ADVANCED PENETRATION TESTING

Advisory Services

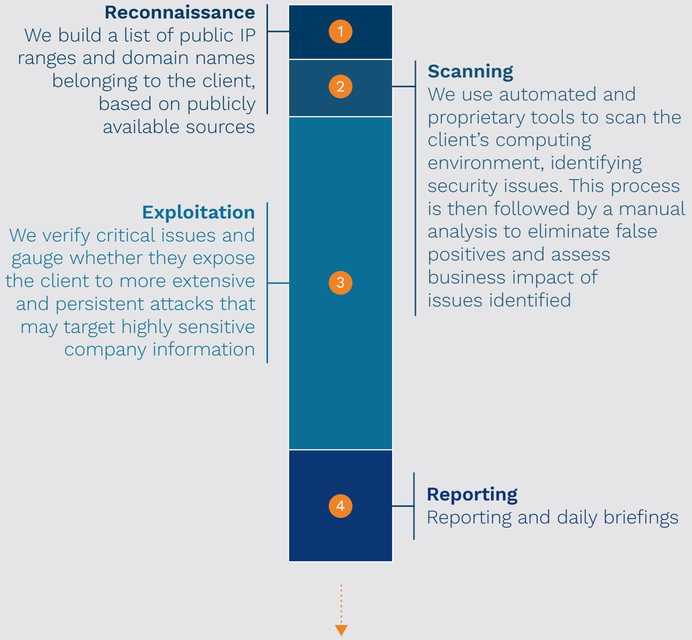
Identify vulnerable systems, safeguard assets and validate security measures.

Security breaches are costly, impacting business performance and shareholder value. As organizations embrace digital transformation and IT environments become more complex, vulnerabilities evolve. Security leaders need to be able to identify these vulnerabilities in their critical assets and know how these vulnerabilities in their critical assets and know they translate into business risk.

Kudelski Security's Advanced Penetration Testing services deliver a systemic, simulated and controlled assessment of your most valuable digital assets and any emerging technologies in the IT perimeter that present new risks to your organization. This exercise of due diligence helps you identify, prioritize and remediate security weaknesses, and provides your team with insights on both how your infrastructure may be attacked and on how prepared your team is to deal with such attacks.

Key Outcomes

- Confirmation of asset vulnerabilities through safe and controlled attack simulations
- Security posture analysis, and accompanying advice and support to address issues identified
- Prioritized remediation plan based on the client's unique business priorities, asset value, and threat landscape
- Enhanced protection of business and networks from risks, thanks to a service that encompasses a robust testing methodology, best-in-class techniques, and actionable recommendations



Reconnaissance
We build a list of public IP ranges and domain names belonging to the client, based on publicly available sources

Scanning
We use automated and proprietary tools to scan the client's computing environment, identifying security issues. This process is then followed by a manual analysis to eliminate false positives and assess business impact of issues identified

Exploitation
We verify critical issues and gauge whether they expose the client to more extensive and persistent attacks that may target highly sensitive company information

Reporting
Reporting and daily briefings

Follow–up during the remediation campaign

The Kudelski Security Advantage

Breadth and depth of testing including the most advanced real-world attack scenarios

Close collaboration and constant communication with client to ensure limited business impact

Qualified, certified, industry-experienced security penetration testers

How We Engage

Define Scope & Goals

We meet with the client to determine testing objectives, scope, and rules of engagement.

Security Assessment Execution

We review the assets in scope for vulnerabilities using proven and well-established methodologies. We confirm vulnerabilities through rigorous testing, using a combination of common attacker techniques, attacker toolkits, as well as proprietary tools.

Deliverables Preparation

We carry out technical and business impact analysis to develop recommendations.

Reporting & Recommendations

We present actionable prioritized recommendations to key stakeholders and deliver final report with full analysis.

Validation Testing

We can retest vulnerabilities to verify that recommended remediation action plans were indeed successful and that no other vulnerabilities have been introduced during the remediation phase.

What We Deliver

Kudelski Security provides a comprehensive portfolio of manual and automated penetration testing assessments. Unlike many penetration testing other services on the market, we do not simply scan for vulnerabilities, but also perform manual researches and exploitation, using a sequencing approach that groups vulnerabilities to confirm attack vectors. We use the common vulnerability scoring system (CVSS) to classify our findings, and combine it with business-relevant information, such as organizational impact and attack complexity. The outcome is a remediation strategy with actions prioritized according to criticality and impact, remediation, strategy and criticality/priority.

We have the capabilities to carry out the following types of assessments:

- Infrastructure & network (both internal and external)
- Web application (both DAST and SAST, covering OWASP Top 10)
- Mobile application (iOS & Android)
- Wireless & Bluetooth
- Hardware devices (e.g. computer, laptop, IoT)
- Malware protection assessment
- Social engineering (physical, phone and/or phishing)

We report on all findings, with relevant actionable content targeted to different stakeholder groups. Deliverables include:

Executive Summary

An overview of the most significant strengths and weaknesses of the security measures pertaining to the assets in scope.

Technical Findings

A technical listing of vulnerabilities identified and their exploitation. This professional opinion on the security posture of assets includes a visual representation that demonstrates the impact of the chained vulnerabilities, in the context of a real-world attack.

Actionable Recommendations

Vulnerabilities from all domains are prioritized with a global ranking, in order to highlight remediation actions with the greatest impact.

Attack Scenarios

A high-level conclusion that helps the CISO communicate effectively with the Board about security priorities and the most appropriate remediation actions, and illustrates their business impact.

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY