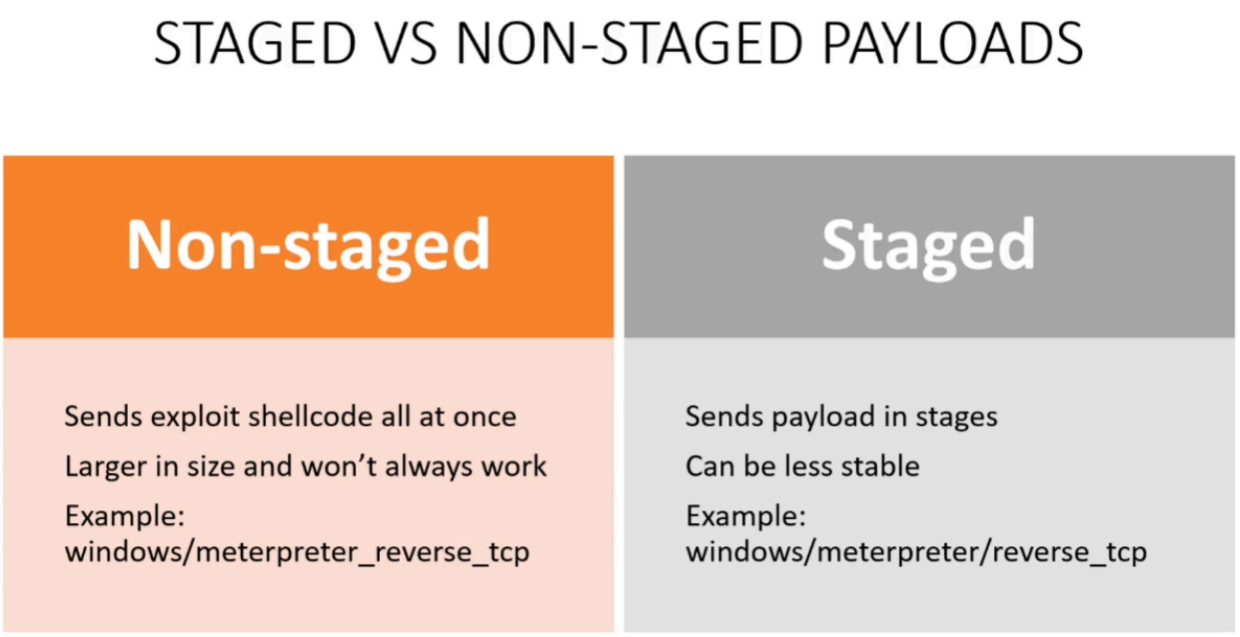
Staged vs. Non-Staged Payloads

The first thing we need to understand before understanding the difference between the two different payload types, is to understand what is a payload.

What is a payload?

A payload is what we are going to run as an exploit. We use different types of payloads, depending on what the target is. We send these payloads to the victim, and attempt to get a shell on the machine.

There are two types of payloads:



Pay attention to the example above. In Metasploit, the difference between a Non-Staged payload, and a Staged one is the " / " symbol, which is called " forward slash".

The Staged one contains the forward slash.

Take away here is, if we are using a payload that does not work, maybe try the non-staged version or vice-versa. Then, if the exploit should be correct, then we can try a bind shell instead of a reverse shell, or vice-versa.