Find Weaknesses Before Attackers Do

Network Penetration Testing

Your network is the backbone of your business, but it's also a prime target. Misconfigurations, outdated software, and overlooked entry points can expose organizations to costly breaches. RKON's Network Penetration Testing goes beyond surface-level scans to emulate real-world adversaries, helping you identify, validate, and remediate vulnerabilities.

Our Approach

- Combine automated scanning with rigorous manual validation
- Leverage open-source, commercial, and proprietary tools
- Simulate attacker TTPs to expose real-world risk
- Provide collaborative debriefs to transfer knowledge to your team

Benefits

- Highly curated findings based on validated impact. Every issue is triaged by business risk, exploitability, and remediation feasibility.
- Meet **compliance** and industry frameworks
- Every deliverable includes role-specific reporting
- We include **remediation validation and retesting** for critical findings in every engagement. We do not consider the work complete until your issues are confirmed resolved.

Why RKON

Our engagements routinely deliver:

- Real exploitation evidence, not just findings
- $250,000+ in risk reduction per test
- 75% fewer critical exposures identified post-engagement
- 50–70% fewer recurring audit findings
- 80% time savings on remediation planning
- Executive-ready, prioritized findings every time

What We Deliver

External & Internal Pen Testing

- Identify and safely exploit weaknesses across perimeter and internal systems
- Validate patch levels, segmentation, and access controls
- Assess exposures in wireless, IoT, and network appliances

Manual Exploitation & Validation

- Human-led testing to confirm true exploitability
- Proof-of-concept evidence showing business risk
- Prioritized remediation recommendations

Identity & Access Governance

- Test for attacker pathways beyond initial access
- Examine user privilege assignments and pivot opportunities
- Identify exposures in identity, directory services, and shared resources

Custom Threat Simulation

- Tailored scenarios reflecting your industry's threat landscape
- Aligned with frameworks like PTES, NIST SP 800-115, and MITRE ATT&CK
- Attack narratives that simulate authentic real-world campaigns