Penetration Testing

Adopt a proactive approach to identify and exploit vulnerabilities in your security defence and detection systems.

Resort to *Penetration Testing* to assess your infrastructure capacity to resist cutting-edge attack techniques.

Cyber-attacks are getting more and more sophisticated, forcing organizations to implement advanced protection and detection solutions. Consequently it's getting complicated for companies to continuously assess their effective capacity to face such threats. While most IT resources are aimed at ensuring business continuity, the fast-changing threat landscape might be a challenge for them. Consequently, your teams may lack the time, expertise and familiarity to be fully aware of the latest attack methods and vectors.

Apply methodologies used by cyber criminals to access your corporate data and reduce your attack surface by identifying and mitigating vulnerabilities within your IT environment.

Most organizations have implemented sophisticated security controls and incident response plans to face the exponential growth of cyber attacks. But unless they are regularly tested for potential weaknesses, cyber criminals can exploit hidden vulnerabilities and endanger your business continuity.

Therefore, Orange supports organisations by providing *Penetration Testing* intended to demonstrate how an attacker would gain unauthorised access to your environment by using similar tactics and techniques.

When should you perform Penetration Testing?

- Before a system, network or application is deployed and put in production;
- When your system is getting stable;
- After a cyber attack;

How often?

- From quarterly to yearly depending on your exposure to cyber risks (i.e. industry, online...);
- When new legislation and regulations are published , requiring new security measures;
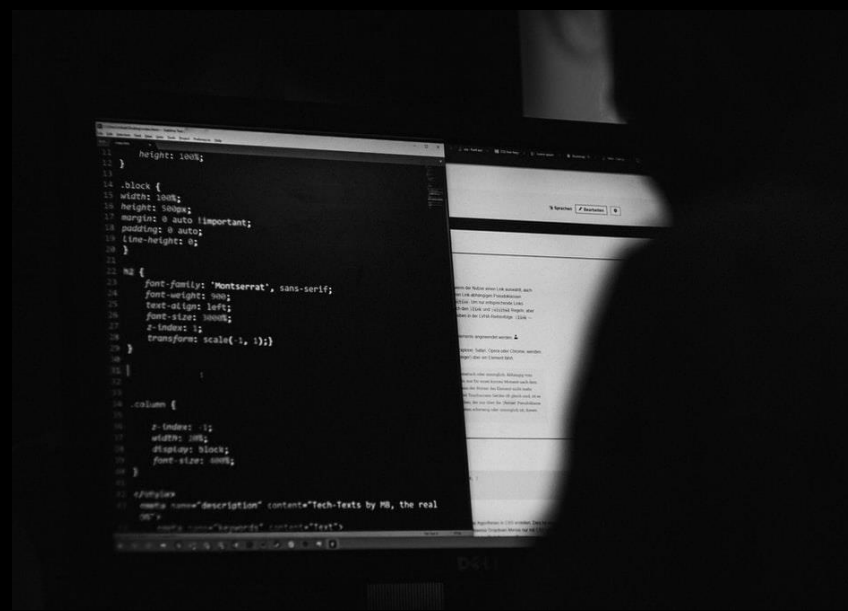
Penetration Testing benefits

- Identify potential vulnerabilities before an attacker does;
- Provide information helping your security team to mitigate vulnerabilities;

- Improve your incident response capacities with real attack simulations;
- Provide proof of compliancy to your business partners and authorities;

How does Penetration Testing work?

Use of **several techniques** including vulnerability scanning, exploitation of vulnerabilities, password cracking…

Supported by Orange **Ethical hackers**

Reporting including actionable **recommendations** from our experts
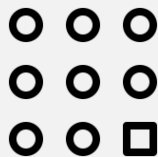
In-house **methodologies** and use of industry **standards** (i.e. OWASP)

Which perimeter can be addressed by a Penetration Testing?

Internal & External network

- Identify vulnerabilities of internet-accessible systems to gain access to internal resources;
- Simulate insider activity exploiting his access to corporate data;

Web & Mobile application

- Use of the OWASP standard to assess the security of web-based applications;
- Exploit mobile device vulnerabilities;

Red Team

- Simulate a real-world attack;
- Discover the easiest path to exploit a vulnerability within your infrastructure;