

Flag:

"NtQu3ry1nf0rm@t10nPr0(355R@!s33xc3pt!onD3bugPr1v1l3g3
St@ckT1m3CCS3lf-P3BF1ndW1nd0wH1d1ng@nt1-R3v3rs3"

Mô tả:

- Chương trình kiểm tra xem có trong chế độ debug k? có => exit
- Chương trình tồn tại lỗi => sinh lỗi => lỗi, exit
- Cần tìm input đầu vào sao cho sau khi press "check" button, ta thu được 100

Debug - danh sách lỗi và sửa lỗi:

1. SetUnhandledExceptionFilter

0040103F	8BF8	mov edi,eax	edi:EntryPoint
00401041	E8 58080000	call <JMP.&SetUnhandledExceptionFilter>	edx:EntryPoint, edi:EntryPoint
00401046	8BD7	mov edx,edi	
00401048	F7F0	div eax	
0040104A	86C6	xchg dh,al	
0040104C	25 FFFF0000	and eax,FFFF	
00401051	A9 DF000000	test eax,DF	
00401056	75 F0	jne antidebug.401048	
00401058	33C0	xor eax,eax	
0040105A	8B00	mov eax,dword ptr ds:[eax]	

- Khi debug, hàm trả về NULL (0) => eax = 0 => lỗi khi div eax
- 0x401056: Nếu khác không => nhảy đến 0x401048 (div eax)
=> bỏ qua 2 lệnh này, jmp đến phần lệnh tiếp theo

0040103F	8BF8	mov edi,eax	
00401041	E8 58080000	call <JMP.&SetUnhandledExceptionFilter>	
00401046	8BD7	mov edx,edi	
00401048	EB 12	jmp antidebug.40105C	
0040104A	86C6	xchg dh,al	
0040104C	25 FFFF0000	and eax,FFFF	
00401051	A9 DF000000	test eax,DF	
00401056	EB 04	jmp antidebug.40105C	
00401058	33C0	xor eax,eax	
0040105A	8B00	mov eax,dword ptr ds:[eax]	
0040105C	6A 00	push 0	
0040105E	E8 05080000	call <JMP.&GetModuleHandleA>	

2. Bug

00401771	66:F7D3	not bx	
00401774	66:3B1D 0F324000	cmp bx,word ptr ds:[40320F]	0040320F: " ""
00401778	74 07	je antidebug.401784	
0040177D	6A 00	push 0	
0040177F	E8 CC000000	call <JMP.&ExitProcess>	
00401784	61	popad	
00401785	5D	pop ebp	

=> je thành jmp

00401771	66:F7D3	not bx	
00401774	66:3B1D 0F324000	cmp bx,word ptr ds:[40320F]	0040320F: " ""
00401778	EB 07	jmp antidebug.401784	
0040177D	6A 00	push 0	
0040177F	E8 CC000000	call <JMP.&ExitProcess>	
00401784	61	popad	
00401785	5D	pop ebp	
00401786	C2 0800	ret 8	

3. IsDebuggerPresent

- return 0, nếu process không chạy trong luồng debug
- return khác 0, nếu process chạy trong luồng debug

0040114F	FF35 20374000	push dword ptr ds:[403720]	
00401155	E8 74070000	call <JMP.&SendMessageA>	
0040115A	E8 1B070000	call <JMP.&IsDebuggerPresent>	
0040115F	85C0	test eax, eax	
00401161	0F85 EF000000	jne antidebug.401256	
00401167	64:8B1D 30000000	mov ebx, dword ptr ds:[30]	
0040116E	837B 68 00	cmp dword ptr ds:[ebx+68], 0	
00401172	0F85 DE000000	jne antidebug.401256	
00401178	8B43 18	mov eax, dword ptr ds:[ebx+18]	
0040117B	8378 0C 02	cmp dword ptr ds:[eax+C], 2	
0040117F	0F85 D1000000	jne antidebug.401256	
00401185	8378 10 00	cmp dword ptr ds:[eax+10], 0	
00401189	0F85 C7000000	jne antidebug.401256	
0040118F	8D35 9A104000	lea esi, dword ptr ds:[40109A]	esi:EntryPoint
00401195	B0 47	mov al, 47	47: 'G'
00401197	0205 09324000	add al, byte ptr ds:[403209]	

=> return khác 0 => jne True khi chạy debug.

- 0x401256: exit process

=> jmp or nop it

Breakpoint Not Set	FF35 20374000	push dword ptr ds:[403720]	
00401155	E8 74070000	call <JMP.&SendMessageA>	
0040115A	E8 1B070000	call <JMP.&IsDebuggerPresent>	
0040115F	85C0	test eax, eax	
00401161	90	nop	
00401162	90	nop	
00401163	90	nop	
00401164	90	nop	
00401165	90	nop	
00401166	90	nop	
00401167	64:8B1D 30000000	mov ebx, dword ptr ds:[30]	
0040116E	837B 68 00	cmp dword ptr ds:[ebx+68], 0	
00401172	90	nop	
00401173	90	nop	
00401174	90	nop	
00401175	90	nop	
00401176	90	nop	
00401177	90	nop	
00401178	8B43 18	mov eax, dword ptr ds:[ebx+18]	[ebx+18]: "Q%43÷"
0040117B	8378 0C 02	cmp dword ptr ds:[eax+C], 2	
0040117F	0F85 D1000000	jne anti6.401256	
00401185	8378 10 00	cmp dword ptr ds:[eax+10], 0	
00401189	90	nop	
0040118A	90	nop	
0040118B	90	nop	
0040118C	90	nop	
0040118D	90	nop	
0040118E	90	nop	
0040118F	8D35 9A104000	lea esi, dword ptr ds:[40109A]	esi:EntryPoint
00401195	B0 47	mov al, 47	47: 'G'

4. ZwQueryInformationProcess

- Trả về thông tin về process

0040120D	C705 14374000 000	mov dword ptr ds:[403714], 0	
00401217	6A 00	push 0	
00401219	6A 04	push 4	
0040121B	68 14374000	push antidebug.403714	
00401220	6A 07	push 7	
00401222	6A FF	push FFFFFFFF	
00401224	E8 FD050000	call <JMP.&ZwQueryInformationProcess>	
00401229	85C0	test eax, eax	
0040122B	75 29	jne antidebug.401256	
0040122D	8D35 A4104000	lea esi, dword ptr ds:[4010A4]	esi:EntryPoint

=> return khác 0, là port dùng để debug

=> jne True => exit

=> nop or jump

00401208	A3 0C374000	mov dword ptr ds:[40370C],eax	
0040120D	C705 14374000 000	mov dword ptr ds:[403714],0	
00401217	6A 00	push 0	
00401219	6A 04	push 4	
0040121B	68 14374000	push anti6.403714	
00401220	6A 07	push 7	
00401222	6A 00	push 0	
00401224	E8 FD050000	call <JMP.&ZwQueryInformationProces	
00401229	85C0	test eax,eax	
0040122B	EB 00	jmp anti6.40122D	
0040122D	8D35 A4104000	lea esi,dword ptr ds:[4010A4]	
00401233	B0 4F	mov al,4F	4F: 'O'
00401235	0205 14374000	add al,byte ptr ds:[403714]	

5. ZwSetInformationThread

Ở debug, thread được tạo ra dừng gửi thông báo về các debug event

00401529	9C	pusnra	
0040152A	6A 00	push 0	
0040152C	6A 00	push 0	
0040152E	6A 11	push 11	
00401530	6A FE	push FFFFFFFE	
00401532	E8 F5020000	call <JMP.&ZwSetInformationThread>	
00401537	FF75 08	push dword ptr ss:[ebp+8]	
0040153A	E8 6B030000	call <JMP.&strlen>	
0040153E	A3 10374000	mov dword ptr ds:[403710],eax	

=> jmp bỏ qua lệnh này

00401528	60	pushad	
00401529	9C	pushfd	
0040152A	EB 0B	jmp anti6.401537	
0040152C	6A 00	push 0	
0040152E	6A 11	push 11	
00401530	6A FE	push FFFFFFFE	
00401532	E8 F5020000	call <JMP.&ZwSetInformationThread>	
00401537	FF75 08	push dword ptr ss:[ebp+8]	
0040153A	E8 6B030000	call <JMP.&strlen>	
0040153F	A3 10374000	mov dword ptr ds:[403710],eax	
00401544	8B4D 10	mov ecx,dword ptr ss:[ebp+10]	
00401547	304D 18	cmp dword ptr ss:[ebp+18],ecx	

6. CheckRemoteDebuggerPresent

- return 0, nếu không ở debug
- return khác 0, nếu ở debug

0040135C	C501	lds eax,tword ptr ds:[ecx]	ecx: EntryPoint
0040135E	0000	add byte ptr ds:[eax],al	
00401360	68 14374000	push antidebug.403714	
00401365	6A FF	push FFFFFFFF	
00401367	E8 C6040000	call <JMP.&CheckRemoteDebuggerPres	
0040136C	833D 14374000 00	cmp dword ptr ds:[403714],0	
00401373	0F85 DDFEFFFF	jne antidebug.401256	
00401379	0BC0	or eax,eax	
0040137B	0E9405 0A324000	sete byte ptr ds:[40320A]	

=> jmp or nop lệnh jne

0040135C	C501	lds eax,tword ptr ds:[ecx]	
0040135E	0000	add byte ptr ds:[eax],al	
00401360	68 14374000	push antidebug.403714	
00401365	6A FF	push FFFFFFFF	
00401367	E8 C6040000	call <JMP.&CheckRemoteDebuggerPres	
0040136C	833D 14374000 00	cmp dword ptr ds:[403714],0	
00401373	90	nop	
00401374	90	nop	
00401375	90	nop	
00401376	90	nop	
00401377	90	nop	
00401378	90	nop	
00401379	0BC0	or eax,eax	
0040137B	0F9405 0A324000	sete byte ptr ds:[40320A]	

7. bug (from GetTickCount)

0040107C	E8 F3070000	call <JMP.&GetTickCount>
00401081	2B05 18374000	sub eax,dword ptr ds:[403718]
00401087	3D 2C010000	cmp eax,12C
0040108C	76 07	jbe antidebug.401095
0040108E	6A 00	push 0
00401090	E8 BB070000	call <JMP.&ExitProcess>
00401095	E8 2F000000	call antidebug.4010C9
0040109A	EA CB87DAD2 EB88	jmp far 88EB:D2DA87CB
004010A1	D4 8A	aam 8A

=> jbe thành jmp

0040107C	E8 F3070000	call <JMP.&GetTickCount>
00401081	2B05 18374000	sub eax,dword ptr ds:[403718]
00401087	3D 2C010000	cmp eax,12C
0040108C	EB 07	jmp antidebug.401095
0040108E	6A 00	push 0
00401090	E8 BB070000	call <JMP.&ExitProcess>
00401095	E8 2F000000	call antidebug.4010C9
0040109A	AD	lodsd
0040109B	8CC0	mov eax,es
0040109D	9D	nonfd

Tìm flag:

- Đoạn compare:

0040141A	A1 0C374000	mov eax,dword ptr ds:[40370C]	64: 'd'
0040141F	83F8 64	cmp eax,64	64: 'd'
00401422	72 0A	jnb antidebug.40142E	edi: "2345678", 004034E0: "12345678"
00401424	C705 0C374000 640	mov dword ptr ds:[40370C],64	esi: "tQu3ryInf0rm@t10nPr0(355R@!s33xc3pt!onD3bugPr1v1l3g3St
00401428	8B0D 0C374000	mov ecx,dword ptr ds:[40370C]	
00401434	8D3D E0344000	lea edi,dword ptr ds:[4034E0]	
0040143A	8D35 01304000	lea esi,dword ptr ds:[403001]	
00401440	FC	cld	
00401441	F3:A6	repe cmpsb	
00401443	290D 0C374000	sub dword ptr ds:[40370C],ecx	

=> ecx = value[0x40370C] = len(input)
edi point to [0x4034E0] = input
esi point to [0x403001] = "flag"

=> output: number of compared character in input (until end of input or not equal)

=> flag:

"NtQu3ryInf0rm@t10nPr0(355R@!s33xc3pt!onD3bugPr1v1l3g3St@ckT
1m3CCS3lf-P3BF1ndW1nd0wH1d1ng@nt1-R3v3rs3"