

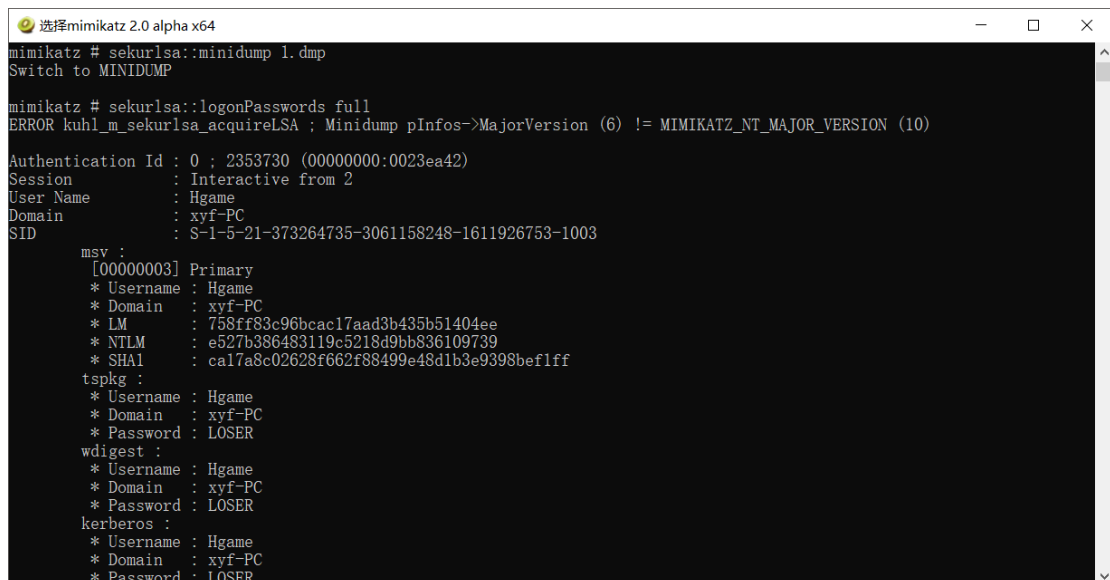
MISC

1. warmup

解压得到一个 GIF，经各种试探后发现…这压根不是个 GIF，winhex 打

14	15	ANSI	ASCII
00	00	MDMP	"S±a
00	00		Ê„a\&
00	00		\$ Ð
00	00	0E	ô Ü
00	00	0A	ˆ ˆ \

开开头是 MDMP 的字样，查找之后发现文件拓展名应该是 .dmp，用 mimikatz 打开



```
选择mimikatz 2.0 alpha x64
mimikatz # sekurlsa::minidump l.dmp
Switch to MINIDUMP

mimikatz # sekurlsa::logonPasswords full
ERROR kuhl_m_sekurlsa_acquireLSA ; Minidump pInfos->MajorVersion (6) != MIMIKATZ_NT_MAJOR_VERSION (10)

Authentication Id : 0 ; 2353730 (00000000:0023ea42)
Session           : Interactive from 2
User Name         : Hgame
Domain            : xyf-PC
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

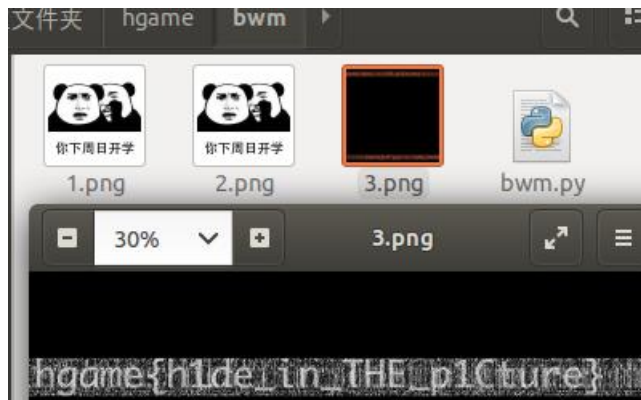
wdigest :
* Username : Hgame
* Domain   : xyf-PC
* Password : LOSER

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

Password: LOSER，根据 hint 找个工具转一下就可以了。

2.暗藏玄机

解压以后是个双图，放 Stegsolve 里比较，看不出啥，winhex 也看不出。查了之后知道了是盲水印，



, bwm 跑了一下也出来了。

嗯...我觉得我再励志一下就可以当个 misc 选手了...