

## Ck HGAME 2019 week-4 writeup

### MISC

#### Warmup

#### 利用 Mimikatz

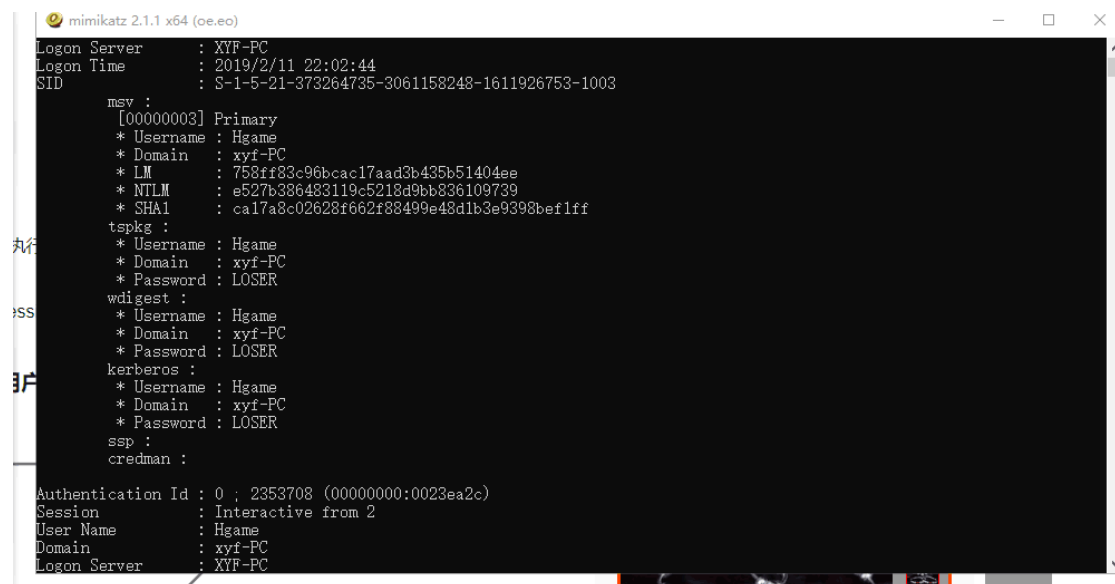
先关了杀毒的软件

然后 用管理员身份打开 mimikatz

Privilege : : debug

Sekurlsa : : minidump 1.gif

Sekurlsa : : logonPasswords full 得到如图



```
mimikatz 2.1.1 x64 (oe.oe)
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 :

Authentication Id : 0 : 2353708 (00000000:0023ea2c)
Session          : Interactive from 2
User Name        : Hgame
Domain           : xyf-PC
Logon Server     : XYF-PC
```

LOSER 即密码

然后 给 LOSER 进行 sha256 加密

