GUIDEPOINT SECURITY

# [INSIGHTS REPORT]: 5 Common Pentesting Pitfalls to Avoid

Effective penetration testing requires the use of appropriate planning, scoping, and methodologies, as well as a commitment to understand the outcomes and apply relevant mitigations to the security operations process. For organizations to achieve their security objectives during a penetration test and maximize their return on investment (ROI), penetration testing needs to be focused, purposeful, and designed to avoid the most common pitfalls and missteps that often plague successful penetration testing outcomes.

## Pitfall #1: Don’t Panic!

Penetration testing can sometimes confuse businesses, particularly around what it means and what it will involve. Frantic questions and comments may drive the initial conversation, such as “How much of this do I have to do myself?” or “I don’t know what a red team is!” or “We’re on a super tight timeline to get this done.” For a business in need of a penetration test, the best thing to do is take a deep breath and proceed the right way: understand why penetration testing is important and take some time upfront to define the scope and rules of engagement.

## Pitfall #2: Failing to understand your purpose

The reasons why organizations engage in penetration testing vary. Some organizations use penetration testing to meet compliance requirements. Others want to ensure the safety and confidentiality of sensitive data, as well as customer goodwill. Some businesses view penetration testing as an opportunity to prove to their executives that their systems are not as secure as the company thinks they are. Other companies may have just implemented some new security technology or software that they want to ensure is working. All of these are entirely valid reasons for why companies initiate the penetration testing process. But penetration testing needs to be driven by more than just generalities, and a successful penetration testing effort requires forethought and planning.

## Pitfall #3: Inadequate objective definition and understanding

Penetration testing objectives can vary, depending on the overall purpose and goals (which is why avoiding Pitfall #2 is so important!). Common pentesting objectives include:

- Conduct an inventory of the attack surface
- Identify security gaps
- Test effectiveness of security
- Demonstrate real-world impacts
- Drive awareness and prioritization
- Ensure regulatory compliance (e.g., NIST, HIPAA, PCI, FFIEC, NYDFS (23 NYCRR 500) and FINRA)

When defining objectives, it is critical to understand and detail overly general hypotheticals like these when defining penetration testing objectives.

- “I want to see if we’re actually vulnerable.”
- “I think we’re vulnerable, but no one cares.”
- “I think our defenses are working but want to be more certain.”
- “I need help justifying this ‘policy,’ ‘procedure,’ ‘tool,’ or ‘service.’

## Pitfall #4: Insufficient understanding of influences and dependencies

Once you’ve detailed any hypotheticals, recognizing and managing the influences and dependencies will help you better understand objectives and goals. For example:

- Informing and engaging with all corporate stakeholders to determine requirements, as well as address any concerns.
- Identifying the party that is requesting a penetration test, such as an executive or compliance auditor.
- Clarifying the process to enable a complete understanding of the penetration test results.
- Determining which individuals or teams will receive the penetration test output (e.g., technical materials, non-technical content, attestations, etc.)
- Understanding who is to receive the penetration testing “assurances.”

## Pitfall #5: Lack of Communication

During penetration testing, it is important to be conscious of who you're communicating with during the penetration testing process and provide the various individuals involved in the testing with the type of information that will be useful to them. For example, technical staff will likely want to know the details of the tests so they can address future potential problems, while executives may not be interested in the minutiae but instead will want straightforward and basic narratives that they can share with the board in order to drive programs and funding.

The ultimate goal of this process is to provide the business with a model to prioritize activities within the penetration testing process by first obtaining meaningful information on any concerns or issues, such as business environment or operational impact and risk levels.

## Author

**Victor Wieczorek**
VP, AppSec and Threat & Attack Simulation
Guidepoint Security

Victor Wieczorek is an information security professional with a broad range of experience in both defensive and offensive security roles. His prior work included delivering various security projects to a wide spectrum of clients with a primary focus on penetration testing, social engineering and security architecture design. As a penetration tester holding both the Offensive Security Certified Expert (OSCE) and Offensive Security Certified Professional (OSCP) certifications, he has helped organizations identify a multitude of weaknesses with a focus on root cause remediation.

## About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.