

SCP_이다영



범인의 노트북

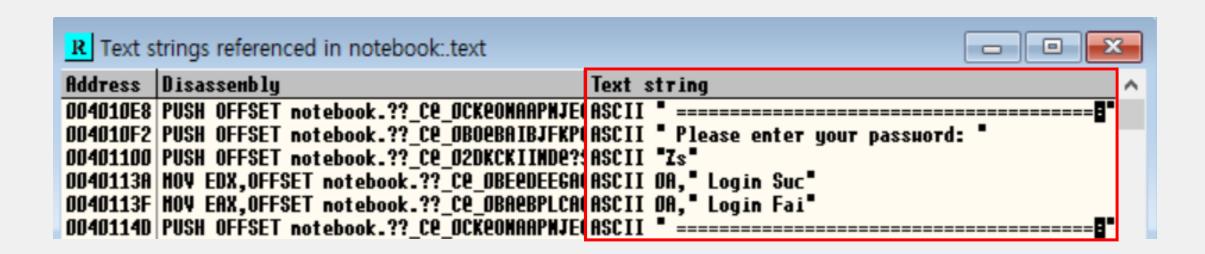
Emily와 Clay의 아파트

Reversing

범인의 노트북

수사관인 당신은 범인을 뒤쫓던 중 범인의 노트북과 메모장을 발견하였다. 메모장에는 노트북 비밀번호로 추정되는 'open'이 적혀있다. 바로 입력해보았지만 올바른 비밀번호가 아니다. 하지만 open과 연관성이 있을 것이다. 시간이 없다! 얼른 진짜 비밀번호를 찾아보자! ■ C:\Users\djssl\Desktop\H험인의 노트북\notebook.exe

■ C:\Users\djssl\Desktop\H인의 노트북\notebook.exe



0040133D	١.	56	PUSH ESI	Arg2
0040133E		FF30	PUSH DHORD PTR DS:[EAX]	Arg1
00401340		E8 3BFDFFFF	CALL notebook.main	Luain
00401345		83C4 DC	ADD ESP,OC	
00401348		8BFO	HOV ESI,EAX	

00401080	-\$	55	SH EBP
00401081		8BEC	W EBP,ESP
00401083		83EC 20	B ESP,20
00401086		A1 04304000	V EAX,DHORD PTR DS:[_security_cookie]
0040108B		3305	IR EAX, EBP
0040108D		8945 FC	V DHORD PTR SS:[EBP-4],EAX
		A1 08214000	Y EAX,DHORD PTR DS:[??_Ce_04PHOCAHAAe
00401095			A EDX,DHORD PTR SS:[EBP-C]
00401098			W DHORD PTR SS:[EBP-C],EAX

004010E8	>	68 10214000	PUSH OFFSET notebook.??_Ce_OCKEONAAPHJE(rformat = " =================================
004010ED	۱.	E8 2EFFFFFF	CALL notebook.printf Lprintf
004010F2	۱.	68 3C214DDD	PUSH OFFSET notebook.??_Ce_OBOeBAIBJFKP(rformat = " Please enter your password: "
			CALL notebook.printf
004010FC	۱-	8D45 E0	LEA EAX,DHORD PTR SS:[EBP-20]

		HOV AL.BYTE PTR SS:[EBP+ECX-C]	10진수: 111
		CHP AL,6F	111 아스키코드: o
	75 07	JMZ SHORT notebook.004010C4	111 이스기고드. 0
		HOV BYTE PTR SS:[EBP+ECX-C1,70	
004010C2 .v	EB 1F	JHP SHORT notebook.004010E3	
004010C4 > :	3C 70	CHP AL,70	
004010C6	75 07	JMZ SHORT notebook.004010CF	
004010C8 . I	C6440D F4 6E	HOV BYTE PTR SS:[EBP+ECX-C],6E	
	EB 14	JHP SHORT notebook.004010E3	
004010CF > 1	3C 65	CHP AL,65	
00401001	75 07	JMZ SHÓRT notebook.004010DA	
004010D3 .	C6440D F4 62	HOV BYTE PTR SS:[EBP+ECX-C],62	
00401008	EB 09	JHP SHORT notebook.004010E3	
004010DA >	3C 6E	CHP AL,6E	
004010DC	75 05	JMZ SHORT notebook.004010E3	
004010DE .	C6440D F4 73	HOV BYTE PTR SS:[EBP+ECX-C],73	
	41	INC ECX	
	3BCA	CHP ECX,EDX	
	7C CD	LJL SHORT notebook.004010B5	
DD IDIDEO	I C CD	-AF 0110V1 110FEDOOK*DD 1DTDD2	I

-

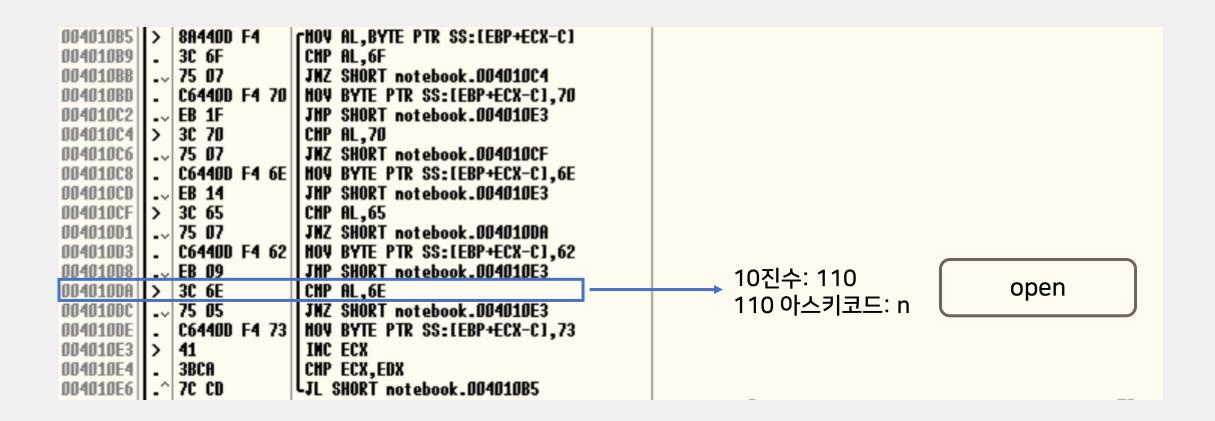
00.40	agne II.	004400	E4 L	HOU OF BUTT DID OF LEBB. FOU OF	-		1		
	010B5 >			HOV AL, BYTE PTR SS:[EBP+ECX-C]					
0040	J10B9 .	3C 6F		CHP AL.6F					
0040	J1OBB .	v 75 O7		JMZ SHORT notebook.004010C4					
0040	J1OBD .	C6440D	F4 70	HOW BYTE PTR SS:[EBP+ECX-C],70					
0040	010C2 .	√ EB 1F		JHP SHORT notebook.004010E3					
0040	010C4 >	3C 70		CHP AL,70					
0040	01006	v 75 O7		JMZ SHÓRT notebook.004010CF					
0040	J10C8 .	C6440D		HOV BYTE PTR SS:[EBP+ECX-C],6E					
0040	DIOCD .	√ EB 14		JHP SHORT notebook.004010E3					
0040	010CF >	3C 65		CHP AL,65					
0040	010D1 .	v 75 O7		JMZ SHORT notebook.004010DA					
	010D3 .	C6440D	F4 62	HOV BYTE PTR SS:[EBP+ECX-C1,62					
0040	J10D8 .	√ EB 09		JHP SHORT notebook.004010E3					
0040	J1DDA 🗀 >	3C 6E		CHP AL,6E					
0040	010DC .	v 75 O5		JMZ SHORT notebook.004010E3					
0040	D10DE .	C6440D	F4 73	HOV BYTE PTR SS:[EBP+ECX-C1,73					
0040	010E3 >	41		INC ECX					
0040	010E4 .	3BCA		CMP ECX,EDX					
0040	010E6 .	^ 7C CD	l l	JL SHORT notebook.004010B5					
						-		_	

004010B5 > 88440D F4 r	HOV AL,BYTE PTR SS:[EBP+ECX-C]	
	CMP AL,6F	
	JMZ SHÓRT notebook.004010C4	
	HOV BYTE PTR SS:[EBP+ECX-C],70	
	JHP SHORT notebook_004010F3	. 10진수: 112
00401004 > 30 70	CHP AL.70 -	<u> </u>
	JMZ SHORT notebook.004010CF	112 아스키코드: p
	HOW BYTE PTR SS:[EBP+ECX-C1,6E	
1. 1.	JHP SHORT notebook.004010E3	
004010CF > 3C 65	CHP AL,65	
	JMZ SHÓRT notebook.004010DA	
	HOW BYTE PTR SS:[EBP+ECX-C1,62	
1. 1.	JHP SHORT notebook.004010E3	
	CHP AL,6E	
	JMZ SHÓRT notebook.004010E3	
	HOW BYTE PTR SS:[EBP+ECX-C1,73	
	INC ECX	
	CHP ECX,EDX	
	JL SHORT notebook.004010B5	

004010B5 > 8A440D F4	CHOV AL, BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F	CHP AL,6F
004010BB 75 07	JMZ SHORT notebook.004010C4
004010BD . C6440D F4 7	HOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 EB 1F	JHP SHORT notebook.004010E3
004010C4 > 3C 70	CHP AL.70
004010C6 75 0 7	JMZ SHORT notebook.004010CF
- II I	HOV BYTE PTR SS:[EBP+ECX-C1,6E
004010CD EB 14	JHP SHORT notebook.004010E3
004010CF > 3C 65	CHP AL,65
00401001 75 07	JMZ SHORT notebook.004010DA
00401003 . C6440D F4 6	1
004010D8 EB 09	JHP SHORT notebook.004010E3
004010DA > 3C 6E	CHP AL,6E
004010DC 75 05	JMZ SHORT notebook.004010E3
	HOV BYTE PTR SS:[EBP+ECX-C1,73
004010E3 > 41	INC ECX
004010E4 . 3BCA	CHP ECX,EDX
004010E6 .^ 7C CD	LJL SHORT notebook.004010B5

004010B9 . 3C 6F 004010BB . 75 07 004010BD . C6440D F4 70 004010C2 . EB 1F 004010C6 . 75 07 004010C8 . C6440D F4 6E 004010CD . EB 14 004010CF > 3C 65 004010D1 . 75 07	CHOY AL,BYTE PTR SS:[EBP+ECX-C] CHP AL,6F JMZ SHORT notebook.004010C4 HOY BYTE PTR SS:[EBP+ECX-C],70 JHP SHORT notebook.004010E3 CHP AL,70 JMZ SHORT notebook.004010CF HOY BYTE PTR SS:[EBP+ECX-C],6E JHP SHORT notebook.004010E3 CHP AL,65 JMZ SHORT notebook.004010DA HOY BYTE PTR SS:[EBP+ECX-C],62 JHP SHORT notebook.004010E3 CHP AL,6E JMZ SHORT notebook.004010E3	10진수: 101 101 아스키코드: e
004010D8 EB 09 004010DA > 3C 6E 004010DC 75 05	JHP SHORT notebook.004010E3 CHP AL,6E	

004010B5 > 8A440D F4	CHOV AL, BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F	CHP AL,6F
004010BB 75 07	JMZ SHORT notebook.004010C4
	HOV BYTE PTR SS:[EBP+ECX-C1,70
004010C2 EB 1F	JHP SHORT notebook.004010E3
004010C4 > 3C 70	CHP AL,70
00401006 75 07	JMZ SHORT notebook.004010CF
	HOW BYTE PTR SS:[EBP+ECX-C1,6E
004010CD EB 14	JHP SHORT notebook.004010E3
	CHP AL_65
	JMZ SHORT notebook.004010DA HOV BYTE PTR SS:[EBP+ECX-C],62
00401008 EB 09	JHP SHORT notebook.004010E3
004010DA > 3C 6E	CHP AL,6E
004010DC 75 05	JMZ SHORT notebook.004010E3
	HOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41	INC ECX
004010E4 . 3BCA	CHP ECX,EDX
004010E6 .^ 7C CD	LJL SHORT notebook.004010B5



004010B5		CHOV AL.BYTE PTR SS:[EBP+ECX-C]	. 10진수: 111
004010B9		CHP AL,6F	_ :
004010BB	75 07	JMZ SHORT notebook.004010C4	111 아스키코드: o
004010BD	. C6440D F4 70	HOV BYTE PTR SS:[EBP+ECX-C1,70	
004010C2	EB 1F	JHP SHORT notebook.004010E3	
004010C4	> 30 70	CHP AL,70	
00401006	75 07	JMZ SHORT notebook.004010CF	
004010C8		•	
004010CD	.~ EB 14	JHP SHORT notebook.004010E3	
	> 3C 65	CHP AL,65	
004010D1	., 75 07	JMZ SHORT notebook.004010DA	
004010D3		HOV BYTE PTR SS:[EBP+ECX-C1,62	
004010D8	. EB 09	JHP SHORT notebook.004010E3	
004010DA			
		CHP AL,6E	
004010DC	.~ 75 05	JMZ SHORT notebook.004010E3	
004010DE		HOV BYTE PTR SS:[EBP+ECX-C1,73	
004010E3	-	INC ECX	
004010E4		CHP ECX,EDX	
004010E6	.^ 7C CD	LJL SHORT notebook.004010B5	

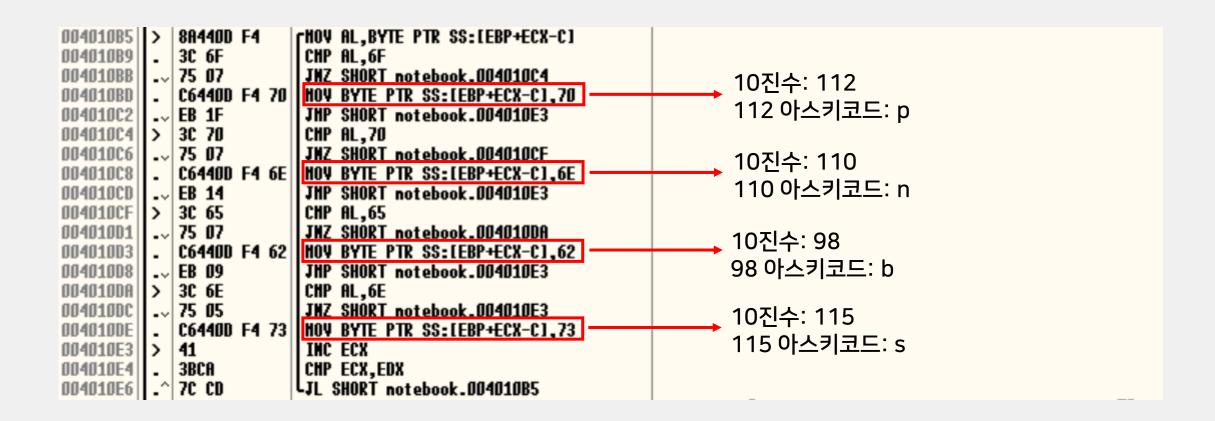
004010B5 > 88440D F4 CH	DV AL,BYTE PTR SS:[EBP+ECX-C]	
	HP AL,6F	
	MZ SHORT notebook.004010C4	40714.440
		10진수: 112
	DV BYTE PTR SS:[EBP+ECX-C1,70	112 아스키코드: p
004010C2 EB 1F J	HP SHORT notebook.004010E3	112 912712 . p
004010C4 > 3C 70 CI	HP AL,70	
004010C6 75 07 JI	NZ SHORT notebook.004010CF	
	DV BYTE PTR SS:[EBP+ECX-C],6E	
	HP SHORT notebook.004010E3	
	HP AL,65	
	•	
	MZ SHORT notebook.004010DA	
	DV BYTE PTR SS:[EBP+ECX-C1,62	
00401008 EB 09 JI	HP SHORT notebook.004010E3	
004010DA > 3C 6E CI	HP AL,6E	
18 1	NZ SHÓRT notebook.004010E3	
	DV BYTE PTR SS:[EBP+ECX-C1,73	
	NC ECX	
	•	
004010E6 .^ 7C CD LJI	L SHORT notebook.004010B5	
	HP ECX,EDX	

004010B5		8A440D	F4		rHOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9	I٠	3C 6F			CMP AL,6F
004010BB	-~	75 O7			JMZ SHORT notebook.004010C4
004010BD	l-	C6440D	F4	70	HOW BYTE PTR SS:[EBP+ECX-C].70
004010C2	l	EB 1F			JHP SHORT notebook.004010E3
004010C4	 >	3C 70			CHP AL,70
004010C6		75 07			JNZ SHORT notebook.004010CF
004010C8	١.	C6440D	F4		HOW BYTE PTR SS:[EBP+ECX-C],6E
004010CD	l	EB 14			JHP SHORT notebook.004010E3
004010CF	 >	3C 65			CHP AL,65
004010D1	I	75 07			JMZ SHÓRT notebook.004010DA
004010D3	١.	C6440D	F4		HOW BYTE PTR SS:[EBP+ECX-C],62
004010D8	I	EB 09			JHP SHORT notebook.004010E3
004010DA	 >	3C 6E			CHP AL,6E
004010DC	I	75 05			JMZ SHORT notebook.004010E3
004010DE	Ι.		F4	73	HOV BYTE PTR SS:[EBP+ECX-C1,73
004010E3	b	41	-		INC ECX
004010E4		3BCA			CHP ECX,EDX
004010E6					-JL SHORT notebook.004010B5

```
004010B5 >
             88440D F4
                          CHOY AL, BYTE PTR SS:[EBP+ECX-C]
             3C 6F
004010B9
                           CHP AL,6F
004010BB
          ... 75 07
                           JMZ SHORT notebook.004010C4
             C6440D F4 70
004010BD
                           HOV BYTE PTR SS:[EBP+ECX-C],70
004010C2
          ... EB 1F
                           JHP SHORT notebook.004010E3
004010C4
             3C 70
                           CHP AL,70
00401006
          ... 75 07
                           JMZ SHORT notebook.004010CF
             C6440D F4 6E
00401008
                           HOW BYTE PTR SS:[EBP+ECX-C],6E
004010CD
          ... EB 14
                           JHP SHORT notebook.004010E3
004010CF
             3C 65
                           CHP AL,65
          ... 75 07
                           JMZ SHORT notebook.004010DA
004010D1
             C6440D F4 62
                           HOV BYTE PTR SS:[EBP+ECX-C],62
004010D3
004010D8
          ... EB 09
                           JHP SHORT notebook.004010E3
             3C 6E
                           CHP AL,6E
004010DA
          ... 75 05
                           JMZ SHORT notebook.004010E3
004010DC
004010DE
             C6440D F4 73 HOV BYTE PTR SS:[EBP+ECX-C1,73
004010E3
             41
                           INC ECX
                                                                            for (i = 0; i < len; i++)
             3BCA
                           CHP ECX, EDX
004010E4
                           LJL SHORT notebook.004010B5
004010E6
             7C CD
```

				_		
004010B5	>	8A440D	F4		CHON HIBATE BLE SETEBB+ECX-CI	
004010B9	-	3C 6F			CHP AL,6F	
004010BB		75 07			JMZ SHORT notebook.004010C4	
004010BD			F4	70 H	HOV BYTE PTR SS:[EBP+ECX-C1,70	
004010C2	-	EB 1F	٠.		JHP SHORT notebook.004010E3	
004010C4	•					
	,	3C 70			CHP AL,70	
004010C6	•~	75 07			JMZ SHORT notebook.004010CF	
004010C8	-	C644DD	F4	6E	HOV BYTE PTR SS:[EBP+ECX-C1,6E	
004010CD	-~	EB 14			JHP SHORT notebook.004010E3	
004010CF	>	3C 65			CHP AL,65	
00401001		75 07			JMZ SHORT notebook.004010DA	
004010D3	- ·		F4	62	HOV BYTE PTR SS:[EBP+ECX-C1,62	
00401008	-	EB 09	• •	۱۱ ۵	JHP SHORT notebook.004010E3	
	•					
004010DA	,	3C 6E			CHP AL,6E	
004010DC	-~				JMZ SHORT notebook.004010E3	
004010DE	-	C6440D	F4	73	HOW BYTE PTR SS:[EBP+ECX-C1,73	
004010E3	>	41			INC ECX	
004010E4		3BCA			CHP ECX, EDX for $(i = 0; i < len; i++)$	
004010E6		7C CD			LJL SHORT notebook.004010B5	
DD IDIDEO	•	10 00			-AF AHAVI HATERAAKIRARA	

004010B5	> 8A440D F4	rHOV AL.BYTE PTR SS:[EBP+ECX-C]	
004010B9	. 3C 6F	CHP AL,6F	
004010BB	75 07	JMZ SHORT notebook.004010C4	
004010BD	. C6440D F4 70	HOV BYTE PTR SS:[EBP+ECX-C1,70	
004010C2	EB 1F	JMP SHORT notebook.004010E3	
004010C4	> 30 70	CHP AL,70	
004010C6	75 07	JMZ SHORT notebook.004010CF	for
00401008	. C6440D F4 6E	HOV BYTE PTR SS:[EBP+ECX-C1,6E	
004010CD	EB 14	JHP SHORT notebook.004010E3	if
004010CF	> 30 65	CHP AL,65	else if
004010D1	75 O7	JMZ SHORT notebook.004010DA	else if
004010D3	. C6440D F4 62	HOV BYTE PTR SS:[EBP+ECX-C1,62	
004010D8	.√ EB 09	JHP SHORT notebook.004010E3	else if
004010DA	> 3C 6E	CHP AL,6E	
004010DC	75 O5	JMZ SHORT notebook.004010E3	
004010DE		HOV BYTE PTR SS:[EBP+ECX-C1,73	
004010E3		INC ECX	
004010E4		CHP ECX,EDX	
004010E6	.^ 7C CD	LJL SHORT notebook.004010B5	



■ C:\Users\djssl\Desktop\H인의 노트북\notebook.exe

scpCTF{pnbs}

Reversing

Emily와 Clay의 아파트

Emily와 Clay가 살고있는 아파트는 층수가 무려 100층까지 있다. 그렇다면 Emily의 집은 몇 층일지 아래 프로그램을 통해 맞춰보자. Clay는 내일 이사를 가므로, 맞는 층수를 입력했을 때 'It's a wrong approach.'가 나오도록 HXD로 수정해보자. * 각 문장의 맨 앞은 무조건 공백이다.

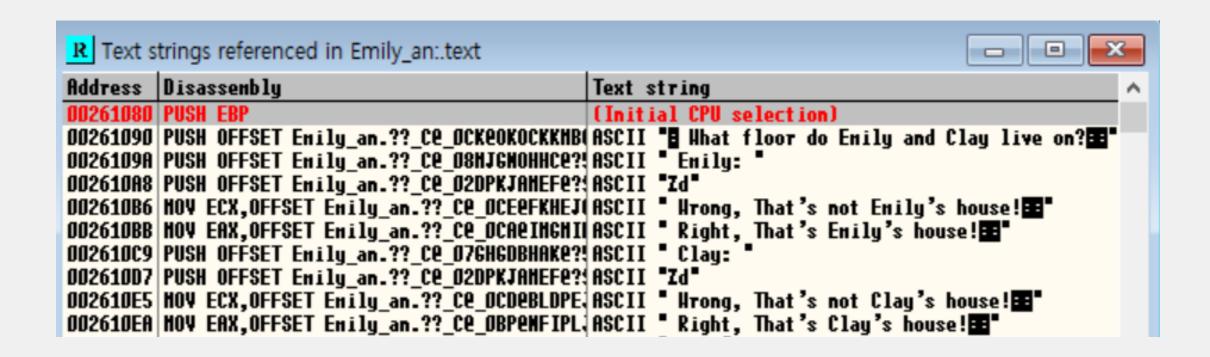
> → Emily가 사는 층 + 수정 완료한 영역의 끝 주소값 Ex) scpCTF{721524)

■ C:\work\CTF\Emily and Clay's APT\Release\Emily and Clay's APT.exe

```
What floor do Emily and Clay live on?

Emily: 29
Wrong, That's not Emily's house!

Clay: 40
Wrong, That's not Clay's house!
```



```
PUSH EBP
00261080 🖎
             55
00261081
             8BEC
                          HOW EBP,ESP
00261083
            83EC OC
                          SUB ESP,OC
00261086
             A1 04302600
                          HOV EAX,DHORD PTR DS:[__security_cookie]
0026108B
             33C5
                          XOR EAX, EBP
0026108D
             8945 FC
                          HOY DHORD PTR SS:[EBP-4],EAX
00261090
             68 08212600
                          PUSH OFFSET Enily_an.??_C0_OCK0CKKHB(rformat = "| Hhat floor do Enily and Clay live on?
             E8 86FFFFFF
                          CALL Enily an.printf
00261095
                                                                  Lprintf
                          PUSH OFFSET Enily_an.??_Ce_08HJGHOHHCe?!rformat = " Enily: "
             68 34212600
0026109A
            E8 7CFFFFFF
                          CALL Enily an.printf
0026109F
                                                                  Lprintf
002610A4
            8D45 F8
                          LEA EAX, DHORD PTR SS: [EBP-8]
002610A7
             50
                          PUSH EAX
                          PUSH OFFSET Enily_an.??_C@_O2DPKJAHEF@?{rformat = "Zd"
002610A8
            68 40212600
002610AD
            E8 9EFFFFFF
                         CALL Enilu an.scanf
                                                                  scanf
                                                                          65
002610B2 .
            837D F8 41
                         CHP DHORD PTR SS:[EBP-8],41
                         HOV ECX,OFFSET Enily_an.??_C0_OCE0FKHEJ( ASCII " Hrong, That's not Enily's house!
002610B6 .
            B9 64212600
                          HOV EAX,OFFSET Enily_an.??_C@_OCA@IHGHI| ASCII " Right, That's Enily's house!
            B8 44212600
002610BB | .
                          CHOVME EAX, ECX
002610C0
            0F45C1
                          PUSH EAX
002610C3
             50
                                                                  fornat
002610C4 .
            E8 57FFFFFF
                          CALL Enily an printf
                                                                  Lprintf
```

```
PUSH EBP
00261080 r$
            55
00261081
           8BEC
                        HOW EBP, ESP
00261083
           83EC DC
                        SUB ESP.OC
00261086
            A1 04302600
                        HOV EAX, DHORD PTR DS:[ security cookie]
0026108B
            33C5
                        XOR EAX, EBP
           8945 FC
                        HOY DHORD PTR SS:[EBP-4].EAX
0026108D
00261090
            68 08212600
                        PUSH OFFSET Enily_an.??_C@_OCK@OKOCKKHB(rformat = "| Hhat floor do Enily and Clay live on?
00261095
           E8 86FFFFFF
                        CALL Enily an.printf
                                                             Lprintf
0026109A .
                        PUSH OFFSET Enily_an.?? C@ D8HJGNOHHC@?!rformat = " Enilu: "
           68 34212600
           E8 7CFFFFFF
                        CALL Enily an.printf
0026109F
                                                             Lprintf
002610A4 .
                        LEA EAX, DHORD PTR SS:[EBP-8]
           8D45 F8
002610A7
           50
                        PUSH EAX
002610A8
           68 40212600
                        PUSH OFFSET Enily an.?? C@ D2DPKJAHEF@?!rformat = "Zd"
002610AD | .
           E8 9EFFFFFF
                       CALL Enily an.scanf
                                                             -scanf
                        CHP DHORD PTR SS:[EBP-8],41
           837D F8 41
002610B6 .
           B9 64212600
                        HOV ECX,OFFSET Enily an.?? CO OCEOFKHEJ( ASCII " Hrong, That's not Enily's house!
                        002610BB | -
           B8 44212600
00261000
           OF45C1
                        CHOVME EAX, ECX
                        PUSH EAX
002610C3
            50
                                                             format
002610C4 .
           E8 57FFFFFF
                        CALL Enily an.printf
                                                             Lprintf
```

■ C:\work\CTF\Emily and Clay's APT\Release\Emily and Clay's APT.exe

```
What floor do Emily and Clay live on?
Emily: 65
                         PUSH OFFSET Enily_an.??_Ce_08HJGHOHHCe?!cformat = " Enily: "
0026109A
            68 34212600
0026109F
            E8 7CFFFFFF
                         CALL Enily_an.printf
                                                                Lprintf
002610A4
            8D45 F8
                         LEA EAX, DHORD PTR SS: [EBP-8]
002610A7
            50
                         PUSH EAX
DD261DA8
            68 40212600
                         PUSH OFFSET Enily_an.??_C@_O2DPKJAHEF@?{cformat = "Zd"
            E8 9EFFFFFF
                         CALL Enily an.scanf
002610AD
                                                                Lscanf
                         CHP DHORD PTR SS:[EBP-8],41
002610B2
            837D F8 41
002610B6
            B9 64212600
                         | HOV ECX,OFFSET Enily_an.??_C0_OCE0FKHEJ( ASCII " Hrong, That's not Enily's house!■
                         HOV EAX,OFFSET Enily an.?? Ce OCAEIHGHII ASCII " Right, That's Enily's house!■"
002610BB
            B8 44212600
                         CHOVNE EAX.ECX
002610C0
            0F45C1
002610C3
                                                                format = " Right, That's Enily's house!
                         PUSH EAX
            E8 57FFFFFF CALL Enily an.printf
                                                                printf
```

■ C:\work\CTF\Emily and Clay's APT\Release\Emily and Clay's APT.exe

```
What floor do Emily and Clay live on?
Emily: 7
                        PUSH OFFSET Enily_an.??_Ce_08HJGNOHHCe?!cformat = " Enily: "
0026109A
            68 34212600
            E8 7CFFFFFF
                         CALL Enily an.printf
0026109F
                                                               printf
                         LEA EAX, DHORD PTR SS:[EBP-8]
002610A4
            8D45 F8
00261087
                         PUSH EAX
            50
002610A8
            68 40212600
                         PUSH OFFSET Emily_an.??_C@_O2DPKJAHEF@?{cformat = "Zd"
002610AD
            E8 9EFFFFFF
                         CALL Enily an.scanf
                                                                Lscanf
                         CHP DHORD PTR SS:[EBP-8],41
002610B2
            837D F8 41
            B9 64212600
                        | HOV ECX,OFFSET Enily_an.??_C@_OCE@FKHEJ( ASCII " Hrong, That's not Enily's house!■
002610B6
                         MOV EAX,OFFSET Enily_an.??_C@_OCA@IHGHI| ASCII " Right, That's Enily's house!
002610BB
            B8 44212600
            OF45C1
00261000
                         CHOVNE EAX.ECX
                                                               format = " Hrong, That's not Enily's house!
002610C3
                         PUSH EAX
002610C4 . E8 57FFFFFF CALL Enily an.printf
                                                               printf
```

```
|PUSH OFFSET Enily_an.??_C@_076HGDBHAK@?{rformat = " Clay: "
00261009
             68 88212600
002610CE
             E8 4DFFFFFF
                          CALL Enily_an.printf
                                                                  printf
002610D3
            8D45 F4
                          LEA EAX, DHORD PTR SS:[EBP-C]
00261006
             50
                          PUSH EAX
                          PUSH OFFSET Emily_an.??_C@_O2DPKJAHEF@?{\format = "Zd"
002610D7
             68 40212600
002610DC
             E8 6FFFFFFF
                         CALL Enily an.scanf
                                                                  Lscanf
002610E1
             837D F4 51
                         CHP DHORD PTR SS:[EBP-C],51
002610E5 .
             B9 B0212600
                         HOV ECX,OFFSET Enily_an.??_C@_OCD@BLDPE\ ASCII " Hrong, That's not Clay's house!■"
                          HOV EAX,OFFSET Enily_an.??_C@_OBP@MFIPL; ASCII " Right, That's Clay's house!■
002610EA .
            B8 90212600
                          CHOVME EAX, ECX
002610EF .
            OF45C1
                                                                 format
002610F2
             50
                          PUSH EAX
002610F3 .
            E8 28FFFFFF
                          CALL Enily an.printf
                                                                  Lprintf
```

```
002610E5 .
            B9 B0212600 | HOV ECX,OFFSET Enily_an.??_C0_OCD0BLDPE\ ASCII " Hrong, That's not Clay's house!
                         MOV EAX,OFFSET Enily an.?? C@ OBP@MFIPL | ASCII " Right, That's Clay's house!■
002610EA | .
            B8 90212600
002610EF .
            0F45C1
                         CHOVME EAX, ECX
002610F2
                         PUSH EAX
            50
                                                                 format
002610F3
            E8 28FFFFFF
                        CALL Enily an.printf
                                                                 Lorintf
002610F8 .
            68 D4212600 | PUSH OFFSET Enily an.?? C@ OSPDJBBECF@pirconnand = "pause"
002610FD .
            FF15 9020260(CALL DHORD PTR DS:[<&api-ns-uin-crt-run| Lsystem
00261103
            8B4D FC
                         HOY ECX, DHORD PTR SS: [EBP-4]
00261106
            83C4 28
                         ADD ESP,28
            33CD
                         XOR ECX, EBP
00261109
            33CO
                         XOR EAX, EAX
0026110B
0026110D
            E8 04000000 | CALL Enily an. security check cookie
```

00262190=0FFSET Enily_an.??_Ce_0BPeMFIPLJJ0e?5Right?0?5That?8s?5Clay?8s?5house?\$CB?6?6e (ASCII " Right, That's Clay's hous

Address Hex dump ASCII																
00262190 20 52											Right					
002621A0 6C 61											_		_			
002621B0 20 57											Hrong 11 to					
DDEOETED OF 1	1 20	13 00	. 01	17 2	((3	CD 00	01 7	3 13	03	21) L C 1 C	ıy s	lious	e:		
00001370	27	72	20 4	er e	E 7	4 20	4 5	6D	60	60	79	27	72	20	60	's not Emily's h
																-
00001380	6F	75 '	73 (65 2	1 0	A OA	. 00	20	43	60	61	79	3A	20	00	ouse! Clay: .
00001390	20	52	69 (67 (8 7	4 2C	20	54	68	61	. 74	27	73	20	43	Right, That's C
000013A0	6C	61 '	79 2	27	13 2	0 68	6F	75	73	65	21	0A	0A	00	00	lay's house!
000013B0	20	57 '	72 (6F 6	E 6	7 2C	20	54	68	61	74	27	73	20	6E	Wrong, That's n
000013C0	6F	74 2	20 4	43 6	C 6	1 79	27	73	20	68	6F	75	73	65	21	ot Clay's house!
00001370	27	73	20 (6E (F 7	4 20	45	6D	69	60	79	27	73	20	68	's not Emily's h
00001380	6F	75	73 (65 2	21 0	A OA	00	20	43	60	61	79	ЗА	20	00	ouse! Clay: .
00001390	20	49	74 :	27 7	3 2	0 61	20	77	72	6F	6E	67	20	61	70	It's a wrong ap
000013A0	70	72	6F (61 (3 6	8 2E	00	75	73	65	21	0A	0A	00	00	proachuse!
000013B0	20	57	72	6F (E 6	7 20	20	54	68	61			73		6E	Wrong, That's n
000013C0											6F					ot Clay's house!

■ C:\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Users\Use

```
What floor do Emily and Clay live on?
Emily: 65
Right, That's Emily's house!
Clay: 81
It's a wrong approach.계속하려면 아무 키나 누르십시오 . . .
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00001390 20 49 74 27 73 20 61 20 77 72 6F 6E 67 20 61 70 It's a wrong ap
000013A0 70 72 6F 61 63 68 2E 00 75 73 65 21 0A 0A 00 00 proach..use!....
```

scpCTF{6513A7}

