Setting up the environment

Computer Science, Texas Tech University

Setting up the environment

In this exercise, we are going to run the rootkit: WindowsRegistryRootkit with the given link address: https://github.com/Cr4sh/WindowsRegistryRootkit

This rootkit will exploit the vulnerability of the win32k.sys on the 32bit OS. That is, hiding the shellcode in Registry value, and employs the function win32k!bInitializeEUDC() to get execution when Window startup.

This rootkit will be run on Windows7 SP1 32bit (it does not work with 64 bit). We setup a clean windows 7 trial version. We install Chrome browser only.

Purpose of the study:

In this study, I try to locate the shellcode hiding in the Registry.

Existing approach

I've tried multiple approach with Linux but none of them get succeeded. The hardest problem is reading the memory dump file in Linux. I followed a lot of approaches on the internet. The most complete one is: https://www.jamesbower.com/linux-memory-analysis/ which have the following important steps.

1) We'll first make sure our Ubuntu 16.04 Server box is completely upgraded.

2) Next we will install the proper dependencies for both LiME and Volatility.

3) We'll install and configure LiME.

4) Then we'll install and configure Volatility.

5) Finally, we'll create a test memory dump for the memory analysis. And use it to test that Volatility is working.

I've tried different version of Linux, but none of them worked.

```
vjnh@vjnh-VirtualBox:~/volatility$ sudo python vol.py -f test.lime --profile=Li
nuxUbuntu1604x64 linux_pslist
Volatility Foundation Volatility Framework 2.6
Offset             Name                 Pid             PPid            Uid
        Gid    DTB                Start Time
------------------ -------------------- -------------- -------------- -------
-------- ------ ------------------ ----------
No suitable address space mapping found
Tried to open image as:
 MachOAddressSpace: mac: need base
 LimeAddressSpace: lime: need base
 WindowsHiberFileSpace32: No base Address Space
 WindowsCrashDumpSpace64BitMap: No base Address Space
 WindowsCrashDumpSpace64: No base Address Space
 HPAKAddressSpace: No base Address Space
```

Current Approach ended up with setting up Windows in virtual machine and run a rootkit inside that environment. Dump the memory file and use volatility to analyze that file.

Procedure for memory acquisition.

1. Download Windows 7 SP1 from Microsoft page. Trial version expire in 30 days. Set default memory size to 8GB to speed up the installation.
2. After setting up the Windows 7, we install Chrome. Download the **DumpIt** and the rootkit **WindowRegistryRootkit**.
3. Shutdown Windows 7, set the memory RAM to 1Gb. At this time, we don't need to much RAM for the system, so 1Gb is reasonable.
4. Run the Rootkit, dump the memory file, and copy this memory file to the host folder.

Analyzing process.

There are two approaches to analyze the window memory file. If we use Windows as the main operating system, we can use Volatility for Windows at this link below

http://www.volatilityfoundation.org/24

If we use Linux, we can get volatility at: https://github.com/volatilityfoundation/volatility

In this report, I used Volatility for Window, this picture below shows the screenshot of the first command. The recommend profiles are Win7SP0x86 and Win7SP1x86.

```
C:\Users\iDVLab\Documents\vol>volatility-2.5.standalone.exe -f Win7.raw imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\iDVLab\Documents\vol\Win7.raw)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x82952c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82953c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-05-04 04:48:19 UTC+0000
     Image local date and time : 2018-05-03 21:48:19 -0700
```

The first one (as we usually select) is not always true. Since, I know that my OS is Win7SP1x86, so my command will be shown in Figure below.

```
C:\Users\iDVLab\Documents\vol>volatility-2.5.standalone.exe -f May4.raw --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------
0x84212798 System                    4      0     79      545 ------      0 2018-05-04 06:43:47 UTC+0000
0x85754830 smss.exe                268      4      2       29 ------      0 2018-05-04 06:43:47 UTC+0000
0x858b7d40 csrss.exe               344    328      9      451      0      0 2018-05-04 06:43:48 UTC+0000
0x85175a58 wininit.exe             380    328      3       76      0      0 2018-05-04 06:43:48 UTC+0000
0x85176928 csrss.exe               388    372      7      198      1      0 2018-05-04 06:43:48 UTC+0000
0x8595c610 services.exe            444    380     12      207      0      0 2018-05-04 06:43:48 UTC+0000
0x85976870 lsass.exe               452    380      8      559      0      0 2018-05-04 06:43:48 UTC+0000
0x85978b90 lsm.exe                 460    380     10      145      0      0 2018-05-04 06:43:48 UTC+0000
0x85977b90 winlogon.exe            472    372      5      117      1      0 2018-05-04 06:43:48 UTC+0000
0x859f1a18 svchost.exe             592    444     10      358      0      0 2018-05-04 06:43:49 UTC+0000
0x85a0a150 VBoxService.ex          656    444     12      117      0      0 2018-05-04 06:43:49 UTC+0000
0x85971d40 svchost.exe             708    444      9      287      0      0 2018-05-04 04:43:50 UTC+0000
0x85a368f0 svchost.exe             776    444     20      456      0      0 2018-05-04 04:43:50 UTC+0000
0x85a63b48 svchost.exe             880    444     24      454      0      0 2018-05-04 04:43:50 UTC+0000
0x85a6b9c0 svchost.exe             916    444     47     2467      0      0 2018-05-04 04:43:50 UTC+0000
0x85a75100 audiodg.exe             980    776      6      130      0      0 2018-05-04 04:43:50 UTC+0000
0x85a90030 svchost.exe            1088    444     11      287      0      0 2018-05-04 04:43:50 UTC+0000
0x85aa3c28 svchost.exe            1196    444     19      398      0      0 2018-05-04 04:43:50 UTC+0000
0x85aca570 spoolsv.exe            1296    444     12      281      0      0 2018-05-04 04:43:51 UTC+0000
0x85ae0a40 svchost.exe            1332    444     19      320      0      0 2018-05-04 04:43:51 UTC+0000
0x85b33030 svchost.exe            1432    444     15      248      0      0 2018-05-04 04:43:51 UTC+0000
0x85c28568 taskhost.exe           1924    444     10      201      1      0 2018-05-04 04:43:54 UTC+0000
0x85c34d40 taskeng.exe            1980    916      4       79      0      0 2018-05-04 04:43:55 UTC+0000
0x85c47d40 dwm.exe                1992    880      3       71      1      0 2018-05-04 04:43:55 UTC+0000
0x85c41358 explorer.exe           2012   1972     36      968      1      0 2018-05-04 04:43:55 UTC+0000
0x86b823d0 VBoxTray.exe           1508   2012     13      154      1      0 2018-05-04 04:43:55 UTC+0000
0x85cb6030 GoogleCrashHan         2004   1584      6       94      0      0 2018-05-04 04:43:55 UTC+0000
0x851215d0 SearchIndexer.         2036    444     11      617      0      0 2018-05-04 04:44:01 UTC+0000
0x85b8f7e0 wmpnetwk.exe           1352    444      9      212      0      0 2018-05-04 04:44:01 UTC+0000
0x84fd25d8 WmiPrvSE.exe           2784    592      6      116      0      0 2018-05-04 04:44:52 UTC+0000
0x84320b30 mscorsvw.exe           3960    444      6       76      0      0 2018-05-04 21:04:45 UTC+0000
0x843aa030 sppsvc.exe             4088    444      4      147      0      0 2018-05-04 21:04:46 UTC+0000
0x843ef680 svchost.exe            1580    444     11      308      0      0 2018-05-04 21:04:46 UTC+0000
0x843ae9c0 WmiPrvSE.exe            860    592      8      185      0      0 2018-05-04 21:04:47 UTC+0000
0x85251030 TrustedInstall         2420    444      9      399      0      0 2018-05-04 21:05:32 UTC+0000
0x86af0438 SearchProtocol          144   2036      7      328      0      0 2018-05-04 21:05:51 UTC+0000
0x8598bb50 SearchFilterHo         2664   2036      5      105      0      0 2018-05-04 21:05:54 UTC+0000
0x85c477b8 rootkit_instal         2824   2012      1       72      1      0 2018-05-04 21:06:03 UTC+0000
0x84386bf8 conhost.exe            2132    388      2       53      1      0 2018-05-04 21:06:03 UTC+0000
0x85afe4c0 WMIADAP.exe            2084    916      6       89      0      0 2018-05-04 21:06:45 UTC+0000
0x84958798 DumpIt.exe             2800   2012      2       39      1      0 2018-05-04 21:07:36 UTC+0000
0x847f6ac8 conhost.exe            3384    388      2       54      1      0 2018-05-04 21:07:36 UTC+0000
```

We can see the rootkit_install is shown when we run the pslist. Going to detail of this process

```
C:\Users\iDVLab\Documents\vol>volatility-2.5.standalone.exe -f May4.raw --profile=Win7SP1x86 dlllist -p 2824
Volatility Foundation Volatility Framework 2.5
************************************************************************
rootkit_instal pid:   2824
Command line : "C:\Users\iDVLab\Downloads\WindowsRegistryRootkit-master\WindowsRegistryRootkit-master\bin\rootkit_installer.exe"
Service Pack 1

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00230000    0x2a000     0xffff C:\Users\iDVLab\Downloads\WindowsRegistryRootkit-master\WindowsRegistryRootkit-master\bin\rootkit_installer.exe
0x77420000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
0x75b20000    0xd4000     0xffff C:\Windows\system32\kernel32.dll
0x75800000    0x4a000     0xffff C:\Windows\system32\KERNELBASE.dll
0x76ff0000    0xc9000     0xffff C:\Windows\system32\USER32.dll
0x775f0000    0x4e000     0xffff C:\Windows\system32\GDI32.dll
0x759b0000     0xa000     0xffff C:\Windows\system32\LPK.dll
0x75c40000    0x9d000     0xffff C:\Windows\system32\USP10.dll
0x76e40000    0xac000     0xffff C:\Windows\system32\msvcrt.dll
0x76a10000    0xa0000     0xffff C:\Windows\system32\ADVAPI32.dll
0x759c0000    0x19000     0xffff C:\Windows\SYSTEM32\sechost.dll
0x75a70000    0xa1000     0xffff C:\Windows\system32\RPCRT4.dll
0x754a0000    0x4c000     0xffff C:\Windows\system32\apphelp.dll
0x6a920000   0x218000     0xffff C:\Windows\AppPatch\AcGenral.DLL
0x75480000    0x1b000        0x6 C:\Windows\system32\SspiCli.dll
0x75ce0000    0x57000       0x1e C:\Windows\system32\SHLWAPI.dll
0x742f0000    0x40000        0x8 C:\Windows\system32\UxTheme.dll
0x73b00000    0x32000        0xc C:\Windows\system32\WINMM.dll
0x73d50000     0xf000        0x6 C:\Windows\system32\samcli.dll
0x770c0000   0x15c000       0x13 C:\Windows\system32\ole32.dll
0x759e0000    0x8f000       0x12 C:\Windows\system32\OLEAUT32.dll
0x73a50000    0x14000        0x6 C:\Windows\system32\MSACM32.dll
0x74b70000     0x9000        0x6 C:\Windows\system32\VERSION.dll
0x75d90000   0xc4a000        0x6 C:\Windows\system32\SHELL32.dll
0x70d30000     0x3000        0x6 C:\Windows\system32\sfc.dll
0x70d20000     0xd000        0x2 C:\Windows\system32\sfc_os.DLL
0x74bd0000    0x17000        0x6 C:\Windows\system32\USERENV.dll
0x75570000     0xb000        0x6 C:\Windows\system32\profapi.dll
0x73fc0000    0x13000        0x7 C:\Windows\system32\dwmapi.dll
0x76ab0000   0x19d000        0x6 C:\Windows\system32\SETUPAPI.dll
0x75620000    0x27000        0xc C:\Windows\system32\CFGMGR32.dll
0x75850000    0x12000        0x6 C:\Windows\system32\DEVOBJ.dll
0x75870000   0x136000        0xc C:\Windows\system32\urlmon.dll
0x76ef0000     0xf5000        0x6 C:\Windows\system32\WININET.dll
0x77220000   0x1fb000        0xc C:\Windows\system32\iertutil.dll
0x756e0000   0x11d000        0x6 C:\Windows\system32\CRYPT32.dll
0x755e0000     0xc000        0x6 C:\Windows\system32\MSASN1.dll
0x70900000    0x12000        0x6 C:\Windows\system32\MPR.dll
0x77560000    0x1f000        0x2 C:\Windows\system32\IMM32.DLL
0x76c60000    0xcc000        0x1 C:\Windows\system32\MSCTF.dll
0x754f0000     0xc000        0x1 C:\Windows\system32\CRYPTBASE.dll
```

We can see a list of libraries this process called. We can also see what's going on if the user gives any commands by using the consoles parameter

```
*************************************************************

 Windows kernrel rootkit PoC using registry values processing BoF.
 FOR INTERNAL USE ONLY!

 (c) 2012 Oleksiuk Dmytro (aka Cr4sh)
 cr4sh@riseup.net

*************************************************************

[+] Disabling DEP...
The operation completed successfully.
The operation completed successfully.
[+] 1-st shellcode size is 67 bytes
[+] 2-nd shellcode size is 350 bytes
AnalyseWin32k(): "\Windows\WindowStations" referenced at offset 0x00005f97
AnalyseWin32k(): win32k!UserInitialize() found at offset 0x00005f7f
AnalyseWin32k(): "FontLinkDefaultChar" referenced at offset 0x00014e44
AnalyseWin32k(): win32k!bInitializeEUDC() CALL EDI found at offset 0x00014e4d
nt!MmIsAddressValid() offset is 0x0000a12a
nt!PsGetCurrentProcess() offset is 0x0009f13c
nt!PsGetProcessWin32Process() offset is 0x000a6f84
nt!ExAllocatePool() offset is 0x00015da6
nt!RtlQueryRegistryValues() offset is 0x002649ee
nt!DbgPrint() offset is 0x000121ea
[+] Saving 2-nd shellcode to "System\CurrentControlSet\Control\Configuration Dat
a"...
[+] SUCCESS
[+] Saving rootkit image to "System\CurrentControlSet\Control\PCI"...
[+] SUCCESS
[+] Adding malicious data for value "Software\Microsoft\Windows NT\CurrentVersio
n\FontLink\FontLinkDefaultChar"...
[+] SUCCESS
*************************************************
```

From this log file, we have some information such as

Shellcode is saved to “System\CurrentControlSet\Control\Configuration Data”

Rootkit image is saved to “System\CurrentControlSet\Control\PCI”…

And Malicious data for value is saved in “Software\Microsoft\Windows NT\CurrentVersion\FontLink\FontLinkDefaultChar”

We could go further by investing Registry.

First, let’s see what is current registry saved in memory by using hivelist

```
C:\Users\iDVLab\Documents\vol>volatility-2.5.standalone.exe -f May4.raw --profile=Win7SP1x86 hivelist
Volatility Foundation Volatility Framework 2.5
Virtual    Physical   Name
---------- ---------- ----
0x8900c800 0x25a6a800 [no name]
0x8901a4c8 0x2592c4c8 \REGISTRY\MACHINE\SYSTEM
0x89042008 0x343d9008 \REGISTRY\MACHINE\HARDWARE
0x890bc9c8 0x183049c8 \SystemRoot\System32\Config\DEFAULT
0x89612008 0x0ae5f008 \SystemRoot\System32\Config\SECURITY
0x89656298 0x17a52298 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x896a49c8 0x1b5de9c8 \SystemRoot\System32\Config\SAM
0x89760500 0x2e1f2500 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x8e8999c8 0x1d9d49c8 \??\C:\Windows\System32\config\COMPONENTS
0x8f073008 0x1cb1e008 \Device\HarddiskVolume1\Boot\BCD
0x8f0739c8 0x1cb1e9c8 \SystemRoot\System32\Config\SOFTWARE
0x921bb380 0x17345380 \??\C:\System Volume Information\Syscache.hve
0x922619c8 0x15e529c8 \??\C:\Users\iDVLab\AppData\Local\Microsoft\Windows\UsrClass.dat
0x923219c8 0x204fe9c8 \??\C:\Users\iDVLab\ntuser.dat
0xb698e9c8 0x0a8149c8 \??\C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT
```

Not much information I can find from here. So I dump the Registry into files with command “registrydump”. It gives me a list of registry files.

```
C:\Users\iDVLab\Documents\vol>volatility-2.5.standalone.exe -f May4.raw --profile=Win7SP1x86 dumpregistry -D dump/
```

registry.0x8e8999c8.COMPONENTS.reg	5/4/2018 6:55 PM	Registration Entries	29,960 KB
registry.0x8f0739c8.SOFTWARE.reg	5/4/2018 6:55 PM	Registration Entries	23,544 KB
registry.0x8f073008.BCD.reg	5/4/2018 6:55 PM	Registration Entries	28 KB
registry.0x890bc9c8.DEFAULT.reg	5/4/2018 6:55 PM	Registration Entries	156 KB
registry.0x896a49c8.SAM.reg	5/4/2018 6:55 PM	Registration Entries	24 KB
registry.0x921bb380.Syscachehve.reg	5/4/2018 6:55 PM	Registration Entries	108 KB
registry.0x8900c800.no_name.reg	5/4/2018 6:55 PM	Registration Entries	8 KB
registry.0x8901a4c8.SYSTEM.reg	5/4/2018 6:55 PM	Registration Entries	9,840 KB
registry.0x922619c8.UsrClassdat.reg	5/4/2018 6:55 PM	Registration Entries	128 KB
registry.0x923219c8.ntuserdat.reg	5/4/2018 6:55 PM	Registration Entries	504 KB
registry.0x89042008.HARDWARE.reg	5/4/2018 6:55 PM	Registration Entries	28 KB
registry.0x89612008.SECURITY.reg	5/4/2018 6:55 PM	Registration Entries	24 KB
registry.0x89656298.NTUSERDAT.reg	5/4/2018 6:55 PM	Registration Entries	240 KB
registry.0x89760500.NTUSERDAT.reg	5/4/2018 6:55 PM	Registration Entries	236 KB
registry.0xb698e9c8.SCHEMADAT.reg	5/4/2018 6:55 PM	Registration Entries	6,400 KB

Open the registry and find the path based on the consoles log, I found interesting values

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]
"PreshutdownOrder"=hex(7):77,00,75,00,61,00,75,00,73,00,65,00,72,00,76,00,00,\
  00,67,00,70,00,73,00,76,00,63,00,00,00,74,00,72,00,75,00,73,00,74,00,65,00,\
  64,00,69,00,6e,00,73,00,74,00,61,00,6c,00,6c,00,65,00,72,00,00,00,00,00
"WaitToKillServiceTimeout"="12000"
"CurrentUser"="USERNAME"
"BootDriverFlags"=dword:00000000
"ServiceControlManagerExtension"=hex(2):25,00,73,00,79,00,73,00,74,00,65,00,6d,\
  00,72,00,6f,00,6f,00,74,00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,\
  33,00,32,00,5c,00,73,00,63,00,65,00,78,00,74,00,2e,00,64,00,6c,00,6c,00,00,\
  00
"SystemStartOptions"=" EXECUTE  NOEXECUTE=ALWAYSOFF  PAE"
"SystemBootDevice"="multi(0)disk(0)rdisk(0)partition(2)"
"FirmwareBootDevice"="multi(0)disk(0)rdisk(0)partition(1)"
"Configuration Data"=hex:40,50,41,51,90,90,90,90,90,90,90,90,90,90,90,90,90,40,\
  50,41,51,90,90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,90,90,\
  90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,90,90,90,90,90,90,90,90,90,\
  40,50,41,51,90,90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,90,\
  90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,90,90,90,90,90,90,90,\
  90,40,50,41,51,90,90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,\
  90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,90,90,90,90,90,90,\
  90,90,40,50,41,51,90,90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,\
  90,90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,90,90,90,90,90,\
  90,90,90,40,50,41,51,90,90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,\
  90,90,90,90,90,90,90,90,90,90,90,90,90,40,50,41,51,90,90,90,90,90,90,90,\
  90,90,90,90,cc,8b,f3,e8,00,00,00,00,5b,81,eb,a8,16,23,00,66,33,f6,66,81,3e,\
  4d,5a,74,08,81,ee,00,10,00,00,eb,f1,89,b3,02,18,23,00,8b,8b,0e,18,23,00,2b,\
  f9,89,bb,fe,17,23,00,8b,8b,26,18,23,00,03,ce,0f,20,c0,25,ff,ff,fe,ff,0f,22,\
```

This data is in Hex value, we need to convert them into ASCII. I found the shellcode

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]
"PreshutdownOrder"=[REG_MULTI_SZ] wuauserv gpsvc trustedinstaller
"WaitToKillServiceTimeout"="12000"
"CurrentUser"="USERNAME"
"BootDriverFlags"=[REG_DWORD] 0
"ServiceControlManagerExtension"=[REG_EXPAND_SZ] %systemroot%\system32\scext.dll
"SystemStartOptions"=" EXECUTE  NOEXECUTE=ALWAYSOFF  PAE"
"SystemBootDevice"="multi(0)disk(0)rdisk(0)partition(2)"
"FirmwareBootDevice"="multi(0)disk(0)rdisk(0)partition(1)"
"Configuration Data"=[REG_BINARY:<UTF16-LE,2-byte>] ##j8Bjh}u##*#PPCI&!
"PCI"=[REG_BINARY:<UTF16-LE,2-byte>] @.$L0A<h@t a@ @XdBogusProtoxNxxxC!xNx"xtTCPIPxxdwinlogon.exed!xx)x\HTTP.sys\mrxsmb.sys\mrxsmb10.sys
\mrxsmb20.sys\srv.sys\srv2.sys
\secdrv.sysxxhal.dllntoskrnl.exehal.dllhalacpi.dllhalapic.dllhalmps.dllhalaacpi.dllhalmacpi.dllntoskrnl.exentkrnlpa.exentkrnlmp.exentkrpamp.exeH
bjpP ---oE280xp@]xQE]GEutuDuG>?$Etjj-t EjM1tju(}UEMUMU,%Mh0E&jEBTQsHE1Mj,%jjjjhMjjj EMUh0RHAABH-jjjM@jjj-|jjh$j<jj6}--(uu4uu8u@-tM$,
%EQtH9t:vj5BMjMUEU`UE9t:vjmQjjjjjMUE9:jUMUEjjEEBHB-tj-!EUEMUUt-jEMUUEMM~j-=..}ttQHttQHTUvH1H4"4Mj#$jjtj=.uE+uT.~..HD.A...-
ELutEQMtMzHEBEuMLtEHEtEy%tEUHBj<j"( $ek4Pdx-j-}E-EUDTju\ AtHHjEE hMtUEMEEUUE|ME}MMUUEBxtEEEUMUU (`jjT'jtj jttjQuB.Hu@.$LP@NPptv @a+@@$ j |\  j !
h0+j+!jjh t !jjh"<"(""j $vv$$$j$ $ #$ jjjjt  ##|#jj $# $##j  tj$$ ap.pmppdpdp.pmpp"pdp).fWeCedtT{cdZse;:e AA^`lyRJ2&kjhjhj9Eh..MU.hu-j-.
+.....-.jjj|U4MEj-PMEHBJtQQJtQ;UMHDsUQUU<_*gA%gy~yXeBHtc9s4rtTnjfi1de@[gilX
```

We can see that the shellcode is attached to winlogon.exe, upon start next time, this shellcode will run. END!