kali linux渗透测试

第15课 使用Veil-Evasion绕过杀毒软件

在大多数人们的心目中都会认为一个安装了杀毒软件的系统就是安全的。因为杀毒软件会清除掉所有对系统有害的程序。
看了之前视频教程的朋友，一定会有这样的疑问，系统只要安装一个杀毒软件就可以搞定所有的木马，我们现在还学习远程控制程序有什么用呢?

如果真的是这样的话,那么任何的 Payload就都没有用途了。不过事实并非如此,接下来我们来介绍一些可以绕过杀毒软件的方法。其实方法有很多,但是其中很多优秀的方法需要一些编译和汇编的知识,这里我们只介绍一种简单的而且可以绕过杀毒软件查杀的工具：Veil-Evasion

杀毒软件采用了模式匹配或者特征匹配的工作模式,如果一个程序中不存在病毒库中的特征码,那么杀毒软件就不会认为这是一个病毒文件。因此我们需要修改或者掩盖恶意软件的特征码,这样杀毒软件就很有可能不会阻止这个软件的运行。

安装命令

```
git clone https://github.com/Veil-Framework/Veil-Evasion.git
setup.sh -c
```

启动

```
python Veil-Evasion.py
```

谢谢观赏