When planning a penetration test for your internal systems, it's crucial to clearly understand what "internal" encompasses, the scope of testing, and how pricing and methodologies can impact the quality and usefulness of the engagement. In this article, we'll unravel what internal systems typically include, highlight key considerations such as access requirements, and explain the differences between manual pentesting and scan-only assessments. We'll also touch on team composition with OSCP-certified testers and common pricing models with references to companies like Hackeroo, binsec group GmbH, and Pentest Collective GmbH who are shaping the market with transparency and professionalism.

What Exactly Counts as "Internal" in Pentesting?

"Internal" can have varying meanings depending on context, but in penetration testing it generally refers to systems and networks accessible from within your organization's perimeter, without requiring public internet access or third-party VPNs. Let's break down common categories that often fall under internal scope:

1. Internal Network

This includes:

- Corporate LAN and Wi-Fi networks
- Subnetworks separated by VLANs but reachable internally
- Network appliances such as internal DNS, DHCP, Active Directory Domain Controllers
- Internal routing and firewall devices

Testers simulate attacks as if they were employees, attackers with physical access, or compromised accounts already inside the network perimeter.

2. Internal Applications

Internal applications are those built or hosted exclusively for employee or contractor use. Examples include:

- Intranet portals

- Internal CRMs or ERPs
- APIs accessible only from the internal network or VPN
- Custom tools for finance, HR, or operations that are not exposed publicly

Access to these apps usually requires being on the internal network or connected securely via company VPN, often with additional authentication layers.

3. Access Requirements Define Scope Boundaries

Understanding how an attacker might gain access is critical to scoping the test. For internal pentests, common access assumptions include:

- Tester has physical or logical access to internal network segments
- Tester possesses credentials simulating a typical end-user or privileged employee (greybox testing)
- Testing starts where an employee machine would be placed, not from internet-facing endpoints

Requests to test beyond these assumptions (for example, starting from zero knowledge outside the perimeter or via physical attacks) must be made explicit and scoped appropriately.

Why Transparent Pricing and Fixed-Price Quotes Matter

Pricing in penetration testing can be confusing, with black-box costs, vague hourly estimates, and sales-first approaches that obscure real cost drivers. Leading companies such as **Hackeroo**, **binsec group GmbH**, and **Pentest Collective GmbH** emphasize transparency and clarity in pricing to build trust and help clients budget responsibly.

For instance, a typical *daily rate* for manual internal pentests might start at around **1.160€ per day**. This rate often covers:

- Engagement scoping
- On-site or remote test execution
- Report writing and debriefs
- Re-tests of remediated findings (sometimes included)

Fixed-price quotes allow companies to avoid surprise fees during or after the engagement and encourage a better scope definition upfront. They also distinguish serious manual pentests from simple automated scans that carry different effort levels and risks of missed vulnerabilities.

Manual Pentesting vs Scan-Only Assessments: What's the Difference?

It's essential to clear up a common buzzword confusion in the industry: an automated scan is *not* a penetration test. Many vendors offer scan-only reports with vulnerability scanner outputs but call them pentests, leading to inflated expectations and inadequate security measures.

Manual pentesting typically involves:

- Deep reconnaissance and system enumeration tailored per environment
- Customized exploit attempts combining multiple vectors
- Privilege escalation and lateral movement testing in internal networks
- Logical tests for business logic flaws in internal apps

- Human verification to avoid false positives

Automated scans, while useful for baseline assessments, fail to unearth complex attack paths and creative misuse of legitimate functions. Thus, engaging testers from companies like **binsec group GmbH** and **Pentest Collective GmbH** who perform manual assessments ensures deeper coverage and practical findings.

The Value of OSCP-Certified Testers and Balanced Teams

The skills and certifications of your pentest team matter immensely. The **OSCP (Offensive Security Certified Professional)** credential is widely recognized in the cybersecurity field as a rigorous indicator of hands-on penetration testing capability.

Organizations like **Hackeroo** pride themselves on comprising teams that blend senior and junior OSCP-certified testers. This setup offers many advantages:

- Experienced seniors provide strategic attack planning and oversight
- Juniors handle supporting tasks, increasing efficiency and consistency
- Mentoring ensures knowledge transfer and innovation
- A balance of fresh perspectives and seasoned judgment

This approach also improves cost-effectiveness, allowing clients to benefit from expert-led tests without excessive price premiums.

Why Greybox Testing is a Practical Default for Internal Pentests

When assessing internal systems, **greybox testing** is often the most realistic and productive approach. Greybox means the tester receives limited to moderate information about the environment — such as network diagrams, user credentials, or application documentation — simulating an attacker who has gained some foothold or insider knowledge but lacks full access.

This approach balances effort and insight by providing testers enough context to focus on meaningful vulnerabilities without requiring exhaustive discovery work from scratch. It aligns well with many internal scenarios where a compromised employee account or workstation might be the initial vector.

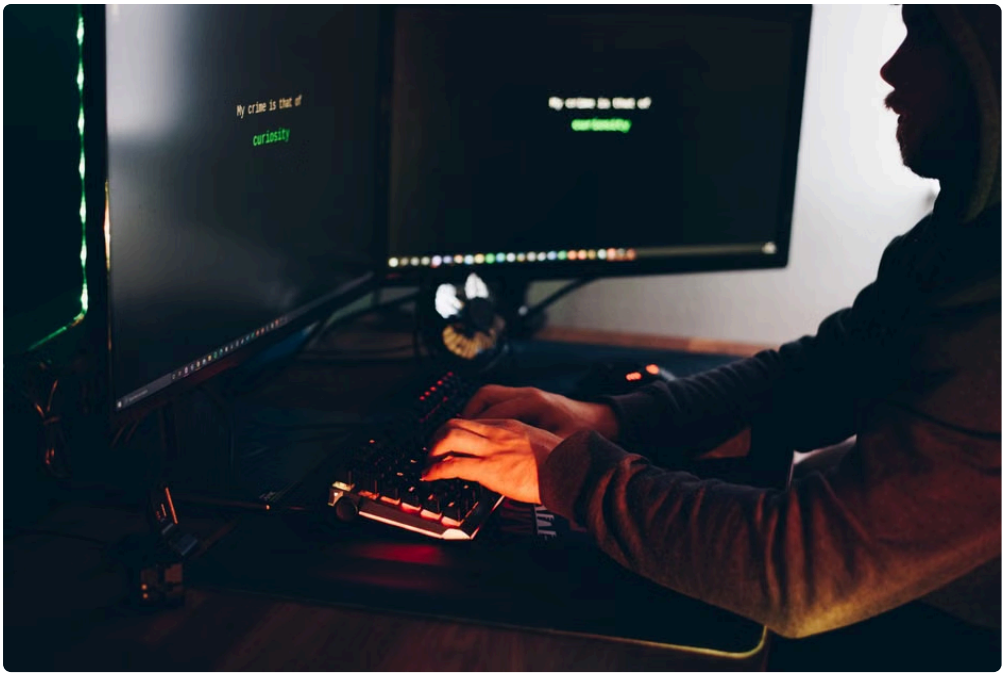
In contrast, blackbox tests (zero knowledge) can be time-consuming and less targeted, while whitebox tests (full info to testers) may overlook realistic attacker blind spots.

Summary: Key Takeaways for Internal Pentesting

Consideration Best Practice / Industry Norm Define “Internal” Scope Includes internal networks, not internet-exposed; internal applications needing network or VPN access Access Requirements Assume tester has internal network or VPN access and possibly employee credentials (greybox) Pricing Transparency Fixed-price quotes starting around 1.160€ per day; no vague hourly estimates Assessment Type Manual pentesting over scan-only reporting for thoroughness Team Composition OSCP-certified testers combining senior and junior levels Testing Methodology Greybox serves as practical default for internal engagements

Partnering with the Right Pentest Provider

When selecting a pentest provider for your internal systems, look for teams that:



- Offer clear, upfront scope definitions focusing on your internal app and network environments
- Present transparent and fixed-price quotes like those from **Hackeroo**, **binsec group GmbH**, and **Pentest Collective GmbH**
- Use manual techniques led by OSCP-certified testers
- Provide comprehensive reports beyond checklists, with practical remediation advice
- Are willing to answer technical questions candidly rather than focusing solely on sales language

By understanding what counts as internal and choosing your pentest partner carefully, you empower your security team with actionable insights that truly protect your organization.

About the author: With over 12 years of experience as an in-house security lead at a Berlin SaaS company and now a freelance security writer, the author specializes in helping teams scope penetration tests and prepare for audits focusing on web apps, APIs, and internal https://hackeroo.com/en/ networks in B2B environments.