# Penetration Tests and Ethical Hacking Services

A penetration test, also known as a pentest or ethical hacking, is an authorised simulated cyberattack on an IT/ OT system, performed to ultimately evaluate the cybersecurity of that digital system. At Kiwa we perform tailormade pentests of which the results provide valuable insights to the owners of the tested system. Especially in these times where cybersecurity incidents are increasingly common, it is recommended to have your system properly penetration tested.

Digitalisation, the Internet of Things (IoT) and other technological developments offer great opportunities across different industries. However, if proper security is not in place, unattended vulnerabilities can lead to cybercrime and cyberattacks by hackers or other adverse groups. This can seriously damage daily operations and business continuity. Moreover, the safety and privacy of people involved may be at risk.

## Rigorous testing

The penetration tests performed by Kiwa rigorously test the cybersecurity of systems to discover possible vulnerabilities and weaknesses. This is done to illustrate the corresponding risks and threats which may potentially be harmful for your business, organisation or system. Kiwa's experts combine specific industry knowledge with extensive security experience, enabling us to thoroughly explore an organisation, business or system from the perspective of a hacker and perform rigorous penetration tests.

## What is penetration testing or ethical hacking?

A penetration test, not to be mistaken for a Vulnerability Assessment, essentially consists of two parts. The first part is simulating a hack or a cyberattack against an organisation or business through one or more of their systems. In this part the ethical hackers at Kiwa attempt to get access to the organisation's 'crown jewels' (e.g. the personal identifiable information of customers) by making use of possible vulnerabilities which the penetration testers come across during the course of the tests and attacks. Of course this simulated attack is performed according to pre-arranged rules of engagement.

The second part of penetration test consists of reporting on the found vulnerabilities. These vulnerabilities may potentially be harmful to the organisation or business and are categorised into various risk levels. The penetration tests reports produced by Kiwa include, among other things:

- An executive summary illustrating the overall context of the findings of our penetration test;
- An overview as well as detailed explanation on the found security issues and vulnerabilities;
- The associated risk levels with regards to the potential impact are also addressed in the report.

More details on the procedure that Kiwa follows during penetration tests can be found below.

## The 7 phases of penetration testing

A penetration test is an elaborate procedure which consists of the following main steps or phases:

1. Scoping: Kiwa and the client agree upon several key points such as the scope of the test, overall goal, target, timespan, rules of engagement, crown jewels etc.;
2. Intelligence Gathering: Kiwa will use various sources to gather as much information about the target as possible, including researching the organisation, generating threat intelligence, and other relevant information that could come in handy when in the exploit phase (phase 4);
3. Vulnerability Analysis: Kiwa identifies the vulnerabilities of the target network. The penetration tester will send probes to the target network, collect preliminary information, and then use the feedback to develop an attack plan;
4. Exploitation: Kiwa attempts to break into the system according to the agreements defined during the scoping phase;
5. Post-Exploitation: Every exploited system is cleaned after gathering data for the testing report. This phase removes all agents, scripts, temporary files, etc. The clean-up process ensures that all installed 'attack material' is removed and returns the system configuration to its original, pre-engagement, state;
6. Reporting: Based on the findings of the previous phases and a thorough analysis, the results of the penetration test are reported in a structural and understandable manner;
7. Executive Summary/Debriefing: The report of step 6 is thoroughly discussed with the customer.

## Pentest formats

A penetration test can have three different formats. Each of these format takes a different approach to simulating a cyberattack:

- A white box penetration test: All necessary information such as system information, access to high level privilege accounts, source code etc. are provided in advance to Kiwa. With everything that there is to know on the system Kiwa formulates its plan to perform the exploitation to reach the crown jewels.

# Penetration Tests and Ethical Hacking Services

- A black box penetration test: Kiwa does not have any inside information on the system that will be penetration tested. General available information about this system (for example which can be found through Google) is the basis on which Kiwa will attempt to perform exploitation and get access to the crown jewels.
- A grey box penetration test: A combination of the previous two where limited knowledge of the target is shared with Kiwa. Information such as architecture, background information, access to low level privilege accounts is provided to Kiwa.

## Take the extra leap in protecting your business

With digitalisation, internet technology and everything surrounding it, cybersecurity has become something organisations should not take lightly. Kiwa's penetration tests are targeted towards any organisation that provides services through means of the internet and organisations that manufacture internet connected products. There can be a lot of nuance in these types of systems, services and products and that is why Kiwa's pentesting experts tailor their services towards the needs of organisations. In this way the outcomes of the penetration test provide real and useful insights into the security of the organisation.

| White box | Black box | Gray box |
|---|---|---|
| All knowledge of the system under test | No inside knowledge of the system under test | Some inside knowledge of the system under test |

## Why Kiwa?

Kiwa is a trusted and independent third party that performs tests to provide the basis for guaranteed quality. For years we have been testing and certifying HVAC parts and systems, performing FPC audits in factories and assessing involved employees. As systems and organisations are digitalising so do our means of testing and inspecting.

Performing penetration tests is one of the methods to address the cybersecurity of your organisation or business. As good cybersecurity is very important in our digital age, Kiwa is heavily involved in providing high quality, useful penetration tests and services. We are your partners for progress.