Exploit Development Community (Http://Expdev-Kiuhnm.Rhcloud.Com/)

Mona 2 (http://expdev-kiuhnm.rhcloud.com/2015/05/19/mona-2/)

(http://expdev-kiuhnm.rhcloud.com/2015/05/19/mona-2/)

Mona 2 is a very useful extension developed by the Corelan Team. Originally written for Immunity Debugger, it now works in WinDbg as well.

Installation in WinDbg

You'll need to install everything for both WinDbg x86 and WinDbg x64:

1. Install Python 2.7 (download it from here (https://www.python.org/downloads/))
   Install the x86 and x64 versions in different directories, e.g. c:\python27(32) and c:\python27.
2. Download the right zip package from here (http://pykd.codeplex.com/), and extract and run vcredist_x86.exe and vcredist_x64.exe.
3. Download the two exes (x86 and x64) from here (http://pykd.codeplex.com/) and execute them.
4. Download windbglib.py and mona.py from here (https://github.com/corelan) and put them in the same directories as windbg.exe (32-bit and 64-bit versions)

windbg.exe (32-bit and 64-bit versions).

5. Configure the symbol search path as follows:
    1. click on File→Symbol File Path
    2. enter

```
SRV*C:\windbgsymbols*http://msdl.microsoft.com/download/symbols
```

    3. save the workspace (File→Save Workspace).

Running mona.py under WinDbg

Running mona.py in WinDbg is simple:

1. Load the pykd extension with the command

```
.load pykd.pyd
```

2. To run mona use

```
!py mona
```

To update mona enter

```
!py mona update
```

Configuration

Working directory

Many functions of mona dump data to files created in the mona's working directory. We can specify a working directory which depends on the process name and id by using the format specifiers %p (process name) and %i (process id). For instance, type

```
!py mona config -set workingfolder "C:\mona_files\%p_%i"
```

Exclude modules

You can exclude specific modules from search operations:

```
!mona config -set excluded_modules "module1.dll,module2.dll"
!mona config -add excluded_modules "module3.dll,module4.dll"
```

Author

You can also set the author:

```
!mona config -set author Kiuhnm
```

This information will be used when producing metasploit compatible output.

Important

If there's something wrong with WinDbg and mona, try running WinDbg as an administrator.

Mona's Manual

You can find more information about Mona here (https://www.corelan.be/index.php/2011/07/14/mona-py-the-manual/).

Example

This example is taken from Mona's Manual.

Let's say that we control the value of ECX in the following code:

```
1 MOV    EAX, [ECX]
2 CALL   [EAX+58h]
```

We want to use that piece of code to jmp to our shellcode (i.e. the code we injected into the process) whose address is at ESP+4, so we need the call above to call something like "ADD ESP, 4 | RET ".
There is a lot of indirection in the piece of code above:

1. (ECX = p1) → p2
2. p2+58h → p3 → "ADD ESP,4 | RET"

First we need to find p3:

```
!py mona config –set workingfolder c:\logs
!py mona stackpivot –distance 4,4
```

The function stackpivot finds pointers to code equivalent to "ADD ESP, X | RET" where X is between min and max, which are specified through the option "-distance min,max ".
The pointers/addresses found are written to c:\logs\stackpivot.txt.
Now that we have our p3 (many p3s!) we need to find p1:

```
!py mona find –type file –s "c:\logs\stackpivot.txt" –x * –of
fset 58 –level 2 –offsetlevel 2
```

Let's see what all those options mean:

- "-x *" means "accept addresses in pages with any access level" (as another example, with "-x X" we want only addresses in executable pages).
- "-level 2" specifies the level of indirection, that is, it tells mona to find "a pointer (p1) to a pointer (p2) to a pointer (p3)".

- The first two options (-type and -s) specifies that p3 must be a pointer listed in the file "c:\logs\stackpivot.txt".
- "-offsetlevel 2" and "-offset 58" tell mona that the second pointer (p2) must point to the third pointer (p3) once incremented by 58h.

Don't worry too much if this example isn't perfectly clear to you. This is just an example to show you what Mona can do. I admit that the syntax of this command is not very intuitive, though.

Example

The command findwild allows you to find chains of instructions with a particular form.

Consider this example:

```
!mona findwild –s "push r32 # * # pop eax # inc eax # * # ret
n"
```

The option "-s" specifies the shape of the chain:

- instructions are separated with '#'
- r32 is any 32-bit register
- * is any sequence of instructions

The optional arguments supported are:

- -depth <nr>: maximum length of the chain
- -b <address>: base address for the search
- -t <address>: top address for the search
- -all: returns also chains which contain "bad" instructions, i.e. instructions that might break the chain (jumps, calls, etc…)

ROP Chains

Mona can find ROP gadgets and build ROP chains, but I won't talk about this here because you're not supposed to know what a ROP chain is or what ROP is. As I said, don't worry if this article doesn't make perfect sense to you. Go on to the next article and take it easy!

Bio | Latest Posts

Massimiliano Tomassoli

Computer scientist, software developer, reverse engineer and student of computer security (+ piano player & music composer)

Leave a Reply

2 Comments on "Mona 2"

Notify of new follow-up comments | Email | ›

Join the discussion

Sort by: newest | oldest | most voted

Guest

Tom 6 months 10 days ago

Is “2. Download the right zip package from here, and extract and run vcredist_x86.exe and vcredist_x64.exe” ‘here’ supposed to link to http://pykd.codeplex.com/ (http://pykd.codeplex.com/) as well as in step 3?

0 | Reply - Share Hide Replies ∧

Author

Massimiliano Tomassoli (http://expdev-kiuhnm.rhcloud.com/author/admin/) 6 months 10 days ago

Yes. Go to the download page and download pykd-0.2.0.29-python-2.7.zip.

0 | Reply - Share

LOG IN

Username

Password

Log In ☐ Remember Me

Lost your password? (http://expdev-kiuhnm.rhcloud.com/wp-login.php?action=lostpassword)
Register (http://expdev-kiuhnm.rhcloud.com/wp-login.php?action=register)

Search ⋯ Search

RECENT POSTS

More space on the stack (http://expdev-kiuhnm.rhcloud.com/2015/06/13/more-space-on-the-stack/)

IE11: Part 2 (http://expdev-kiuhnm.rhcloud.com/2015/06/02/ie11-part-2/)

IE11: Part 1 (http://expdev-kiuhnm.rhcloud.com/2015/06/02/ie11-part-1/)

IE10: Use-After-Free bug (http://expdev-kiuhnm.rhcloud.com/2015/06/01/ie10-use-free-bug/)

IE10: God Mode (2) (http://expdev-kiuhnm.rhcloud.com/2015/06/01/ie10-god-mode-2/)

RECENT COMMENTS

Massimiliano Tomassoli on Shellcode (http://expdev-kiuhnm.rhcloud.com/2015/05/22/shellcode/#comment-179)

Begineer on Shellcode (http://expdev-kiuhnm.rhcloud.com/2015/05/22/shellcode/#comment-178)

Massimiliano Tomassoli on IE10: God Mode (2) (http://expdev-kiuhnm.rhcloud.com/2015/06/01/ie10-god-mode-2/#comment-177)

Massimiliano Tomassoli on Shellcode (http://expdev-kiuhnm.rhcloud.com/2015/05/22/shellcode/#comment-176)

hidehamu on IE10: God Mode (2) (http://expdev-kiuhnm.rhcloud.com/2015/06/01/ie10-god-mode-2/#comment-175)

ARCHIVES

June 2015 (http://expdev-kiuhnm.rhcloud.com/2015/06/)

May 2015 (http://expdev-kiuhnm.rhcloud.com/2015/05/)

RECENT TOPICS

Problem with loading mona and windbglib (http://expdev-kiuhnm.rhcloud.com/forums/topic/problem-with-loading-mona-and-windbglib/)

Shellcode getHash confusion (http://expdev-kiuhnm.rhcloud.com/forums/topic/shellcode-gethash-confusion/)

bstr information disclosure (http://expdev-kiuhnm.rhcloud.com/forums/topic/bstr-information-disclosure/)

Trivial RE questions (http://expdev-kiuhnm.rhcloud.com/forums/topic/trivial-re-questions/)

Exploitme2 cannot find pattern.txt (http://expdev-kiuhnm.rhcloud.com/forums/topic/exploitme2-cannot-find-pattern-txt/)

RECENT REPLIES

Problem with loading mona and windbglib (http://expdev-kiuhnm.rhcloud.com/forums/topic/problem-with-loading-mona-and-windbglib/#post-1247)

Shellcode getHash confusion (http://expdev-kiuhnm.rhcloud.com/forums/topic/shellcode-gethash-confusion/#post-1228)

Shellcode getHash confusion (http://expdev-kiuhnm.rhcloud.com/forums/topic/shellcode-gethash-confusion/#post-1227)

bstr information disclosure (http://expdev-kiuhnm.rhcloud.com/forums/topic/bstr-information-disclosure/#post-1214)

bstr information disclosure (http://expdev-kiuhnm.rhcloud.com/forums/topic/bstr-information-disclosure/#post-1213)

GOOGLE ANALYTICS STATS

Powered by WordPress (http://www.wordpress.org/)