PacketLabs

Penetration Testing
beyond the checkbox

Everyone has the right to cybersecurity, privacy and a thriving future. Let's talk.

Welcome to Packetlabs

Why Packetlabs 03

Services Overview 04

Infrastructure Penetration Testing 05

Objective-Based Penetration Testing 06

Application Security Testing 07

DevSecOps 08

Cyber Maturity Assessment 09

Compromise Assessment 10

Purple Teaming 11

Ransomware Penetration Testing 12

Red Teaming 13

Contact 14

Why Packetlabs?

We help foster safe digital spaces where everyone has the right to privacy, cybersecurity, and a thriving future

We protect and secure organizations from costly cybersecurity breaches by collaborating with them to enhance their security posture. Our expert-level penetration testing services are thorough and tailored to your organization's needs.

Beyond OSCP certified

Packetlabs is a passionate team of highly trained ethical hackers with the industry's most advanced certifications. OSCP is our minimum requirement with team members going above and beyond to gain certified expertise in OSEP, OSWP, OSED, OSWE, CISSP, CISA, GWAPT, GMOB, GSNA, GXPN and GCIH.

OFFENSIVE security

PEN-200 (OSCP) PEN-300 (OSEP) PEN-210 (OSWP) EXP-301 (OSED) WEB-300 (OSWE)

CISSP

CISA

GWAPT GMOB GSNA GXPN GCIH

Services Overview

Protect proactively

Our findings serve one key purpose - **strengthening your security posture.** With our comprehensive methodology, we not only analyze complex attack paths to find vulnerabilities, we offer up solutions that actually move the needle.

“We work with people across any industry to improve their security posture.

Some industries we serve

- Agriculture
- Construction
- Education
- Energy / Utilities
- Financial
- Government
- Healthcare
- Hospitality
- Insurance / Group Benefits
- Loyalty
- Manufacturing
- Media
- Minerals & Mining
- MSP
- Real Estate
- Retail
- SaaS
- Telecommunications
- Transportation

Roles we work with

- IT Professionals
- Security Program Leaders
- Procurement
- Executives
- Managed Service Providers
- App Development Agencies
- Lawyers

Infrastructure Penetration Testing

Find weaknesses others overlook in your IT infrastructure

Our penetration testing is more than just a vulnerability scan. Automated testing accounts for only 5% of what we do. The other 95% consists of manually simulated real-life attacks conducted by our ethical hackers to uncover your network vulnerabilities and protect your future. We tell the full story of how a vulnerability can lead to a compromise.

Our difference

We deliver a **detailed penetration test report** outlining our findings and offer tactical and strategic recommendations to enhance your security posture.

Benefit from our **comprehensive testing methodologies** that tackle hard-to-find vulnerabilities, demonstrating their potential impact.

Utilize our narrative-approach reporting enabling you to show **actionable insights** and set attainable goals for your organization.

Objective-Based Penetration Testing

Reduce the risk of a breach within a specific objective-based goal

Simulate real-world, covert, goal-oriented attacks. Take conventional penetration testing to the next level by gaining in-depth insight into the vulnerabilities that lead to specific goal-based objectives. Rather than defining the scope of targets, objectives are defined, for example: obtain access to a high-security network or access to sensitive information.

Our difference

- **Testing is coverage-based** and attempts to find as many paths to your network as possible; not just the easy ones.
- Each objective is thoroughly documented with an **attack narrative** to illustrate how it was achieved and the timeline of events.
- Our skilled testers have a hacker mindset to provide **real-world internal and external attack scenarios** so that you can discover the strength in your current security posture.

Which service is right for you?

	Infrastructure	Objective-Based
Thorough Foundational Assessment of Networks and Systems	✓	✓
Network Security	✓	✓
System Hardening	✓	✓
OS and Third-Party Patching	✓	✓
Authentication Attacks	✓	✓
Cryptography Attacks	✓	✓
Email Phishing	✗	✓
Ransomware Assessment	✗	✓
Active Directory Bloodhound Assessment	✗	✓
Active Directory Password Audit	✗	✓
Antivirus Bypass	✗	✓
Adversary Simulation	✗	✓
Physical Security Attacks	✗	✓
Social Engineering (Phone/ In-person)	✗	✓

Application Security Testing

Go beyond automated testing with extensive manual processes

The basis of our application security testing is guided by an enhanced version of the OWASP testing methodology. We evaluate the security of web and mobile applications to protect against cyberattacks. From source-code, all the way up to the browser – an application security assessment measures the effectiveness of your in-house developed applications. By simulating a hack, we assess the controls you currently have in place.

Our difference

- Our **customized methodology**, based on OWASP, finds vulnerabilities that may be missed by automation testing alone.
- Our **detailed application security report** includes an executive summary that outlines the overall state of the application and our technical findings coupled with recommendations.
- **Documentation of attacks** with multiple exploits outlines how an attacker could chain vulnerabilities together to compromise your application.

DevSecOps

Discover vulnerabilities in your development lifecycle

Our recurring testing service helps discover vulnerabilities in a client's application development lifecycle. DevSecOps is integrated early in your development cycle and can act as an extension of your development team to find and flag vulnerabilities within your existing defect management systems before User Acceptance Testing.

Our difference

- **Find and flag vulnerabilities** within existing defect management system prior to user acceptance testing, systems integration testing, application, or end-user testing.
- Immediately implement application security testing that requires a **different skill set than internal QA teams** to ensure all vulnerabilities are found.
- Fixed and **predictable QA spend** provides an opportunity to reduce operating expenses.

Which service is right for you?

	Application Security Testing	DevSecOps
DAST (dynamic application security testing)	✓	✓
SAST (static application security testing)	✓	✓
Coverage beyond OWASP Top 10	✓	✓
Web, Mobile, API	✓	✓
Continuous, Full Development Lifecycle Support	✗	✓
CI/CD Integration	✗	✓
Defect Tracking	✗	✓

Cyber Maturity Assessment

The industry's best value for revitalizing your security strategy and IT environment

Get a health check that evaluates the security within your organization and ultimately provides a security road map. We provide a security road map that strengthens business security posture and is the first step to becoming compliant and achieving contractual, regulatory and internal stakeholder requirements.

Our difference

- **One-on-one consultation and on-demand support** to gain further insight, strengthen compliance, and exceed customer expectations.
- **CISSP certified consultant with an attacker mindset** provides an in-depth assessment and optimization of your cybersecurity posture to meet government regulations and contractual requirements.
- **Holistic approach, focused on people, technology, and processes** for a complete environmental assessment and actionable security road map with strategic guidance.

Compromise Assessment

Our compromise assessment uncovers past or present threats

Our team identifies undetected threat actors who are in your network currently or in the past. Testing includes both automated and manual inspection conducted across firewalls, endpoints, and servers to ensure a thorough examination of your IT infrastructure systems and applications. Our ethical hackers uncover threats like zero day malware, trojans, ransomware, and other anomalies that may go undetected in standard automated vulnerability scans.

Our difference

Comprehensive assessment of your system based on **industry trends, local and global threats, OSINT gathering,** and more to detect past or present actors.

Assess the efficiency of your current security controls and processes from endpoint to endpoint to eliminate the guesswork, reduce dwell time and resource costs.

Ensure an effective, secure Merger and Acquisition transactions for customers and other stakeholders.

Purple Teaming

Evaluate all phases of an attack lifecycle with an assess-exploit-track-consult approach

Our red team works with your internal security operations team to bridge the gap between offensive techniques and response efforts. Our Purple Teaming service provides experiential insights, resources, and assessments shared in real-time, simulating real-life attack scenarios that offer your company's internal blue team a more in-depth threat detection understanding.

Our difference

- Shed light on **possible attack scenarios not detected** and create rules in workflows to detect these attacks for the future.
- **Real-time feedback using the MITRE ATT&CK Framework and associated TTPs** through real-life attack scenarios which allow your blue team to reverse engineer attacks to optimize the defensive strategy.
- Assess associated risk level to make **tactical and strategic recommendations.**
- Document and draft report outlining **key observations.**

Ransomware Penetration Testing

Our ransomware penetration test determines the likelihood of a ransomware attack

Ransomware penetration testing evaluates the preparedness and risk of a ransomware attack. Our comprehensive assessment identifies gaps in people, processes, and technology, to determine the likelihood and readiness for a ransomware attack.

In addition to a complete analysis of the security program against the Cybersecurity Framework Profile for Ransomware Risk Management (NISTIR 8374), and a technical assessment of security controls, a full penetration test is conducted to measure the robustness of your systems.

Our difference

- We understand the **potential impacts** on a business if a ransomware attack were to occur. Our comprehensive testing helps identify weaknesses in your current security controls.
- Beyond thorough testing, we schedule meetings with stakeholders to **identify gaps in policies, standards, and procedures.**
- Both data protection and recovery are paramount to Packetlabs. Our team **identifies recovery capabilities** and ensures backups to critical systems can't be compromised.

Red Teaming

Find paths to your most critical assets while also testing your response capabilities.

Red teaming is a full scope, multi-layered, simulated attack designed to get a holistic review of the level of risk and vulnerabilities across people, processes and technologies in an organization.

The ethical hacker will identify and test your exposures for weaknesses using social engineering and stealth to avoid detection.

Red teaming is most useful when an organization has a robust security program in place and is looking beyond a traditional penetration test.

Approach Options

1. A timed approach where our team tries to get access to a specific objective or goal from the outside.

2. A split approach where our team sets a specific number of days to attempt to penetrate the network from the outside, followed by several days in an assumed breach scenario to see what damage can be done if someone obtains access.

Our difference

- Our realistic **simulated attack from the outside in** with the option for an assumed breach scenario begins with a black box assessment to simulate various external threat actors and evaluates the likelihood of a remote compromise via phishing or external perimeter.
- Identify your **blue team's capability** to quickly identify and respond to active threats and gaps as the ethical hacker navigates your environment covertly.
- Find paths to your **most critical assets** by identifying users that would be most vulnerable, or most targeted by attackers and see how exposed your most valuable data is if it were targeted.

Ready to strengthen your security posture?

There's simply no room for compromise.

Get in touch to share your cybersecurity needs with our team and get a free quote.

---

647 797 9230 info@packetlabs.net packetlabs.net

606-6733 Mississauga Road, Mississauga, ON, L5N 6J5

@pktlabs /packetlabs-ltd- @packetlabs

Scan QR code to book a virtual consultation with us.

Packetlabs