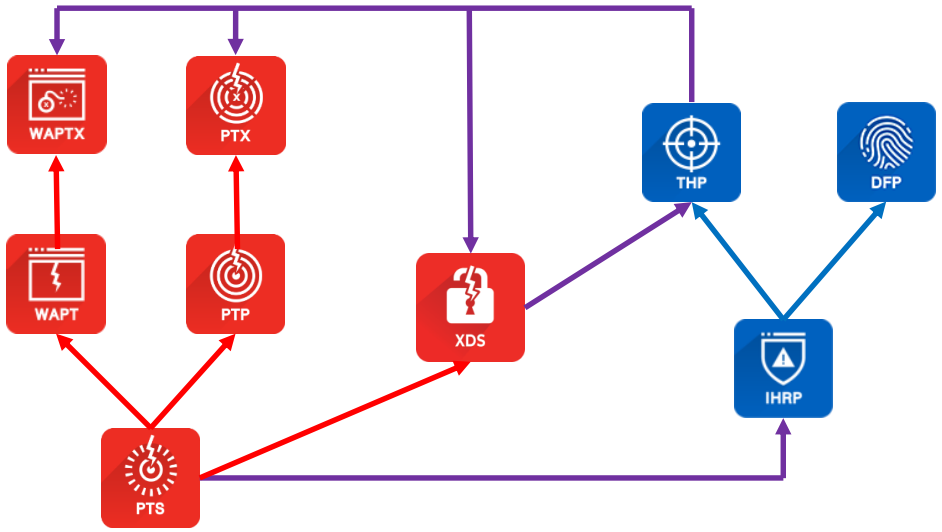
BUILDING YOUR SKILLSET – PHILLIP'S RESOURCE LIST

- The Pwn School Project
- FOSS Tools - OWASP ZAP, Nmap, Nikto, Sqlmap, Wfuzz, OSINT, Post-Exploitation
- Local PentestLab Management Script – bWAPP, WebGoat 7.1, WebGoat 8.0, DVWA, Mutillidae II, OWASP Juice Shop, WPScan Vulnerable Wordpress, OpenDNS Sec Ninjas, Altoro Mutual
- Others – Hack.me, VulnHub.com, Metasploitable, CTFs
- Books et al - WebApp Hacker's Handbook, Tribe of Hackers, Kali Linux Revealed, OWASP Testing Guide, Portswigger WebAppSec Academy
- @PhillipWylie, @EthicalHacker

COMING IN 2020!

eLearnSecurity
Forging security professionals

- Numerous course updates in Q1 and throughout 2020
- Coming in Early Q1
  - ATTN: Bug Hunters!
  - Lab Heavy Course
  - New Enhanced Content
- New Courses & Tech in 2H



Stay Tuned!!

https://www.elearnsecurity.com/course/

Q&A

POST GAME IN EH-NET GROUPS

THANK YOU

FOR JOINING

EH-NET Live!

THE ETHICAL HACKER NETWORK

Follow us:

www.ethicalhacker.net
team@ethicalhacker.net