Occam's Razor

Thinking outside the box helps us cross imaginary boundaries and thus to access possibilities and options that were not recognizable to us at first. Thereby, we will encounter many options, and the whole way to the solution of a problem can become very complicated very fast. The Occam's Razor principle is beneficial for simplifying these circumstances.

Occam's Razor is one of the central principles of modern scientific theory. The principle is based on the following definition:

- `The most straightforward theory is preferable to all others of several sufficient possible explanations for the same state of facts. In other words: The simplest explanation is always the most probable.`

For example, we can assume that our computer has stopped working. There could be many reasons for this, as we can already imagine. It can be because the power supply is faulty, CPU issues, or maybe even the motherboard is fried.

With such or similar problems, we automatically start to list the possibilities of what could be the reason before we start to solve the problem. Many people work by the process of elimination. They eliminate the probable possibilities that could be responsible for the problem. This approach already leads us in the wrong direction and results in considerable effort to solve the problem. With this type of approach, most people would start by taking their computers apart and checking all of the connections. They are looking for the most likely cause but ignoring the simplicity factor.

After all, the question we should be asking is:

- `Why is our computer not getting power?`

When we ask this question, we automatically form associations in our minds that have to do with the word "power ."In this approach, the first thought is usually focused on the power supply. The power supply regulates the power for a computer. Therefore, most people's first thought is that the power supply has a defect and is no longer functional.

Nevertheless, let us not forget to think outside the box when we think of "power ."Because if we set ourselves the limits that it can only be our computer, we limit our options considerably. If we leave these limits, the first point of contact from the computer is the connected socket and the multiple plugs. If we followed this approach, we would see that our multi-plug had been switched off; therefore, the computer had no power to start up.

So, in this case, the most straightforward explanation was also the most probable.

Occam's Razor in Practice

Using Occam's Razor in practice sounds easier than it is in practice. We can state that the simplest explanation is the most probable. However, the fact is that apart from that, it is not always so. We must also distinguish between the individual details and mechanisms and the general picture or concept. In our learning phase (and thus also during our penetration tests against companies), we will encounter many situations in which we learn something new. However, it is crucial to understand the overall concept rather than the individual steps involved. For example, once we are familiar with SQL injection and how it occurs, we may find the individual steps difficult at first. However, once we understand the overall concept, it will be easy for us to discover when a web application is vulnerable to SQL injections.

If we have already dealt with SQL injections and know how they can look, we also understand that the individual steps to detect and exploit them can be very complicated. Nevertheless, what remains the same is the concept. The concept is the main focus when learning new topics.

Another example is the approach to penetration testing, which is very common throughout the cybersecurity community. Everyone discusses the cases that can occur and how best to approach them. Let us think back to Occam's Razor principle and think outside the box.

Anyone who has done at least two or three penetration tests will find that each one is unique. Even if the same systems are used for the clients and servers, their configuration is typically unique. The unique aspects are the stages in a penetration test, which we can learn more about in the Penetration Testing Process module.

```
The simplest explanation for the best approach to penetration testing is that we work with the information we can get.
```

The unique techniques of how we get and use this information are, again, individual steps followed and not the whole concept. The same applies to most exploitation attacks and the individual steps for them. Once we understand the overall picture, adapting to the given situations and conditions is much easier. However, suppose we have only learned the individual steps. In that case, we will have difficulty adapting them to new situations because we do not understand their impact on the systems and their applications.

Later in the process, we will see this phenomenon again and again. Once we have identified the solution to the problem, the process and the steps required to achieve it seem pretty straightforward in most cases. Looking back, it always seems easy once we know the solution. The art, after all, is not to get some flag but to find the way to it.

← Previous Next → Mark Complete & Next

Table of Contents

Learning Progress

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left