When you're planning a penetration test, one of the first questions you might have is: **will I get direct communication with testers, or am I going to be stuck talking only to salespeople?** Transparency and clear communication are vital — especially in security, where misunderstandings or vague scopes can lead to missed vulnerabilities or overruns.

In this post, we'll explore how professional penetration testing companies approach communication, project scoping, pricing, and team composition. We'll mention some market players like *Hackeroo*, *binsec group GmbH*, and *Pentest Collective GmbH*, giving you a sense of industry standards and best practices. We'll also delve into the differences between manual pentesting vs scan-only assessments, the benefits of OSCP-certified testers, and why a greybox approach is often the most practical default.

Why Direct Communication with Testers Matters

Too often, security teams find themselves frustrated because they only talk to sales or account managers who may not have the technical depth to address nuanced questions. Direct access to testers—especially those who will actually work on your project—can make all the difference. Here's why:

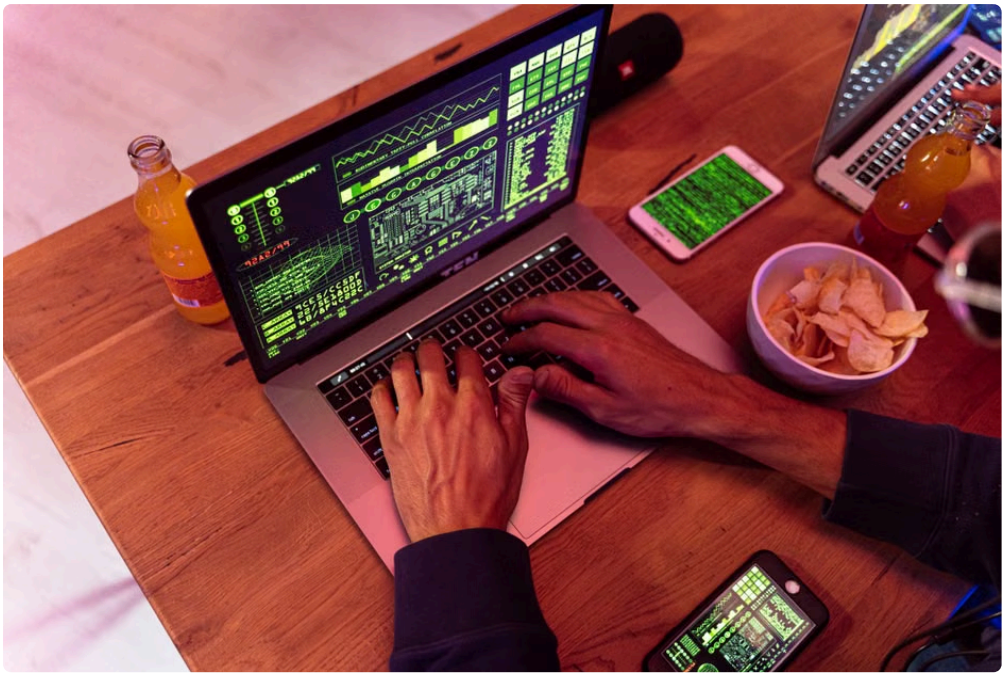
- **Clear requirements and scope:** Testers can help clarify what's truly in scope and suggest realistic goals.
- **Technical questions:** If you're curious about tools, techniques, or risk exposure, testers provide substantive answers from experience, not scripts.
- **Better reporting expectations:** Understanding what the report will cover and how findings are triaged comes directly from testers' standpoint.
- **Flexibility:** If adjustments are needed mid-assessment, you can discuss them directly, avoiding delays or misinterpretations.

Companies like *Hackeroo* emphasize this philosophy by offering a project scoping call where engineers from their pentest teams engage directly with clients' technical staff. This upfront collaboration helps set realistic expectations and prevents scope creep.

Common Roadblocks in Communication

Many pentest companies rely heavily on sales teams to handle client conversations. While sales reps excel in contract negotiation and customer relationships, they often lack the deep technical knowledge needed for meaningful dialogue on cyber risk nuances or vulnerability details.

Here's a story that illustrates this perfectly: learned this lesson the hard way.. Beware of situations where early conversations feel evasive on technical points or when sales representatives dodge your questions about which tools testers use, team qualifications, or how findings are triaged. Such red flags often indicate a "checklist-only" or scan-centric approach rather than a manual, investigative pentest.



Manual Pentesting Versus Scan-Only Assessments

A critical aspect that's often blurred is the distinction between comprehensive manual penetration testing and automated scan-only assessments. This difference drastically impacts results and communication needs.

Aspect Manual Pentesting Scan-Only Assessment Approach Hands-on exploration of systems by skilled testers Automated vulnerability scanning tools without manual validation False Positives Reduced by tester verification Higher rate, needs manual follow-up Complex Vulnerabilities Identifies business logic and chained exploits Misses non-technical/complex issues Communication Closer, more technical engagement Often limited, report delivered by sales or account teams

Leading providers like *binsec group GmbH* and *Pentest Collective GmbH* stress manual pentesting in their service offerings, ensuring that their testers hold certifications like OSCP (Offensive Security Certified Professional). This ensures testers not only rely on tools but also possess the skill to https://hackeroo.com/en/ think creatively and adapt during testing.

Pricing Transparency and Fixed-Price Quotes

Pricing is another arena where transparency matters. You want to avoid vague “call us for pricing” or complex, hidden fees. A company that presents fixed-price quotes or clear daily rates upfront is easier to budget for and builds trust.

For example, companies such as *Hackeroo* advertise a daily rate starting at **1.160€ per day**. This rate typically includes a mix of senior and junior testers, project scoping calls, the manual pentesting effort, and the delivery of a quality report.

Breaking down the daily rate might look like this:

- Senior tester with OSCP certification for strategic oversight and complex exploitation (50%)
- Junior tester with foundational certifications for supporting repetitive tasks and documentation (50%)

Clear pricing empowers your procurement and management teams to make informed decisions without last-minute surprises.

Fixed-Price Versus Time-and-Materials

Fixed-price engagements work well when scope is well understood and stable, reducing financial risk. Conversely, time-and-materials contracts allow flexibility when the environment or scope is uncertain but can lead to unpredictable costs.

During the *project scoping call*, experienced companies like *binsec group GmbH* walk through your environment and goals carefully to recommend the best pricing model for your needs.

Team Composition and Certifications: Why OSCP Matters

Many companies highlight tester certifications as a mark of quality. The OSCP (Offensive Security Certified Professional) is considered a gold standard for pentesters—indicating hands-on skills in penetration techniques, creative problem-solving, and ethical hacking methodologies.

Multiplying this by having both senior and junior testers on the same team provides:

1. **Senior testers** who can tackle complex issues, mentor juniors, and ensure thorough exploitation.
2. **Junior testers** who can support tasks, conduct initial reconnaissance, and contribute to efficiency.

This blend allows companies like *Pentest Collective GmbH* to deliver high-quality outcomes with cost efficiency, balancing expertise and effort.

Greybox Testing: The Practical Default

Among penetration testing approaches, you’ll hear terms like blackbox, whitebox, and greybox:

- **Blackbox:** No prior knowledge; tester simulates an external attacker.
- **Whitebox:** Full access to source code, architecture diagrams, credentials.
- **Greybox:** Limited knowledge or credentials; common in real-world engagement.

the the greybox approach typically provides the best balance of effort and value. You give testers enough information to prioritize meaningful areas but not so much that the test becomes a simple code review.

I'll be honest with you: companies like hackeroo often recommend greybox for web applications and apis, and tailor the scope during the project scoping call accordingly.

How to Ensure You Get Direct Communication and Technical Clarity

When engaging a pentest provider, consider these practical tips:

1. **Ask for a project scoping call** involving actual testers, not just sales.
2. **Request transparency on pricing, team composition, and certifications.**
3. **Clarify what type of pentesting you'll get** (manual vs scan-only).
4. **Insist on clear channels for technical questions during and after testing.**
5. **Demand sample reports or templates to evaluate depth and style.**

The best companies like *binsec group GmbH* routinely accommodate such requests and see direct technical conversations as part of building trust.

Conclusion

In the penetration testing space, having direct communication with testers rather than only sales staff is a hallmark of a mature, client-focused service. Companies like *Hackeroo*, *binsec group GmbH*, and *Pentest Collective GmbH* emphasize transparent pricing (daily rates starting around **1.160€**), OSCP-certified testers, and collaborative project scoping calls to foster technical clarity.

By insisting on a manual, greybox approach executed by a balanced team of senior and junior testers, you ensure insights beyond the surface vulnerabilities. Ultimately, to avoid "buzzword bingo" confusion, insist on substance over marketing techniques—and you will get a penetration test that truly elevates your security posture.

If you're evaluating pentest providers, start by requesting a technical project scoping call. You'll quickly see which companies prioritize engagement with engineers and which rely too much on scripted sales pitches.