Enumeration with *nmap*

Enumeration is the most critical part of all. The art, the difficulty, and the goal are not to gain access to our target computer. Instead, it is identifying all of the ways we could attack a target we must find.

It's not hard to get access to the target system once we know how to do it. Most of the ways we can get access we can narrow down to the following two points:

- Functions and/or resources that allow us to interact with the target and/or provide additional information.
- Information that provides us with even more important information to access our target.

When scanning and inspecting, we look exactly for these two possibilities. Most of the information we get comes from misconfigurations or neglect of security for the respective services. Misconfigurations are either the result of ignorance or a wrong security mindset. For example, if the administrator only relies on the firewall, Group Policy Objects (GPOs), and continuous updates, it is often not enough to secure the network.

Enumeration is the key.

That's what most people say, and they are right. However, it is too often misunderstood. Most people understand that they haven't tried all the tools to get the information they need. Most of the time, however, it's not the tools we haven't tried, but rather the fact that we don't know how to interact with the service and what's relevant.

That's precisely the reason why so many people stay stuck in one spot and don't get ahead. Had these people invested a couple of hours learning more about the service, how it works, and what it is meant for, they would save a few hours or even days from reaching their goal and get access to the system.

Manual enumeration is a critical component. Many scanning tools simplify and accelerate the process. However, these cannot always bypass the security measures of the services. The easiest way to illustrate this is to use the following example:

Most scanning tools have a timeout set until they receive a response from the service. If this tool does not respond within a specific time, this service/port will be marked as closed, filtered, or unknown. In the last two cases, we will still be able to work with it. However, if a port is marked as closed and Nmap doesn't show it to us, we will be in a bad situation. This service/port may provide us with the opportunity to find a way to access the system. Therefore, this result can take much unnecessary time until we find it.