Forenseec WRITEUP

By using volatility is possible to discover that the file is a Windows memory dump, this is the output from `python2 vol.py imageinfo -f 699cef6a816882f0e02b40e1fe4d7e93.raw` :

```
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x86_18362, Win10x86_17763
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/vittorio/Forensics200/6
                      PAE type : PAE
                           DTB : 0x1a8000L
                          KDBG : 0x81895770L
          Number of Processors : 4
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x80a05000L
                KPCR for CPU 1 : 0x8a125000L
                KPCR for CPU 2 : 0x8a1a0000L
                KPCR for CPU 3 : 0x8a1f3000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-10-03 15:30:35 UTC+0000
     Image local date and time : 2020-10-03 17:30:35 +0200
python2 vol.py imageinfo -f ../699cef6a816882f0e02b40e1fe4d7e93.raw lsadump  51,
```

Now we can use `pslist` volatility plugin in order to see what processes were running at the moment of the dump.

```
kali@kali:~/Downloads/volatility$ python2 vol.py pslist -f 699cef6a816882f0e02b4
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Star
---------- -------------------- ------ ------ ------ -------- ------ ------ ----
0x87d67040 System                    4      0    129        0 ------      0 2020
0x8b02a040 Registry                104      4      4        0 ------      0 2020

...
0x9290b980 TimeVault.exe          5496   3948      6        0      1      0 2020
```

```
...
```

The most suspicius one is the process named `TimeVault.exe` , let's dump the executable file related to the process with the following command:

```
kali@kali:~/Downloads$ python2 procdump -f 699cef6a816882f0e02b40e1fe4d7e93.raw
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x9290b980 0x00820000 TimeVault.exe        OK: executable.5496.exe
python2 vol.py procdump -f 699cef6a816882f0e02b40e1fe4d7e93.raw --dump-dir . -p
```

By opening the resulting executable file with wine, we find out that it requires a password. By launching `strings` in the raw file and using `grep -i TimeVault` as filter we were able to discover an url: `http://timevault.ddns.net:8080/` . The site is not actually up but we find out that the site was reachable by using WaybackMachine, a snapshot is present from October 2013: `https://web.archive.org/web/20201003151234/http://timevault.ddns.net:8080/` . Searching in the source of the page we find an interesting comment: `<!--if my calculations are correct, when this challenge hits 88 miles per hour, you're gonna see some serious PWD c54a1db0b68d3c039df1e25569fc67b7-->` . when we used `c54a1db0b68d3c039df1e25569fc67b7` as password for the executable file we collected a link: `Decrypted data: gamebox1.reply.it/b8216e21b7d4030dc263f82416389175/Wait_a_minute_Zer0_Are_you_telling_me_you_built_a_time_challenge_out_of_a_DeLorean` . The page pointed by the link asked us to login with username and password. At this point we tried several other things, when we tried lsadump plugin, we collected the following output from volatility

```
kali@kali:~/Downloads/volatility$ (git)-[master] % python2 vol.py -f ../699cef6a8
Volatility Foundation Volatility Framework 2.6.1
DPAPI_SYSTEM
0x00000000  2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ,...............
0x00000010  01 00 00 00 ad db 6e 2f f0 4b 37 86 86 00 5f 54   ......n/.K7..._T
0x00000020  50 5b bc 6c 90 03 44 38 16 14 ae 3c 66 c7 3f de   P[.l..D8...<f.?.
0x00000030  aa c3 ae 35 6c 9e 01 f6 c5 99 28 0e 00 00 00 00   ...5l.....(.....

NL$KM
0x00000000  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   @...............
0x00000010  61 a3 c4 dc 7c 2a 72 78 96 d5 14 5d 20 ca 52 d6   a...|*rx...]..R.
0x00000020  9b 04 c2 46 5e d2 b8 1d f7 e3 d9 fb db 25 96 b7   ...F^........%..
0x00000030  cf c9 83 49 20 62 10 fc 94 fc c4 a8 68 79 13 bc   ...I.b......hy..
0x00000040  4f e2 f1 c6 df 66 4a 4a a6 ca 06 21 2f fd 89 c7   O....fJJ...!/...
0x00000050  c8 b8 81 71 48 d3 b0 bd f1 93 35 ba 2b 36 76 ab   ...qH.....5.+6v.

L$_SQSA_S-1-5-21-2222777348-539284984-4271348667-1001
0x00000000  06 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  7b 00 22 00 76 00 65 00 72 00 73 00 69 00 6f 00   {.".v.e.r.s.i.o.
0x00000020  6e 00 22 00 3a 00 31 00 2c 00 22 00 71 00 75 00   n.".:.1.,.".q.u.
0x00000030  65 00 73 00 74 00 69 00 6f 00 6e 00 73 00 22 00   e.s.t.i.o.n.s.".
0x00000040  3a 00 5b 00 7b 00 22 00 71 00 75 00 65 00 73 00   :.[.{.".q.u.e.s.
0x00000050  74 00 69 00 6f 00 6e 00 22 00 3a 00 22 00 57 00   t.i.o.n.".:.".W.
0x00000060  68 00 61 00 74 00 20 00 77 00 61 00 73 00 20 00   h.a.t...w.a.s...
0x00000070  79 00 6f 00 75 00 72 00 20 00 66 00 69 00 72 00   y.o.u.r...f.i.r.
0x00000080  73 00 74 00 20 00 70 00 65 00 74 00 19 20 73 00   s.t...p.e.t...s.
0x00000090  20 00 6e 00 61 00 6d 00 65 00 3f 00 22 00 2c 00   ..n.a.m.e.?.".,.
0x000000a0  22 00 61 00 6e 00 73 00 77 00 65 00 72 00 22 00   ".a.n.s.w.e.r.".
0x000000b0  3a 00 22 00 62 00 65 00 64 00 74 00 69 00 6d 00   :.".b.e.d.t.i.m.
0x000000c0  65 00 62 00 75 00 64 00 64 00 79 00 22 00 7d 00   e.b.u.d.d.y.".}.
0x000000d0  2c 00 7b 00 22 00 71 00 75 00 65 00 73 00 74 00   ,.{.".q.u.e.s.t.
0x000000e0  69 00 6f 00 6e 00 22 00 3a 00 22 00 57 00 68 00   i.o.n.".:.".W.h.
0x000000f0  61 00 74 00 19 20 73 00 20 00 74 00 68 00 65 00   a.t...s...t.h.e.
0x00000100  20 00 6e 00 61 00 6d 00 65 00 20 00 6f 00 66 00   ..n.a.m.e...o.f.
0x00000110  20 00 74 00 68 00 65 00 20 00 63 00 69 00 74 00   ..t.h.e...c.i.t.
0x00000120  79 00 20 00 77 00 68 00 65 00 72 00 65 00 20 00   y...w.h.e.r.e...
0x00000130  79 00 6f 00 75 00 20 00 77 00 65 00 72 00 65 00   y.o.u...w.e.r.e.
0x00000140  20 00 62 00 6f 00 72 00 6e 00 3f 00 22 00 2c 00   ..b.o.r.n.?.".,.
0x00000150  22 00 61 00 6e 00 73 00 77 00 65 00 72 00 22 00   ".a.n.s.w.e.r.".
0x00000160  3a 00 22 00 62 00 65 00 64 00 74 00 69 00 6d 00   :.".b.e.d.t.i.m.
0x00000170  65 00 62 00 75 00 64 00 64 00 79 00 22 00 7d 00   e.b.u.d.d.y.".}.
0x00000180  2c 00 7b 00 22 00 71 00 75 00 65 00 73 00 74 00   ,.{.".q.u.e.s.t.
0x00000190  69 00 6f 00 6e 00 22 00 3a 00 22 00 57 00 68 00   i.o.n.".:.".W.h.
0x000001a0  61 00 74 00 20 00 77 00 61 00 73 00 20 00 79 00   a.t...w.a.s...y.
0x000001b0  6f 00 75 00 72 00 20 00 63 00 68 00 69 00 6c 00   o.u.r...c.h.i.l.
0x000001c0  64 00 68 00 6f 00 6f 00 64 00 20 00 6e 00 69 00   d.h.o.o.d...n.i.
0x000001d0  63 00 6b 00 6e 00 61 00 6d 00 65 00 3f 00 22 00   c.k.n.a.m.e.?.".
0x000001e0  2c 00 22 00 61 00 6e 00 73 00 77 00 65 00 72 00   ,.".a.n.s.w.e.r.
0x000001f0  22 00 3a 00 22 00 62 00 65 00 64 00 74 00 69 00   ".:.".b.e.d.t.i.
0x00000200  6d 00 65 00 62 00 75 00 64 00 64 00 79 00 22 00   m.e.b.u.d.d.y.".
0x00000210  7d 00 5d 00 7d 00 00 00 00 00 00 00 00 00 00 00   }.].}...........

python2 vol.py -f ../699cef6a816882f0e02b40e1fe4d7e93.raw lsadump   12,73s user 1
```

With a little bit of guessing we find out that the following credentials works on the login form of the page: `Zer0:bedtimebuddy` .
Once we logged in, we got the flag: `{FLG:3v3n_R4M_l4st_f0r3v3r}`