第四课 Meterpreter的介绍与使用（理论Basic）

Author：陈殷

公众号：山丘安全攻防实验室

Meterpreter是Metasploit框架中的一个扩展模块，作为溢出成功以后的攻击载荷使用，攻击载荷在溢出攻击成功以后给我们返回一个控制通道。

使用它作为攻击载荷能够获得目标系统的一个Meterpreter shell的链接。
Meterpreter shell作为渗透模块有很多有用的功能，比如添加一个用户、隐藏一些东西、打开shell、得到用户密码、上传下载远程主机的文件、运行cmd.exe、捕捉屏幕、得到远程控制权、捕获按键信息、清除应用程序、显示远程主机的系统信息、显示远程机器的网络接口和IP地址等信息。

另外Meterpreter能够躲避入侵检测系统。

meterpreter使用了大量的反射dll注入技术，meterpreter使用的反射dll不会在磁盘上留下任何文件，直接是载入内存的，所以有很好的躲避杀软的效果。

Metasploit提供了各个主流平台的Meterpreter版本，包括Windows、Linux，同时支持x86、x64平台，另外，Meterpreter还提供了基于PHP和Java语言的实现。

Meterpreter的工作模式是纯内存的，好处是启动隐藏，很难被杀毒软件监测到。不需要访问目标主机磁盘，所以也没什么入侵的痕迹。
Meterpreter还可以简化任务创建多个会话。可以来利用这些会话进行渗透。

在Metasploit Framework中，Meterpreter是一种后渗透工具，它属于一种在运行过程中可通过网络进行功能扩展的动态可扩展型Payload。

主要作用：信息收集、提权、注册表操作、令牌操纵、哈希利用、后门植入等等

Meterpreter类型
1、反向shell：reverse_tcp（基于tcp）
基于TCP的反向链接反弹shell，速度稳定
例如：Payload: window/x64/meterpreter/reverse_tcp
2、反向shell：reverse_http（基于http）
基于http的反向链接反弹shell，稳不稳定看网速了
例如：payload: windows/meterpreter/reverse_http
3、正向shell：bind_tcp（基于tcp）
基于TCP的正向连接shell，内网跨网段时使用，攻击机主动连接shell
例如：payload: linux/x86/meterpreter/bind_tcp

Payloads分类：
1、single，single是一种完全独立的Payload
2、stager ，stager这种Payload负责建立目标用户与攻击者之间的网络连接，并下载额外的组件或应用程序。一
种常见的Stagers Payload就是reverse_tcp，它可以让目标系统与攻击者建立一条tcp连接
3、stage，stage是Stager Payload下载的一种Payload组件，这种Payload可以提供更加高级的功能，而且没有大小

限制。
stager和stage就像web入侵里面提到的小马和大马一样,由于exploit环境的限制,可能不能一下子把stage传过去,需
要先传一个stager，stager在攻击者和目标之间建立网络连接，之后再把stage传过去进行下一步的行动

Meterpreter命令介绍：
输入shell即可进入交互式命令执行界面，windows解决中文乱码问题，输入chcp 65001
help帮助
1、核心命令：
• background - 将当前会话移动到后台
• exit - 终止 meterpreter 会话
• help - 帮助菜单
• irb - 进入 Ruby 脚本模式
• migrate - 移动到一个指定的 PID 的活动进程
• quit - 终止 meterpreter 会话
• run - 执行以后它选定的 meterpreter 脚本（如运行关闭杀软脚本、启动远程桌面脚本等）
• use - 加载 meterpreter 的扩展（使用mimikatz等）

后面的课程我会讲到如何使用meterpreter，这节课只用作理论铺垫。

文章作者：陈殷

文章出处：山丘安全攻防实验室