Service Overview

SynAck Solutions delivers comprehensive External Infrastructure Penetration Testing that simulates real-world adversary tactics against your internet-facing assets. Our certified operators use the same techniques, tools, and tradecraft employed by sophisticated threat actors to identify exploitable vulnerabilities before they can be leveraged in a genuine attack.

Every engagement follows the Penetration Testing Execution Standard (PTES) methodology, mapped to the MITRE ATT&CK framework, and is conducted by certified professionals with extensive experience across critical infrastructure, financial services, and enterprise environments.

Business Value

- Identify and remediate exploitable vulnerabilities before attackers find them
- Validate the effectiveness of perimeter security controls, monitoring, and alerting
- Meet compliance obligations: ISO 27001, PCI DSS, Essential Eight, APRA CPS 234, SOCI Act
- Receive actionable, prioritised remediation guidance with clear business context
- Gain confidence in your external security posture through independent expert assessment
- Executive-ready reporting with strategic recommendations beyond individual findings
- Benchmark your security maturity against industry peers and threat landscape trends

What's Included

- Passive and active reconnaissance of all in-scope external assets and services
- Port scanning, service enumeration, and technology fingerprinting across all targets
- Automated and manual vulnerability identification with false-positive elimination
- Controlled exploitation of confirmed vulnerabilities with full evidence capture
- CVSS v3.1 severity scoring with MITRE ATT&CK TTP mapping for every finding
- SSL/TLS configuration analysis and certificate chain validation
- DNS security assessment: zone transfer, subdomain enumeration, and DNSSEC
- Web surface testing: default credentials, exposed panels, information disclosure
- Branded report: executive summary, findings, ATT&CK heatmap, recommendations
- Delivery in four formats: Word, PDF, interactive HTML, and Google Doc
- Post-engagement debrief and remediation guidance with your technical team

Scope

The engagement covers all internet-facing infrastructure owned or operated by the client, including but not limited to:

- Public IP address ranges and externally routable subnets
- External DNS records, mail servers (MX), and name servers (NS)
- Web applications and API gateways accessible from the internet
- VPN concentrators, remote access gateways, and SSL portals
- Cloud-hosted services (AWS, Azure, GCP) with external exposure
- Externally accessible management interfaces (RDP, SSH, SNMP)

Scope boundaries are defined collaboratively during pre-engagement and formally documented in the Rules of Engagement. Testing windows and escalation contacts are agreed in advance.

What's Excluded

- Internal network penetration testing (available as a separate engagement)
- Social engineering, phishing, or vishing campaigns
- Physical security testing or facility access assessments
- Denial-of-service or destructive testing of any kind
- Third-party hosted assets without explicit written authorisation
- Source code review or deep application-layer testing beyond external exposure
- Wireless network assessments (available as a separate engagement)

Methodology

Our methodology aligns with PTES and incorporates OWASP Testing Guide v4.2 for web-facing assets. Each finding is scored using CVSS v3.1 with full vector strings and mapped to MITRE ATT&CK Enterprise techniques. Remediation includes tactical fixes and strategic recommendations.

Engagement Timeline

A typical external infrastructure assessment runs 5-10 business days depending on scope size and complexity. Final report delivery within 5 business days of testing completion. Re-test of remediated findings available within 30 days at 30% of initial engagement cost. Expedited timelines available on request.

Get Started

Contact us to discuss your requirements and receive a tailored proposal. We will work with you to define scope, agree on rules of engagement, and schedule testing at a time that suits your operations.

info@synack.au | https://www.synack.au

ABN 88 667 784 956