
A day in the life of a Penetration Tester

Penetration Tester

Do you like the idea of planning and launching an active 'hacking attempt'? Do you like the idea of protecting organisations by identifying holes and gaps in security? Are you creative and love problem solving? Are you able to think outside the box and then capture your process in order to build a better more secure solution? Then Pentesting might be right for you!

Penetration Testing, pentesting, white hat hacking or ethical hacking, is one of the more glamorous IT security jobs. It is a highly sought-after capability that is currently suffering a massive skills shortage, and thus the opportunities to gain work in this field are plentiful.

A penetration test is defined as an authorised hacking attempt targeting an organisations infrastructure, applications and staff, with the aim of gaining access to its virtual assets. The pentester assumes the role of an external or internal threat and tries to penetrate the target organisation network. By finding vulnerabilities the pentester' outcome is to recommend solutions to harden security defences by eliminating vulnerabilities and advising on areas that are susceptible for compromise.

So what does a day working as a Penetration Tester actually look like?

Depending on the organisation and the amount of work that is on, a typical day for one penetration tester may look a lot different from another's. Generally speaking, whilst not actively working on an engagement, a penetration tester will spend time working on professional development, mastering techniques through practical application and researching current news and security trends, attend security conferences and meetings, and potentially engage in activities such as bug bounty programs.

While actively working on a job however, a penetration tester's day will include tasks such as:

- Planning a penetration test
- Creating or selecting appropriate tools to utilise during testing
- Interrogating and testing networks, applications, or systems.
- Diligently record and documenting the test
- Identifying and researching vulnerabilities using test results
- Reviewing and evaluating findings
- Developing proof of concepts

**WITHYOU
WITHME**

- Making remediation recommendations
- Engaging directly with clients
- Significant amounts of report writing

A penetration tester may work either on-site at the target organisation, or remotely from home or office to target the organisation from an external perspective. All testing is done via the use of computers, and conducted either solo, or as part of a team reporting to a lead pentester.

It is easy to romanticise about a career as an 'ethical hacker', however don't be fooled, this job is highly technical and not for the faint of heart. However, if you love problem solving, creative thinking, and are motivated to constantly learn more about the industry and develop your skills, penetration testing may be right for you.

**WITHYOU
WITHME**