THE BRIDGE

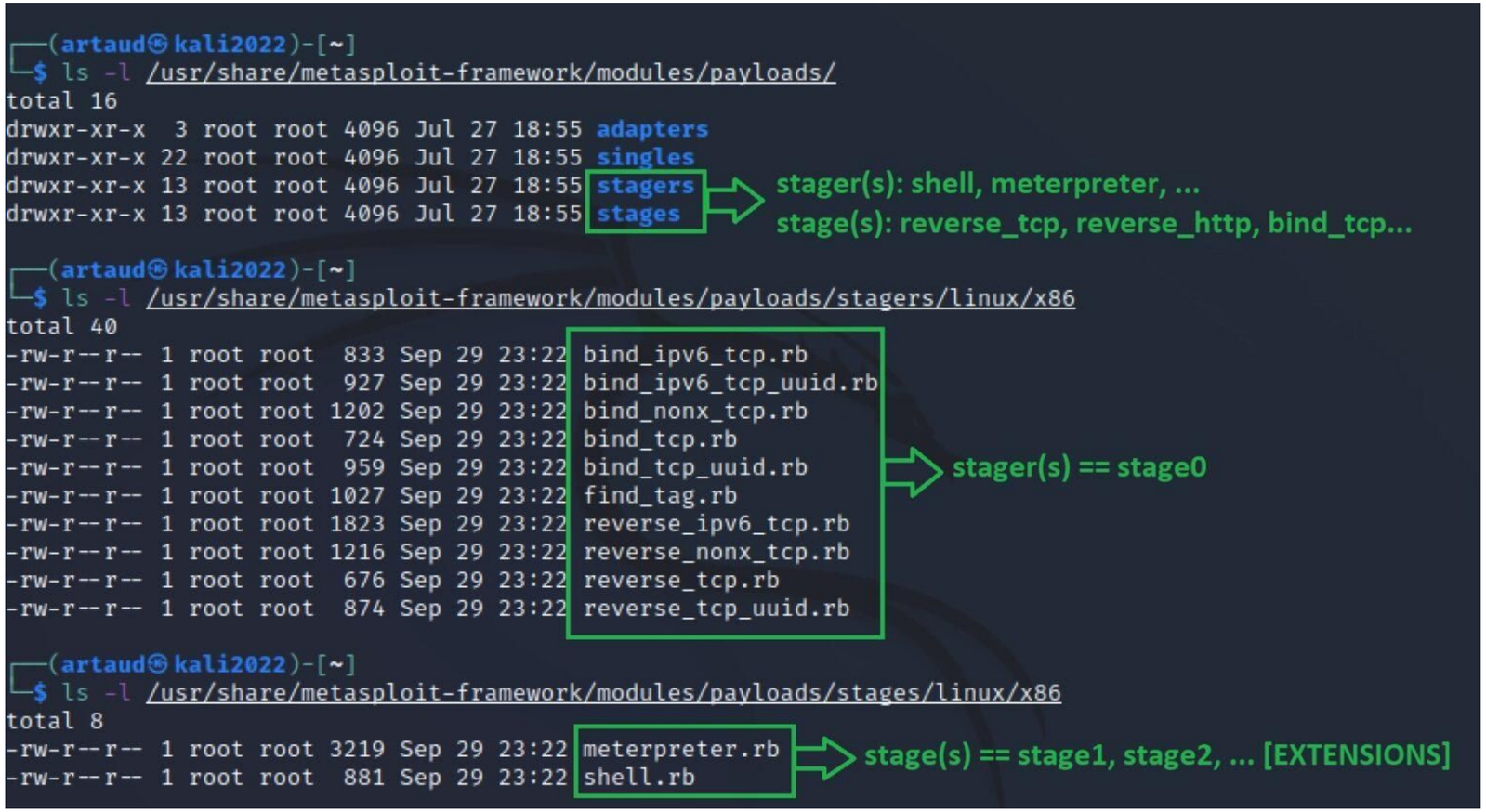
CYBER SECURITY

Metasploit II
Payloads y Sessions

¿Qué veremos?

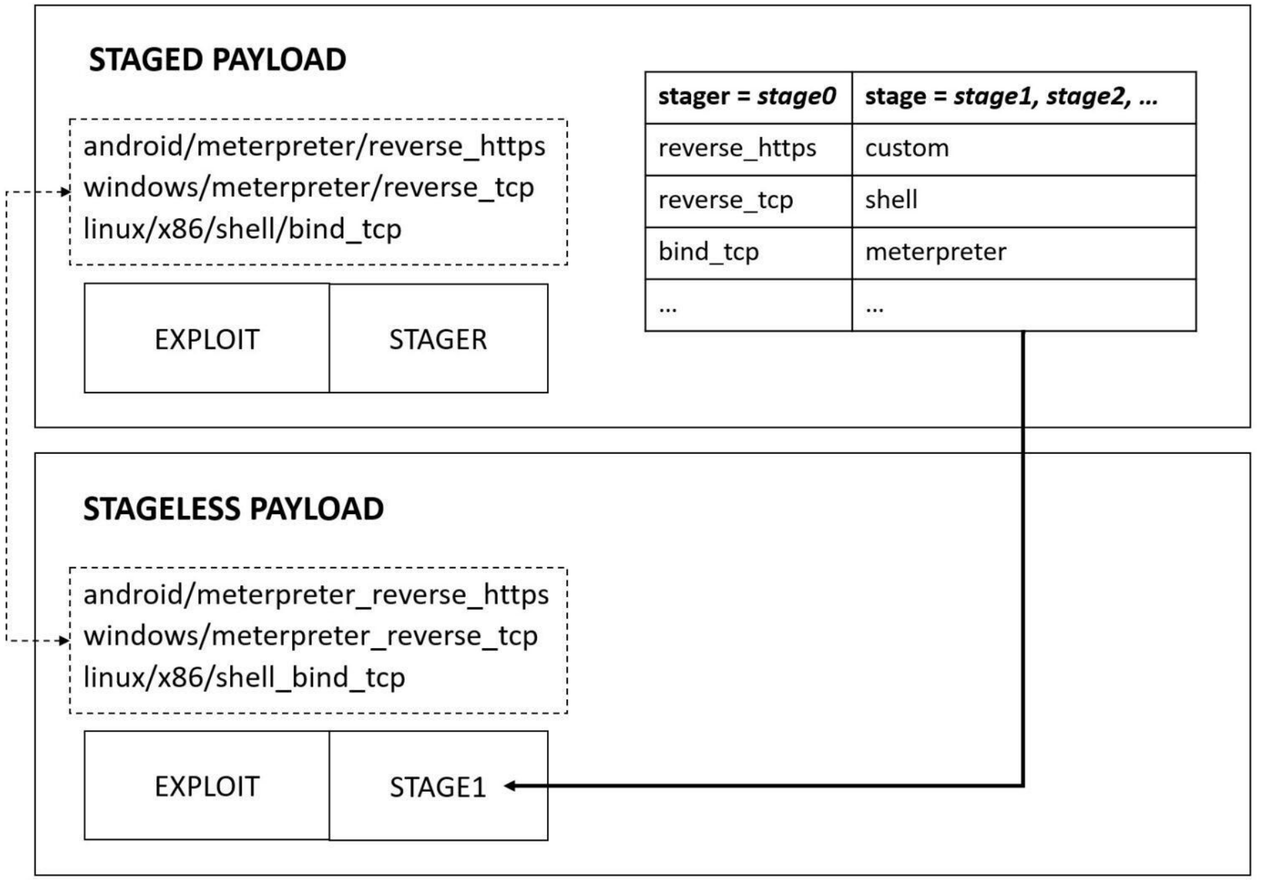
- Metasploit framework:
  - Payloads
  - Sessions

Payloads



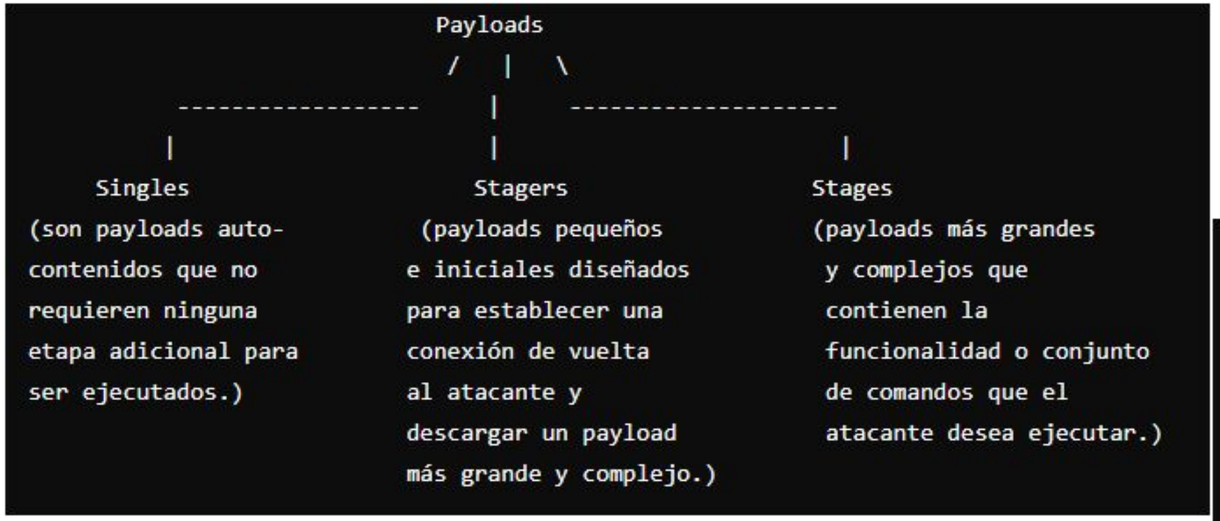
https://www.malwaresa.com/docs/exploit/metasploit-payloads-msfvenom/4-3-4-4-staged-vs-stageless-payload-con-opciones-avanzadas/

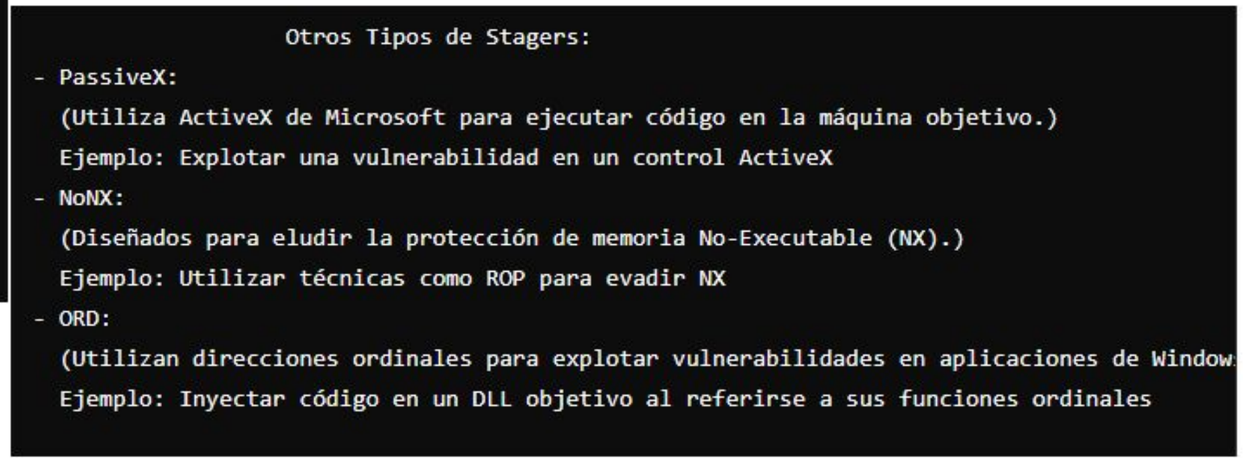
Payloads

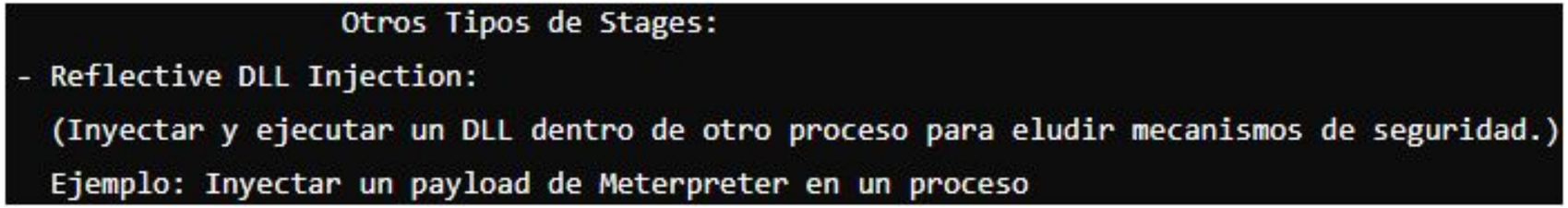


https://www.malwaresa.com/docs/exploit/metasploit-payloads-msfvenom/4-3-4-4-staged-vs-stageless-payload-con-opciones-avanzadas/

Payloads


Payloads
Singles
(son payloads auto-contenidos que no requieren ninguna etapa adicional para ser ejecutados.)
Stagers
(payloads pequeños e iniciales diseñados para establecer una conexión de vuelta al atacante y descargar un payload más grande y complejo.)
Stages
(payloads más grandes y complejos que contienen la funcionalidad o conjunto de comandos que el atacante desea ejecutar.)


Otros Tipos de Stagers:
- PassiveX:
(Utiliza ActiveX de Microsoft para ejecutar código en la máquina objetivo.)
Ejemplo: Explotar una vulnerabilidad en un control ActiveX
- NoNX:
(Diseñados para eludir la protección de memoria No-Executable (NX).)
Ejemplo: Utilizar técnicas como ROP para evadir NX
- ORD:
(Utilizan direcciones ordinales para explotar vulnerabilidades en aplicaciones de Windows
Ejemplo: Inyectar código en un DLL objetivo al referirse a sus funciones ordinales


Otros Tipos de Stages:
- Reflective DLL Injection:
(Inyectar y ejecutar un DLL dentro de otro proceso para eludir mecanismos de seguridad.)
Ejemplo: Inyectar un payload de Meterpreter en un proceso

Sessions

```
msf > sessions -h
Usage: sessions [options] or sessions [id]

Active session manipulation and interaction.

OPTIONS:

    -C   Run a Meterpreter Command on the session given with -i, or all
    -K        Terminate all sessions
    -c   Run a command on the session given with -i, or all
    -h        Help banner
    -i   Interact with the supplied session ID
    -k   Terminate sessions by session ID and/or range
    -l        List all active sessions
    -q        Quiet mode
    -r        Reset the ring buffer for the session given with -i, or all
    -s   Run a script on the session given with -i, or all
    -t   Set a response timeout (default: 15)
    -u   Upgrade a shell to a meterpreter session on many platforms
    -v        List sessions in verbose mode
    -x        Show extended information in the session table

Many options allow specifying session ranges using commas and dashes.
For example:  sessions -s checkvm -i 1,3-5  or  sessions -k 1-2,5,6
```


THE
BRIDGE