

# 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 .....0.....
0x00b70030 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 00 .....0.....

```

```

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 e9 cd d7 c5 7b 00 00 00 00 00 00 00 .5.....{.....
0x00cb0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0.....
0x00cb0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0.....
0x00cb0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0.....

```

**Event Properties - Event 1102, Eventlog**

General	Details
Special privileges assigned	
Subject:	
Security ID: CONTOSO\dadmin	
Account Name: dadmin	
Account Domain: CONTOSO	
Logon ID: 0x55CD1D	
Privileges:	
Log Name: Security	
Source:	Eventlog
Event ID:	1102
Level:	Information
User:	N/A
OpCode:	Info
More Information: <a href="#">Event Log Online</a>	

**Event Properties - Event 4672, Eventlog**

General	Details
The audit log was cleared.	
Subject:	
Security ID: CONTOSO\dadmin	
Account Name: dadmin	
Domain Name: CONTOSO	
Logon ID: 0x55CD1D	
Log Name: Security	
Source:	Eventlog
Event ID:	1102
Level:	Information
User:	N/A
OpCode:	Info
More Information: <a href="#">Event Log Online</a>	

Copy
Close

**Event Properties - Event 4672, Eventlog**

General	Details
Special Logon	
Keywords: Audit Success	
Computer: DC01.contoso.local	
Task Category: Special Logon	
Log Name:	Security
Source:	Micros
Event ID:	4672
Level:	Information
User:	N/A
OpCode:	Info
More Information: <a href="#">Event Log Online</a>	

**Event Properties - Event 1102, Eventlog**

General	Details
Audit Success	
Keywords: Log clear	
Computer: DC01.contoso.local	
Task Category: Log clear	
Log Name:	Security
Source:	Eventlog
Event ID:	1102
Level:	Information
User:	N/A
OpCode:	Info
More Information: <a href="#">Event Log Online</a>	

Copy
Close

\$Alcune domande



→ lsass.exe

HACKINBO®  
Winter 2018 Edition

# \$Alcune domande



HACKINBO®  
Winter 2018 Edition

wininit.exe

lsass.exe

# \$Alcune domande



HACKINBO®  
Winter 2018 Edition

wininit.exe

%SystemRoot%\System32\lsass.exe

lsass.exe

## \$Alcune domande



HACKINBO®  
Winter 2018 Edition

lsaiso.exe

# \$Alcune domande



HACKINBO®  
Winter 2018 Edition

wininit.exe

lsaiso.exe

## \$Alcune domande



HACKINBO®  
Winter 2018 Edition

wininit.exe

%SystemRoot%\System32\lsaiso.exe

lsaiso.exe

# \$Alcune domande



HACKINBO®  
Winter 2018 Edition

svchost.exe

# \$Alcune domande



**HACKINBO®**  
Winter 2018 Edition

**services.exe**  
(maggior parte)

**svchost.exe**

# \$Alcune domande



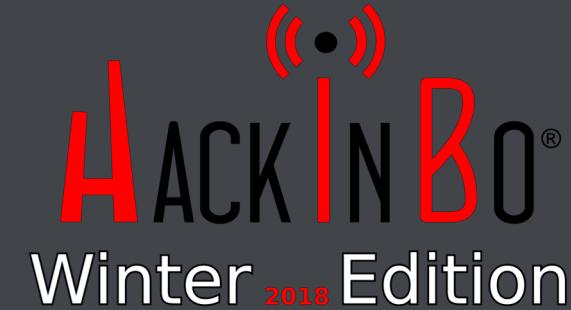
**HACKINBO®**  
Winter 2018 Edition

**services.exe**  
(maggior parte)

%SystemRoot%\system32\svchost.exe

**svchost.exe**

# \$Memory forensics



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



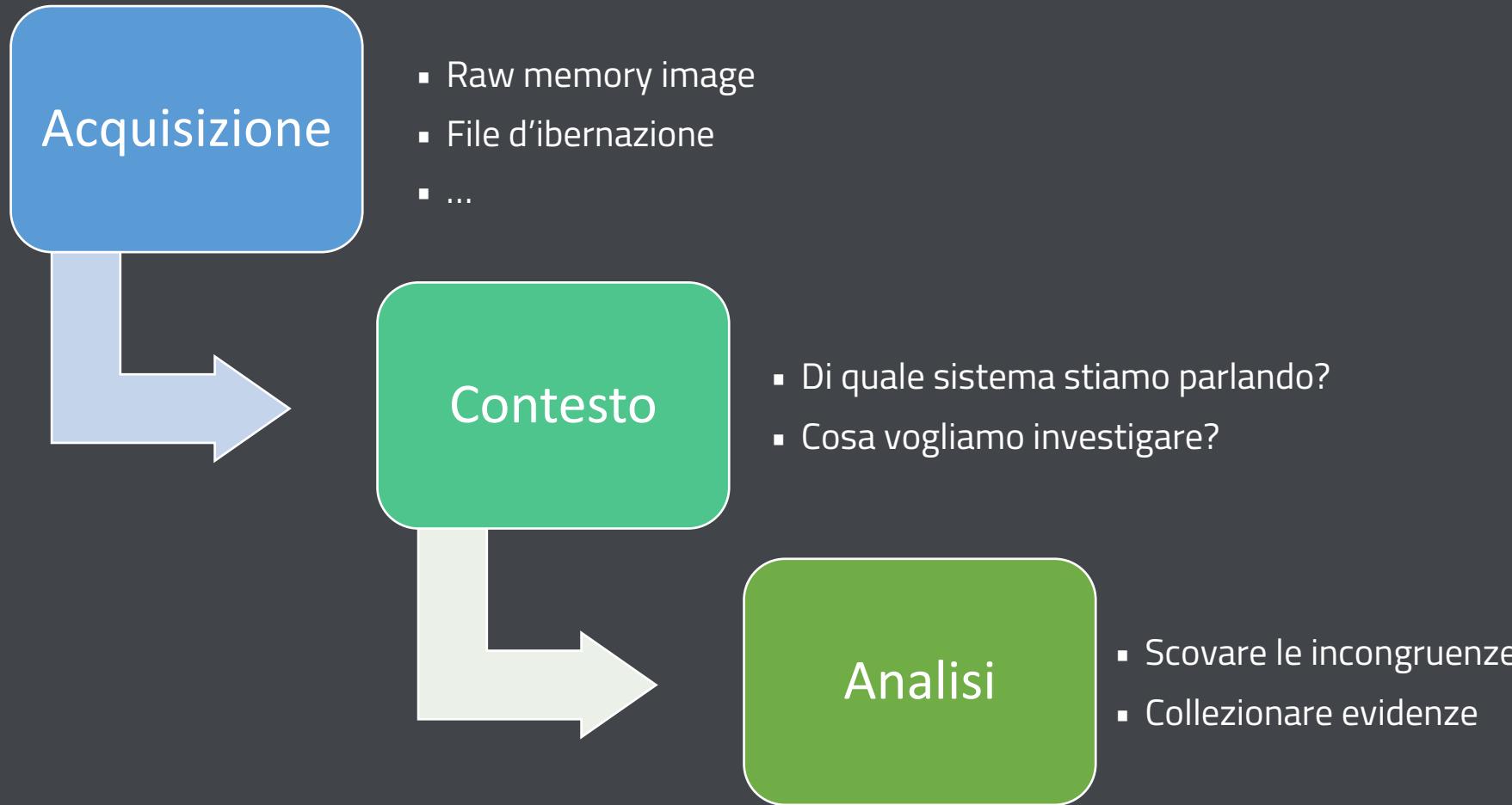
- Troviamo praticamente **tutto**
  - Processi
  - Sockets
  - Indirizzi IP
  - Encryption key
  - Passwords
  - Clipboards
  - Malware (**rootkit incluso**)

# \$Memory forensics



- 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](http://forensic.belkasoft.com/en/ram-capturer)
  - ...
- **Dead system**
  - **Hiberfil.sys**
  - Pagefile.sys
  - Swapfile.sys

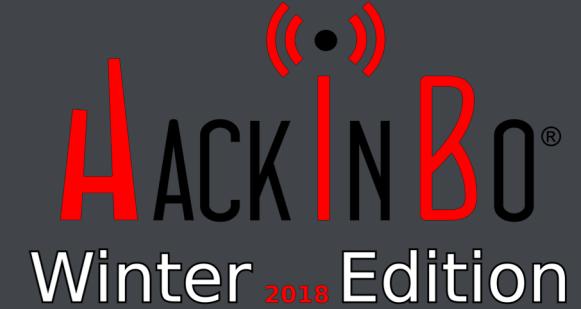
# \$Memory forensics - contesto

- 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.

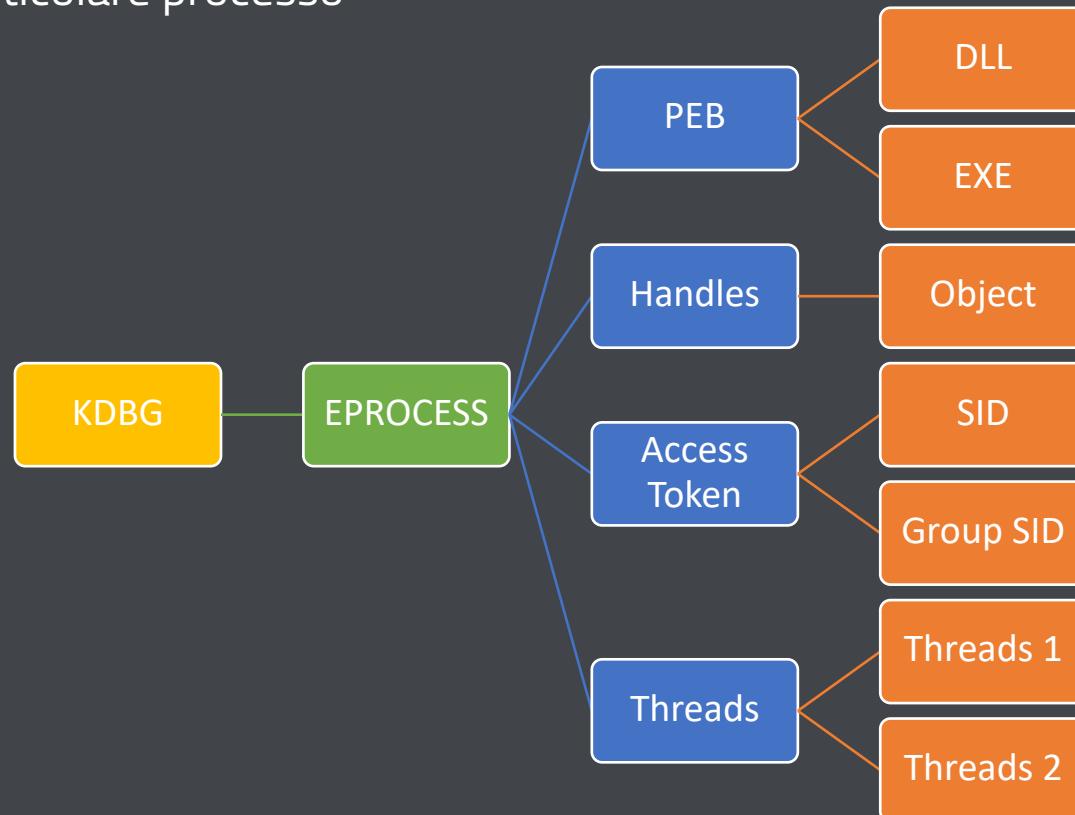
# \$Memory forensics



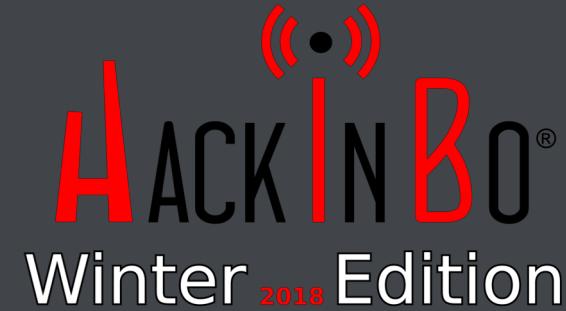
- Trovato il KDBG, si aprono le porte dell'**EPROCESS**
- L'EPROCESS ci aiuta a parsare tutta la struttura della memoria
  - Contiene tutta la lista dei processi
  - Ogni processo avrà il suo specifico **PEB** (Process Environment Block) nel quale troveremo il percorso **esatto** del processo, le relative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



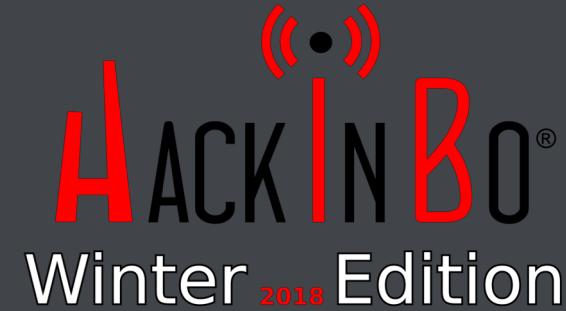
# \$Memory forensics - analisi



`./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 : 0xffffdff000L
          KUSER_SHARED_DATA : 0xffffdf0000L
```

# \$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 : 0xfffffff000L
KUSER_SHARED_DATA : 0xffffdf00000L
```

# \$Memory forensics - analisi

`./vol.py -f <immagine> pslist`

Samaritan at Samaritan_o in ~/volatility using └─ ./vol -f DemoHiB.img pslist							
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							
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`

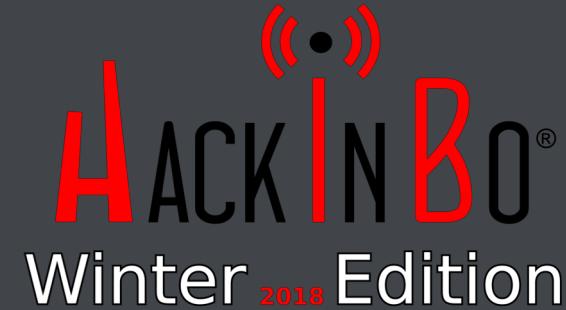
Samaritan at Samaritan_o in ~/volatility using └─ ./vol -f DemoHiB.img pslist							
Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64
0x823c8830	System	4	0	55	254	-----	0
0x8230aad8	smss.exe	564	4	3	19	-----	0
0x822ca2c0	csrss.exe	636	564	10	356	0	0
0x81f63020	winlogon.exe	660	564	16	502	0	0
0x81f22020	services.exe	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`

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:wsctnfy.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



`./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)
```

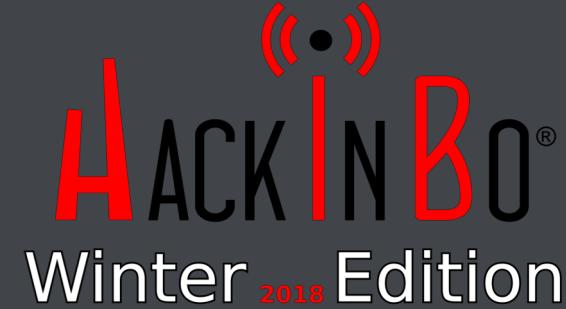
# \$Memory forensics - analisi



`./vol.py -f <immagine> connscan`

```
Samaritan at Samaritan_o in ~/volatility using
└o ./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
0x100000000	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\xpssp2res.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
0x100000000	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\xpssp2res.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
0x100000000	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\xpssp2res.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.dll

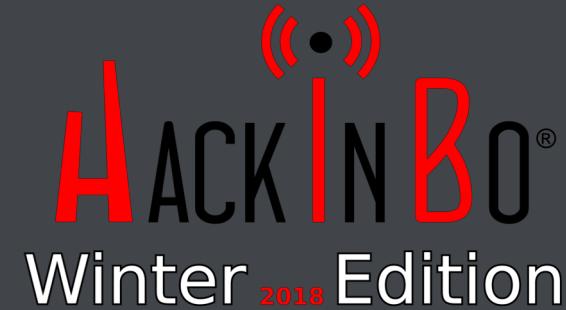
# \$Memory forensics - analisi



```
./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

```
./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 (NtEnumValueKey) 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\Test\Prefetch.Test\Prefetch\Prefetch.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\Test\Prefetch.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\MSVCR7.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\SORTDEFAULT.NLS
```

**Downloads**

- PECmd0500.zip
- Source code (zip)
- Source code (tar.gz)

© 2016 GitHub, Inc. Terms Privacy Security Contact Help

# \$Intrusion Forensics

- Prefetch Analysis

```
D:\Temp λ git clone https://github.com/EricZimmerman/PECmd.git
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\SORTDEFAULT.NLS
```

**Downloads**

- PECmd0500.zip
- Source code (zip)
- Source code (tar.gz)

# \$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\SORTDEFAULT.NLS
```

**Downloads**

- PECmd0500.zip
- Source code (zip)
- Source code (tar.gz)

© 2016 GitHub, Inc. Terms Privacy Security Contact Help

# \$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\APISCHHEMA.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\CompatCacheParser\CompatCacheParser\bin\Release (master)
λ AppCompatCacheParser.exe -t c:\Temp\SYSTEM2SETS -s c:\Temp
AppCompat Cache 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

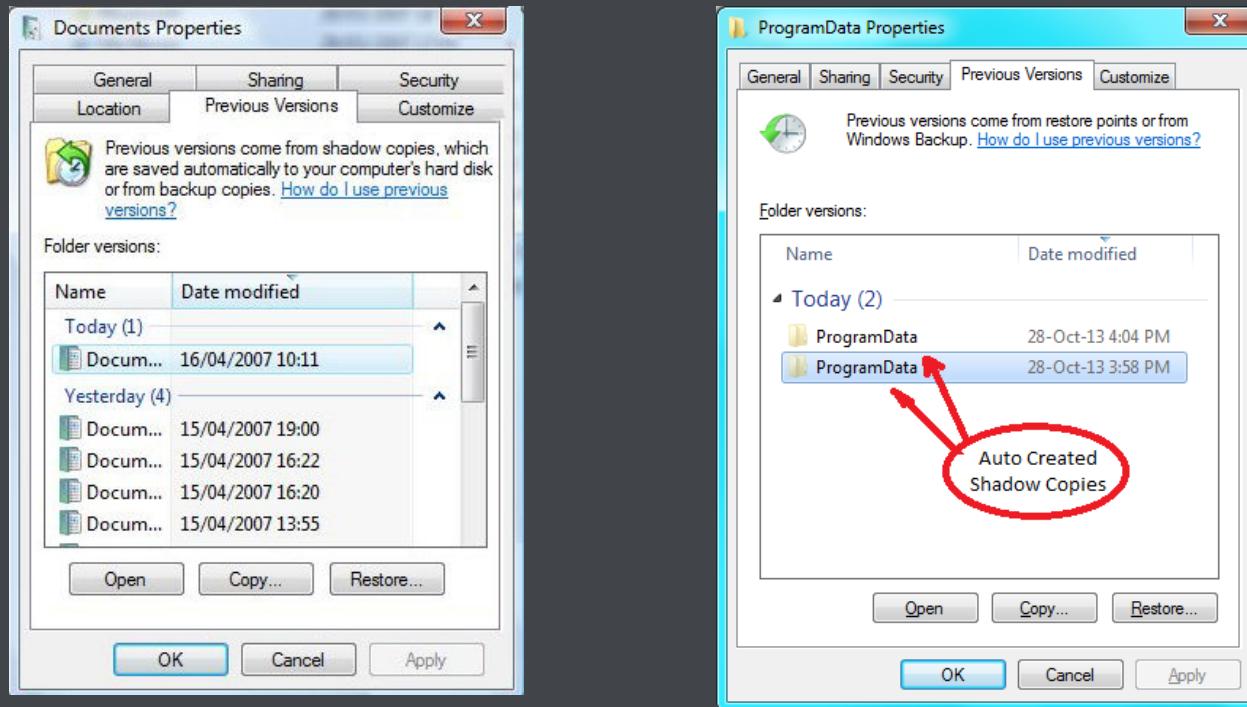
Results will be saved to 'c:\Temp\Windows7x64_Windows2008R2_SYSTEM2SETS_AppCompatCache.tsv'

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

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.34.139:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.34.135
[*] Meterpreter session 2 opened (192.168.34.139:4444 -> 192.168.34.135:1739) at 2013-07-30 06:30:28 -0400
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089c0:::more you are able to
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f3f07224e22c5dc9e3d50224ebbf04b7:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:41361b1534272026576c22449c3b6aff:::
user:1003:b34ce522c3e4c8774a3b108f3fa6cb6d:a87f3a37d73085c45f9416be5787d86:::
peru:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089c0:::
IUSR_HP-SRV01:1108:6dbad79696399a35bac6f-70675-0001-0100012015E5-1-72-7-074A5C01-04-0000000000000000
IWAM_HP-SRV01:1109:015839b59b7a2b8926c2
albert:1114:d0b22b77a558f4c1511a02b6cac
nina:1115:3993fcde5c417d12e72c57ef50f76
nick:1116:681e9a747943826f824a5691239d4
jasmine:1117:cbc501a4d222778365c4a55f32
joy:1118:f5d13a813b5d5ffac467021088dc70
HP-SRV01$:1007:aad3b435b51404eeaad3b435

Authentication Id : 0 ; 2858340 <00000000:002b9d64>
Session           : Service from 0
User Name         : svc-SQLDBEngine01
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-22

msv :
    * Username : svc-SQLDBEngine01
    * Domain  : ADSECLAB
    * NTLM    : d0abfc0cb689f4cdc8959a1411499
    * SHA1    : 46f0516e6155eed60668827b0a4da
tspkg :
    * Username : svc-SQLDBEngine01
    * Domain  : ADSECLAB
    * Password : ThisIsAGoodPassword99!
wdigest :
    * Username : svc-SQLDBEngine01
    * Domain  : ADSECLAB
    * Password : ThisIsAGoodPassword99!
kerberos :
    * Username : svc-SQLDBEngine01
    * Domain  : LAB.ADSECURITY.ORG
    * Password : ThisIsAGoodPassword99!
ssp :
credman :
```



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > list_tokens -u
```

Delegation Tokens Available

```
=====
MAROON\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
```

Impersonation Tokens Available

```
=====
NT AUTHORITY\ANONYMOUS LOGON
```

# \$Intrusion Forensics

- Uso di credenziali legittime



## Detection

### Event Logs

4624 – logons  
4720 – account creation  
4776 – local account auth  
4672 – privileged account usage

### Login ‘anomali’

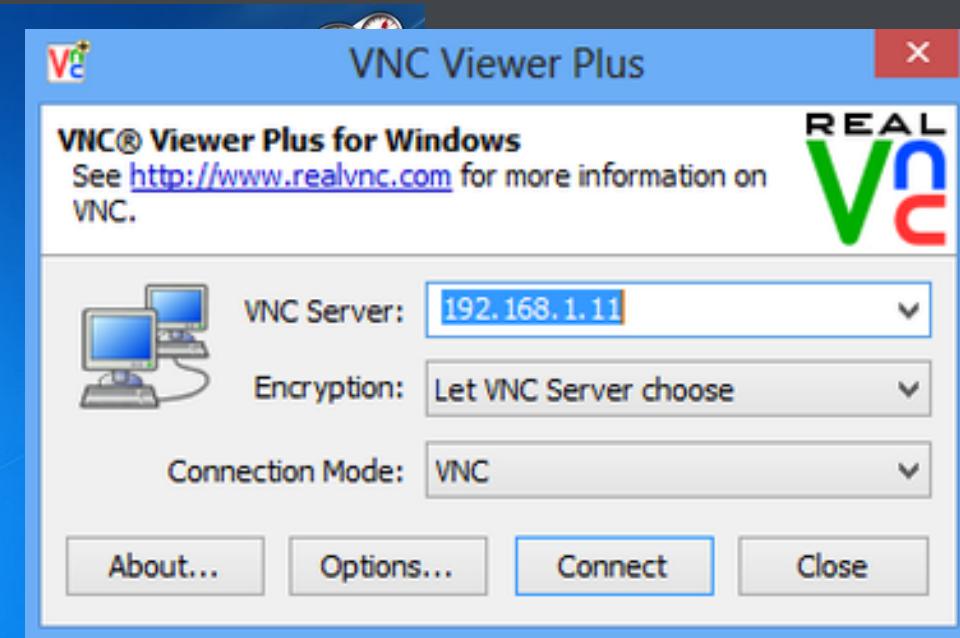
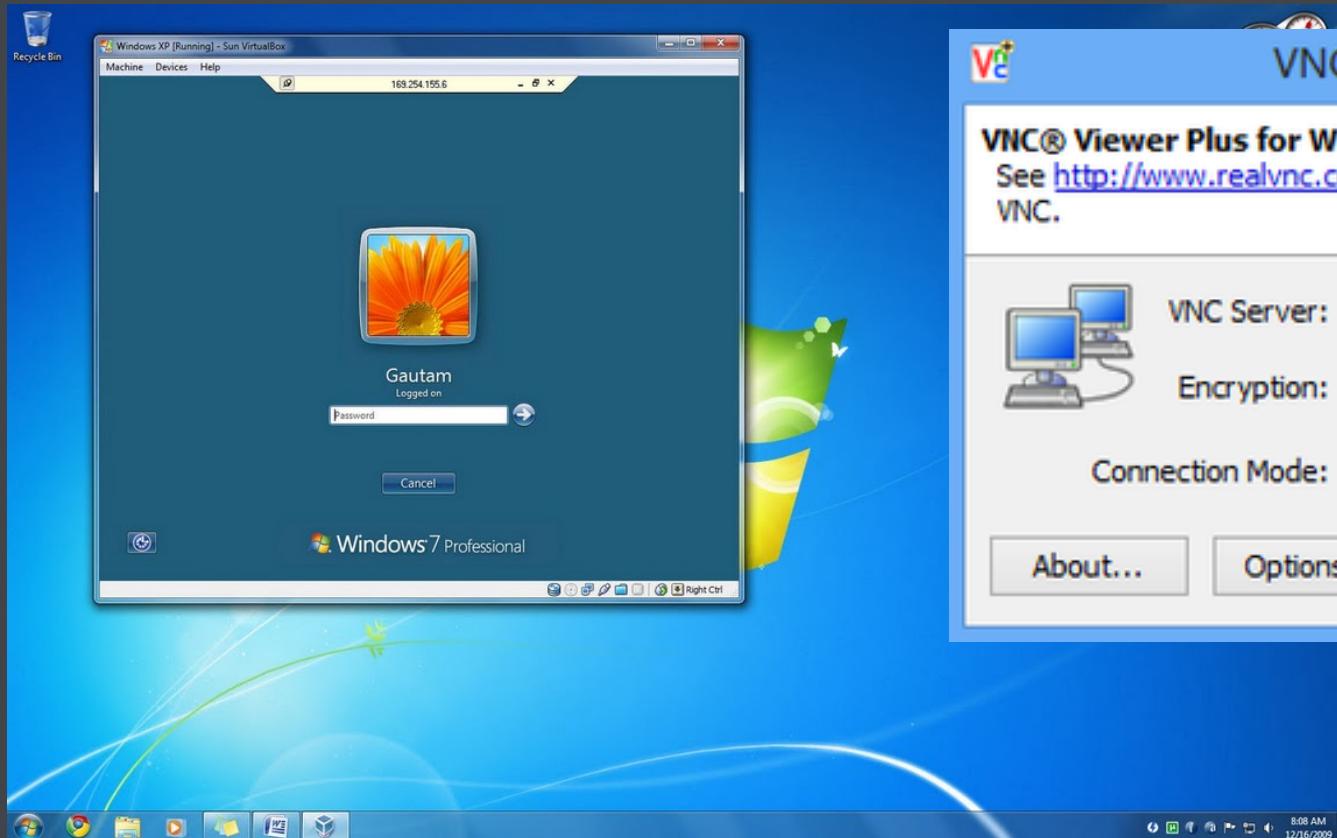
Workstation -> Workstation  
Accesso a reti ‘ristrette’ (DMZ)

### Login fuori orario di lavoro

Monitorare la creazione di nuovi account

# \$Intrusion Forensics

- Servizi di Desktop Remoto



HACKINB0®  
Winter 2018 Edition

# \$Intrusion Forensics

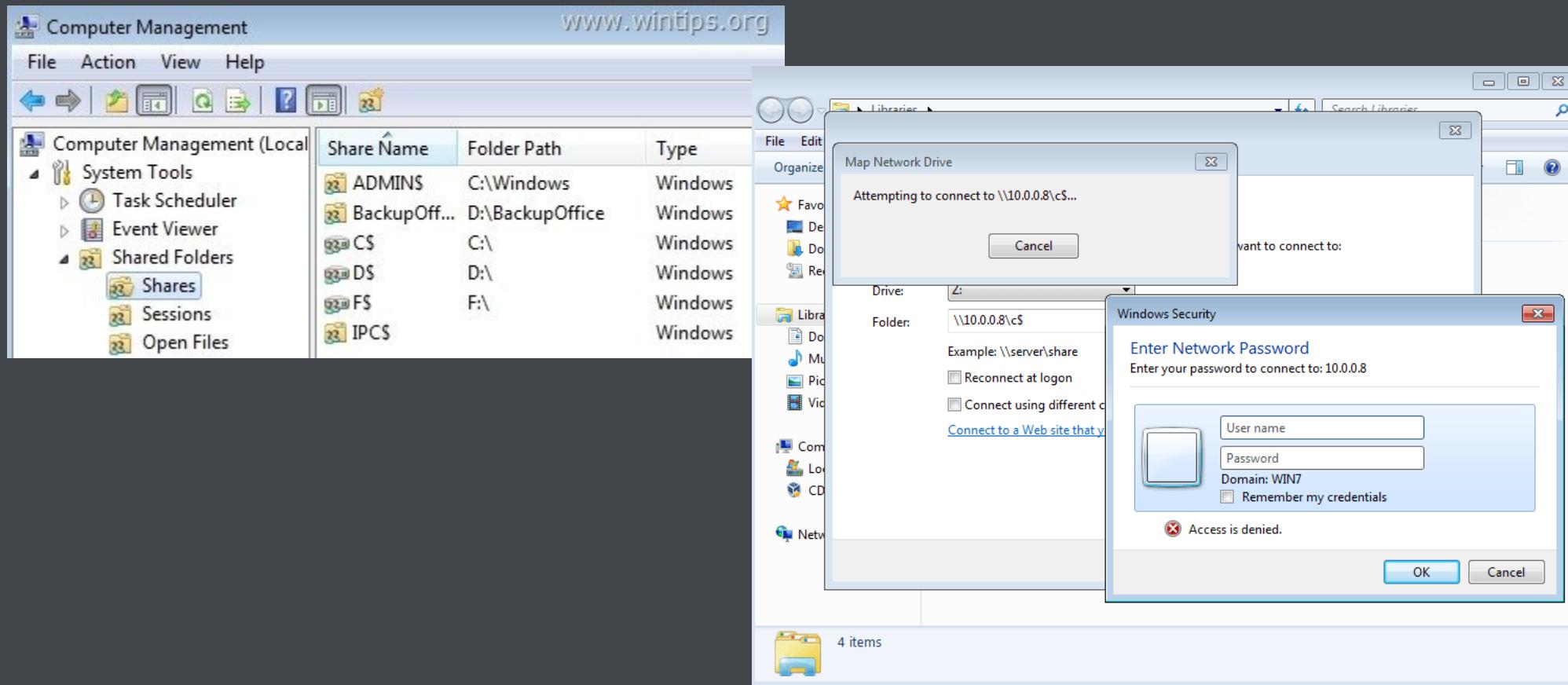
- Servizi di Desktop Remoto



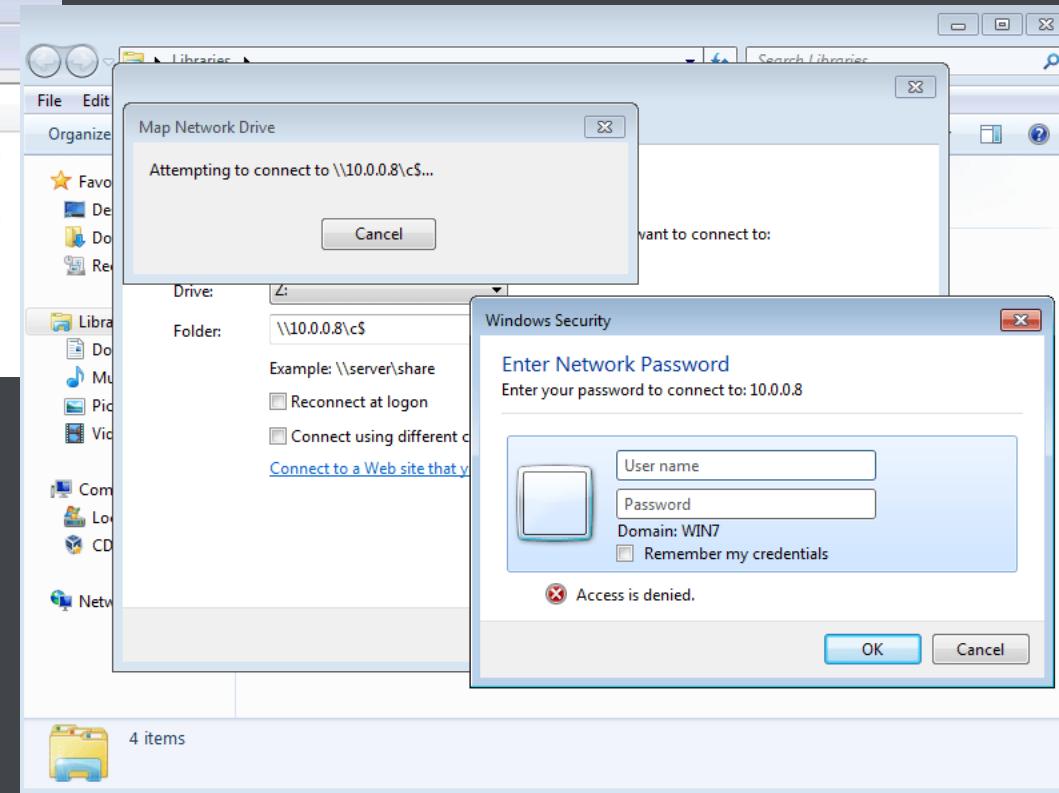
Detection
Event Logs 4624 Logon Type 10 (RDP) 4624 Logon Type 2 (VNC) 4778/4779 – eventi di sessioni RDP
Controllo sulle applicazioni installate
Controllo dei log di specifiche applicazioni Teamviewer VNC
Tracking di particolari processi Evento 4688 RDPClip.exe

# \$Intrusion Forensics

- Windows Admin Shares



Share Name	Folder Path	Type
ADMIN\$	C:\Windows	Windows
BackupOff...	D:\BackupOffice	Windows
C\$	C:\	Windows
DS	D:\	Windows
FS	F:\	Windows
IPCS		Windows



# \$Intrusion Forensics

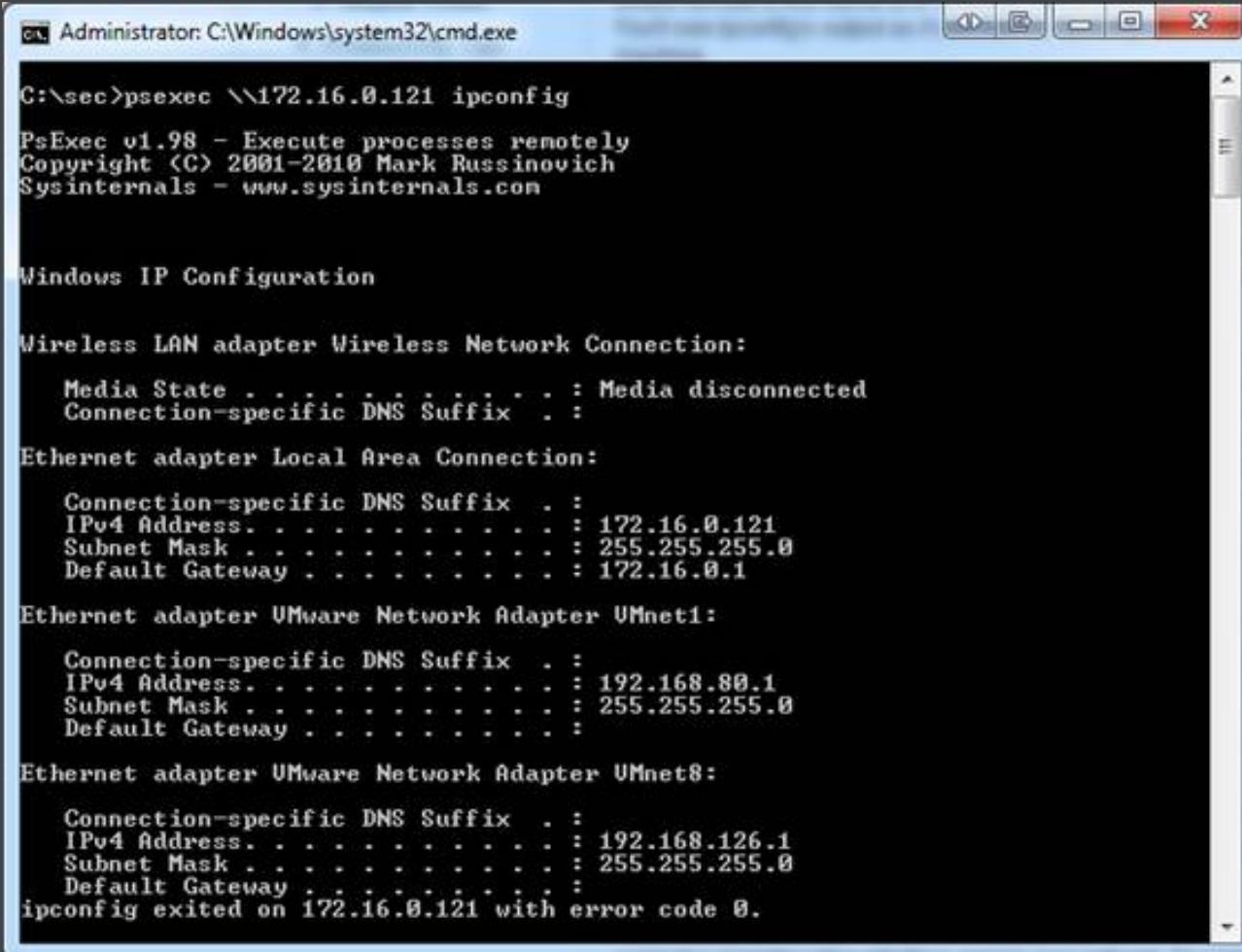
- Windows Admin Shares



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



Administrator: C:\Windows\system32\cmd.exe

```
C:\sec>psexec \\172.16.0.121 ipconfig
PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . . . . . :
  IPv4 Address . . . . . : 172.16.0.121
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 172.16.0.1

Ethernet adapter VMware Network Adapter VMnet1:
  Connection-specific DNS Suffix . . . . . :
  IPv4 Address . . . . . : 192.168.80.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:
  Connection-specific DNS Suffix . . . . . :
  IPv4 Address . . . . . : 192.168.126.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
ipconfig exited on 172.16.0.121 with error code 0.
```

# \$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/PSEXSV**C

Pipes

# \$Intrusion Forensics

- Windows Remote Management Tools



The image shows a Windows terminal session with four windows open:

- Administrator: C:\Windows\System32\cmd.exe**: Displays the output of the command `sc queryex Spooler`, showing details about the Spooler service.
- C:\Documents and Settings\Purusothaman>schtasks**: Displays a list of scheduled tasks with columns for TaskName, Next Run Time, and Status. Tasks listed include Adobe Flash Player Updater, AdobeAAMUpdater-1.0-PURUSOTH-Purusot, AppleSoftwareUpdate, AutoKMS, FacebookUpdateTaskUserS-1-5-21-82351, GoogleUpdateTaskUserS-1-5-21-8235182, GoogleUpdateTaskUserS-1-5-21-8235182, GoogleUpdateTaskUserS-1-5-21-8235182, and GoogleUpdateTaskUserS-1-5-21-8235182.
- Vc server3**: Displays the output of the command `at`, showing a scheduled job named "copyret.bat" added at 23:00 every Monday through Friday.
- Administrator: C:\Windows\system32\cmd.exe**: Displays the output of the command `winrs -r:wsdc1 ipconfig`, showing the Windows IP Configuration for the Ethernet adapter.

# \$Intrusion Forensics

- Windows Remote Management Tools



## 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

Anomalia

Network forensics

# \$Intrusion Forensics

- Powershell/WMIC



The image shows two windows side-by-side. On the left is a Windows PowerShell window titled 'Administrator: Windows PowerShell'. It contains the following command and its output:

```
PS C:\> Invoke-command -Session $s {Import-module ActiveDirectory}
PS C:\> Invoke-command -Session $s {get-ADUser -Identity bobs}

PSCoomputerName : ussdc
RunspaceId       : 792fbc79-9d05-4b7d-9f91-61a76cc8657f
PSShowComputerName : True
DistinguishedName : CN=Bob Smith,OU=JasonTestOU,DC=uss,DC=local
Enabled          : True
GivenName        : Bob
Name             : Bob Smith
ObjectClass      : user
ObjectGUID       : d280a287-d8fa-481f-9d19-d9b15f072b5a
SamAccountName   : Bobs
SID              : S-1-5-21-3888464180-4096713327-4097488401-3340
Surname          : Smith
UserPrincipalName : Bobs@uss.local
```

On the right is a Command Prompt window titled 'Command Prompt'. It contains the following command and its output:

```
C:\junk>wmic qfe list brief
```

Description	FixComments	HotFixID	InstallDate	InstalledBy	InstalledOn	Name	ServicePackInEffect	Status
Update		KB2693643			1/8/2016			
Update		KB3124200		NT AUTHORITY\SYSTEM	1/6/2016			
Update		KB3124262		NT AUTHORITY\SYSTEM	1/29/2016			
Security Update		KB3124263		NT AUTHORITY\SYSTEM	1/14/2016			
Security Update		KB3135173		NT AUTHORITY\SYSTEM	2/11/2016			
Update		KB3139907		NT AUTHORITY\SYSTEM	3/1/2016			
Update		KB3140741		NT AUTHORITY\SYSTEM	3/23/2016			
Update		KB3140743		NT AUTHORITY\SYSTEM	3/2/2016			
Security Update		KB3140768		NT AUTHORITY\SYSTEM	3/14/2016			
Update		KB3149135		NT AUTHORITY\SYSTEM	6/15/2016			
Security Update		KB3172729		NT AUTHORITY\SYSTEM	8/10/2016			
Update		KB3173428		NT AUTHORITY\SYSTEM	7/13/2016			
Security Update		KB3174060		NT AUTHORITY\SYSTEM	7/13/2016			

# \$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



Malware can **hide**, but it must **run!**

Cit.

\$Conclusioni



Grazie!