002.1 Pentesting methodologies

What is it?

When you've been testing for a while, you'll start to see patterns emerge. Some testers have better quality standards than others and some will have totally different ways of testing. To make this more uniform and deliver a better end product for our customers, we can rely on a standardized methodology. A unified way of testing but how do we define that with so many different technologies and requirements out there? That is where methodologies come into play, they are a set of unified guidelines that can help you perform your pentests better and give the client a better level of coverage.

Why use a methodology

Of course, everyone can hack but the complete process (including documentation) can get quite complex. We want to make sure to always deliver the same quality but we can only do that if we always follow roughly the same guidelines for every type of test. You might find it funny that only 5 big methodologies exist at the moment, given the number of different types of pentesting we can do but these methodologies go very deep and cover every aspect of the pentest. Some are more specialized than others and aim at more of a niche market while others are more general.

Picking the right one

With these options on the table, how do we pick the correct one? First, we have to go over what they are all for and what they cover so let’s dive in.

Which methodologies exist?

OSSTMM

Open Source Security Testing Methodology Manual, Phew, that is a mouthful! In their own words,

> This is a methodology to test the operational security of physical locations, human interactions, and all
> forms of communications such as wireless, wired, analog, and digital.

So, given this information we can easily deduct this type of pentest is useless when it comes to a web application for example. The focus of this methodology is to isolate the threats from the assets. They share one big belief that some might oppose heavily: “Given their guidelines, assets can be secured 100%”. We’ll dive deeper into why they believe that in its’ own separate chapter.

OWASP WSTG, MSTG

OWASP is an organization of volunteers that does more than just set up top 10’s every few years. They will forever hold my respect for creating so many guides in regards to pentesting, securing your applications, and much more. The WSTG or web security testing guide is one of them and it is a complete methodology that talks about documentation, execution, and reporting. The Mobile security testing guide is its cousin that focuses on testing mobile applications and their API calls.

NIST

NIST SP 800-115 is a name you will often hear in our fields, in their own words:

> The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

As you might have guessed, this is a methodology that revolves all around standards and you may find that it digs deep into organizational level pentesting. They focus heavily on covering a broad scope and include everything from physical to network to application pentesting. This methodology will allow you to asses an organisation and give them a report with good visibility into their security maturity.

PTES

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

ISSAF

The Information System Security Assessment Framework (ISSAF) is a peer reviewed structured framework that categorizes information system security assessment into various
domains & details specific evaluation or testing criteria for each of these domains. It aims to
provide field inputs on security assessment that reflect real life scenarios. ISSAF should primarily be used to fulfill an organization’s security assessment requirements and may additionally be used as a reference for meeting other information security needs. ISSAF includes the crucial facet of security processes and, their assessment and hardening to

get a
complete picture of the vulnerabilities that might exists.