

Understanding Payloads in Metasploit

What Does Payload Mean?

A payload in Metasploit refers to an exploit module. There are three different types of payload modules in the Metasploit Framework: **Singles**, **Stagers**, and **Stages**. These different types allow for a great deal of versatility and can be useful across numerous types of scenarios. Whether or not a payload is staged, is represented by '/' in the payload name. For example, *windows/shell_bind_tcp* is a single payload with no stage, whereas *windows/shell/bind_tcp* consists of a stager (bind_tcp) and a stage (shell).

Contents

- [1 Singles](#)
- [2 Stagers](#)
- [3 Stages](#)

Singles

Singles are payloads that are self-contained and completely standalone. A Single payload can be something as simple as adding a user to the target system or running calc.exe.

These kinds of payloads are self-contained, so they can be caught with non-metasploit handlers such as netcat.

Stagers

Stagers setup a network connection between the attacker and victim and are designed to be small and reliable. It is difficult to always do both of these well so the result is multiple similar stagers. Metasploit will use the best one when it can and fall back to a less-preferred one when necessary.

Windows NX vs NO-NX Stagers

- Reliability issue for NX CPUs and DEP
- NX stagers are bigger (VirtualAlloc)
- Default is now NX + Win7 compatible

Stages

Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits such as [Meterpreter](#), VNC Injection, and the iPhone 'ipwn' Shell.

Payload stages automatically use 'middle stagers'

- A single recv() fails with large payloads
- The stager receives the middle stager
- The middle stager then performs a full download
- Also better for RWX