What is a pen test?

Minimise the risk of a successful cyberattack with the help of Hoffmann's creative hackers. Have I been hacked? The question these days is not whether your organisation will be hacked but when it will be hacked. You may have even already been hacked without your realising it. No matter how big or small your business is, cybercriminals never stop in their quest for new ways to penetrate organisations like yours. Hackers are becoming increasingly creative in their methods. Fortunately, so are Hoffmann's pen testers. Do not get caught off guard—have your IT infrastructure regularly checked by Hoffmann's certified ethical hackers. By doing so, you will ensure your IT infrastructure is resilient and be prepared for unknown threats.

Pen testing facts

On average, it takes 16 days for a company to discover a hack—this is also known as 'Cyberattack Dwell Time'. There have even been incidents in which the hack was only discovered after several weeks or even months.

In 82% of all cases, the hack itself happens in a single minute.

In nearly 100% of all cases, hindsight makes clear how the incident could have been prevented.

Periodic pen testing

A penetration test (pen test) shows whether your organisation is sufficiently resilient against digital attacks. It provides insight into vulnerabilities in your IT infrastructure and the potential consequences of those vulnerabilities. Regular security and resilience testing is imperative. This is especially true when you add new systems to your infrastructure, but also because new hardware and software vulnerabilities are discovered every day. This also applies to the hardware and software you already have in use!

CCV, ISO 27001 and NEN 7510

Hoffmann is certified by the CCV (Centre for Crime Prevention and Safety). Pen tests are therefore carried out according to the conditions and requirements of the CCV quality mark. The CCV quality mark offers reliability and guarantees the quality of the pen tests performed.

Are you in the process of obtaining ISO 27001 or NEN 7510 (healthcare sector) certification? Hoffmann can conduct penetration testing to examine whether the technical security of your IT systems is satisfactory.

Our approach: visible impact through pen testing

Hoffmann's imaginative pen testers go a step further than the average pen tester. They do not just work through a standard checklist but use their creativity and ingenuity to really penetrate the environment. They then show concretely what hackers can be capable of.

- They are Offensive Security Certified Professional (OSCP) certified pen testers.
- Hoffmann's pen tests are always carried out under indemnification provisions, and we determine the scope (scope) of the investigation together with you.
- We map your current security level so you can improve your IT security preventively.

Clear reporting & advice

The pen test report describes the key digital access doors that were tested, how this was done and the tools that were used for this purpose. The pen test findings are classified according to a rating system that ranges from low to medium to high to critical. This is done using either the Common Vulnerability Scoring System (CVSS) methodology or the NCSC-NL matrix (the Dutch equivalent of the CVSS). Using one of the two, we assess and prioritise the vulnerabilities in a comprehensive, customised advisory report.

How does pen testing work?

Many organisations find it difficult to define their core requirements. Therefore, our consultants try to make this concrete during the comprehensive intake we do beforehand. In addition to the risks that apply to every organisation, we identify your organisation's core concerns and the associated risks. Based on the input from the intake meeting, we determine together with you which key access doors will be tested to access company-sensitive data, and in what way.

It is also important that you have a picture, which can also be based on our input, of the systems that need to be tested. We call this scope determination. You can, of course, provide this information yourself, but we can also ascertain the nature of your organisation's digital footprint and systems by gathering open-source intelligence (OSINT).

Corporate network (the internal and external infrastructure)

Cybercriminals will do everything they can to penetrate your internal network from the outside. But (malicious) employees and guests can also expose important company data from within.

What options does a hacker have once they have managed to circumvent the first lines of defence and gain access to an internal workplace, for example? Is your network adequately protected against this, and has it been segmented, for example?

When you think of pen testing, you might easily assume that it is carried out entirely remotely. Nothing could be further from the truth. Hoffmann recommends looking at your infrastructure not only from the outside (the internet), but also from within your own office or from the immediate vicinity of your premises. Criminals can capture wi-fi signals relatively simply and thus attempt to penetrate your network remotely. An on-site (in-house) pen test by Hoffmann will give you insight into the risks you may currently be facing in this regard.

(Web) applications

(Web) applications and services linked to the internet are important access doors to sensitive data for criminals. Technical vulnerabilities could potentially even lead to access to the internal company network.

Mobile & IoT

Mobile apps and internet of things (IoT) devices are always connected to other (web) services and APIs. The sensitive data processed via this route can be intercepted by cybercriminals over the network.

CCV quality seal

Hoffmann is CCV-certified for pen testing. As a result, you can rest assured that pen testing is guaranteed to be carried out according to exacting standards. Penetration tests are also performed according to international standards.

- The penetration testing execution standard (PTES)
- The Open Source Security Testing Methodology Manual (OSSTMM) for IT infrastructure
- The OWASP Mobile Security Testing Guide (MASTG) for mobile applications

Types of pen testing

We determine together with you how much prior knowledge the pen tester will work with per system, application or network (‘black box’, ‘grey box’ or ‘white box’). The testing is done within a pre-arranged time frame (a timebox). Pen testing can also consist of a combination of black box, grey box or white box approaches. On the next page we

explains the differences between the methods.

Black box pen test	Grey box pen test	White box pen test
Our ethical hackers start the pen testing by attacking your systems with no prior knowledge. They will use open-source intelligence (OSINT) to map out your organisation in detail and identify any (publicly) available information. Examples include email addresses, outdated passwords or even (internal) documents. This method approximates the approach a cybercriminal would take to an attack. Black box pen tests are therefore the most frequently chosen type of pen test.	Our hackers are given limited access to the systems, from where we further investigate the vulnerabilities. This scenario corresponds to that of a hacker already having access to your systems. This could include them gaining access through malware or a successful phishing attack. In this very realistic scenario, an employee might find themselves (unintentionally) involved in a cyberattack, for example.	All information is provided beforehand to search for vulnerabilities in a targeted and efficient manner. Here, we study designs, source code, documentation and other available information to advise you on how to improve security.

Combination of tests

Naturally, we can perform any combination of the different types of pen tests. Therefore, we generally recommend starting with a black box pen test and then moving on to a grey box pen test. This can be done with the information provided or with the information our ethical hacker has obtained during the black box test.

Would you like information on pentesting?

Do you have any questions? Or are you interested in a red teaming assessment? If so, please feel free to contact us with no further obligation on your part.

☎ +31 (0)88- 298 66 00

✉ info@hoffmann.nl

Our specialists would be happy to share their ideas on with you.