Phillip Wylie

Starting a Career as an Ethical Hacker

MY PATH INTO CYBER

- System Administrator
- Network Security
- Application Security
- Pentesting

Agenda

- My Path Into Cyber
- What is Ethical Hacking?
- Ethical Hacking Jobs
- Starting a Career as an Ethical Hacker
- Learning Resources
- Certifications & Degrees

About Me

- Offensive Security Professional
- Offensive Security Educator
- 23+ Years IT and Cybersecurity Experience
- Associates Degree in Computer Networking
- Certifications – OSCP, GWAPT, CISSP

My Path Into Cyber

- System Administrator
- Network Security
- Application Security
- Pentesting (Ethical Hacking)

Permission to Hack

"With great power comes great responsibility."

Only hack if you have permission and even better written permission. Hacking without permission is illegal.

What is Ethical Hacking?

- Assessing security from an adversarial perspective, attempting to exploit vulnerabilities to gain unauthorized access to systems and sensitive data (aka hacking).
- Penetration Testing or Pentesting for short, is the professional term for ethical hacking.
- Ethical Hacking is a type of security assessment.

Why Ethical Hacking Important

- Assesses security from an adversarial perspective
- Better understanding of security risk severity
- Exploitable (hackable) vulnerabilities are higher risk and a higher priority for remediation as well as justification for budgeting.

Ethical Hacking Jobs

- Penetration Tester
- Social Engineer
- Red Team Operator
- Bug Bounty Hunter
- Security Researcher

Ethical Hacking Skills In Other Areas

- SOC (Security Operations Center) Analysts
- Network Security Analysts and Engineers
- DFIR (Digital Forensics and Incident Response
- Purple Teams (where defensive and offensive security collaborate to improve defenses)
- Application Security

Ethical Hacking Targets

- Networks – Wired, Wireless
- Applications – Web App, Binary, Mobile, Cloud
- Hardware – Network Hardware, IoT (Internet of Things), Medical Devices
- Transportation – Automobiles, Trucks, Mass Transit
- People – Social Engineering
- Buildings – Physical Security (often Included in Social Engineering)

Ethical Hacking Methodology

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

- *Reference: Penetration Testing Execution Standard (PTES) - www.pentest-standard.org*

Types of Security Assessments

- Vulnerability Scans – just running a vulnerability scanner.
- Vulnerability Assessments – vulnerability scanning plus vulnerability validation.
- Pentest – Vulnerability Assessment plus exploitation (aka hacking)
- Red Team/Adversarial Tests – testing blue teams, attack simulation, less restrictive scope

Starting a Career as an Ethical Hacker

Technical Skills

- Computer Hardware – CompTIA A+
- Operating Systems (Windows & Linux) - CompTIA A+
- Networking – CompTIA Network+
- Security - CompTIA Security+
- Coding – Scripting & Programming

Starting a Career as an Ethical Hacker

Hacking Skills

- CTFs (Capture The Flag)
- Bug Bounties
- Online Hacking Platforms - Hack The Box & Try Hack Me
- Home Lab

Learning Resources

Paid Resources

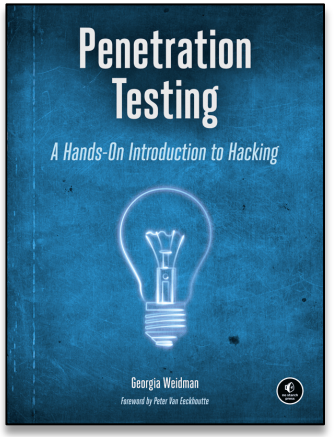
- SANS Institute: sans.org
- INE (formerly eLearn Security): ine.com
- Offensive Security: offensive-security.com
- Pentester Academy: pentesteracademy.com
- Pentester Lab: pentesterlab.com
- The Cyber Mentor: academy.tcm-sec.com

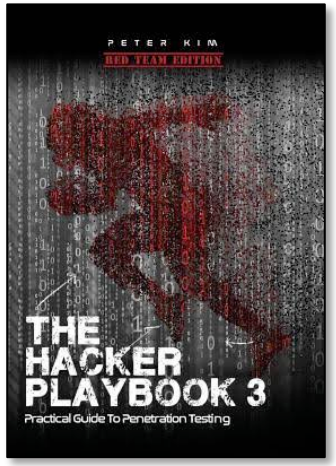
Free Resources

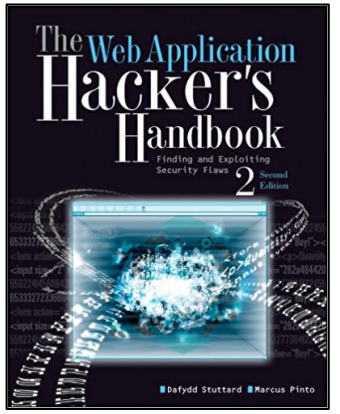
- Bugcrowd University: bugcrowd.com/university/
- HackerOne: hacker101.com
- SANS Pentesting Blog: pen-testing.sans.org/blog/
- HackingTutorials.org
- Web Security Academy: portswigger.net/web-security
- owasp.org
- Hack The Box: HackTheBox.eu (free & paid)
- Try Hack Me: TryHackMe.com (free & paid)
- Over The Wire CTF: overthewire.org
- Under The Wire CTF: underthewire.tech

Books

- Penetration Testing
  A Hands-On Introduction to Hacking
- The Hackers Playbook 2 & 3
- The Web Application Hacker's Handbook:
  Discovering and Exploiting Security Flaws 2nd Edition







Certifications

Entry Level
- CEH – eC-Council
- PenTest+ - CompTIA
- eJPT – eLearn Security/INE

Intermediate
- GPEN – SANS/GIAC
- OSCP – Offensive Security
- eCPPT – eLearn Security/INE
- GWAPT – SANS/GIAC
- eWPT – eLearn Security/INE

Advanced
- GxPN – SANS/GIAC
- OSCE – Offensive Security
- eCPTX – eLearn Security/INE
- eWPTX – eLearn Security/INE

Degrees

- Computer Science
- Cybersecurity
- Software Development
- Information Technology
- SANS Masters Degree (most ethical hacking related courses)

Take A Ways

- Learn Technology
  - Computers
  - Networking
  - Coding - Scripting & Programming
- Learn to Hack
  - CTFs
  - Online Hacking Platforms – Hack The Box & TryHackMe
  - Home Lab
  - Bug Bounties

Thank you!