Command & Control - level 2 ✍

Title: Memory analysis

Point: 15 Points

Level: Easy

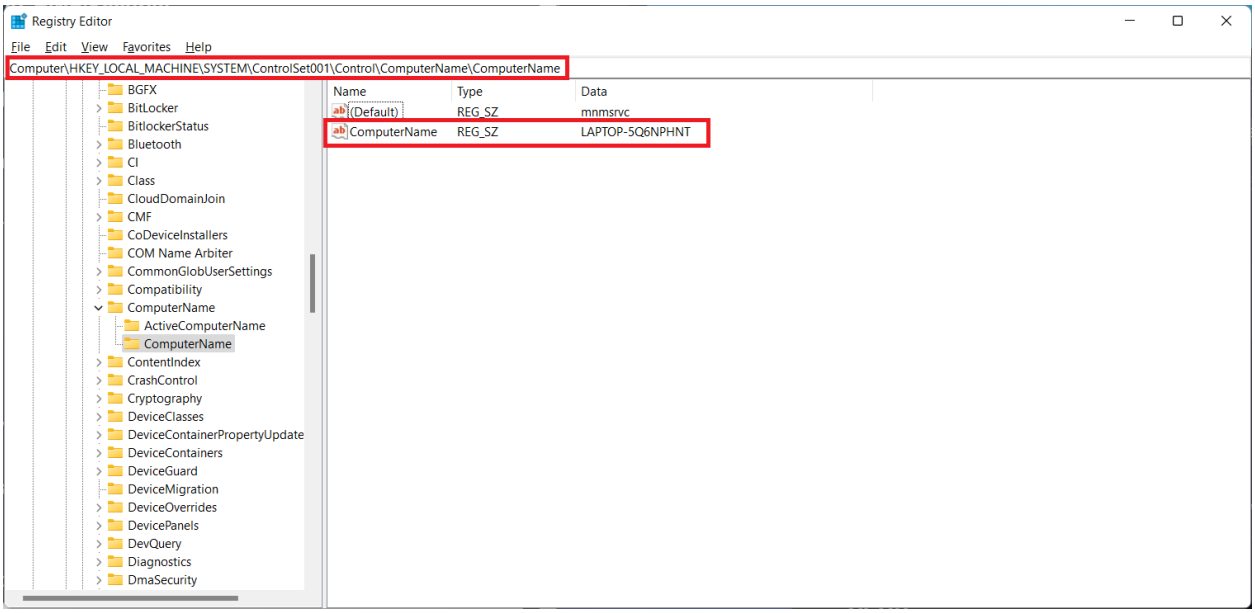
Description: Congratulations Berthier, thanks to your help the computer has been identified. You have requested a memory dump but before starting your analysis you wanted to take a look at the antivirus' logs. Unfortunately, you forgot to write down the workstation's hostname. But since you have its memory dump you should be able to get it back!

The validation flag is the workstation's hostname.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

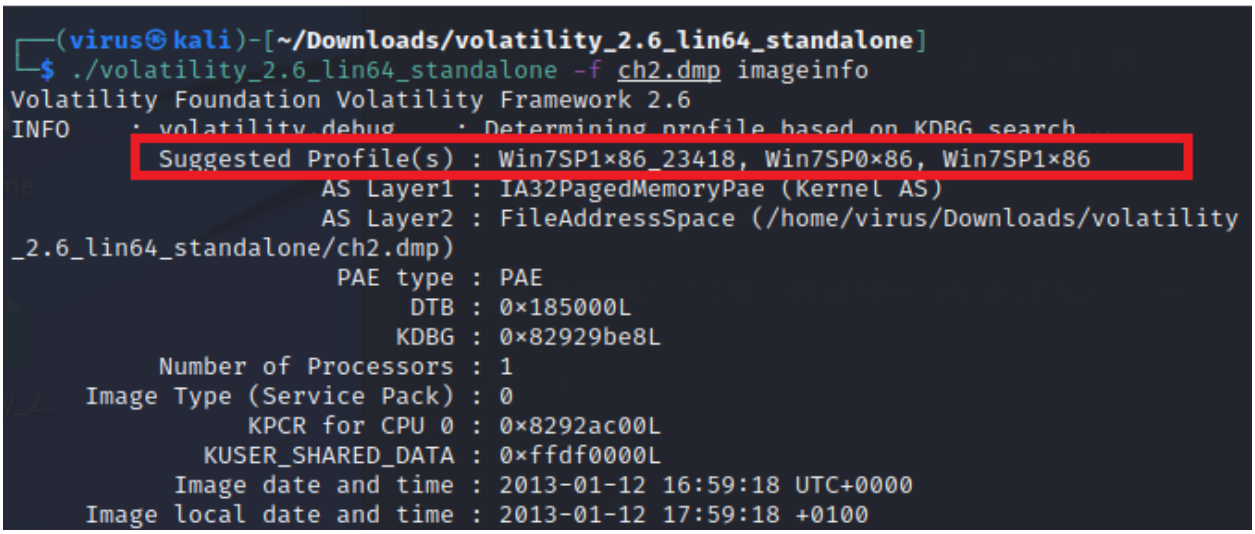
Solution:

Công cụ sử dụng: `Volatility`
Ta nhận được một file nén nhiều lớp.
Giải nén với **Bzip2**: `bzip2 -d ch2.tbz2`
Giải nén với **POSIX tar archive**: `tar -xf ch2.tar`
Bây giờ ta sẽ dump file **ch2.dmp**. Sau đó chúng ta có thể lấy **hostname** thông qua `registry`. Thông thường thông tin này được lưu trữ ở path `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName`
Ví dụ, trên máy của mình:



Ban đầu ta dump để lấy các **Profile** khả dụng. Sử dụng `imageinfo`:

```
./volatility_2.6_lin64_standalone -f ch2.dmp imageinfo
```



Dùng `Win7SP0x86` hoặc bất kỳ phiên bản profile nào khác để "nạo" thông tin trên registry Use `hivelist`:

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 hivelist
```

```
┌──(virus㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClas
s.dat
0x9aad6148 0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY
0x9aba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720 0x0a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8b20c008 0x039e1008 [no name]
0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD
```

Chúng ta sẽ dump thông tin ở địa chỉ cụ thể (ở đây mình quan tâm đến `\REGISTRY\MACHINE\SYSTEM` có địa chỉ ảo là `0x8b21c008`) trong **hivelist** và "chiết xuất " giá trị . Sử dụng `printkey` với flag `-K` để chỉ ra phần còn lại của **path KPCR**:

```
./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 printkey -o
0x8b21c008  -K 'ControlSet001\Control\ComputerName\ComputerName'
```

```
┌──(virus㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ch2.dmp --profile=Win7SP0x86 printkey -o 0
x8b21c008  -K 'ControlSet001\Control\ComputerName\ComputerName'
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2013-01-12 00:58:30 UTC+0000

Subkeys:

Values:
REG_SZ                        : (S) mnmsrvc
REG_SZ        ComputerName    : (S) WIN-ETSA91RKCFP
```

Vậy là xong <3

FLag: **WIN-ETSA91RKCFP**