

BLUEPRINT

Penetration Testing

Find out how an attacker would get in – before someone really tries.

A penetration test is a controlled, pre-agreed attack on your systems. It shows which vulnerabilities can actually be exploited, how far an attacker could get and what the impact would be. Unlike an automated scan, you get verified findings without false alarms.

What we test

- external, internet-facing infrastructure
- the internal network – what an attacker or malware could do once inside
- web applications and their APIs
- the configuration and resilience of key systems

How we work

- 1 We agree on the scope, rules of engagement and timing (black-box, grey-box or white-box).
- 2 We combine automated tools with manual testing based on recognised methodologies such as OWASP.
- 3 Critical findings are reported immediately, not just in the final report.
- 4 We walk your team through the results and verify the fixes once they are in place.

What you get

- an executive summary that needs no technical background
- a technical write-up of every finding, including how to reproduce it
- severity ratings and concrete remediation advice
- confirmation that the fixes really work

AI

AI in practice AI speeds up automated reconnaissance and preparation; every finding is verified manually.

Who it's for organisations that run internet-facing services, develop their own applications or need independent proof of security for customers, auditors or regulators.

Let's plan a test of your systems.

info@anomalis.cz · +420 603 106 456 (24/7 for urgent cases) · www.anomalisit.cz

Anomalis IT s.r.o. · Korunní 2569/108, 101 00 Prague 10, Czech Republic · Company ID 09717404 · VAT ID CZ09717404