1、(2分)

【逆向分析】读汇编是逆向基本功。

编译环境为linux gcc x86-64  
调用约定为System V AMD64 ABI  
请不要利用汇编器，IDA等工具。。这里考的就是读汇编与推算汇编结果的能力

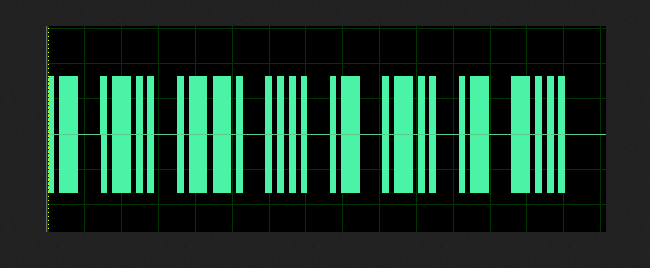
main函数如下：

int main(int argc, char const \*argv[])  
{  
  char input[] = {0x0,  0x67, 0x6e, 0x62, 0x63, 0x7e, 0x74, 0x62, 0x69, 0x6d,  
                  0x55, 0x6a, 0x7f, 0x60, 0x51, 0x66, 0x63, 0x4e, 0x66, 0x7b,  
                  0x71, 0x4a, 0x74, 0x76, 0x6b, 0x70, 0x79, 0x66 , 0x1c};  
  func(input, 28);  
  printf("%s\n",input+1);  
  return 0;  
}

**答案read\_asm\_is\_the\_basic**

2、(2分)

【密码学】滴答滴答



答案：alphalab

3、(2分)

【取证分析】一天下午小白出去吃饭，临走之前还不忘锁了电脑，这时同寝室的小黑想搞点事情，懂点黑客和社工知识的小黑经过多次尝试获得了密码成功进入电脑，于是便悄悄在电脑上动起手脚了，便在桌面上写着什么，想给小白一个惊喜，同时还传送着小白的机密文件，正巧这时小白刚好回来，两人都吓了一跳，小黑也不管自己在电脑上留下的操作急忙离开电脑，故作淡定的说：“我就是随便看看”。

1. 那么问题来了，小白的密码是啥？

答案：19950101

4、(2分)

【取证分析】 对题目所给的文件进行取证分析，获取系统环境变量中的机密信息

答案：66d7724d872da91af56907aea0f6bfb

5、(2分)

【取证分析】 从历史操作记录中获取敏感信息并提交。

答案：1s4g76jk89f

6、(2分)

【取证分析】 VIM恢复

答案：1wu8rijmdkf9odls

7、(2分)

【取证分析】 One of our agents managed to sniff important piece of data transferred transmitted via USB, he told us that this pcap file contains all what we need to recover the data can you find it ?

答案：SN1FF\_TH3\_FL4G\_0V3R\_U58

8、(2分)

【取证分析】 Hint：DD、USB

答案：ggmgk05096

9、(2分)

【取证分析】 Once more our agents managed to sniff data passed over USB, they told us that this is high profile data hidden by people knows what they are doing, they have dedicated devices for reading that secret file format. Can you help us finding what is the secret message?

答案：Wh0\_N33d5\_K1nDl3\_t0\_3X7R4Ct\_K1ND13\_F1rMw4R3

10、(2分)

【取证分析】 对题目所给的文件进行取证分析，获取系统中flag账号的ntlm的hash值进行提交

答案：3008c87294511142799dca1191e69a0f

11、(2分)

【取证分析】 对题目所给的文件进行取证分析，获取记事本中的内容

答案：5bd2510a83e82d271b7bf7fa4e0970d1

12、(2分)

【逆向分析】PY交易

答案：d3c0mpil1n9\_PyC

13、(2分)

【逆向分析】 ImagePrc

答案：TOG

14、(2分)

【逆向分析】 或许你需要去学习下IDA的使用，但是只需要学一点点就能做这题了  
PS:IDA里面按R可以把奇怪的数字变成字符串

答案：Welcome\_To\_RE\_World!

15、(2分)

【逆向分析】 ELFCrackme

答案：4092849uio2jfklsj4kl

16、(2分)

【逆向分析】 EasyKeygen

答案：K3yg3nm3

17、(2分)

【逆向分析】 EasyCrack

答案：Ea5yR3versing

18、(2分)

【逆向分析】 Crackme1

答案：D3M4\_x1Y4\_w4NsUI

19、(2分)

【逆向分析】  
Talent Yang loves to customize his own obfuscator. Unfortunately, he lost his seed when he was watching Arsenal's UEFA game. What a sad day! His team and his seed were lost together. To save him, could you help him to get back his seed? We can not save the game, but we may be able to find out his seed.

Compile: ollvm.clang -Xclang -load -Xclang lib0opsPass.so -mllvm -oopsSeed=THIS\_IS\_A\_FAKE\_SEED source.c

Clang && LLVM Version: 3.9.1

答案：B0s5x1AOb3At0bF~

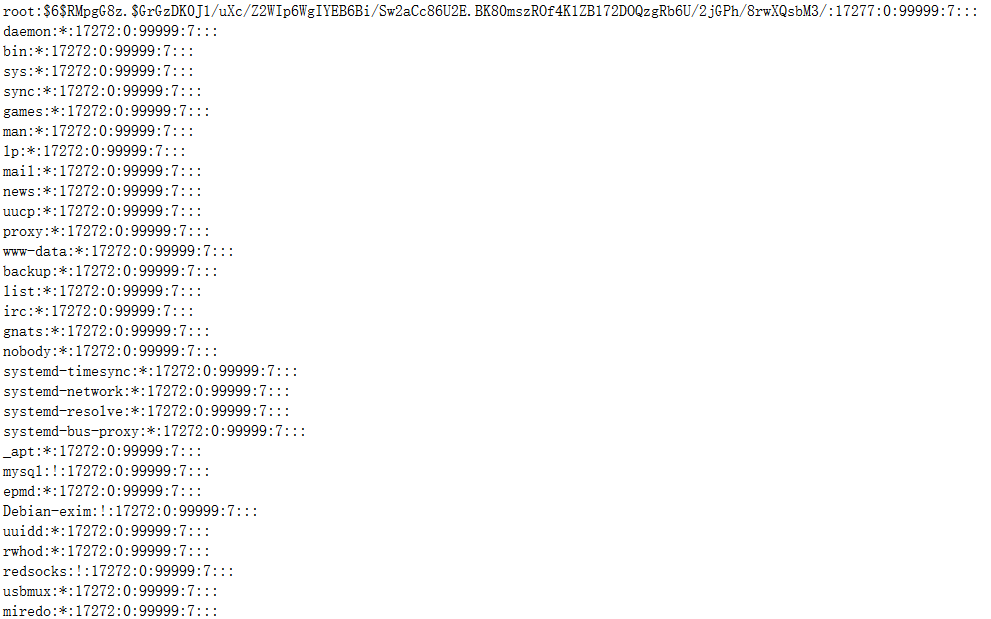
20、(2分)

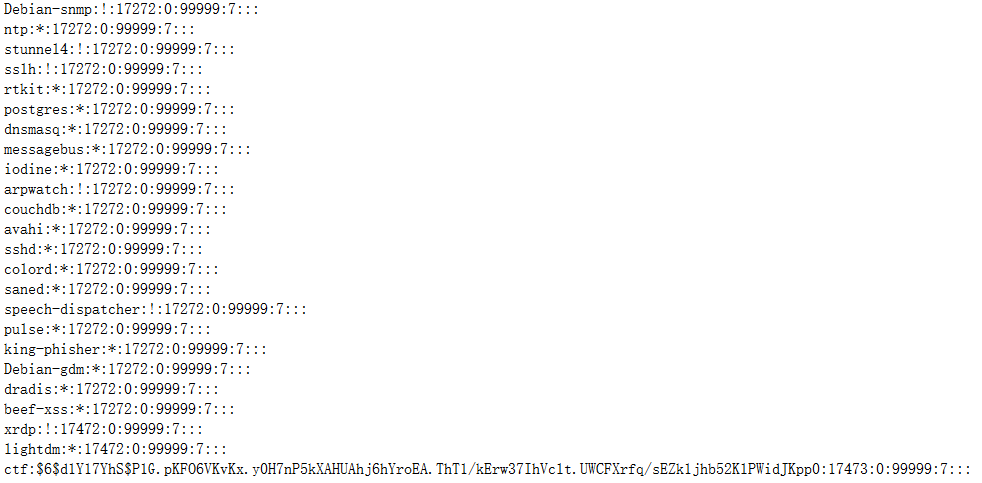
【逆向分析】 We permutate the opcode of python2.7, and use it to encrypt the flag.. Try to recover it!

答案：Gue55\_opcode\_G@@@me

21、(2分)

【密码学】Linux系统密码





答案：5201314

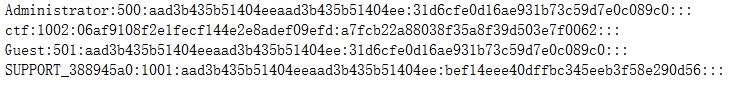
22、(2分)

【密码学】 33 53 21 41 43 74 43 53 63 83 32 71 42 63 62 32

答案：flagisilovephone

23、(2分)

【密码学】 我的密码忘了，你能帮我找回吗？



答案：good-luck

24、(2分)

【密码学】 从网页中找到登陆密码。

答案：91aee1e0d6a80a8b5fe190d7ad254d7f

25、(2分)

【密码学】 密文：U2FsdGVkX19PuxOY5/W+kfD11dhgSbz51GoOSb9pJJIGbW75qXuivEkf5fr5R03Q

答案：Xlsro4l67Do27E

26、(2分)

【密码学】 你能发现什么？

答案：20141014

27、(2分)

【密码学】 python大法好！  
这里有一段丢失的md5密文  
e9032???da???08????911513?0???a2  
要求你还原出他

已知线索 明文为： TASC?O3RJMV?WDJKX?ZM

答案：e9032994dabac08080091151380478a2

28、(2分)

【密码学】 密码是什么呢？

答案：h1\_c7f

29、(2分)

【密码学】 密文：ytfvbhn tgbgy hjuygbn yhnmki tgvhn uygbnjm uygbn yhnijm  
你能从键盘上发现什么？

答案：Areuhack

30、(2分)

【密码学】 密文：V1ROU2JXVXlTbWhqTWxabVRtcFNPUT09

答案：base\_64

31、(2分)

【数据分析】根据所给的数据包进行分析获取其中的密码

答案：backdoorm8te

32、(2分)

【数据分析】 获取ftp密码进行提交

答案：cdts3500

33、(2分)

【数据分析】 找到这个telnet会话的用户密码

答案：user

34、(2分)

【数据分析】 报告首长！发现一只苍蝇。。

在哪？

here!

卧槽？！好大一坨苍蝇。。

答案：m1Sc\_oxO2\_Fly

35、(2分)

【数据分析】 对所给的菜刀数据包分析，获得flag

答案：c7265f898a52fcc4

36、(2分)

【数据分析】 对给出的dns数据包进行分析得出flag

答案：FLAG-FT47cMX26pWyFSI6RPWaSr5YRw

37、(2分)

【数据分析】 Find the flag!

答案：d316759c281bf925d600be698a4973d5

38、(2分)

【数据分析】 You are a member of a covert agency that is spying on one of their intelligence targets. They have managed to MiTM (Man-in-The-Middle) one of the target employees and are monitoring his HTTP traffic. It is of vital importance that you extract the correct password he submitted to [www.2dehands.be](http://www.2dehands.be).

答案：safefromNSA.

39、(2分)

【数据分析】 请根据题目去下载相应的数据包http.pcap对其进行分析得到flag

答案：GehFMsqCeNvof5szVpB2Dmjx

40、(2分)

【数据分析】 利用wireshark工具对已给出的数据包进行分析，找到数据包中的敏感字符，拿到其密文，该密文可能是利用MD5加密的，也可能是利用Base64位加密的，需要把密文利用解密工具解出来，解密出来的明文值就是我们要提交的key值。

答案：ISCCTESTpas

41、(2分)

【隐写】 what kali？？

答案：feb81d3834e2423c9903f4755464060b

42、(2分)

【隐写】 开盖有惊喜

答案：7adf6f07e0810003c585a7be97868a90

43、(2分)

【隐写】 PDF也疯狂

答案：security\_through\_obscurity

44、(2分)

【隐写】 N种方法解决

答案：dca57f966e4e4e31fd5b15417da63269

45、(2分)

【隐写】 NS weiC

答案：THe-battLe-of-weiNan

46、(2分)

【隐写】 NS shuD

答案为：w4R\_0f\_YiLing

47、(2分)

【隐写】 Magic pictures

答案：int3r5tingxor

48、(2分)

【隐写】 In Hex, No One Can Hear You Complain

答案为docx—why—not—doccz

49、(2分)

【隐写】 Excel也疯狂

答案：sh1yanba

50、(2分)

【隐写】 Doc是什么鬼

答案：k42bP8khgqMZpCON