GRYPHON SECURITY

Internal Penetration Testing

Assumed Breach Simulation. Clear Operational Impact.

A focused cybersecurity assessment designed to simulate realistic internal attack scenarios, where the objective is to understand how an attacker could operate **after initial access has already been achieved**.

Organizations increasingly face threats that originate from within the network perimeter—compromised user accounts, infected workstations, malicious insiders, or third-party access. This service provides leadership with a clear, defensible understanding of how internal weaknesses could be exploited to expand access, escalate privileges, and reach sensitive systems.

Traditional security reviews assess controls in isolation. Internal penetration testing demonstrates how attackers actually move, persist, and succeed once inside.

What We Do

We conduct a controlled internal penetration test designed to simulate real-world post-compromise activity within the internal network and cloud environment.

The assessment identifies exploitable weaknesses in authentication, authorization, segmentation, and system configuration that could enable lateral movement, privilege escalation, persistence, or access to sensitive data. Testing is performed safely, ethically, and within an approved scope to validate real-world exploitability, not hypothetical exposure.

The result is evidence-based insight into how an internal compromise could evolve and what systems and data would ultimately be at risk.

Why This Matters

Many security incidents do not fail at the perimeter; they fail **after access is obtained**. Internal weaknesses often determine the true blast radius of an attack.

Internal penetration testing demonstrates:

- How far an attacker could move once inside
- Which systems and data could be reached from a single foothold
- Where segmentation and access controls break down
- How privilege escalation and persistence could occur
- Where detection and response may be delayed or ineffective

This service equips leadership with defensible, real-world clarity about internal risk before an incident forces exposure.

Our Testing Approach

This service uses a structured, risk-focused internal penetration testing methodology.

Testing begins from an assumed-breach perspective, simulating an attacker operating from a compromised workstation, user account, or internal network segment. Controlled exploitation is used to validate lateral movement, privilege escalation, and access to high-value systems. Where in scope, persistence mechanisms and trust relationships are evaluated to demonstrate realistic compromise scenarios.

The engagement is not a certification, compliance audit, or automated scan. It is a deliberate simulation designed to answer one core question:

"If an attacker already had a foothold inside the environment, how much damage could they realistically do?"

What's Tested

Testing scope is tailored to the organization but commonly includes:

- **Authentication & Access Control**
  Credential storage, reuse, privilege boundaries, and access enforcement
- **Internal Attack Surface**
  Exposed services, trust relationships, and weak segmentation points
- **Endpoint & Lateral Movement Paths**
  Ability to pivot between systems, users, and network segments
- **Privilege Escalation Opportunities**
  Abuse or misconfiguration of elevated access, service accounts, or delegation
- **Detection & Visibility Gaps**
  Ability to identify and respond to suspicious internal activity

Findings are contextualized to the organization's actual architecture and operational workflows.

What You Receive

You receive clear, actionable deliverables – not raw scan output:

- **Executive Summary**
  Plain-English overview of internal risk exposure and impact
- **Risk-Rated Findings**
  Critical → High → Medium → Low → Informational
- **Documented Attack Paths**
  How an attacker could progress internally, with operational impact explained
- **Evidence-Backed Remediation Roadmap**
  Prioritized 30 / 60 / 90-day recommendations

Reports are suitable for executive leadership, technical remediation teams, and governance review.

Who This Service Is For

This service is designed for:

- Organizations with internal networks, hybrid environments, or cloud identity platforms
- Environments concerned about insider threat, credential compromise, or ransomware spread
- Organizations validating segmentation, privilege management, and internal monitoring
- Teams seeking proof-based insight into post-breach risk

This Service Is *Not* Designed For

- Organizations seeking a checkbox compliance assessment
- Organizations looking for managed SOC services or tool resale
- Environments without leadership commitment to remediation and improvement

Gryphon Security focuses on clarity, independence, and defensible outcomes.

Why Gryphon Security

- Real-world offensive tradecraft
- Evidence-driven, non-alarmist reporting
- Clear articulation of internal attacker impact
- No product resale or vendor bias
- Built for executives and technical teams alike

We focus on what matters and how attackers actually operate.

Next Steps

An initial conversation is structured, confidential, and obligation-free.

We will:

- Confirm internal scope and environment
- Discuss key risk concerns
- Explain exactly what testing will and will not include

We will not pressure you into tools, managed services, or long-term contracts.

Gryphon Security, LLC
Offensive Security & Risk-Based Testing
info@gryphonsec.com | www.gryphonsec.com