Service Overview

SynAck Solutions delivers comprehensive Internal Network Infrastructure Penetration Testing that simulates a threat actor who has gained initial access to your corporate environment. Our certified operators replicate the tactics, techniques, and procedures used by advanced persistent threats to identify weaknesses in network segmentation, Active Directory configuration, privilege boundaries, and lateral movement paths before a real adversary exploits them.

Every engagement follows the Penetration Testing Execution Standard (PTES) methodology, mapped to the MITRE ATT&CK framework, and is conducted by certified professionals with deep experience across enterprise Windows and Linux environments, hybrid cloud architectures, and operational technology networks.

Business Value

- Validate internal network segmentation and identify lateral movement paths to critical assets
- Assess Active Directory security posture including privilege escalation and delegation weaknesses
- Test detection and response capabilities of internal security controls (EDR, SIEM, NDR)
- Meet compliance obligations: ISO 27001, PCI DSS, Essential Eight, APRA CPS 234, SOCI Act
- Identify trust relationship abuse, credential reuse, and misconfigured service accounts
- Receive actionable, prioritised remediation guidance with clear business context
- Benchmark internal security maturity against real-world adversary tradecraft

What's Included

- Internal network reconnaissance and host discovery across all in-scope subnets
- Active Directory enumeration: users, groups, GPOs, trusts, ACLs, and delegation
- Privilege escalation testing on Windows and Linux hosts
- Credential harvesting, relay attacks, and Kerberos abuse (Kerberoasting, AS-REP roasting)
- Lateral movement via SMB, WMI, PSRemoting, RDP, and pass-the-hash/ticket techniques
- Network service exploitation: SMB, LDAP, DNS, SNMP, NFS, and database services
- VLAN hopping and network segmentation bypass assessment
- Sensitive data discovery across file shares, databases, and internal applications
- 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 internal network infrastructure accessible from an agreed starting position, including but not limited to:

- Internal IP address ranges and VLANs as defined in the Rules of Engagement
- Active Directory domains, forests, and trust relationships
- Windows and Linux servers, workstations, and network appliances
- Internal web applications, management consoles, and administration portals
- File shares, databases, and internal collaboration platforms
- Network infrastructure: switches, routers, firewalls (management interfaces)

Testing is conducted on-site or via a secure remote access appliance deployed to an agreed network segment. Starting position (e.g. unauthenticated, standard user, or specific VLAN) is defined collaboratively during pre-engagement scoping.

What's Excluded

- External infrastructure 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
- Operational technology (OT/SCADA) systems unless explicitly scoped
- Source code review or deep application-layer testing beyond internal exposure
- Wireless network assessments (available as a separate engagement)

Methodology

Our methodology aligns with PTES and integrates MITRE ATT&CK Enterprise tactics for post-compromise assessment. Testing progresses through network reconnaissance, vulnerability identification, exploitation, privilege escalation, lateral movement, and objective completion. Each finding is scored using CVSS v3.1 with full vector strings and mapped to ATT&CK techniques. Remediation includes tactical fixes and strategic hardening recommendations.

Engagement Timeline

A typical internal infrastructure assessment runs 5-15 business days depending on scope size, network complexity, and starting position. 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, starting position, 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