

DSECRG

Python Arsenal for Reverse Engineering

Dmitry "D1g1" Evdokimov

DSecRG, Security Researcher



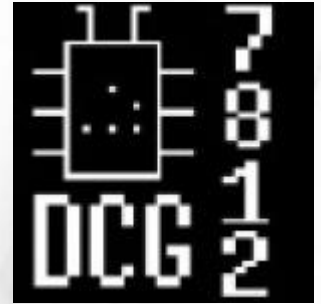
ZERO
NIGHTS

www.zeronights.ru



#whoami

- Security Researcher in DSecRG
 - RE
 - Fuzzing
 - Mobile security
- Organizer: DCG #7812
- Editor in “XAKEP”



ERPScan
Security Scanner for SAP

Intro

OllyDbg



GDB
The GNU Project
Debugger

Perl?!

Dmitriy Evdokimov @evdokimovds 15 ноября
I'm going to release "Python arsenal for RE" website on #ZeroNights security conference
Свернуть ← Ответить ↻ Ретвитнуть ★ В избранное

6 РЕТВИТОВ

15 ноября 12 в 10:27 утра · Подробнее

red plait @real_redp 15 ноября
@evdokimovds с двумя с половиной неработающими скриптами для ida python, как обычно ?
Развернуть

Perl binding for IDA Pro: <http://cyrplw.svn.sourceforge.net/viewvc/cyrplw/perl/>
<http://redplait.blogspot.ru/2011/08/perl-inside-ida-pro.html>

Ruby?

- Metasm - the Ruby assembly manipulation suite
- Idarub - Ruby plugin for IDAPro
- Ragweed - scriptable Win32/Linux/OSX debugger written in ruby
- frasm - Ruby bindings for distorm64
- LeafRub - x86 ELF Analysis and Debugging
- rbkb - A miscellaneous collection of command-line tools and ruby library helpers related to pen-testing and reversing
- jdi_hook - JRuby based scriptable Java debugger using the JDI interface
- ???



Python!

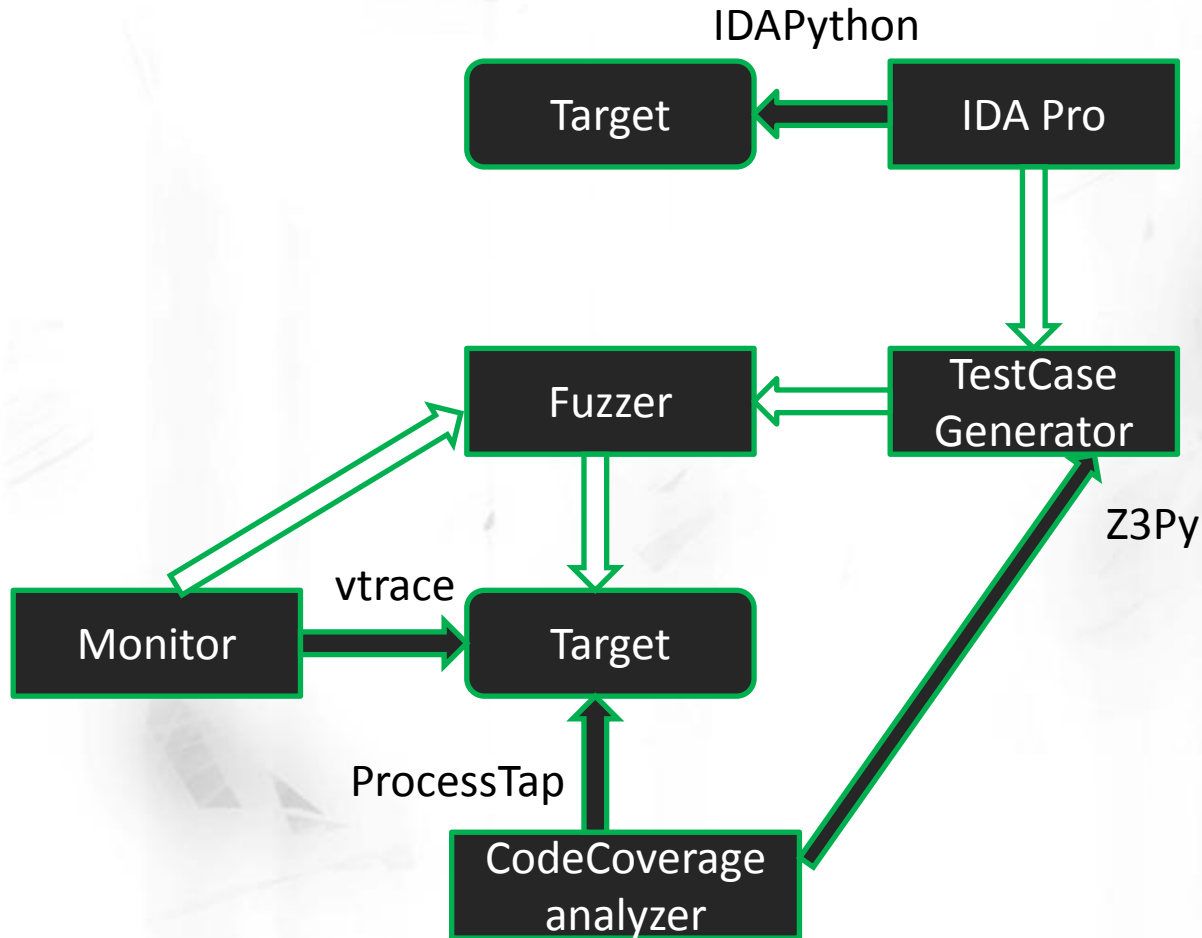
BeaEnginePython
bochs-python-
instrumentation
Buggery
Ctypes
Deviare
dislib
diStorm
FrASM
IDAPython
ImmLIB
libdisassemble
lldb
llvmpy
Macholib
Miasm
OllyPython
PDBparse
PEEL
pefile
PIDA

PinPy
ProcessTap
pyasm
PyBox
PyCodin
pydasm
Pydb
PyDBG
PyDbgEng
pydbg
PyDevTools
pydot
pydusa
PyEA
PyELF
Pyelftools
PyEMU
pyew
pygdb
pyHIEW


pykd
Pylibemu
pylibscizzle
pyMem
pymasad
pyREtic
PySTP
python-adb
python-haystack
python-ptrace
PythonGdb
pytracer
radapy
ramooflax
uhooker
Vivisect
vtrace
WinAppDbg
Z3-python
Z3Py
...



Example



The first idea




Digital Security
Research Group

DSecRG — Research Center of ERPScan Company

Python arsenal for RE

[v. 1.1]



Dmitriy "D1g1" Evdokimov
DSecRG
Email: d_evdokimov@dsecrg.com
Twitter: [@evdokimovds](https://twitter.com/evdokimovds)

www.erpscan.com • www.dsecrg.com

Web portal

<http://pythonarsenal.dsecrg.ru/>

<http://pythonarsenal.erpscan.com/>

Site:Main

Home		Search		Feedback		About		Python Arsenal for Reverse Engineering	
B		M		P cont.		P cont.		R	
BeaEnginePython		Macholib		Pydb		pyHIEW		radapy	
bochs-python-instrumentation		Miasm		PyDBG		pykd		ramooflax	
Buggery		O		PyDbgEng		Pylibemu		U	
C		OllyPython		pydbg		pylibscizzle		uhooker	
Ctypes		P		PyDevTools		pyMem		V	
D		PDBparse		pydot		pymasaki		Vivisect	
Deviare		PEEL		pydusa		pyREtic		vtrace	
dislib		pefile		PyEA		PySTP		W	
diStorm		PIDA		PyELF		python-adb		WinAppDbg	
F		PinPy		Pyelftools		python-haystack		Z	
FrASM		ProcessTap		PyEMU		python-pttrace		Z3-python	
I		pyasm		pyew		PythonGdb		Z3Py	
IDAPython		PyBox		pygdb		pytracer			
ImmLIB		PyCodin							
L		pydasm							
libdisassemble									
lldb									
llvmpy									

Library:Description

bochs-python-instrumentation	
Author(s)	Ero Carrera (@erocarrera)
Site project	https://github.com/zynamics/bochs-python-instrumentation
Tag(s)	debugger , emulator
License	???
Python versions	2.5
Platforms	win/lin
Processors (Architecture)	x86/x64
Base project	Bochs (2.4.5 and 2.4.6)
Description	This patch for Bochs provides a Python interpreter instead of Bochs' own debugger, yet still providing the debugger functionality. It also allows to interact with the instrumentation interface on-demand, by dynamically associating Python methods to handle instrumentation events.
Tools	???

Feedback

Site:Search

Search

Project

Author(s)

Tag(s) binding DBI debugger disassembler DWARF reader
 dynamic assembler ELF reader emulator hooker interface
 intermediate language Mach-O reader monitoring of processes PDB symbols
 PE reader sandbox scripting engine search in memory SMT solver
 static analysis static/dynamic code analyser STP virtualization
 visualization wrapper

Python versions ??? 2.x 3.x

Platforms ??? win lin mac bsd darwin freebsd solaris

Processors
(Architecture) ??? x86 x64 ARM PowerPC

Base project

Site:Feedback

Z3Py

Author(s)	Microsoft Research
Site project	http://research.microsoft.com/en-us/um/redmond/projects/z3/
Tag(s)	SMT , STP , solver
License	???

Home

Search

Feedback

About

(Architecture)	
Base project	Z3
Description	Python interface for Z3. It covers all main features in the Z3 API. Z3 is a high-performance theorem prover being developed at Microsoft Research.
Tools	???
Useful links	guide

Feedback

Conclusion

- Gratz!
 - Anton Astafiev
- Future work
 - Update/implementation/fix
 - Development
 - News
 - Statistics/graph/chart



Contact



Twitter: @evdokimovds

E-mail: d.evdokimov@dsecrg.com

