Vulnerability Assessments

There are mainly 4 types of vulnerability assessments that we perform usually.

- **External Scans** - If a client tasks us with an external vulnerability scan, they mean to analyze one or more systems that are accessible from the internet. Targets in an external vulnerability scan are often web applications, systems in the demilitarized zone (DMZ), and public-facing services.

- **Internal Scans** - Internal vulnerability scan where we have direct access to either a part of or the complete internal network of a client. When a client tasks us with this kind of vulnerability scan, we either get VPN access or we perform the scan on-site. The intention is to get an overview of the security status of the internal network. It is important to analyze which vectors an attacker can use after breaching the perimeter.

- **Unauthenticated Scans** - When we perform a vulnerability scan on a system without providing credentials, it is called an unauthenticated vulnerability scan. Unauthenticated scans are made to find vulnerabilities in remotely accessible services on a target. Therefore, they map the system with all open ports and provide us with an attack surface by matching the information to vulnerability databases as mentioned before.

- **Authenticated Scans** - Most scanners can be configured to run authenticated scans, in which the scanner logs in to the target with a set of valid credentials. In most instances, authenticated scans use a privileged user account to have the best visibility into the target system. The goal of authenticated vulnerability scans is to check for vulnerable packages, missing patches, or configuration vulnerabilities.
