RED RAINE LABS

PRE-ENGAGEMENT CHECKLIST

How to Prepare for a Penetration Test

Five steps to walk into your next engagement with a scope that is actually testable and a team that knows what is coming.

How to prepare for a penetration test matters almost as much as the test itself. Running a pentest against the wrong scope, scheduling it during a system migration, or springing it on an unprepared team wastes budget and produces results nobody can act on.

Work through this document with your team. Every step has items to check off and space to write down the decisions you make, so by the last page you are holding your own pre-engagement plan rather than a stack of notes. Bring it to your scoping call and we will finalize the details together.

1. **Inventory Your Assets and Identify What's Critical**
   You cannot scope what you have not inventoried.
2. **Formalize Your Scope**
   Turn the inventory into a document, including what is excluded.
3. **Schedule Around Other Changes**
   Testing a moving target turns results into noise.
4. **Brief Your Teams, and Decide Who Gets Advance Notice**
   Especially the SOC. Make that call on purpose.
5. **Establish Rules of Engagement and Lock Down Access**
   Contacts, an emergency stop, credentials, cloud provider policies.

STEP 1 Inventory Your Assets and Identify What's Critical

You cannot scope what you have not inventoried.

- [ ] **List everything.** Servers, endpoints, network segments, cloud tenants (Azure, AWS, GCP), web apps, APIs, SaaS platforms, and any AI or LLM integrations.
- [ ] **Flag your crown jewels.** What holds sensitive data, what faces customers, and what would hurt the business most if an attacker compromised it.
- [ ] **Decide which environments belong in this engagement,** at a high level: external network, internal network, web apps, cloud and M365, wireless, AI integrations.

ENVIRONMENTS IN SCOPE

CROWN JEWELS THAT MUST NOT FALL

STEP 2 Formalize Your Scope

A vague scope produces a report that does not hold up when you need it.

- [ ] **Turn the inventory into an actual scope document:** IP ranges, domains, app URLs, cloud tenant IDs, and the specific AI integrations or endpoints you want included.
- [ ] **Decide what to explicitly exclude, and put it in writing:** legacy systems you are retiring, third-party-hosted assets you do not control, and production systems too fragile to touch.
- [ ] **Confirm the scope with the testing firm before testing begins,** so everyone is on the same page.

IN SCOPE

EXPLICITLY OUT OF SCOPE

STEP 3 Schedule Around Other Changes

Results become noise when you are testing a moving target.

- [ ] **Do not run a pentest during a migration, major deployment, or infrastructure overhaul.** Check the change calendar first.
- [ ] **Sequence the test after big projects finish, not during them.** That also gives you a cleaner baseline for the next test.
- [ ] **Give us a window, not a fixed date.** Most engagements run one to three weeks. Mark a broad stretch of clear calendar and we will set the exact dates inside it.

EARLIEST WE CAN START

LATEST YOU NEED RESULTS

CHANGE FREEZES, MIGRATIONS OR DEPLOYMENTS TO AVOID

STEP 4 Brief Your Teams, and Decide Who Gets Advance Notice

Everyone who could react to the traffic should know the plan, or be excluded from it deliberately.

- [ ] **Loop in internal IT and security staff, any MSSP or MDR provider, and relevant stakeholders** (leadership, compliance, legal) before testing begins.
- [ ] **Make a deliberate call on the SOC.** Tell them in advance to avoid isolated systems and accounts and measure detection with foreknowledge, or keep them blind for a true read on detection and response. Neither is wrong, so pick one on purpose.
- [ ] **Make sure whoever is on call knows a pentest is happening** and can verify who authorized the traffic.

SOC APPROACH FOR THIS ENGAGEMENT

☐ Notified in advance ☐ Kept blind (true detection test)

TEAMS AND VENDORS BRIEFED

STEP 5 Establish Rules of Engagement and Lock Down Access

The last mile: who to call, what the tester can reach, and whose rules apply.

- [ ] **Nail down points of contact and an emergency stop procedure** for the testing window you set in Step 3, so if something unexpected happens everyone knows who to call and how to pause.
- [ ] **Provide whatever access the engagement actually requires:** allowlisted source IPs for external testing, network access for internal testing, and test credentials for web application or Active Directory testing.
- [ ] **Check your cloud provider's testing rules.** Microsoft, AWS and Google each publish penetration testing policies; some require pre-notification, and some exclude certain services from testing entirely. Confirm before testing an M365 or Azure tenant.

PRIMARY POINT OF CONTACT

TECHNICAL POINT OF CONTACT

WHO CAN AUTHORIZE A STOP

EMERGENCY STOP PROCEDURE

ACCESS TO PROVIDE BEFORE DAY ONE

- [ ] Allowlisted source IPs
- [ ] Internal network access
- [ ] Test credentials

CLOUD PROVIDER POLICIES CHECKED / PRE-NOTIFICATION FILED

Before You Sign Off

Every box ticked means your scope is testable, your team is ready, and the engagement can start on schedule.

- [ ] Asset inventory is complete and the crown jewels are flagged.
- [ ] Scope document written, with IP ranges, domains, app URLs and tenant IDs.
- [ ] Exclusions are in writing.
- [ ] Scope confirmed with the testing firm before any testing begins.
- [ ] Testing window locked in and clear of migrations and major deployments.
- [ ] Internal IT and security, MSSP or MDR, and stakeholders briefed with the dates.
- [ ] SOC notification decision made on purpose, and documented.
- [ ] Points of contact and an emergency stop procedure written down.
- [ ] Access provisioned: allowlisted IPs, network access, and test credentials.
- [ ] Cloud provider testing policies checked, and any pre-notification filed.

OPEN QUESTIONS TO RAISE ON THE SCOPING CALL

Bring this to a scoping call

Red Raine Labs is a Michigan-based, owner-operated penetration testing firm. Every engagement means hands-on exploitation, not automated scanning paired with a template report. You work directly with the person doing the testing. Finish this checklist, then send it over and we will turn it into a scope.

redrainelabs.com/#quote