

2021陇剑杯网络安全大赛wp-内存取证（详细题解）

原创

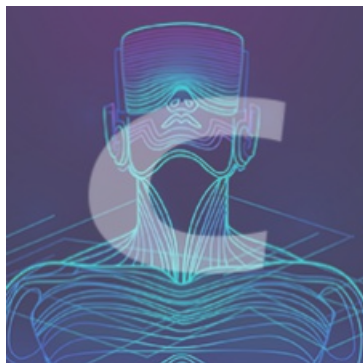
偷一个月亮 于 2021-09-15 14:28:11 发布 1393 收藏 1

分类专栏: [2021陇剑杯网络安全大赛 CTF](#) 文章标签: [网络安全](#)

本文为博主原创文章，未经博主允许不得转载，否则追究法律责任。

本文链接: <https://blog.csdn.net/yiqiushi4748/article/details/120307882>

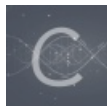
版权



[2021陇剑杯网络安全大赛](#) 同时被 2 个专栏收录

8 篇文章 46 订阅

订阅专栏



[CTF](#)

43 篇文章 5 订阅

订阅专栏

6.1



使用volatility对内存进行分析，配合mimikatz插件跑密码

```

root@m3rser:~/桌面# volatility -f Target.vmem --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6
Module  User          Domain          Password
-----
wdigest CTF             WIN-QUN5RVOOF27 flag{W31C0M3 T0 THiS 34SY F0R3NSiCX}
wdigest WIN-QUN5RVOOF27$ WORKGROUP
root@m3rser:~/桌面#

```

6.2

根据提示，使用filescan命令在内存中查找文件，发现华为备份文件

HUAWEI P40_2021xxxxxx, 搜索后发现多个相关文件，最后发现HUAWEI P40_2021-aa-bb xx.yy.zz.exe 为一自解压文件，解压后即备份

```

0x00000007e15d6b0 1 1 R--r-d \Device\HarddiskVolume1\Windows\System32\zh-CN\FerretBase.dll.mui
0x00000007e15f380 8 0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\hidusb.sys
0x00000007e15f780 17 0 RW-r-d \Device\HarddiskVolume1\Directory
0x00000007e15f4d0 9 0 R--r-d \Device\HarddiskVolume1\Windows\System32\credssp.dll
0x00000007e161c80 16 0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\zh-CN\rdhss.sys.mui
0x00000007e161d80 1 1 ----- \Device\NamedPipe\ntsvcs
0x00000007e163070 2 1 ----- \Device\NamedPipe\ntsvcs
0x00000007e1635e0 16 0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\shlwapi.dll
0x00000007e1639e0 1 1 ----- \Device\NamedPipe\scerpc
0x00000007e163b30 2 1 ----- \Device\NamedPipe\scerpc
0x00000007e163d80 1 1 ----- \Device\NamedPipe\scerpc
0x00000007e164b40 16 0 R--r-
\Device\HarddiskVolume1\Windows\WinSxS\Manifests\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e4
0x00000007e164cc0 12 0 R--r- \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb xx.yy.zz.exe
0x00000007e165590 15 0 R--r-d \Device\HarddiskVolume1\Windows\System32\FirewallAPI.dll
0x00000007e1659e0 1 1 ----- \Device\Afd\Endpoint
0x00000007e165f20 15 0 R--r-d \Device\HarddiskVolume1\Windows\System32\shqps.dll
0x00000007e1684b0 14 0 R--r-d \Device\HarddiskVolume1\Windows\System32\bcrypt.dll
0x00000007e168a00 7 0 R--r-d \Device\HarddiskVolume1\Windows\System32\authz.dll
0x00000007e168e00 15 0 R--r-d \Device\HarddiskVolume1\Windows\System32\ncrypt.dll
0x00000007e16b3f0 1 1 R--r- \Device\HarddiskVolume1\Windows\System32
0x00000007e16bd20 7 0 R--r-d \Device\HarddiskVolume1\Windows\System32\syntfy.dll
0x00000007e16c560 10 0 R--r-d \Device\HarddiskVolume1\Windows\System32\smapi.dll
0x00000007e16d280 15 0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\portcls.sys
0x00000007e16d6b0 1 1 RW---- \Device\HarddiskVolume1\Windows\System32\config\SECURITY.LOG1
0x00000007e16d7e0 1 1 RW---- \Device\HarddiskVolume1\Windows\System32\config\SECURITY.LOG2
0x00000007e16d9d0 1 1 RW---- \Device\HarddiskVolume1\Windows\System32\config\SECURITY

```

此电脑 > DATA (E:) > 随剑杯 > x64 > HUAWEI P40_2021-aa-bb-xx.yy.zz

名称	修改日期	类型	大小
picture	2021/8/29 15:45	文件夹	
alarm.db	2021/8/29 15:45	Data Base File	12 KB
info.xml	2021/8/29 15:55	XML 文档	3 KB
picture.xml	2021/8/29 15:45	XML 文档	1 KB

找到解密工具kobackupdec，根据上一步提示，根据提示将空格替换为_，解密成功



flag{TH4NK Y0U FOR DECRYPTING MY DATA}