Penetration testing

The threat of a cyberattack is one of the greatest risks organizations are facing today. The volume and sophistication of the attacks have increased exponentially and led to a wave of data breaches involving the theft of customer information and intellectual property. Over the years, the demand for penetration testing has increased substantially as businesses have recognized the need to provide assurance that they are protected from internal and external threats.

How can we help?

Our penetration testing services provide you with:

- An independent and objective security assessment of your IT systems, clearly highlighting the security risks to corporate and customer data from both external and internal threats.
- Objective insights into technical security vulnerabilities (and the people and processes associated with them) by showing how an attacker can compromise your networks and systems or socially engineer valuable information.
- A clear statement of your security risks and priorities so that you can focus on fixing the most important issues.
- A record of common IT security technical shortfalls and failings at your company, such that common issues in your development and deployment processes can be identified and remedied to facilitate improved security in future-deployed systems.

The candidates for penetration testing include…

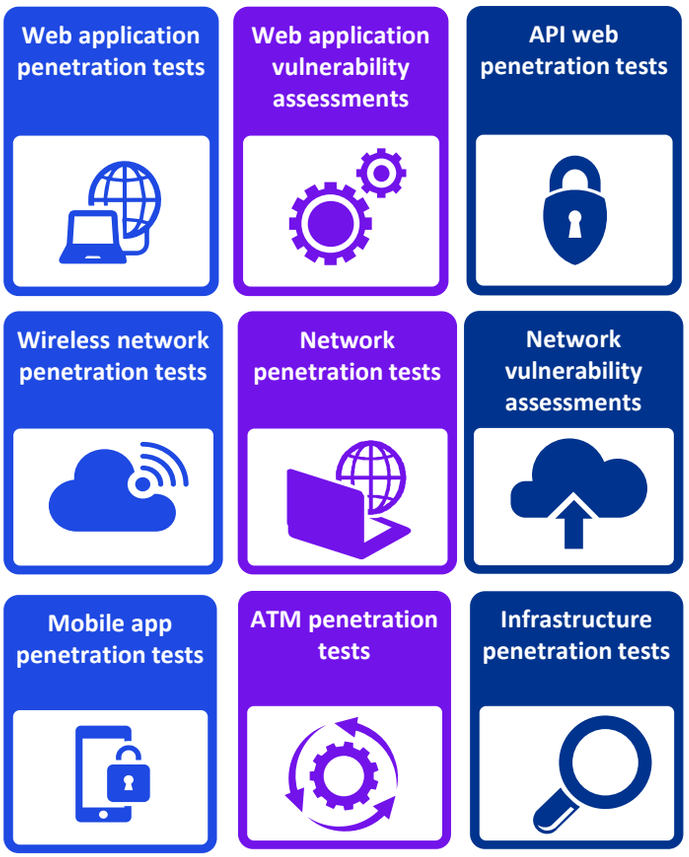
- Internet facing systems (i.e. anything public)
- Systems accessed from outside the trust boundary by a third party (i.e. a client and/or supplier facing solution that is not publicly accessible)
- Internal systems with a high inherent risk rating (i.e. the misuse of a system if not secured can cause significant business disruptions)
- Systems where there is concern about a particular risk or a case of misuse/abuse that needs to be addressed (e.g. logical separation of client data in a multi-tenanted solution; competency concerns for secure configurations, etc.)
- Systems that use new technological components previously not deployed or for existing technology when used/deployed in a significantly different way or where there are compliance or contractual requirements to do so for a system whether or not it is covered by the above points (i.e. required by a client, or industry compliance requirements e.g. in financial services (FS) or the public sector).

Why do we do penetration testing? .

- To prevent financial losses caused by both external and internal attacks to your organization, operating system, network, database applications and infrastructure
- To determine the likelihood of exploits through a particular set of attack vectors
- To assess the magnitude and the business or operational impacts of a successful attack
- To meet other requirements, such as client expectations, and regulatory and industry standards
- To identify vulnerabilities that otherwise may be difficult or impossible to detect, by using a combination of tools and professional expertise.

Different types of penetration testing:

Our penetration testing scenarios include white, grey and black box testing. We can perform infrastructure, web and mobile application penetration testing across all technology types through defined methodologies which cover the attack paths taken by real-world hackers. KPMG's services include:



Our team has the following certifications:

- CREST Registered Penetration Tester (CRT)
- Certified Red Team Expert (CRTE)
- Certified Red Team Professional (CRTP)
- Offensive Security Certified Professional (OSCP)
- CREST Practitioner Security Analyst (CPSA)
- Certified Ethical Hacker (CEH)
- Microsoft Certified

Achievements of the KPMG Security Testing team:

- KPMG is CREST accredited.
- KPMG was recognized as a Strong Performer in Cyber Risk Quantification by Forrester in their report entitled "The Forrester WaveTM: Cyber Risk Quantification, Q3 2023".

The KPMG approach

Penetration testing has increased substantially as businesses have recognized the need to provide assurance that they are protected from internal and external threats.

We base our approach on the proposition that an information asset's value, threats and vulnerabilities represent the level of risk associated with that asset. As the significance of any of these factors increases, the relevant risk also increases. Conversely, reducing any of these factors reduces the risk. All these factors must be understood before it is possible to assess risk in a reliable manner. Our penetration studies assess and quantify threats and vulnerabilities associated with specific target environments.

Our KPMG Penetration Testing services strive to provide you with an independent and objective security assessment of your IT systems, clearly highlighting the security risks to corporate and customer data from both external and internal threats.

Contact us

KPMG Siddharta Advisory
21st Floor Menara Astra
5-6, Jl. Jend. Sudirman
Jakarta 10220, Indonesia
T: +62 21 8060 2828

Freddie Mulyadi
Partner
Freddie.Mulyadi@kpmg.co.id

Rudy Anggam P
Senior Manager
Rudy.Prihartanto@kpmg.co.id

kpmg.com/id

Some or all of the services described herein may not be permissible for KPMG Audit clients and their affiliates or related entities.