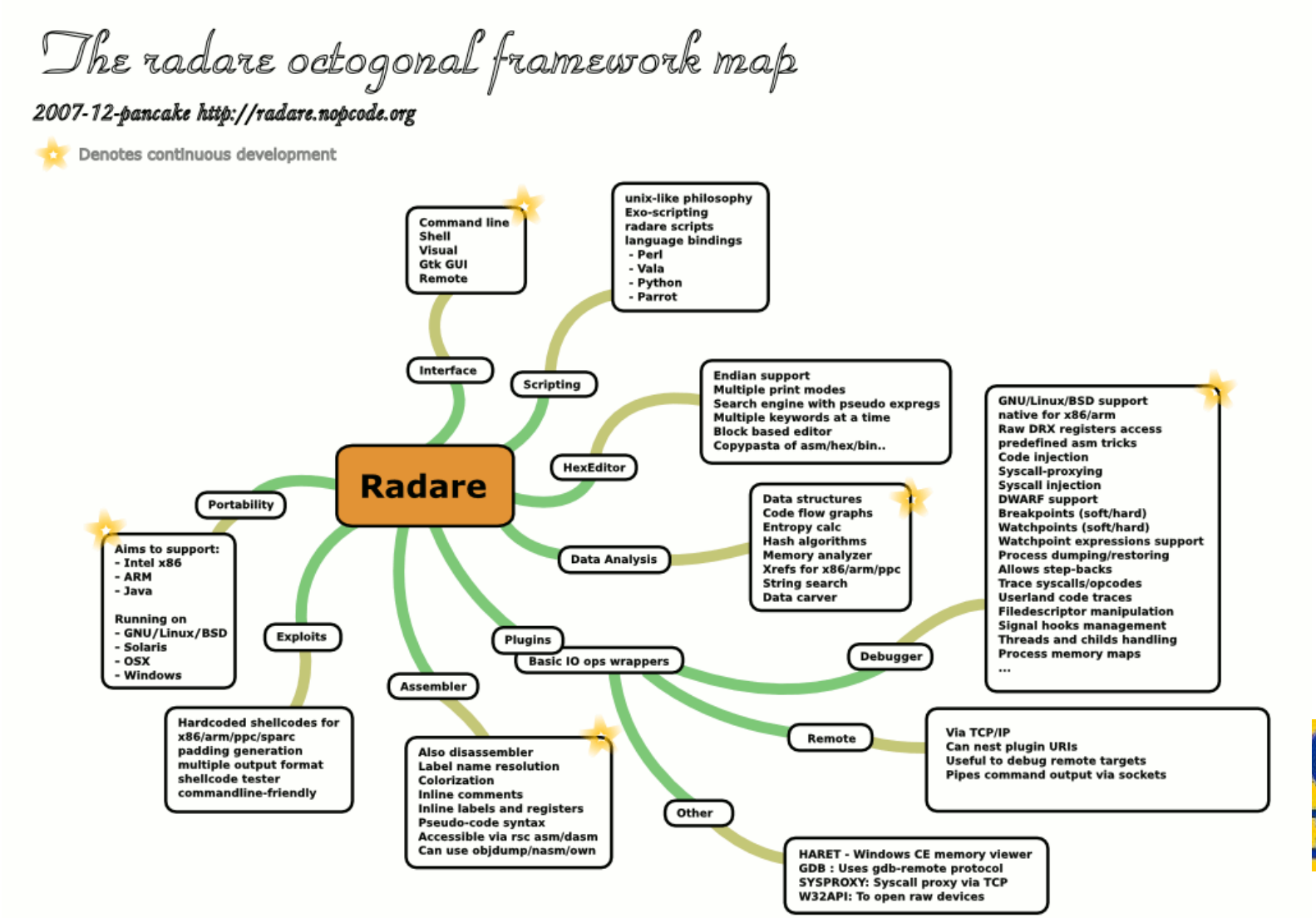
radare

Easing binary analysis for fun and profit

Overview


The radare octogonal framework map
2007-12-pancake http://radare.nopcode.org
Denotes continuous development
Radare
Interface
Command line
Shell
Visual
Gtk GUI
Remote
Scripting
unix-like philosophy
Exo-scripting
radare scripts
language bindings
- Perl
- Vala
- Python
- Parrot
HexEditor
Endian support
Multiple print modes
Search engine with pseudo expregs
Multiple keywords at a time
Block based editor
Copypasta of asm/hex/bin..
Data Analysis
Data structures
Code flow graphs
Entropy calc
Hash algorithms
Memory analyzer
Xrefs for x86/arm/ppc
String search
Data carver
Debugger
GNU/Linux/BSD support
native for x86/arm
Raw DRX registers access
predefined asm tricks
Code injection
Syscall-proxying
Syscall injection
DWARF support
Breakpoints (soft/hard)
Watchpoints (soft/hard)
Watchpoint expressions support
Process dumping/restoring
Allows step-backs
Trace syscalls/opcodes
Userland code traces
Filedescriptor manipulation
Signal hooks management
Threads and childs handling
Process memory maps
...
Plugins
Basic IO ops wrappers
Remote
Via TCP/IP
Can nest plugin URIs
Useful to debug remote targets
Pipes command output via sockets
Other
HARET - Windows CE memory viewer
GDB : Uses gdb-remote protocol
SYSPROXY: Syscall proxy via TCP
W32API: To open raw devices
Assembler
Also disassembler
Label name resolution
Colorization
Inline comments
Inline labels and registers
Pseudo-code syntax
Accessible via rsc asm/dasm
Can use objdump/nasm/own
Exploits
Hardcoded shellcodes for
x86/arm/ppc/sparc
padding generation
multiple output format
shellcode tester
commandline-friendly
Portability
Aims to support:
- Intel x86
- ARM
- Java
Running on
- GNU/Linux/BSD
- Solaris
- OSX
- Windows

IO with plugins

Basic file input/output access wrapped with plugins:

- Posix IO
- W32 IO
- Remote TCP IO
- EWF (Encase disk images)
- Debugger
- Haret
- ...

Hexadecimal editor

- The radare shell interprets simple commands to move around the binary file and perform operations like write bytes, seek, dump blocks in different formats, etc..
- Supports perl and python scripting.
- Zoom mode to have a whole overview of entropy, printable chars, flags, etc..
- Read, write, compare, copy/paste data.
- Shell integration. Supports pipes, shell escapes, ..
- Visual mode with simple keybindings

Debugger

- Using the debugger IO plugin it's possible to natively debug programs on UNIX systems or Windows(R).
- Supports raw memory access like reading a plain file.
- Child filedescriptor manipulation
- Context dump/restore. Allows stepbacks
- Breakpoints(soft/hard), Watchpoints with expressions
- Raw DRX access
- Syscall injection and proxying
- Thread and fork control
- Execution trace
- Signal handling and manipulation
- Syscall tracing
- Mmap files on child's memory

Data analysis

- Radare comes with different tools to analyze binaries:
  - rsc rfile-foreach – runs 'file' program on each offset of the file to find file headers
  - bindiff – find binary differences between two files
  - bytediff- “”
  - hasher – multiple algorithms , hash per pieces, entropy, hamming distance ,...
  - Interprets data blocks as C data structures with 'rsc spcc'.

GML graph generation from an ELF

Exploit framework

- Radare comes with some tools to ease the development of exploits or low level code snippets to patch binaries.
  - Rasm – Radare Assembler – portable patch assembler (most common assembly opcodes) for x86, arm, ppc and java.
  - Rasc – Radare ShellCode – metasploit-like tool with syscall-proxying and hardcoded database of shellcodes. Prefixing/appending traps, nops, numeric series or 'A's.

Pid:// - Attach to programs and analyze crash backtraces.

Disassembler

- Radare supports disassembling and code analysis for intel, arm, ppc and Java.
- Supports intel, at&t and pseudocode disassembling
- The code analysis structures can be compared to bindiff code flows.
- Allows to add inline comments, allows to fake the base address to map memory addresses with file ones.
- Can mix dwarf information, and symbol information.
- ObjDump, Nas, Gas integration

Search Engine

Supports multiple binary keyword search:

- Range limited searches
- string, wide char string, hexpair, opcodes, ..
- execute commands for each result
- Supports binary masks per keyword
- Supports pseudo-regular expression
- Find expanded AES keys

GUI

- A minimalistic C based Gtk+ frontend with VTE is currently used.
- A native Vala Gtk with Cairo is under development.
- Code graphs to graphically navigate the program.

Other stuff

- rabin allows to get information from ELF, PE, CLASS files
- Read WCE/WM device's memory with HARET plugin.
- Find code xrefs on raw files for x86, ppc, arm
- Data Carver
- Assembly opcodes dictionary (rsc adict)
- Commandline assembler/disassembler (rsc asm/dasm)
- Automatization tasks with shellscripts

Q/A? || Cya!

http://radare.nopcode.org/