GRYPHON
SECURITY

External Penetration Testing

Real-World Attack Simulation. Clear Business Impact.

A focused cybersecurity assessment designed to simulate realistic external attacks against organizational systems, where operational continuity, data protection, and organizational trust are critical.

Organizations face an evolving external threat landscape. Internet-exposed systems, remote access technologies, cloud services, and identity platforms are frequent targets for ransomware operators, credential theft, and data extortion campaigns. This service provides leadership with a clear, defensible understanding of how an external attacker could realistically compromise the environment using controlled, authorized adversarial techniques.

Traditional security reviews identify what *should* be secure. Penetration testing demonstrates what an attacker can *actually* exploit.

What We Do

We conduct a controlled external penetration test designed to simulate real-world cyberattacks against internet-facing systems, networks, applications, and cloud environments.

The assessment identifies exploitable vulnerabilities, misconfigurations, and attack paths that could allow unauthorized access, privilege escalation, lateral movement, or data exposure. Testing is performed safely, ethically, and within an approved scope to validate actual exploitability rather than theoretical weakness.

The result is evidence-based insight into how an intrusion could occur and how far it could realistically progress.

Why This Matters

External security gaps create risk far beyond technical inconvenience. Successful attacks can lead to data exposure, ransomware deployment, service disruption, regulatory impact, and reputational damage.

Penetration testing demonstrates:

- What attackers can realistically exploit
- How weaknesses can be chained into meaningful compromise
- Where detection and response may fail
- Which risks materially threaten operations and continuity

This service equips leadership with defensible, real-world clarity before an incident forces decisions under pressure.

Our Testing Approach

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

Testing begins with authorized reconnaissance and attack surface discovery, followed by controlled exploitation to validate access and impact. Where in scope, lateral movement and privilege escalation paths 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 external attacker tried to break in, could they succeed, and what would happen next?"

What's Tested

Testing scope is tailored to the organization but commonly includes:

- **Authentication & Access Control**
  Credential handling, MFA enforcement, exposed authentication endpoints, and privilege boundaries
- **Attack Surface Exposure**
  Externally accessible systems, services, applications, and cloud entry points
- **Endpoint & Lateral Movement Paths**
  Abilty to pivot from initial access toward internal systems, where permitted by scope
- **Privilege Escalation Opportunities**
  Misuse or abuse of elevated access resulting from configuration weaknesses or credential exposure

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

What You Receive

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

- **Executive Summary**
  Plain-English overview for leadership and stakeholders
- **Risk-Rated Findings**
  Critical → High → Medium → Low → Informational
- **Documented Attack Paths**
  How an attacker could progress, with business 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 internet-facing systems or remote access infrastructure
- Businesses seeking proof-based security insight

- Environments concerned with ransomware, credential compromise, or data exposure
- Organizations validating the effectiveness of existing security controls

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 attacker impact
- No product resale or vendor bias
- Built for executives and technical teams alike

We focus on what matters and what attackers actually exploit.

Next Steps

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

We will:

- Confirm 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