

Flag: “vcstraining{Running_in_VM_is_ridiculous}”

Mô tả:

- Input được truyền khi gọi chương trình
- Với mỗi chuỗi đầu vào, xâu đầu ra khác nhau
- Khi chạy tại máy thật, ta nhận được gợi ý: “Congratulation! Use this password to unlock the flag: BROKENVM (Pass it as argument)” (str0)
- Khi chạy tại máy ảo, chương trình kiểm tra và làm đầu vào mặc định để tạo ra chuỗi đầu ra thay đổi, không nhận được str0

=> Vô hiệu hóa / làm chương trình không kiểm tra được việc chương trình đang chạy trên máy ảo

Debug - Danh sách lỗi và sửa lỗi

1. Compare “VMWARE”

```
00A31AAB C785 4CF5FFFF 4834A3 mov dword ptr ss:[ebp-AB4],antix1.A3344
00A31AB5 C785 50F5FFFF 6C32A3 mov dword ptr ss:[ebp-AB0],antix1.A3326
00A31ABF 90 nop
00A31AC0 FF76 04 push dword ptr ds:[esi+4]
00A31AC3 8B56 FC mov edx,dword ptr ds:[esi-4]
00A31AC6 FF36 push dword ptr ds:[esi]
00A31AC8 E8 E3F9FFFF call antix1.A31480
00A31ACD 83C4 08 add esp,8
00A31AD0 85C0 test eax,eax
00A31AD2 74 01 je antix1.A31AD5
00A31AD4 47 inc edi
00A31AD5 83C6 0C add esi,C
00A31AD8 83EB 01 sub ebx,1
00A31ADB 75 E3 jne antix1.A31AC0
00A31AE0 8B9D 8BF5FFFF mov ebx,dword ptr ss:[ebp-A48]
00A31AE3 8A87 283BA300 mov al,byte ptr ds:[edi+A33B28]
00A31AE5 6A 00 push 0
```

=> bỏ qua đoạn check, jmp từ 0xA31ABF đến 0xA31ADD

```
00A31AAB C785 4CF5FFFF 4834A3 mov dword ptr ss:[ebp-AB4],antix1.A3344
00A31AB5 C785 50F5FFFF 6C32A3 mov dword ptr ss:[ebp-AB0],antix1.A3326
00A31ABF E8 1C jmp antix1.A31ADD
00A31AC0 90 nop
00A31AC1 90 nop
00A31AC3 8B56 FC mov edx,dword ptr ds:[esi-4]
00A31AC6 FF36 push dword ptr ds:[esi]
00A31AC8 E8 E3F9FFFF call antix1.A31480
00A31ACD 83C4 08 add esp,8
00A31AD0 85C0 test eax,eax
00A31AD2 74 01 je antix1.A31AD5
00A31AD4 47 inc edi
00A31AD5 83C6 0C add esi,C
00A31AD8 83EB 01 sub ebx,1
00A31ADB 75 E3 jne antix1.A31AC0
00A31AE0 8B9D 8BF5FFFF mov ebx,dword ptr ss:[ebp-A48]
00A31AE3 8A87 283BA300 mov al,byte ptr ds:[edi+A33B28]
00A31AE5 6A 00 push 0
```

2. GetFileAttribytesW

Hàm trả về thuộc tính của 1 file hay 1 đường dẫn file

=> return thuộc tính nếu thành công

=> return FFFFFFFF nếu thất bại

[ebp-A2C]: C:.\P.r.o.g.r.a.m. .F.i.l.e.s. .(x.8.6).\V. M.W.a.r.e.\

=> đây là đường dẫn đến file sẽ đọc

00A31CC7	8D85 D4F5FFFF	lea eax,dword ptr ss:[ebp-A2C]	
00A31CCD	50	push eax	
00A31CCE	FF15 9030A300	call dword ptr ds:[&PathCombineW]	
00A31CD4	8D85 D4F5FFFF	lea eax,dword ptr ss:[ebp-A2C]	
00A31CDA	50	push eax	
00A31CDB	FF15 2430A300	call dword ptr ds:[&GetFileAttributesW]	
00A31CE1	83F8 FF	cmp eax,FFFFFFFF	
00A31CE4	74 09	je antix1.A31CEF	
00A31CE6	A8 10	test al,10	
00A31CE8	A0 3E3BA300	mov al,byte ptr ds:[A33B3E]	00A33B3E: "WXYZ"
00A31CED	75 05	jne antix1.A31CF4	
00A31CEB	A0 3D3BA300	mov al,byte ptr ds:[A33B3D]	00A33B3D: "VWXYZ"
00A31CF4	33FF	xor edi,edi	
00A31CF6	8B43 03	mov byte ptr ds:[ebx+3],al	ebx+3: "°\rð°ip«««««ipip°
00A31CF9	C785 78F5FFFF 6036A3	mov dword ptr ss:[ebp-A88],antix1.A33660	

Chạy trong máy ảo => hàm trả về thành công (khác FFFFFFFF)

=> Mặc định jmp (je => jmp) từ 0xA31CE4 đến 0xA31CEF

00A31CCD	50	push eax	
00A31CCE	FF15 9030A300	call dword ptr ds:[&PathCombineW]	
00A31CD4	8D85 D4F5FFFF	lea eax,dword ptr ss:[ebp-A2C]	
00A31CDA	50	push eax	
00A31CDB	FF15 2430A300	call dword ptr ds:[&GetFileAttributesW]	
00A31CE1	83F8 FF	cmp eax,FFFFFFFF	
00A31CE4	EB 09	jmp antix1.A31CEF	
00A31CE6	A8 10	test al,10	
00A31CE8	A0 3E3BA300	mov al,byte ptr ds:[A33B3E]	00A33B3E: "WXYZ"
00A31CED	75 05	jne antix1.A31CF4	
00A31CEB	A0 3D3BA300	mov al,byte ptr ds:[A33B3D]	00A33B3D: "VWXYZ"
00A31CF4	33FF	xor edi,edi	
00A31CF6	8B43 03	mov byte ptr ds:[ebx+3],al	ebx+3: "°\rð°ip«««««ipip°
00A31CF9	C785 78F5FFFF 6036A3	mov dword ptr ss:[ebp-A88],antix1.A33660	

3. Compare "VMWARE"

Tương tự 1

00A31D37	C785 90F5FFFF 8436A3	mov dword ptr ss:[ebp-A70],antix1.A33684	
00A31D41	C785 94F5FFFF BC36A3	mov dword ptr ss:[ebp-A6C],antix1.A336BC	
00A31D48	0F1F4000 00	nop dword ptr ds:[eax+eax],eax	[ebp-A6C]:L"00:50:56", A336BC:L"00:50:56"
00A31D50	8B8CF5 78F5FFFF	mov ecx,dword ptr ss:[ebp+esi*8-A88]	
00A31D57	E8 34F8FFFF	call antix1.A31590	
00A31D5C	85C0	test eax,eax	
00A31D5E	74 01	je antix1.A31D61	
00A31D60	47	inc edi	
00A31D61	46	inc esi	
00A31D62	83FE 04	cmp esi,4	
00A31D65	7C E9	j1 antix1.A31D50	
00A31D68	8A87 283BA300	mov al,byte ptr ds:[edi+A33B28]	edi+A33B28: "ABCDEFGH IJLKMNOPQRSTUVWXYZ"
00A31D6D	33F6	xor esi,esi	
00A31D6F	68 88020000	push 288	

=> Bỏ qua loop (phần check)

=> jmp qua từ 0xA3D48 đến 0xA3D67

00A31D2D	C785 8CF5FFFF A036A3	mov dword ptr ss:[ebp-A74],antix1.A336A0	[ebp-A74]:L"00:1C:14", A336A0:L"00:1C:14"
00A31D37	C785 90F5FFFF 8436A3	mov dword ptr ss:[ebp-A70],antix1.A33684	
00A31D41	C785 94F5FFFF BC36A3	mov dword ptr ss:[ebp-A6C],antix1.A336BC	[ebp-A6C]:L"00:50:56", A336BC:L"00:50:56"
00A31D48	EB 1A	jmp antix1.A31D67	
00A31D4D	90	nop	
00A31D4E	90	nop	
00A31D4F	90	nop	
00A31D50	8B8CF5 78F5FFFF	mov ecx,dword ptr ss:[ebp+esi*8-A88]	
00A31D57	E8 34F8FFFF	call antix1.A31590	
00A31D5C	85C0	test eax,eax	
00A31D5E	74 01	je antix1.A31D61	
00A31D60	47	inc edi	
00A31D61	46	inc esi	
00A31D62	83FE 04	cmp esi,4	
00A31D65	7C E9	j1 antix1.A31D50	
00A31D68	8A87 283BA300	mov al,byte ptr ds:[edi+A33B28]	edi+A33B28: "ABCDEFGH IJLKMNOPQRSTUVWXYZ"
00A31D6D	33F6	xor esi,esi	
00A31D6F	68 88020000	push 288	
00A31D74	56	push esi	

4. CreateFileW - vmci

Tạo hoặc mở 1 file hoặc thiết bị I/O

=> return handle nếu thành công

=> return FFFFFFFF nếu thất bại

