

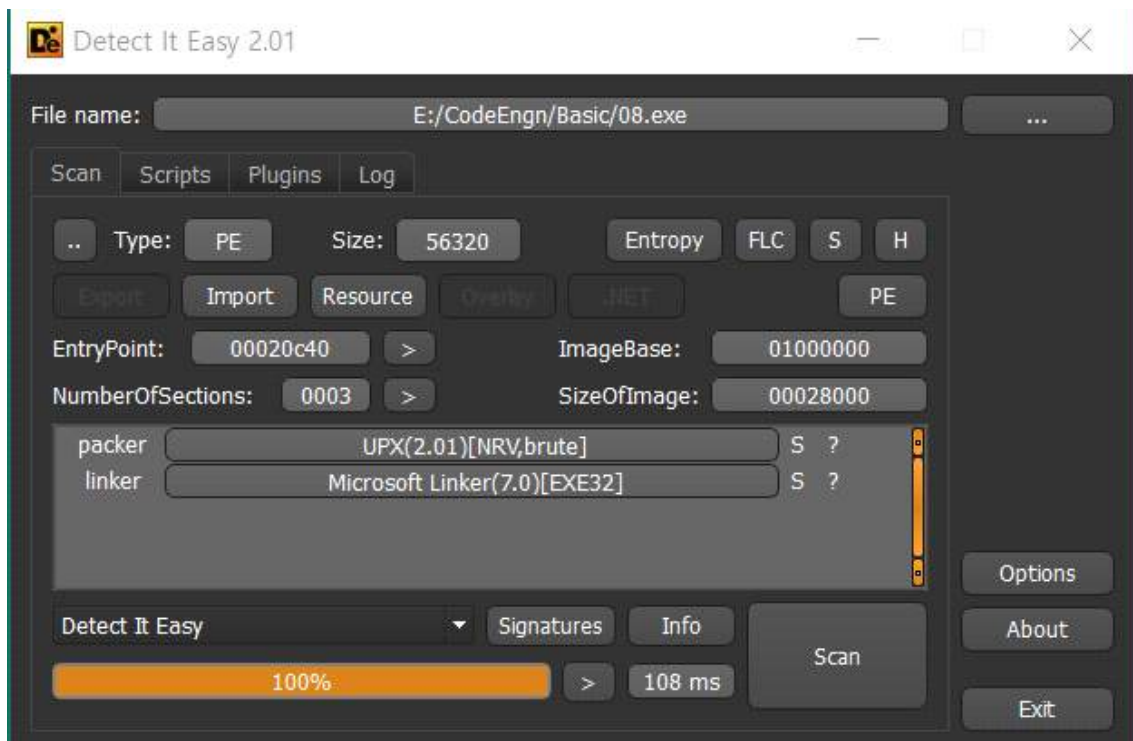
2019.02.14. CodeEngn RCE L08

Tree to Tree



OEP구하는 문제

OEP는 리얼 EP(EntryPoint)라고 할 수 있다.



또 UPX! 버전은 다르다 2.01버전! UPX는 모든버전 언팩하는게 똑같다.

pushad에 breakpoint를 걸고

주소	Module/Label/Exception	상태	디스어셈블리	Hits	Summary
01020C40	<08.exe.EntryPoint>	One-time	pushad	0	진입점 중단점

popad를 찾으로 밑으로 쭉욱 내리면

popad아래부분에 jmp 명령어에 breakpoint걸고

01020DBD	61	popad
01020DBE	8D 44 24 80	lea eax, dword ptr ss:[esp-80]
01020DC2	6A 00	push 0
01020DC4	39 C4	cmp esp, eax
01020DC6	75 FA	jne 08.1020DC2
01020DC8	83 EC 80	sub esp, FFFFFFF80
01020DCB	E9 A5 16 FF FF	jmp 08.1012475

실행 후 점프 하면 OPE를 찾을 수 있다.

01012475	6A 70	push 70	
01012477	68 E0 15 00 01	push 08.10015E0	
0101247C	E8 47 03 00 00	call 08.10127C8	
01012481	33 DB	xor ebx, ebx	
01012483	53	push ebx	
01012484	8B 3D 20 10 00 01	mov edi, dword ptr ds:[<&GetModuleHandleA>]	edi:EntryPoint
0101248A	FF D7	call edi	edi:EntryPoint
0101248C	66:81 38 4D 5A	cmp word ptr ds:[eax], 5A4D	
01012491	75 1F	jne 08.1012482	
01012493	8B 48 3C	mov ecx, dword ptr ds:[eax+3C]	ecx:EntryPoint
01012496	03 C8	add ecx, eax	ecx:EntryPoint
01012498	81 39 50 45 00 00	cmp dword ptr ds:[ecx], 4550	ecx:EntryPoint
0101249E	75 12	jne 08.1012482	
010124A0	0F B7 41 18	movzx eax, word ptr ds:[ecx+18]	
010124A4	3D 08 01 00 00	cmp eax, 108	
010124A9	74 1F	je 08.10124CA	
010124AB	3D 08 02 00 00	cmp eax, 208	

OEP 01012475