Enumeration Principles

Enumeration is a widely used term in cyber security. It stands for information gathering using active (scans) and passive (use of third-party providers) methods. It is important to note that OSINT is an independent procedure and should be performed separately from enumeration because `OSINT is based exclusively on passive information gathering` and does not involve active enumeration of the given target. Enumeration is a loop in which we repeatedly gather information based on what data we have or have already discovered.

Information can be gathered from domains, IP addresses, accessible services, and many other sources.

Once we have identified targets in our client's infrastructure, we need to examine the individual services and protocols. In most cases, these are services that enable communication between customers, the infrastructure, the administration, and the employees.

If we imagine that we have been hired to investigate the IT security of a company, we will start to develop a general understanding of the company's functionality. For example, we need to understand how the company is structured, what services and third-party vendors it uses, what security measures may be in place, and more. This is where this stage can be a bit misunderstood because most people focus on the obvious and try to force their way into the company's systems instead of understanding how the infrastructure is set up and what technical aspects and services are necessary to be able to offer a specific service.

An example of such a wrong approach could be that after finding authentication services like SSH, RDP, WinRM, and the like, we try to brute-force with common/weak passwords and usernames. Unfortunately, brute-forcing is a noisy method and can easily lead to blacklisting, making further testing impossible. Primarily, this can happen if we do not know about the company's defensive security measures and its infrastructure. Some may smile at this approach, but experience has shown that far too many testers take this type of approach.

`Our goal is not to get at the systems but to find all the ways to get there.`

We can think of this as an analogy of a treasure hunter preparing for his expedition. He would not just grab a shovel and start digging in some random spot, but he would plan and gather his gear and study maps and learn about the terrain he has to cover and where the treasure may be so he can bring the proper tools. If he goes around digging holes everywhere, he will cause damage, waste time and energy, and likely never achieve his goal. The same can be said for understanding a company's internal and external infrastructure, mapping it out, and carefully formulating our plan of attack.

The enumeration principles are based on some questions that will facilitate all our investigations in any conceivable situation. In most cases, the main focus of many penetration testers is on what they can see and not on what they cannot see. However, even what we cannot see is relevant to us and may well be of great importance. The difference here is that we start to see the components and aspects that are not visible at first glance with our experience.

- What can we see?
- What reasons can we have for seeing it?
- What image does what we see create for us?
- What do we gain from it?
- How can we use it?
- What can we not see?
- What reasons can there be that we do not see?
- What image results for us from what we do not see?

An important aspect that must not be confused here is that there are always exceptions to the rules. The principles, however, do not change. Another advantage of these principles is that we can see from the practical tasks that we do not lack penetration testing abilities but technical understanding when we suddenly do not know how to proceed because our core task is not to exploit the machines but to find how they can be exploited.

No.	Principle
1.	There is more than meets the eye. Consider all points of view.
2.	Distinguish between what we see and what we do not see.
3.	There are always ways to gain more information. Understand the target.

To familiarize ourselves with these principles, we should write down these questions and principles where we can always see them and refer back to them with ease.

Next ➜ Mark Complete & Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left