Packetlabs

Penetration Testing Buyer's Guide

Everything you need to know about Penetration Testing to make an informed decision.

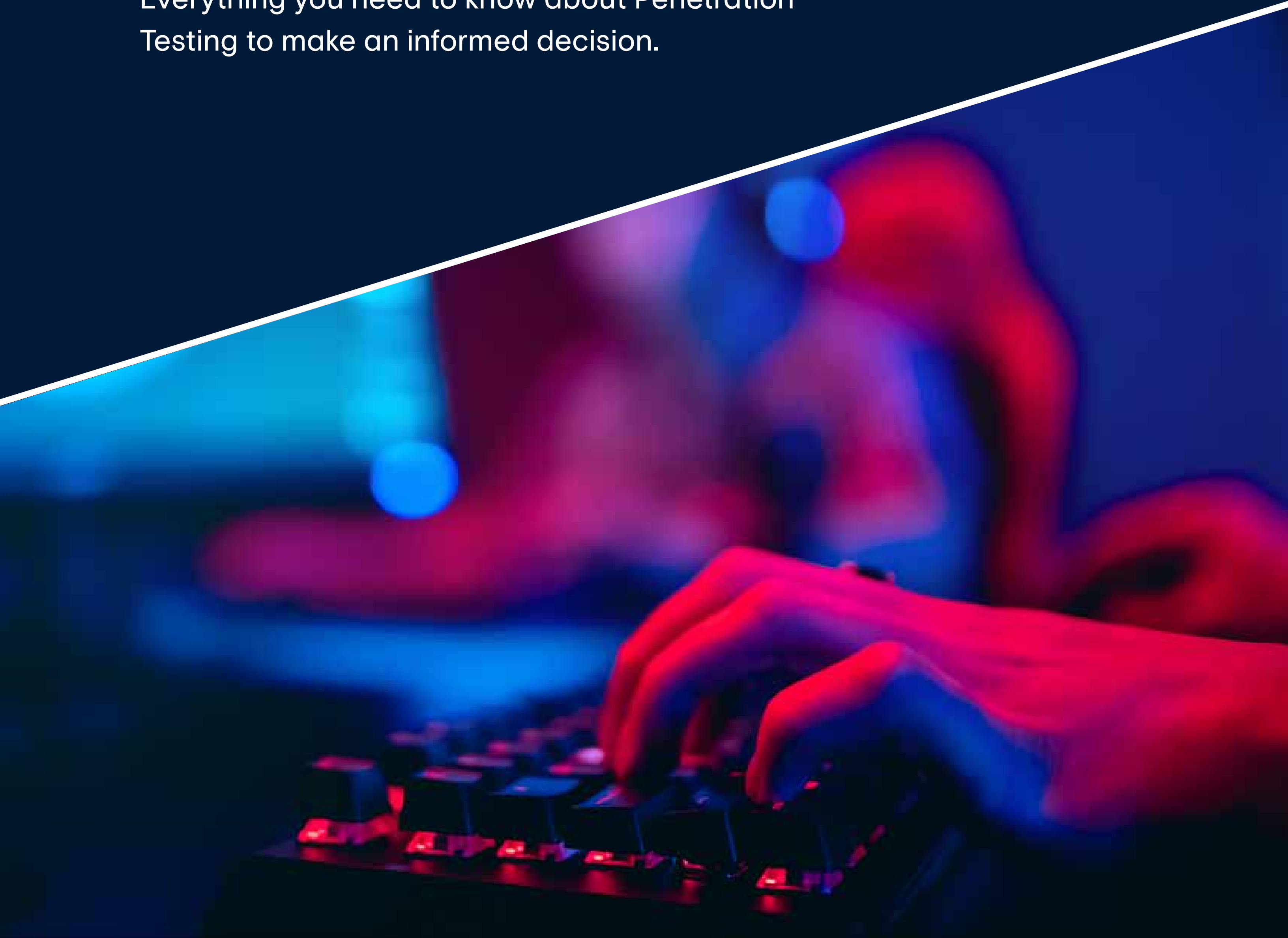

Table of Contents

Overview

When it comes to cybersecurity, there is no one-size-fits-all solution. The best way to protect your organization is to have a comprehensive security strategy that includes multiple layers of defense. One important element of a strong security strategy is penetration testing.

Penetration testing, also known as pen testing or ethical hacking, is a simulated cyberattack carried out by security experts to expose vulnerabilities in an organization's IT infrastructure. By identifying and exploiting these vulnerabilities, pen testers can help organizations strengthen their defenses against real-world attacks.

Penetration testing can be a valuable tool for organizations of all sizes. However, with so many different providers and services available, it can be difficult to know where to start.

This Buyer's Guide is designed to help you navigate the world of pen testing and help you make an informed decision about which service is right for your organization.

This guide includes:

- The benefits of conducting a penetration test
- How a penetration test can affect your cyber insurance premiums
- Penetration testing frameworks, standards and methodologies
- Factors that influence cost
- What should be included in a report
- Packetlabs reporting options (traditional vs. PTaaS)
- What to look for in a penetration testing provider
- 20 questions to ask a penetration testing provider

Introduction

Looking at the Numbers

The demand for enhanced cybersecurity is increasing as businesses continue to rely on evolving technologies and employ more remote workers. In 2020, 78% of Canadian organizations experienced at least one cyberattack. This figure rose to 85.7% in 2021 and projections show this number continuing to increase.

87% **of Canadian businesses experienced at least 1 cyberattack in 2021**

Despite the rise of cyberattacks, only 35% of Canadian businesses are planning to implement new cybersecurity measures. This leaves 65% of businesses with the mindset that they are not impacted by cybersecurity or don't know how to address increased cyber risk.

The Cost of a Breach

Cyberattacks, including data breaches, ransomware attacks and phishing attacks can be costly. In 2021, the average cost of a data breach in Canada was $5.4 million - up from 4.5 million only a year before.

Cost is only one of the impacts of a cyberattack - businesses can also experience reputation damage, legal costs and the loss of customers which can be devastating to the organization.

The average cost of a data breach is $5.4 million

What's the solution?

While there isn't a guaranteed way to prevent every single cyberattack, one important step businesses can take is to **invest in penetration testing.**

Benefits of a Pentest

Cyber criminals are becoming smarter and more malicious, deploying attacks that impose increasingly higher costs on victim organizations. A single security gap can lead to critical data being ransomed or even worse, permanently destroyed, and business operations being interrupted. Penetration testing is one part of a broader risk management program that seeks to ensure that an enterprise can sustain business operations indefinitely.

Benefits of Penetration Testing

- Increase your security posture
- Protect your data and your clients' data
- Meet regulatory compliance standards and/or requirements (PCI - DSS, HIPPA, SOC-2)
- Meet cyber insurance requirements

There are many reasons for ongoing penetration testing including meeting regulatory standards or other requirements, but ultimately it comes down to three things:

01

Reducing the risk of a successful cyberattack

02

Mitigating the impact of a successful cyberattack

03

Meeting cyber insurance requirements

Infrastructure Pentesting

What you'll get:

- A thorough foundational assessment of networks and systems
- Identify all paths to Domain Admin
- System hardening recommendations
- OS and third-party patching assessment
- Identify insecure configurations within on-prem and cloud environments
- Uncover the impacts of techniques, tactics, and procedures commonly used by ransomware
- A comprehensive report with detailed findings and remediation steps

Cyber Insurance

While once a recommendation for lower insurance rates, cyber insurance companies now require certain security measures, plans and processes to be in place. These include, but are not limited to, incident response plans, regular penetration testing and security awareness training for employees. For businesses that don't have these measures in place, coverage may not cover the full cost of the attack or even be denied altogether.

Packetlabs can help you identify any exploitable vulnerabilities in your servers and networks that may cause your insurance provider to reject renewals or deny coverage.

Requirements are Changing

- Most insurers now require proof of a incidence response plan
- Some insurers require companies to have regular pentests and security audits by 3rd party firms
- Premiums are increasing across the board
- Insurance may be denied without a pentest
- Current geo-political tensions may increase the amount of denied claims

Pentest VS Vulnerability Scan

Our company slogan, "Ready for more than a VA?®" was designed to draw attention to the widespread misconception between a VA scan and a pentest. The terms are sometimes used interchangeably but are two very different things.

A **Vulnerability Assessment (VA)** is a passive analysis of your systems to look for known vulnerabilities. This is usually done with a vulnerability scanner that will test for common CVEs (Common Vulnerabilities and Exposures). These scanners can be run both internally or externally.

Do I need both?

The short answer is: yes.

A vulnerability scan on its own is not enough. Although VA scans are valuable tools to help stay on top of the security of your environment regularly, it should be understood that they come with limitations.

Sometimes low-risk findings in a VA scan are identified as high-risk in a pentest. This is because a pentest explores your environment from an attacker's perspective. It separates the noise and outlines the most critical findings that require remediation and explains why.

A Pentest, on the other hand, is an active analysis of your systems to look for both known and unknown vulnerabilities. This is done by simulating a real-world attack on your systems and then trying to exploit any vulnerabilities that are found. A pentest can be run internally or externally depending on the nature of the engagement.

Journey to Cyber Security

Recommended Road Map

3 Year Plan

Year 3
Evaluate enterprise response to active adversary

Year 2
Align security strategy to exceed industry standards

Year 1
Identify and mitigate high-risk vulnerabilities

YEAR 1

The first step is to focus on identifying and mitigating high-risk vulnerabilities. This includes conducting a comprehensive penetration test to identify potential risks, implementing security controls to mitigate those risks, and testing the effectiveness of those controls.

YEAR 2

The following year, focus on aligning your security strategy to meet and exceed industry-leading standards. This includes implementing a robust security program that goes beyond compliance requirements, and establishing secure communications.

YEAR 3

Once your security program is in place we shift the focus to evaluating your enterprise's response to an active adversary. This includes testing your incident response plan, practicing for various types of security incidents, and conducting regular security exercises.

This may include:

- Objective-Based Penetration Test
- Ransomware Penetration Test
- Application Security Test

This may include:

- Maturity Assessment
- Infrastructure Penetration Test
- Compromise Assessment

This may include:

- Red Teaming
- Purple Teaming

Packetlabs

Services

Infrastructure Penetration Testing

Uncover vulnerabilities residing within your infrastructure and provide a detailed attack narrative to help evaluate the impacts of each finding.

Objective-Based Penetration Testing

Simulate real-world, covert, goal-oriented attacks to find as many paths to your network as possible in addition to a full penetration test.

Ransomware Penetration Testing

Identify gaps in people, processes, and technology, to determine the preparedness and risk of a ransomware attack.

Application Security Penetration Testing

Evaluate the security of web and mobile applications guided by an enhanced version of the OWASP testing methodology.

DevSecOps

Discover vulnerabilities during the development lifecycle that are within your existing defect management tracking systems before being promoted to production.

Purple Teaming

Identify gaps in your alerting capability with a collaborative, simulated red team exercise that utilizes MITRE ATT&CK tactics, techniques, and procedures (TTPs).

Red Teaming

Identify and test exposures for weaknesses with a full scope, multi-layered, simulated attack.

Cloud & Containers Penetration Testing

Uncover vulnerabilities within your AWS, Azure, and Google cloud and containers environments that can undermine your security posture.

Blockchain Security Testing

Protect your decentralized applications and smart contracts from vulnerabilities that are plaguing the cryptocurrency industry.

Testing Approaches

Black-Box vs. Grey-Box vs White-Box

A penetration test aims to identify potential vulnerabilities in your systems before an attacker does. The level of access and knowledge granted to the tester will determine how comprehensive and accurate the test results will be.

Defining the concerns you would like to resolve is essential to designing a customized approach that will effectively meet the necessary security requirements and result in the most value from your penetration testing investment.

	Black-Box *aka closed box penetration testing*	**Grey-Box** *combination of black-box and white-box testig*	**White-Box** *aka open box penetration testing*
Goal	Mimics a true cyberattack	Assess vulnerability to insider threats	Simulate an attacker gaining access to a privileged account
Access Level	Zero access or internal information	Some access and internal information	Complete open access to applications and systems
Pros	Most realistic	Most efficient of time and funds	Most comprehensive
Cons	Time consuming and more likely to miss a vulnerability	No noteworthy cons	Least efficient for time and funds and more data is released to tester

Frameworks, Standards & Methodologies

Packetlabs methodologies, frameworks and standards are derived from the following and are enhanced by our internal team.

- OWASP testing methodology (OWASP top 10 mobile, API, Web, ASVS)
- SANS Pentest Methodology
- MITRE ATT&CK framework for enterprises
- NIST SP800-115 to ensure compliance with most regulatory requirements.

How Often Should You Conduct a Penetration Test?

Regular penetration testing can help limit exposure time - the period between vulnerability scans or penetration tests, when new vulnerabilities may have been publicly disclosed, or changes to the network environment or configuration may have introduced new vulnerabilities.

The minimum recommended interval is once per year or after significant changes to infrastructure or business operations have been made.

However, depending on the business criticality of the systems being tested, and the resources available for remediation, some organizations may opt for quarterly or monthly testing.

Organizations with high-security requirements may also be required to complete a pentest at specific intervals for compliance, cyber insurance renewals or when a merger or acquisition (M&A) is being considered.

Factors That Influence Cost

The cost of a pentest can vary greatly depending on the scope and complexity of the engagement, but the typical range of a quality professional test is between $5K - $150K.

Typical range for quality pentesting is between $5K - $150K

Factors

- Qualifications of testers (experienced & qualified testers will be more thorough)
- Complexity of the target environment
- Desired scope of the test
- Type of testing conducted (white-box/grey-box/black-box, internal/external)
- Robustness of methodology (including % of manual vs. automated testing
- Duration of the engagement

Is it Worth the Price?

The Return on Security Investment (ROSI) metric is the appropriate method of calculating the ROI of penetration testing. It compares the total avoided costs of potential security breaches to the cost incurred by penetration testing.

ROSI = (Security expense avoided – prevention cost) / prevention cost

Example

If your company can expect to avoid even a minor security breach that would cost $100,000 over the next year, and the price of a penetration testing engagement were estimated to be $10,000, then the ROSI calculation would be 9 times the cost.

ROSI = ($100,000 - $10,000) / $10,000 = 9

Why Hire a Qualified Pentester

It is important to hire a qualified penetration tester as it can be the difference between having a secure network and one that is vulnerable to attack. A qualified penetration tester will have the skills and knowledge necessary to find weaknesses in a system and exploit them. They will also be able to recommend countermeasures to fix the vulnerabilities.

All Packetlabs pentesters are required to have a minimum of OSCP (a globally recognized and industry-leading ethical hacking certification offered by Offensive Security). While OSCP is the Packetlabs minimum requirement, many team members go above and beyond to gain additional certified expertise including:

- Evasion Techniques and Breaching Defenses (OSEP)
- Offensive Security Wireless Attacks (OSWP)
- Windows User Mode Exploit Development (OSED)
- Offensive Security Web Expert (OSWE)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Mobile Device Security Analyst (GMOB)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- GIAC Certified Incident Handler (GCIH)
- GCPN Cloud Penetration Tester

Beyond OSCP Certified

Reporting

Packetlabs offers two methods of reporting - traditional and our PTaaS platform.

Packetlabs

Penetration Test Report

ACME Inc.

Report Sections Include

- Risk Level Report
- Executive Summary
- Approach
- Methodology
- Technical Findings
- Recommendations

Traditional Report

Packetlabs traditional report is designed to provide you with the most actionable and comprehensive data possible. The report will outline all vulnerabilities that were found during the engagement, as well as recommend remediation steps.

A Packetlabs pentest report also includes an executive summary, which is perfect for sharing high-level findings with upper management or the board. The report is generated in PDF format and can be customized to include your company logo and branding.

1. Risk Level Descriptions

Risk Ratings

mmary

ation Testing

Download a sample report

PTaaS Online Platform

Packetlabs PTaaS platform is your reporting and workflow management solution. This unified platform provides real-time insights, improved collaboration between teams and tracking for all your pen testing efforts. By automating the data collection process, PTaaS enables you to quickly view findings, prioritize efforts, request retests after remediation and monitor progress.

PTaaS Package Benefits

Integration with JIRA and Service Now

Secure access to past and current reports

Real-time insights and progress monitoring

Instant retest request capabilities

Increased collaboration between teams

Invite all key stakeholders as users

20 Questions to Ask Providers

Here are the top 20 questions you should ask a potential cybersecurity service provider before hiring them:

Company & Tester Qualifications

1. What are the organizational certifications held by your company?
2. Are you SOC 2 Type II accredited?
3. Who would be conducting a penetration test and what are their qualifications?
4. Do you perform background and screening checks of your team members?
5. Do you use contractors for pentesting?
6. Are all pentesters located in Canada/US?
7. Which certifications do your specialists hold?

Process & Methodology

8. What is your penetration testing methodology?
9. How do you maintain internal security in your company?
10. Does your penetration testing service include remediation service?
11. How much of your delivery is automated versus manual?
12. How much of the penetration test is tools-based?
13. Will my services remain available during a penetration test?
14. Are retests of identified vulnerabilities included?
15. What methods or channels of communication are used with testers?
16. Will I have a dedicated project manager?

Reporting & Beyond

17. What is covered in your penetration testing report?
18. What format are the results available in?
19. Do you have an example assessment reports available?
20. Does the ability to retest expire after a specific amount of time?

About Packetlabs

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

Packetlabs is a Canadian SOC2 certified cybersecurity firm specializing in expert penetration testing. We offer a number of services to help strengthen your security posture including infrastructure penetration testing, web and mobile application testing, ransomware pen testing, social engineering, red team exercises, source-code reviews and exploit development.

Our penetration testing often uncovers hard-to-find vulnerabilities that were missed on a prior pentest because of our devotion to constant training and learning. Our team is humble and eager to learn and always applies new tactics in each and every one of our engagements.

Why Choose Packetlabs?

	Other Pentesting Companies	**Packetlabs**
SOC2 Type II Accredited	✗	✓
Canadian Data Residency	✗	✓
No Outsourcing	✗	✓
No Egos, Ever	✗	✓
No False Positive Findings	✗	✓
Coverage-Based Approach	✗	✓
OSCP-Minimum Staffing	✗	✓
95% Manual Testing	✗	✓
Quick Engagement Starts	✗	✓
Open Retest Time Frame	✗	✓

Notes

Notes

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