2021-内存取证wp

原创

Maya_Soy 于 2021-06-15 15:22:32 发布 688 收藏 9

分类专栏： 内存取证 Kali volatility 文章标签： python kali

本文链接：https://blog.csdn.net/Maya_Soy/article/details/117924561

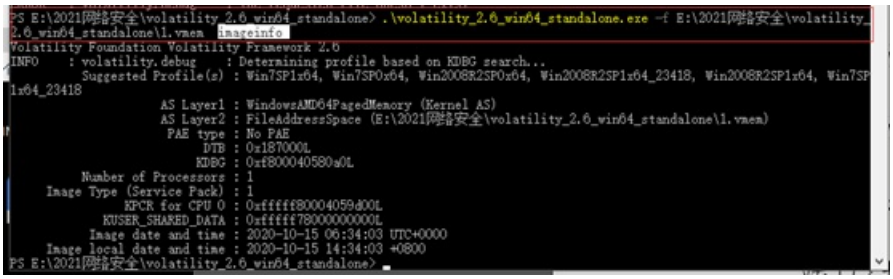
使用工具

```
volatility WinHex
```

1. 从内存中获取到用户admin的密码并且破解密码,作为flag提交；

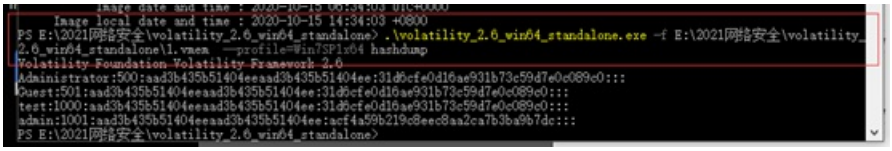
使用imageinfo得到操作系统

```
volatility.exe -f E:\网络安全\volatility\1.vmem imageinfo
```

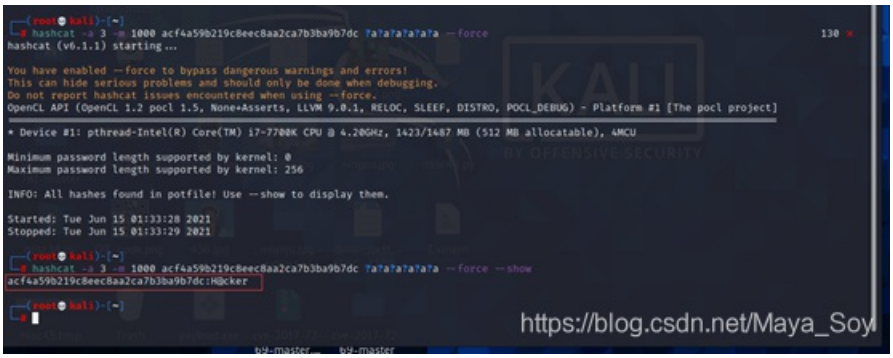


使用hashdump得到密码hash

```
volatility.exe -f E:\网络安全\volatility\1.vmem --profile=Win7SP1x64 hashdump
```

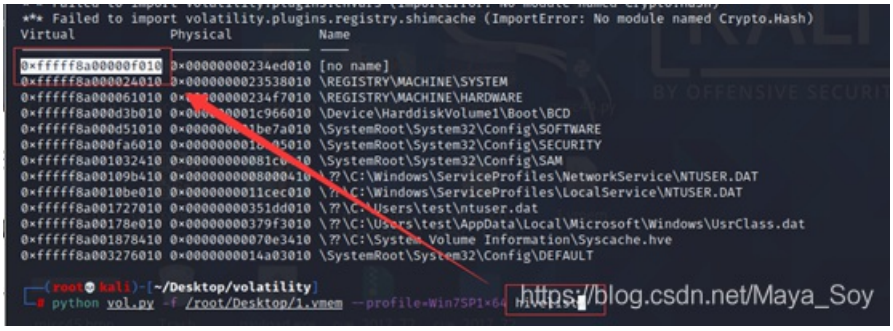


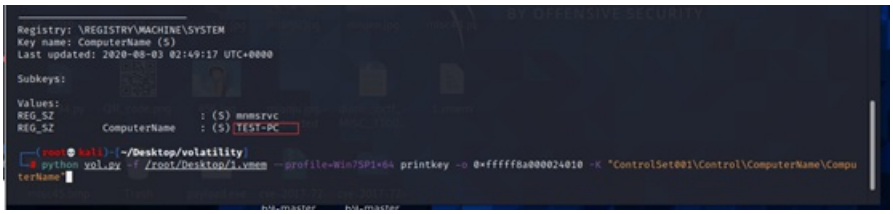
使用hashcat破解密码hash，得到明文密码



2. 获得当前系统的主机名，将主机名作为flag提交；

```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 hivelist
```



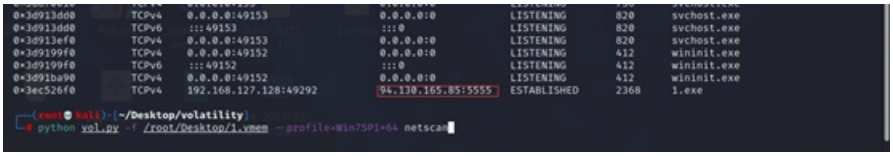


3. 获取当前系统浏览器搜索过的关键词，作为Flag提交；

```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 iehistory
```

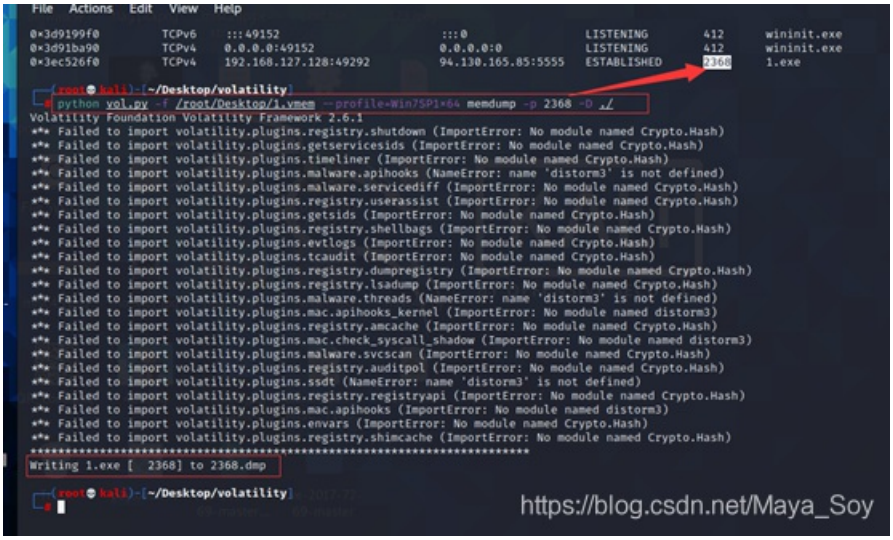
4. 当前系统中存在挖矿进程，请获取指向的矿池地址，作为Flag提交；

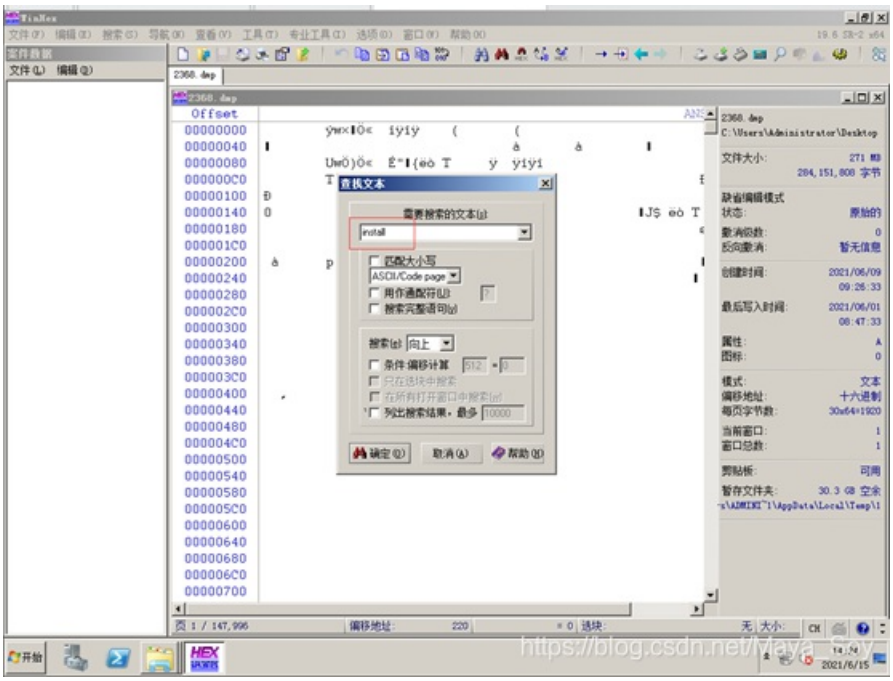
```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 netscan
```



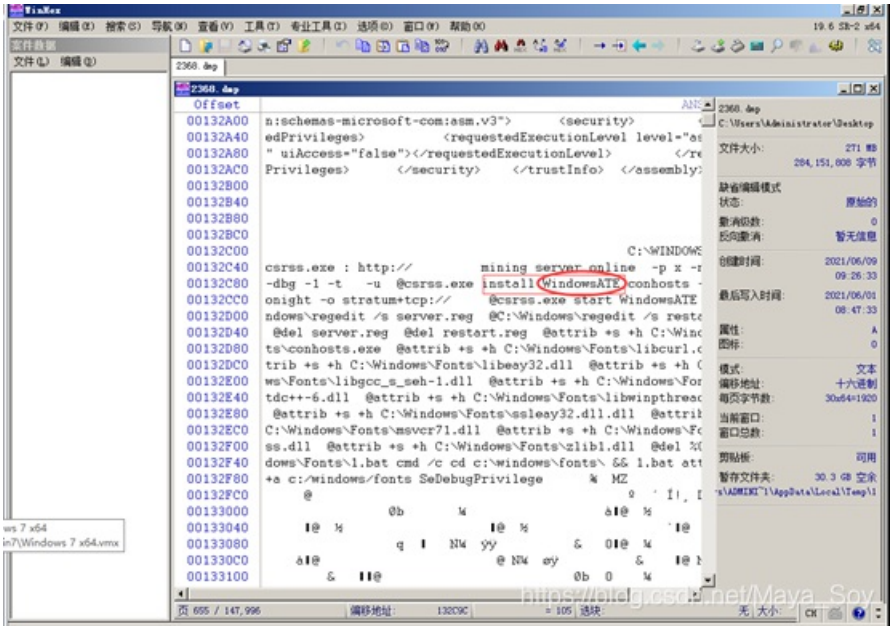
5. 恶意进程在系统中注册了服务，请将服务名以Flag{服务名}形式提交。

将进程导出来，然后使用Winhex分析






```
flag{WindowsATE}
```



6. 黑客在登录系统后下载了文件，请将文件内容作为flag提交；

```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 filescan | grep flag
```

```
┌──(root💀kali)-[~/Desktop/volatility]
└─# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 filescan | grep flag
Volatility Foundation Volatility Framework 2.6.1
0x000000003b33fb70     16      0 R--rwd \Device\HarddiskVolume2\Users\test\Desktop\flag.txt
0x000000003d9cc580      2      0 RW-rw- \Device\HarddiskVolume2\Users\test\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk

┌──(root💀kali)-[~/Desktop/volatility]
└─# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 filescan | grep flag
```

```
┌──(root💀kali)-[~/Desktop/volatility]
└─# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000003b33fb70 -D ./
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
DataSectionObject 0x3b33fb70    None    \Device\HarddiskVolume2\Users\test\Desktop\flag.txt

┌──(root💀kali)-[~/Desktop/volatility]
└─# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000003b33fb70 -D ./
```



```
┌──(root💀kali)-[~/Desktop/volatility]
└─# ls
2368.dmp      CHANGELOG.txt  dist                          LICENSE.txt  PKG-INFO          README.txt  tools                vo
AUTHORS.txt   contrib        file.None.0xfffffa800f6b6200.dat  Makefile     pyinstaller       resources   volatility
build         CREDITS.txt    LEGAL.txt                     MANIFEST.in  pyinstaller.spec  setup.py    volatility.egg-info

┌──(root💀kali)-[~/Desktop/volatility]
└─# cat file.None.0xfffffa800f6b6200.dat
flag{dasdqwdxczaqwcascas}

┌──(root💀kali)-[~/Desktop/volatility]
└─#
```