The process of a Penetration Test

At DIGITPOL, every Pentest begins with an interview to define scope, methods, budget, and schedule. We'll send a contract detailing the agreed-upon terms, possibly including an NDA. Then, the Pentest proceeds in three phases:

1

Reconnaissance

In the exploration phase, ethical hackers map potential entry points, including infrastructure and systems, searching for easy targets. It's a crucial step in the process.

2

Launch The Attack

Following exploration, the ethical hackers attack your systems, seeking entry points and exploiting vulnerabilities to access sensitive data. We document each step and provide recorded sessions in the final report.

3

Report the Findings

During a Pentest, ethical hackers identify vulnerabilities and classify them by risk for your organization. They provide a detailed report with conclusions and recommendations for better security, guiding issue resolution.

Certification

Passing the penetration testing earns your organization a certification, showcasing expertise in assessing and securing computer systems, networks, and applications.

Penetration Testing Service - Hong Kong

A penetration test, or pen test, is a cybersecurity check where ethical hackers simulate attacks on systems to find vulnerabilities. It helps identify weaknesses that could be exploited by malicious actors.

In Hong Kong, Digitpol conducts penetration tests to evaluate cybersecurity. We simulate attacks to uncover vulnerabilities and provide detailed reports with recommendations for improved security.

Penetration Testing Methods

As a standard there are three Pentest methods can be distinguished. These are well-known as black box testing, gray box testing and white box testing. None of these methods are considered the best but applied depending on your situation and after a consultation, the right approach can be applied. Each variant has its own pros and cons and will discover slightly different outcomes. The right choice therefore depends entirely on the stage of development, network circumstances and past testing.

Black Box Testing

In a black box Pentest, the ethical hacker operates with no prior knowledge of the target system, mimicking real-life scenarios. This approach assesses overall security but may miss complex vulnerabilities due to the lack of prior insight.

Gray Box Testing

In a gray box Pentest, the tester has partial information, simulating an insider attack. This approach assesses vulnerabilities while testing defenses against both insiders and external attackers.

White Box Testing

In white box penetration testing, the tester gets detailed information upfront, enabling thorough analysis and uncovering complex vulnerabilities. Yet, it may not mirror real-world attacks as attackers lack such detailed info.