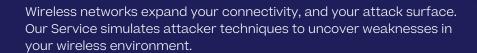


WIRELESS PENETRATION TESTING SERVICE



From rogue access points to weak encryption, we test the infrastructure, devices, and protocols that support your organization's connectivity.



What we test:

Wireless Network Architecture:

Evaluate access points, segmentation, coverage, and broadcast behavior.

Authentication & Encryption Protocols:

Review standards in use (e.g., WPA2, WPA3) and detect downgrade vulnerabilities or weak pre-shared keys.

Common Wireless Attack Vectors:

Simulate attacks such as Evil Twin, rogue AP, deauthentication, and credential capture.

Client Device Exposure:

Assess how user devices interact with access points and if they're vulnerable when roaming.

Risk of Unauthorized Access:

Measure how easily unauthorized users could join the network or move laterally.

WHY CHOOSE US?

Real-World Wireless Attack Assessment:

We emulate actual attacker behavior, not just tool-based scans.

In-Depth Reporting:

From technical findings to executive insights, our reports are built for action.

On-Site Testing Expertise:

Our team handles sensitive in-person assessments with discretion and precision.

Built for Compliance and Risk Reduction:

Results map to frameworks and provide tangible evidence for audit readiness.

OUTCOMES YOU Can expect

- Insight into real-world wireless vulnerabilities
- Identification of misconfigurations and insecure access points
- Recommendations for improving encryption, authentication, and segmentation
- Clarity around user device risk and network visibility
- Support for compliance with wireless-related controls (PCI DSS, ISO 27001, NIST)

EMPOWERING YOUR SECURITY OPERATIONS

- Wireless Vulnerability Assessment Report
- Penetration Test Findings with Impact Analysis
- Risk Prioritization and Tactical Recommendations
- Executive Summary for Stakeholder Briefings
- Post-Engagement Debrief and Support