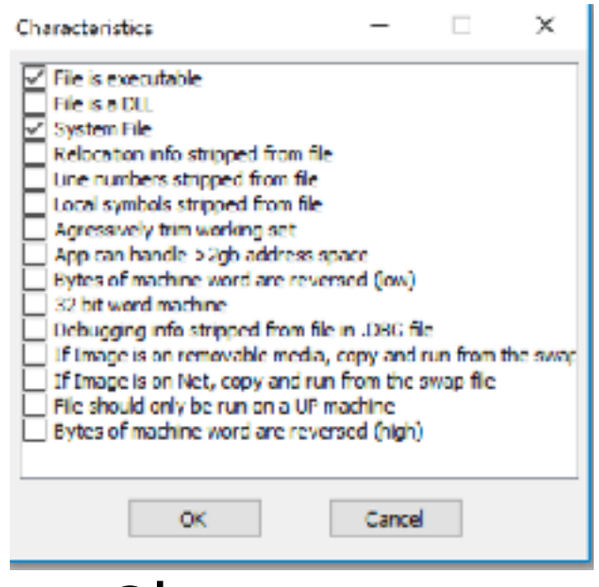
리버싱 3주차

이응창

broken.exe

- 과제는 broken.exe와 iat_broken.exe를 복구 하는 것이다. 먼저 broken.exe를 복구 해보자.

broken.exe



- 그때 배웠던 file_header의 file_executable_image와 32bit_image의 or연산으로 나타나지는 것을 참조해 보았을 때, 이 파일에선 file_executable_image와 system_file이 체크되어 있는 것으로 보았을 때, or 연산으로 0x1002가 되어야 하는데 characteristic에는 2002가 적혀 있다. 무언가 잘못 됨을 깨닫고, 수정해주고 실행해보았다.

broken.exe

```
C:WUsersWLee EungChang>cd C:WUsersWLee EungChangWDesktopWreversing

C:WUsersWLee EungChangWDesktopWreversing>broken.exe
Hell, World
C:WUsersWLee EungChangWDesktopWreversing>_
```

- 간단하게 성공했다.

iat_broken.exe

- 일단 얘는 제목부터 iat가 부서졌다고 하는데 iat에 무언가 문제가 있나보다 생각하고 들어간다.

iat_broken.exe

Import Directory RVA	00000180	Dword	00012054	.rdata
Import Directory Size	00000184	Dword	00000028	

pFile	Data	Description	Value
00010854	0001207C	Import Name Table RVA	
00010858	00000000	Time Date Stamp	
0001085C	00000000	Forwarder Chain	
00010860	000122D6	Name RVA	KERNEL32.dll
00010864	0000D000	Import Address Table RVA	

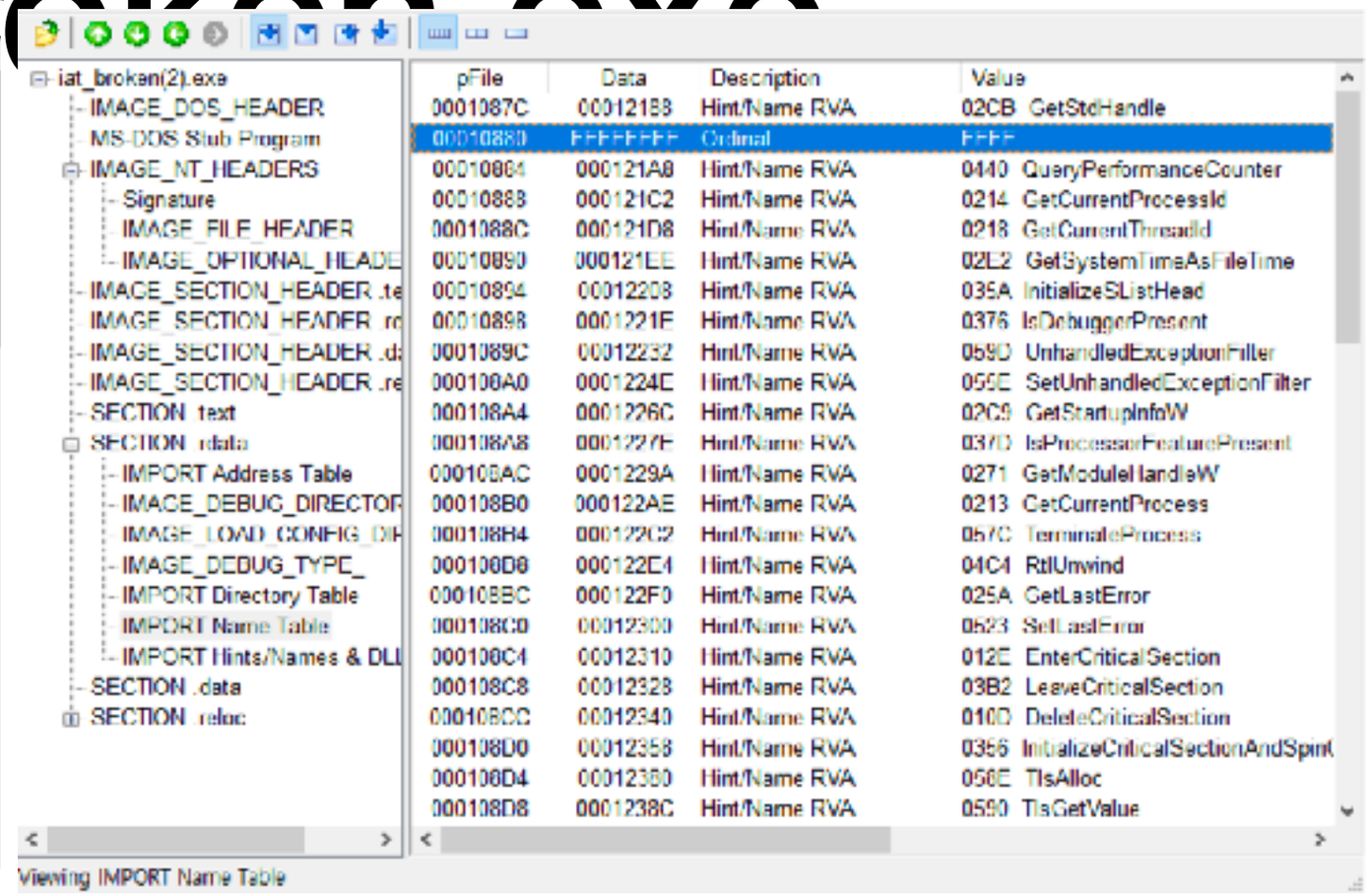
- 자 일단, import name table RVA 는 import directory RVA 에 import directory size를 더한 값과 같다는 것을 PE view에서 확인이 가능하다. 0x12054 + 0x28 = 0x1207C 이다.
- 그리고 image import descriptor 구조체 배열의 시작주소는 import name table RVA가 됨을 알았다.
- 그리고 original first thunk는 import name table RVA를 나타내며 0x1207C임을 알았다.
- IID의 name은 0x122D6. 그리고 IAT의 RVA 주소인 first thunk는 0xD000이란 것 까지 알았다.

iat_broken.exe

- pe view에서 section(.rdata)에서 IAT와 INT 확인이 가능하다.
- ppt에서 설명해놓은 대로 본다면 IIBN(image import by name)은 INT의 구조체 인데 IAT도 초기 상태에는 IIBN 구조체를 가르켜야 한다. 구해올 함수의 실제 주소를 얻어오면 IAT는 overwrite 되는 식이다.

iat_broken.exe

pFile	Data	Description	Value
0000B800	00012188	Hint/Name RVA	02CB GetStdHandle
0000B804	00012198	Hint/Name RVA	05FA WriteConsoleA
0000B808	000121A8	Hint/Name RVA	0440 QueryPerformanceCounter
0000B80C	000121C2	Hint/Name RVA	0214 GetCurrentProcessId
0000B810	000121D8	Hint/Name RVA	0218 GetCurrentThreadId
0000B814	000121EE	Hint/Name RVA	02E2 GetSystemTimeAsFileTime
0000B818	00012208	Hint/Name RVA	035A InitializeSListHead
0000B81C	0001221E	Hint/Name RVA	0376 IsDebuggerPresent
0000B820	00012232	Hint/Name RVA	059D UnhandledExceptionFilter
0000B824	0001224E	Hint/Name RVA	055E SetUnhandledExceptionFilter
0000B828	0001226C	Hint/Name RVA	02C9 GetStartupInfoW
0000B82C	0001227E	Hint/Name RVA	037D IsProcessorFeaturePresent
0000B830	0001229A	Hint/Name RVA	0271 GetModuleHandleW
0000B834	000122AE	Hint/Name RVA	0213 GetCurrentProcess
0000B838	000122C2	Hint/Name RVA	057C TerminateProcess
0000B83C	000122F4	Hint/Name RVA	04C4 RtlUnwind
0000B840	000122F0	Hint/Name RVA	025A GetLastError
0000B844	00012300	Hint/Name RVA	0523 SetLastError
0000B848	00012310	Hint/Name RVA	012E EnterCriticalSection
0000B84C	00012328	Hint/Name RVA	03B2 LeaveCriticalSection
0000B850	00012340	Hint/Name RVA	010D DeleteCriticalSection
0000B854	00012358	Hint/Name RVA	0356 InitializeCriticalSectionAndSpinC
0000B858	00012380	Hint/Name RVA	058E TlsAlloc
0000B85C	0001238C	Hint/Name RVA	0590 TlsGetValue



- 두개 띄어놓고 보았는데 저기 FFFFFF구간이 무언가 수상하다. 왜 저렇게 되어있을까 누가봐도 심상치 않다.

iat_broken.exe

- 그러면 원래는 IAT도 초기상태에는 IIBN 구조체를 가르켜야 하기에 바꿔줘야 할 필요성이 생겼다.

iat_broken.exe

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00012188	00012188	02CB	GetStdHandle
00012198	00012198	05FA	WriteConsoleA

- 자 저기 원래 FFFF값이 들어가있었는데 00012198로 맞춰줍니다.

iat_broken.exe

- 패치 후 저장하니 관리자 권한으로 파일이 생성됩니다. 그래서, 관리자 권한으로 cmd를 열어서 실행시켜주니 정상적으로 파일에서 hell,world가 출력됩니다. 완료~!