


Kudelski Labs - Device Hardware and Software Penetration Testing

# Assess Real-World Attacks to Uncover Vulnerabilities and Strengthen Device Security

 Device Hardware and Software Penetration Testing is a black-box Red Team engagement in which Kudelski Labs simulates adversarial actions to assess exposure to threats and identify security weaknesses across hardware, software, and network interfaces.

Our experts follow the typical path of attackers, leveraging current techniques, tools, and threat intelligence, to expose security gaps and assess device resilience. We provide clear, actionable recommendations to strengthen defenses and can perform a short retest phase to validate the correct remediation of identified vulnerabilities.

## Comprehensive Device Security Testing

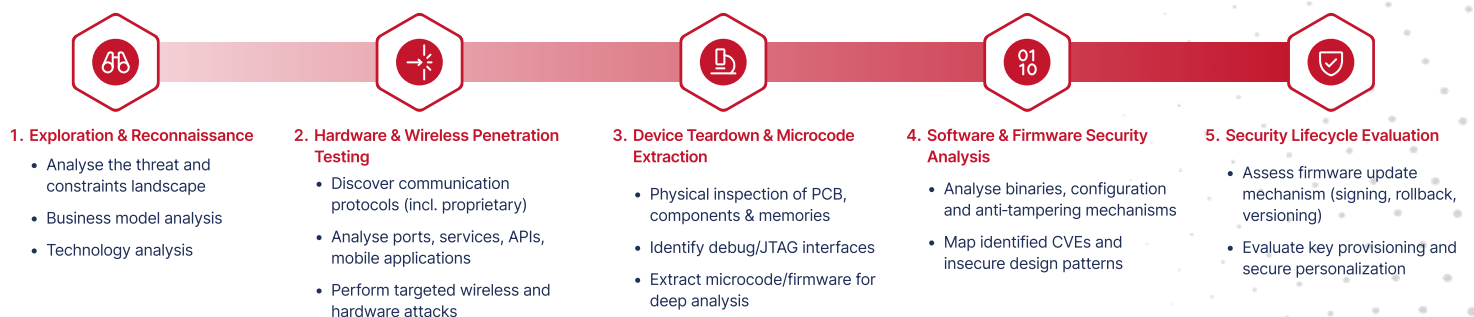
- Real-world adversarial attacks
- Hardware, software, network, remote & local attack coverage
- Actionable insights with remediation retest

## Understand How Attackers See Your Device

- Assess the impact of realistic adversarial behavior with a black-box Red Team approach, using state-of-the-art techniques and advanced tools. Leveraging 30 years of experience in connected device assessment
- Uncover weaknesses from Chip to Cloud
- Validate the implementation of the security lifecycle
- Provide actionable insights and remediation guidance to strengthen device security

## Our Penetration Testing Approach

Kudelski Labs evaluates your device exactly as an attacker would, using a structured black-box methodology that examines exposed interfaces, hidden attack surfaces, and internal components. This approach identifies exploitation paths and reveals weaknesses that could be used by malicious actors or competitors.





# Penetration Testing insights

Our penetration testing delivers deep technical insights and practical recommendations.

- Real-world attacker simulation via black-box Red Team approach using a proprietary methodology
- Use of state-of-the-art techniques and advanced tools to access code and data
- Hardware, firmware, software, wireless and cloud-interface coverage
- Full device teardown and internal architecture analysis
- Microcode extraction for deep firmware review
- Automated + manual vulnerability analysis including CVE mapping
- Actionable, prioritized recommendations with remediation validation retest

## What This Testing Reveals

Our penetration testing highlights:

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Hardware vulnerabilities and exploitable design flaws       | <input checked="" type="checkbox"/> Cryptographic implementation issues                     |
| <input checked="" type="checkbox"/> Weaknesses in communication interfaces and exposed services | <input checked="" type="checkbox"/> Debug interfaces or undocumented access channels        |
| <input checked="" type="checkbox"/> Firmware and software misconfigurations                     | <input checked="" type="checkbox"/> Risks during provisioning, or firmware update lifecycle |

## Where This Service Delivers Value

Device Hardware and Software Penetration Testing is used to:

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Validate the resilience of a new device before launch                | <input checked="" type="checkbox"/> Strengthen security posture for long-lifecycle products  |
| <input checked="" type="checkbox"/> Secure devices involved in safety-critical or regulated environments | <input checked="" type="checkbox"/> Prevent high-impact product failures, data and code exposure (breach, cloning), costly fixes and recalls |
| <input checked="" type="checkbox"/> Benchmark product security against competitors                       | <input checked="" type="checkbox"/> Create competitive advantage, achieves regulatory compliance   |
| <input checked="" type="checkbox"/> Identify weaknesses in legacy devices before redesign                | <input checked="" type="checkbox"/> Protect long-term revenue streams, intellectual property, brand reputation and customer trust            |
| <input checked="" type="checkbox"/> Support certification or customer security requirements              | <input checked="" type="checkbox"/> Improve product design and engineering efficiency  |

## Strategic Intelligence. Impactful Action.



Our embedded security expertise is rooted in more than three decades of hardware, software and cybersecurity experience. We use our expertise and technology to protect all key assets - devices, identity, data, decisions, commands and actions throughout the lifetime of the device and its ecosystem.

[Explore Our Innovations](#)

[Contact Us](#)