BISHOPFOX

SO YOU WANNA BE A PENTESTER

PENETRATION TESTING **RESOURCE GUIDE**

Looking to break into pen testing? There's a lot you can do on your own. Many of our consultants have built their careers on development and security self-study.

THESE RESOURCES WILL HELP YOU GET STARTED:

LEARN MORE ONLINE

- **PentesterLab** – An introduction to pen testing via tutorials, plus hands-on challenges based on common vulnerabilities
- **Cybrary** – High-quality (and free!) videos on cybersecurity and IT topics, with certificates of completion for courses and CPEs that can be applied towards security certifications
- **Coursera** – Online classes on technical and professional development topics, including programming, with certifications and specializations available
- **OWASP Top 10** – A regularly updated report from the Open Web Application Security Project detailing the 10 most critical risks for web application security

LEARN MORE THE OLD-FASHIONED WAY

- **Web Application Security:** A Beginner's Guide
  — Bryan Sullivan and Vincent Liu*
- **Penetration Testing:** A Hands-On Introduction to Hacking
  — Georgia Weidman
- **Professional Penetration Testing:** Creating and Learning in a Hacking Lab
  — Thomas Wilhelm*
- **The Tangled Web:** A Guide to Securing Modern Web Applications
  — Michal Zalewski
- **Web Application Hackers Handbook:** Finding and Exploiting Security Flaws
  — Dafydd Stuttard

* Bishop Fox partner and/or consultant

GET FAMILIAR WITH INDUSTRY STANDARD TOOLS

- Kali Linux – A Linux distribution that comes preloaded with security tools
- Burp Community Edition – An integrated platform for performing security testing of web applications
- Nmap – A security scanner used to discover hosts and services on networks
- Virtual Box – An application that allows you to simultaneously run multiple operating systems inside multiple virtual machines
- Amazon Web Services (AWS) – Use Amazon Elastic Compute Cloud (EC2) to create and run virtual machines, or instances, in the cloud

TEST YOUR SKILLS

- OverTheWire – Level-based war games designed to help users learn and practice security
- HackThisSite – Articles, forums, and projects, plus web application and programming challenges for all user levels
- OWASP Broken Web Applications Project – A downloadable collection of vulnerable web apps distributed on a virtual machine
- VulnHub – A catalogue of downloadable, intentionally vulnerable, virtual machines, with walkthroughs challenging users to compromise Windows, Linux, and other hosts
- Hack The Box – Host servers you can practice breaking into to capture the flag
- Pursue a Certification – The Offensive Security Certified Professional (OSCP) or GIAC Penetration Tester (GPEN) are both well respected

JOIN YOUR LOCAL SECURITY COMMUNITY

Check out your local OWASP, 2600, BSides, and other chapters to meet up with security enthusiasts in your area!

WANT MORE INFORMATION?

Find free tools, style guides, security paths, and more on the Bishop Fox website, www.bishopfox.com. You will find a comprehensive list of vulnerable web apps, operating system installations, old software, and war game.

Visit **BishopFox.com**

BISHOPFOX