kali linux渗透测试

第9课 为什么微软和谷歌建议大家使用新系统？黑客告诉你原因

威胁建模

在主动侦察和被动侦察之后，测试人员或者攻击者就可以利用已知的信息和漏洞来进行攻击。
在这个阶段，很多人都会犯一个错误，认为自己利用已知的信息，直接击垮目标，就是对自己的最好证明。这么做有时，非但不能成功，而且还会暴露自己。

在真正的攻击开始之前，我们应该先在本地做威胁建模，也就是搭建模拟测试的环境，先进行模拟攻击。我们称为：威胁建模

通过威胁建模，可以提高成功率。

在建模的时候，我们需要考虑目标的类型。对于不同类型的目标，制定不同的方案。

确认目标类型：

首要目标：当这些目标被击垮时，渗透测试人员可以直接达成最后的目的。

次要目标：这些目标可以提供信息（安全控制，密码等等信息）以支持对首要目标进行的攻击

第三目标：这些目标看似与测试或者攻击无关，但是这些目标相对容易攻击，可以为实际的攻击提供信息或者其他的思路。

利用本地漏洞资源

kali Linux系统中，有搜索漏洞数据库(exploitdb)的本地副本，我们可以在终端窗口中输入命令去搜索。

searchsploit 关键词

练习：

Easy File Sharing这个软件，是一种允许访客容易地经由浏览器上传/下载文件的文件分享系统。

我们在kali的本地漏洞库中去搜索这个软件的相关漏洞

searchsploit easy file sharing

练习总结：使用最新的系统，以及相应软件的最新版本，如果软件多年为更新，建议使用其他常更新的软件替代。

谢谢观赏