CTF WEEK4 WP

MISC

1. Akira 之瞳-1

> 拿到raw后缀的文件，百度得知要用到volatility工具。[1]：

> 首先 python vol.py -f important_work.raw imageinfo 得知系统版本。
>
> 列出进程： python vol.py -f important_work.raw --profile=Win2008R2SP0x64 pslist
>
> 在进程中找到了明显要保存出来的进程数据（文件名就叫这个）：

```
0xfffffa800f263b30 important_work         1092   2232      1       16      1
  1 2021-02-18 09:47:15 UTC+0000
```

> 保存出数据：python vol.py -f important_work.raw --profile=Win2008R2SP0x64 -p 1092 -D 123
>
> 直接 foremost： foremost -v -i 123/1092.dmp ,得到 output 文件夹，在文件夹内找到一个加密的压缩包，拖进 winhex 找到此片段：

```
  6    à¿e % ï»¿P
assword is sha25
6(login_password
)
```

> 易知要将登陆密码进行 sha256 加密。
>
> 获取 system 和 sam 地址：
>
> python vol.py hivelist -f important_work.raw --profile=Win2008R2SP0x64
>
> 接着获取账号密码：
>
> python vol.py -f important_work.raw --profile=Win2008R2SP0x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a000bc3410

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
```

> 将密码放到网站: https://www.cmd5.com/ 进行解密：

> 再将此密码进行 sha256 加密得到解压密码：

asdqwe123

在线加密 在线解密

sha256（asdqwe123）= 20504cdfddaad0b590ca53c4861edd4f5f5cf9c348c38295bd2dbf0e91bca4c3

解压得到两张图片，通过其中一张图片的名称 blind 得知是盲水印解密。

使用 BlindWaterMark-master 工具执行：

python bwmforpy3.py decode Blind.png src.png 222.png

得到图片后放大看到了 flag：

hgame{7he_f1ame_brin9s_me_end1ess_9rief}。

---

1. 一开始用的volatility版本过老，会出现一系列问题，但自己完全没有想到这一点，以至于中间被奇怪的问题卡住了，问了一波 Akira 学长才得知了版本问题（又被学长捞了） ↩