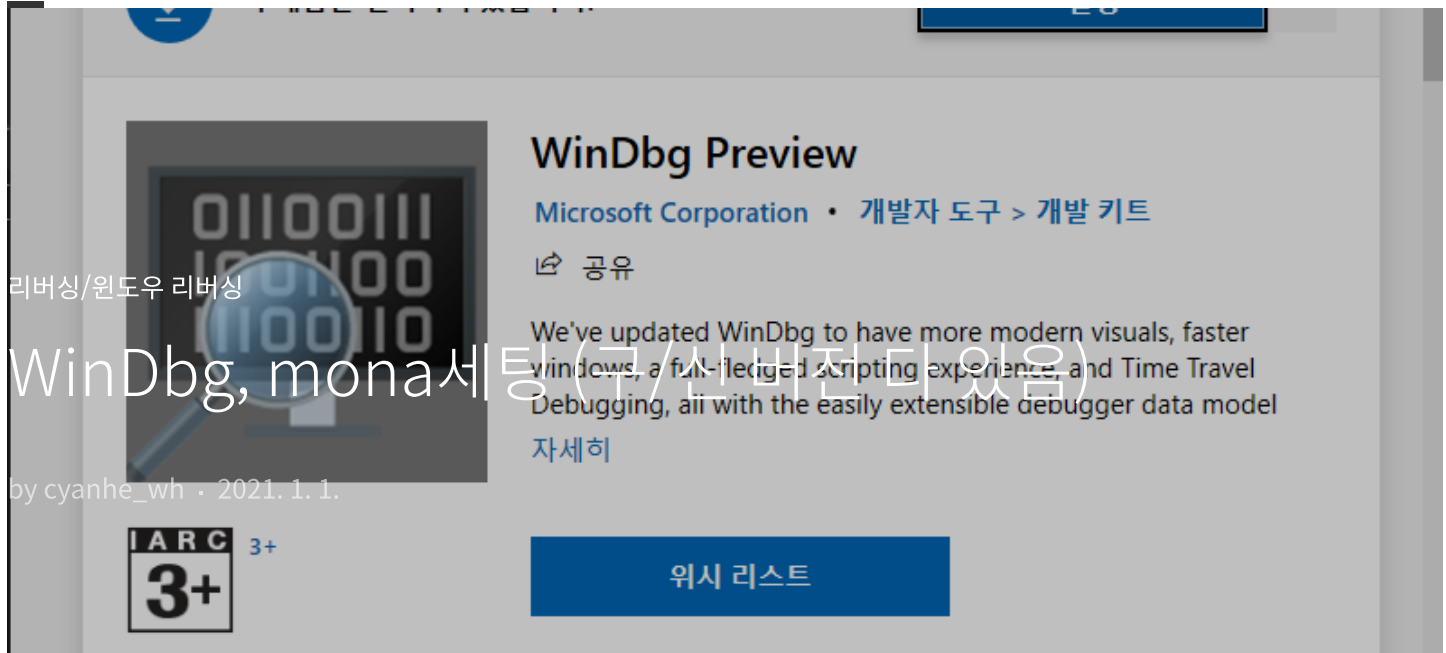


홈



kakaoAdFit

kakaoAdFit

WinDbg Preview 세팅 (최신 버전)

최신 버전은 Microsoft Store에서 다운을 받을 수 있다. App 형태로 나왔다.
검색 창에 WinDbg Preview를 검색하면 나온다.

분류 전체보기

프로그래밍

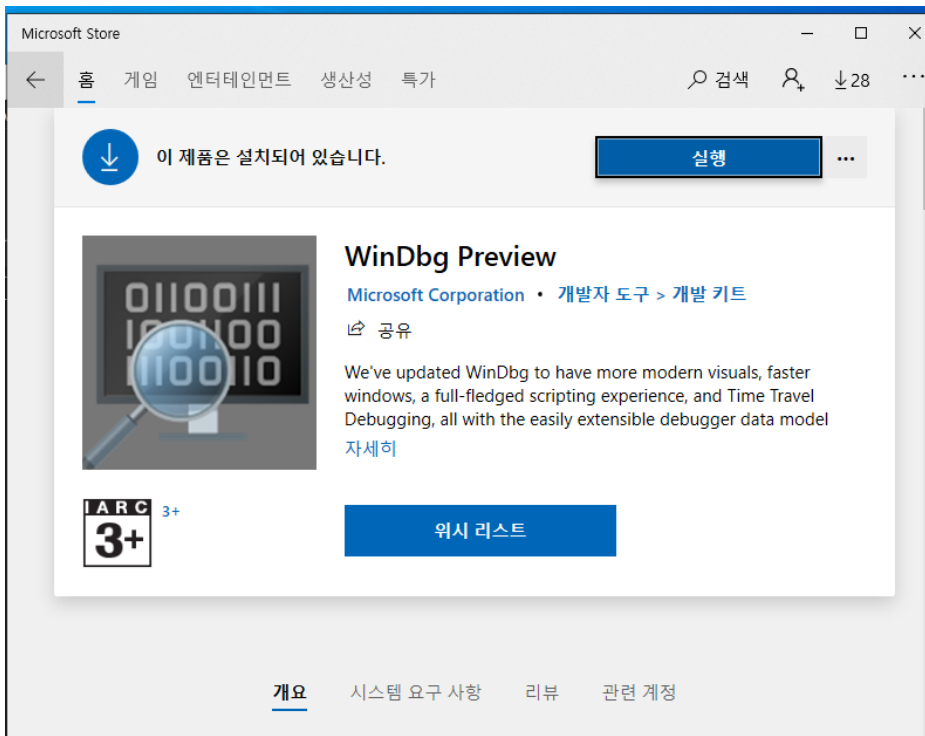
- C언어를 활용한 네트워크 해킹
- Android
- C 언어
- python
- C++
- nodejs

리버싱

- 윈도우 리버싱
- ARM

시스템해킹&보안

- 윈도우 메모리 보호기법
- 리눅스 메모리 보호기법



여기서 설치하면 우선 WinDbg는 설치가 끝난다.

들어가서 symph는 .symfix, .sympath 명령어를 입력하면 자동으로 path가 마이크로 소프트 주소로 세팅된다.

아니면 설정에 들어가서 직접 입력해도된다.

구 버전은 프로그램의 x86, x64 버전이 나뉘어져 있지만 최신 버전인 하나로 다 가능하다.

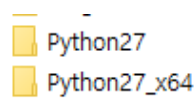
대신 취약점 분석 시 확장 프로그램으로 python이나 mona 같은 툴을 사용할 때, 분석하는 파일이 지원하는 아키텍처에 맞춰 사용해야한다.

(예를 들어 x86 파일을 분석하면, python도 x86으로, x64 파일 분석이면, python도 x64로 사용해야한다.)

mona 세팅

1. python을 설치한다. (2.7 버전으로) 3버전은 다른 것은 지원하지만 mona가 지원을 안한다.

설치할 때 x86, x64 둘다 설치한다.



두 개를 설치하므로 구분되게 폴더 이름을 지어준다. 처음 설치할 때 정하고 수정하지말아야 한다. 나중에 수정하면 Windbg가 잡지못할 수 있다.

2. pip 명령어를 이용해 pykd 모듈을 설치하자.

윈도우 해킹

리눅스 해킹

웹 해킹&보안

SQLInjection

WarGame

LOB(The Lord of the BOF)

Webhacking.kr

pwnable.kr

시스템

윈도우

리눅스

CTF(Capture The Flag)

XMAS 2020

zeroptri 2021

Line 2021

공지사항

최근글 인기글

safe_vector

2021.04.07



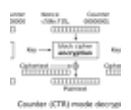
babycrypto3

2021.03.22



babycrypto2

2021.03.22



babycrypto1

2021.03.22



baby sqli

2021.03.12



최근댓글

dest가 아니라 src길이를 ...

ca. C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Python27_x64>python -m pip install --upgrade pykd
```

x86, x64 둘다 해줘야한다.

3. mona, windbglib, pykd.dll 다운받기

- github.com/corelano/mona (mona.py)
- github.com/corelano/windbglib (windbglib)
- github.com/pykd/pykd-ext/-/wikis/Downloads(pykd.dll)

여기서 필요한 파일

1. mona.py
2. windbglib에 있는 (pykd03.zip파일에 있는 msdia120.dll)
3. pykd.dll (x86, x64 둘 다, 이름을 바꿔서 구분해 주는 것이 좋다.)

다운을 받아서 msdia120.dll은 regsvr32 명령어를 통해서 등록을 할 것이다.

할 때 관리자 권한으로 cmd에서 해야 성공한다. 그렇지 않으면 계속 실패할 것이다.

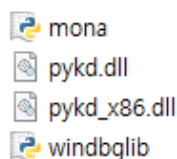
이것을 해야 mona가 실행이 된다.

```
C:\Users\User\Desktop\tools>regsvr32 msdia120.dll
```

이제 세팅은 거의 다 끝났다.

구버전에서는 사용할 파일들을 로드하거나 실행할 때 편하게 하기 위해 WinDbg의 경로에 넣어둔다. 그런데 최신버전은 App이다보니 경로가 막혀있다. 권한을 줘서 마음대로 변경해 할 수 있지만, 잘못하면 App에 대한 오류가 발생할 수 있으므로 그냥 편한 경로를 통해 사용하는 것을 추천한다.

필요한 파일들을 로컬 디스크 C 최상의 경로에 가져다 둘 것이다.



여기다 두면 경로지정이 편하다.

안녕하세요. 위 자료는 제...

안녕하세요 글쓴이님. 실...

태그

Reversing,

out of bound, 웹해킹,

aarch64,

Arbitrary File Read,

프로세서 상태 레지스터,

실행 상태, 레지스터,

특수 목적 레지스터,

Canary Leak, WinDBG,

webhacking.kr, Crypto,

시스템 레지스터, nodejs,

ARM, 실행상태변경,

익셉션 레벨 변경,

Uninitialized Variable,

web, ARMv8,

Exception Model, pwn,

AES, Stack Overflow,

pwnable.kr, Windows,

Exception Level, PE,

DOS 스택

전체 방문자

21,764

Today : 24

Yesterday : 26

```

77000002 cc          int      3
0:000> .load C:\pykd_x86
0:000> !py
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:19:08) [MSC v.1500 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
(InteractiveConsole)
>>>
Input>

```

우선 x86 파일부터 pykd 파일도 잘 로드가 되고 파이썬도 32bit로 실행된다.

```

>>> 0:000> !py C:\mona
*****
You are running a newer version of pykd.pyd
mona.py was tested against v0.2.0.29
and not against v0.3.4.15
This version may not work properly.
If you are having issues, I recommend to download the correct version from
https://github.com/corelan/windbglib/raw/master/pykd/pykd.zip
(unzip with 7zip)

NOTE: PyKD v0.3.4.15 requires msdia120.dll, which only gets installed via
Alternatively, you can use the copy of msdia120.dll from the pykd.pyd file
(https://github.com/corelan/windbglib/raw/master/pykd/pykd03.zip), but u
*****
Hold on...
[+] Command used:
!py C:\mona.py
'mona' - Exploit Development Swiss Army Knife - WinDBG (32bit)
Plugin version : 2.0 r613
Python version : 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:19:08) [
PyKD version 0.3.4.15
Written by Corelan - https://www.corelan.be
Project page : https://github.com/corelan/mona

-----
|  /  _  \  _  V  _  V  _  V  _  \  https://www.corelan.be
| //  /  /  /  /  /  /  /  /  /  /  https://www.corelan-training.com
| //  /  /  \  \  \  \  \  \  \  \  #corelan (Freenode IRC)

```

mona도 잘 실행된다.

```

00007ff9`0c3bf780 cc          int      3
0:000> .load C:\pykd
0:000> !py
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
(InteractiveConsole)
>>>
[4]

```

이제 x64 파일을 열어서 pykd와 python을 실행해봤다. 잘 로드가 되고 python도 64bit로 잘 실행된다.

```
>>> 0:000> !py C:\mona
*****
You are running a newer version of pykd.pyd
mona.py was tested against v0.2.0.29
and not against v0.3.4.15
This version may not work properly.
If you are having issues, I recommend to download the correct version from
https://github.com/corelan/windbglib/raw/master/pykd/pykd.zip
(unzip with 7zip)

NOTE: PyKD v0.3.4.15 requires msdia120.dll, which only gets installed via
Alternatively, you can use the copy of msdia120.dll from the pykd.pyd file
(https://github.com/corelan/windbglib/raw/master/pykd/pykd03.zip), but us
*****
Hold on...
[+] Command used:
!py C:\mona.py
'mona' - Exploit Development Swiss Army Knife - WinDBG (64bit)
Plugin version : 2.0 r613
Python version : 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [P
PyKD version 0.3.4.15
Written by Corelan - https://www.corelan.be
Project page : https://github.com/corelan/mona
-----
mona.py
```

mona도 x64에서 실행이 잘된다.

이렇게 세팅이 끝났다!!

WinDbg (구 버전)

구버전은 신 버전하고 다른 것은 별거 없다.

우선 WinDbg 설치하는 docs.microsoft.com/ko-kr/windows-hardware/drivers/debugger/debugger-download-tools 사이트에 들어가서 Windows 10 SDK 링크를 들어간다.



Debugging Tools for Windows 10 (WinDbg)

Get Debugging Tools for Windows (WinDbg) from the SDK: [Windows 10 SDK](#). Use the download link on the [Windows 10 SDK](#) page, as the Debugging Tools for Windows are not available as part of Visual Studio.

If you just need the Debugging Tools for Windows, and not the Windows Driver Kit (WDK) for Windows 10, you can install the debugging tools as a standalone component from the Windows Software Development Kit (SDK).

In the SDK installation wizard, select **Debugging Tools for Windows**, and deselect all other components.

시작

Windows 10 SDK는 두 가지 방법으로 다운로드할 수 있습니다. 한 가지 방법은 이 페이지 관리자의 선택적 구성 요소에서 "Windows 10 SDK(10.0.19041.0)"를 선택하여 설치하

이 SDK를 설치하기 전에 다음을 수행합니다.

1. 모든 [시스템 요구 사항](#) 을 검토합니다.
2. 설치하기 전에 Visual Studio 2019를 종료합니다.
3. [릴리스 정보 및 알려진 문제](#) 를 검토합니다.

설치 관리자 다운로드 >

[.ISO 다운로드 >](#)

20/12/16 업데이트됨

여기서 설치파일을 다운받는다.



설치하면 체크하는게 나오는데 Debugging Tools for Windows만 체크해서 설치하면 Windbg가 깔린다. 깔면 x64, x86 둘다 깔린다.

이제 세팅하는 방법은 신버전하고 같은데 좀더 파일을 편하게 로드나 실행하기 위해서는 설치된 경로에 파일을 가져다 두는 것이다.

우선 Windbg가 깔리면 C:\Program Files (x86)에 깔린다.

pykd.dll (x64 파일)은 C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\winext

pykd.dll (x86 파일)은 C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\winext

mona.py은

C:\Program Files (x86)\Windows Kits\10\Debuggers\x64

C:\Program Files (x86)\Windows Kits\10\Debuggers\x86

다 복사해야한다.

해당 경로에 다 해두면 로드나 실행할 때 경로 지정을 안해도 된다.

ex) .load pykd, !py mona

kakaoAdFit

♡ 공감 000

구독하기



'리버싱 > 윈도우 리버싱' 카테고리의 다른 글

RVA와 섹션 (0)	2021.01.21
PE 파일의 전체 구조 (0)	2021.01.21
PE 파일 (0)	2021.01.17
<u>WinDbg, mona세팅 (구/신 버전 다 있음)</u> (0)	2021.01.01
WinDbg Preview (0)	2020.12.31
디버깅 환경 (0)	2020.12.29

태그

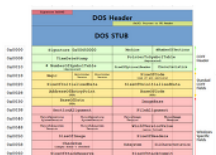
Mona

pykd

WinDBG

WinDbg Preview

관련글



PE 파일의 전체 ...

PE 파일

WinDbg Preview

디버깅 환경

댓글 0

이름

비밀번호

여러분의 소중한 댓글을 입력해주세요.

☐ 비밀글

등록



