Staged vs Non-Staged Payloads

Day 21/365

Payloads

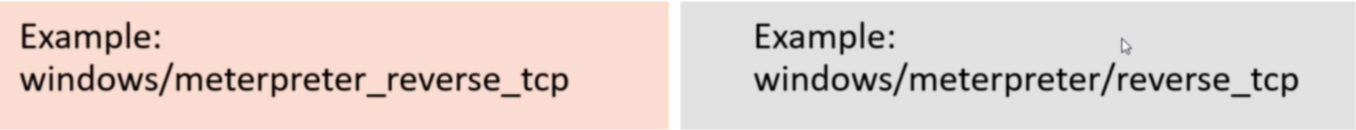
A payload is what we are going to run as an exploit

- Windows type payload
- Linux type payload
- Meterpeter payload

We send a payload to attempt to get a shell on the victim's machine

2 main types of payloads

- Non-staged
  - Sends exploit shellcode all at once
  - Larger in size and won't always work
- Staged
  - Sends payload in staged
  - Can be less stable



Example:
windows/meterpreter_reverse_tcp

Example:
windows/meterpreter/reverse_tcp

Non staged and Staged

the / lets us know that i's a staged payload

If a payload does not work, try the other type (assuming it's the right exploit)
