🏹

# 001. Defining what a pentest is

## What is a pen test?

Are we testing fountain pens? ball pens? This joke is as old as pen testing itself yet it remains funny. Of course, pen testing is a collection of actions with a specific goal in mind but what that goal is can differ from test to test and the actions as well. Generally, we know 5 phases in a pentest which we will touch on later. First, we will describe what a pen test is and try to define a set of deliverables that will help us both explain and prove our work to our clients. I want you to remember the word client very well! This is going to be your number 1 priority throughout your complete test. Let’s dive into the meaning first.

### So much more than just finding an issue

The whole goal of a pen test is so much more than just finding issues, we have to guide our clients, and provide them with adequate support and a level of coverage that will help them better understand their security situations. It all starts with the fact that our clients are often not experts in cybersecurity, they might have a general idea of the flow but they will not generally know the best course of action, that is where you come in. You are to guide your client in first determining a goal that is SMART (**Specific, Measurable, Attainable, Relevant, and Timely**). With this goal in mind, we can determine what actions are required to achieve their desired level of coverage and you can give them an estimation of your work that is either based on the job in total or on the number of hours you put in. This is all easier said than done because how do you determine that coverage and what is a good way of working? Thankfully we do not have to reinvent the wheel here and can turn to existing methodologies in some cases to at least give us a solid basis on which we can lean to determine our strategy.

### In scope/Out of scope

Whatever methodology you pick, you will always be bound to a certain scope. It is important to inform yourself about this scope. **YOU NEED TO COMMUNICATE. I can not stress this enough!** If you are unsure about anything regarding the scope or anything else, you have to ask. To assume is to make an ass out of u and me. Be patient and don't start randomly attacking websites, make sure your tools are also set to properly take this scope in mind. When we come to specific tools, we will talk more about this but for now, it is important to know that the scope needs to be clearly defined and approved by both parties.

## Being ethical

At first sight, it might seem easy to be ethical but the word itself is loaded with pretends. In my opinion, we all draw the border of morality to where we would go ourselves. For example, we might think it ethical to keep data secret but is it really ethical if the data you are keeping secret is harming other people?

You have to do your due diligence and not be afraid to cut off toxic clients but that being said, you do have to put your client first generally speaking though. You have to protect them from unethical actors and from company espionage. You will have signed an NDA by now with your client (we will get back to this later) and you are to hold to this.

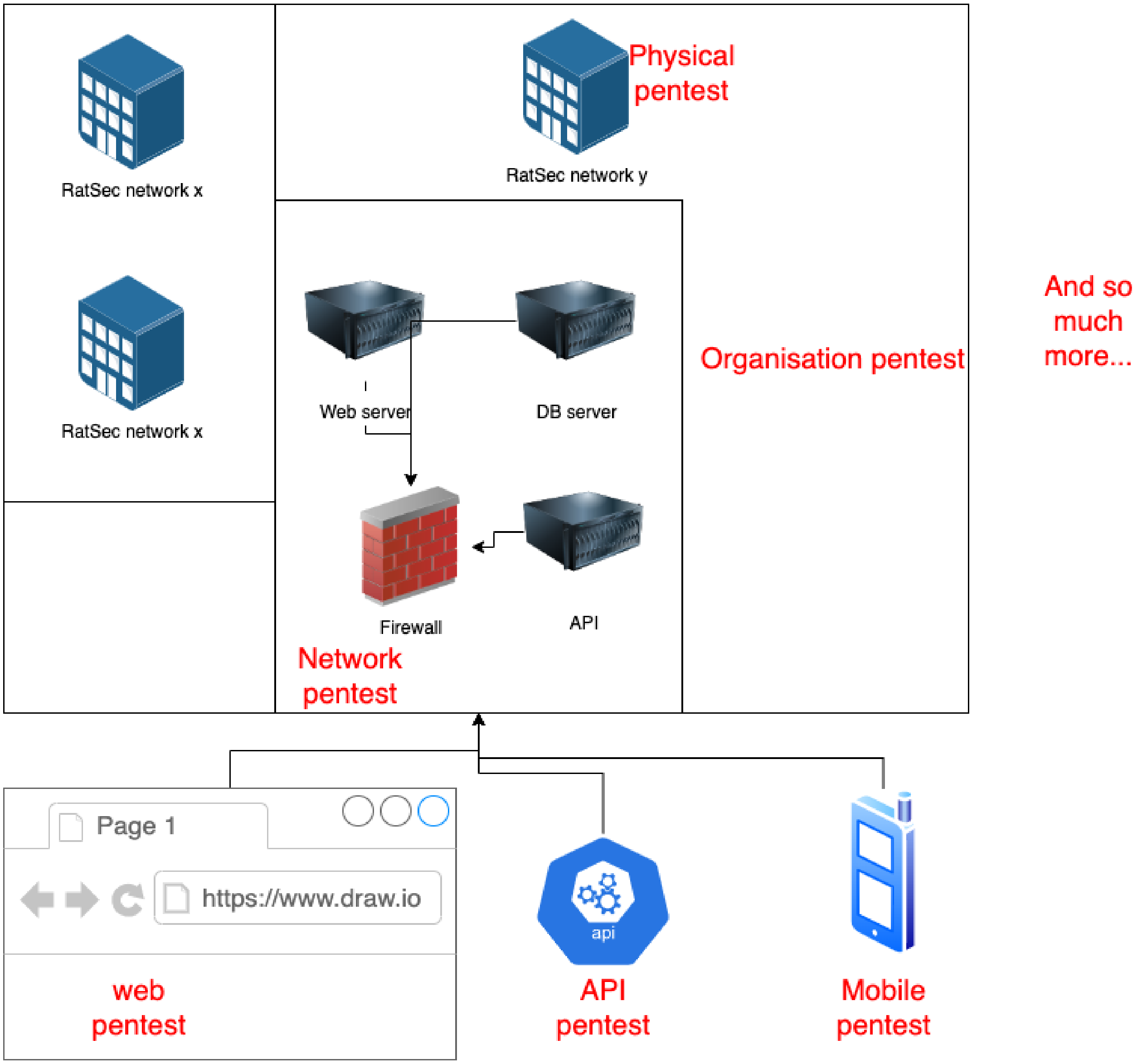
# The types of a pen test

In general, we have a vast amount of different types of pen test. I'll give you a bit of a summary but know that there are even more than what I have noted here:

- Network pentest
- Organization pentest
- Web pentest
- Mobile pentest
- API pen-testing
- Cloud-hybrid infrastructure testing
- Iot pentest
- Web 3.0 pentest

- Metaverse pentest
- Social engineering
- Automotive pentest
- Physical pentest

Let’s zoom in on some of these and describe them in a bit more detail. Again, please note that this list is by no means comprehensive and is changing all the time with new technologies coming out.



## Network pentest

Network-related pen tests are often relying heavily on tools. You want to enumerate as much as possible and it usually starts with a port scan. This can be done either internally or externally and extensive networking knowledge. The goal is often to exploit logic, exploit misconfigurations or weaknesses in the architecture or deny access to the infrastructure through a DoS attack for example.

The same test can happen on an organisational level which will usually span multiple networks or one larger network but the goals and methods stay relatively similar.

## Web pentest

Between network pen tests and web pen tests, these are the most requested types at the time of writing (April 2022) but we can slowly observe a shift towards mobile as well. While also relying on tools, this type of pen test also relies on the knowledge of the tester. It has been proven time and time again that automated scanners will only find a fraction of the exploits. I do think they are a requirement though. I compare it to hacking with a companion that is very diligent but not very effective. The goal is to get a reverse shell to get on the server, find a web exploit such as XSS, get access to files on the system or deny access to the infrastructure with a DoS attack for example. Tools often include MiTM proxies such as burp suite or OWASP ZAP and vulnerability scanners.

## API pentest

This type is marked by the usage of tools such as postman and ReadyAPI. We can also write our own code in python for example for interaction with an API. It has its own top 10 vulnerability types drafted by OWASP and there is no set methodology for this. It often relies heavily on documentation, technical knowledge of the tester, and discovery of attack surface. We want to try and exploit logic, find weaknesses and unexplored attack surfaces, or deny access through a DoS attack again for example.

# The deliverables of a pentest

When we perform a pentest, we need to have proof of our work and we need to be able to brief our clients in a way they can understand through documentation. This is verifiable later on and will rule out any possible discussions. The deliverables that are involved can differ slightly as not all are always required but the following **are** always required in my opinion:

- NDA
- Test plan
- Test report
- Debriefing
- Sign-off slip

We also have a few deliverables that are optional:

- Automation Assets such as scripts
- Notices of engagement
- Man-in-The-Middle proxy (such as OWASP ZAP) save files
- Other test assets such as test cases

An NDA is something we already briefly touched on. The test plan is an asset we will make a separate article on as it deserves a lot of attention and of course an example as well.

As for the test report, we have to make sure to include the following items:

- Vulnerabilities found
- Steps to reproduce
- Actual result
- Expected result
- Summary
- CVSS score

A nice summary is also required and usually, statistics about the vulnerabilities and coverage are also included. After writing your report, you need to deliver it to the client and debrief them. This can be a short audio/video recording or even just a summary on mail. They need a quick status update on the security of their assets under test. I include a sign-off slip that basically says the following:

“The agreed-upon work in the contract and described in the test plan has been delivered in a timely manner by the testing party and to a level that is approved by the client”. I sign it myself and let the client sign it. This again helps us in ruling out any discussions that might arise at a later date and will soft-force the client to take the report seriously and investigate if it is according to their standards. Any extra work after this point will probably be billed.

# Checklists

We have much more to talk about like the importance of checklists but I have already stolen enough of your time for now. Subscribe for part 2.

To be continued...