rasotec

FREE CHECKLIST

Pentest Readiness Checklist

How to prepare for your penetration test, so that testing time goes into finding vulnerabilities

A well-prepared pentest starts faster, causes fewer interruptions and produces more meaningful results. Work through this list before the kickoff call with your testing provider. Not every item applies to every test: a black box test needs very little information, while gray and white box tests benefit from as much as you can provide.

1 Goals and scope

- [ ] **Define the goal.** Compliance evidence (e.g. ISO 27001, PCI DSS), a release or acceptance test, a check after major changes, or a general assessment of your security posture.
- [ ] **List the targets in scope:** IP ranges, domains and subdomains, URLs, applications, APIs, mobile apps, cloud tenants or accounts.
- [ ] **List what is out of scope,** e.g. third-party services you do not own, fragile legacy systems or production databases that must not be touched.
- [ ] **Choose the approach:** black box (no prior knowledge), gray box (limited information or accounts) or white box (full documentation and source code).
- [ ] **Choose the environment:** production or a staging environment that matches production closely enough for the results to be meaningful.

2 Authorization and legal

- [ ] **Written authorization** from the owner of every system in scope, signed by someone who is allowed to grant it.
- [ ] **Third-party permissions:** check the testing policies of your hosting, cloud and SaaS providers, and inform managed service providers that operate systems in scope.
- [ ] **Contract, NDA and rules of engagement** agreed: permitted techniques, prohibited actions, handling of sensitive data found during the test.

3 Access and information

- [ ] **Test accounts** for every relevant role, ideally two per role so that access between users and tenants can be tested. Use test data, not real customer data.
- [ ] **Network access** for internal tests: a VPN account, a jump host or a network port, plus any required client certificates.
- [ ] **Documentation:** architecture and network diagrams, API specifications (e.g. OpenAPI or Postman collections), and source code for white box tests.
- [ ] **Decide on security controls:** should the testers' IP addresses be allowlisted in the WAF or IPS, or should the test also show what these controls block?
- [ ] **Ask for the testers' source IP addresses** so you can recognize their traffic in your logs.

4 Operations and safety

- [ ] **Test window agreed,** including maintenance windows and periods without testing, e.g. month-end processing or peak sales days.
- [ ] **Business-critical systems identified,** with agreed limits for intrusive tests.
- [ ] **Backups verified** for systems in scope, especially in production.
- [ ] **Contacts exchanged:** a technical contact and an escalation contact on both sides who can be reached during the test window.
- [ ] **Inform your IT team, SOC or MDR provider** so that alerts are not treated as a real incident, unless detection and response are part of what you want to test.
- [ ] **Stop criteria defined:** who may pause or stop the test, and how, if a system behaves unexpectedly.

5 After the test

- [ ] **Report recipients defined.** Treat the report as confidential and share it only with the people who need it.
- [ ] **Owners assigned** for remediation, with deadlines based on the severity of each finding.
- [ ] **Walkthrough scheduled** with the testers to discuss findings and remediation options.
- [ ] **Retest planned** to verify that the fixes are effective.
- [ ] **Test accounts and access removed** or disabled once testing is complete.

Ready for your pentest?

rasotec is a penetration testing company based in Austin, Texas. After each test, we hold at least two follow-up meetings with you and retest the vulnerabilities found free of charge within one year.

Book a free 30-minute consultation · **contact@rasotec.com** · **www.rasotec.com**