

PENETRATION TEST

Protect your business by anticipating the latest cyber security threats!



The impact of operating in an increasingly connected world with greater dependence on information technology is that cyber attacks are inevitable. It is important to assess an organisation's cyber defences so that it is prepared in the event of an attack.

Penetration testing allows a system's defences to be tested in a real-life scenario. This allows companies to better understand their cyber weaknesses and focus their time and resources on critical threats and vulnerabilities.

OBJECTIVES

- ◆ Identify attack vectors
- ◆ Identify vulnerabilities
- ◆ Evaluate security controls
- ◆ Measure compliance with security standards

The goal ? To significantly increase your safety posture immediately!

DURATION

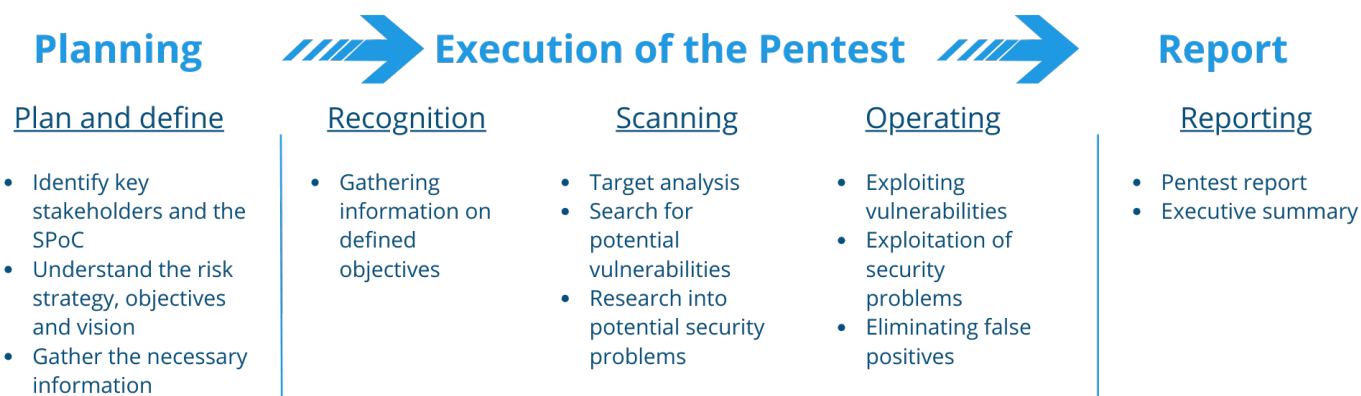
The duration of penetration tests varies according to the attack surface to be analysed. They are always tailored to the company's needs.

THE AREAS INVOLVED:

- ◆ Web applications: from showcase sites to more complex applications
- ◆ Infrastructure: from checking the security of software implementation to verifying the infrastructure as a whole using blackbox, greybox and whitebox tests.
- ◆ Social engineering: testing employee responsiveness using phishing campaigns.

On average, less than 7 days are needed between the start of the test and the report for the smallest areas to be tested, but the time obviously depends on the size of the company and its infrastructure.

THE STEPS



OUR APPROACH

With quality above all else, the Rsecure Ethical Hacking team has chosen to adopt a semi-manual approach.

The advanced methodology does not rely on ready-made software solutions. The focus is on delivering tangible results, using our critical thinking skills and extensive experience to identify risks relevant to your business. Our penetration tests are fully customised to meet your needs and environment.

Using this approach we have already uncovered critical vulnerabilities that may have gone undetected

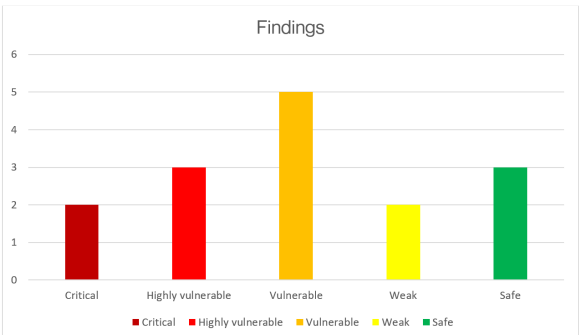
by vulnerability scanners or even the vendor itself, while effectively filtering out false positives.

We use innovative and creative tactics, and our commitment to rigour ensures consistent, high-quality deliverables. This enables security levels to be accurately assessed on a standardised scale.

Our Ethical Hacker team is certified by EC-Council's Certified Ethical Hacking (CEH) certification.



Example of diagram:



Control your cyber risk with regular pentests

