Cyber Forensics Quiz 4

tags: `class`

Suspicious Connections

There were only two connections:

```
~/g/cyber-forensics … hw/quiz4 ./volatility_2.6_lin64_standalone -f example.img  connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
```

Looking at the pid, I found that the suspicious program was svchost.exe

```
0x80ff88d8 svchost.exe            856    676     29      336      0      0 2010-08-11 06:06:24 UTC+0000
```

Dump the memory

```
! ~/g/cyber-forensics … hw/quiz4 strings example.img | grep 193.104.41.75
://193.104.41.75/cbd/75.bro
://193.104.41.75/cbd/75.bro
193.104.41.75
: 193.104.41.75
q CKM193.104.41.75
http://193.104.41.75/cbd/75.bro
193.104.41.75
~/g/cyber-forensics … hw/quiz4
```

URL

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/tspy_zbot.cem

Executable Search Result

```
  REG_SZ         System          : (S)
  REG_SZ         Userinit        : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
  REG_SZ         VmApplet        : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
  REG_DWORD      SfcQuota        : (S) 4294967295
```