dloss / **python-pentest-tools**

Watch 235 | Star 1,954 | Fork 670

Code | Issues 0 | Pull requests 0 | Projects 0 | Security | Insights

Python tools for penetration testers

41 commits | **1** branch | **0** releases | **6** contributors | MIT

Branch: **master** | New pull request | Find file | Clone or download

portantier and **dloss** Update README.md ··· Latest commit `ad79cb0` on Sep 16, 2017

LICENSE	Initial commit	5 years ago
README.md	Update README.md	2 years ago

README.md

Python tools for penetration testers

If you are involved in vulnerability research, reverse engineering or pentesting, I suggest to try out the Python programming language. It has a rich set of useful libraries and programs. This page lists some of them.

Most of the listed tools are written in Python, others are just Python bindings for existing C libraries, i.e. they make those libraries easily usable from Python programs.

Some of the more aggressive tools (pentest frameworks, bluetooth smashers, web application vulnerability scanners, war-dialers, etc.) are left out, because the legal situation of these tools is still a bit unclear in Germany -- even after the decision of the highest court. This list is clearly meant to help whitehats, and for now I prefer to err on the safe side.

Network

- Scapy, Scapy3k: send, sniff and dissect and forge network packets. Usable interactively or as a library
- pypcap, Pcapy and pylibpcap: several different Python bindings for libpcap
- libdnet: low-level networking routines, including interface lookup and Ethernet frame transmission
- dpkt: fast, simple packet creation/parsing, with definitions for the basic TCP/IP protocols
- Impacket: craft and decode network packets. Includes support for higher-level protocols such as NMB and SMB
- pynids: libnids wrapper offering sniffing, IP defragmentation, TCP stream reassembly and port scan detection
- Dirtbags py-pcap: read pcap files without libpcap
- flowgrep: grep through packet payloads using regular expressions
- Knock Subdomain Scan, enumerate subdomains on a target domain through a wordlist
- SubBrute, fast subdomain enumeration tool

- Mallory, extensible TCP/UDP man-in-the-middle proxy, supports modifying non-standard protocols on the fly
- Pytbull: flexible IDS/IPS testing framework (shipped with more than 300 tests)
- Spoodle: A mass subdomain + poodle vulnerability scanner
- SMBMap: enumerate Samba share drives across an entire domain
- Habu: python network hacking toolkit

Debugging and reverse engineering

- Paimei: reverse engineering framework, includes PyDBG, PIDA, pGRAPH
- Immunity Debugger: scriptable GUI and command line debugger
- mona.py: PyCommand for Immunity Debugger that replaces and improves on pvefindaddr
- IDAPython: IDA Pro plugin that integrates the Python programming language, allowing scripts to run in IDA Pro
- PyEMU: fully scriptable IA-32 emulator, useful for malware analysis
- pefile: read and work with Portable Executable (aka PE) files
- pydasm: Python interface to the libdasm x86 disassembling library
- PyDbgEng: Python wrapper for the Microsoft Windows Debugging Engine
- uhooker: intercept calls to API calls inside DLLs, and also arbitrary addresses within the executable file in memory
- diStorm: disassembler library for AMD64, licensed under the BSD license
- Frida: A dynamic instrumentation framework which can inject scripts into running processes
- python-ptrace: debugger using ptrace (Linux, BSD and Darwin system call to trace processes) written in Python
- vdb / vtrace: vtrace is a cross-platform process debugging API implemented in python, and vdb is a debugger which uses it
- Androguard: reverse engineering and analysis of Android applications
- Capstone: lightweight multi-platform, multi-architecture disassembly framework with Python bindings
- Keystone: lightweight multi-platform, multi-architecture assembler framework with Python bindings

- PyBFD: Python interface to the GNU Binary File Descriptor (BFD) library
- CHIPSEC: framework for analyzing the security of PC platforms including hardware, system firmware (BIOS/UEFI), and platform components.

Fuzzing

- afl-python: enables American fuzzy lop fork server and instrumentation for pure-Python code
- Sulley: fuzzer development and fuzz testing framework consisting of multiple extensible components
- Peach Fuzzing Platform: extensible fuzzing framework for generation and mutation based fuzzing (v2 was written in Python)
- antiparser: fuzz testing and fault injection API
- TAOF, (The Art of Fuzzing) including ProxyFuzz, a man-in-the-middle non-deterministic network fuzzer
- untidy: general purpose XML fuzzer
- Powerfuzzer: highly automated and fully customizable web fuzzer (HTTP protocol based application fuzzer)
- SMUDGE
- Mistress: probe file formats on the fly and protocols with malformed data, based on pre-defined patterns
- Fuzzbox: multi-codec media fuzzer
- Forensic Fuzzing Tools: generate fuzzed files, fuzzed file systems, and file systems containing fuzzed files in order to test the robustness of forensics tools and examination systems
- Windows IPC Fuzzing Tools: tools used to fuzz applications that use Windows Interprocess Communication mechanisms
- WSBang: perform automated security testing of SOAP based web services
- Construct: library for parsing and building of data structures (binary or textual). Define your data structures in a declarative manner
- fuzzer.py (feliam): simple fuzzer by Felipe Andres Manzano

- Fusil: Python library used to write fuzzing programs

Web

- Requests: elegant and simple HTTP library, built for human beings
- lxml: easy-to-use library for processing XML and HTML; similar to Requests
- HTTPie: human-friendly cURL-like command line HTTP client
- ProxMon: processes proxy logs and reports discovered issues
- WSMap: find web service endpoints and discovery files
- Twill: browse the Web from a command-line interface. Supports automated Web testing
- Ghost.py: webkit web client written in Python
- Windmill: web testing tool designed to let you painlessly automate and debug your web application
- FunkLoad: functional and load web tester
- spynner: Programmatic web browsing module for Python with Javascript/AJAX support
- python-spidermonkey: bridge to the Mozilla SpiderMonkey JavaScript engine; allows for the evaluation and calling of Javascript scripts and functions
- mitmproxy: SSL-capable, intercepting HTTP proxy. Console interface allows traffic flows to be inspected and edited on the fly
- pathod / pathoc: pathological daemon/client for tormenting HTTP clients and servers
- spidy: simple command-line web crawler with page downloading and word scraping

Forensics

- Volatility: extract digital artifacts from volatile memory (RAM) samples
- Rekall: memory analysis framework developed by Google
- LibForensics: library for developing digital forensics applications

- TrIDLib, identify file types from their binary signatures. Now includes Python binding
- aft: Android forensic toolkit

Malware analysis

- pyew: command line hexadecimal editor and disassembler, mainly to analyze malware
- Exefilter: filter file formats in e-mails, web pages or files. Detects many common file formats and can remove active content
- pyClamAV: add virus detection capabilities to your Python software
- jsunpack-n, generic JavaScript unpacker: emulates browser functionality to detect exploits that target browser and browser plug-in vulnerabilities
- yara-python: identify and classify malware samples
- phoneyc: pure Python honeyclient implementation
- CapTipper: analyse, explore and revive HTTP malicious traffic from PCAP file

PDF

- peepdf: Python tool to analyse and explore PDF files to find out if they can be harmful
- Didier Stevens' PDF tools: analyse, identify and create PDF files (includes PDFiD, pdf-parser and make-pdf and mPDF)
- Opaf: Open PDF Analysis Framework. Converts PDF to an XML tree that can be analyzed and modified.
- Origapy: Python wrapper for the Origami Ruby module which sanitizes PDF files
- pyPDF2: pure Python PDF toolkit: extract info, spilt, merge, crop, encrypt, decrypt...
- PDFMiner: extract text from PDF files
- python-poppler-qt4: Python binding for the Poppler PDF library, including Qt4 support

Misc

- InlineEgg: toolbox of classes for writing small assembly programs in Python
- Exomind: framework for building decorated graphs and developing open-source intelligence modules and ideas, centered on social network services, search engines and instant messaging
- RevHosts: enumerate virtual hosts for a given IP address
- simplejson: JSON encoder/decoder, e.g. to use Google's AJAX API
- PyMangle: command line tool and a python library used to create word lists for use with other penetration testing tools
- Hachoir: view and edit a binary stream field by field
- py-mangle: command line tool and a python library used to create word lists for use with other penetration testing tools
- wmiexec.py: execute Powershell commands quickly and easily via WMI
- Pentestly: Python and Powershell internal penetration testing framework
- hacklib: Toolkit for hacking enthusiasts: word mangling, password guessing, reverse shell and other simple tools

Other useful libraries and tools

- IPython: enhanced interactive Python shell with many features for object introspection, system shell access, and its own special command system
- Beautiful Soup: HTML parser optimized for screen-scraping
- matplotlib: make 2D plots of arrays
- Mayavi: 3D scientific data visualization and plotting
- RTGraph3D: create dynamic graphs in 3D
- Twisted: event-driven networking engine
- Suds: lightweight SOAP client for consuming Web Services
- M2Crypto: most complete OpenSSL wrapper
- NetworkX: graph library (edges, nodes)
- Pandas: library providing high-performance, easy-to-use data structures and data analysis tools

- pyparsing: general parsing module
- lxml: most feature-rich and easy-to-use library for working with XML and HTML in the Python language
- Whoosh: fast, featureful full-text indexing and searching library implemented in pure Python
- Pexpect: control and automate other programs, similar to Don Libes `Expect` system
- Sikuli, visual technology to search and automate GUIs using screenshots. Scriptable in Jython
- PyQt and PySide: Python bindings for the Qt application framework and GUI library

Books

- Violent Python by TJ O'Connor. A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
- Grey Hat Python by Justin Seitz: Python Programming for Hackers and Reverse Engineers.
- Black Hat Python by Justin Seitz: Python Programming for Hackers and Pentesters
- Python Penetration Testing Essentials by Mohit: Employ the power of Python to get the best out of pentesting
- Python for Secret Agents by Steven F. Lott. Analyze, encrypt, and uncover intelligence data using Python
- Python Web Penetration Testing Cookbook by Cameron Buchanan et al.: Over 60 Python recipes for web application testing
- Learning Penetration Testing with Python by Christopher Duffy: Utilize Python scripting to execute effective and efficient penetration tests
- Python Forensics by Chet Hosmer: A Workbench for Inventing and Sharing Digital Forensic Technology
- The Beginner's Guide to IDAPython by Alexander Hanel

Talks, slides and articles

- Python & Reverse Engineering Software by Alexander Hanel
- Python Arsenal for Reverse Engineering by Dmitriy Evdokimov at RUCTF 2016

More stuff

- SecurityTube Python Scripting Expert (SPSE) is an online course and certification offered by Vivek Ramachandran.
- SANS offers the course SEC573: Python for Penetration Testers.
- The Python Arsenal for Reverse Engineering is a large collection of tools related to reverse engineering.
- There is a SANS paper about Python libraries helpful for forensic analysis (PDF).
- For more Python libaries, please have a look at PyPI, the Python Package Index.