kali linux渗透测试

第10课 远程控制实现的基本原理

在发现目标主机漏洞之后，我们可以在Kali 本地的漏洞数据库中去搜索对应的漏洞渗透模块。

比如，在上一期教程中，我们演示的39009.py。通过这个漏洞渗透模块，我们成功的让目标主机上的软件服务崩溃掉，并且在目标主机上成功启动了计算器程序。但这似乎并不是我们想要的结果。

如果成功渗透目标主机，你会希望代码实现什么功能?

1. 让目标主机系统服务崩溃
2. 在目标主机上执行某个程序
3. 直接控制目标主机

显然，控制目标主机是最令人激动的。按照这个目的，我们在目标主机上执行的代码，应该是一个远程控制程序。

曾经红极一时的灰鸽子就是一个远程控制软件

远程控制软件被广泛使用，我们可以使用它完成办公，远程协助等等工作。

远程控制程序的组成：主控端和被控端

如何在Kali Linux中生成被控端

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**，这个命令是著名渗透测试软件**Metasploit**的一个功能。

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

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

1. 打开Metasploit
2. 使用handler作为主控端，use exploit/multi/handler
3. 设置payload，lhost，lport参数
4. 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

谢谢观赏