Pakagrong Lebel - The White Hat Lab

Red Teaming Security Assessment Checklist V1.0

A comprehensive and professional guide for adversarial security testing operations. This document outlines a structured methodology that ensures all elements of red team operation are addressed, including scoping, reconnaissance, execution, analysis, and long-term improvement.

November 20, 2025

Table of Content

Red Teaming in the Age of Escalating Cyber Threats

Organisations face unprecedented cyber risks and the costs are staggering. IBM's 2025 Cost of a Data Breach report shows the global average breach runs about **$4.44 million** (and in the U.S. it hit a record **$10.22 million**) [1]. Even as defenses improve, attackers keep shifting tactics. For example, business-email-compromise (BEC) schemes in 2025 alone caused an estimated **$6.3 billion** in losses worldwide [2]. Critical industries remain prime targets: healthcare still has the highest breach costs (around **$7.42 million** per incident) [1]. These trends make it clear that organizations can't afford to fall behind today's sophisticated threats.

Attackers have grown more advanced. Recent studies show roughly **16% of breaches** in 2025 involved adversaries using AI tools (often to automate phishing or generate deepfakes) [1]. Real-world examples illustrate the stakes: in late 2025 hackers leaked personal data on **5.7 million Qantas** airline customers after a ransom demand was refused [3]. Around the same time, a cyber-extortion campaign stole roughly **570 GB** of internal code and client data from Red Hat (IBM's open-source unit) during a supply-chain attack [3]. Each of these incidents combined technical exploits with social or third-party weaknesses; exactly the kind of complex, multi-vector threat profile that adversaries use today.

This is where **red teaming** makes a difference. Unlike standard vulnerability scans, red teaming casts a wide net: it mimics real-world attackers across cyber, physical, and human domains. A skilled red team will attempt network intrusions, test physical access controls, and even conduct live social-engineering attacks to emulate a true adversary. Industry research underscores the payoff: organizations with mature red team programs see dramatically better results. For example, one analysis found companies running regular red-team exercises experienced about **25% fewer security incidents** and **35% lower breach costs** compared to those without [1]. Another study noted those firms had **64% fewer** total incidents overall [1]. In short, thinking like an attacker helps teams uncover hidden gaps before criminals do.

Red Teaming Checklist: Definition, Components, and Benefits

Definition and Purpose

A red teaming checklist is essentially a structured roadmap for a simulated attack exercise [4]. It documents the exercise's objectives, scope, and methods specifying which assets will be tested, which techniques will be used, and who on the team is responsible for each task [4] [5]. By spelling out the goals and boundaries up front, the checklist keeps the red team focused and aligned with the organisation's priorities and compliance requirements.

Core Components of a Red Teaming Checklist

A comprehensive red teaming checklist typically covers several core elements [6]:

- **Scope and Roles:** Define what systems, networks, or data are in scope and outline each team member's role. This makes clear who is on the red team, what targets they will test, and what objectives they must achieve [6].
- **Targets & Rules of Engagement (RoE):** List the specific assets to test and the rules of engagement. This specifies what actions are allowed or forbidden (for example, attack methods that are off-limits) so the team can probe defenses aggressively without causing unintended harm [6].
- **Reconnaissance Guidelines:** Provide instructions for intelligence gathering on the target. This might include approved scanning techniques, open-source intelligence methods, and any limits on information collection, ensuring reconnaissance is thorough but controlled [6].
- **Documentation & Reporting:** Establish how findings should be recorded and communicated. The checklist should set standards (for example, using specific report templates or formats) so that all discoveries and evidence are logged consistently and clearly [6].
- **Mitigation Planning:** Assign responsibility for remediating issues discovered during the test. In other words, it should describe how identified vulnerabilities will be tracked and fixed, including who owns each follow-up action [6].

These elements ensure the team knows exactly what to do and how to do it, while also providing structure for later analysis and remediation.

Benefits of Using a Red Teaming Checklist

Using a checklist brings several important advantages for security teams:

- **Consistency:** It helps each red teaming exercise follow a standardized process, so no critical steps are overlooked. This consistency makes it easy to compare results across different tests and build on past findings [6].
- **Compliance:** Many organizations are required to demonstrate that they conduct regular security testing. A documented checklist provides clear evidence of the steps taken and can simplify audit reporting [6].
- **Collaboration:** By clearly defining roles, responsibilities, and procedures, the checklist ensures all team members including consultants or other departments are on the same page. This clarity improves coordination and efficiency during the exercise [6].
- **Reduced Risk:** Explicit rules of engagement in the checklist prevent the red team from going too far. Documenting these guardrails (for example, which systems to avoid or how to handle live systems) keeps the test controlled and minimises the chance of accidental damage [6].

Together, these benefits show why checklists are invaluable to modern red team exercises: they promote thorough, repeatable testing and help stakeholders trust that the exercise was well planned and managed.

Phase 1: Foundational Preparation

Establish the foundation of the security assessment, including roles, responsibilities, and methodologies.

- [ ] Establish clear boundaries for the security assessment (target systems, infrastructure components, and strategic goals)
- [ ] Catalogue primary stakeholders across departments (Information Technology, Security Operations, Executive Leadership)
- [ ] Build a specialised assessment team with validated competencies in digital attacks, human-factor exploits, and facility security
- [ ] Distribute specific operational functions to team participants (team coordinator, infrastructure testers, behavioural exploitation specialists)
- [ ] Create secure information exchange channels connecting offensive, defensive, and collaborative security units
- [ ] Specify which attack methods and procedures will be authorised for deployment
- [ ] Verify adherence to legal requirements and professional conduct standards
- [ ] Create standardised documentation frameworks for operational parameters, technical materials, communication hierarchies, and event recording
- [ ] Deploy testing infrastructure components (command servers, isolated testing networks)
- [ ] Evaluate organisational risk exposure from planned assessment activities
- [ ] Obtain formal authorisation and resource commitment from executive management

Phase 2: Strategic Preparation

Define operational guidelines, methodologies, and constraints before execution.

- ☐ Formalise the operational boundaries document specifying sanctioned methods, protected systems, maximum intrusion depth, and information exchange procedures
- ☐ Establish specific success criteria for the assessment team
- ☐ Execute preparatory intelligence activities: public information research, network infrastructure identification, personnel digital footprint analysis, external vulnerability surface mapping
- ☐ Catalogue potential intrusion pathways (digital, physical, human-focused)
- ☐ Create response procedures for discovering legitimate security vulnerabilities
- ☐ Ensure assessment activities satisfy regulatory obligations (ISO 27001, NIST frameworks, GDPR requirements)
- ☐ Establish contingency protocols for unplanned service interruptions
- ☐ Design specific attack sequences: authentication bypass, network traversal, deceptive communication campaigns, unauthorised facility entry, malicious insider behaviour simulation
- ☐ Obtain security leadership validation before proceeding with operations

Phase 3: Active Operations

Simulate real-world attacks while maintaining detailed documentation of all actions.

- ☐ Hold comprehensive team orientation to confirm shared understanding
- ☐ Initiate attack sequence execution with meticulous evidence capture
- ☐ Deploy targeted deceptive emails and credential capture techniques
- ☐ Conduct infrastructure vulnerability exploitation
- ☐ Perform software and interface security evaluation
- ☐ Execute human manipulation techniques (voice calls, identity falsification, strategic placement of compromised media)
- ☐ Attempt physical barrier circumvention (unauthorised following, mechanical bypass)
- ☐ Maintain continuous activity records documenting specific actions, successfully compromised resources, and visual documentation
- ☐ Conduct frequent coordination meetings (twice per day recommended) to evaluate progress and modify approach
- ☐ Report critical security weaknesses to designated personnel immediately
- ☐ Preserve normal business operations and prevent unintended service disruption
- ☐ Utilise security validation platforms and simulation tools
- ☐ When discovering actual vulnerabilities, record thoroughly and alert appropriate teams
- ☐ Maintain strict compliance with operational guidelines

Phase 4: Analysis & Remediation

Document findings and develop actionable recommendations for remediation.

- ☐ Facilitate internal team assessment discussion to examine discoveries and insights
- ☐ Produce detailed documentation containing security weaknesses, offensive techniques, business impact evaluation, and supporting evidence
- ☐ Deliver findings to leadership, security personnel, and relevant organizational units
- ☐ Execute collaborative validation session with defensive and cooperative security teams
- ☐ Rank vulnerabilities by criticality and exploitation feasibility
- ☐ Construct detailed remediation plan with designated ownership and completion timelines
- ☐ Record security deficiencies for regulatory compliance and future reference
- ☐ Partner with defensive teams to verify remediation effectiveness
- ☐ Address high-priority issues rapidly and monitor ongoing progress
- ☐ Establish executive responsibility for security enhancement implementation

Phase 5: Program Maturation & Continuous Enhancement

Ensure ongoing enhancement of security assessment processes.

- ☐ Execute comprehensive post-operation review sessions with offensive and defensive participants
- ☐ Document key learnings and opportunities for methodology improvement
- ☐ Revise operational parameters based on acquired knowledge
- ☐ Enhaunce attack techniques and broaden future assessment coverage
- ☐ Provide specialised training on emerging threat patterns and novel attack vectors
- ☐ Plan subsequent validation testing to confirm remediation success
- ☐ Implement automation capabilities for repetitive assessment components
- ☐ Monitor evolving adversary capabilities, including artificial intelligence-enabled attack methods
- ☐ Maintain alignment with updated regulatory frameworks and industry best practices
- ☐ Foster ongoing collaboration across security teams
- ☐ Ensure persistent advancement of security assessment methodologies

Common Pitfalls in Red Teaming

- **Omitting AI/ML model testing:** As organisations adopt AI-driven systems, many still neglect to validate these models within security reviews. Industry experts warn that AI/ML applications "have an even greater attack surface" than traditional software and thus demand continuous security testing [6]. In line with this, recent guidance emphasizes building AI solutions with "secure foundations" that explicitly *"enable AI-model testing"* as part of resilience measures [7]. Failing to incorporate adversarial evaluation of AI/ML systems leaves critical vulnerabilities unexamined.

- **Human error remains dominant:** Data show that unintentional actions by people are at the root of most breaches. For example, a 2025 industry study found that roughly **95% of all data breaches involve human error** [8]. Organizations cite failures like misconfigured systems, lost credentials, or social engineering missteps as the primary factor in security incidents. This underscores that without robust processes and training to catch and prevent simple mistakes, red team exercises – no matter how sophisticated – will identify issues that organizations must still address through better user awareness and procedure.

- **Using unrealistic or outdated scenarios:** Red team exercises that rely on canned or simplistic attack chains will miss real risks. Security experts advise against **"creating unrealistic scenarios that don't match real-world constraints or exploited pathways"** and caution not to "overlook common, low-tech and low-complexity attack methods that are perennially effective" [9]. In practice, this means exercises should mirror current threat tactics – for example, leveraging the latest adversary tools and targeting the same systems attackers do – rather than repeating stale patterns. Outdated scenarios can lull defenders into a false sense of security by highlighting only trivial flaws while serious gaps remain untested.

- **Insufficient executive engagement:** Red teaming often fails to influence strategy when business leaders are not directly involved. Surveys report that a significant fraction of non-technical executives cannot even interpret security findings – for instance, one report found **24% of non-technical leaders needed help to understand incident dashboards** [10]. At the same time, many CISOs say boards and C-suite members underestimate breach risks and offer little guidance. This disconnect means critical issues uncovered by red teams

may not be prioritised; when leadership does not fully grasp the threats, red team results can go unheeded and strategy remains misaligned.

- **Neglecting remediation and follow-through:** Finally, organizations frequently fail to act on red team findings. A recent penetration-testing survey found that nearly 20% of CISOs admit they run penetration tests **only to meet compliance requirements, rather than to improve security** [11]. In effect, test results become checkboxes instead of catalysts for change. Supporting this, a 2025 study reported that **92% of breached organizations believe better basic cyber hygiene could have prevented their incidents** [12]. In other words, even when weaknesses are found (by a red team or otherwise), many teams fall short on actually fixing them. Without disciplined follow-up – tracking recommendations, measuring remediation, and holding teams accountable – red team engagements yield little lasting benefit.

Each of these pitfalls can be addressed through continuous improvement. Security leaders emphasize that red teaming must be an ongoing process: exercises should evolve with the threat landscape (especially incorporating AI/ML concerns), involve stakeholders from the board to the SOC, and include mechanisms to ensure all findings are remediated. By learning from experience and adapting testing methods and organizational practices over time, red teams can close these gaps and strengthen overall cyber resilience.

Strengthening Security Beyond Checklists

Red teaming is most effective when approached as an evolving practice rather than a one time evaluation. Continuous refinement of methods, proactive engagement across the organisation, and timely adoption of emerging threat intelligence are essential for sustaining resilience. A disciplined and adaptive red team program strengthens defenses, enhances response capabilities, and promotes a culture of preparedness throughout the organisation.

References

[1] Galyer, L. (2025, April 23). *Understanding red team exercises*. DigitalXRAID. https://www.digitalxraid.com/red-team-exercises-guide/

[2] Labs, K. (2024, December 31). Top 15 data breaches of 2025 and their financial impacts. *Keepnet Labs*. https://keepnetlabs.com/blog/top-15-data-breaches

[3] Writer, T. | C. (2025, November 11). *List of recent data breaches in 2025*. Bright Defense. https://www.brightdefense.com/resources/recent-data-breaches/

[4] SysTools. (2023, September 4). *Red team in cyber security - Definition, roles, purpose & benefits*. SysTools Managed Services. https://systoolsms.com/blog/red-team-in-cyber-security/

[5] Mindgard. (2025, October 29). The complete red teaming checklist (with PDF download). *Mindgard*. https://mindgard.ai/blog/red-teaming-checklist

[6] *Unleashing the power of AI: The KPMG pioneering approach to AI security*. (n.d.). KPMG. Retrieved November 20, 2025, from https://kpmg.com/us/en/articles/2025/unleashing-power-ai.html

[7] Accenture. (n.d.). *State of cybersecurity resilience 2025*. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-Cybersecurity-report.pdf

[8] mimecast. (n.d.). *Human risk has surpassed technology gaps as the biggest cybersecurity challenge for organizations around the globe as demonstrated in the findings of our SOHR 2025 Report*. Mimecast. Retrieved November 20, 2025, from https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/

[9] Inkson, G. (2025, July 15). *Crafting realistic scenarios for red teaming*. NetSPI. https://www.netspi.com/blog/executive-blog/red-teaming/part-2-crafting-realistic-scenarios-for-red-teaming/

[10] Cytactic. (2025, September 18). 70% of security leaders say internal misalignment creates more chaos than threat actors: Cytactic's 2025 state of cybersecurity incident response management (CIRM) report. *PR Newswire*. https://www.prnewswire.com/il/news-releases/70-of-security-leaders-say-internal-misalignment-creates-more-chaos-than-threat-actors-cytactics-2025-state-of-cybersecurity-incident-response-management-cirm-report-302560507.html

[11] Horizon3.ai. (2025, March 26). *The state of cybersecurity in 2025*. Horizon3.Ai. https://horizon3.ai/downloads/research/annual-insights-report-the-state-of-cybersecurity-in-2025/

[12] Swimlane (2025) *"Cracks in the Foundation: Why Basic Security Still Fails"* https://www.businesswire.com/news/home/20251112850678/en/New-Report-Reveals-92-of-Breached-Organizations-Admit-Stronger-Cyber-Hygiene-Could-Have-Prevented-Incident