如果你热爱漏洞研究、逆向工程或者渗透测试，我强烈推荐你使用 Python 作为编程语言。它包含大量实用的库和工具，本文会列举其中部分精华。

网络

Scapy, Scapy3k: 发送，嗅探，分析和伪造网络数据包。可用作交互式包处理程序或单独作为一个库。
pypcap, Pcapy, pylibpcap: 几个不同 libpcap 捆绑的python库
libdnet: 低级网络路由，包括端口查看和以太网帧的转发
dpkt: 快速，轻量数据包创建和分析，面向基本的 TCP/IP 协议

Impacket: 伪造和解码网络数据包，支持高级协议如 NMB 和 SMB
pynids: libnids 封装提供网络嗅探，IP 包碎片重组，TCP 流重组和端口扫描侦查

Dirtbags py-pcap: 无需 libpcap 库支持读取 pcap 文件
flowgrep: 通过正则表达式查找数据包中的 Payloads
Knock Subdomain Scan: 通过字典枚举目标子域名
SubBrute: 快速的子域名枚举工具
Mallory: 可扩展的 TCP/UDP 中间人代理工具，可以实时修改非标准协议
Pytbull: 灵活的 IDS/IPS 测试框架（附带超过300个测试样例）

调试和逆向工程

Paimei: 逆向工程框架，包含 PyDBG, PIDA,pGRAPH
Immunity Debugger: 脚本 GUI 和命令行调试器
mona.py: Immunity Debugger 中的扩展，用于代替 pvefindaddr
IDAPython: IDA pro 中的插件，集成 Python 编程语言，允许脚本在 IDA Pro 中执行
PyEMU: 全脚本实现的英特尔32位仿真器，用于恶意软件分析
pefile: 读取并处理 PE 文件
pydasm: Python 封装的 libdasm
PyDbgEng: Python 封装的微软 Windows 调试引擎
uhooker: 截获 DLL 或内存中任意地址可执行文件的 API 调用
diStorm: AMD64 下的反汇编库
python-ptrace: Python 写的使用 ptrace 的调试器
vdb/vtrace: vtrace 是用 Python 实现的跨平台调试 API, vdb 是使用它的调试器
Androguard: 安卓应用程序的逆向分析工具
Capstone: 一个轻量级的多平台多架构支持的反汇编框架。支持包括ARM,ARM64,MIPS和x86/x64平台。
PyBFD: GNU 二进制文件描述(BFD)库的 Python 接口

Fuzzing

Sulley: 一个模糊器开发和模糊测试的框架，由多个可扩展的构件组成的
Peach Fuzzing Platform: 可扩展的模糊测试框架(v2版本 是用 Python 语言编写的)
antiparser: 模糊测试和故障注入的 API
TAOF: (The Art of Fuzzing, 模糊的艺术)包含 ProxyFuzz, 一个中间人网络模糊测试工具
untidy: 针对 XML 模糊测试工具
Powerfuzzer: 高度自动化和可完全定制的 Web 模糊测试工具
SMUDGE: 纯 Python 实现的网络协议模糊测试
Mistress: 基于预设模式，侦测实时文件格式和侦测畸形数据中的协议
Fuzzbox: 媒体多编码器的模糊测试
Forensic Fuzzing Tools: 通过生成模糊测试用的文件，文件系统和包含模糊测试文件的文件系统，来测试取证工具的鲁棒性
Windows IPC Fuzzing Tools: 使用 Windows 进程间通信机制进行模糊测试的工具
WSBang: 基于 Web 服务自动化测试 SOAP 安全性
Construct: 用于解析和构建数据格式(二进制或文本)的库

Construct: 用于解析和构建数据格式(二进制或文本)的库
fuzzer.py(feliam): 由 Felipe Andres Manzano 编写的简单模糊测试工具
Fusil: 用于编写模糊测试程序的 Python 库

Web

Requests: 优雅，简单，人性化的 HTTP 库
HTTPie: 人性化的类似 cURL 命令行的 HTTP 客户端
ProxMon: 处理代理日志和报告发现的问题
WSMap: 寻找 Web 服务器和发现文件
Twill: 从命令行界面浏览网页。支持自动化网络测试
Ghost.py: Python 写的 WebKit Web 客户端
Windmill: Web 测试工具帮助你轻松实现自动化调试 Web 应用
FunkLoad: Web 功能和负载测试
spynner: Python 写的 Web浏览模块支持 Javascript/AJAX
python-spidermonkey: 是 Mozilla JS 引擎在 Python 上的移植，允许调用 Javascript 脚本和函数
mitmproxy: 支持 SSL 的 HTTP 代理。可以在控制台接口实时检查和编辑网络流量
pathod/pathoc: 变态的 HTTP/S 守护进程，用于测试和折磨 HTTP 客户端

取证

Volatility: 从 RAM 中提取数据
Rekall: Google 开发的内存分析框架
LibForensics: 数字取证应用程序库
TrIDLib: Python 实现的从二进制签名中识别文件类型
aft: 安卓取证工具集恶意软件分析

pyew: 命令行十六进制编辑器和反汇编工具，主要用于分析恶意软件
Exefilter: 过滤 E-mail，网页和文件中的特定文件格式。可以检测很多常见文件格式，也可以移除文档内容。
pyClamAV: 增加你 Python 软件的病毒检测能力
jsunpack-n: 通用 JavaScript 解释器，通过模仿浏览器功能来检测针对目标浏览器和浏览器插件的漏洞利用
yara-python: 对恶意软件样本进行识别和分类
phoneyc: 纯 Python 实现的蜜罐
CapTipper: 分析，研究和重放 PCAP 文件中的 HTTP 恶意流量

PDF

peepdf: Python 编写的PDF文件分析工具，可以帮助检测恶意的PDF文件
Didier Stevens’ PDF tools: 分析，识别和创建 PDF 文件(包含PDFiD，pdf-parser，make-pdf 和 mPDF)
Opaf: 开放 PDF 分析框架，可以将 PDF 转化为 XML 树从而进行分析和修改。
Origapy: Ruby 工具 Origami 的 Python 接口，用于审查 PDF 文件
pyPDF2: Python PDF 工具包包含：信息提取，拆分，合并，制作，加密和解密等等

pyPDF2: Python PDF 工具包包含：信息提取，拆分，合并，制作，加密和解密等等
PDFMiner: 从 PDF 文件中提取文本
python-poppler-qt4: Python 写的 Poppler PDF 库，支持 Qt4

杂项

InlineEgg: 使用 Python 编写的具有一系列小功能的工具箱
Exomind: 是一个利用社交网络进行钓鱼攻击的工具
RevHosts: 枚举指定 IP 地址包含的虚拟主句
simplejson: JSON 编码和解码器，例如使用 Google’s AJAX API
PyMangle: 命令行工具和一个创建用于渗透测试使用字典的库
Hachoir: 查看和编辑二进制流

其他有用的库和工具

IPython: 增强的交互式 Python shell
Beautiful Soup: HTML 解析器
matplotlib: 制作二维图
Mayavi: 三维科学数据的可视化与绘图
RTGraph3D: 在三维空间中创建动态图
Twisted: Python 语言编写的事件驱动的网络框架
Suds: 一个轻量级的基于SOAP的python客户端
M2Crypto: Python 语言对 OpenSSL 的封装
NetworkX: 图库(边, 节点)
Pandas: 基于 Numpy 构建的含有更高级数据结构和工具的数据分析包
pyparsing: 通用解析模块
lxml: 使用 Python 编写的库，可以迅速、灵活地处理 XML
Whoosh: 纯python实现的全文搜索组件
Pexpect: 控制和自动化程序
Sikuli: 使用 Jython 脚本自动化基于截图进行视觉搜索
PyQt 和PySide: Python 捆绑的 Qt 应用程序框架和 GUI 库

书籍

Violent Python TJ O’Connor著: 详细介绍黑客，取证分析，渗透测试和安全工程师的书 (注：乌云社区有中文翻译版，感谢草帽小子-DJ和crown、prince 的翻译)
Grey Hat Python Justin Seitz著: Python 编程用于黑客和逆向工程
Black Hat Python Justin Seitz著:Python 编程用于黑客和渗透测试
Python Penetration Testing Essentials Mohit著:借助 Python 的力量做到最好的渗透测试
Python for Secret Agents Steven F. Lott著: 使用 Python 分析，加密和分析数据

其他

SecurityTube Python Scripting Expert (SPSE) 由 Vivek Ramachandran 提供的在线课程和认证

SANS 提供的相关课程 SEC573: Python for Penetration Testers

Python Arsenal for Reverse Engineering: 收集有大量逆向工程相关的工具

这是 SANS 关于用于取证分析的 Python 库的论文 (PDF)

更多 Python 的库可以在 PyPI 中查找

（注：译者将原文中部分Google Code的链接更换为了Github）

***原文：Github，FB小编xiaix编译，转自须注明来自FreeBuf黑客与极客（FreeBuf.COM）**