Penetration tester

Penetration testers simulate cyberattacks to identify and report security flaws on computer systems, networks and infrastructure, including internet sites

You will perform authorised tests on computer systems, using the same methods as a real attacker, to expose weaknesses in their security that could be exploited by criminals.

You can choose to specialise in manipulating a particular type of system, such as:

- networks and infrastructures
- Windows, Linux and Mac operating systems
- embedded computer systems
- web/mobile applications
- cloud environments
- application programming interfaces
- SCADA (supervisory control and data acquisition) control systems
- Internet of Things (IoTs).

As well as identifying problems, you may also provide advice on how to minimise risks.

You may work in-house for large companies where system security is a crucial function. However, more commonly you'll work for a security consultancy or risk management organisation, where you'll work with external clients testing the vulnerability of their systems. It's also possible to work on a freelance basis, by securing contracts from organisations.

Penetration testers are also known as pen testers or ethical hackers.

Responsibilities

As a penetration tester, you'll need to:

- plan and carry out remote testing of a client's network, computer systems or web/mobile applications or onsite testing of their infrastructure to expose weaknesses in security
- work with clients to determine their requirements from the test, for example, the number and type of systems they would like testing
- simulate security breaches to test a system's relative security

- create and implement new penetration testing methods, scripts and tools
- check for gaps in security that could occur from human error, for example inadequate password policies or login permissions, and advise on best practice to minimise risk
- create reports and recommendations from your findings, including the security issues uncovered and level of risk
- advise on methods to fix or lower security risks to systems
- present your findings, risks and conclusions to management and other relevant parties
- consider the impact your 'attack' will have on the business and its users
- understand how the flaws that you identify could affect a business, or business function, if they're not fixed
- carry out training for users to minimise future security risks.

Salary

- Starting salaries for junior penetration testers fall between £25,000 and £40,000, depending on your experience.
- Experienced penetration testers can earn between £40,000 and £65,000.
- Salaries for senior and team leader roles are between £60,000 and £80,000, depending on your professional qualifications and experience. However, this figure can be significantly higher depending on the industry you work in.

Salaries can vary widely depending on a range of factors such as your location, the type of employer you work for (e.g. in-house or consultancy) and the sector you work in, as well as your skills, experience and qualifications.

You'll usually receive a range of employee benefits that may include bonuses, a company pension scheme, private medical insurance, gym membership, and sponsored training and development opportunities.

Income figures are intended as a guide only.

Working hours

You'll typically work a 37 to 40 hour week, but flexible working practices are common, and you may need to work outside of a typical 9am to 5pm pattern.

Part-time and hybrid working is possible. Short-term contracts and freelance work are also available. With several years' experience, you can move into self-employed or consultancy work.

What to expect

- You may work in an office, or from home, and are likely to travel frequently to meet clients (unless you work in-house). Most, if not all, of your time will be spent at a computer when not in meetings.
- Jobs are available throughout the UK and job security is generally good.
- You'll have a high level of responsibility and will need to feel comfortable with this. You will also need to keep learning throughout your career to stay one step ahead of new security threats.
- Although more companies are addressing the gender imbalance in the IT sector, women are still underrepresented. This is a recognised issue and steps are being taken to redress the balance. There are various schemes around to encourage more women into penetration testing and other technical roles. These include WISE, Cyber Security Challenge UK, WeAreTechWomen and Girl Geeks.
- There are opportunities for qualified cyber security experts to work overseas.

Qualifications

To enter this industry, you'll usually need a relevant degree, in-depth knowledge of computer operating systems and networks, and experience in a role related to information security.

Useful degree subjects include:

- computer science
- computing and information systems
- cyber security
- forensic computing
- network management
- computer systems engineering.

You're unlikely to go straight from graduation into a penetration tester role and will usually need some industry experience. Some large organisations, however, offer cyber security graduate schemes, which include penetration testing.

It's possible to get into the career with an unrelated degree, as long as you have a strong foundation in computer systems. If your degree is in an unrelated subject, studying for an information security related postgraduate qualification could be helpful. Do your research

before applying to make sure the course meets your career requirements. Search for postgraduate courses in cyber security.

It's also possible to take a Level 6 Cyber Security Technical Professional (Integrated Degree) apprenticeship, combining work with part-time study at a university. The Civil Service also offers a Government Security Cyber Degree Apprenticeship (Level 6), which trains you to become a technical cyber specialist with the responsibility of helping the Government protect the UK.

You'll often be expected to have one or more professional penetrating testing qualifications (trainee and graduate roles will usually include training and certification in these qualifications as part of the role). These include:

- CREST - Registered Penetration Tester (CRT)
- OffSec - Certified Professional (OSCP)
- EC-Council - Certified Ethical Hacker

Look at job adverts for penetration testers to get a feel for which certifications employers are looking for.

It's also possible to work as a penetration tester without a degree if you have significant experience in information security and hold industry certifications.

You may need to undertake security clearance checks when applying for jobs.

Skills

You'll need to have:

- an in-depth understanding of computer systems and their operation
- excellent spoken and written communication to explain your methods to a technical and non-technical audience
- attention to detail, to be able to plan and execute tests while considering client requirements
- the ability to think creatively and strategically to penetrate security systems
- good time management and organisational skills to meet client deadlines
- ethical integrity to be trusted with a high level of confidential information
- the ability to think laterally and 'outside the box'
- teamwork skills, to support colleagues and share techniques

- exceptional analytical and problem-solving skills and the persistence to apply different techniques to get the job done
- business skills to understand the implications of any weaknesses you find
- commitment to continuously updating your technical knowledge base.

You will also need skills in programming languages such as Python and Shell scripting.

Work experience

You should get as much relevant experience as possible so you can develop your skills, build contacts and show prospective employers what you can do. There are a growing number of cyber security related work experience schemes and activities available.

You can practise and develop your penetration testing skills in various ways online. Cyber Security Challenge UK, for example, runs a series of competitions, learning programmes and networking initiatives designed to support and enhance cyber talents. They also partner with the National Crime Agency to deliver CyberLand, games which test and improve your cyber skills. Find out more at CyberGamesUK.

Another way of developing your skills is through Hack the Box, an online platform where you can improve your penetration testing skills through gamification.

Other useful activities include capture the flag (CTF) events, where teams or individuals must hack and defend systems to 'capture' a file or code. This type of exercise gives you the chance to hone your cyber security skills and develop your network of contacts.

You can also follow security experts on Twitter, set up a LinkedIn profile, join online security groups, attend industry conferences and events, and read cyber security publications, websites and blogs.

You may also consider broader experience in IT development and programming, as these fields provide essential foundations of knowledge for penetration testers. Internships and sandwich-placement opportunities are available in these roles and can be found on large jobsites or by speculatively contacting employers.

Find out more about the different kinds of work experience and internships that are available.

Employers

There are opportunities to work as a penetration tester across both the public and private sector, on an employed or freelance (contract) basis.

You will often work for security consultancy firms who employ penetration testers to work on client contracts. Opportunities also exist to work in-house for national and multinational companies, as well as for small and medium-sized companies.

Typical employers include:

- banks and financial services providers
- cloud services
- hospitals and other healthcare organisations
- local and national government
- media tech companies
- retail companies
- utilities and energy companies.

Look for job vacancies at:

- CWJobs
- Cyber Security Jobs
- CyberSecurityJobsite
- IT JobsWatch
- Technojobs

Vacancies are also advertised on professional networking sites such as LinkedIn.

Specialist recruitment agencies such as Cybershark Recruitment and Barclay Simpson also advertise vacancies.

You can also find work in this industry by making targeted speculative applications directly to companies. This can be an especially successful approach if you're looking for work with small and medium-sized organisations, who may be more likely to take on less experienced penetration testers.

The National Cyber Security Centre has a list of verified suppliers who can conduct authorised penetration tests of public sector and (Critical national infrastructure) CNI systems and networks, which you could use to contact companies speculatively. CREST also has a searchable database of accredited member companies providing penetration testing.

Professional development

Continuing professional development (CPD) forms a vital part of your career as you'll be expected to stay ahead of new hacking methods by keeping your skills and knowledge up to date. You'll need to keep on top of current technologies and how they may be exploited by criminals.

There are some graduate schemes in cyber security available, which will usually provide a structured development programme, mentoring and the opportunity to undertake placements in various departments.

It's common to undertake industry-specific qualifications to demonstrate your understanding, knowledge and experience. Several organisations offer professional industry qualifications with varying levels of accreditation, from entry-level through to managerial level. For senior-level roles, it's often a prerequisite to hold one or more of the advanced certifications, such as the CREST Certified level examinations.

The CHECK scheme allows companies approved by the National Cyber Security Centre (NCSC) to provide qualified penetration testers to work on IT systems for the government and other public sector bodies. To qualify as a CHECK team member (CTM) or team leader (CTL), you'll need to pass an NCSC-accredited CREST or Cyber Scheme examination.

Career prospects

Your first role will typically be in a junior systems administrator, IT development or IT support role. With experience and relevant professional qualifications, you can move into the role of penetration tester.

After working as a penetration tester for around three to five years, you can progress into a team leader position. Then, with a further two to three years of experience as a team leader, you'll be a specialist practitioner and will be able to apply for larger-scale project leader and management roles.

With several years' experience, you can move into consultancy work or set up as a self-employed penetration tester.

Career prospects are good at all levels for people with the right combination of skills, qualifications and experience.