Pentesting 101 Part 2: The Pre-Req's of Scoping a Penetration Test Engagement

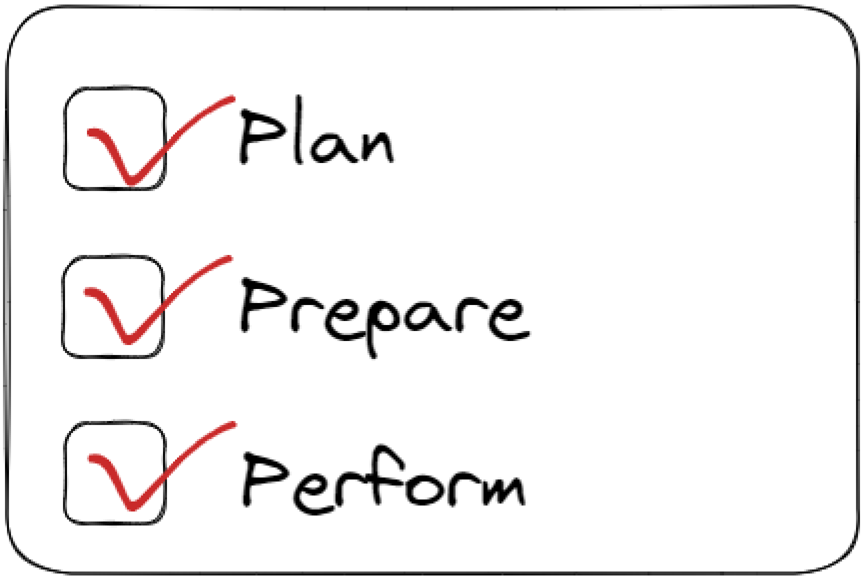
labs.lares.com/pentesting-101-pt2

Steve Spence

June 22, 2023

Following our previous post, let's build on this and continue moving forward.

So, now that we have identified the reason for driving, you need to carry out a penetration test, along with any required testing types. The next step is setting ourselves up for success. The key to this is pretty simple….



The key to success

Scoping

Scoping is one of the most important parts of a penetration testing engagement, as it determines/ensures that both the client's expectations are fulfilled and that enough time is allocated to ensure that the penetration test is performed correctly.

- **Not enough time,** and the test team will struggle to finish in time and could well miss vital things or provide an incomplete report.
- **Conservatively overestimating** *(or slightly over-scoping)* runs fewer risks because the penetration test team can dig deeper into any system/application/environment in scope.

Reporting an accurate *(or even slightly overestimated, for a reason mentioned above)* scope is the first step to ensuring project success!

The prerequisites to successfully scope a penetration test, irrespective of the type of test, should involve the following:

1. All relevant risk owners.
2. Technical staff knowledgeable about the target system.
3. A representative of the penetration test team, this could also be multiple testers, if specialist skillsets are required.

So, for example, where the goal of the test is to ensure good vulnerability/risk management, this would be more suited to an "open-box" penetration test:

1. Risk owners should outline any areas of special concern.
2. Technical staff should outline the technical boundaries of the organisation's IT estate.
3. The penetration test team should identify what testing they believe will give a full picture of the vulnerability status of the estate.

Assuming one already exists, a current vulnerability assessment should be shared with the testers at this stage. Testing can then be designed to support a reasonable opinion on the accuracy and completeness of the pre-existing vulnerability assessment.

Special requirements

During scoping, you should outline any issues which might impact upon testing. This might include the need for out-of-hours testing, any critical systems where special handling restrictions are required, or other issues specific to your organisation.

Constraints

Ok, so let us address the elephant in the room, COST! Penetration testing is not cheap, nor is it a "one size fits all" type of approach.

More often than not, the cost of penetration testing activities and duration is impacted by cost; however, this does not mean that you will not receive a 'fit for purpose' assessment, but it does mean you will have to be realistic about the coverage and depth of testing you are expecting.

The easiest way to do this is by prioritizing assets, e.g., identifying business critical infrastructure, assets and resources that, if compromised or taken down, would adversely impact your business reputation and brand.

Doing so will give you the coverage and depth needed on business-critical applications, assets and environments, making spending more cost-effective and relevant.

For example, a customer login portal and underlying database that facilitates access to personally identifiable information (PII) would need more coverage and scrutiny than a single-page web app serving only static content or an external facing server acting as a load balancer with well-defined rules implemented.

With this in mind, where cost is a contributing factor, customizing the level of depth on different parts of the assessment is a pragmatic approach to getting the best bang for your buck!

Plan of action

Now that we are aware of the above considerations, the scoping process should flow quite naturally, and ultimately, the output of the scoping exercise should be a document stating:

1. The technical boundaries of the test.
2. The types of assessment and tests expected.
3. The timeframe and the amount of effort necessary to deliver the testing - are usually given in terms of resource days.
4. Depending on the type of approach agreed upon, this document may also contain several scenarios or specific 'use cases' to test.
5. The penetration testing team's requirements. This will allow you to do any necessary preparation before the test date. For example, by creating test accounts or simply allocating desk space.
6. Any compliance or legislative requirements that the testing plan must meet.
7. Any specific reporting requirements, for example, the inclusion of CVSS scores or use of recognised severity levels i.e., Critical, High, Medium, Low and Informational. For example, OWASP Risk Rating Methodology.
8. Any specific time constraints on testing or reporting that a penetration testing company will need to consider when allocating resources.
9. Reporting. The test plan and actions are important; however, how that information is conveyed is even more important. The report is the main deliverable of any engagement.

Summary

In summary, as mentioned at the very start of the post, setting yourself/your organisation up for success from the outset is crucially important. The points covered above serve as a basis for you to build upon and tweak to your needs/requirements.

Scoping penetration testing does not need to be hard, daunting, or long-winded!

Remember, the …

Devil is in
the detail