Getting Into Pentesting – A Recruiters Perspective

James Riley
Penetration Tester & TVM
Recruitment Specialist
Who Am I?

A specialist recruiter of 2 years focusing on penetration testing market exclusively

Work with 80% of the market in pentesting so have a good unbiased view of most companies hiring practices

Active within the community - Silver Sponsor of Bsides London and Manchester,
Member of the ISSA-Uk London Chapter and exhibitor at InfoSec Europe

....Definitely Not Marcus Hutchins
What is Penetration Testing?
Black Hats & White Hats

Black Hats (The Bad Guys) These are the rogue hackers you see in movies that maliciously crack systems to try and hold company & customer data to ransom.

Grey Hats - they will illegally hack a companies infrastructure to highlight a vulnerability to the owners. They will often set a deadline for the company to patch this before publishing it online to draw attention so the company is forced to fix. They do this to build a rep and get a job as a White Hat

White Hats (The Good Guys) - Often can be reformed Black Hats but also IT professionals that have participated in corporate run ‘Capture The Flags’ or have qualifications like OSCP. They test a company infrastructure and report on possible vulnerabilities. They are known also as Ethical Hackers and….Pen Testers.

‘Black Hat’ comes from the cowboy films where the outlaw would wear a black stetson

‘White Hat’ refers to The Lone Ranger and other TV lawmen who would wear a white Stetson.
**Spotlight on: penetration testing**

- **5.5k** candidates
- **1.5k** job ads live
- **£45k** average salary

**Density of candidates**

- **High**
- **Med.**
- **Low**

**Gender breakdown**

- **89%** Male
- **11%** Female

**Experience breakdown**

- 0-3 years: 18%
- 3-4 years: 23%
- 5-7 years: 59%
- 8+ years: 59%

**Top job titles**

1. Security Analyst
2. Security Consultant
3. Information Security Consultant
4. Senior Security Consultant
5. Penetration Tester
Trends - What Makes a Good Pen Tester?

Certifications & Experience

OWASP
Open Web Application Security Project

CREST®

OFFENSIVE®
security
OSCP

OFFENSIVE®
security
OSCE

Cyber Security Challenge UK

TIGERSCHEME
Providing excellence in penetration testing

CHECK
Where To Start?

Networking Events BlackHat, Bsides, DC4420 & LinkedIn
Should I go to Uni?

Top UNIVERSITIES for cyber talent
1. Sheffield Hallam
2. Coventry University
3. University of Greenwich
4. Loughborough University
5. University of Portsmouth
6. University of Leeds
7. Staffordshire University
8. University of Manchester
9. Middlesex University
10. Kingston University

Top COURSES for cyber talent
1. Computer Science
2. Information Technology
3. Computer & Information Sciences
4. Computer Systems Networking & Communications
5. Maths
6. Electronic Engineering
7. Computer & Information Systems Security
8. Business Administration & Management
9. Physics
10. Information Science/Studies
But I’m leaving the Military?
What Do Clients Say?

CEH™
CERTIFIED ETHICAL HACKER

VS

OFFENSIVE security
OSCP

OWASP
Open Web Application Security Project
A MUST READ BOOK for decent web application security coverage. I would combine with some decent web application practical exercises as a knowledge building exercise. The authors of this book have paid exercises online, however there is also free stuff like OWASP WebGoat:


Introduction to network/infrastructure testing, often used for initial CREST theory exam revision, there are two editions worth looking at 2nd and 3rd edition:

https://www.amazon.co.uk/Network-Security-Assessment-Know-Your/dp/0596510306

https://blog.g0tmi1k.com/2011/06/basic-linux-privilege-escalation/ T

This one is for Windows and Linux, comes with free VMs: https://github.com/sagishahar/lpeworkshop

Good pentesting book series:
https://www.amazon.com/Hacker-Playbook-Practical-Penetration-Testing/dp/1494932636
https://www.amazon.com/Hacker-Playbook-Practical-Penetration-Testing/dp/1512214566/

Hacking Exposed series:
https://www.amazon.co.uk/s/ref=nb_sb_ss_i_2_7?url=search-alias%3Dstripbooks&field-keywords=hacking+exposed&sprefix=hacking%2Cstripbooks%2C162


Online hacking challenges, worth trying out, some of these are similar to OSCP quality: https://www.hackthebox.eu/
https://www.hackthissite.org/
Thanks For Listening!
Feel Free to Follow me on linkedin or twitter @JaYR_ARMCyber

Any Questions?