NWG

HACKING YOUR BUSINESS FOR THE GOOD OF YOUR BUSINESS:

The Essential Guide to High-Quality Penetration Testing

EBOOK

Why conduct penetration tests?

Penetration testing — or “ethical hacking” — provides a proactive, real-world assessment of your security posture, revealing vulnerabilities and security gaps before malicious actors can exploit them.

By simulating real-world attacks, penetration tests give you the insights you need to prioritize risks, harden defenses, and make informed security investments. In short, penetration testing is a critical tool for any organization serious about protecting its assets, reputation, and bottom line in the face of ever-evolving cyber threats.

How do they work?

A penetration test is not a mere academic exercise or game of 'capture the flag'. Nor should it foster an adversarial relationship with your team.

The ethical hacker's role isn't to prove they're smarter than anyone. The true goal of these exercises is to identify risks that malicious actors could exploit. Once these risks are uncovered, a prioritized remediation roadmap can be developed to guide your security efforts. A penetration test should require very little involvement from your team. In fact, we recommend limiting your team's engagement until attacks are detected, ensuring a realistic assessment of your detection and response capabilities.

A comprehensive penetration test typically takes three weeks, delivering rapid yet thorough results. Upon completion, you'll receive a crystal-clear, concise, and action-oriented report that not only identifies your risks but also translates them into business terms.

It's important to keep in mind that penetration test results reflect your security posture at a specific point in time. New vulnerabilities emerge quickly and threats evolve constantly.

A single penetration test, while valuable, only provides a snapshot of your current risk profile. To maintain a strong security stance, organizations should consider conducting periodic penetration tests.

Regular testing helps ensure that your defenses remain effective against the latest threats and that any new vulnerabilities are identified and addressed promptly.

A full scope, high-quality penetration test would typically include the following steps:

What are the hallmarks of a high-quality penetration test?

Here are the five key principles:

COMPREHENSIVE

A penetration test goes well beyond vulnerability testing. The aim is to identify complex interactions and configurations in your environment that could be exploited by a threat actor. It requires thinking like a threat actor, a deep understanding of the target environment and customizing the approach to uncover hidden vulnerabilities.

NON-DISRUPTIVE

Your business should not be disrupted by these tests. This is particularly important in critical environments. Therefore, penetration tests should be conducted by formally trained, highly experienced professionals who operate with surgical precision.

CONTEXTUAL

Unlike automated scans that merely identify and list known vulnerabilities, a high-quality penetration test must provide context. This helps you understand your risk profile in depth and guides you in prioritizing and mitigating risks effectively. This tailored analysis is key for making informed decisions to protect your assets and business operations.

In short, it should give you points that apply to your environment.

COMMUNICATIVE

high-quality penetration testing involves constant communication, it is an open dialogue of discovery, feedback, and learning between the pentesters and your business. It is not just delivering a final report.

For instance, if a critical vulnerability is discovered, testing may be halted until the issue is addressed, ensuring immediate response to pressing security concerns.

COHERENT

A high-quality penetration test will be coherent throughout the engagement, and the final report should reflect a unified approach where methodologies, expertise and documentation are aligned.

It should also be coherent with your security strategy, approach and resources. The report should be accurate, clear and immediately actionable.

“ For penetration testing to be relevant and valuable, knowing how *real* attacks are being done is a must ”

Steve Fuller, NWG Founder

		High-quality Penetration Testing	Average Penetration Testing
Practitioners	Highly skilled, up-to-date ethical hackers	✓	?
	Experience with current, complex technologies and domains	✓	✗
	Current knowledge of real attacks tactics and evolution	✓	?
	Understanding of your organization's specific needs and approach to security and risk	Deep understanding	Basic notion of generic business and IT approaches
Analysis	Applicability of findings	✓ **Considers broader context:** Takes into account the organization's environment and business	✗ Unable to rate the risk specifically related to the organization
	Risk assessment approach	Unique assessment of the company	Generic severity ratings
	Accuracy of risk assessment	**Full:** Holistic approach	Partial
Reporting	Brief with actionable insights	✓	✗
	Meaningful risk categorizations	✓ Applicable to your organization's unique case	✗ Generic
	Containing effective mitigation measures	✓	✗

When it comes down to it, you want penetration testers who are more than just skilled technicians.

Look for seasoned professionals who can put their findings into the context of your unique business needs. Rather than handing you a generic checklist, they should provide a tailored analysis that paints a clear picture of your risk landscape. But the real value lies in the final deliverable: a concise, high-quality report that's easy for stakeholders to understand and act upon.

The best penetration testing reports provide clear, prioritized recommendations that your team can put into practice right away to strengthen your security posture. Insist on a report that's not just technically sound, but also business-savvy and immediately actionable.

“ If you receive a penetration test report at 3pm, you should be able to start implementing by 3:15pm ”

Chris Neuwirth, NWG Senior Ethical Hacker

Pitfalls to avoid in penetration testing

With over 25 years of industry experience and insights from partners and clients, we've identified several common pitfalls in penetration testing:

- **AN ADVERSARIAL APPROACH:** Your penetration testing vendor should be a partner, not an adversary trying to catch you off guard.
- **DELAYED COMMUNICATION:** Critical vulnerabilities shouldn't be kept under wraps until the final report. Your vendor should promptly notify you and provide guidance on remediation.
- **IMPRACTICAL REPORTING:** A complex, lengthy report that's difficult to act upon defeats the purpose of testing. Reports should be concise, clear, and actionable.
- **SCOPE CREEP:** Purple teaming, vulnerability scanning, and security management are valuable but distinct from penetration testing. A true penetration test should maintain a clear scope.
- **INEXPERIENCED TESTERS:** Penetration testing tools can be disruptive when misused. Testers should be well-versed in their tools to avoid unintended consequences like system crashes or network flooding.

When to consider high-quality penetration testing

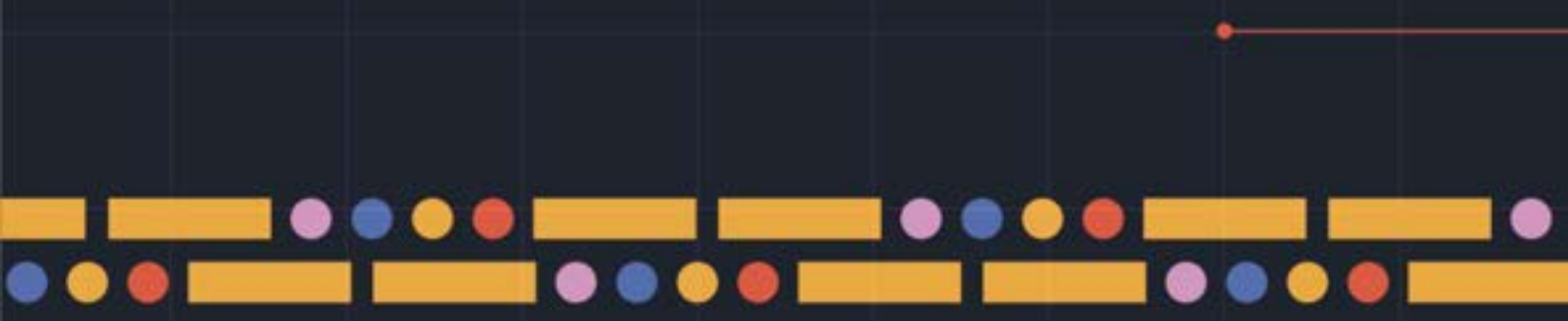
Your penetration tests don’t seem to be as actionable as they could / are difficult to understand

If you have conducted penetration tests but they don’t seem to provide you with relevant, specific, and actionable advice; or the reports are simply too cumbersome and complex for you to implement and the suggestions might not have a positive impact on the security of your business, it may be a sign you should consider other options.

You are already doing vulnerability scans but need help in prioritizing your security investments

Vulnerability scans are useful practice for the business. Yet, in order to have a clear picture of your risks and, more importantly, prioritize your security investments in a logical, efficient, and effective way, you may benefit substantially from a high-quality penetration test.

When you need to answer the question “What is the real-world effectiveness of my security against today’s threats?” you should look at high-quality penetration testing



Security in general and pentests in particular are areas where keeping up with new developments is key, together with a deep technical knowledge and a strong, tested methodology.

Tactics and methods used by real attackers change at a very fast pace, so keeping up is challenging for any security team. A vendor providing high-quality penetration testing would reflect the current “real life” attacks without disrupting your real business.

Finally, given the constant and fast change in attacks, best practice recommends regular testing for a continued understanding of your risks and the ability to prioritize so you can deliver business value.

Additional reading and next steps

FROM OUR BLOG

Lessons Learned from Analyzing 20+ Penetration Test Reports: A Critique and Reflection

Qualities of a Great Penetration Test

Difference Between Pentest and Vulnerability Management and Why You Need Both

Book a scoping discussion with NWG: networksgroup.com/get-started

(888) 798-1012
info@networksgroup.com

455 E Eisenhower Pkwy, Suite 300
Ann Arbor, MI 48108
networksgroup.com