21-06-2015 14:07 #1

klaus

Exploit Development Course Part 2: Mona 2 (Перевод: klaus)

Перейти к содержанию

Введение

Mona 2 – это очень полезное и удобное расширение разработанное Corelan Team. Первоначально было написано для Immunity Debugger, но сейчас расширение также работает и в WinDbg.

Установка в WinDbg

Вам надо будет установить всё из списка как для 32-х битной версии WinDbg так и для 64-х битной:

1. Установите Python 2.7 (скачать можно отсюда)
2. Установите x86 и x64 в разные папки, к примеру c:\python27(32) и c:\python27.
3. Скачайте zip архив отсюда (кнопка для скачивания справа), распакуйте и запустите vcredist_x86.exe и vcredist_x64.exe.
4. Скачайте два исполняемых файла (x86 и x64) отсюда и запустите их на выполнение.
5. Скачайте windbglib.py и mona.py отсюда и поместите их в ту же директорию что и windbg.exe (32-х и 64-х битные версии).
6. Сконфигурируйте пути поиска символов следующим образом:
    1. Выполните File→Symbol File Path
    2. Введите:

        Code:

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

    3. Сохраните рабочее окружение (File→Save Workspace).

Запуск mona.py в WinDbg

Процесс запуска mona.py в WinDbg простой:

1. Загрузите pykd расширение следующей командой:

   Code:

   ```
   .load pykd.pyd
   ```

2. Для запуска mona используйте:

   Code:

   ```
   !py mona
   ```

Для обновления mona достаточно ввести такую команду:

Code:

```
!py mona update
```

Конфигурирование

Рабочая директория

Многие функции mona дампят данные в файлы созданные в рабочей директории mona'ы. Мы можем указать рабочую директорию расположение которой будет зависеть от форматных спецификаторов (имя процесса и его идентификатор) которые мы будем использовать при формировании пути. *%p* (process name) и *%i* (process id)это имя процесса и идентификатор соответственно.

Пример:

Code:

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

Исключение модулей

Вы можете исключить определенные модули из поисковых операций:

Code:

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

Авторство

Также можно установить автора:

Code:

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

Эта информация будет использоваться при произведении совместного вывода с metasploit.

Важное замечание

Если при настройке WinDbg и mona у Вас появились какие-то ошибки, попробуйте запустить WinDbg от имени администратора.

Руководство по Mona

Вы можете найти больше информации о Mona здесь.

Пример

Данный пример взят из документации по Mona.

Скажем, мы управляем значением регистра ECX следующим кодом:

Code:

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

Мы хотим использовать этот кусок кода с целью сделать jmp в наш шеллкод (то есть код, который мы инжектировали в процесс) адрес которого по адресу *ESP + 4*. Так что нам нужен CALL показанный выше для вызова чего-то подобного этому "*ADD ESP, 4 | RET*".

Есть много косвенных ссылок в куске кода выше:

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

Первое что нам надо, так это найти p3:

Code:

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

Функция stackpivot находить указатели на код эквивалентные "*ADD ESP, X | RET*" где значение X между min и max которые определяются через опцию "-distance min,max".

Указатели/адреса которые были найденные будут записаны в c:\logs\stackpivot.txt.

Теперь, когда у нас есть p3 (много p3!) нам надо найти p1:

Code:

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

Давайте разберем что все эти опции значат:

- "-x *" значит «принимать адреса в страницах с любым уровнем доступа» (другой подобный пример с "-x X" означает, что мы хотим только адреса в выполняемых страницах памяти).
- "-level 2" задает уровень косвенности, то есть, это говорит mona'е найти «указатель (p1) на указатель (p2) на указатель (p3)».
- Первые два параметра (-type and -s) указывают на то, что p3 должен быть указателем перечисленным в файле "c:\logs\stackpivot.txt".
- "-offsetlevel 2" и "-offset 58" говорят mona'е что второй указатель (p2) должен указывать на третий указатель (p3) как только произойдет инкремент значением 58h.

Не беспокойтесь если данный пример не слишком ясен или очевиден вам. Цель данного примера показать на что способна Mona. Но я признаю, что синтаксис этих команд не очень интуитивен.

Пример

Команда findwild позволяет Вам найти цепочку инструкций конкретного описания.

Рассмотрим этот пример:

Code:

```
!mona findwild -s "push r32 # * # pop eax # inc eax # * # retn"
```

Аргумент "*-s*" задает вид цепочки:

- Инструкции разделены символом '#'
- r32 - это любой 32-х битный регистр
- * - любая последовательность инструкций

Поддерживаемые необязательные аргументы:

- -depth <nr>: максимальная длина цепочки
- -b <address>: базовый адрес для поиска
- -t <address>: верхний адрес для поиска
- -all: также будет возвращать цепочки с некорректными инструкциями, то есть инструкции, которые могут прервать цепочку (jmp, call и т.д.)

ROP цепочки

Mona может находить ROP гаджеты (ROP gangets) и строить ROP цепочки, но я не буду говорить об этом здесь из-за того, что вы не осведомлены о том что такое ROP цепочка или что такое ROP вообще. Как я говорил ранее, не беспокойтесь о том факте, что данная статья не раскрывает много для Вас. Переходите на следующую статью и не беспокойтесь!

© Translated by **klaus (r0 Crew)**

Last edited by root; 04-07-2015 at 14:11.

Do not follow the ancient masters, seek what they sought. (c) Matsuo Bashō

Reply With Quote | Blog this Post | Спасибо

6 пользователя(ей) сказали спасибо:

Dark Koder (22-06-2015) **Darwin** (22-06-2015) **dukeBarman** (21-06-2015) nosos (21-06-2015) **root** (21-06-2015) **ximera** (21-06-2015)

+ Reply to Thread

Quick Navigation **Материалы** **Top**

« Previous Thread | Next Thread »

Tags for this Thread

commands, **how to install**, **in цштвипб monapy**, **mona 2**, **mona examples**, **rop**
View Tag Cloud

Posting Permissions

You may not post new threads BB code is On

You may not post new threads	**BB code** is On
You may not post replies	**Smilies** are On
You may not post attachments	**[IMG]** code is On
You may not edit your posts	HTML code is Off

Forum Rules