When organizations look to bolster their security posture, the phrase **red teaming** often comes up. But what does it truly entail? Does red teaming include elements like social engineering and process abuse, or is it limited to technical exploitation? And how do companies like Hackeroo, binsec group GmbH, and Pentest Collective GmbH approach these challenges?

In this article, we'll explore the scope of red teaming, the role of social engineering and process abuse, differences between manual pentesting and scan-only assessments, the importance of team composition featuring OSCP-certified testers, and pricing transparency—all viewed through the lens of people, process, and technology.

Understanding Red Teaming

First off, let's define what red teaming involves. Designed to mimic an advanced adversary, a *red team* conducts a comprehensive emulation of real-world attackers targeting an organization's people, processes, and technology. Unlike standard vulnerability scans that produce automated reports, red teaming is manual, adaptive, and focused on **bypassing controls** and **staying undetected**.

Red team engagements often push beyond technical vulnerabilities to test organizational resilience, including physical security, employee security awareness, and operational workflows.

Is Social Engineering Part of Red Teaming?

The short answer: **Yes, social engineering is frequently a critical element of red teaming exercises.** After all, attackers commonly exploit the human factor—whether through phishing, pretext phone calls, or in-person interactions—to gain initial access or escalate privileges.

Leading security firms such as Hackeroo explicitly include social engineering tactics in their red team offerings to simulate this attack vector realistically. Likewise, binsec group GmbH frames social engineering as a key pillar to test the 'people' layer in security. Pentest Collective GmbH often combines process abuse with social engineering to uncover gaps that purely technical tests might miss.

Process abuse here refers to leveraging or circumventing internal policies and workflows in unintended ways. For example, exploiting an approval process flaw or abusing employee offboarding steps.

People, Process, Technology: The Triad of Security

From an effective red teaming perspective, organizations should be mindful of the **people, process, technology** triad:

- **People:** Humans are the most unpredictable component. Social engineering aims to exploit this weakness.
- **Process:** Flawed or poorly enforced security procedures offer attackers an entry point via process abuse.
- **Technology:** The actual systems, networks, and applications that need protection.

Red teaming tests the entire triad. Without evaluating all three, teams risk missing attack vectors that real adversaries will find.

Bypassing Controls and Staying Undetected

A hallmark of red teaming is not just breaking in, but doing so while **staying undetected**. This contrasts with vulnerability scans or automated tools that often alert defenses as soon as they start probing. Manual, OSCP-

certified testers understand how to carefully tread through an environment, exploiting weaknesses without triggering alarms.

Manual Pentesting vs Scan-Only Assessments

It's important to distinguish red teaming and manual pentesting from mere scan-only assessments. Many vendors offer "pentests" that rely primarily on automated scanning tools. While these scans can be useful for identifying known vulnerabilities, they fall short in testing an organization’s real-world attack readiness.

Red teams and manual pentesters from firms like Hackeroo or Pentest Collective GmbH bring OSCP-certified expertise to blend technical skill with creativity. This approach uncovers complex issues like business logic flaws, chained exploits, social engineering weaknesses, and process abuse that scanners miss.

To put it simply:

Aspect Scan-only Assessment Manual Pentesting / Red Teaming Technique Automated scans Manual testing, creativity, targeted exploitation Scope Known vulnerabilities in technology People, process, technology with social engineering and process abuse Detection Often noisy and triggers alerts Stealthy, mimics real attacker behavior Output Vulnerability list Contextualized attack scenarios, exploitation paths

Team Composition and OSCP Certification

When selecting a red team or pentest provider, team composition is paramount. Companies like binsec group GmbH emphasize a mix of senior and junior testers, ensuring knowledge transfer and comprehensive coverage. Having OSCP (Offensive Security Certified Professional) certification is often a baseline standard—indicating that testers have demonstrated hands-on offensive skills through rigorous practical exams.

An effective team blends deep experience with fresh perspectives. Seniors provide strategic direction and handle complex exploit chains, while juniors perform foundational tasks and support breadth testing.

Why Greybox Testing Makes Sense as a Default

Greybox testing, where the tester has partial knowledge of internal systems (such as limited user credentials), strikes a practical balance between blackbox (no knowledge) and whitebox (full knowledge) assessments. This approach realistically models many attacker scenarios who may have gained some foothold or insider information.

Hackeroo and Pentest Collective GmbH often recommend greybox methodology by default because:

- It enhances test effectiveness by focusing on realistic attacker assumptions.
- Improves efficiency, enabling testers to use partial data to find deeper issues.
- Balances confidentiality, only sharing what's needed with testers.

Transparent Pricing and Fixed-Price Quotes

Anyone serious about red teaming should expect clear and upfront pricing, avoiding vague estimates or hidden fees. For example, leading providers such as Hackeroo offer transparency with a daily pentest scoping questionnaire rate starting at **1.160€ per day**.

Fixed-price quotes based on agreed scopes help manage expectations and budgets effectively. During scoping, it's essential to have a one-sentence summary of the test boundaries to avoid scope creep.

Many customers get frustrated with pricing models that appear nebulous, or vendors who dodge technical questions in favor of sales talk. Companies like binsec group GmbH stress the importance of opening up lines of clear communication from the start.

Summary: What Red Teaming Includes

1. **Technical Exploitation:** Network, application, and system vulnerabilities.
2. **Social Engineering:** Phishing, pretexting, and other human-targeted attacks to bypass user controls.

3. **Process Abuse:** Leveraging procedural or policy weaknesses, such as business process flaws.
4. **Stealthy Execution:** Designed to stay under the radar, emulating real attacker behavior.
5. **Manual, Skilled Testing:** Employs OSCP-certified experts and team blends to deliver comprehensive coverage.
6. **Greybox Methodology:** Realistic approach based on partial internal knowledge.
7. **Transparent Pricing:** Clear daily rates and fixed quotes aligned to defined scopes.

Final Thoughts

If you're considering a red team exercise, inquire clearly: *Does your scope explicitly include social engineering and process abuse?* Avoid companies that offer only automated scans or shy away from these critical layers of testing.

Reputable providers like Hackeroo, binsec group GmbH, and Pentest Collective GmbH understand that true security lies at the intersection of people, process, and technology. With transparent pricing—starting at around 1.160€ per day—and OSCP-certified testers operating in a greybox framework, you get a realistic assessment that helps your organization prepare for today's sophisticated threats.

Remember, not all "pentests" are created equal. When it comes to red teaming, social engineering and process abuse aren't optional extras—they're essential.