Pentesting 101 Part 1: So, you need or want a Pentest

labs.lares.com/pentesting-101-pt1

Steve Spence June 5, 2023

penetrationtesting

So, that day has finally come when you've been tasked with obtaining a penetration test for that project you've built or are accountable for, or perhaps you've been informed that it's necessary due to "compliance requirements".

Steve Spence

Jun 5, 2023 • 7 min read

So, you need or want a Pentest….

So, that day has finally come when you've been tasked with obtaining a penetration test for that project you've built or are accountable for, or perhaps you've been informed that it's necessary due to "compliance requirements".

If you're completely unfamiliar with penetration testing or have limited experience, this can quickly be an unfamiliar or even daunting process!

You are probably thinking:

- Where do I start?
- What type of test/testing do I require?
- What does the testing need to achieve?
- What's the deliverable I need to meet?

Hopefully, this blog post will answer any questions you may have or at least helps lighten the load with all the moving parts you will encounter or have to deal with pre and post-engagement by the end of this post; you should better understand what penetration testing is, the differences in the types of approaches and how each has various pros and cons.

With that in mind, let's dive in!

First off, what is Penetration Testing?

'Penetration testing' is probably one of the most misused/misunderstood Cyber Security terms and concepts currently being discussed. People use it interchangeably, within the same conversation, regularly.

The UK National Cyber Security Centre (NCSC) describe Penetration Testing, as in the actual 'doing' aspect of things, as the following:

> A method for gaining assurance in the security of an IT system/environment, by attempting to breach some or all of that system's/environment's security, using the same tools and techniques as an adversary might.

They go on to further state that:

> A penetration test should be thought of as similar to a financial audit. Your finance team tracks expenditure and income day to day. An audit by an external group ensures that your internal team's processes are sufficient.

In my opinion, this is one of the best definitions and explanations I've come across. I would also like to mention that it is beneficial to consider the term 'Penetration Testing' as an umbrella term. Expanding on this idea, it encompasses various types of security assessments that fall within its scope.

There can be a lack of comprehension regarding the differences between a Vulnerability Assessment and an offensive security assessment, such as "Closed-Box," "Insider Threat," and "Red Team" assessments.

Unfortunately, these assessments are frequently lumped together under the umbrella term "penetration testing,". While there may be shared components among the various types of penetration assessments, such as a defined methodology or specific actions, it is crucial to recognize that each assessment type is distinct and should be considered within its unique context.

A key take-way at this point here is:

Vulnerability scanning ≠ Penetration Testing

To be clear, the above says that a vulnerability scan does not equal a penetration testing engagement.

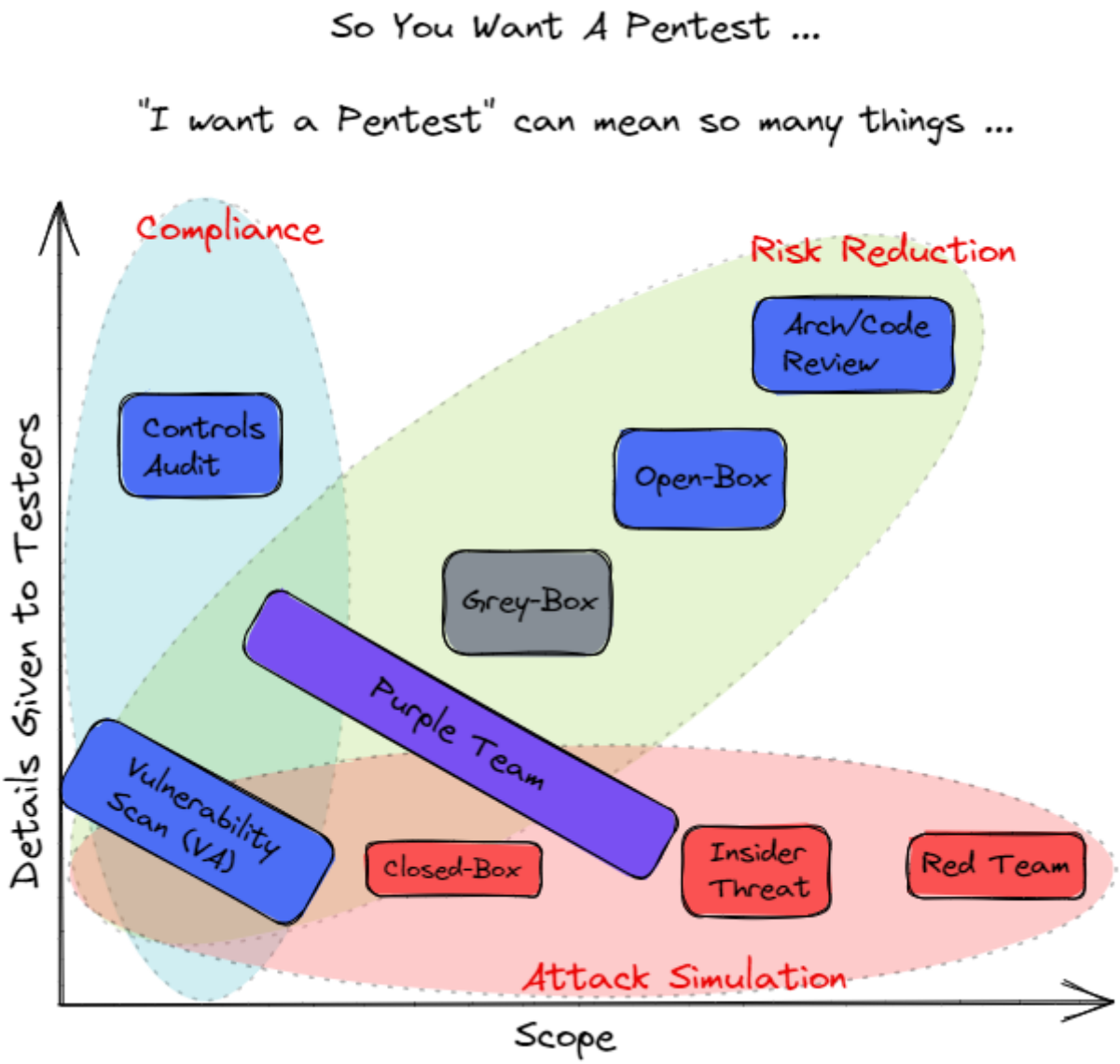
Deciding what type of Penetration Testing you may need?

So, if you've read this far, you're likely trying to familiarise yourself with a 'Penetration Test' and the types of assessments you might need. With this in mind, here are a few things *(in general)* to note before you go any further.

1. Identify the reason driving the need/requirement for penetration testing. Is it:
    - **Compliance/Regulatory based.**
    - **Risk Reduction.**
    - **Attack Simulation.**
2. Identify high-value/business critical assets.
3. Identify and understand the various controls and/or capabilities related to the points above.
4. Identify a set of realistic expectations for the test, based on time and budget available.

Working through the points above will result in the 'why' and the 'what'; the how will be discussed in the penetration testing scoping process.

Visuals are the best way to convey a point, so with that in mind, we have prepared this:



At its core, Penetration Testing is testing to find as many vulnerabilities and configuration issues as possible in the time allotted and exploiting those vulnerabilities to determine the risk/severity of the vulnerability.

This does not necessarily mean uncovering new vulnerabilities (zero days); it's more often looking for known, unpatched vulnerabilities. Like Vulnerability Assessments, Penetration Testing is designed to find and assess any identified vulnerabilities to ensure they are not false positives. Penetration Testing goes further as the tester attempts to exploit the given vulnerability.

Exploitation can happen in numerous ways, and once a vulnerability is exploited, a good tester will not stop *(unless specifically called out in the scope of work or rules of engagement)*. They will continue to find and exploit other vulnerabilities, chaining attacks together to reach the client's goals.

Each organisation is different; as such, these goals will inevitably change but usually includes access to Personally Identifiable Information (PII), Protected Health Information (PHI), and proprietary business secrets.

Vulnerability Assessment

Vulnerability assessment intends to identify vulnerabilities within a network, web application and/or service. A vulnerability assessment involves automated network security scanning tools, whose results are the output to or listed in a report.

It is important to note that findings reflected in a vulnerability assessment report generally are not backed by an attempt to exploit them; some of them may be false positives and, as such, do not provide any indication to a business/organisation on how susceptible they are to these findings, therefore potentially impacting upon any plan prioritised remediation planning.

Open, Grey and Closed-Box Penetration Testing

These are probably the three most conducted penetration testing types a business/organisation opts for. Here's a quick breakdown of each type:

Closed-Box:

- This type of penetration test requires no previous information and usually takes the approach of an uninformed attacker. As such, the penetration tester has no previous information about the target system and will step through the same 'discovery' phase known as open-source intelligence gathering (OSINT).
- **Benefit:** It simulates a more realistic attack scenario
- **Disadvantages**: Testing time cannot be maximised in certain scenarios, along with some areas of the infrastructure/environment might remain untested

Grey-Box:

- This type of penetration test represents either:
    - Someone with partial knowledge of an environment.
    - Someone who may have low level user credentials.
    - An external party who may have located information that has been misplaced. As such this could inadvertently be used by a threat actor.
- **Benefits:** Helps understand the risk from a low-level user's perspective, as well as helps to identify weaknesses around privilege escalation
- **Disadvantages:** Testing time cannot be maximised in certain scenarios, along with some areas of the infrastructure/environment might remain untested.

Open-Box:

- This type of penetration test relies on the knowledge, provided in advance by the client, relating to their digital footprint, internals of the target environment, to accurately define test cases and attack vectors.

- **Benefits:**
  - Comprehensive testing.
  - Maximises testing time.
  - Extends the testing area where closed-box testing cannot reach, such as quality of code, application design, architecture review etc.
- **Disadvantages:**
  - It does not reflect any external threat type or threat actor.
  - Security policies, controls and procedures may have to be relaxed to facilitate access and testing.

Purple Team Assessments

Purple Team assessments have continued to grow in popularity and demand due to how these assessments approach an organisation's security posture and needs. Mature or well-funded organisations may well have taken time and effort to build out both a defensive (Blue) team and an offensive (red) team to approach their security needs proactively; however, more often than not, one of two main things happen:

1. Each team works ‘siloed’ from each other, resulting in a lack of communication, co-operation and communication.
2. An organisation only can build out one team and naturally they opt for a defensive (blue team).

Irrespective of the above points, a purple team engagement can be extremely beneficial to an organization, as the purple team can “bridge the gap” between these two teams, consequently establishing lines of communication and/or facilitating the emulation of a threat actor and attack simulation.

Either way, by leveraging the existing skills and talents that blue and red teams bring to the table and using them to identify strengths and weaknesses across the organization’s security controls, a purple team engagement can accurately measure those controls and the maturity of the organization’s progress.

Offensive Security/Scenario-Based Assessments

Offensive Security/Scenario based assessments are a specific subset of penetration testing. These are commonly referred to as ‘Red Team’ Assessments and are similar to penetration testing in many ways; however, these engagements are more targeted.

The goal of the assessment is **NOT** to find as many vulnerabilities as possible. The goal is to test the organisation's detection and response capabilities by achieving a specific goal, for example, achieving a specific goal and verifying if access to financial data or client data can be achieved from the perspective of a standard user.

The ‘red team’ will try to get in and access sensitive information in any way possible and as quietly as possible. These types of assessments look to emulate a malicious actor with targeted attacks whilst looking to avoid detection. In short, the team will seek to emulate

and employ tactics, techniques, and procedures similar to an Advanced Persistent Threat (APT) group.

An APT group can target any individual or organisation; however, recently, certain APTs have targeted specific types of businesses, such as Healthcare, Financial/Insurance, Private Defence contractors and Government entities. With this in mind, it is important to understand your company/organisation's postulated threat; doing so will allow any assessment to be specific to your needs and provide an overall better experience and usable set of results.

Assessments such as these are also normally longer in duration than Penetration Tests. A Penetration Test often takes place over a 1–2-week period, though it can run longer depending on what's in scope/the size of the test team. In contrast, an Offensive Assessment could be over a much longer time frame and will most certainly consist of multiple people and skill sets.

Such assessments do not look for multiple vulnerabilities but for those vulnerabilities that will achieve the engagement-defined goals. Methods used during more Offensive Assessments, such as Red Teaming, include Social Engineering (Physical and Electronic), Wireless, External infrastructure and many more.

An Offensive Assessment is NOT for everyone, though and should be performed by organisations with mature security programs. These organisations generally have various cyber programmes focused on vulnerability management, penetration testing, threat modelling and asset management.

Lets recap...

In summary, we've discussed what the term penetration testing can mean, the considerations that need to be taken to identify the right type of penetration testing engagement(s) for your organisation and, at a high level, provided some insight into the key types of penetration testing engagements that occur, along with various "Pros" and "Cons".

If you are ever in doubt or unsure what you need, seeking assistance from a dedicated organisation, which provides such services regularly, is the first step to maturing your security posture, awareness and understanding of penetration testing.

Over time you will become more informed and able to take more ownership of this process.

From here, the next steps involved, now that you've identified what you need, you need to identify the scope of the engagement, whatever it may be! This will be covered in part 2 of the 'Pentesting 101'.

How can we help?

Here at Lares, we help empower organizations to maximize their security Potential.

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching.

If you would like any further information, you can get in touch here or head over to the Lares.com website for more information about how we can help.