

Misc

Warmup

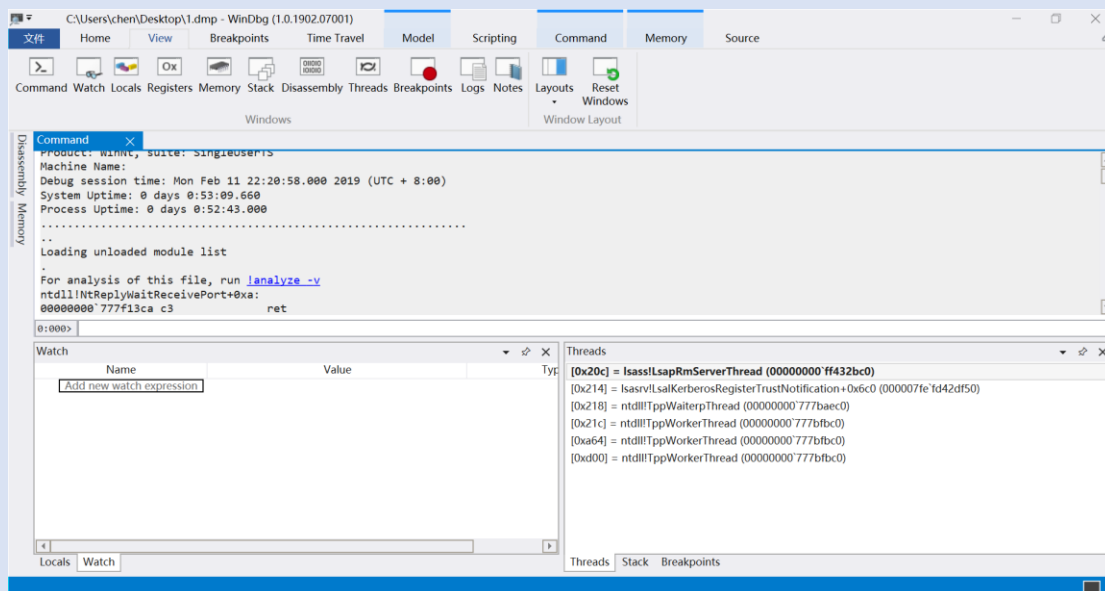
URL:

先在 010 editor 里分析一下文件头标志

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	4D	44	4D	50	93	A7	B1	61	0C	00	00	00	20	00	00	00	MDMP" \$±a....
0010h:	00	00	00	00	CA	84	61	5C	26	18	00	00	00	00	00	00Ê,,a\&.....
0020h:	03	00	00	00	24	01	00	00	D0	01	00	00	11	00	00	00\$...Ð.....
0030h:	8C	01	00	00	F4	02	00	00	04	00	00	00	DC	1B	00	00	œ...ô.....Û...
0040h:	80	04	00	00	0E	00	00	00	24	00	00	00	5C	20	00	00	€.....\$....\ ..
0050h:	09	00	00	00	F0	19	00	00	D6	BC	00	00	10	00	00	00ö...ô½.....
0060h:	90	64	00	00	46	58	00	00	07	00	00	00	38	00	00	00	.d..FX.....8...
0070h:	B0	00	00	00	0F	00	00	00	E8	00	00	00	E8	00	00	00	°.....è....è...
0080h:	0C	00	00	00	10	00	00	00	36	58	00	00	00	00	00	006X.....

dib	42 4D	device-independent bitmap
DLL	4D 5A 90	
DMP	4D 44 4D 50 93 A7	Windows minidump file
DMS	44 4D 53 21	Amiga DiskMasher compres
doc	0D 44 4F 43	DeskMate Document file

发现是 dmp 文件，于是改后缀名，可以用 WinDbg 打开和分析：



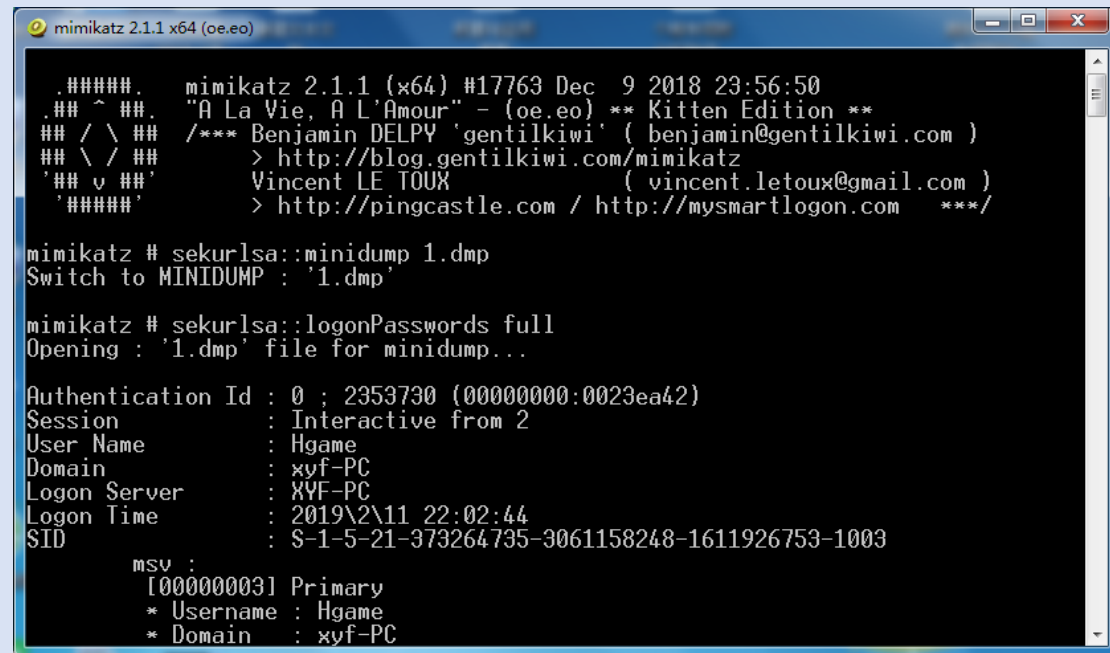
然而运行!analyze -v 之后并没有找到关于用户的有用信息（题目让我们找管理员密码）

后来放出的 hint 里提示说用 mimikatz。我去了解了下，发现 mimikatz 可以从 dmp 文件中很方便地获取用户明文密码。下载下来之后发现在 win10 运行有问题，管理员运行之后打开一瞬间就关掉了（说好的最新版本是针对 win10 的呢），然后借了我妈的电脑（win7 系统）才正常运行了 mimikatz。

直接管理员运行 mimikatz.exe 就能打开, (先把 1.dmp 跟它放在同一目录下)然后输入如下命令:

第一步 sekurlsa::minidump 1.dmp

第二步 sekurlsa::logonPasswords full



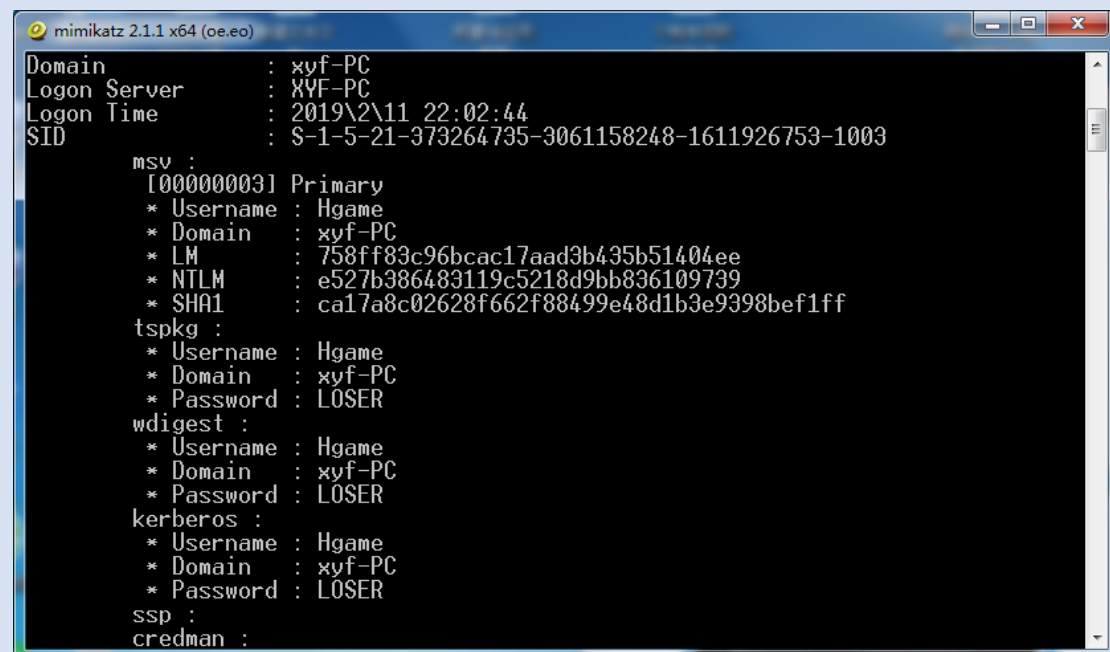
```
mimikatz 2.1.1 (x64) #17763 Dec  9 2018 23:56:50
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::minidump 1.dmp
Switch to MINIDUMP : '1.dmp'

mimikatz # sekurlsa::logonPasswords full
Opening : '1.dmp' file for minidump...

Authentication Id : 0 ; 2953730 (00000000:0023ea42)
Session           : Interactive from 2
User Name         : Hgame
Domain            : xyf-PC
Logon Server      : XYF-PC
Logon Time        : 2019\2\11 22:02:44
SID               : S-1-5-21-373264735-3061158248-1611926753-1003

msv :
[00000003] Primary
* Username : Hgame
* Domain   : xyf-PC
```



```
Domain            : xyf-PC
Logon Server      : XYF-PC
Logon Time        : 2019\2\11 22:02:44
SID               : S-1-5-21-373264735-3061158248-1611926753-1003

msv :
[00000003] Primary
* Username : Hgame
* Domain   : xyf-PC
* LM       : 758ff83c96bcac17aad3b435b51404ee
* NTLM     : e527b386483119c5218d9bb836109739
* SHA1     : ca17a8c02628f662f88499e48d1b3e9398bef1ff

tspkg :
* Username : Hgame
* Domain   : xyf-PC
* Password : LOSER

wdigest :
* Username : Hgame
* Domain   : xyf-PC
* Password : LOSER

kerberos :
* Username : Hgame
* Domain   : xyf-PC
* Password : LOSER

ssp :
credman :
```

得到了管理员密码 LOSER。转换成 SHA256 之后加上 hgame{}就是 flag 了:

明文:

LOSER

散列/哈希算法:

SHA1

SHA224

SHA256

SHA384

SHA512

HmacSHA1

HmacSHA224

HmacSHA256

HmacSHA384

HmacSHA512

哈希值:

dd6dffcd56b77597157ac6c1beb514aa4c59d033098f806d88df89245824d3f5

这周只做出一道题，自闭了。坐等官方 write up