Staged VS Non-staged payload

Before going further with the Staged and Non-staged payload. Lets understand the term **"payload"** first.

In the context of exploitation, a payload refers to the malicious code or data that is delivered to a target system to achieve a specific goal, such as gaining remote access, stealing sensitive data, or disrupting operations. Payloads can be delivered through various means, including exploits, phishing attacks, or social engineering tactics.

Staged Payloads

Staged payloads are a type of payload that is delivered in multiple stages. The initial stage, often referred to as the **"stager"** or **"dropper"** is a small, lightweight payload that is designed to establish a connection with the attacker's system. Once the stager is executed, it downloads and executes the second stage, which is the main payload. This approach allows for more flexibility and stealth, as the initial stage can be designed to evade detection by security software.

Non-Staged Payloads

Non-staged payloads, on the other hand, are self-contained and do not require multiple stages to deliver the payload. These payloads are often larger and more complex, containing all the necessary code to achieve the desired objective. Non-staged payloads can be more straightforward to deliver, but they may be more detectable by security software due to their larger size and complexity.

Suppose, we send an phishing email to our target. Once the target clicks on our payload. If it is a staged one, then the dropper will first execute on its machine and then pull the main payload from our attacking server and after the main payload is executed we will receive a reverse shell back. But on the other hand, in stageless payloads, once the victim clicks on the payload, we will receive the connection instantly.

Now at this point, you might be thinking then we have to use the stageless payload as it gives us result instantly. But that's not the case everytime. To understand this, lets see the difference between both of them.

Key Differences

- **Size and Complexity**: Staged payloads are typically smaller and more lightweight, while non-staged payloads are larger and more complex.
- **Delivery Mechanism**: Staged payloads are delivered in multiple stages, while non-staged payloads are delivered in a single stage.
- **Stealth and Evasion**: Staged payloads are often designed to evade detection by security software, while non-staged payloads may be more detectable due to their larger size and complexity.
- **Flexibility and Customization**: Staged payloads offer more flexibility and customization options, as the initial stage can be designed to adapt to different environments and scenarios.
