

姓			名	薛旗	学			伯	20155362
班			级	软信-1503	指	导	教	师	程维
实	验	名	称		2	破解」	<b> </b>	注入	-
开	设	学	期		2017	-20	18 貧	<b>第一</b>	学 期
开	设	时	间		第 1	周一		第	8 周
报	告	日	期			201	7.11.	05	
<u>-</u>	山	4	体		评	贠		人	程维
F F	疋	成	须		评	定	日	期	

东北大学软件学院

## 实验一:

1.扫描类型选择两者之间的值,并根据倒计时秒数选择合适的区间逐步进行扫描,直到查找 到唯一变量。



3.双击该变量,将该地址转入下方列表。

激活	描述	地址	类型	值	
$\boxtimes$	无描述	024E4EC0	4 Bytes	40	4

4. 勾选"激活"选项,将数值锁定,可以发现倒计时程序数值不变。



5.双击"值"处,在弹出的对话框中填入"9999",单机确定,列表"值"处的值变为 9999.

更改值					×			
请输入新的值	:							
9999								
· · ·			确定(0)	<b>D</b>	<b>4</b>		C	
6.通过练习。							7	
倒计时破解练习								×
破解倒计时约	东习: ——							
			Ĺ	通过:			/	
<b>尔</b> 哈一,					0			
<b>1</b> .扫描类型:	精确扫描	,输入的	的扫描数值	与动态智	密码的第一个	个值一到	汝。	
围合流动体力								
- 固定密码练习:	密码为: 09	0812						
	P	3	0	2	6	6	4	
	🗱 Cheat Engin	e 6.3					- • ×	
	Eile Edit Tai	ble D3D <u>I</u>	<u>H</u> elp 00000:	364-CheatEngin	eTrainer2.exe		ß	
F	Address	Value	Previou *	新的扫	₩ Next Scan	ſ	Undo Scan	
	00030F7C	3	3	1	<u>i</u> :		Settings	
	00132494 00133EBC	3 3	3 3	🗖 Hex 🚦				
	00134040 001342EC	3	3	Scan Type 🛔	情确数值 1. 中世			

2.按第一步的方法进行多次扫描,直到得到唯一的地址信息。

固定密码练习	. 密码为. (	090812						
	. ц.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,							
		$\cap$	5	6	6	ર	7	
		U	U	0	0	0		_
	🐔 Cheat Eng	ine 6.3						
	<u>File E</u> dit T	able D3D	Help	10264.CheatEngi	ooTrainer? eve			
			0000	iuso4-cheaterigi	ie Haneiz, exe			
	Found: 92	Value	Proviou	▲ \$605+3	Have Score			
	023F37A0	0	0				Settings	
	02434C7C	0	0	Hex	∎. ]			
	02434C94 02434CAC	0	0	Scan Type	精确数值		•	
得到唯一地	也址信息。							
司定密码练习;	· 密码为: 0	90812						
		9	Δ	5	7	7	7	
		L	0	9		- 1		
ſ	🐔 Cheat Engir	ne 6.3						
	<u>File E</u> dit Ta	able D3D	<u>H</u> elp		P		_	
	2 🖻 目		0000	0364-CheatEngir	neTrainer2.exe			
	Found: 1			]				
	Address	Value	Previous	新的扫	描 Next Scan		Undo Scan Settings	
	UZ3F3/AU	2	2	Hev				
				Scan Type	唐确對值		-	
					IN WORALD			

4.双击该唯一变量,将该地址转入下方列表。

激活	描述	地址	类型	值	
$\boxtimes$	无描述	023F37A0	4 Bytes	0	×

5.在 CE 下方的地址上右键,选择"Find out what writes to this address"。

🐔 下列代码写入到 023F37A0	×
C., Instruction 2 72236037 - 89 44 31 04 - mov [rcx+rsi+04],eax	Replace
	Show disassembler
	Add to the codelist
	More information

6.选中唯一信息,点击"Replace",输入 nop 并确定。可以发现密码将被固定。



7.在 CE 下方地址信息上右键,选择 "Browse this memory region",进入内存查看器。

🐔 Memory Viewer	
File Search View Debug Tools Kerne	l tools
	clrCoUninitializeEE+3592B
地址         字节         操作码	注释 🔺
clrCoUninitializ/90 nop	
clrCoUninitializ:83 3D 38D37772 00 cmp	dword ptr [E49B337A],00 122
clrCoUninitializ/0F85/643B2200 jne	clrCreateHistoryReader+8858
clrCoUninitializ/5E pop	rsi
clrCoUninitializ/8B E5 mov	esp,ebp
clrCoUninitializ/5D pop	rbp
clrCoUninitializ/C2 0400 ret	0004 4
clrCoUninitializ:85 C9 test	ecx,ecx
clrCoUninitializ:0F84 F2E01E00 je	clr_CreateHistoryReader+55B4
clrCoUninitializ:8B D1 mov	edx,ecx
clrCoUninitializ:56 push	fsi
clrCoUninitializ/8D 72 02 lea	esi,[rdx+02]
clrCoUninitializ/0FB7 02 movzx	eax,word ptt [rdx]
	no operation
保护:读/写 基址=023F3000 长度=24	F000
地址 AO A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF 0123456789ABCDEF
023F37A0 00 00 00 00 04 00 00 00	08 00 00 02 00 00 00
023F37B0 02 00 00 00 08 00 00 00	00 00 00 00 30 5A 41 70
U23F37CU UU UU UU UU UU UU UU UU	UU UU UU UU AC 6D 41 70 mAp
023F37D0 00 00 00 00 00 00 00 00 00	
023F37E0 00 00 00 00 00 00 00 00 00 00 00 00 0	
023F3800 00 00 00 00 48 A5 98 6F	68 E0 40 02 0C E0 40 02H oh @ @.
023F3810 00 00 00 00 BC A5 98 6F	00 00 00 00 08 B4 40 02 o <mark>.</mark> @. —
023F3820 00 00 00 00 00 00 00 00	4C 38 3F 02 F4 01 14 00L8?
023F3830 FE 08 A0 04 1D 26 F4 76	00 01 00 00 38 36 3F 02& v86?.
U23F384U 14 38 3F U2 AU 11 11 UU	UU UU UI UU L4 A8 31 /1 .8/ Iq 24 D0 21 71 06 00 00 00
023F3860 4D 00 6F 00 75 00 73 00	54 D0 51 71 00 00 00 00 4 1q 65 00 5δ 00 00 00 00 00 Μ σ μ s e 7
023F3870 00 00 00 80 34 D8 31 71	10 00 00 00 4D 00 61 00 4 1gM.a.
023F3880 67 00 65 00 6C 00 6C 00	61 00 6E 00 20 00 4D 00 g.e.l.l.a.nM.
023F3890 53 00 57 00 48 00 45 00	45 00 4C 00 00 00 00 00 Š.W.H.E. <mark>E.L</mark>
023F38A0 00 00 00 80 34 D8 31 71	OF 00 00 00 4D 00 53 00 4 1qM.S.
UZ3F38BU 57 UU 48 UU 45 UU 45 UU	4C UU 5F UU 5Z UU 4F UU W.H.E.E.LR.U.

8.修改相应地址位置的数值,使最后的密码值为090812。

保护:读/3	写	基	b上=(	)23B	7300	) O C	长度	<u>t</u> =24	4F0(	00						
地址	ΑO	Å1	A2	ÀЗ	Α4	A5	Α6	A7	Α8	Α9	ÅΆ	ÅΒ	AC	AD	ΑE	ΔF
023F37A0	00	00	00	00	09	00	00	00	00	00	00	00	08	00	00	00
023F37B0	01	00	00	00	02	0.0	00	00	00	00	00	00	30	5A	41	70

9.通过练习。



# 实验三:

1.	扫描类型:	精确扫描,	输入的扫描	苗数值与	正确密码	码的第一	个值一致		
,	动态密码练习					414214			
	动态密码练习:		ĪĹ	E确	密石	马:	780	587	
		(	) 6	<b>j</b>	6	2	5	7	
		🐔 Cheat Engin	e 6.3						
		<u>F</u> ile <u>E</u> dit Ta	ble D3D <u>H</u> elp	p					
		🔜 产 릚 Found: 1,884		000008	A4-CheatEngi	ineTrainer3.exe			Ê
		Address 00030F9C 000B311C 000C14C4 000C5EAC	Value         I           7         7           7         7           7         7           7         7           7         7	Previou * 7 7 7 7	新的扫 f 日ex Scan Type	描 Next Sca 直: <mark>7</mark> 精确数值	an	Undo Scan	Settings

2.多次扫描,直到扫描到唯一地址信息。

态密码练习	· ·	•						
态密码练习:								
		Ī	E确	密码	] ]:	266	680	
	0	,	7	0	2	7	3	
	Cheat Engine	6.3						
E	ile <u>E</u> dit Tab	e D3D <u>H</u>	elp					
8	3 🖻 🖬 🛛		000008	3A4-CheatEngi	neTrainer3.ex	e		<u>í</u>
Fou	und: 4							5
À	address	Value	Previous	新的扫	描 Next:	Scan	Undo Scan	Chear Engline
0	23037A8	2	2	ſ	<u>ة:</u>			Settings
C	2321690	2	2	Hex	2			
	23D19BC	2	2		-			
	)245522C	18930	2	Scan Type	精确数值		•	

### 3.扫描得到唯一地址信息。

动态密码练习:						
		正确	角密	码:	180	672
	8	2	3	8	8	1
🗮 CI	neat Engine 6.3					- • •

	<u>File E</u> dit Table D3D <u>H</u> elp	p		
		00000BA4-CheatEngine	Trainer3.exe	
	Found: 1			
	Address Value J	Previous 新的扫描	Next Scan	Undo Scan
	023037A8 1 :	1 值:		Settings
Ý		🔲 Hex 🧻		
		Scan Type 精	确数值 🔹 👻	
		Value Type 43	<b>学节                                     </b>	
			. 0,	
4. 双击,将其法	加载到卜万的地址列表	甲。		
x62.x−7	late 1.1			
激活 抽述	地址	奕型 1		
│ │ │ 一 元 描述	023037	A8 4 Bytes 7		*

5.按实验二的方法,查找写入该地址的代码。选中唯一信息,点击"Replace",输入 nop 并确定。可以发现密码将被固定。

🐔 下列代码写入到 023037A8	23
C         Instruction           3         71B76037 - 89 44 31 04 - mov [rex+rsi+04],eax	Replace
Cheat Engine 代码: 你要给代码起个什么名称? nopl	e codelist
OK Cancel	ormation
	copy memory

6.可以看到当前的正确密码和动态密码信息,他们并不一致。

													****			
保护:读/3	写	基t	独上=(	0230	0300	00 -	长度	=23	3F00	00						
地址	Α8	Α9	AA	AΒ	AC	AD	ΑE	AF	B0	B1	B2	B3	B4	B5	B6	B7
023037A8	07	00	00	00	01	00	00	00	03	00	00	00	04	00	00	00
023037B8	08	00	00	00	05	00	00	00	02	00	00	00	00	00	00	00
023037C8	00	00	00	00	00	00	00	00	03	00	00	00	02	00	00	00
023037D8	00	00	00	00	30	5A	53	72	00	00	00	00	00	00	00	00

7.修改相应地址处的值,使正确密码和动态密码的值一致。

保护 :读/3	ş	基:	5址=02303000 长度=23F000													
地址	Α8	Α9	ÅΑ	AΒ	AC	AD	ΑE	ΑF	B0	B1	B2	B3	B4	B5	B6	B7
023037A8	07	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
023037B8	00	00	00	00	00	00	00	00	07	00	00	00	00	00	00	00
023037C8	00	00	00	00	00	00	00	00	00	00	00	00	00	0.0	00	00

8.当正确密码和动态密码值一致时,显示已通过。



● 代码注入练习 反汇编与注入代码练习	]:				<u></u>
更改进度			40%		
	🐔 Cheat Engine 6.3				
	File Edit Table D	03D <u>H</u> elp 000009AC	CheatEngineTrainer4.exe	Ē	
	Address         Val:           00537008         40           0053700C         40           022D438C         40           022F4C9C         40	ue Previous 40 40 40 40 40 5 V	新的扫描 Next Scan 值: 一 Hex 40 ican Type 有确数值 alue Type 4字节	Undo Scan Settings	

3.点击更改进度,观察发现,地址信息数量仍为4,不再发生改变,因此以下操作需在这四个变量上进行尝试。



4.首先尝试第一个。类似实验二和实验三的方法,查找写入该地址的代码。

2



5.点击"Show disassemble",显示反汇编,打开内存查看器。在"Tool"菜单中选择"Auto assemble"(自动汇编),在弹出的界面中,选择"Template"菜单项下的"Code injection"(代码注入),然后在弹出的地址填写窗口处点击确定,可发现自动汇编已帮我们创建了一部分代码。通过实践观察,该部分代码对解决问题没有帮助,继续实践。

2



**6**.通过实践,第三个地址变量对解决问题有帮助。此处只展示对解决问题有帮助的操作方法。 按以上类似的方法,查找写入该地址的代码。

🐔 Cheat Engine 6.3			×
File Edit Table D3D	😴 下列代码写入到 022D438C	<b>×</b>	-
Found: 4 Address Value 00537008 30 0053700C 20 022D436C 20 022F4C9C 0	C Instruction 1 00300FF5 - 83 80 58010000 F6 - add dword ptr [e 1 7221E24F - 89 01 - mov [rcx].eax	Replace Show disassembler Add to the codelist More information	ttings
	< ► 00300EE1 - 90 - non	dad (ogn ontonidos)	lhack
Memoru) (jour	00300FF2 - 88 45 F0 - mov eax,[ebp-10] 00300FF5 - 83 80 58010000 F6 - add dword ptr [eax+ 00300FFC - 88 45 F0 - mov eax,[ebp-10] 00300FFF - 83 88 58010000 00 - cmp dword ptr [eax-		أسالحديجة

#### 7.打开内存查看器。

🐔 Memory Viewer 📃 🗖 🗖 💌									
File Sear	rch View Debug To	ols Kerne	l tools						
<u> </u>			00300FF5						
地址	字节	操作码		注释		*			
00300FF5	83 80 58010000 F6	add	dword ptr [eax+00000159],-04	246					
00300FFC	8B 45 F0	MOY	eax,[ebp-10]	_					
00300FFF	83 B8 58010000 00	cmp	dword ptr [eax+00000158],00	0					
00301006		sete	al						
00301009		MOYZX	eax,ai Jaha 001 anu						
0030100C	03 40 F0 93 7D F9 00	COD	dword ptr [ebp.08] 00	0					
00301013	74.24	ie	00301039	0					
00301015	90	nop							
00301016	8B 0D D8222D03	mov	ecx,[032D22D8]						
0030101C	E8 23DEC56F	call	System.Windows.Forms.ni.dll+7	71					
00301021	89 45 F4	mov	[ebp-0C],eax						
00301024	90	nop							
00301025	E8 5E533870	call	System.ni.dll+136388						
0030102A	89 45 EC	MOY	[ebp-14],eax						
00301020	86 4U EC	moy	ecx.[eop-14]	•.					
			add (sign extend	ed)					
8.同样的	操作方法,进入付	代码注入	界面,研究代码。		<b>. Q ,</b>	•			
🐔 Auto -	assemble								
File Vie	ew Template								
1 a1	1 <b>alloc</b> (newmern, 2048)								
2 <b>la</b>	2 label (returnhere)								
3 <b>la</b>	<b>bel</b> (originalco	de)							
4 <b>la</b>	<b>bel</b> (exit)								

5
6 newmem: //this is allocated memory, you have read,write,execute .
7 //place your code here
8
9 originalcode:
10 add dword ptr [eax+00000158],-0Å
11
12 exit:

13 jmp returnhere
14
15 00300FF5:
16 jmp newmem
17 nop

returnhere:

nop

18

19

9.可以发现第 10 行的代码是解决问题的关键。源码通过累加-OA,使得每次点击"更改进度" 按钮,进度递减 10。我们可以从这里下手,解决问题。

```
9 originalcode:
10 add dword ptr [eax+00000158],-0A
11
```

10.将累加-OA 改为+OA, 注入后的代码通过累加+OA, 使得每次点击"更改进度"按钮, 进度递增 10。点击"Execute"完成代码注入。

9	originalcode:	
10	add dword ptr	[ <mark>eax+</mark> 00000158],+OA

## 11.点击"更改进度"按钮,使进度递增到100。

📲 代码注入练习 反汇编与注入代码练习:		×
更改进度		
	80%	
12.进度达到 100,通过练习。		
<mark></mark>		
汉孔 编 司 在 八1 4 马 赤 小 :	已通过	2.

## **教师评语或评价表格:**(任课教师可根据实际情况,做适当调整) 评语及评价表格的字体颜色为红色

评价表格示例:(考核标准与教学大纲中的实验考核标准一致)

考核标准	得分
(1)正确理解和掌握实验所涉及的概念和原理(10%);	
(2) 按实验要求合理设计数据结构和程序结构(20%);	
(3)能设计测试用例,运行结果正确(20%);	
(4)认真记录实验数据,原理及实验结果分析准确(40%);	
(5)实验报告规范(10%)。	