north green

HOW TO START YOUR CAREER IN PENETRATION TESTING

A HOW TO GUIDE

If you want a career in penetration testing, but don't know where to start, this e-book will take you through what you need to know, with plenty of advice and tips throughout.

Written By:

Dan Cannon

INTRODUCTION

Let's be honest.

The cyber security industry is a mystery to most people.

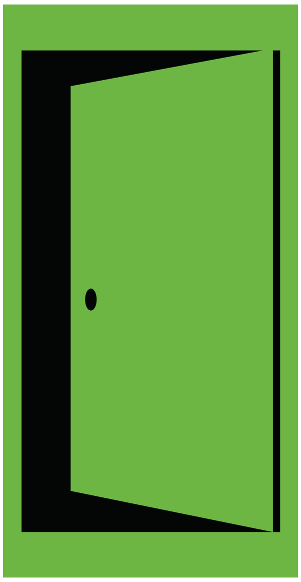
There is constant publicity of the skills gap that is threatening public and private sector institutions and yet individuals who want to have a career in this industry struggle to find their footing.

'Breaking into' cyber security is hard.

Part of the challenge is that cyber security has come to mean all manner of things. You cannot break into cyber security anymore than you can break into industries such as engineering. Much like the expansive field of engineering, cyber security is a broad and multifaceted domain that encompasses various disciplines.

In this e-book, we'll focus on one of the most exciting and dynamic aspects of cyber security—penetration testing.

We'll guide you through the intricacies, providing a roadmap to help you develop the skills needed to become a successful penetration tester as well as the steps needed to get your foot in the door.



1 SO, WHAT IS **PENTESTING?**

First and foremost, if you're thinking of a career in penetration testing, let's make sure you know what it is.

Penetration testing is a type of authorised security test, where skilled professionals simulate an attack on a computer system or application.

Pentesters use the same tools, techniques and processes as attackers, with a goal of identifying any security risks that could be leveraged by a malicious attacker to their advantage.

While being a penetration tester is often referred to as being one of the 'good guys' or an 'ethical hacker', it is important to note that one of the key words here is that this activity is authorised.

Penetration testing is focussed on identifying issues that can impact security and providing guidance on how to reduce the risk to an organisation.

This career means that you will develop the same skills as those who attack companies and compromise computer systems (and there is nothing wrong with pwning a network if you have permission) but that all your actions will be approved and all activity will be conducted in a lawful manner.

So even when you find some really amazing issues or bypass security controls, it is important to always remember that this is a career and profession that requires strong moral fibre and an eagerness to beat the system to make it better.

2 HOLLYWOOD VS **REALITY**

Everyone has a preconceived notion of just what they think hacking is - and what a career as a penetration tester would include.

This section is not aimed at crushing those dreams, but rather in making sure that you understand the reality of a career in pentesting and what the role actually involves.

In movies and TV shows, hacking is often portrayed as a glamorous, fast-paced activity where a lone genius types furiously on a keyboard and gains access to secure systems within seconds. While these scenes are entertaining, they are far from the truth.

In reality, penetration testing is a structured and methodical process that involves a variety of skills and tools. Some key aspects that differentiate real-world pentesting from its Hollywood counterpart are:

Preparation and planning:

Before any testing begins, a significant amount of time is spent on preparation. This includes understanding the scope of the test, getting authorisation, and defining the rules of engagement.

Understanding the target system:

A substantial amount of time is dedicated to getting to know the system you are attacking. This includes activities like port scanning and mapping out the website's structure. Until you have a clear picture of what is there, you cannot begin to look for potential weaknesses.

HOLLYWOOD VS **REALITY**

Tool useage:

While Hollywood hackers seem to accomplish everything with a single tool or script, real pentesters use a wide range of tools, each designed for specific tasks. These tools need to be configured and used appropriately, and understanding their limitations is crucial.

Manual testing:

Automated tools can only get you so far. Much of penetration testing involves manual testing and creativity. This might include crafting specific payloads, exploiting identified vulnerabilities, and chaining multiple exploits together.

Documentation and reporting:

A significant part of pentesting involves documenting findings and creating comprehensive reports. These reports detail the vulnerabilities found, the methods used to exploit them, and recommendations for mitigation. This requires strong communication skills and attention to detail.

3 TYPES OF PENTESTING ROLES

So now we know what pentesting is, let's talk about the different types of roles that exist within this field.

Internal security teams vs cyber security consultants

One thing to consider is not only what type of tester you want to be but who you want to work for. The choice between working within an internal security team and joining a cybersecurity consultancy can significantly influence the trajectory of your career, and the decisions you make to secure your first role.

Internal security teams

Internal security teams play an important role in protecting an organisation's assets. Typically found in companies with a mature understanding of the potential impact of cyber threats, these teams conduct thorough security assessments internally.

Collaborating closely with various business units, internal testers engage in regular assessments with a unique advantage – time. As company employees, they have the luxury to delve deeply into potential issues, working alongside colleagues to identify and comprehend risks. This collaborative approach is facilitated by a profound understanding of the company's intricacies, allowing testers to tailor their strategies effectively.

In advanced setups, large organisations may establish internal red teams, comprising of seasoned security testers. These teams perpetually seek new attack vectors, conduct research, and develop cutting-edge exploits or payloads for testing purposes.

TYPES OF **PENTESTING ROLES**

Security consultancies

IOn the flip side, security consultancies operate with penetration testing teams that offer their expertise to diverse clients across various industries for short durations. This approach ensures an impartial evaluation, free from concerns about conflicts of interest.

As employees of the consultancy, pentesters in this setting must rapidly adapt their skills to navigate different technologies and environments efficiently. Time becomes a critical factor, with clients paying for penetration tests by the day. Consultants must also deliver detailed and well-documented reports with actionable recommendations.

Efficiency is not the only demand; consultants are also tasked with representing their consultancy to clients. The need to reassure clients of their proficiency often leads to a higher emphasis on qualifications. Adaptability and effective communication are paramount, given the varying requirements of different clients. A cyber security consultant must not only identify concerns, but also articulate them clearly, fostering an understanding of potential risks among clients with diverse needs.

Within security consultancies, you also need to consider whether you want to work for a CHECK company or not. CHECK is the National Cyber Security Centre's (NCSC's) scheme to ensure that testers who work on government systems have the required skillset.

While both CHECK and non-CHECK companies are very similar, a key consideration is whether or not you want to or are able to obtain security clearance. Most CHECK consultancies will want to put you through some level of security clearance so that you can test government systems. While the process of obtaining security clearance (SC) is relatively simple, some people choose not to go through it and this should factor into how you view potential future employers.

4 WHAT **SKILLS** DO I **NEED**?

Even though you are looking for your first job in penetration testing, it is crucial to show that you have a strong foundation in IT and cybersecurity.

Demonstrating your knowledge in key areas will make you a more attractive candidate.

Some of the essential skills and knowledge areas you should focus on include:

Networking

Understanding networking fundamentals is paramount for a budding pentester. Networking is the backbone of the internet and all digital communications, so a deep understanding of it will serve you well.

Start by grasping concepts like IP addressing, subnetting, and the OSI model. These basics help you understand how data moves across networks and how devices communicate. You should familiarise yourself with how routing and switching work, which involves understanding network masks and how computers can communicate across different networks. This knowledge is crucial for identifying potential points of entry and understanding the broader architecture of the systems you're testing.

TCP/UDP Ports

Knowledge of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports is also crucial. These protocols are the primary ways data is sent and received over the internet.

Learn the differences between TCP and UDP connections, how they are established, and why different services use them. For instance, TCP is used for reliable, connection-oriented services like web browsing, while UDP is used for faster, connectionless services like streaming. Familiarise yourself with commonly used ports for services and applications, as this will help you recognise potential vulnerabilities and plan effective penetration tests.

Nmap scanning

Nmap is a powerful tool for network discovery and security auditing. As a penetration tester, being proficient with Nmap is essential. Start with the basics of Nmap scanning techniques, such as TCP, SYN, and UDP scanning.

Practice using Nmap in a controlled environment to develop confidence in identifying active hosts and open ports.

This tool helps you map out the network, understand what services are running, and where potential vulnerabilities might lie. Mastery of Nmap scanning is a highly valued skill in penetration testing.

Web vulnerabilities

Web applications are a common target for attackers, making it critical to understand web vulnerabilities. Familiarise yourself with the Open Worldwide Application Security Project's (OWASP) Top Ten vulnerabilities.

This list outlines the most common security risks in web applications. Use the resources provided by OWASP to gain a better understanding of issues like injection attacks, cross-site scripting (XSS), and security misconfigurations. Understanding these vulnerabilities will help you identify weaknesses in web applications and develop strategies to exploit them ethically and responsibly.

Password cracking

Passwords are often the weakest link in security. Mastering password cracking techniques is essential for uncovering weak authentication mechanisms.

Learn about common password hashing algorithms and the tools used to crack them, such as John the Ripper or Hashcat. Practice cracking hashed passwords in a controlled environment to understand how attackers might gain access through weak passwords. This skill is crucial for demonstrating how easily poorly protected accounts can be compromised.

Vulnerability scanning and exploitation

Proficiency in using vulnerability scanning tools is another essential skill. Tools like Nessus are used to identify weaknesses in systems. Understand the entire process of vulnerability scanning and exploitation.

This involves conducting thorough research, understanding the impact of identified vulnerabilities, and responsibly testing them in controlled environments. Virtual labs and Capture the Flag (CTF) platforms provide hands-on experience, allowing you to practice and refine your skills in a safe setting.

5 HOW MUCH **CAN I EARN?**

Too many people shout from the rooftops about junior positions with salaries that range from £50,000 - £80,000.

Should you be offered a junior position with that salary, my advice is to say YES and hold on tight, as this is far from the norm.

Unfortunately, the challenge is that all companies are different. A realistic range of starting salary for a junior penetration tester is anywhere between £25,000 and £35,000. The real money comes to those who then hone their craft. It is possible to double or triple a starting salary within the first five years of your career by focussing on learning the skills your employer finds valuable, demonstrating that you are able to work effectively, and taking any opportunities to undertake training or qualifications your employer values.

Be aware that career progression, and therefore salary progression, varies from company to company. Some companies will invest time and energy training you and will expect it to take a while before you are ready to deliver penetration tests solo. Others will throw you in at the deep end and hope you can swim. These different approaches can suit different people - and can impact the speed at which you are able to showcase your growing skill and value to the company, therefore impacting speed of pay rises.

It is best to focus on making sure you are learning the key skills needed to be successful before chasing higher salaries.

6 COMMON PITFALLS TO **AVOID**

As this is a fantastic career in a constantly changing industry, there are lots of organisations that will sell you a dream that will never become a reality.

Unfortunately, throughout my career I have seen people trying to break into the industry, fooled into taking the wrong qualifications and having an inflated wage expectation that has meant they have struggled to get that first role.

Certified Ethical Hacker (CEH)

CEH is a globally recognised qualification for aspiring penetration testers. Unfortunately, it is commonly recognised as very low value and not respected by many hiring managers with an ounce of technical capability.

There are many organisations that will encourage those starting their careers to pay for CEH and promise that they will walk into £70,000 jobs afterwards. This is not true. Including CEH on a CV is unlikely to be the deciding factor in whether or not a candidate will advance to an interview.

Unrecognised qualifications

There are multiple organisations that aim to create qualifications that help the industry and provide benchmarks of skills. However, there are organisations that aim to simply monetise qualifications by creating exams that offer little value.

While all exams have to start with no reputation, it is important to take the time to check any qualification you choose to work towards to verify its validity.

Newly established exams or examination bodies are best avoided unless you can find evidence that the qualifications are valued.

Inadequate practical experience

Relying solely on theoretical knowledge or non-practical certification can lead to challenges getting your first job. Hands on practice, whether on your own laptop, with free resources, or through paid training, show that you have the drive to learn the skills needed to be successful.

Hands on practice will also make you more confident in your knowledge and provide areas for discussion during an interview. Being able to talk about practical activities and the skills you are learning can be invaluable.

7 TO **CERTIFY** OR NOT?

One of the reasons first jobs are hard to find is that not all companies are set up and prepared to offer structured training and development for new starters.

Unfortunately, this takes time and an unskilled and inexperienced tester let loose can be a dangerous thing.

One of the approaches that can be taken by those looking for their first role is to demonstrate that they already have the necessary skills to be a productive member of the team.

It should be noted that in no way am I suggesting that you need to pay for training or exams to get your first job (many organisations invest in training and qualifications for new starters who have shown they have the drive and curiosity needed to succeed), this is just one of several options to try to stand out).

If you decide that training or qualifications are the route you want to take to demonstrate your skillset (which is by no means a requirement), it is important that you do not waste your time and energy. Selecting the right certification is a strategic decision and should align with your career goals.

Consider the industry recognition and global acceptance of the qualification before making any choice. It should be noted that the more respected a qualification, the further away it is from 'entry level' knowledge; take that into consideration when deciding whether to attempt these certifications or whether to just build the pre-requisite knowledge through study and practice.

8 CERTIFICATION OVERVIEW

This topic could be an e-book in itself, so in the interest of simplicity, I have included three certifications that would each be immediately recognised and understood by anyone hiring penetration testers in the UK. *(However OSCP and CREST both have a global audience, so would also be useful outside the UK too.)*

So, in no particular order...

Offensive Security Certified Professional (OSCP)

OSCP, offered by Offensive Security, is one of the most widely recognised certifications that a penetration tester can obtain to demonstrate their capability.

With a focus on developing practical skills and hands on experience, as well as a mantra to 'Try Harder', anyone who holds the OSCP certification has demonstrated a commitment to developing their skills and will be able to talk knowledgeably about different techniques and exploits used to compromise targets.

While Offensive Security qualifications are well respected, it should be noted that this is not an introductory course or qualification. Those who undertake OSCP need to be committed to putting in the time required to explore the lab environments and prepare for the exam.

To obtain the OSCP certification, you will be required to undertake a 24-hour practical exam, where you are tasked with compromising a series of machines. Once this has been completed, a report must be written within the next 24 hours, showcasing an ability to communicate security concerns and explain the vulnerabilities identified.

CREST Practitioner Security Analyst (CPSA) and CREST Registered Tester (CRT)

CREST is a global membership body, responsible for maintaining standards and delivering professional certifications.

With its origins in the UK, CREST certifications are well respected and have the added benefit of being accredited by the NCSC CHECK Scheme (something important to consider if you will be pursuing work in a CHECK consultancy).

The CPSA qualification is a multiple-choice exam comprising of 120 questions that must be answered within two hours. The content of the exam can be varied and include networking, infrastructure testing, web testing, tooling, and more.

The CRT qualification can only be attempted if you already hold CPSA and requires you to demonstrate your hands on skill. The exam is a 2.5 hour long, hands-on exam where you will demonstrate your capability by practically hacking into systems and websites, as well as demonstrating your ability to understand networking and Windows desktop breakout techniques.

Cyber Scheme Team Member (CSTM)

The Cyber Scheme is a UK based examination body that also has exams accredited by the NCSC Check Scheme.The CSTM qualification consists of three parts: a one hour multiple-choice exam, a one hour essay question paper, and a 2.5 hour practical exam, which ends in an interview with an assessor.

When taking this exam, candidates are required to demonstrate their breadth of knowledge in theoretical papers and hands on skillset in the practical assessment. It should be noted that failure to pass any individual aspect of the exam will lead to an overall result of a fail.

9 HOW DO I FIND MY **FIRST JOB?**

After all of this though, there is no point if you can't find employment.

To get that all important first job, keep an eye on vacancies visible on recruitment platforms or social media such as LinkedIn, but also get involved with the cyber security industry.

By attending events and conferences, you can start to learn more about this industry, talk to other attendees, and also talk to sponsors who are commonly recruiting or will be looking to recruit in the future.

BSides

BSides conferences are the best recommendation for those looking to break into cyber. These are community driven conferences that are organised and run by cyber professionals and enthusiasts.

They lack the corporate feel of larger conferences and instead provide a real community feel where you will be able to listen to interesting talks, and meet interesting people. (Larger BSides conferences may also have hands-on activities to take part in, such as lock picking, car hacking, robot fighting or CTFs.)

BSides are regional and cost very little, so wherever you are, simply look into BSides events near you and attend if you can.

Network

If you are up for it, network at events like BSides or other events near you.
If you don't want to do this in person, there is nothing wrong with reaching out to people remotely and seeing if they would be up for a chat and to give a bit of advice. Some people will be too busy and that's fine, some will be happy to chat and that's great.

If you can build a network of people you talk to, you may be able to find out about companies to approach or avoid, and job roles that are not publicised, but that exist for the right candidate at the right time.

LinkedIn and other social media

Not all employers will use recruiting companies, some will use social media platforms (or their websites) to advertise current vacancies.

Take a proper look at the job spec that is published so that you can understand the skills needed for different roles and think about whether you need to spend more time on your development before applying.

Do not take yourself out of the running though if you don't meet 100% of their desired skills. If this is a junior role, it is likely that hiring managers will accept that potential candidates would be unlikely to know everything.

Turning individuals into experts

North Green Security is a leader in penetration testing and cyber security training. Offering a comprehensive range of courses to suit you. We are here to provide guidance and skills that will make you more successful.

Our trainers have over 12 years experience creating and delivering training courses that get results

MORE **ABOUT US**

Phone
0844 502 0042

Email
training@northgreensecurity.com

Website
www.northgreensecurity.com

Discord
https://discord.gg/w7K8yVaFbD

www.northgreensecurity.com

NORTH GREEN SECURITY

Increasing security through education, training and testing

North Green Security is a leader in penetration testing and cyber security training. Offering a comprehensive range of courses to suit you. We are here to provide guidance and skills that will make you more successful.

Our trainers have over 12 years experience creating and delivering training courses that get results

CYBER SECURITY TRAINING TO PROGRESS YOUR CAREER

Training courses

Explore our catalogue of training courses ranging from half-day targeted workshops, to week long courses all designed and delivered by experts that can teach you the skills needed to take your next steps

https://northgreensecurity.com/upcoming-events/

North Green Academy

For those who prefer self-study and want to learn around their schedule, the north green academy provides an ever growing library of videos to teach you the skills needed to drive your career forward

https://www.ngsacademy.co.uk/

Have the best career possible

Our trainers are cyber security professionals who know the skills you need to be successful. Reach out for a chat, or book onto a training course