Intro to Ethical Hacking & Penetration Testing

Course Syllabus

Author: Dave Porcello
grep8000 [at] gmail [dot] com
https://packetbeard.blogspot.com
Twitter: @DavePorcello

Course Description

This workshop is a beginner's introduction to the ethical hacking process. Also known in the industry as "penetration testing", ethical hacking is a highly in-demand skill set, exciting profession, and key part of any organization's cybersecurity program.

Through understanding how cyber attacks really work, we can more effectively protect ourselves. In simulating the capabilities of real-world cyber attackers, ethical hackers identify gaps in security controls and provide a realistic measurement of business risk. In essence, ethical hackers find security holes before the real cyber criminals do.

Using hands-on labs and step-by-step technical walkthroughs, we'll cover the real-world tools and techniques used by today’s ethical hacking professionals.

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 Windows password strength
- Open password-protected files
- Subvert vulnerable software applications
- Monitor keystrokes & user activity
- Leverage common phishing techniques
- Create backdoored programs & documents

You'll also get:

- A 40+ page technical guide with step-by-step instructions & screenshots.
- A portable lab environment so you can continue practicing on your own.
- Additional tools, resources, & techniques to take your skills to the next level.

Course Outline

Getting Started:

- What is Ethical Hacking?
- Course Tips for Success

- Authorization & Consent
- Gear Check
- Getting online
- Getting the Lab Materials
- Installing VirtualBox
- Importing the Lab VMs
- Kali Linux basics

Intelligence Gathering:

- Open-Source Intelligence (OSINT)
- Google recon

Scanning & Enumeration:

- Port scanning
- Service enumeration
- Vulnerability scanning

Software Exploitation:

- Metasploit
- Meterpreter

Password Cracking:

- Password guessing
- Online cracking
- Password-protected files
- Offline (hash) cracking

Social Engineering:

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

Wrapping up:

- Pentesting Standards
- Pentesting Books
- Pentesting Practice Labs
- Pentesting Certifications

Class Prerequisites

To participate in this class, you will need:

- A Windows or Mac laptop with:

  - Windows 8/10 or macOS
  - Working WiFi hardware
  - 64-bit CPU (1.8GHz+ / 4 cores recommended)
  - At least 8GB memory (16 recommended)
  - 50GB free disk space

  SHARED OPTION: If you are unable to run all lab virtual machines on your laptop, you will still be able to participate by using one of the shared lab systems.

- Intermediate-to-advanced proficiency using your computer's operating system.
- Some experience with the Windows/Mac/Linux command line, computer networking, and web technologies is recommended.

Instructor Bio

Dave 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 on Good Morning America, NPR, CNN, Forbes, Wired, and "Mr. Robot". In his 20 years of field experience Dave has also served as Security Director for Vermont Mutual, cybersecurity professor at Norwich University, and advisor for NPR and several public figures.

Legal Disclaimer

In this class we will be conducting various computer security assessment techniques within a safe and isolated lab environment. Accessing computer systems or information outside of this environment without proper authorization is not just unethical, but also highly illegal and may be punishable under the U.S. Computer Fraud and Abuse Act, among other U.S. and international laws and regulations. As the instructor of this class, I do not condone or support the use of these tools or techniques in support of any unauthorized, non-consensual, illegal, or unethical activities. By participating in this class you must agree to these terms and will be required to sign a waiver before accessing the lab systems.