Python语言的优点

易学易用

学习一种新编程语言时，往往会遇到各种各样的问题。为了解决这些问题，Python语言做了大量努力。比如，Python中不必声明变量类型，而在运行时动态确定。此外，也不需要用户对内存进行管理，这些工作由解释器自动执行。

功能强大

Python是开源语言，全世界开发人员一直在自发改进Python，不断开发创建各种功能强大的库。其他语言中要使用数十行代码才能完成的功能，在Python中只需要使用简单的几行代码即可搞定。

扩展性良好

Windows、UNIX、Mac、Android操作系统都可以使用Python，只需在目标操作系统中安装相应解释器即可。Python内置多种编程接口，借助它可以在Python中使用其他语言开发的API，对功能进行无限扩展。

开发速度快

Python 语法简单，且拥有大量功能强大的库，与其他编程语言相比，使用Python能够更快速地开发应用程序。在竞争激烈且对开发速度有严格要求的行业，使用Python进行开发是十分必要的。

Python 黑客攻击用途

Python提供了丰富多样的模块，这些模块几乎可以直接用于所有黑客攻击领域。对于黑客攻击模块不提供的领域，可以借由ctypes调用操作系统提供的原生API。简言之，使用Python几乎可以攻击所有领域，比如应用程序、Web、网络、系统等，下面分别介绍各领域Python黑客攻击技术。

应用程序黑客攻击：可以向运行中的应用程序插入任意DLL或者源代码，拦截用户的键盘输入以盗取密码。此外，还可以将黑客攻击代码插入图片文件，在网络散布传播。

Web黑客攻击：可以创建网页爬虫，收集Web页面包含的链接，实现SQL注入，向处理用户输入的部分注入错误代码。使用Python可以实现简单的网络浏览器功能，通过操纵HTTP包，上传Web shell攻击所需文件。

网络黑客攻击：可以实施网络踩点，搜索系统开放的端口，收集并分析网络上的数据包，进行网络嗅探。伪装服务器地址，实施IP欺骗攻击，非法盗取敏感信息。也可以大量发送数据包，实施拒绝服务式攻击，使服务器陷入瘫痪，无法正常对外提供服务。

系统黑客攻击：黑客可以编写后门程序以控制用户PC，开发用于搜索并修改PC注册表的功能。还可以利用应用程序的错误，通过缓冲区溢出或格式字符串实施攻击。

根据黑客攻击实施的位置将其分为五大类，分别为系统黑客攻击、应用程序黑客攻击、Web黑客攻击、网络黑客攻击以及其他黑客攻击技术。

系统黑客攻击针对的是计算机内核。通过系统黑客攻击，可以侵入计算机内核管理的内存、注册表等区域，非法获取其中数据或root权限。应用程序黑客攻击是围绕用户运行的程序实施的黑客攻击。通过向应用程序注入包含恶意代码的DLL或调试操作，拦截用户的键盘输入。Web黑客攻击利用网络浏览器与Web服务器的结构漏洞实施黑客攻击，它是目前最常用的黑客攻击技术。网络黑客攻击基于网络实施黑客攻击，包括常见的Dos攻击、网络包嗅探（Spoofing)等。此外，还有无线网络黑客攻击与社会工程黑客攻击技术等。