

kali linux渗透测试

The background features a dark blue color scheme with a glowing hexagonal grid pattern. Several padlock icons are scattered across the grid. In the bottom-left corner, there is a stylized globe composed of a network of white dots and lines, representing a global network or data flow.

第18课 网络安全渗透测试很难学吗？有了 Metasploit，一切就简单多了

Metasploit发展史

在没有漏洞渗透工具框架的时候，渗透测试人员往往需要自己收集漏洞渗透用的代码，甚至有时需要自己编写针对漏洞用的代码。这个时期的渗透测试效率是比较低的，而且想要成为一个合格渗透测试者的学习成本也是相当高的。

2003年左右,美国的H.D Moore (世界著名的黑客)和Spoonm创建了一个集成了多个漏洞渗透工具的框架。随后,这个框架在2004年的世界黑客交流会(Black Hat Briefings)上备受关注, Spoonm在大会的演讲中提到, Metasploit的使用如此简单, 以至于你只需要找到一个目标, 单击几下鼠标左键就可以完成渗透, 一切就和电影里面演的一样酷。强大的功能再加上简单的操作使得Metasploit在安全行业迅速地传播开来, 很快就成为业内最著名的工具。目前的Metasploit存在多个版本, 其中既有适合企业使用的商业版本Metasploit Pro, 也有适合个人使用的免费版本Metasploit Community。Kali Linux 2中默认安装好了Metasploit Community, 我们教程的讲解也将围绕这个版本进行展开。



打开的方式

- 1.快捷工具栏
- 2.在所有程序中打开
- 3.使用命令：msfconsole 打开

需要注意的是，不用在意Metasploit启动的图案，每次可能都不相同。



这里面一共提供了7个种类的模块，我们首先来介绍一下常用模块的作用。

漏洞渗透模块(exploits)：这类模块正是我们之前讲解的重点,绝大多数人在发现了目标的漏洞之后,往往不知道接下来如何利用这个漏洞。而漏洞渗透模块则解决了这个问题，每一个模块对应着一个漏洞，发现了目标的漏洞之后，我们无需知道漏洞是如何产生的，甚至无需会编程，只需要知道漏洞的名字，然后执行对应的漏洞模块，就可以实现对目标的入侵。

攻击载荷模块(payload)：这类模块就是我们之前提到的被控端程序,它们可以帮助我们在目标上完成远程控制操作。通常这些模块既可以单独执行,也可以和漏洞渗透模块一起执行。

辅助模块(auxiliary)：进行信息收集的模块,例如一些信息侦查、网络扫描类的工具。

后渗透攻击模块(post)：当我们成功地取得目标的控制权之后,就是这类模块大显身手的时候,它可以帮助我们提高控制权限、获取敏感信息、实施跳板攻击等。



使用Help命令，查看帮助

show

search

use



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, overlaid with a network of white and blue lines and dots. Scattered throughout the background are several padlock icons, some of which are open, symbolizing digital security or vulnerabilities. The overall aesthetic is high-tech and futuristic.

谢谢观赏