Can you hide [malware] forever?

@samaritan_o

http://bit.ly/2fL3nM5

alessandro.dicarlo@bit4law.it

Alessandro Di Carlo

27 Ottobre 2018

$WHOAMI

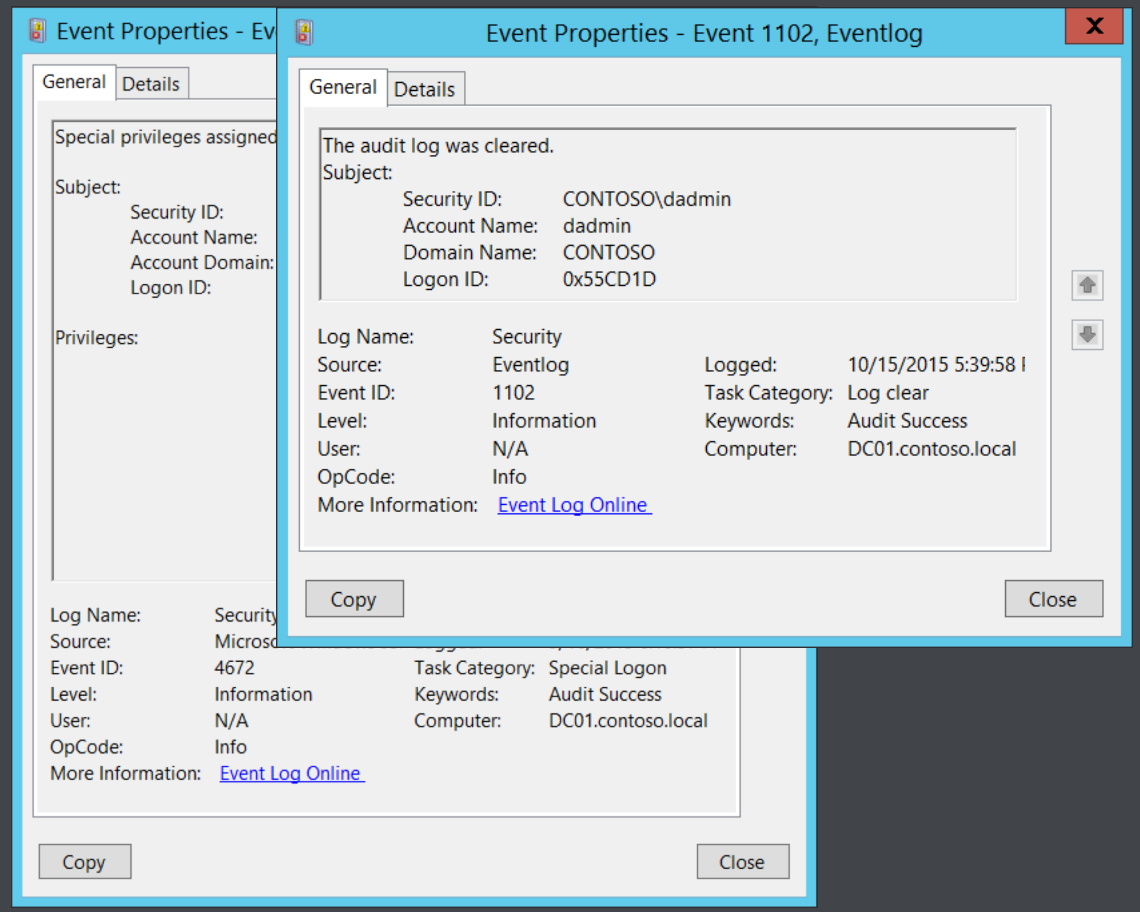
- **CTO** at BIT4LAW
- National and International speaker
- SANS Lethal Forensicator
- **GCFA** - GIAC Certified Forensic Analyst
- **eCPPT** – eLearnSecurity Certified Professional Penetration Tester
- **eWAPT** – eLearnSecurity Web Application Penetration Tester
- **ONIF** – (ISC)2 – IISFA Active Member

$Perché questo talk

- Molti anni come penetration tester
- Pwned, reverse shell – reverse shell, Pwned
- …Lateral Movement…
- …Data exfiltration
- Poi la fatidica domanda: **Ma quante evidenze dei miei PT mi porto dietro?!?**

CHMOD.EXE-2487E885.pf	12/17/2016 10:40 PM	PF File	3 KB
CHROME.EXE-5349D2D7.pf	12/28/2016 9:37 PM	PF File	7 KB
CHROME.EXE-5349D2D8.pf	12/28/2016 9:50 PM	PF File	10 KB
CHROME.EXE-5349D2D9.pf	12/16/2016 9:34 PM	PF File	20 KB
CHROME.EXE-5349D2DA.pf	12/28/2016 9:26 PM	PF File	15 KB
CHROME.EXE-5349D2DD.pf	12/28/2016 12:18 AM	PF File	7 KB
CHROME.EXE-5349D2DE.pf	12/28/2016 9:37 PM	PF File	7 KB
CHROME.EXE-5349D2DF.pf	12/28/2016 9:37 PM	PF File	9 KB
CITRIXONLINELAUNCHER.EXE-73AE6288.pf	12/14/2016 11:40 AM	PF File	14 KB
CLEAR.EXE-34BAE403.pf	12/25/2016 3:35 PM	PF File	3 KB
CLEAR.EXE-F98CBA81.pf	12/17/2016 10:40 PM	PF File	4 KB
CMD.EXE-0BD30981.pf	12/24/2016 6:16 PM	PF File	4 KB
CMD.EXE-6D6290C5.pf	12/28/2016 6:19 PM	PF File	5 KB
CMP.EXE-D222ADA0.pf	12/17/2016 11:23 AM	PF File	3 KB

```
Process: svchost.exe Pid: 856 Address: 0xb70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00b70000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00b70010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00b70020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00b70030  00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00   ................



Process: svchost.exe Pid: 856 Address: 0xcb0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00cb0000  b8 35 00 00 00 e9 cd d7 c5 7b 00 00 00 00 00 00   .5.......{......
0x00cb0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00cb0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00cb0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```



HackInBo® Winter 2018 Edition

$Alcune domande

lsass.exe

$Alcune domande

wininit.exe

lsass.exe

$Alcune domande

HackInBo® Winter 2018 Edition

wininit.exe

%SystemRoot%\System32\lsass.exe

lsass.exe

$Alcune domande

Isaiso.exe

HackInBo® Winter 2018 Edition

$Alcune domande

wininit.exe

lsaiso.exe

HACK IN BO®
Winter 2018 Edition

$Alcune domande

wininit.exe

%SystemRoot%\System32\lsaiso.exe

lsaiso.exe

$Alcune domande

HACK IN BO®
Winter 2018 Edition

svchost.exe

$Alcune domande

services.exe
(maggior parte)

svchost.exe

HACK IN BO®
Winter 2018 Edition

$Alcune domande

HACK IN BO®
Winter 2018 Edition

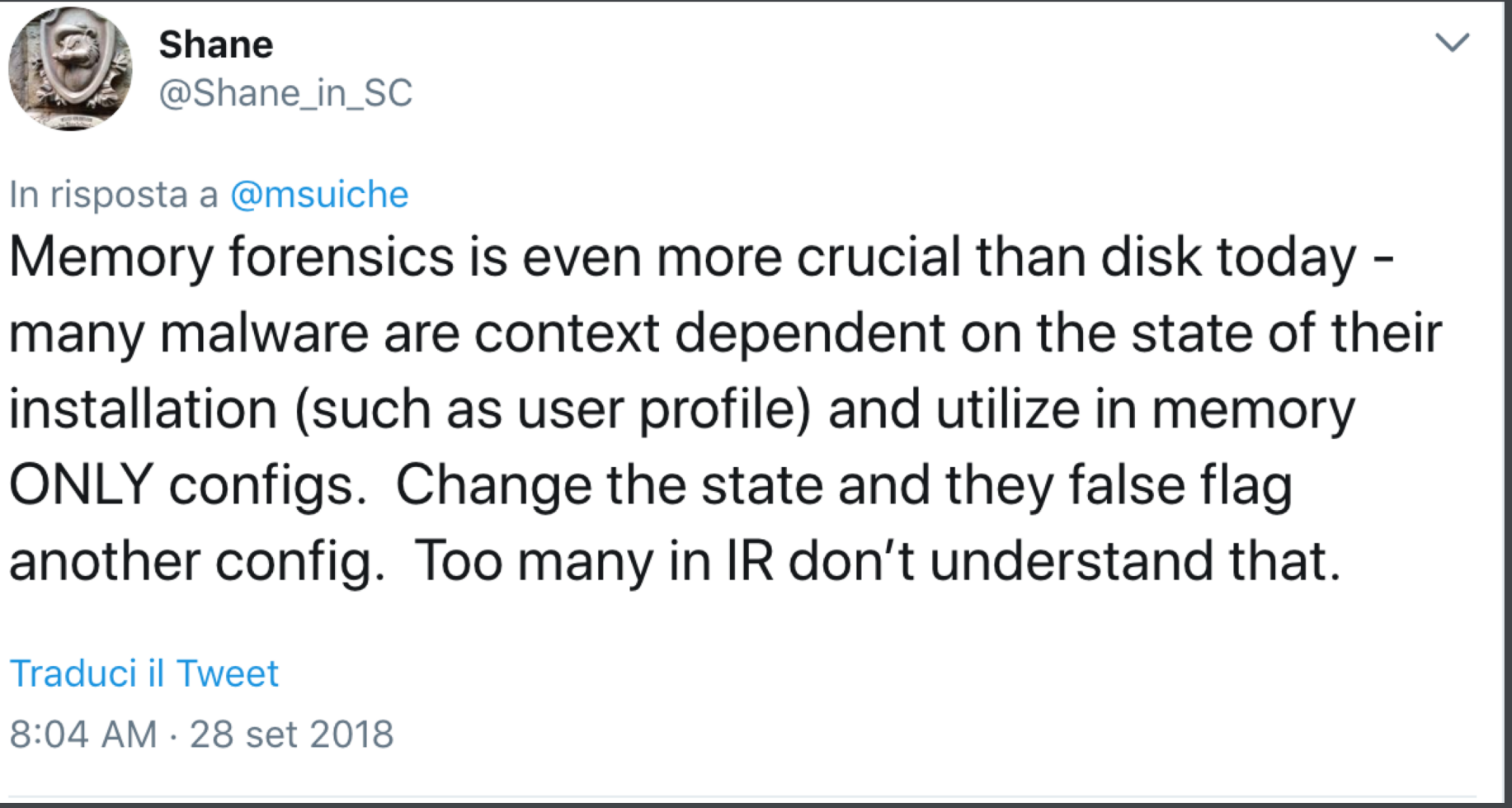
services.exe
(maggior parte)

%SystemRoot%\system32\svchost.exe

svchost.exe

$Memory forensics

HackInBo® Winter 2018 Edition



Shane
@Shane_in_SC

In risposta a @msuiche

Memory forensics is even more crucial than disk today - many malware are context dependent on the state of their installation (such as user profile) and utilize in memory ONLY configs. Change the state and they false flag another config. Too many in IR don't understand that.

Traduci il Tweet

8:04 AM · 28 set 2018

$Memory forensics

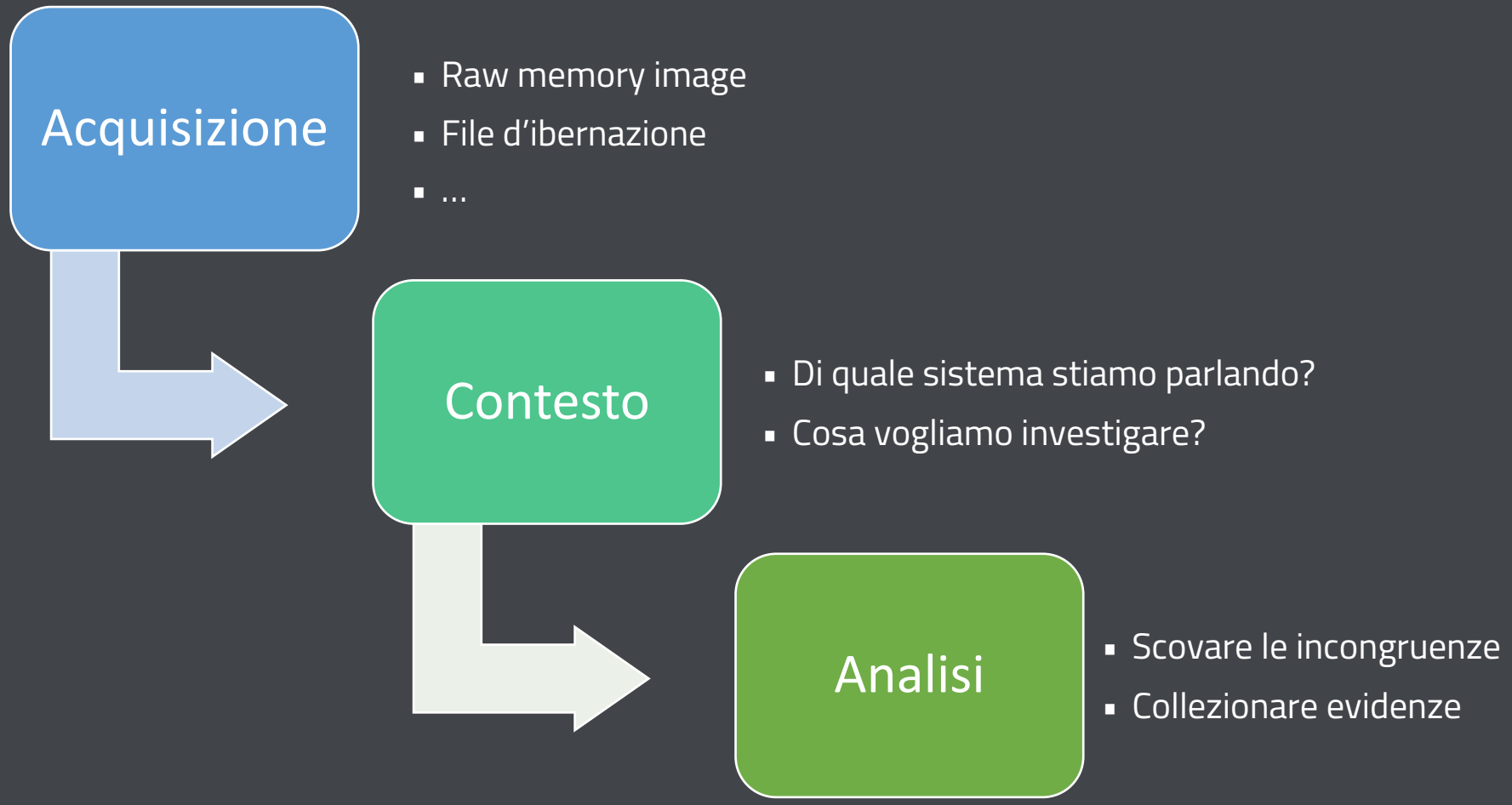
- Troviamo praticamente **tutto**
  - Processi
  - Sockets
  - Indirizzi IP
  - Encryption key
  - Passwords
  - Clipboards
  - Malware (**rootkit incluso**)

$Memory forensics

HackInBo® Winter 2018 Edition

- Quali sono i vantaggi?
  - È il miglior posto dove trovare ‘’incongruenze’’ (perché quel **PID** ha quel **PPID?**)
  - Collezionare evidenze che non possono essere trovate altrove
    - Attività del browser (modalità **incognito** ☺)
    - Chat history
    - …

$Memory forensics



$Memory forensics - acquisizione

- **Live system**
  - **DumpIT –** https://www.comae.io
  - **WinPMEM –** http://www.rekall-forensics.com/downloads.html
  - **Belkasoft Ram Capturer –** forensic.belkasoft.com/en/ram-capturer
  - **...**
- **Dead system**
  - **Hiberfil.sys**
  - Pagefile.sys
  - Swapfile.sys

$Memory forensics - contesto

- La memoria non è in un formato progettato per essere estratta e capita
- È progettata per essere **eseguita**
- Di conseguenza non è per nulla facile analizzarla
- Come facciamo a dargli un senso?
    - Kernel Debugger Data Block (**KDBG**)
    - Kernel Processor Control Region (**KPCR**)
    - Directory Table Base (**DTB**)

$Memory forensics - KDBG

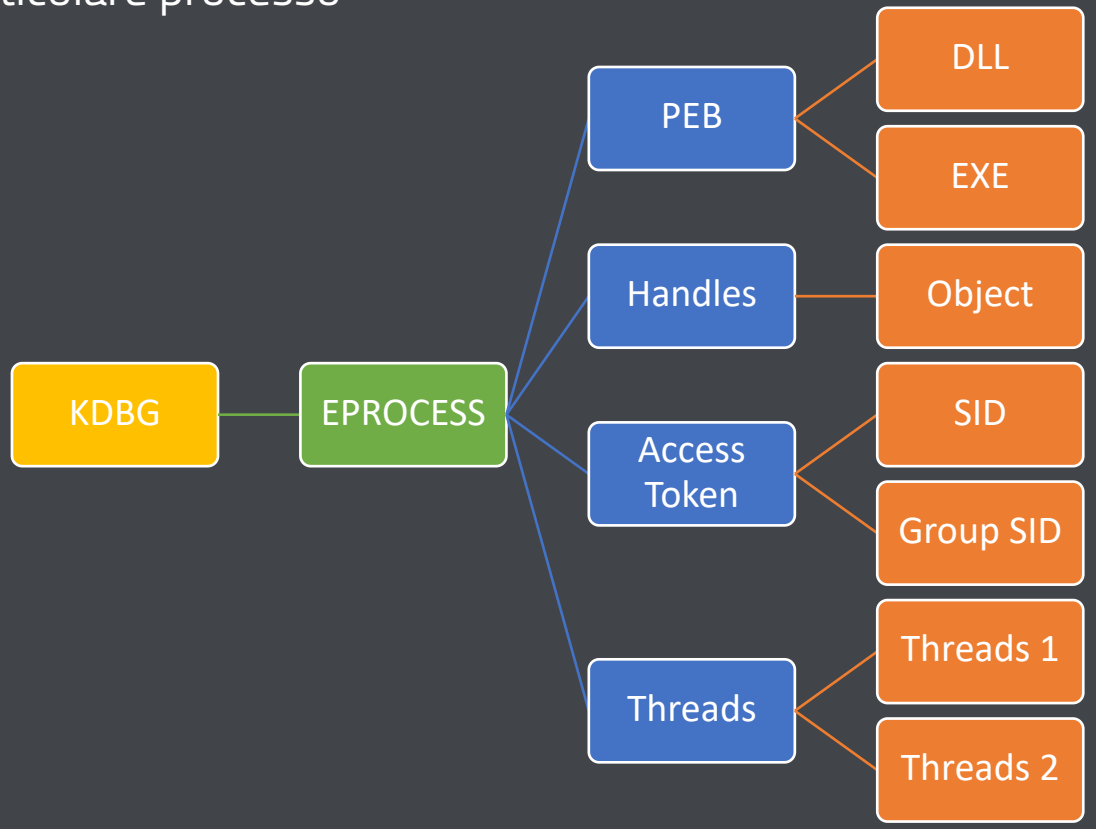
- Il KDBG è la chiave per comprendere l'immagine di una memoria
- È una struttura dati i cui puntatori possono essere usati per trovare la lista dei processi del sistema
- Come possiamo trovare il KDBG? In due modi:
  - Tramite signature
  - Trovando il KPCR (Kernel Process Control Region)
- Per velocizzare il processo, tool di analisi come Rekall e Volatility utilizzano dei profili ben definiti per trovare **PsActiveProcessHead**, **Directory Table Base (DTB)** , etc.

$Memory forensics

- Trovato il KDBG, si aprono le porte dell'**EPROCESS**
- L'EPROCESS ci aiuta a parsare tutta la struttura della memoria
  - Contiene tutta la lista dei processi
  - Ogni processo avrà il suo specifico **PEB** (Process Environment Block) nel quale troveremo il percorso esatto del processo, le relative DLLs, etc.

$Memory forensics

- Fondamentale risulta essere il **VAD** (Virtual Address Descriptor)
- Il VAD è il componente che tiene traccia di ogni singola sezione di memoria assegnata ad un particolare processo



$Memory forensics - analisi

./vol.py –f <immagine> *imageinfo*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img 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 (/Users/Samaritan/volatility/DemoHiB.img)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545b60L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
```

$Memory forensics - analisi

./vol.py –f <immagine> *imageinfo*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img 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 (/Users/Samaritan/volatility/DemoHiB.img)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545b60L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
```

$Memory forensics - analisi

./vol.py –f <immagine> *pslist*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64
---------- -------------------- ------ ------ ------ -------- ------ ------
0x823c8830 System                    4      0     55      254 ------      0
0x8230aad8 smss.exe                564      4      3       19 ------      0
0x822ca2c0 csrss.exe               636    564     10      356      0      0
0x81f63020 winlogon.exe            660    564     16      502      0      0
0x81f22020 services.exe            704    660     15      254      0      0
0x82164da0 lsass.exe               716    660     21      342      0      0
0x822cb458 vmacthlp.exe            872    704      1       25      0      0
0x81e54da0 svchost.exe             884    704     17      208      0      0
0x81da4590 svchost.exe             968    704     10      241      0      0
0x81f739b0 svchost.exe            1088    704     70     1445      0      0
0x8232c020 svchost.exe            1140    704      5       60      0      0
0x81e91da0 svchost.exe            1212    704     14      208      0      0
0x8219b630 spoolsv.exe            1512    704     10      129      0      0
0x81da71a8 explorer.exe           1672   1624     15      586      0      0
0x81f1c7e8 VMwareTray.exe         1984   1672      1       37      0      0
0x81dc1a78 VMwareUser.exe         2004   1672      8      228      0      0
0x81f1a650 ctfmon.exe             2020   1672      1       71      0      0
0x81dc2570 VMwareService.e        1032    704      3      175      0      0
0x81d33628 alg.exe                 464    704      6      105      0      0
0x81f96220 wscntfy.exe            1260   1088      1       39      0      0
0x8231eda0 msiexec.exe            1464    704      6      294      0      0
0x81e4d648 cmd.exe                 840   1672      1       33      0      0
0x81dbdda0 iexplore.exe            796    884      8      152      0      0
0x82161558 MIRAgent.exe            456    840      1       77      0      0
```

Hack In Bo® Winter 2018 Edition

$Memory forensics - analisi

./vol.py –f <immagine> *pslist*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64
---------- -------------------- ------ ------ ------ -------- ------ ------
0x823c8830 System                    4      0     55      254 ------      0
0x8230aad8 smss.exe                564      4      3       19 ------      0
0x822ca2c0 csrss.exe               636    564     10      356      0      0
0x81f63020 winlogon.exe            660    564     16      502      0      0
0x81f22020 services.exe            704    660     15      254      0      0
0x82164da0 lsass.exe               716    660     21      342      0      0
0x822cb458 vmacthlp.exe            872    704      1       25      0      0
0x81e54da0 svchost.exe             884    704     17      208      0      0
0x81da4590 svchost.exe             968    704     10      241      0      0
0x81f739b0 svchost.exe            1088    704     70     1445      0      0
0x8232c020 svchost.exe            1140    704      5       60      0      0
0x81e91da0 svchost.exe            1212    704     14      208      0      0
0x8219b630 spoolsv.exe            1512    704     10      129      0      0
0x81da71a8 explorer.exe           1672   1624     15      586      0      0
0x81f1c7e8 VMwareTray.exe         1984   1672      1       37      0      0
0x81dc1a78 VMwareUser.exe         2004   1672      8      228      0      0
0x81f1a650 ctfmon.exe             2020   1672      1       71      0      0
0x81dc2570 VMwareService.e        1032    704      3      175      0      0
0x81d33628 alg.exe                 464    704      6      105      0      0
0x81f96220 wscntfy.exe            1260   1088      1       39      0      0
0x8231eda0 msiexec.exe            1464    704      6      294      0      0
0x81e4d648 cmd.exe                 840   1672      1       33      0      0
0x81dbdda0 iexplore.exe            796    884      8      152      0      0
0x82161558 MIRAgent.exe            456    840      1       77      0      0
```

$Memory forensics - analisi

./vol.py –f <immagine> *pslist*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64
---------- -------------------- ------ ------ ------ -------- ------ ------
0x823c8830 System                    4      0     55      254 ------      0
0x8230aad8 smss.exe                564      4      3       19 ------      0
0x822ca2c0 csrss.exe               636    564     10      356      0      0
0x81f63020 winlogon.exe            660    564     16      502      0      0
0x81f22020 services.exe            704    660     15      254      0      0
0x82164da0 lsass.exe               716    660     21      342      0      0
0x822cb458 vmacthlp.exe            872    704      1       25      0      0
0x81e54da0 svchost.exe             884    704     17      208      0      0
0x81da4590 svchost.exe             968    704     10      241      0      0
0x81f739b0 svchost.exe            1088    704     70     1445      0      0
0x8232c020 svchost.exe            1140    704      5       60      0      0
0x81e91da0 svchost.exe            1212    704     14      208      0      0
0x8219b630 spoolsv.exe            1512    704     10      129      0      0
0x81da71a8 explorer.exe           1672   1624     15      586      0      0
0x81f1c7e8 VMwareTray.exe         1984   1672      1       37      0      0
0x81dc1a78 VMwareUser.exe         2004   1672      8      228      0      0
0x81f1a650 ctfmon.exe             2020   1672      1       71      0      0
0x81dc2570 VMwareService.e        1032    704      3      175      0      0
0x81d33628 alg.exe                 464    704      6      105      0      0
0x81f96220 wscntfy.exe            1260   1088      1       39      0      0
0x8231eda0 msiexec.exe            1464    704      6      294      0      0
0x81e4d648 cmd.exe                 840   1672      1       33      0      0
0x81dbdda0 iexplore.exe            796    884      8      152      0      0
0x82161558 MIRAgent.exe            456    840      1       77      0      0
```

$Memory forensics - analisi

./vol.py –f <immagine> *pstree*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     55    254 1970-01-01 00:00:00 UTC+0000
. 0x8230aad8:smss.exe                                 564      4      3     19 2009-04-16 16:10:01 UTC+0000
.. 0x81f63020:winlogon.exe                            660    564     16    502 2009-04-16 16:10:06 UTC+0000
... 0x81f22020:services.exe                           704    660     15    254 2009-04-16 16:10:06 UTC+0000
.... 0x81f739b0:svchost.exe                          1088    704     70   1445 2009-04-16 16:10:07 UTC+0000
..... 0x81f96220:wscntfy.exe                         1260   1088      1     39 2009-04-16 16:10:22 UTC+0000
.... 0x81da4590:svchost.exe                           968    704     10    241 2009-04-16 16:10:07 UTC+0000
.... 0x81dc2570:VMwareService.e                      1032    704      3    175 2009-04-16 16:10:16 UTC+0000
.... 0x8231eda0:msiexec.exe                          1464    704      6    294 2009-04-16 16:11:02 UTC+0000
.... 0x81e54da0:svchost.exe                           884    704     17    208 2009-04-16 16:10:07 UTC+0000
..... 0x81dbdda0:iexplore.exe                         796    884      8    152 2009-05-05 19:28:28 UTC+0000
.... 0x81e91da0:svchost.exe                          1212    704     14    208 2009-04-16 16:10:09 UTC+0000
.... 0x81d33628:alg.exe                               464    704      6    105 2009-04-16 16:10:21 UTC+0000
.... 0x8219b630:spoolsv.exe                          1512    704     10    129 2009-04-16 16:10:10 UTC+0000
.... 0x822cb458:vmacthlp.exe                          872    704      1     25 2009-04-16 16:10:07 UTC+0000
.... 0x8232c020:svchost.exe                          1140    704      5     60 2009-04-16 16:10:08 UTC+0000
... 0x82164da0:lsass.exe                              716    660     21    342 2009-04-16 16:10:06 UTC+0000
.. 0x822ca2c0:csrss.exe                               636    564     10    356 2009-04-16 16:10:06 UTC+0000
 0x81da71a8:explorer.exe                             1672   1624     15    586 2009-04-16 16:10:10 UTC+0000
. 0x81f1c7e8:VMwareTray.exe                          1984   1672      1     37 2009-04-16 16:10:11 UTC+0000
. 0x81e4d648:cmd.exe                                  840   1672      1     33 2009-05-05 15:56:24 UTC+0000
.. 0x82161558:MIRAgent.exe                            456    840      1     77 2009-05-05 19:28:40 UTC+0000
. 0x81dc1a78:VMwareUser.exe                          2004   1672      8    228 2009-04-16 16:10:11 UTC+0000
. 0x81f1a650:ctfmon.exe                              2020   1672      1     71 2009-04-16 16:10:11 UTC+0000
```

$Memory forensics - analisi

HACK IN BO® Winter 2018 Edition

./vol.py –f <immagine> *getsids*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img --profile=WinXPSP3x86 getsids -p 796
Volatility Foundation Volatility Framework 2.6
iexplore.exe (796): S-1-5-18 (Local System)
iexplore.exe (796): S-1-5-32-544 (Administrators)
iexplore.exe (796): S-1-1-0 (Everyone)
iexplore.exe (796): S-1-5-11 (Authenticated Users)
```

$Memory forensics - analisi

./vol.py –f <immagine> *connscan*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img --profile=WinXPSP3x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x0205ece0 192.168.157.10:1050      222.128.1.2:443           1672
0x020611f8 192.168.157.10:1053      218.85.133.23:89          796
0x032c01f8 192.168.157.10:1053      218.85.133.23:89          796
0x0337dce0 192.168.157.10:1050      222.128.1.2:443           1672
0x08a4ace0 192.168.157.10:1050      222.128.1.2:443           1672
0x18200ce0 192.168.157.10:1050      222.128.1.2:443           1672
```

$Memory forensics - analisi

./vol.py –f <immagine> *dlllist* –p <*pid*>

```
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll
0x10000000     0x9000        0x1 C:\WINDOWS\system32\irykmmww.dll
0x78050000    0xd0000        0x2 C:\WINDOWS\system32\WININET.dll
0x00710000     0x9000        0x2 C:\WINDOWS\system32\Normaliz.dll
0x71ab0000    0x17000        0xd C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000       0x10 C:\WINDOWS\system32\WS2HELP.dll
0x00150000     0xc000        0x1 C:\WINDOWS\system32\irykmmww.dll
0x5ad70000    0x38000        0x2 C:\WINDOWS\system32\uxtheme.dll
0x76fd0000    0x7f000        0x2 C:\WINDOWS\system32\CLBCATQ.DLL
0x77050000    0xc5000        0x2 C:\WINDOWS\system32\COMRes.dll
0x00e80000   0x2c5000        0x1 C:\WINDOWS\system32\xpsp2res.dll
0x76ee0000    0x3c000        0x2 C:\WINDOWS\system32\RASAPI32.dll
0x76e90000    0x12000        0x3 C:\WINDOWS\system32\rasman.dll
0x5b860000    0x55000        0x4 C:\WINDOWS\system32\NETAPI32.dll
0x76eb0000    0x2f000        0x2 C:\WINDOWS\system32\TAPI32.dll
0x76e80000     0xe000        0x3 C:\WINDOWS\system32\rtutils.dll
0x76b40000    0x2d000        0x2 C:\WINDOWS\system32\WINMM.dll
0x769c0000    0xb4000        0x1 C:\WINDOWS\system32\USERENV.dll
0x722b0000     0x5000        0x1 C:\WINDOWS\system32\sensapi.dll
0x71a50000    0x3f000        0x4 C:\WINDOWS\System32\mswsock.dll
0x76fc0000     0x6000        0x1 C:\WINDOWS\system32\rasadhlp.dll
0x662b0000    0x58000        0x1 C:\WINDOWS\system32\hnetcfg.dll
0x71a90000     0x8000        0x1 C:\WINDOWS\System32\wshtcpip.dll
0x77c70000    0x24000        0x1 C:\WINDOWS\system32\msv1_0.dll
0x76d60000    0x19000        0x1 C:\WINDOWS\system32\iphlpapi.dll
************************************************************************
```

$Memory forensics - analisi

./vol.py –f <immagine> *dlllist* –p <*pid*>

```
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll
0x10000000     0x9000        0x1 C:\WINDOWS\system32\irykmmww.dll
0x78050000    0xd0000        0x2 C:\WINDOWS\system32\WININET.dll
0x00710000     0x9000        0x2 C:\WINDOWS\system32\Normaliz.dll
0x71ab0000    0x17000        0xd C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000       0x10 C:\WINDOWS\system32\WS2HELP.dll
0x00150000     0xc000        0x1 C:\WINDOWS\system32\irykmmww.dll
0x5ad70000    0x38000        0x2 C:\WINDOWS\system32\uxtheme.dll
0x76fd0000    0x7f000        0x2 C:\WINDOWS\system32\CLBCATQ.DLL
0x77050000    0xc5000        0x2 C:\WINDOWS\system32\COMRes.dll
0x00e80000   0x2c5000        0x1 C:\WINDOWS\system32\xpsp2res.dll
0x76ee0000    0x3c000        0x2 C:\WINDOWS\system32\RASAPI32.dll
0x76e90000    0x12000        0x3 C:\WINDOWS\system32\rasman.dll
0x5b860000    0x55000        0x4 C:\WINDOWS\system32\NETAPI32.dll
0x76eb0000    0x2f000        0x2 C:\WINDOWS\system32\TAPI32.dll
0x76e80000     0xe000        0x3 C:\WINDOWS\system32\rtutils.dll
0x76b40000    0x2d000        0x2 C:\WINDOWS\system32\WINMM.dll
0x769c0000    0xb4000        0x1 C:\WINDOWS\system32\USERENV.dll
0x722b0000     0x5000        0x1 C:\WINDOWS\system32\sensapi.dll
0x71a50000    0x3f000        0x4 C:\WINDOWS\System32\mswsock.dll
0x76fc0000     0x6000        0x1 C:\WINDOWS\system32\rasadhlp.dll
0x662b0000    0x58000        0x1 C:\WINDOWS\system32\hnetcfg.dll
0x71a90000     0x8000        0x1 C:\WINDOWS\System32\wshtcpip.dll
0x77c70000    0x24000        0x1 C:\WINDOWS\system32\msv1_0.dll
0x76d60000    0x19000        0x1 C:\WINDOWS\system32\iphlpapi.dll
************************************************************************
```

$Memory forensics - analisi

./vol.py –f <immagine> *dlllist* –p <*pid*>

```
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll
0x10000000     0x9000        0x1 C:\WINDOWS\system32\irykmmww.dll
0x78050000    0xd0000        0x2 C:\WINDOWS\system32\WININET.dll
0x00710000     0x9000        0x2 C:\WINDOWS\system32\Normaliz.dll
0x71ab0000    0x17000        0xd C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000       0x10 C:\WINDOWS\system32\WS2HELP.dll
0x00150000     0xc000        0x1 C:\WINDOWS\system32\irykmmww.dll
0x5ad70000    0x38000        0x2 C:\WINDOWS\system32\uxtheme.dll
0x76fd0000    0x7f000        0x2 C:\WINDOWS\system32\CLBCATQ.DLL
0x77050000    0xc5000        0x2 C:\WINDOWS\system32\COMRes.dll
0x00e80000   0x2c5000        0x1 C:\WINDOWS\system32\xpsp2res.dll
0x76ee0000    0x3c000        0x2 C:\WINDOWS\system32\RASAPI32.dll
0x76e90000    0x12000        0x3 C:\WINDOWS\system32\rasman.dll
0x5b860000    0x55000        0x4 C:\WINDOWS\system32\NETAPI32.dll
0x76eb0000    0x2f000        0x2 C:\WINDOWS\system32\TAPI32.dll
0x76e80000     0xe000        0x3 C:\WINDOWS\system32\rtutils.dll
0x76b40000    0x2d000        0x2 C:\WINDOWS\system32\WINMM.dll
0x769c0000    0xb4000        0x1 C:\WINDOWS\system32\USERENV.dll
0x722b0000     0x5000        0x1 C:\WINDOWS\system32\sensapi.dll
0x71a50000    0x3f000        0x4 C:\WINDOWS\System32\mswsock.dll
0x76fc0000     0x6000        0x1 C:\WINDOWS\system32\rasadhlp.dll
0x662b0000    0x58000        0x1 C:\WINDOWS\system32\hnetcfg.dll
0x71a90000     0x8000        0x1 C:\WINDOWS\System32\wshtcpip.dll
0x77c70000    0x24000        0x1 C:\WINDOWS\system32\msv1_0.dll
0x76d60000    0x19000        0x1 C:\WINDOWS\system32\iphlpapi.dll
**************************************************************************
```

irykmmww.d1l

$Memory forensics - analisi

./vol.py –f <immagine> *svcscan*

```
Offset: 0x38ab98
Order: 252
Start: SERVICE_DEMAND_START
Process ID: -
Service Name: irykmmww
Display Name: irykmmww
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\irykmmww
```

$Memory forensics - analisi

./vol.py –f <immagine> *svcscan ssdt | grep -v ntoskrnl | grep -v win32k*

```
┌─Samaritan at Samaritan_o in ~/volatility using
└─○ ./vol -f DemoHiB.img --profile=WinXPSP3x86 ssdt | grep -v ntoskrnl | grep -v win32k
Volatility Foundation Volatility Framework 2.6
[x86] Gathering all referenced SSDTs from KTHREADs...
Finding appropriate address space for tables...
SSDT[0] at 80501b9c with 284 entries
  Entry 0x0042: 0xf836fe9c (NtDeviceIoControlFile) owned by irykmmww.sys
  Entry 0x0047: 0xf83706dc (NtEnumerateKey) owned by irykmmww.sys
  Entry 0x0049: 0xf837075e (NtEnumerateValueKey) owned by irykmmww.sys
  Entry 0x0077: 0xf837028f (NtOpenKey) owned by irykmmww.sys
  Entry 0x0091: 0xf8370a8c (NtQueryDirectoryFile) owned by irykmmww.sys
  Entry 0x00ad: 0xf836fe3e (NtQuerySystemInformation) owned by irykmmww.sys
  Entry 0x00b1: 0xf837091a (NtQueryValueKey) owned by irykmmww.sys
```

$Memory forensics - analisi

HACK IN BO® Winter 2018 Edition

./vol.py –f <immagine> *svcscan ssdt | grep -v ntoskrnl | grep -v win32k*

```
Samaritan at Samaritan_o in ~/volatility using
 ./vol -f DemoHiB.img --profile=WinXPSP3x86 ssdt | grep -v ntoskrnl | grep -v win32k
Volatility Foundation Volatility Framework 2.6
[x86] Gathering all referenced SSDTs from KTHREAD...
Finding appropriate address space for tables...
SSDT[0] at 80501b9c with 284 entries
  Entry 0x0042: 0xf836fe9c (NtDeviceIoControlFile) owned by irykmmww.sys
  Entry 0x0047: 0xf83706dc (NtEnumerateKey) owned by irykmmww.sys
  Entry 0x0049: 0xf837075e (NtEnumerateValueKey) owned by irykmmww.sys
  Entry 0x0077: 0xf837028f (NtOpenKey) owned by irykmmww.sys
  Entry 0x0091: 0xf8370a8c (NtQueryDirectoryFile) owned by irykmmww.sys
  Entry 0x00ad: 0xf836fe3e (NtQuerySystemInformation) owned by irykmmww.sys
  Entry 0x00b1: 0xf837091a (NtQueryValueKey) owned by irykmmww.sys
```

ROOTKIT

$Intrusion Forensics

- **Prefetch Analysis**

```
D:\Temp
λ PECmd.exe -f d:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf -k "lpk, global"
PECmd version 0.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Keywords: temp, tmp, lpk, global

Processing 'd:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf'

Executable name: CMD.EXE
Hash: 4A81B364
Version: Windows Vista or Windows 7

Run count: 2
Last run: 1/16/2016 1:26:42 PM -07:00

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME2 Serial: 88008C2F Created: 1/16/2016 2:15:18 PM -07:00 Directories: 6 File references: 22

Directories referenced: 6

0: \DEVICE\HARDDISKVOLUME2\WINDOWS
1: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING
2: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD
3: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION
4: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING
5: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32

Files referenced: 16

00: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
01: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
03: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LOCALE.NLS
05: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CMD.EXE
06: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSVCRT.DLL
07: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\WINBRAND.DLL
08: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USER32.DLL
09: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\GDI32.DLL
10: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LPK.DLL
11: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USP10.DLL
12: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\IMM32.DLL
13: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSCTF.DLL
14: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD\BASEBRD.DLL
15: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
-------------------------------------------------------------
```

$Intrusion Forensics

- **Prefetch Analysis**

```
D:\Temp
λ PECmd.exe -f d:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf -k "lpk, global"
PECmd version 0.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Keywords: temp, tmp, lpk, global

Processing 'd:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf'

Executable name: CMD.EXE
Hash: 4A81B364
Version: Windows Vista or Windows 7

Run count: 2
Last run: 1/16/2016 1:26:42 PM -07:00

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME2 Serial: 88008C2F Created: 1/16/2016 2:15:18 PM -07:00 Directories: 6 File references: 22

Directories referenced: 6

0: \DEVICE\HARDDISKVOLUME2\WINDOWS
1: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING
2: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD
3: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION
4: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING
5: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32

Files referenced: 16

00: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
01: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
03: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LOCALE.NLS
05: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CMD.EXE
06: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSVCRT.DLL
07: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\WINBRAND.DLL
08: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USER32.DLL
09: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\GDI32.DLL
10: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LPK.DLL
11: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USP10.DLL
12: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\IMM32.DLL
13: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSCTF.DLL
14: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD\BASEBRD.DLL
15: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
----------------------------------------------------------
```

$Intrusion Forensics

- **Prefetch Analysis**

```
D:\Temp
λ PECmd.exe -f d:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf -k "lpk, global"
PECmd version 0.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Keywords: temp, tmp, lpk, global

Processing 'd:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf'

Executable name: CMD.EXE
Hash: 4A81B364
Version: Windows Vista or Windows 7

Run count: 2
Last run: 1/16/2016 1:26:42 PM -07:00

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME2 Serial: 88008C2F Created: 1/16/2016 2:15:18 PM -07:00 Directories: 6 File references: 22

Directories referenced: 6

0: \DEVICE\HARDDISKVOLUME2\WINDOWS
1: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING
2: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD
3: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION
4: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING
5: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32

Files referenced: 16

00: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
01: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
03: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LOCALE.NLS
05: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CMD.EXE
06: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSVCRT.DLL
07: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\WINBRAND.DLL
08: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USER32.DLL
09: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\GDI32.DLL
10: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LPK.DLL
11: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USP10.DLL
12: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\IMM32.DLL
13: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSCTF.DLL
14: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD\BASEBRD.DLL
15: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
-------------------------------------------------------------
```

$Intrusion Forensics

- **Prefetch Analysis**

```
D:\Temp
λ PECmd.exe -f d:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf -k "lpk, global"
PECmd version 0.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Keywords: temp, tmp, lpk, global

Processing 'd:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf'

Executable name: CMD.EXE
Hash: 4A81B364
Version: Windows Vista or Windows 7

Run count: 2
Last run: 1/16/2016 1:26:42 PM -07:00

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME2 Serial: 88008C2F Created: 1/16/2016 2:15:18 PM -07:00 Directories: 6 File references: 22

Directories referenced: 6

0: \DEVICE\HARDDISKVOLUME2\WINDOWS
1: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING
2: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD
3: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION
4: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING
5: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32

Files referenced: 16

00: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
01: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
03: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LOCALE.NLS
05: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CMD.EXE
06: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSVCRT.DLL
07: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\WINBRAND.DLL
08: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USER32.DLL
09: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\GDI32.DLL
10: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LPK.DLL
11: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USP10.DLL
12: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\IMM32.DLL
13: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSCTF.DLL
14: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD\BASEBRD.DLL
15: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
------------------------------------------------------------
```

$Intrusion Forensics

- **Prefetch Analysis**

```
D:\Temp
λ PECmd.exe -f d:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf -k "lpk, global"
PECmd version 0.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Keywords: temp, tmp, lpk, global

Processing 'd:\Code\Prefetch\Prefetch.Test\TestFiles\Win7\CMD.EXE-4A81B364.pf'

Executable name: CMD.EXE
Hash: 4A81B364
Version: Windows Vista or Windows 7

Run count: 2
Last run: 1/16/2016 1:26:42 PM -07:00

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME2 Serial: 88008C2F Created: 1/16/2016 2:15:18 PM -07:00 Directories: 6 File references: 22

Directories referenced: 6

0: \DEVICE\HARDDISKVOLUME2\WINDOWS
1: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING
2: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD
3: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION
4: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING
5: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32

Files referenced: 16

00: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
01: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
03: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LOCALE.NLS
05: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CMD.EXE
06: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSVCRT.DLL
07: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\WINBRAND.DLL
08: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USER32.DLL
09: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\GDI32.DLL
10: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\LPK.DLL
11: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\USP10.DLL
12: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\IMM32.DLL
13: \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSCTF.DLL
14: \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD\BASEBRD.DLL
15: \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
---------------------------------------------------------
```

$Intrusion Forensics

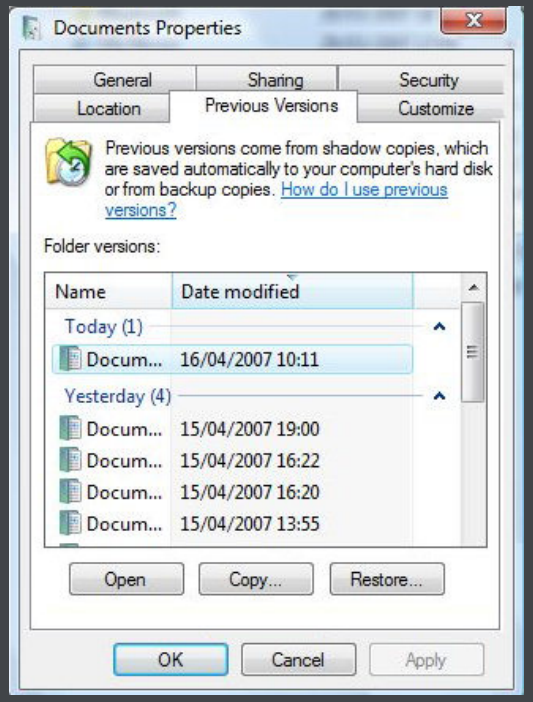
- **Application Compatibility - ShimCache**

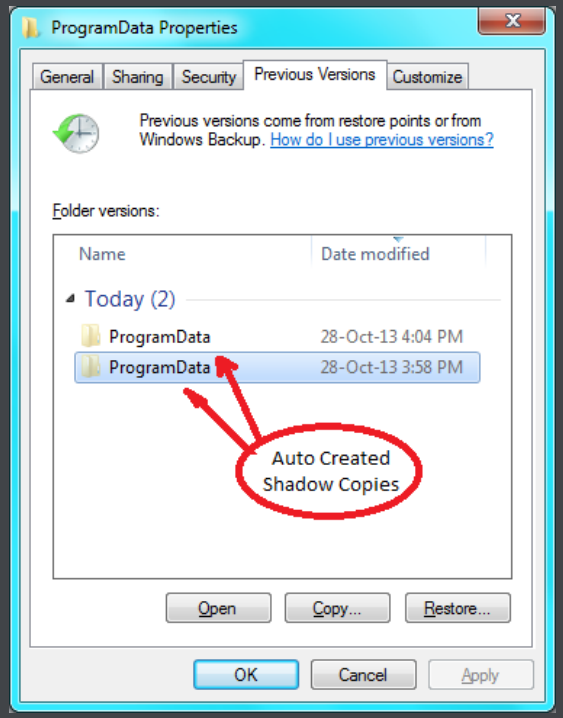
```
d:\Code\AppCompatCacheParser\AppCompatCacheParser\bin\Release (master)
λ AppCompatCacheParser.exe -h c:\Temp\SYSTEM2SETS -s c:\Temp
AppCompatCache Parser version 0.9.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser

Processing hive 'c:\Temp\SYSTEM2SETS'

***The following ControlSet00x keys will be exported: 1,2. Use -c to process keys individually

Results will be saved to 'c:\Temp\Windows7x64_Windows2008R2_SYSTEM2SETS_AppCompatCache.tsv'

Found 82 cache entries for Windows7x64_Windows2008R2 in ControlSet001
Found 12 cache entries for Windows7x64_Windows2008R2 in ControlSet002
```

- https://binaryforay.blogspot.it/2015/05/introducing-appcompatcacheparser.html
- https://github.com/mandiant/ShimCacheParser

$Intrusion Forensics

- **Shadow Copy Volumes**





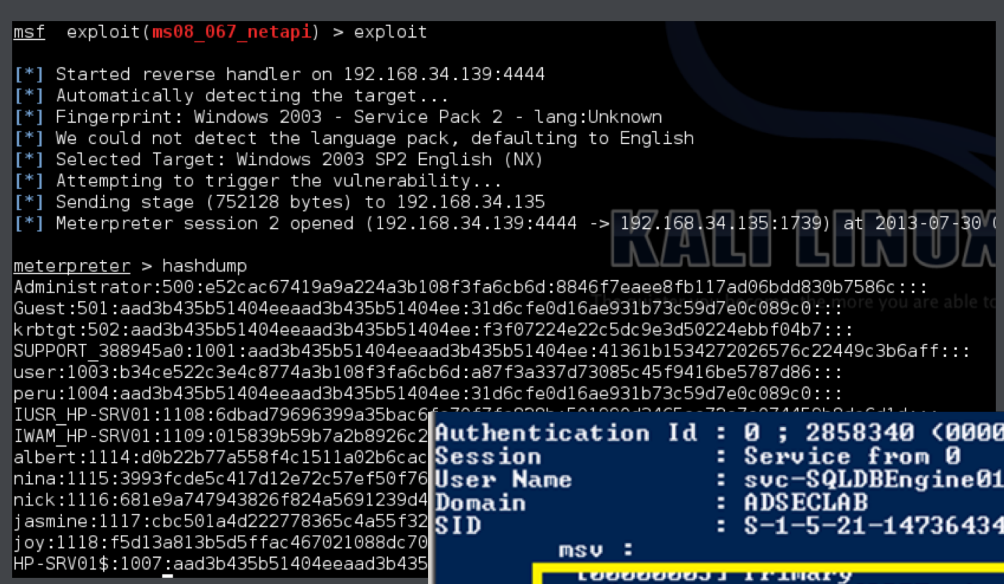
- Paragonabili ad uno snapshots di una macchina virtuale
- Permettono di recuperare file critici (events logs, file cancellati, chiavi di registro, etc.)

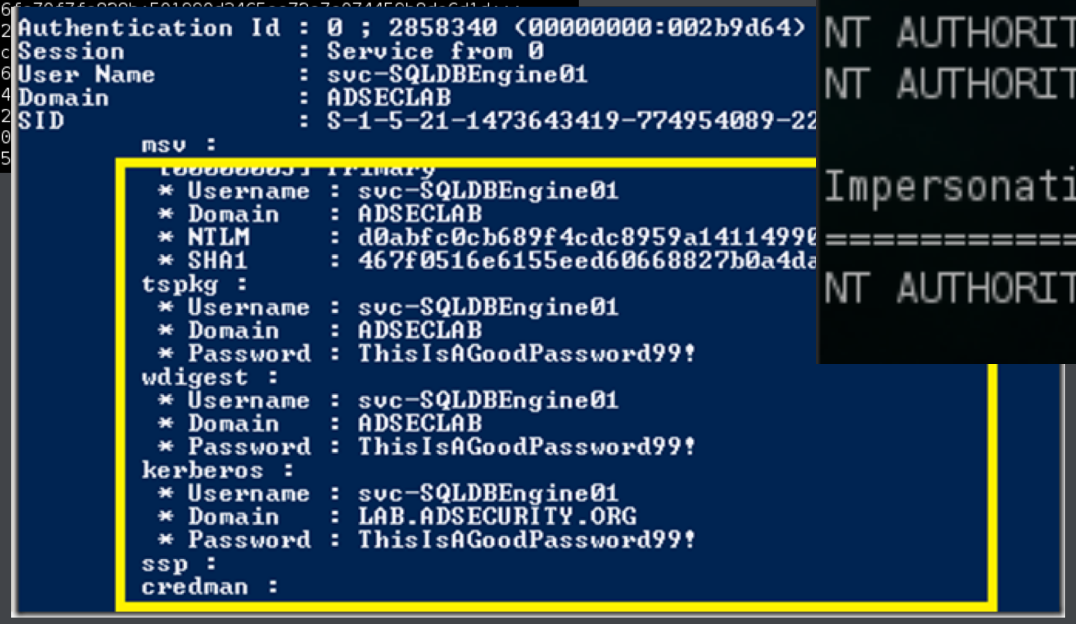
$Intrusion Forensics

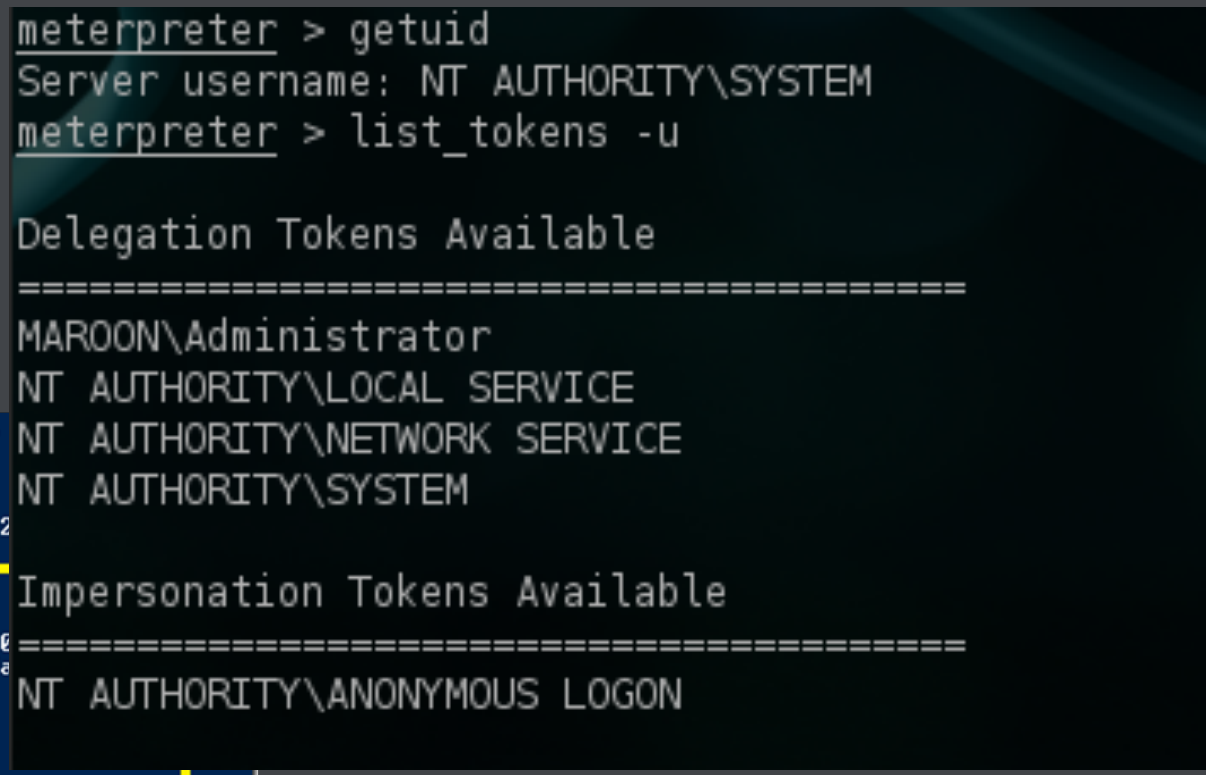
- Uso di credenziali legittime e creazione di un account
- Servizi di Remote Desktop
- Windows Admin Shares
- PsExec
- Windows Remote Management Tools
- Powershell/WMIC
- Exploitation di vulnerabilità ed applicazioni

$Intrusion Forensics

- **Uso di credenziali legittime**







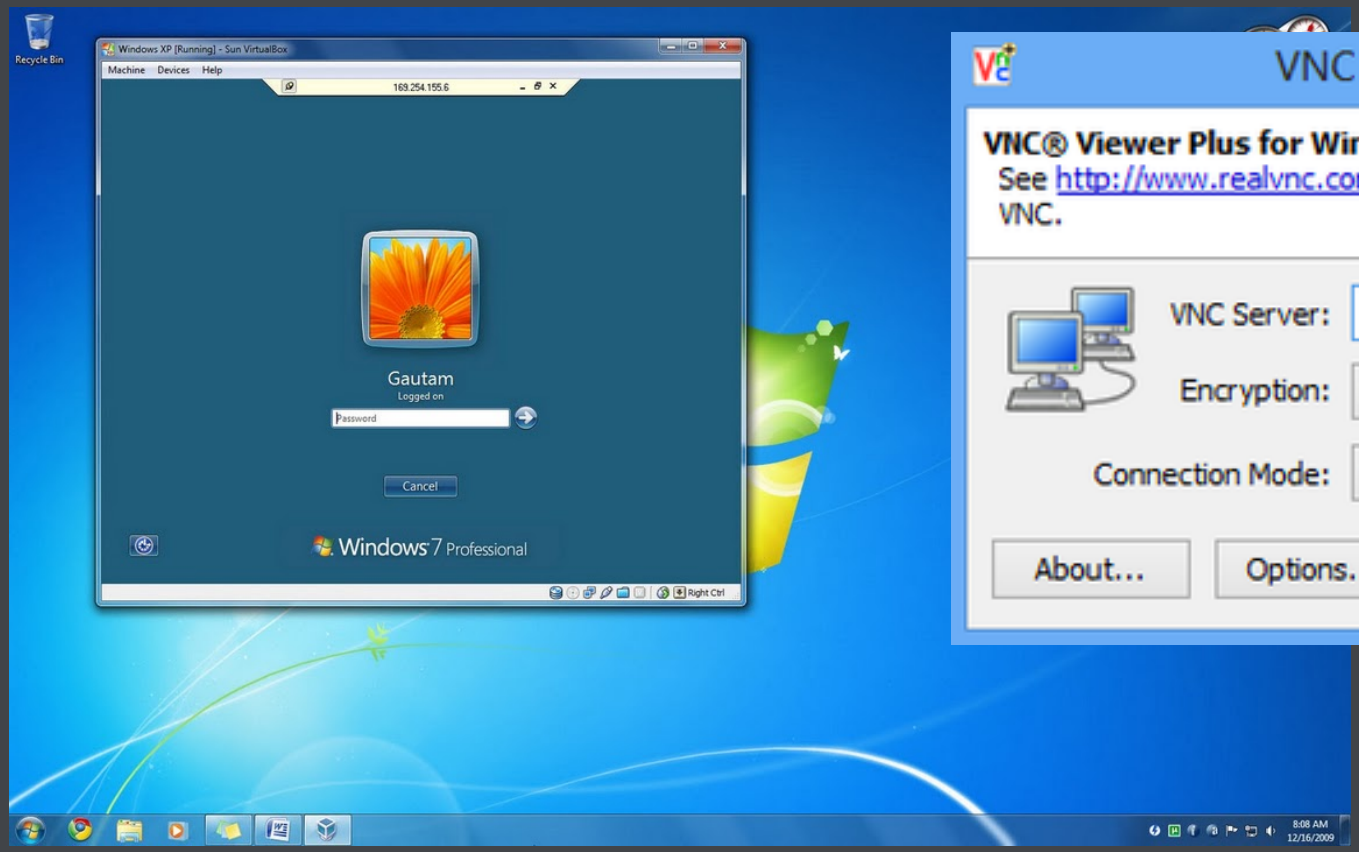
$Intrusion Forensics

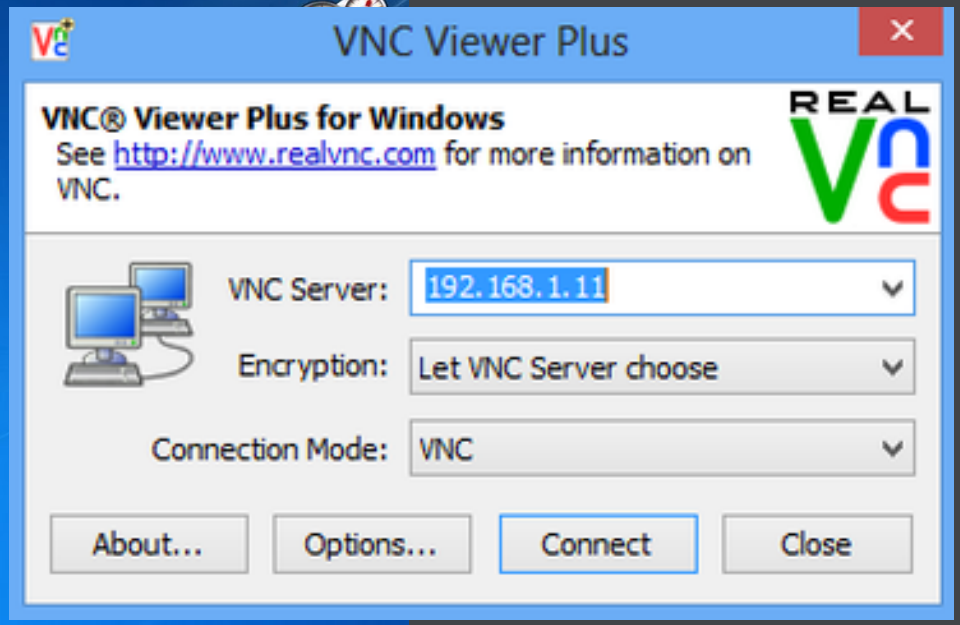
- **Uso di credenziali legittime**

Detection
Event Logs 4624 – logons 4720 – account creation 4776 – local account auth 4672 – privileged account usage
Login ‘anomali’ Workstation -> Workstation Accesso a reti ‘ristrette’ (DMZ)
Login fuori orario di lavoro
Monitorare la creazione di nuovi account

$Intrusion Forensics

- **Servizi di Desktop Remoto**





$Intrusion Forensics

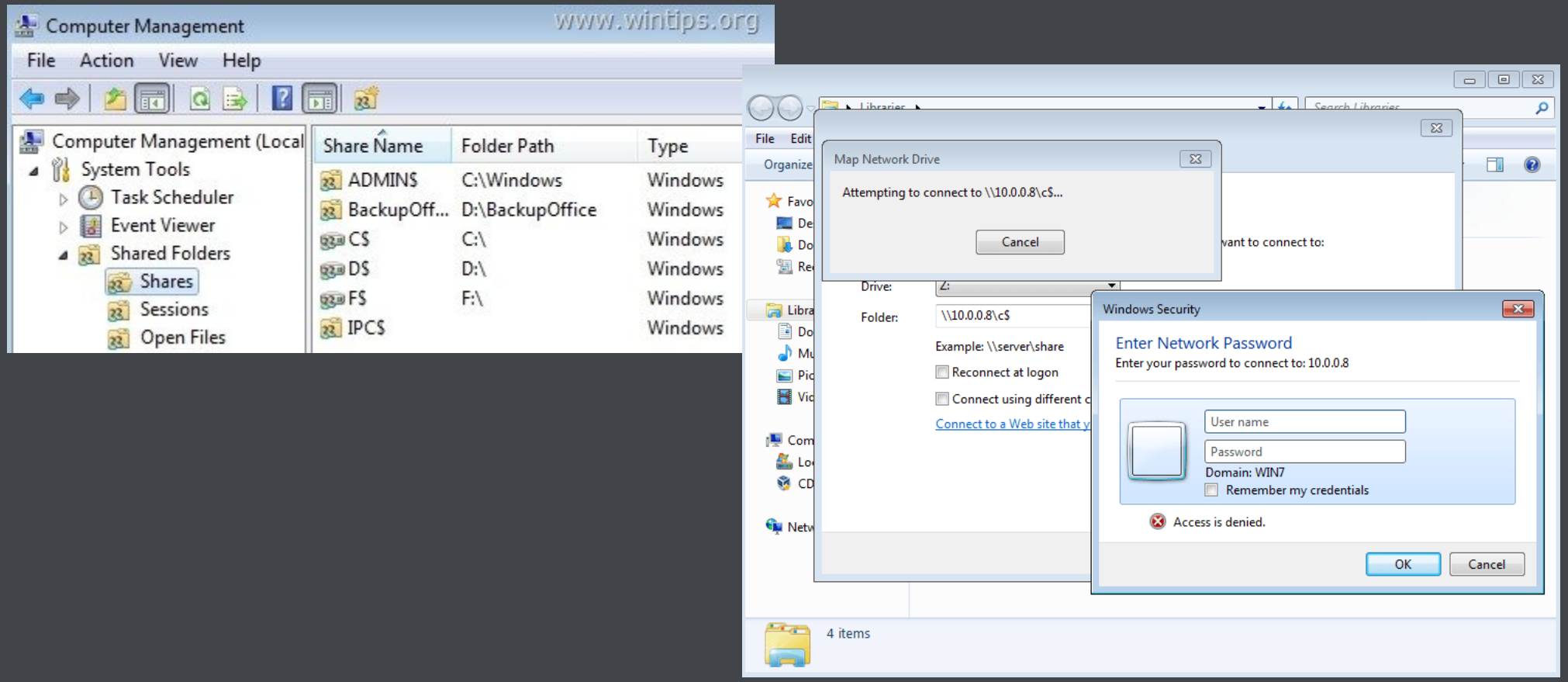
- **Servizi di Desktop Remoto**

Detection
Event Logs 4624 Logon Type 10 (RDP) 4624 Logon Type 2 (VNC) 4778/4779 – eventi di sessioni RDP
Controllo sulle applicazioni installate
Controllo dei log di specifiche applicazioni Teamviewer VNC
Tracking di particolari processi Evento 4688 RDPClip.exe

$Intrusion Forensics

- **Windows Admin Shares**

HACK IN BO®
Winter 2018 Edition



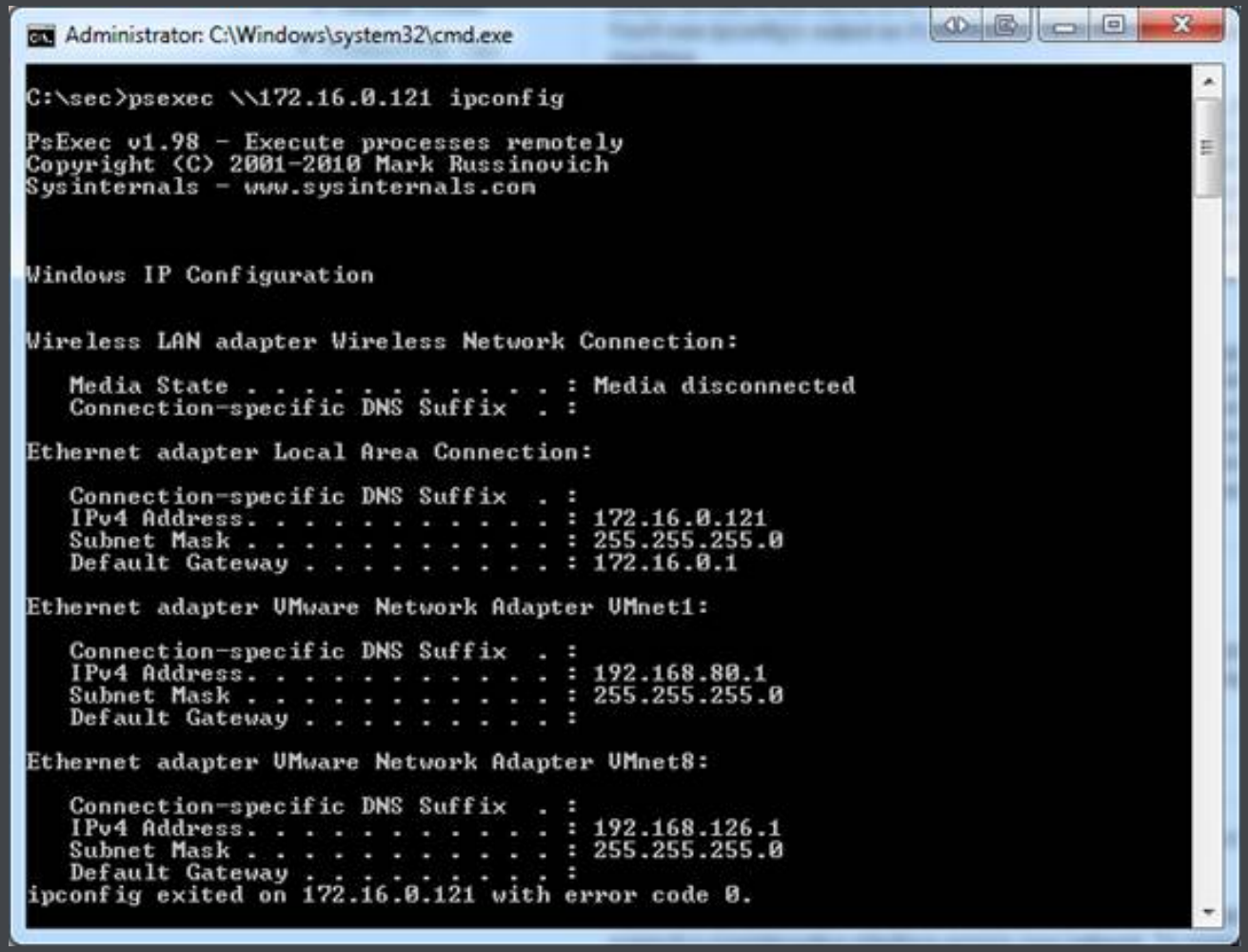
$Intrusion Forensics

- **Windows Admin Shares**

Detection
Event Logs 4624 Logon Type 3 4672 – uso di account privilegiato 5140 – accesso a cartelle di rete
Controllo dei comandi digitati sulla command line
Network forensics
Analisi di registri

$Intrusion Forensics

- **PsExec**



$Intrusion Forensics

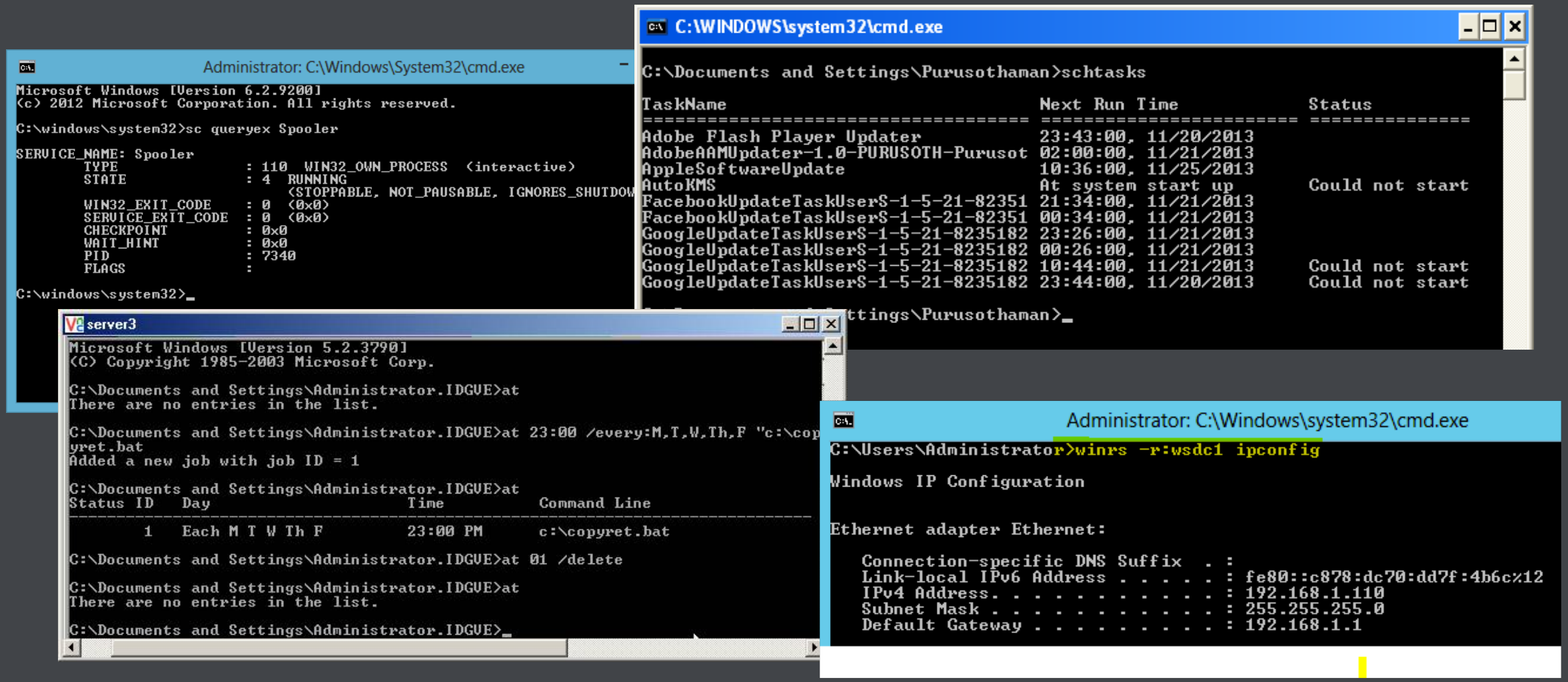
- **PsExec**

Detection
Indagine sul File System PSEXESVC.exe Utilizzo del parametro ‘-c’ (push di binari nel target)
Event Logs Logon Creazione di servizi (System log) Controllo dei comandi digitati sulla command line
Analisi della memoria Presenza dei processi **PSEXEC/PSEXSVC** Pipes

$Intrusion Forensics

- **Windows Remote Management Tools**

HACK IN BO® Winter 2018 Edition



$Intrusion Forensics

- **Windows Remote Management Tools**

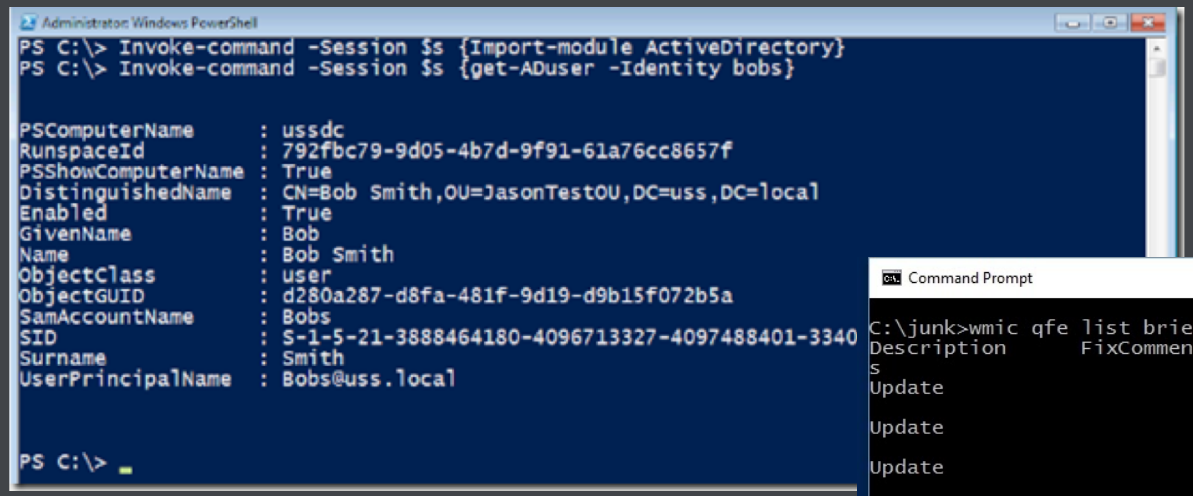
HACK IN BO® Winter 2018 Edition

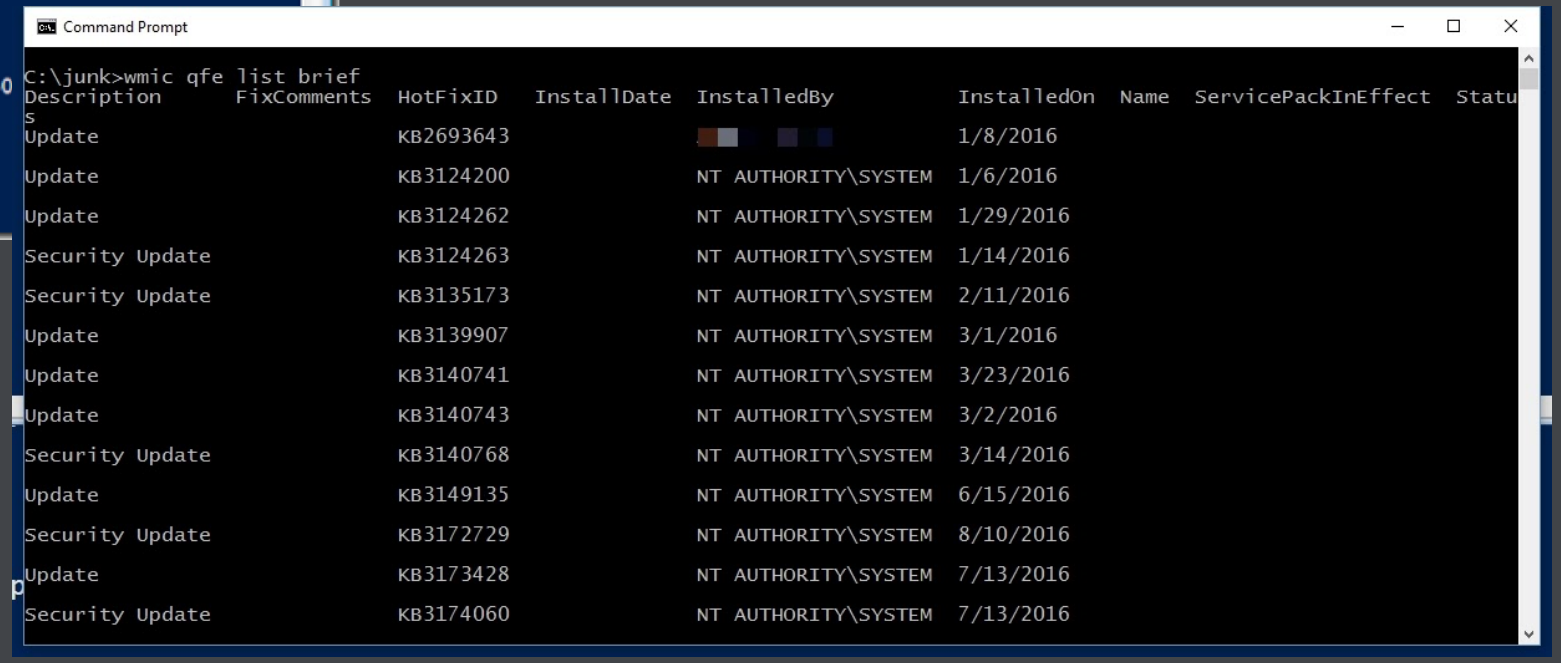
Detection
Indagine sul File System Esecuzione di programmi File .job Data ultima modifica chiavi di registro File/Script ‘particolari’
Event Logs Logon Creazione di servizi (System log) Controllo dei comandi digitati sulla command line Logs del Task Scheduler
Tracking dei processi Event ID 4688 Anomalie
Network forensics

$Intrusion Forensics

- **Powershell/WMIC**

HACK IN BO® Winter 2018 Edition





$Intrusion Forensics

- **Powershell/WMIC**

Detection
Esecuzione di applicazioni wmic.exe (sorgente) wmiprvse.exe (destinatario) powershell.exe (sorgente) wsmprovhost.exe (destinatario)
Event Logs Logon Log di script Powershell (dipende…)
Tracking dei processi Event ID 4688
Network forensics
Remote Management Service

$Intrusion Forensics

- **Exploitation di vulnerabilità**

- Vulnerabilità presenti su Web Application
- Shellshock
- MS017-010...cosa vi ricorda??
- RAT (Remote Access Tools)
- Meterpreter
- ...

$Intrusion Forensics

- **Exploitation di vulnerabilità**

Detection
Crash delle applicazioni Crash reports Event logs
Antivirus/HIPS log
Tracking dei processi Event ID 4688 Anomalie nei processi Code injection
Threat Intelligence

$Conclusioni

HackInBo® Winter 2018 Edition

Malware can hide, but it must run!

Cit.

$Conclusioni

HackInBo® Winter 2018 Edition

Grazie!