Crypto

- easy_rsa

感觉是很明显的共模攻击，但答案差太远，多个脚本答案一致，将变量和函数输出后发现egcd函数的最大公因数为3，才发现e1和e2不互质，将结果开立方根后还是不对，再立方发现与原结果不符，应该是精确问题，凑了一下将末尾644改为789（好像是这个数）得到正确flag。

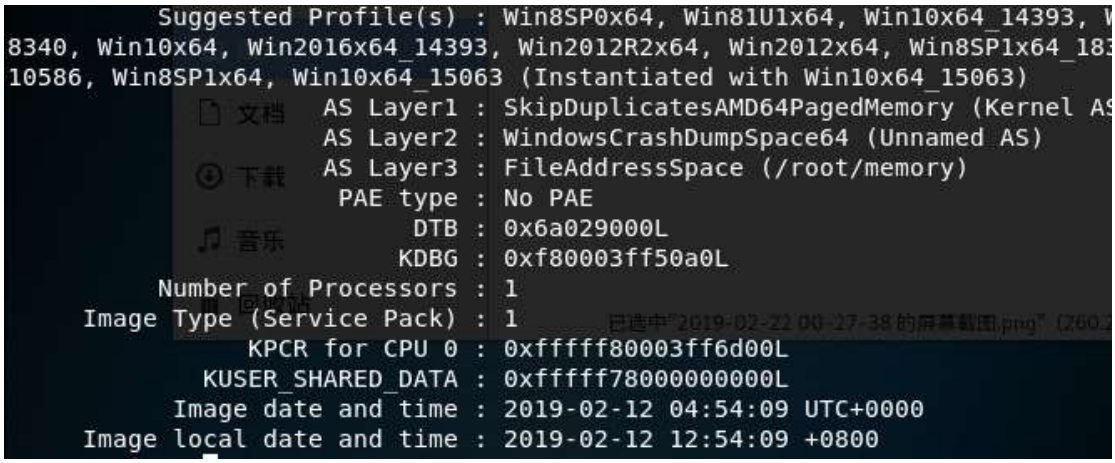
Misc

- Warmup

file指令查看文件类型为minidump，用mimikatz查看得到密码，转化为sha256提交flag。

```
mimikatz # privilege::debug
Privilege '20' OK

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

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

Authentication Id : 0 ; 2353730 (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
         * 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
Logon Time        : 2019/2/11 22:02:44
SID               : S-1-5-21-373264735-3061158248-1611926753-1003
        msv :
```

- Clodown



用file指令，显示为full dump，应该是完全内存转储，文件大小2g也比较符合。可以用kali自带的volatility打开。

查了下资料，获取密码要打开注册表查看system和sam，但根据提供的profile打开都不正确，搞了很久后用windbg打开发现版本为Win7SP1x64(之前打开是SP0?)。

```
Symbol search path is: srv*
Executable search path is:
Windows 7 Kernel Version 7601 (Service Pack 1) UP Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 7601.17592.amd64fre.win7sp1_gdr.110408-1631
Machine Name:
```

```
root@kali:~# volatility -f memory --profile=Win7SP1x64 hashdump -y 0
24010 -s 0xfffff8a003652010
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
xyf:1001:aad3b435b51404eeaad3b435b51404ee:0bb8d932bbfee69fbc874214f3
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:291e1d2ec16a080
271cc:::
Hgame:1003:aad3b435b51404eeaad3b435b51404ee:e527b386483119c5218d9bb8
```

输入指令得到

```
root@kali:~# volatility -f memory --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a003652010 0x00000000260a9010 \SystemRoot\System32\Config\SAM
0xfffff8a0062bd010 0x000000002143e010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a00000f010 0x000000002bfa9010 [no name]
0xfffff8a000024010 0x000000002bf34010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a0000652d0 0x000000002c3772d0 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0007e1010 0x0000000027e59010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0007f8280 0x00000000279dd280 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a001041350 0x000000001de7c350 \??\C:\Windows\ServiceProfiles\Netwo
SER.DAT
0xfffff8a001087010 0x000000001071a010 \??\C:\Windows\ServiceProfiles\Local
R.DAT
0xfffff8a0017dd010 0x000000000bd36010 \??\C:\System Volume Information\Sys
0xfffff8a002054010 0x000000006509d010 \??\C:\Users\xyf\ntuser.dat
0xfffff8a0020be010 0x00000000078b6010 \??\C:\Users\xyf\AppData\Local\Micro
UsrClass.dat
0xfffff8a00364f010 0x0000000025e26010 \SystemRoot\System32\Config\DEFAULT
```

NTLM，转化为sha256提交。

- 暗藏玄机

双图，有几种可能，先使用compare指令比较两幅图，得到新图。

很明显的盲水印，github上下载盲水印脚本解决。