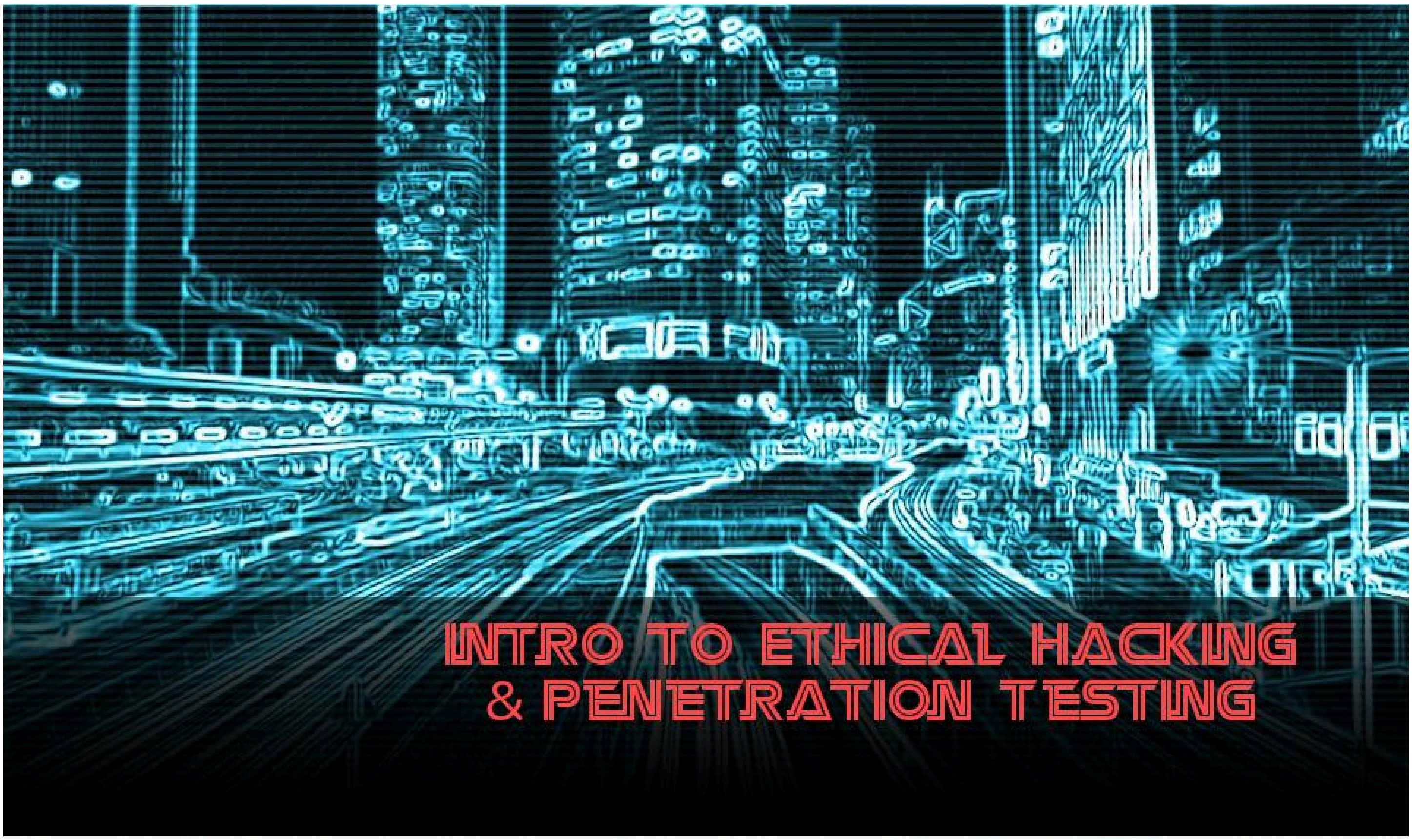

The Bay Area School of Hacking (BASH) Presents:

Intro to Ethical Hacking & Penetration Testing

Course Syllabus

Authored by:
David Porcello, founder of Pwnie Express &
Bay Area School of Hacking (BASH)

Course Description

Ethical hacking (aka penetration testing) is an important part of any holistic cybersecurity strategy. By simulating the capabilities of real-world attackers, penetration testers identify gaps in security controls and measure the effectiveness of an organization’s security program.

This introductory 1-day course is a technical, hands-on, labs-based walkthrough of the penetration testing process, with coverage of industry-standard tools and techniques used by pentesting professionals.

Based on industry-standard methodologies such as the Penetration Testing Execution Standard (PTES), this course is intended as a primer to prepare you for a college-level security testing course or industry certification program, such as Comptia Pentest+, SANS GPEN, CEH, or OSCP.

Learning Objectives

Upon successful completion of this class you will understand how ethical hackers use their professional skills to:

- Engage in an authorized penetration test
- Conduct online intelligence gathering
- Scan & enumerate target systems
- Test password strength
- Open password-protected files
- Subvert vulnerable software applications
- Monitor keystrokes & user activity
- Leverage common phishing techniques
- Create backdoored programs & documents
- Test web application security
- Escalate privileges to gain administrator access

You'll also get:

- A 70-page technical guide with step-by-step instructions & screenshots.
- A hosted lab environment so you can continue practicing on your own.
- Additional tools, resources, & techniques to take your skills to the next level.

Instructor Bio

David Porcello is an independent security researcher, consultant, instructor, presenter, founder of Pwnie Express, and creator of the award-winning Pwn Plug and other security testing devices featured in Wired, Ars Technica, PC Magazine, Forbes, Good Morning America, and "Mr. Robot". David has created covert hacking devices for DARPA, hosted workshops at the Defcon security conference, and provided technical expertise for NPR's Project Eavesdrop. In his 25 years of field experience, David has served as Principal Security Engineer at Udemy, adjunct cybersecurity professor at Norwich University, and Security Director for Vermont Mutual Insurance Company.

Course Outline

Getting Started:

- What is Ethical Hacking?
- Course Tips for Success
- Authorization & Consent
- Getting the Course Materials
- Accessing the Lab Environment
- Kali Linux Basics

Intelligence Gathering:

- Open-Source Intelligence (OSINT)
- Google recon

Scanning & Enumeration:

- Port scanning
- Service enumeration
- Vulnerability scanning

Password Cracking:

- Password spraying
- Password searching
- Password-protected files
- Online cracking
- Offline (hash) cracking

Software Exploitation:

- Metasploit
- Meterpreter

Social Engineering:

- Spear phishing
- Credential harvesting
- Fake software updates
- Backdoored PDF files

Web Application Pentesting:

- Directory brute-forcing
- Hacking Wordpress
- Parameter fuzzing
- Local File Inclusion (LFI)
- Log poisoning & Remote Code Execution (RCE)

Privilege Escalation:

- Linux privilege escalation
- Windows privilege escalation

Wrapping up:

- Pentesting Standards
- Pentesting Books
- Pentesting Practice Labs
- Pentesting Certifications
- Hacking/Security Conferences

Prerequisites

- A Windows, Mac, or Linux laptop with working wifi is required to access the hosted lab environment.
- Some experience with the Windows/macOS/Linux command line, computer networking, and web technologies is recommended.