

Hunting for Credentials Dumping in Windows Environment

Teymur Kheirhabarov

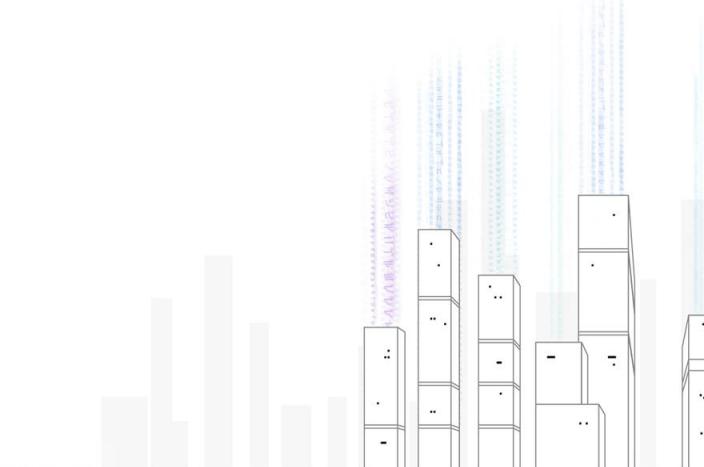
ZERO
NIGHTS



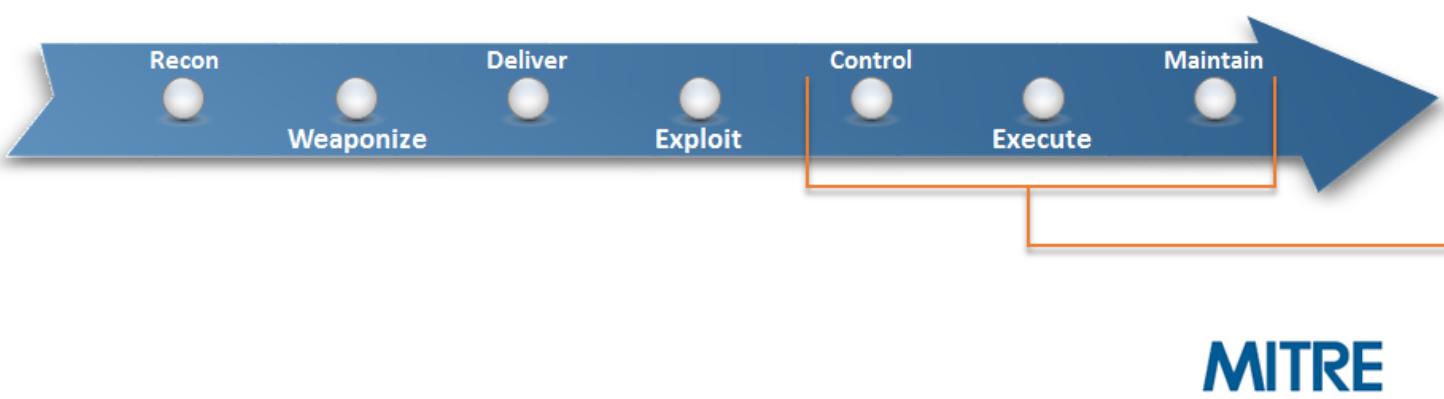


- Senior SOC Analyst @Kaspersky Lab
- SibSAU (Krasnoyarsk) graduate
- Ex- System admin
- Ex- Infosec admin
- Ex- Infosec dept. head
- Twitter @HeirhabarovT
- www.linkedin.com/in/teymur-kheirkhabarov-73490867/

Who am I?



www.zeronights.org
#zeronights



What are we going to talk about?

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

Credential Dumping Technique

ID	T1003
Tactic	Credential Access
Platform	Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Permissions Required	Administrator, SYSTEM
Data Sources	API monitoring, Process command-line parameters, Process monitoring, PowerShell logs
CAPEC ID	CAPEC-567

Credential dumping is the process of obtaining account login and password information from the operating system and software.

We will look at different methods of dumping credentials in Windows environment and how to detect them via logs (native Windows, Sysmon)



- [APT1](#) has been known to use credential dumping
- [APT28](#) regularly deploys both publicly available and custom password retrieval tools on victims
- [APT3](#) has used a tool to dump credentials by injecting itself into lsass.exe
- [Axiom](#) has been known to dump credentials
- [Cleaver](#) has been known to dump credentials
- [FIN6](#) has used [Windows Credential Editor](#) for credential dumping, as well as Metasploit's [PsExec](#) NTDSGRAB module to obtain a copy of the victim's Active Directory database
- Even ransomware use credential dumping

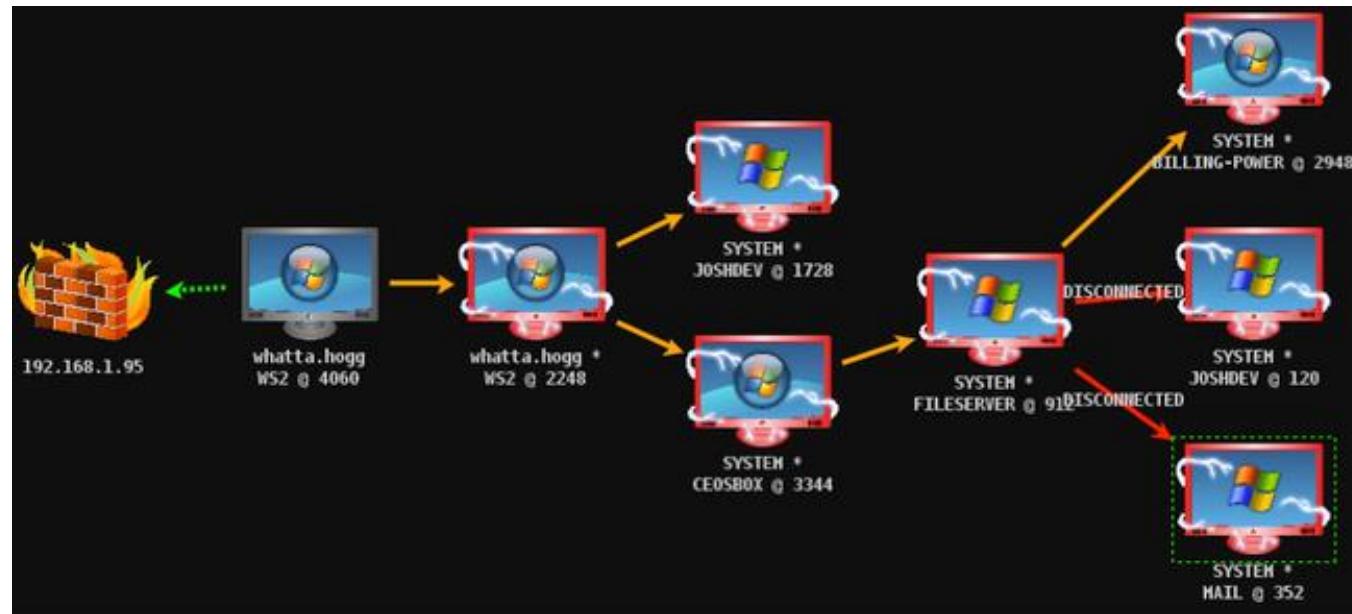
Why is it so important?





How will adversaries use dumped credentials?

Dumped credentials can be used to perform [Lateral Movement](#) and access restricted information



<https://www.phdays.ru/program/231388/>



Hunting Lateral Movement in Windows Infrastructure

Teymur Kheirkhabarov





What can be dumped and where from?

- **LSASS memory:** clear-text passwords of logged on users, Kerberos tickets, Kerberos encryption keys, SmartCard/Token PIN codes, LM/NTLM hashes, DPAPI Domain Backup Key, Domain Trust Auth Information, cached DPAPI MasterKeys, cached SysKey (need to decrypt SAM/LSA Secrets/Cached credentials/NTDS.dit), clear-text passwords of accounts, stored in Credential Manager;
- **SAM registry hive/file:** LM/NTLM hashes of local users;
- **SECURITY registry hive/file:** cached credentials, LSA Secrets (account passwords for services, password used to logon to Windows if auto-logon is enabled);
- **NTDS.dit file:** hashes of domain accounts, Domain Backup Key;
- **SYSTEM registry hive/file:** SysKey, that need to decrypt SAM/LSA Secrets/Cached credentials/NTDS.dit.





- LSASS memory contain a lot of sensitive data that can be dumped!
- This data protected by LsaProtectMemory and can be unprotected by LsaUnprotectMemory (used symmetric encryption, keys can be found in LSASS memory).
- There several ways:
 - online from ring3 – OpenProcess...;
 - online from ring0 – use driver for accessing LSASS memory;
 - offline from LSASS memory dumps;
 - offline from other sources, that contain LSASS memory (virtual machine memory files, crashdumps, hibernation file).

Dumping from LSASS memory

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 747368 <00000000:000b6768>
Session          : Interactive from 2
User Name        : DWM-2
Domain           : Window Manager
Logon Server     : <null>
Logon Time       : 07.11.2017 19:16:05
SID              : S-1-5-90-2

msv :
[000000003] Primary
* Username : WIN-FJRNSLDJHD2$
* Domain  : TEST
* NTLM    : f9228579f8bdf37020d91b267f223d3e
* SHA1    : c3a1b23634d3c0d51a18299801129774282614c1

tspkg :
wdigest :
* Username : WIN-FJRNSLDJHD2$
* Domain  : TEST
* Password : 36 63 dc 18 c6 50 15 6d 84 25 6c c0 28 24 9c e7 f9 b5 52 6
8 79 0a ce 24 2b ba 36 e8 3b e3 e7 3a b1 97 63 f2 a7 27 b6 14 46 8e 6a f7 0d e7
f8 80 2d 3c e9 c1 06 97 fb 35 a3 0c 5d bd 8b 51 54 68 67 08 32 f7 79 00 82 24 40
7a d6 1e 4a d4 dc 4e 30 48 5b 23 89 50 98 24 54 d5 04 a2 48 a9 b0 a9 b8 38 85 b
c 60 72 6d 90 83 42 45 d7 4a 93 50 97 5c aa 95 93 b6 8a 50 05 92 6c b6 c9 56 ef
17 78 14 c2 26 7b 54 e9 db 08 fc 4a c3 94 66 66 5f 4f a1 8b e1 df c1 f7 63 97 62
23 f3 f0 b8 6e 43 48 21 59 e1 70 85 b0 ea fb 65 4c 67 5f b4 c4 15 50 a4 93 1d c
e c6 c6 78 42 01 1c 2f 40 8a 57 a3 f9 52 50 e2 ad 53 ec 48 45 fe 92 f3 2f dd 35
e5 0e 7d 8d 04 07 e0 91 fa df ec 68 03 f2 23 9f e6 90 2e 62 b5 36 34 c1 b1 01 0b
43 ef 6e 62 6e cb ac
```

Tools: Mimikatz, Invoke-Mimikatz, Windows Credential Editor (WCE), fgdump, pwdump6, pwdumpX, taskmgr/procdump/sqldumper, WinDbg mimikatz plugin, Volatility mimikatz plugin



Dumping from LSASS memory

What data can be extracted from LSASS memory in different Windows?

	Primary			CredentialKeys				tspkg	wdigest		kerberos				livessp	ssp	dpapi	credman 6
	LM	NTLM	SHA1	NTLM	SHA1	Root	DPAPI	off	on	off	on	pass 1	PIN 4	tickets	eKeys			
Windows XP/2003																		
Local Account								2										
Domain Account								2					5					
Windows Vista/2008 & 7/2008r2																		
Local Account																		
Domain Account																		
Windows 8/2012																		
Microsoft Account																		
Local Account																		
Domain Account																		
Windows 8.1/2012r2																		
Microsoft Account	3			3			3	3		3								
Local Account	3			3			3	3		3								
Domain Account	3			3			3	3		3								
Domain Protected Users	3			3			3	3		3								
Windows 8.1 vault for user's authentication																		



Dumping from LSASS memory LSASS memory access. Sysmon events

Event Properties - Event 1, Sys

General Details

Process Create:
UtcTime: 2017-11-07 15:23:57.758
ProcessGuid: {d134eb5b-d00d-5a01-0000-001061191800}
ProcessId: 4780
Image: C:\tools\mimikatz\x64\notepad.exe
CommandLine: notepad.exe "privilege::debug" "sekurlsa::logonpasswordexport"
CurrentDirectory: C:\tools\mimikatz\x64\
User: TEST\Administrator
LogonGuid: {d134eb5b-ce36-5a01-0000-00201b980b00}
LogonId: 0xB981B
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=2C527D980EB30DAA789492283F9BF69E, SHA256=FB55414848281F804858CE188C3DC659D129E283BD62D58D34F6E6F56
ParentProcessGuid: {d134eb5b-ce78-5a01-0000-001034dc1100}
ParentProcessId: 5116
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"

Event Properties - Event 10, Sysmon

General Details

Process accessed:
UtcTime: 2017-11-07 15:23:57.826
SourceProcessGUID: {d134eb5b-d00d-5a01-0000-001061191800}
SourceProcessId: 4780
SourceThreadId: 1420
SourceImage: C:\tools\mimikatz\x64\notepad.exe
TargetProcessGUID: {d134eb5b-c61e-5a01-0000-001017c80000}
TargetProcessId: 564
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1010
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+967da|C:\Windows\system32\KERNELBASE.dll+271a|C:\tools\mimikatz\x64\notepad.exe+6dc6c|C:\tools\mimikatz\x64\notepad.exe+6dfd9|C:\tools\mimikatz\x64\notepad.exe+6db91|C:\tools\mimikatz\x64\notepad.exe+4ae04|C:\tools\mimikatz\x64\notepad.exe+4ac3a|C:\tools\mimikatz\x64\notepad.exe+4a98f|C:\tools\mimikatz\x64\notepad.exe+73935|C:\Windows\system32\KERNEL32.DLL+15bd|C:\Windows\SYSTEM32\ntdll.dll+743d1



Dumping from LSASS memory LSASS memory access. Lets hunt it!

```
source_name:"Microsoft-Windows-Sysmon" AND event_id:10 AND
event_data.TargetImage:"*\lsass.exe" AND -event_data.GrantedAccess:(0x40
0x1400 0x1000 0x10000) AND -event_data.SourceImage:(*\taskmgr.exe"
"\procexp64.exe" "*\procexp.exe" "*\sm.exe" "*\csrss.exe" "*\wininit.exe"
"\wmiprvse.exe")
```

Time	computer_name	event_data.SourceImage	event_data.TargetImage	event_data.GrantedAccess	task
► November 8th 2017, 02:34:02.502	WIN-FJRNSLDJHD2.test.local	C:\tools\PwDump6\servpw64.exe	C:\Windows\system32\lsass.exe	0x1f3fff	Process accessed (rule: ProcessAccess)
► November 8th 2017, 02:11:21.187	pc0002.test.local	C:\Windows\cioyj.exe	C:\Windows\system32\lsass.exe	0x1f1fff	Process accessed (rule: ProcessAccess)
► November 8th 2017, 02:06:38.704	pc0002.test.local	C:\Windows\vdcpqepjk.exe	C:\Windows\system32\lsass.exe	0x1f1fff	Process accessed (rule: ProcessAccess)
► November 8th 2017, 01:52:52.710	pc0002.test.local	C:\Windows\ueoimxq.exe	C:\Windows\system32\lsass.exe	0x1f1fff	Process accessed (rule: ProcessAccess)
► November 7th 2017, 23:17:12.860	pc0002.test.local	C:\tools\mimikatz\win32\mimikatz.exe	C:\Windows\system32\lsass.exe	0x1038	Process accessed (rule: ProcessAccess)
► November 7th 2017, 23:17:12.859	pc0002.test.local	C:\tools\mimikatz\win32\mimikatz.exe	C:\Windows\system32\lsass.exe	0x1010	Process accessed (rule: ProcessAccess)
► November 7th 2017, 20:33:01.050	WIN-FJRNSLDJHD2.test.local	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe	C:\Windows\system32\lsass.exe	0x143a	Process accessed (rule: ProcessAccess)
► November 7th 2017, 20:17:38.435	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\system32\lsass.exe	0x143a	Process accessed (rule: ProcessAccess)



Dumping from LSASS memory LSASS memory access. Native Windows events. Is it possible?

<https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1507-and-1511>



In Windows 10, versions 1507 a default process SACL was added to LSASS.exe to log processes attempting to access LSASS.exe. The SACL is L"S:(AU;SAFA;0x0010;;;WD)".

You can enable this under **Advanced Audit Policy Configuration\Object Access\Audit Kernel Object**. This can help identify attacks that steal credentials from the memory of a process

The screenshot shows a Windows PowerShell window and the 'Audit Kernel Object Properties' dialog.

PowerShell Commands:

- PS C:\> \$p = Get-NtProcess -Name lsass.exe -Access GenericAll,AccessSystemSecurity
- PS C:\> \$sd = \$p.GetSecurityDescriptor("sacl")
- PS C:\> \$sd.Sacl | Format-List
- PS C:\> \$sd.Tosddl("sacl")

Audit Kernel Object Properties Dialog:

- Policy Tab:** Shows 'Audit Kernel Object' selected.
- Configure the following audit events:**
 - Success
 - Failure

Annotations:

- An annotation labeled 'Request SACL Access' points to the command '\$sd.Tosddl("sacl")'.
- An annotation labeled 'Request SACL' points to the command '\$sd.Sacl | Format-List'.
- An annotation labeled 'SACL' points to the output of the '\$sd.Sacl | Format-List' command, specifically the 'AceType' row.
- An annotation labeled 'SACL as SDDL' points to the output of the '\$sd.Tosddl("sacl")' command.



Dumping from LSASS memory
LSASS memory access. Native Windows events. And what about <Windows 10?

It is also possible to change LSASS.exe SACL in earlier Windows versions (<10). To automate this process you can write script and configure it to run on system startup

The screenshot illustrates the steps to change the SACL for the LSASS process (lsass.exe) in Windows.

- Process Explorer:** Shows the LSASS process (lsass.exe) selected in the list. A pink arrow points to the context menu, which includes options like "Properties...".
- lsass.exe:564 Properties Dialog:** The "Properties" dialog for lsass.exe is open. A pink arrow points to the "Security" tab. The "Owner" section shows "Administrators (TEST\Administrators)". The "Integrity level" is set to "System Mandatory Level".
- Advanced Security Settings Dialog:** The "Advanced Security Settings for lsass.exe: 564" dialog is open. A pink arrow points to the "Permissions" tab, which lists "Everyone" with "Full Control".
- Audit Kernel Object Properties Dialog:** A smaller window titled "Audit Kernel Object Properties" is open, showing the "Audit Kernel Object" policy and audit events configuration. A pink arrow points to the "Success" checkbox under "Configure the following audit events".

www.zeronights.org #zeronights



Event Properties - Event 4688, Microsoft Windows

General Details

A new process has been created.

Subject:

Security ID:	TEST\Administrator
Account Name:	Administrator
Account Domain:	TEST
Logon ID:	0xB981B

Process Information:

New Process ID:	0x18bc
New Process Name:	C:\tools\mimikatz\x64\notepad.exe
Token Elevation Type:	TokenElevationTypeDefault (1)
Creator Process ID:	0x13fc
Process Command Line:	notepad.exe "privilege::debug" "sekurlsa::logonpasswords" "sekurlsa::tickets /export"

Dumping from LSASS memory LSASS memory access. Native Windows events

Event Properties - Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

Security ID:	TEST\Administrator
Account Name:	Administrator
Account Domain:	TEST
Logon ID:	0xB981B

Object:

Object Server:	Security
Object Type:	Process
Object Name:	\Device\HarddiskVolume2\Windows\System32\lsass.exe
Handle ID:	0x1b8
Resource Attributes:	-

Process Information:

Process ID:	0x18bc
Process Name:	C:\tools\mimikatz\x64\notepad.exe

Access Request Information:

Transaction ID:	{00000000-0000-0000-0000-000000000000}
Accesses:	Read from process memory Undefined Access (no effect) Bit 12

Access Reasons:

Access Mask:

Privileges Used for Access Check:

Restricted SID Count:



Dumping from LSASS memory LSASS memory access. Lets hunt it, using Windows events!

event_id:4656 AND event_data.ObjectName:"\|\\sass.exe" AND -event_data.AccessMask:(0x1400 0x40 0x1000 0x100000) AND -event_data.ProcessName:("\|taskmgr.exe" "\|procesp64.exe" "\|procesp.exe" "\|lsm.exe" "\|csrss.exe" "\|wininit.exe" "\|wmiprvse.exe" "\|vmtoolsd.exe")*

Time	computer_name	event_id	event_data.ProcessName	event_data.ObjectName	event_data.AccessMask
► November 8th 2017, 02:34:02.502	WIN-FJRNSLDJHD2.test.local	4,656	C:\tools\PwDump6\servpw64.exe	\Device\HarddiskVolume2\windows\System32\1sass.exe	0x1f3fff
► November 7th 2017, 20:33:01.050	WIN-FJRNSLDJHD2.test.local	4,656	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe	\Device\HarddiskVolume2\windows\System32\1sass.exe	0x143a
► November 7th 2017, 20:17:38.435	WIN-FJRNSLDJHD2.test.local	4,656	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	\Device\HarddiskVolume2\windows\System32\1sass.exe	0x143a
► November 7th 2017, 20:13:29.921	WIN-FJRNSLDJHD2.test.local	4,656	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	\Device\HarddiskVolume2\windows\System32\1sass.exe	0x143a
► November 7th 2017, 19:57:24.896	WIN-FJRNSLDJHD2.test.local	4,656	C:\tools\mimikatz\x64\notepad.exe	\Device\HarddiskVolume2\windows\System32\1sass.exe	0x1010



[Andrew Douma](#)

@securitystreak

Читать



Don't rely on the configured #SACL to detect
#malicious code trying to #exploit the
memory in #LSASS
[tyranidslair.blogspot.co.uk/2017/10/bypass ...](https://tyranidslair.blogspot.co.uk/2017/10/bypass-...)

🌐 Язык твита: английский

16:32 - 9 окт. 2017 г.



<https://tyranidslair.blogspot.ru/2017/10/bypassing-sacl-auditing-on-lsass.html>

LSASS memory access. Native Windows events. Some bad news

Dumping from LSASS memory



Event Properties - Event 8, Sysmon

General Details

Mimikatz (lsadump::lsa /inject)

CreateRemoteThread detected:

UtcTime: 2017-11-07 16:32:12.028

SourceProcessGuid: {d134eb5b-dca3-5a01-0000-00107b312e00}

SourceProcessId: 4436

SourceImage: C:\tools\mimikatz\x64\notepad.exe

TargetProcessGuid: {d134eb5b-c61e-5a01-0000-001017c80000}

TargetProcessId: 564

TargetImage: C:\Windows\System32\lsass.exe

NewThreadId: 2108

StartAddress: 0x000000FD33EF0000

StartModule:

StartFunction:

Event Properties - Event 8, Sysmon

General Details

PWDump6

CreateRemoteThread detected:

UtcTime: 2017-11-07 23:11:21.187

SourceProcessGuid: {3261c166-3d99-5a02-0000-00102ab38500}

SourceProcessId: 1512

SourceImage: C:\Windows\cioyj.exe

TargetProcessGuid: {3261c166-aed7-5a01-0000-0010e4e00000}

TargetProcessId: 496

TargetImage: C:\Windows\System32\lsass.exe

NewThreadId: 5176

StartAddress: 0x006901A0

StartModule:

StartFunction:

Dumping from LSASS memory

CreateRemoteThread into LSASS. Sysmon events

Event Properties - Event 8, Sysmon

General Details

Isadump

CreateRemoteThread detected:

UtcTime: 2017-11-08 00:11:31.632

SourceProcessGuid: {3261c166-4bb3-5a02-0000-001058239e00}

SourceProcessId: 4228

SourceImage: C:\tools\lsadump2.exe

TargetProcessGuid: {3261c166-aed7-5a01-0000-0010e4e00000}

TargetProcessId: 496

TargetImage: C:\Windows\System32\lsass.exe

NewThreadId: 4652

Event Properties - Event 8, Sysmon

General Details

Windows Credential Editor (WCE)

CreateRemoteThread detected:

UtcTime: 2017-11-08 11:07:23.654

SourceProcessGuid: {d134eb5b-e56b-5a02-0000-0010caa3d700}

SourceProcessId: 26496

SourceImage: C:\Users\ADMINI~1\AppData\Local\Temp\2\9e52cbe2-8847-44bf-8add-b0a360d3ece0.exe

TargetProcessGuid: {d134eb5b-c61e-5a01-0000-001017c80000}

TargetProcessId: 564

TargetImage: C:\Windows\System32\lsass.exe

NewThreadId: 26228

StartAddress: 0x000000FD33F2082C

StartModule:

StartFunction:



Dumping from LSASS memory CreateRemoteThread into LSASS. Lets hunt it!

source_name:"Microsoft-Windows-Sysmon" AND event_id:8 AND event_data.TargetImage:"\|lsass.exe"*

Time	computer_name	event_data.SourceImage	event_data.TargetImage	task
► November 8th 2017, 02:11:21.187	pc0002.test.local	C:\Windows\cioyj.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
► November 8th 2017, 02:06:38.996	pc0002.test.local	C:\Windows\vdcpqepjk.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
► November 8th 2017, 01:52:52.712	pc0002.test.local	C:\Windows\ueoimxq.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
► November 7th 2017, 19:32:13.035	WIN-FJRNSLDJHD2.test.local	C:\tools\mimikatz\x64\notepad.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
► November 7th 2017, 15:45:24.534	WIN-FJRNSLDJHD2.test.local	C:\Users\ADMINI~1\AppData\Local\Temp\2\g64-173.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
► November 7th 2017, 15:43:43.161	WIN-FJRNSLDJHD2.test.local	C:\Users\ADMINI~1\AppData\Local\Temp\2\servpw64.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
► November 7th 2017, 12:08:53.159	WIN-FJRNSLDJHD2.test.local	C:\Users\ADMINI~1\AppData\Local\Temp\2\60bed852-da53-4cc6-95ae-98d760245951.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
► November 6th 2017, 23:59:16.326	pc0002.test.local	C:\Users\duser\Desktop\calc86.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)

Event Properties - Event 7, Sysmon

General

Details

PWDump6 (x86)

Image loaded:

UtcTime: 2017-11-07 23:11:21.188

ProcessGuid: {3261c166-aed7-5a01-0000-0010e4e00000}

ProcessId: 496

Image: C:\Windows\System32\lsass.exe

ImageLoaded: C:\Windows\lsremora.dll

Hashes: MD5=74345E6451B830EBB144045EDAD274E1,SHA256

=AFF0FAFC63696937B4DBD2EC8DF8263F7BEBFED01567E613F869D3A9ABB47B8E

Signed: false

Signature:

SignatureStatus: Unavailable

Event Properties - Event 7, Sysmon

General

Details

PWDump6 (x64)

Image loaded:

UtcTime: 2017-11-07 23:34:02.503

ProcessGuid: {d134eb5b-c61e-5a01-0000-001017c80000}

ProcessId: 564

Image: C:\Windows\System32\lsass.exe

ImageLoaded: C:\tools\PwDump6\lsremora64.dll

Hashes: MD5=A65749EE53F55D034E8CCB057639C074,SHA256=

=533562C073AF7F052C08614FEBAD51B61A5C92EE2E842D70FF5D2E4EC964BBCB

Signed: false

Signature:

SignatureStatus: Unavailable

Dumping from LSASS memory
Unsigned image loading into LSASS. Sysmon events



Event Properties - Event 7, Sysmon

General

Details

PWDumpX

Image loaded:

UtcTime: 2017-11-07 23:48:03.967

ProcessGuid: {3261c166-aed7-5a01-0000-0010e4e00000}

ProcessId: 496

Image: C:\Windows\System32\lsass.exe

ImageLoaded: C:\Windows\System32\DumpExt.dll

Hashes: MD5=BAF49D419C56E48F35B43AB189F03AEF,SHA256

=F0C17FBB30D2FB4C02E63C857F5AF0A144CC07FBE262803247F21DFF7193FA36

Signed: false

Signature:

SignatureStatus: Unavailable



Event Properties - Event 7, Sysmon

General

Details

Windows Credential Editor (WCE)

Image loaded:

UtcTime: 2017-11-08 11:07:23.656

ProcessGuid: {d134eb5b-c61e-5a01-0000-001017c80000}

ProcessId: 564

Image: C:\Windows\System32\lsass.exe

ImageLoaded: C:\Windows\Temp\wceaux.dll

Hashes: MD5=A024AF6D8E29527A722CB5DA2F8ECE55,SHA256

=F3229244CCC349E3EC843EB6BAD547C559FE52795393E949D45170086108237B

Signed: false

Signature:

SignatureStatus: Unavailable



Dumping from LSASS memory Unsigned image loading into LSASS. Lets hunt it!

`source_name:"Microsoft-Windows-Sysmon" AND event_id:7 AND event_data.Image:"*\\"lsass.exe" AND event_data.Signed:false`

Time ▾	computer_name	event_data.Image	event_data.ImageLoaded	event_data.Signed	task
▶ November 8th 2017, 14:07:23.781	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\lsass.exe	C:\Windows\Temp\wceaux.dll	false	Image loaded (rule: ImageLoad)
▶ November 8th 2017, 14:07:23.770	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\lsass.exe	C:\Windows\Temp\wceaux.dll	false	Image loaded (rule: ImageLoad)
▶ November 8th 2017, 02:50:39.382	pc0002.test.local	C:\Windows\System32\lsass.exe	C:\Windows\System32\DumpExt.dll	false	Image loaded (rule: ImageLoad)
▶ November 8th 2017, 02:34:02.503	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\lsass.exe	C:\tools\PwDump6\lsremora64.dll	false	Image loaded (rule: ImageLoad)
▶ November 8th 2017, 02:11:21.188	pc0002.test.local	C:\Windows\System32\lsass.exe	C:\Windows\lsremora.dll	false	Image loaded (rule: ImageLoad)
▶ November 8th 2017, 02:06:38.997	pc0002.test.local	C:\Windows\System32\lsass.exe	C:\Windows\lsremora.dll	false	Image loaded (rule: ImageLoad)
▶ November 7th 2017, 15:43:43.162	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\lsass.exe	C:\Users\ADMINI~1\AppData\Local\Temp\2\lsremora64.dll	false	Image loaded (rule: ImageLoad)



Windows Server 2012 R2 and Windows 8.1 includes a new feature called [LSA Protection](#). It prevents non-protected processes from interacting with LSASS.

To allow it, set the value of the registry key RunAsPPL in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa to dword:00000001



ap @decoder_it · 13 авг.

Still using "old" Windows 2012 without Credential Guard? How about **RunAsPPL** to block credential theft?



ionstorm @ionstorm · 30 июн.

В ответ @Antonlovesdn @r0wdy_

RunAsPPL/LSASS Protection may work in preventing dumping credentials from memory, I haven't tested recently but it worked a while back

🌐 Язык твита: английский

But... Mimikatz can bypass it, using its own driver. Even more... It can unprotect any protected processes 😊

Dumping from LSASS memory
And what about LSA protection?

```
mimikatz 2.0 alpha x64 (oe.eo)

#####
## ^ ##
## { } ## /* * *
## v ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## ##### http://blog.gentilkiwi.com/mimikatz (oe.eo)
with 15 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /id:502 /inject
ERROR kuhl_m_lsadump_lsa_getHandle ; OpenProcess (0x00000005)
Domain : LAB / S-1-5-21-2929287289-1204109396-1883388597

RID : 000001f6 (502)
User : krbtgt
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003

mimikatz # !+
[*] mimikatz driver not present
[+] mimikatz driver successfully registered
[+] mimikatz driver ACL to everyone
[+] mimikatz driver started

mimikatz # !processprotect /process:lsass.exe /remove
Process : lsass.exe
PID 716 -> 00/00 [0-0-0]

mimikatz # lsadump::lsa /id:502 /inject
Domain : LAB / S-1-5-21-2929287289-1204109396-1883388597

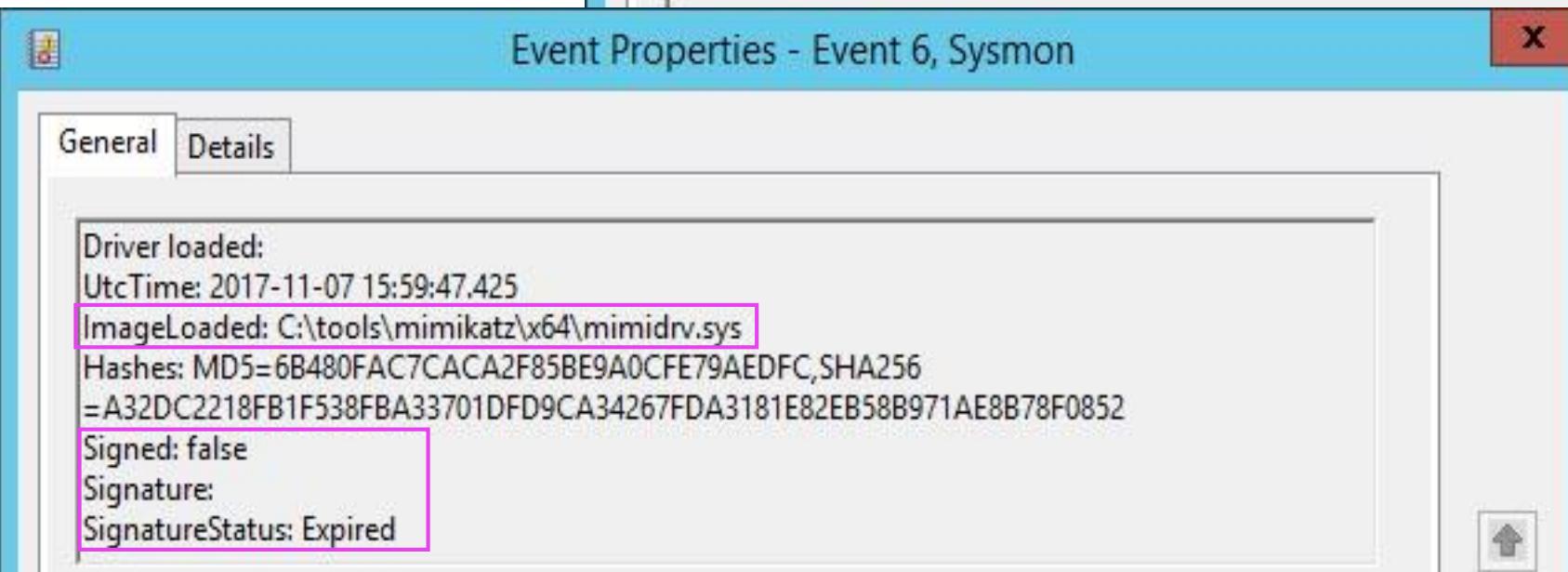
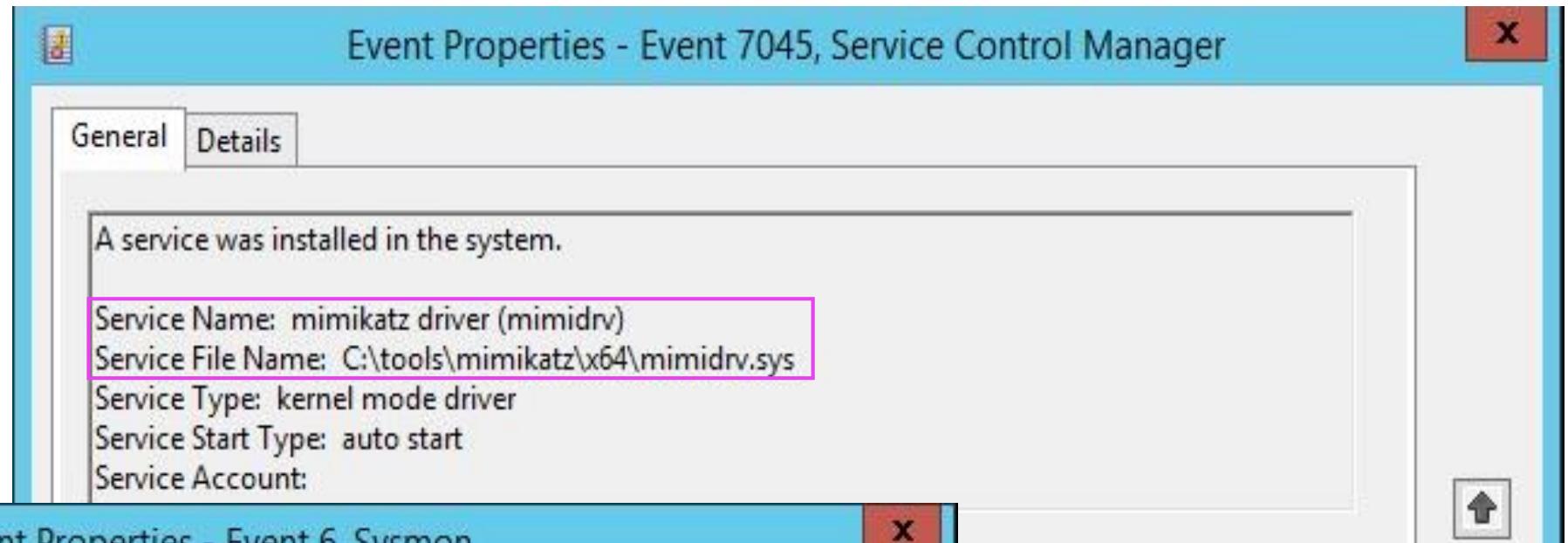
RID : 000001f6 (502)
User : krbtgt

* Primary
  LM :
  NTLM : 3f66b877d01affcc631f465e6e5ed449

* WDigest
  01 a68990164b4dfefa47c2e998f19eb74c
  02 29901e4c556d4479c71219b74712b4af
  03 b64cddb3ad03fe65bae8cdc4182ca774
  04 f68990164b4dfefa47c2e998f19eb74c
```



Dumping from LSASS memory Installation of Mimikatz driver





Dumping from LSASS memory Installation of Mimikatz driver. Lets hunt it!

*event_id:7045 AND (event_data.ServiceName:*mimidrv* OR event_data.ImagePath:*mimidrv*)*

Time ▾	computer_name	event_id	event_data.ServiceName	event_data.ImagePath	event_data.ServiceType
▶ November 7th 2017, 18:59:47.398	WIN-FJRNLSLDJHD2.test.local	7,045	mimikatz driver (mimidrv)	C:\tools\mimikatz\x64\mimidrv.sys	kernel mode driver
▶ November 7th 2017, 13:35:50.336	WIN-FJRNLSLDJHD2.test.local	7,045	mimikatz driver (mimidrv)	C:\tools\mimikatz\x64\mimidrv.sys	kernel mode driver

*event_id:6 AND source_name:"Microsoft-Windows-Sysmon" AND (event_data.ImageLoaded:*mimidrv* OR event_data.Signed:false)*

Time ▾	computer_name	event_data.ImageLoaded	event_data.SignatureStatus	event_data.Signed	task
▶ November 7th 2017, 18:59:47.430	WIN-FJRNLSLDJHD2.test.local	C:\tools\mimikatz\x64\mimidrv.sys	Expired	false	Driver loaded (rule: DriverLoad)
▶ November 7th 2017, 17:46:57.896	WIN-FJRNLSLDJHD2.test.local	C:\tools\mimikatz\x64\mimidrv.sys	Expired	false	Driver loaded (rule: DriverLoad)



Dumping from LSASS memory

Offline credentials dumping, LSASS memory dump

SqlDumper Administrator: Command Prompt

```
C:\Program Files\Microsoft SQL Server\110\Shared>tasklist | findstr lsass
lsass.exe          568 Services          0    71 064 K

C:\Program Files\Microsoft SQL Server\110\Shared>SqlDumper.exe 568 0 0x01100
Parsed parameters:
ProcessID = 568
ThreadId = 0
Flags = 0x120
MiniDumpFlags = 0x1966
SqlInfoPtr = 0x0000000000000000
DumpDir = <NULL>
ExceptionRecordPtr = 0x0000000000000000
ContextPtr = 0x0000000000000000
ExtraFile = <NULL>
InstanceName = <NULL>
ServiceName = <NULL>
Callback type 11 not used
Callback type 15 not used
Callback type 7 not used
MiniDump completed: SQLDmpr0001.mdmp
```

Task Manager

Name	PID	Status	User name	CP
LogonUI.exe	852	Runn...	SYSTEM	0
lsass.exe	568	Runn...	SYSTEM	0
Microsoft.ActiveDire...				0
mmc.exe				0
msdtc.exe				0
notepad++.exe				0
notepad.exe				0

Right-click context menu for lsass.exe:

- End task
- End process tree
- Set priority
- Set affinity
- Analyze wait chain
- UAC virtualization
- Create dump file

ProcDump Administrator: Command Prompt

```
C:\tools>procdump64.exe -ma lsass.exe

ProcDump v9.0 - Sysinternals process dump
Copyright (C) 2009-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

[03:09:55] Dump 1 initiated: C:\tools\lsass.exe_171116_030955.dmp
[03:09:55] Dump 1 writing: Estimated dump file size is 91 MB.
[03:09:55] Dump 1 complete: 91 MB written in 0.2 seconds
[03:09:55] Dump count reached.
```

Select mimikatz 2.1.1 x64 (oe.eo)

```
mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 509580 <00000000:0007c68c>
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : <null>
Logon Time        : 16.11.2017 2:52:26
SID               : S-1-5-90-2
msv :
[00000003] Primary
* Username : WIN-FJRNSLDJHD2$
* Domain  : TEST
* NTLM     : f9228579f8bdff37020d91b267f223d3e
* SHA1    : c3a1b23634d3c0d51a18299801129774282614c1
tspkg :
wdigest :
```

Extract credentials from lsass memory dump



Dumping from LSASS memory

Access LSASS memory for dump creation. Sysmon events

Event Properties - Event 10, Sysmon

General Details

Process accessed:
UtcTime: 2017-11-15 23:16:52.087
SourceProcessGUID: {d134eb5b-c7c6-5a0c-0000-0010e0831d00}
SourceProcessId: 3952
SourceThreadId: 4000
SourceImage: C:\Windows\system32\Taskmgr.exe
TargetProcessGUID: {d134eb5b-c4b0-5a0c-0000-00103fc90000}
TargetProcessId: 568
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1FFFFF
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+967da|C:\Windows\SYSTEM32\ntdll.dll+80a60|C:\Windows\system32\KERNEL32.DLL+13a57|C:\Windows\system32\KERNEL32.DLL+13b8f|C:\Windows\system32\dbghelp.dll+11d3ac|C:\Windows\system32\dbghelp.dll+11b1c5|C:\Windows\system32\dbghelp.dll+3791d|C:\Windows\system32\dbghelp.dll+3d37a|C:\Windows\system32\dbghelp.dll+34aaa|C:\Windows\system32\Taskmgr.exe+98ed5|C:\Windows\system32\KERNEL32.DLL+15bd|C:\Windows\SYSTEM32\ntdll.dll+743d1

Event Properties - Event 10,

General Details

Process accessed:
UtcTime: 2017-11-15 23:15:03.096
SourceProcessGUID: {d134eb5b-ca77-5a0c-0000-0010faf92800}
SourceProcessId: 732
SourceThreadId: 2068
SourceImage: C:\tools\procdump64.exe
TargetProcessGUID: {d134eb5b-c4b0-5a0c-0000-00103fc90000}
TargetProcessId: 568
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1FFFFF
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+967da|C:\Windows\SYSTEM32\ntdll.dll+80a60|C:\Windows\system32\KERNEL32.DLL+13a57|C:\Windows\system32\KERNEL32.DLL+13b8f|C:\Windows\SYSTEM32\dbghelp.dll+11d3ac|C:\Windows\SYSTEM32\dbghelp.dll+11b1c5|C:\Windows\SYSTEM32\dbghelp.dll+3791d|C:\Windows\SYSTEM32\dbghelp.dll+3d37a|C:\Windows\SYSTEM32\dbghelp.dll+34aaa|C:\Windows\tools\procdump64.exe+12b40|C:\Windows\tools\procdump64.exe+12575|C:\Windows\tools\procdump64.exe+12495|C:\Windows\tools\procdump64.exe+12149|C:\Windows\system32\KERNEL32.DLL+15bd|C:\Windows\SYSTEM32\ntdll.dll+743d1



Dumping from LSASS memory Access LSASS memory for dump creation. Lets hunt it

*source_name:"Microsoft-Windows-Sysmon" AND event_id:10 AND
event_data.TargetImage:"*\lsass.exe" AND event_data.CallTrace:*dbghelp**

Time ▾	computer_name	event_data.SourceImage	event_data.TargetImage	event_data.CallTrace
November 16th 2017, 03:00:57.844	WIN-FJRNSLDJHD2.test.local	C:\Program Files\Microsoft SQL Server\110\Shared\SqlDumper.exe	C:\Windows\system32\lsass.exe	C:\Windows\SYSTEM32\ntdll.dll+967da C:\Windows\SYSTEM32\ntdll.dll+80a60 C:\Windows\system32\KERNEL32.DLL+13a57 C:\Windows\system32\KERNEL32.DLL+13b8f C:\Program Files\Microsoft SQL Server\110\Shared\dbghelp.dll+82630 C:\Program Files\Microsoft SQL Server\110\Shared\dbghelp.dll+85773 C:\Program Files\Microsoft SQL Server\110\Shared\dbghelp.dll+7e2ac C:\Program Files\Microsoft SQL Server\110\Shared\dbghelp.dll+76d51 C:\Program Files\Microsoft SQL Server\110\Shared\dbghelp.dll+774dd C:\Program Files\Microsoft SQL Server\110\Shared\SqlDumper.exe+bf20 C:\Program Files\Microsoft SQL Server\110\Shared\SqlDumper.exe+8f65 C:\Program Files\Microsoft SQL Server\110\Shared\SqlDumper.exe+1040b C:\Program Files\Microsoft SQL Server\110\Shared\SqlDumper.exe+10652 C:\Program Files\Microsoft SQL
November 16th 2017, 02:38:16.371	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\system32\lsass.exe	C:\Windows\SYSTEM32\ntdll.dll+967da C:\Windows\SYSTEM32\ntdll.dll+80a60 C:\Windows\system32\KERNEL32.DLL+13a57 C:\Windows\system32\KERNEL32.DLL+13b8f C:\Windows\SYSTEM32\BgHelp.dll+11d3ac C:\Windows\SYSTEM32\BgHelp.dll+11b1c5 C:\Windows\SYSTEM32\BgHelp.dll+3791d C:\Windows\SYSTEM32\BgHelp.dll+3d37a C:\Windows\SYSTEM32\BgHelp.dll+34aaa C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\e22255eb455ea82b67a64858c9c590d1\System.Management.Automation.ni.dll+7cb70cf8(wow64) C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll+124113 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll+123fde C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll+8ee66 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll+8eba6 C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\f9f73f178cc2e4493598ee1bd411c3e8\mscorlib.ni.dll+486bac C:\Windows\assembly\NativeImages_v4.0.30319_64\msc
November 16th 2017, 02:16:52.088	WIN-FJRNSLDJHD2.test.local	C:\Windows\system32\Taskmgr.exe	C:\Windows\system32\lsass.exe	C:\Windows\SYSTEM32\ntdll.dll+967da C:\Windows\SYSTEM32\ntdll.dll+80a60 C:\Windows\system32\KERNEL32.DLL+13a57 C:\Windows\system32\KERNEL32.DLL+13b8f C:\Windows\system32\dbghelp.dll+11d3ac C:\Windows\SYSTEM32\dbghelp.dll+11b1c5 C:\Windows\SYSTEM32\dbghelp.dll+3791d C:\Windows\SYSTEM32\dbghelp.dll+3d37a C:\Windows\SYSTEM32\dbghelp.dll+34aaa C:\Windows\SYSTEM32\Taskmgr.exe+98ed5 C:\Windows\SYSTEM32\KERNEL32.DLL+15bd C:\Windows\SYSTEM32\ntdll.dll+743d1
November 16th 2017, 02:15:03.096	WIN-FJRNSLDJHD2.test.local	C:\tools\procdump64.exe	C:\Windows\system32\lsass.exe	C:\Windows\SYSTEM32\ntdll.dll+967da C:\Windows\SYSTEM32\ntdll.dll+80a60 C:\Windows\system32\KERNEL32.DLL+13a57 C:\Windows\system32\KERNEL32.DLL+13b8f C:\Windows\SYSTEM32\dbghelp.dll+11d3ac C:\Windows\SYSTEM32\dbghelp.dll+11b1c5 C:\Windows\SYSTEM32\dbghelp.dll+3791d C:\Windows\SYSTEM32\dbghelp.dll+3d37a C:\Windows\SYSTEM32\dbghelp.dll+34aaa C:\tools\procdump64.exe+12b40 C:\tools\procdump64.exe+12575 C:\tools\procdump64.exe+12495 C:\tools\procdump64.exe+12149 C:\Windows\SYSTEM32\KERNEL32.DLL+15bd C:\Windows\SYSTEM32\ntdll.dll+743d1



Dumping from LSASS memory LSASS memory dump file creation. Sysmon events

Event Properties - Event 11, Sysmon

General Details Procdump create lsass memory dump file

File created:
UtcTime: 2017-11-15 23:15:03.082
ProcessGuid: {d134eb5b-ca77-5a0c-0000-0010faf92800}
ProcessId: 732
Image: C:\tools\procdump64.exe
TargetFilename: C:\tools\lsass.exe_171116_031503.dmp
CreationUtcTime: 2017-11-15 23:15:03.082

Event Properties - Event 11, Sysmon

General Details Powershell create lsass memory dump file

File created:
UtcTime: 2017-11-15 23:38:16.223
ProcessGuid: {d134eb5b-cf75-5a0c-0000-0010972a3f00}
ProcessId: 4940
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\temp\lsass_568.dmp
CreationUtcTime: 2017-11-15 23:38:16.223

Event Properties - Event 11, Sysmon

General Details Taskmgr create lsass memory dump file

File created:
UtcTime: 2017-11-15 23:16:52.085
ProcessGuid: {d134eb5b-c7c6-5a0c-0000-0010e0831d00}
ProcessId: 3952
Image: C:\Windows\system32\Taskmgr.exe
TargetFilename: C:\Users\ADMINI~1\AppData\Local\Temp\2\lsass (2).DMP
CreationUtcTime: 2017-11-15 23:16:52.085

Event Properties - Event 11, Sysmon

General Details Sqldumper create lsass memory dump file

File created:
UtcTime: 2017-11-16 00:07:44.486
ProcessGuid: {d134eb5b-d6d0-5a0c-0000-0010cf536800}
ProcessId: 7424
Image: C:\Program Files\Microsoft SQL Server\110\Shared\SqlDumper.exe
TargetFilename: C:\Program Files\Microsoft SQL Server\110\Shared\SQLDmpr0001.mdmp
CreationUtcTime: 2017-11-16 00:00:57.837



Dumping from LSASS memory LSASS memory dump file creation. Lets hunt it

*source_name:"Microsoft-Windows-Sysmon" AND event_id:11 AND event_data.TargetFilename:/*lsass* AND event_data.TargetFilename:/*dmp*

Time	computer_name	event_data.Image	event_data.TargetFilename	task
► November 16th 2017, 02:38:16.223	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\temp\lsass_568.dmp	File created (rule: FileCreate)
► November 16th 2017, 02:33:16.513	WIN-FJRNSLDJHD2.test.local	C:\Windows\Explorer.EXE	C:\tmp\lsass.exe_171116_031233.dmp	File created (rule: FileCreate)
► November 16th 2017, 02:16:52.085	WIN-FJRNSLDJHD2.test.local	C:\Windows\system32\Taskmgr.exe	C:\Users\ADMINI~1\AppData\Local\Temp\2\lsass (2).DMP	File created (rule: FileCreate)
► November 16th 2017, 02:15:03.082	WIN-FJRNSLDJHD2.test.local	C:\tools\procdump64.exe	C:\tools\lsass.exe_171116_031503.dmp	File created (rule: FileCreate)
► November 16th 2017, 02:14:16.989	WIN-FJRNSLDJHD2.test.local	C:\tools\procdump64.exe	C:\tools\lsass.exe_171116_031416.dmp	File created (rule: FileCreate)
► November 16th 2017, 02:12:33.905	WIN-FJRNSLDJHD2.test.local	C:\tools\procdump64.exe	C:\tools\lsass.exe_171116_031233.dmp	File created (rule: FileCreate)

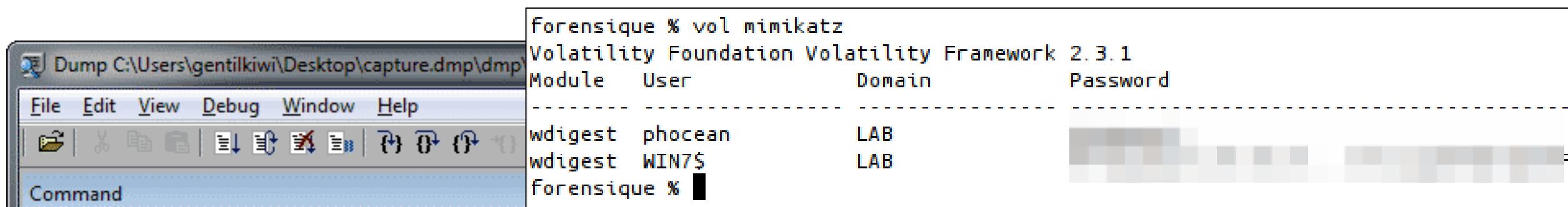


Dumping from LSASS memory Offline credentials dumping. Other sources of LSASS memory

It is also possible to extract credentials from other sources, containing lsass memory:

- Virtual machines memory files (.vmem...);
- Hibernation files (hiberfil.sys) ;
- Crashdumps (.dmp, C:\Windows\Minidump).

Tools: Mimkatz WinDbg extension, Volatility Mimikatz plugin



A screenshot of the Volatility Foundation Volatility Framework 2.3.1 interface. The title bar says "Dump C:\Users\gentilkiwi\Desktop\capture.dmp\dump". The menu bar includes File, Edit, View, Debug, Window, Help. The toolbar has icons for file operations. The main window shows a table of extracted credentials:

Module	User	Domain	Password
wdigest	phocean	LAB	[REDACTED]
wdigest	WIN7\$	LAB	[REDACTED]

The command line at the bottom shows:

```
forensique % vol mimikatz
Volatility Foundation Volatility Framework 2.3.1
Module      User          Domain      Password
-----
wdigest    phocean        LAB
wdigest    WIN7$          LAB
forensique %
```

Below the command line, the output of the .load command is shown:

```
0: kd> .load c:\security\mimikatz\x64\mimilib.dll

#####
# mimikatz 2.0 alpha (x64) release "Kiwi en C" (Nov 24 2013)
## ^ ##
## / \ ## Windows build 7601
## \ / ## /* * *
## v ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## #### http://blog.gentilkiwi.com/mimikatz
##### WinDBG extension ! * * */
```



Dumping from LSASS memory

Offline credentials dumping. Other sources of LSASS memory

Event Properties - Event 5145, Microsoft Windows security auditing.

General Details

A network share object was checked to see whether client can be granted

Subject:

Security ID:	TEST\dadmin
Account Name:	dadmin
Account Domain:	TEST
Logon ID:	0x5E2317

Network Information:

Object Type:	File
Source Address:	172.16.205.151
Source Port:	54700

Share Information:

Share Name:	\?\?\\CS
Share Path:	\??\C:\
Relative Target Name:	tmp\lsass.exe_171116_031233.dmp

Access Request Information:

Access Mask:	0x120089
Accesses:	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes

Event Properties - Event 5145, Microsoft Windows security auditing.

General Details

A network share object was checked to see whether client can be granted

Subject:

Security ID:	TEST\dadmin
Account Name:	dadmin
Account Domain:	TEST
Logon ID:	0x5D14EA

Network Information:

Object Type:	File
Source Address:	172.16.205.151
Source Port:	54697

Share Information:

Share Name:	\?\?\\CS
Share Path:	\??\C:\
Relative Target Name:	tmp\lsass.exe_171116_031233.dmp

Access Request Information:

Access Mask:	0x120089
Accesses:	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes

Event Properties - Event 5145, Microsoft Windows security auditing.

General Details

A network share object was checked to see whether client can be granted

Subject:

Security ID:	TEST\dadmin
Account Name:	dadmin
Account Domain:	TEST
Logon ID:	0x5D14EA

Network Information:

Object Type:	File
Source Address:	172.16.205.151
Source Port:	54697

Share Information:

Share Name:	\?\?\\CS
Share Path:	\??\C:\
Relative Target Name:	tmp\ntds.dit

Access Request Information:

Access Mask:	0x120089
Accesses:	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes



Dumping from LSASS memory Offline credentials dumping. Other sources of LSASS memory. Copying hiberfil/crashdumps via admin shares

*event_id:5145 AND event_data.RelativeTargetName:(*lsass* "*\\windows\\minidump*"
hiberfil *sqlldmpr* "*\\sam*" "*\\ntds.dit" "*\\security*")*

Time ▾	computer_name	event_id	event_data.SubjectUserName	event_data.ipAddress	event_data.ShareName	event_data.RelativeTargetName
▶ November 16th 2017, 03:29:32.026	WIN-FJRNSLDJHD2.test.local	5,145	dadmin	172.16.205.151	\\\c\$	Program Files\Microsoft SQL Server\110\shared\SQLDmpr0001.mdmp
▶ November 16th 2017, 02:52:51.224	WIN-FJRNSLDJHD2.test.local	5,145	dadmin	172.16.205.151	\\\c\$	hiberfil.sys
▶ November 16th 2017, 02:51:58.933	WIN-FJRNSLDJHD2.test.local	5,145	dadmin	172.16.205.151	\\\c\$	tmp\sam
▶ November 16th 2017, 02:51:40.990	WIN-FJRNSLDJHD2.test.local	5,145	dadmin	172.16.205.151	\\\c\$	tmp\lsass.exe_171116_031233.dmp
▶ November 16th 2017, 02:50:50.609	WIN-FJRNSLDJHD2.test.local	5,145	dadmin	172.16.205.151	\\\c\$	tmp\ntds.dit



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit

Offline – grab SAM/SYSTEM/SECURITY/NTDS.dit from compromised host and process it using special tools. Online – run special tool directly on compromised host (this tool will do all necessary work itself)

```
root@bt: /tmp/NTDS_Grab/192.168.1.6
root@bt: /tmp/NTDS_Grab/192.168.1.6# /root/libesedb-20120102/esedbtools/esedbexport ntds
esedbexport 20120102

Opening file.
Exporting table 1 (MSysObjects) out of 12.
Exporting table 2 (MSysObjectsShadow) out of 12.
Exporting table 3 (MSysUnicodeFixupVer2) out of 12.
Exporting table 4 (datatable) out of 12.
Exporting table 5 (hiddentable) out of 12.
Exporting table 6 (link_table) out of 12.
Exporting table 7 (sdpropcounttable) out of 12.
Exporting table 8 (sdproptable) out of 12.
Exporting table 9 (sd_table) out of 12.
Exporting table 10 (MSysDefrag2) out of 12.
Exporting table 11 (quota_table) out of 12.
Exporting table 12 (quota_rebuild_progress_table) out of 12.
Export completed.
root@bt: /tmp/NTDS_Grab/192.168.1.6#
root@bt: /tmp/NTDS_Grab/192.168.1.6# cp ntds.export datatable.3 .
root@bt: /tmp/NTDS_Grab/192.168.1.6# ls
datatable.3 ntds ntds.export sys
root@bt: /tmp/NTDS_Grab/192.168.1.6# /root/metasploit-framework/tools/ntds_hashextract.rb datatable.3 sys
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ac17de104974106a9d19f1a4b3bdceda:::
GOKU$:1000:aad3b435b51404eeaad3b435b51404ee:cfca51f4ca7427bad413ed3ed953c4d3:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7b98b255704ae844d381aefee512db12:::
VAGETAS$:1103:aad3b435b51404eeaad3b435b51404ee:dc94901e2578c901164d41a6eb67593b:::
serveradmin:1104:aad3b435b51404eeaad3b435b51404ee:5b62f9c785dffed9cb81d89df178c837:::
LA-DD980389EF4B$:1105:aad3b435b51404eeaad3b435b51404ee:afe964446fda9cd6a3891db82597dc9c:::
TRUNKS$:1106:aad3b435b51404eeaad3b435b51404ee:83683d96fca79dc0ada0c4f19d18e89f:::
root@bt: /tmp/NTDS_Grab/192.168.1.6# $ secretsdump.py -sam sam.save -security security.save -system system.save LOCAL
Impacket v0.9.11-dev - Copyright 2002-2013 Core Security Technologies

[*] Target system bootKey: 0x602e8c2947d56a95bf9cfad9e0bbbace
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
renadm:500:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
support:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
hdes:6ec74661650377df488415415bf10321:securus.corp.com:SECURUS:::
Administrator:c4a850e0fee5af324a57fd2eeb8dbd24:SECURUS.CORP.COM:SECURUS:::
[*] Dumping LSA Secrets
```



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via direct access to logical volume

Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools.

Tools: Pwdump7, Invoke-NinjaCopy, Samex

```

Administrator: Windows PowerShell
PS C:\Tools\PowerSploit\Exfiltration> Invoke-NinjaCopy -Path C:\Windows\NTDS\ntds.dit -LocalDestination C:\temp\ntds.dit
VERBOSE: PowerShell ProcessID: 6644
VERBOSE: Calling Invoke-MemoryLoadLibrary
VERBOSE: Getting basic PE information from the file
Specified cast is not valid.
At C:\Tools\PowerSploit\Exfiltration\Invoke-NinjaCopy.ps1:2208 char:7
+     if ((\$PEInfo.DllCharacteristics -band $Win32Constants.IMAGE_D ...
+         + CategoryInfo : OperationStopped: () [], InvalidCastException
+         + FullyQualifiedErrorId : System.InvalidCastException

VERBOSE: Allocating memory for the PE and write its headers to memory
Specified cast is not valid.
At C:\Tools\PowerSploit\Exfiltration\Invoke-NinjaCopy.ps1:2266 char:7
+     if ((\$PEInfo.DllCharacteristics -band $Win32Constants.IMAGE_D ...
+         + CategoryInfo : OperationStopped: () [], InvalidCastException
+         + FullyQualifiedErrorId : System.InvalidCastException

VERBOSE: Getting detailed PE information from the headers loaded in memory
VERBOSE: StartAddress: 726277423104 EndAddress: 72627574656
VERBOSE: Copy PE sections in to memory
VERBOSE: Update memory addresses based on where the PE was actually loaded in memory
VERBOSE: Import DLL's needed by the PE we are loading
VERBOSE: Done importing DLL imports
VERBOSE: Update memory protection flags
VERBOSE: Calling dllmain so the DLL knows it has been loaded
VERBOSE: Calling StealthReadFile in DLL
VERBOSE: Read 5242880 bytes. 15745024 bytes remaining.
VERBOSE: Read 5242880 bytes. 10502144 bytes remaining.
VERBOSE: Read 5242880 bytes. 5259264 bytes remaining.
VERBOSE: Read 5242880 bytes. 16384 bytes remaining.
VERBOSE: Read 16384 bytes. 0 bytes remaining.
VERBOSE: Done unloading the libraries needed by the PE
VERBOSE: Calling dllmain so the DLL knows it is being unloaded
VERBOSE: Done!

```

```

Administrator: Command Prompt
C:\>tools>samex.exe ntds
SAMEx - yakovdk@gmail.com - (C) June 2012
(This software comes with NO WARRANTY; your mileage may vary)

["windows", "ntds", "ntds.dit"]
Found ["\\\""]
Found [ "\\\", "windows" ]
Found [ "\\\", "windows", "ntds", "ntds.dit" ]
Found ntds.dit

Exporting Windows\NTDS\NTDS.dit to 'NTDS.out'...
::NTFSFile::
MFT#: 435
Parent: 407
Filename: ntds.dit
Filesize: 20987904 bytes
Sectors: <1089512,31904>
<8409664,896>
<1672336,8192>

```

File System Logical Offsets	
Technique	
ID	T1006
Tactic	Defense Evasion
Platform	Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10
Permissions	Administrator
Required	
Data	API monitoring
Sources	
Defense	File monitoring,
Bypassed	File system access controls



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit
Grabbing via direct access to logical volume. Sysmon events.

Event Properties - Event 9, Sysmon

General Details **Invoke-NinjaCopy (local)**

RawAccessRead detected:
UtcTime: 2017-11-07 12:09:46.355
ProcessGuid: {d134eb5b-a196-5a01-0000-00109c13e500}
ProcessId: 6644
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Device: \Device\HarddiskVolume2

Event Properties - Event 9, Sysmon

General Details **Invoke-NinjaCopy (remote)**

RawAccessRead detected:
UtcTime: 2017-11-07 12:14:13.387
ProcessGuid: {d134eb5b-a38f-5a01-0000-001056c5e700}
ProcessId: 7208
Image: C:\Windows\System32\wsmprovhost.exe
Device: \Device\HarddiskVolume2

Event Properties - Event 9, Sysmon

General Details **PwDump7**

RawAccessRead detected:
UtcTime: 2017-11-07 11:20:34.796
ProcessGuid: {d134eb5b-9701-5a01-0000-00103041d200}
ProcessId: 1724
Image: C:\tools\pwdump7\PwDump7.exe
Device: \Device\HarddiskVolume2

Event Properties - Event 9, Sysmon

General Details **Samex**

RawAccessRead detected:
UtcTime: 2017-11-07 11:35:12.280
ProcessGuid: {d134eb5b-9a70-5a01-0000-001007a2db00}
ProcessId: 5900
Image: C:\tools\samex.exe
Device: \Device\HarddiskVolume2



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via direct access to logical volume. Lets hunt it!

```
source_name:"Microsoft-Windows-Sysmon" AND -event_data.Device:*Floppy* AND
event_id:9 -event_data.Image:(*\\WmiPrvSE.exe" "*\\sdiagnhost.exe"
"*\\SearchIndexer.exe" "*\\csrss.exe" "*\\Defrag.exe" "*\\smss.exe" "System"
"*\\VSSVC.exe" "*\\CompatTelRunner.exe" "*\\wininit.exe" "*\\autochk.exe"
"*\\taskhost.exe" "*\\dfsrs.exe" "*\\vds.exe" "*\\lsass.exe")
```

Time ▾	computer_name	event_data.Image	event_data.Device	task
▶ November 7th 2017, 15:14:00.868	WIN-FJRNSLDJHD2.test.local	C:\\Windows\\System32\\wsmprovhost.exe	\\Device\\HarddiskVolume2	RawAccessRead detected (rule: RawAccessRead)
▶ November 7th 2017, 15:13:55.259	WIN-FJRNSLDJHD2.test.local	C:\\Windows\\System32\\wsmprovhost.exe	\\Device\\HarddiskVolume2	RawAccessRead detected (rule: RawAccessRead)
▶ November 7th 2017, 15:09:46.355	WIN-FJRNSLDJHD2.test.local	C:\\Windows\\System32\\windowsPowerShell\\v1.0\\powershell.exe	\\Device\\HarddiskVolume2	RawAccessRead detected (rule: RawAccessRead)
▶ November 7th 2017, 15:07:46.053	WIN-FJRNSLDJHD2.test.local	C:\\Windows\\System32\\windowsPowerShell\\v1.0\\powershell.exe	\\Device\\HarddiskVolume2	RawAccessRead detected (rule: RawAccessRead)
▶ November 7th 2017, 14:50:23.306	WIN-FJRNSLDJHD2.test.local	C:\\tools\\pwdump7\\PwDump7.exe	\\Device\\HarddiskVolume2	RawAccessRead detected (rule: RawAccessRead)
▶ November 7th 2017, 14:40:59.710	WIN-FJRNSLDJHD2.test.local	C:\\tools\\samex.exe	\\Device\\HarddiskVolume2	RawAccessRead detected (rule: RawAccessRead)



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via shadow copies. VSSAdmin

Shadow Copy (also known as Volume Snapshot Service, Volume Shadow Copy Service or VSS) is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of computer files or volumes, **even when they are in use**. So, it can be used to grab SAM/SECURITY/NTDS.dit files.

```
C:\Windows\system32>vssadmin create shadow /for=C:  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
(C) Copyright 2001-2005 Microsoft Corp.
```

```
Successfully created shadow copy for 'C:'  
Shadow Copy ID: {679a27e9-f53d-43e3-b5c9-6f75ce1d937c}  
Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8
```

```
C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows  
\ntds\ntds.dit c:\Extract\ntds.dit  
1 file(s) copied.
```

```
C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\window  
\system32\config\SYSTEM c:\Extract\SYSTEM  
1 file(s) copied.
```



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via shadow copies. VSSAdmin. Lets hunt it!

*source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND *vssadmin* AND event_data.Image:"*\vssadmin.exe" AND event_data.CommandLine:*shadow* AND event_data.CommandLine:(*list* *create* *delete*)*

Time	computer_name	event_data.ParentImage	event_data.User	event_data.CommandLine	task
▶ November 9th 2017, 15:15:31.149	WIN-FJRNSDLJHD2.test.local	C:\Windows\System32\cmd.exe	TEST\Administrator	vssadmin list shadows	Process Create (rule: ProcessCreate)
▶ November 9th 2017, 15:15:56.355	WIN-FJRNSDLJHD2.test.local	C:\Windows\System32\cmd.exe	TEST\Administrator	vssadmin create shadow /for=C:	Process Create (rule: ProcessCreate)

*event_id:466 AND *vssadmin* AND event_data.NewProcessName:"*\vssadmin.exe" AND event_data.CommandLine:*shadow* AND event_data.CommandLine:(*list* *create* *delete*)*

Time	computer_name	event_data.SubjectUserName	event_data.SubjectDomainName	event_data.NewProcessName	event_data.CommandLine	event_id
▶ November 9th 2017, 15:15:31.143	WIN-FJRNSDLJHD2.test.local	Administrator	TEST	C:\Windows\System32\vssadmin.exe	vssadmin list shadows	4,688
▶ November 9th 2017, 15:15:56.354	WIN-FJRNSDLJHD2.test.local	Administrator	TEST	C:\Windows\System32\vssadmin.exe	vssadmin create shadow /for=C:	4,688



Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Services (AD LDS). It can be used to create backup of NTDS database, using shadow copies mechanism.

Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via shadow copies. ntdsutil



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit
Grabbing via shadow copies. ntdsutil. Lets hunt it!

event_id:4688 AND event_data.NewProcessName:"\\"ntdsutil.exe" AND event_data.CommandLine:*ntds* AND event_data.CommandLine:*create* AND event_data.CommandLine:*full**

Time ▾	computer_name	event_id	event_data.NewProcessName	event_data.CommandLine
▶ November 9th 2017, 15:11:27.733	WIN-FJRNSDLJHD2.test.local	4,688	C:\Windows\System32\ntdsutil.exe	ntdsutil "ac i ntds" "i" "create full C:\temp" q q

source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.Image:"\\"ntdsutil.exe" AND event_data.CommandLine:*ntds* AND event_data.CommandLine:*create* AND event_data.CommandLine:*full**

Time ▾	computer_name	event_data.User	event_data.ParentImage	event_data.CommandLine	task
▶ November 9th 2017, 15:11:27.734	WIN-FJRNSDLJHD2.test.local	TEST\Administrator	C:\Windows\System32\cmd.exe	ntdsutil "ac i ntds" "i" "create full C:\temp" q q	Process Create (rule: ProcessCreate)



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via shadow copies. WMI. Lets hunt it!

Administrator: Command Prompt

```
C:\windows\system32>powershell.exe -Command (gwmi -list win32_shadowcopy).Create('C:\','ClientAccessible')
```

```
GENUS          : 2
CLASS          : __PARAMETERS
SUPERCLASS     :
DYNASTY        : __PARAMETERS
RELPATH        :
PROPERTY_COUNT : 2
DERIVATION     : {}
SERVER         :
NAMESPACE      :
PATH           :
ReturnValue    : 0
ShadowID       : {BBBED259-36EB-43BC-A952-BC5F8F6E7264}
PSComputerName :
```

WMI can also be used for shadow copies creation. This operation can be done using wmic, powershell or programmatically via COM

Administrator: Command Prompt

```
C:\windows\system32>wmic shadowcopy call create Volume='C:\'
Executing (Win32_ShadowCopy)->create()
Method execution successful.
```

```
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
    ShadowID = "{12A89EC1-71FC-4C64-BB8D-929B76CC6020}";
};
```



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via shadow copies. WMI. Lets hunt it!

`source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.Image:(/*\\powershell.exe
/*\\wmic.exe") AND event_data.CommandLine:(*shadowcopy*) AND event_data.CommandLine:(*create*)`

Time	computer_name	event_data.User	event_data.Image	event_data.CommandLine	task
▶ November 16th 2017, 01:57:53.222	WIN-FJRNSLDJHD2.test.local	TEST\Administrator	C:\Windows\System32\wbem\WMIC.exe	wmic shadowcopy call create volume='C:'\'	Process Create (rule: ProcessCreate)
▶ November 16th 2017, 01:57:34.637	WIN-FJRNSLDJHD2.test.local	TEST\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -Command (gwmi -list Win32_ShadowCopy).Create('C:\','ClientAccessible')	Process Create (rule: ProcessCreate)

`event_id:4688 AND event_data.NewProcessName:(/*\\powershell.exe /*\\wmic.exe) AND event_data.CommandLine:(*shadowcopy*) AND event_data.CommandLine:(*create*)`

Time	computer_name	event_id	event_data.SubjectUserName	event_data.SubjectDomainName	event_data.NewProcessName	event_data.CommandLine
▶ November 16th 2017, 01:57:53.221	WIN-FJRNSLDJHD2.test.local	4,688	Administrator	TEST	C:\Windows\System32\wbem\WMIC.exe	wmic shadowcopy call create volume='C:'\'
▶ November 16th 2017, 01:57:34.636	WIN-FJRNSLDJHD2.test.local	4,688	Administrator	TEST	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -Command (gwmi -list Win32_ShadowCopy).Create('C:\','ClientAccessible')



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Shadow copies. Copying SAM/SECURITY/NTDS.dit files. Lets hunt it!

source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.CommandLine:("\\windows\\ntds\\ntds.dit" "*\\system32\\config\\sam" "*\\system32\\config\\security" "*\\system32\\config\\system")*

Time	computer_name	event_data.User	event_data.ParentImage	event_data.CommandLine	event_id
► November 9th 2017, 15:23:23.017	WIN-FJRNSLDJHD2.test.local	TEST\Administrator	C:\Windows\System32\cmd.exe	cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\NTDS\ntds.dit C:\tmp\ntdsdit	1
► November 9th 2017, 15:23:23.003	WIN-FJRNSLDJHD2.test.local	TEST\Administrator	C:\Windows\System32\cmd.exe	cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SECURITY C:\tmp\security	1
► November 9th 2017, 15:23:22.989	WIN-FJRNSLDJHD2.test.local	TEST\Administrator	C:\Windows\System32\cmd.exe	cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SAM C:\tmp\sam	1
► November 9th 2017, 15:23:22.962	WIN-FJRNSLDJHD2.test.local	TEST\Administrator	C:\Windows\System32\cmd.exe	cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SYSTEM C:\tmp\system	1

event_id:4688 AND event_data.CommandLine:("\\windows\\ntds\\ntds.dit" "*\\system32\\config\\sam" "*\\system32\\config\\security" "*\\system32\\config\\system")*

Time	computer_name	event_data.NewProcessName	event_data.CommandLine	event_id
► November 9th 2017, 15:23:23.017	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\cmd.exe	cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\NTDS\ntds.dit C:\tmp\ntdsdit	4,688
► November 9th 2017, 15:23:23.002	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\cmd.exe	cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SECURITY C:\tmp\security	4,688
► November 9th 2017, 15:23:22.988	WIN-	C:\Windows\System32\cmd.exe	cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\System32\config\SAM	4,688



Dumping from SAM/SYSTEM/SECURITY/NTDS.dit
Shadow copies. Create symlink to shadow copies storage. Lets hunt it!

*source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.CommandLine:*mklink* AND event_data.CommandLine:*HarddiskVolumeShadowCopy**

Time	computer_name	event_data.User	event_data.Image	event_data.CommandLine	task
► November 9th 2017, 15:29:47.360	WIN-FJRNSDLJHD2.test.local	TEST\Administrator	C:\Windows\System32\cmd.exe	"C:\Windows\System32\cmd.exe" /c mklink /D C:\tmp\vssstore \\\? \GLOBALROOT\Device\HarddiskVolumeShadowCopy4\	Process Create (rule: ProcessCreate)

*event_id:4688 AND event_data.CommandLine:*mklink* AND event_data.CommandLine:*HarddiskVolumeShadowCopy**

Time	computer_name	event_data.NewProcessName	event_data.CommandLine	event_id
► November 9th 2017, 15:29:47.358	WIN-FJRNSDLJHD2.test.local	C:\Windows\System32\cmd.exe	"C:\Windows\System32\cmd.exe" /c mklink /D C:\tmp\vssstore \\\? \GLOBALROOT\Device\HarddiskVolumeShadowCopy4\	4,688



Select Administrator: Command Prompt

```
C:\temp>reg save hklm\sam sam
The operation completed successfully.

C:\temp>reg save hklm\security security
The operation completed successfully.

C:\temp>reg save hklm\system system
The operation completed successfully.

C:\temp>reg save \\172.16.205.151\hklm\sam 172.16.205.151-sam
The operation completed successfully.

C:\temp>reg save \\172.16.205.151\hklm\security 172.16.205.151-security
The operation completed successfully.

C:\temp>reg save \\172.16.205.151\hklm\system 172.16.205.151-system
The operation completed successfully.
```

Dumping from SAM/SYSTEM/SECURITY
Grabbing via registry. Using reg tool

Event Properties - Event 1, Sysmon

General Details

Process Create:
UtcTime: 2017-11-16 01:14:25.899
ProcessGuid: {d134eb5b-e671-5a0c-0000-00103f108b00}
ProcessId: 9084
Image: C:\Windows\System32\reg.exe
CommandLine: reg save \\172.16.205.151\hklm\sam 172.16.205.151-sam
CurrentDirectory: C:\temp\
User: TEST\Administrator
LogonGuid: {d134eb5b-c52a-5a0c-0000-0020b7fa0700}
LogonId: 0x7FAB7

Event Properties - Event 4688, Microsoft Windows security

General Details

A new process has been created.

Subject:

Security ID:	TEST\Administrator
Account Name:	Administrator
Account Domain:	TEST
Logon ID:	0xB981B

Process Information:

New Process ID:	0x2784
New Process Name:	C:\Windows\System32\reg.exe
Token Elevation Type:	TokenElevationTypeDefault (1)
Creator Process ID:	0x120c
Process Command Line:	reg save hklm\sam sam.hive



Dumping from SAM/SYSTEM/SECURITY

Grabbing via registry. Using reg tool. Lets hunt it!

`event_id:1 AND event_data(CommandLine:/*reg* AND event_data(CommandLine:/*save* AND event_data(CommandLine:(("hklm\\sam" "hklm\\system" "hklm\\security" "hkey_local_machine\\sam" "hkey_local_machine\\system" "hkey_local_machine\\security"))`

Time ▾	computer_name	task	event_data.User	event_data.ParentImage	event_data.Image	event_data.CommandLine
▶ November 7th 2017, 21:17:29.420	pc0002.test.local	Process Create (rule: ProcessCreate)	TEST\dadmin	C:\Windows\System32\cmd.exe	C:\Windows\System32\reg.exe	<code>reg save \\172.16.205.140\hklm\sam sam.hive</code>
▶ November 7th 2017, 21:05:49.753	WIN-FJRNSLDJHD2.test.local	Process Create (rule: ProcessCreate)	TEST\Administrator	C:\Windows\System32\cmd.exe	C:\Windows\System32\reg.exe	<code>reg save hklm\sam sam.hive</code>
▶ November 7th 2017, 21:01:51.430	WIN-FJRNSLDJHD2.test.local	Process Create (rule: ProcessCreate)	TEST\Administrator	C:\Windows\System32\cmd.exe	C:\Windows\System32\reg.exe	<code>reg save hkey_local_machine\system system.hive</code>
▶ November 7th 2017, 21:01:21.135	WIN-FJRNSLDJHD2.test.local	Process Create (rule: ProcessCreate)	TEST\Administrator	C:\Windows\System32\cmd.exe	C:\Windows\System32\reg.exe	<code>reg save hklm\security security.hive</code>



Event Properties - Event 5145, Microsoft Windows security auditing.

General

Details

A network share object was checked to see whether client can be granted desired access.

Subject:

Security ID:	TEST\dadmin
Account Name:	dadmin
Account Domain:	TEST
Logon ID:	0x5C1A54

Account and IP
used to access
Remote Registry

Network Information:

Object Type:	File
Source Address:	172.16.205.151
Source Port:	63017

Share Information:

Share Name:	*\IPC\$
Share Path:	
Relative Target Name:	winreg

Remote registry service pipe

Access Request Information:

Access Mask:	0x12019F
Accesses:	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) ReadEA WriteEA

Dumping from SAM/SYSTEM/SECURITY
Grabbing via remote registry. Lets hunt it!

*event_id:5145 AND
event_data.RelativeTargetName:winreg AND -
event_dataIpAddress:(192.168.7.9 192.168.7.19) ← IP
addresses of admin workstations*

Time	computer_name	event_data.SubjectUserName	event_data.SubjectDomainName	event_data.ShareName	event_data.RelativeTargetName	event_dataIpAddress
November 7th 2017, 21:17:29.260	WIN-FJRNSDLJHD2.test.local	dadmin	TEST	*\IPC\$	winreg	172.16.205.151
November 7th 2017, 20:00:59.039	WIN-FJRNSDLJHD2.test.local	dadmin	TEST	*\IPC\$	winreg	172.16.205.151



DCSync is a variation on credential dumping which can be used to acquire sensitive information from a domain controller. The action works by simulating a domain controller replication process from a remote domain controller.

Any member of Administrators, Domain Admins, or Enterprise Admins as well as Domain Controller computer accounts are able to run DCSync to pull to pull credential data.

Tools: Mimikatz, secretsdump.py from Impacket

Dumping from NTDS.dit remotely DCSync

```
mimikatz # lsadump::dcsync /domain:test.local /user:krbtgt
[DC] 'test.local' will be the domain
[DC] 'WIN-FJRNSLDJHD2.test.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN : krbtgt

** SAM ACCOUNT **

SAM Username : krbtgt
Account Type : 30000000 < USER_OBJECT >
User Account Control : 00000202 < ACCOUNTDISABLE NORMAL_ACCOUNT >
Account expiration :
Password last change : 8/28/2016 12:22:25 AM
Object Security ID : S-1-5-21-1729715525-4152589049-1868270738-502
Object Relative ID : 502

Credentials:
Hash NTLM: c77d9f2311bd9d26073452fe484c3acc
  ntlm- 0: c77d9f2311bd9d26073452fe484c3acc
  lm - 0: 450245c0e6ec5accbb85d9320377b2cc
```

How it works:

- discovers Domain Controller in the specified domain name.
- requests the Domain Controller replicate the user; credentials via GetNCChanges (leveraging [Directory Replication Service \(DRS\) Remote Protocol](#)).



Dumping from NTDS.dit remotely DCSync. Windows events

Event Properties - Event 4624, Microsoft Windows security auditing.

General	Details
An account was successfully logged on.	
Subject:	Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0
Logon Type:	3
Impersonation Level:	Identification
New Logon:	Security ID: TEST\dadmin Account Name: dadmin Account Domain: TEST Logon ID: 0x6B0B8F Logon GUID: {85745003-48fe-4e3c-8f3d-000000000000}
Process Information:	Process ID: 0x0 Process Name: -
Network Information:	Workstation Name: 172.16.205.151 Source Network Address: 172.16.205.151 Source Port: 49974
Detailed Authentication Information:	
Logon Process: Kerberos Authentication Package: Kerberos Transited Sspi	

Event Properties - Event 4662, Microsoft Windows security auditing.

General	Details
An operation was performed on an object.	
Subject :	Security ID: TEST\dadmin Account Name: dadmin Account Domain: TEST Logon ID: 0x6B0B8F
Object:	Object Server: DS Object Type: domainDNS Object Name: DC=test,DC=local Handle ID: 0x0
Operation:	Operation Type: Object Access Accesses: Control Access Access Mask: 0x100 Properties: {1131f6ad-9c07-11d1-f79f-00c04fc2dcfd2} {19195a5b-6da0-11d0-af3d-00c04fd930c9}

Event Properties - Event 4662, Microsoft Windows security auditing.

General	Details
An operation was performed on an object.	
Subject :	Security ID: TEST\dadmin Account Name: dadmin Account Domain: TEST Logon ID: 0x6B0B8F
Object:	Object Server: DS Object Type: domainDNS Object Name: DC=test,DC=local Handle ID: 0x0
Operation:	Operation Type: Object Access Accesses: Control Access Access Mask: 0x100 Properties: {1131f6aa-9c07-11d1-f79f-00c04fc2dcfd2} {19195a5b-6da0-11d0-af3d-00c04fd930c9}

DS-Replication-Get-Changes-All

DS-Replication-Get-Changes-All

www.zeronights.org #zeronights



Benjamin Delpy
@gentilkiwi



Following

#mimikatz DCSync make logs with 'Directory Service Access' DS-Replication-Get-Changes*

Except if you use a DC account

Dumping from NTDS.dit remotely
DCSync using Domain Controller account

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [W] Name

Saved Queries

Delegate Control...

Find...

Change Domain...

Change Domain Controller...

Raise domain functional level...

Operations Masters...

New

All Tasks

View

Refresh

Export List...

Properties

Advanced Security Settings for test

Owner: Administrators (TEST\Administrators) Change

Permissions Auditing Effective Access

For additional information, double-click an audit entry. To modify an audit entry, select it and click the Change button.

Auditing entries:

Type	Principal	Access	Inherited From
Succ...	Everyone	None	None
Succ...	Administrator (TEST\Administrators)	Replicating Directory Changes All	None
Succ...	Administrator (TEST\Administrators)	Replicating Directory Changes	None
Succ...	Administrator (TEST\Administrators)	Replication synchronization	None
Succ...	Administrator (TEST\Administrators)	Replicating Directory Changes All	None
Succ...	Administrator (TEST\Administrators)	None	None
Succ...	Administrator (TEST\Administrators)	None	None
Succ...	Administrator (TEST\Administrators)	None	None
Succ...	Administrator (TEST\Administrators)	None	None
Succ...	Domain Controllers (TEST\DC...)	Replicating Directory Changes All	None

Event Properties - Event 4662, Microsoft Windows security auditing

An operation was performed on an object.

Subject:

Security ID:	TEST\WIN-FJRNSLDJHD2\$
Account Name:	WIN-FJRNSLDJHD2\$
Account Domain:	TEST
Logon ID:	0x7483C4

Object:

Object Server:	DS
Object Type:	domainDNS
Object Name:	DC=test,DC=local
Handle ID:	0x0

Operation:

Operation Type:	Object Access
Accesses:	Control Access
Access Mask:	0x100
Properties:	Control Access
	{1131f6ad-9c07-11d1-f79f-00c04fc2cd2}
	{19195a5b-6da0-11d0-af3d-00c04fd930c9}
	This object and all descendants

NO PROBLEM BRO

www.zeronights.org #zeronights



Dumping from NTDS.dit remotely
DCSync. Lets hunt it!

`event_id:4662 AND event_data.Properties:("{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}"
 "{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}") AND computer_name:("WIN-FJRNSDLJHD2.test.local" "dc2.test.local") ← DCs`

Time ▾	computer_name	task	event_data.SubjectDomainName	event_data.SubjectUserName	event_data.SubjectLogonId	event_data.Properties	event_data.ObjectName
▶ November 7th 2017, 23:20:10.830	WIN-FJRNSDLJHD2.test.local	Director y Service Access	TEST	WIN-FJRNSDLJHD2\$	0x7483c4	%%7688 {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}	%{57172572-b013-4847-953c-59df53ff6adb}
▶ November 7th 2017, 23:07:33.400	WIN-FJRNSDLJHD2.test.local	Director y Service Access	TEST	dadmin	0x6b0b8f	%%7688 {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}	%{57172572-b013-4847-953c-59df53ff6adb}
▶ November 7th 2017, 23:07:33.400	WIN-FJRNSDLJHD2.test.local	Director y Service Access	TEST	dadmin	0x6b0b8f	%%7688 {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}	%{57172572-b013-4847-953c-59df53ff6adb}

`event_id:4624 AND event_data.TargetLogonId:(0x7483c4 0x6b0b8f) AND -
event_data.ipAddress:(“172.16.205.140”“172.16.205.141”) ← Our DCs`

Time ▾	computer_name	task	event_data.ipAddress	event_data.TargetUserName	event_data.TargetLogonId	event_data.TargetDomainName	event_data.LogonType
▶ November 7th 2017, 23:20:10.827	WIN-FJRNSDLJHD2.test.local	Logon	172.16.205.151	WIN-FJRNSDLJHD2\$	0x7483c4	TEST	3
▶ November 7th 2017, 22:43:49.979	WIN-FJRNSDLJHD2.test.local	Logon	172.16.205.151	dadmin	0x6b0b8f	TEST	3



Based on [MS-NRPC] - Netlogon Remote Protocol Tools: Mimikatz

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:dc-1$ /domain:lab.local /ntlm:9c4070e01743ee86055583d0ee5d2366 /impersonate
user    : dc-1$  

domain  : lab.local  

program : C:\Users\Gentil Kiwi\Desktop\mimikatz.exe  

impers. : yes  

NTLM   : 9c4070e01743ee86055583d0ee5d2366
| PID 2096
| TID 2276
| LUID 0 ; 516056 (00000000:0007dfd8)
\ msrv1_0 - data copy @ 0000000003A4620 : OK !
\ kerberos - data copy @ 0000000000334EF8
  \ aes256_hmac    -> null
  \ aes128_hmac    -> null
  \ rc4_hmac_nt    OK
  \ rc4_hmac_old   OK
  \ rc4_md4        OK
  \ rc4_hmac_nt_exp OK
  \ rc4_hmac_old_exp OK
  \ *Password replace -> null
** Token Impersonation **

mimikatz # lsadump::netsync /dc:dc-0.lab.local /user:dc-1$ /ntlm:9c4070e01743ee86055583d0ee5d2366 /account:client-0$  

Account: client-0$  

NTLM  : 33e9a68cf9727fc3b1fcff46226a41b7  

NTLM-1 : 31d6cfe0d16ae931b73c59d7e0c089c0

mimikatz # lsadump::netsync /dc:dc-0.lab.local /user:dc-1$ /ntlm:9c4070e01743ee86055583d0ee5d2366 /account:dc-0$  

Account: dc-0$  

NTLM  : 8cf9f2e33b4a12f5ba2833a797e6dba7  

NTLM-1 : 31d6cfe0d16ae931b73c59d7e0c089c0
```

Dumping from NTDS.dit remotely NetSync

- Ben Campbell @Meatballs_ · 24 мая 2016 г.
В ответ @gentilkiwi
Whats diff between this and dcsyncing specific users?
Язык твита: английский
- 1 1 1 1
- Benjamin Delpy @gentilkiwi · 24 мая 2016 г.
1. DC\$ rights needed (no domain admins)
2. only get NTLM/RC4 keys
3. only for DC/SRV/WKS (no users)
Язык твита: английский
- 2 1 3 1
- Benjamin Delpy @gentilkiwi · 24 мая 2016 г.
and of course: very legacy protocol :) (nrpc)
Язык твита: английский
- 1 2 1 1
- Raiona @Raiona_ZA · 29 мая 2016 г.
So this is dcsync for computer accounts that uses an ancient protocol? Gotta love MS for giving us options :)
Язык твита: английский
- 1 1 1 1
- Benjamin Delpy @gentilkiwi · 29 мая 2016 г.
some will say it's a castrated DCSync, some will say it's enough to play with silver tickets ;)



Dumping from NTDS.dit remotely NetSync. Windows events

Event Properties - Event 4624, Microsoft Windows security

General	
Details	
An account was successfully logged on.	
Subject:	
Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0
Logon Type:	3
Impersonation Level:	Delegation
New Logon:	
Security ID:	TEST\WIN-FJRNSLDJHD2\$
Account Name:	WIN-FJRNSLDJHD2\$
Account Domain:	TEST
Logon ID:	0x807E8B
Logon GUID:	{f2fb59c8-3577-e26e-3be2-349d195389c6}
Process Information:	
Process ID:	0x0
Process Name:	-
Network Information:	
Workstation Name:	
Source Network Address:	172.16.205.151
Source Port:	61071
Detailed Authentication Information:	
Logon Process:	Kerberos
Authentication Package:	Kerberos
Transited Sspi	

Event Properties - Event 5145, Microsoft Windows security auditing.

General	
Details	
A network share object was checked to see whether client can be granted desired access.	
Subject:	
Security ID:	TEST\WIN-FJRNSLDJHD2\$
Account Name:	WIN-FJRNSLDJHD2\$
Account Domain:	TEST
Logon ID:	0x807E8B
Network Information:	
Object Type:	File
Source Address:	172.16.205.151
Source Port:	61071
Share Information:	
Share Name:	*\IPC\\$
Share Path:	
Relative Target Name:	NETLOGON
Access Request Information:	
Access Mask:	0x12019F
Accesses:	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) ReadEA WriteEA



Credentials dumping tools artefacts

	Services	Dropped files	Pipes
Mimikatz	mimikatz service (mimikatzsvc)/*\path to mimikatz binary mimikatz driver (mimidrv)/*\mimidrv.sys	*.kirbi	-
wce	WCESERVICE/*\service image file like GUID	wce_ccache, wce_krbtkts, wceaux.dll	WCEServicePipe
samex	-	SAM.out, NTDS.out, SYSTEM.out	-
PWDumpX	PWDumpX Service / *\DumpSvc.exe	DumpExt.dll, DumpSvc.exe, *-PwHashes.txt	-
cachedump	-	-	\cachedumppipe
lsadump	-	-	\lsadump*
pwdump6	service name like GUID	lsremora.dll, lsremora64.dll, test.pwd	-
fgdump	fgexec/*\fgexec.exe Cachedump/*\cachedump.exe Cachedump/*\cachedump64.exe service name like GUID/*\servpw.exe service name like GUID/*\servpw64.exe	fgexec.exe, pwdump.exe, pstgdump.exe, lsremora.dll, lsremora64.dll, cachedump.exe, cachedump64.exe, servpw64.exe, servpw.exe, test.pwd, *.pwdump, *.fgdump-log	-



Credentials dumping tools artefacts Services. Windows events

Event Properties - Event 7045, Service Control Manager

General Details PWDump6

A service was installed in the system.

Service Name: {2B44C303-F2AF-40D4-9032-0864E330620F}

Service File Name: C:\Windows\cioy.exe

Service Type: user mode service

Service Start Type: demand start

Service Account: LocalSystem

Event Properties - Event 7045, Service Control Manager

General Details Windows Credentials Editor (WCE)

A service was installed in the system.

Service Name: WCESERVICE

Service File Name: C:\Users\ADMINI~1\AppData\Local\Temp\2\9e52cbe2-8847-44bf-8add-b0a360d3ece0.exe -S

Service Type: user mode service

Service Start Type: demand start

Service Account: LocalSystem

Event Properties - Event 7045, Service Control Manager

General Details PWDumpX

A service was installed in the system.

Service Name: {34FEE665-AB06-4A9F-9A4B-926A9D6EAD89}

Service File Name: C:\tools\PwDump6\servpw64.exe

Service Type: user mode service

Service Start Type: demand start

Service Account: LocalSystem

Event Properties - Event 7045, Service Control Manager

General Details Mimikatz RPC service

A service was installed in the system.

Service Name: mimikatz service (mimikatzsvc)

Service File Name: "C:\tools\mimikatz\x64\notepad.exe" rpc::server service::me exit

Service Type: user mode service

Service Start Type: auto start

Service Account: LocalSystem



Credentials dumping tools artefacts Services. Lets hunt it!

```
event_id:7045 AND (event_data.ServiceName:(fgexec cachedump *mimikatz*  
*mimidrv* WCESERVICE *pwdump*) OR event_data.ImagePath:(*fgexec* *dumpsvc*  
*mimidrv* *cachedump* *servpw* *gsecdump* *pwdump*) OR  
event_data.ImagePath.raw:/(\|\|.*\|.*.*\[\{]?[0-9A-Fa-f]{8}-[0-9A-Fa-f]{4}-[0-9A-Fa-  
f]{4}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{12}\[\]?\.exe|scr|cpl|bat|js|cmd|vbs).*/)
```

Time	computer_name	event_data.ServiceName	event_data.ImagePath
► November 16th 2017, 03:11:39.310	pc0002.test.local	fgexec	C:\Windows\fgexec.exe -s -n {EB1FA0F9-DE85-42F1-98EC-3AFFF3A0B392}
► November 16th 2017, 02:57:31.970	pc0002.test.local	CacheDump	"C:\Windows\cachedump.exe" -s
► November 16th 2017, 02:04:43.671	WIN-FJRNSLDJHD2.test.local	mimikatz driver (mimidrv)	C:\tools\mimikatz\x64\mimidrv.sys
► November 8th 2017, 14:07:23.627	WIN-FJRNSLDJHD2.test.local	WCESERVICE	C:\Users\ADMINI~1\AppData\Local\Temp\2\9e52cbe2-8847-44bf-8add-b0a360d3ece0.exe -S
► November 8th 2017, 02:50:39.349	pc0002.test.local	PWDumpX Service	%windir%\system32\DumpSvc.exe
► November 7th 2017, 20:08:39.534	pc0002.test.local	mimikatz service (mimikatzsvc)	"C:\tools\mimikatz\win32\mimikatz.exe" rpc::server service::me exit
► November 7th 2017, 15:43:43.123	WIN-FJRNSLDJHD2.test.local	{7467EBD3-E0C5-42DB-BCA7-8B723867B52B}	C:\Users\ADMINI~1\AppData\Local\Temp\2\servpw64.exe
► November 7th 2017, 12:34:28.725	WIN-FJRNSLDJHD2.test.local	CacheDump	"C:\Users\ADMINI~1\AppData\Local\Temp\2\cachedump64.exe" -s



Credentials dumping tools artefacts Dropped files. Sysmon events

Event Properties - Event 11, Sysmon

Windows Credentials Editor (WCE)

General Details

File created:
UtcTime: 2017-11-08 11:07:29.628
ProcessGuid: {d134eb5b-e571-5a02-0000-0010e3b0d700}
ProcessId: 26044
Image: C:\Users\ADMINI~1\AppData\Local\Temp\2\48b2cbae-01ea-4f47-a0ef-0203269de481.exe
TargetFilename: C:\tools\wce_ccache
CreationUtcTime: 2017-11-05 15:07:38.664

Event Properties - Event 11, Sysmon

Windows Credentials Editor (WCE)

General Details

File created:
UtcTime: 2017-11-08 11:07:29.631
ProcessGuid: {d134eb5b-e571-5a02-0000-0010e3b0d700}
ProcessId: 26044
Image: C:\Users\ADMINI~1\AppData\Local\Temp\2\48b2cbae-01ea-4f47-a0ef-0203269de481.exe
TargetFilename: C:\tools\wce_krbtkts
CreationUtcTime: 2017-11-05 15:07:38.667

Event Properties - Event 11, Sysmon

PWDumpX

General Details

File created:
UtcTime: 2017-11-07 23:48:04.779
ProcessGuid: {d134eb5b-4633-5a02-0000-0010ef5cb900}
ProcessId: 24272
Image: C:\tools\PWDumpX 1.4\PWDumpX.exe
TargetFilename: C:\tools\PWDumpX 1.4\172.16.205.151-PWHashes.txt
CreationUtcTime: 2017-11-07 23:43:49.830

Event Properties - Event 11, Sysmon

Mimikatz

General Details

File created:
UtcTime: 2017-11-07 15:24:01.075
ProcessGuid: {d134eb5b-d00d-5a01-0000-001061191800}
ProcessId: 4780
Image: C:\tools\mimikatz\x64\notepad.exe
TargetFilename: C:\tools\mimikatz\x64\[0;3e7]-2-2-40e10000-WIN-FJRNSLDJHD2\$@krbtgt-TEST.LOCAL.kirbi
CreationUtcTime: 2017-11-07 15:20:13.389



event_id:11 AND event_data.TargetFilename:(/*|\test.pwd"/*|\Isremora.dll" /*|\Isremora64.dll" /*|\fexec.exe" *pwdump* *kirbi /*|\wce_ccache" /*|\wce_krbtkts" /*|\wceaux.dll" *PwHashes* /*|\SAM.out" /*|\SECURITY.out" /*|\SYSTEM.out" /*|\NTDS.out" /*|\DumpExt.dll" /*|\DumpSvc.exe" /*|\cachedump64.exe" /*|\cachedump.exe" /*|\pstgdump.exe" /*|\servpw64.exe" /*|\servpw.exe" /*|\pwdump.exe" /*|fgdump-log*)

Time	computer_name	task	event_data.Image	event_data.TargetFilename
► November 8th 2017, 14:07:29.631	WIN-FJRNLDJHD2.test.local	File created (rule: FileCreate)	C:\Users\ADMINI~1\AppData\Local\Temp\2\48b2cbae-01ea-4f47-a0ef-0203269de481.exe	C:\tools\wce_krbtkts
► November 8th 2017, 14:07:29.630	WIN-FJRNLDJHD2.test.local	File created (rule: FileCreate)	C:\Users\ADMINI~1\AppData\Local\Temp\2\48b2cbae-01ea-4f47-a0ef-0203269de481.exe	C:\tools\wce_ccache
► November 8th 2017, 14:07:23.642	WIN-FJRNLDJHD2.test.local	File created (rule: FileCreate)	C:\Users\ADMINI~1\AppData\Local\Temp\2\9e52cbe2-8847-44bf-8add-b0a360d3ece0.exe	C:\Windows\Temp\wceaux.dll
► November 8th 2017, 03:10:52.137	pc0002.test.local	File created (rule: FileCreate)	C:\Windows\Explorer.EXE	C:\tools\cachedump-1.0\cachedump.exe
► November 8th 2017, 02:50:40.198	WIN-FJRNLDJHD2.test.local	File created (rule: FileCreate)	C:\tools\PWDumpX 1.4\PWDumpX.exe	C:\tools\PWDumpX 1.4\172.16.205.151-PwHashes.txt
► November 8th 2017, 02:50:39.337	pc0002.test.local	File created (rule: System FileCreate)		C:\Windows\System32\DumpExt.dll
► November 8th 2017, 02:50:39.332	pc0002.test.local	File created (rule: System FileCreate)		C:\Windows\System32\DumpSvc.exe
► November 8th 2017, 02:11:21.108	pc0002.test.local	File created (rule: System FileCreate)		C:\Windows\Isremora.dll
► November 8th 2017, 02:06:32.633	pc0002.test.local	File created (rule: System FileCreate)		C:\Windows\test.pwd
► November 7th 2017, 20:39:34.902	WIN-FJRNLDJHD2.test.local	File created (rule: FileCreate)	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe	C:\tools\[0;3e7]-2-2-40e10000-WIN-FJRNLDJHD2\$@krbtgt-TEST.LOCAL.kit

Credentials dumping tools artefacts
Dropped files. Lets hunt it!



Credentials dumping tools artefacts Named pipes. Sysmon events

Event Properties - Event 17, Sysmon

General Details Windows Credentials Editor (WCE)

Pipe Created:
UtcTime: 2017-11-08 11:07:23.638
ProcessGuid: {d134eb5b-e56b-5a02-0000-0010caa3d700}
ProcessId: 26496
PipeName: \WCEServicePipe
Image: C:\Users\ADMINI~1\AppData\Local\Temp\2\9e52cbe2-8847-44bf-8add-b0a360d3ece0.exe

Event Properties - Event 17, Sysmon

General Details Cachedump

Pipe Created:
UtcTime: 2017-11-08 00:20:21.223
ProcessGuid: {3261c166-4dc5-5a02-0000-0010792ba400}
ProcessId: 5580
PipeName: \cachedumppipe
Image: C:\tools\cachedump-1.0\cachedump.exe

Event Properties - Event 17, Sysmon

General Details LSADump

Pipe Created:
UtcTime: 2017-11-08 00:11:31.631
ProcessGuid: {3261c166-4bb3-5a02-0000-001058239e00}
ProcessId: 4228
PipeName: \lsadump2-4228
Image: C:\tools\lsadump2.exe



Credentials dumping tools artefacts Named pipes. Lets hunt it!

`source_name:"Microsoft-Windows-Sysmon" AND event_id:17 AND event_data.PipeName:(*lsadump* *cachedump* *WCEServicePipe*)`

Time ▾	computer_name	task	event_data.Image	event_data.ProcessId	event_data.PipeName
▶ November 8th 2017, 14:07:23.638	WIN-FJRNSLDJHD2.test.local	Pipe Created (rule: PipeEvent)	C:\Users\ADMINI~1\AppData\Local\Temp\2\9e52cb e2-8847-44bf-8add-b0a360d3ece0.exe	26496	\WCEServicePipe
▶ November 8th 2017, 03:20:21.223	pc0002.test.local	Pipe Created (rule: PipeEvent)	C:\tools\cachedump-1.0\cachedump.exe	5580	\cachedumppipe
▶ November 8th 2017, 03:11:31.632	pc0002.test.local	Pipe Created (rule: PipeEvent)	C:\tools\lsadump2.exe	4228	\lsadump2-4228



Credentials dumping tools artefacts Mimikatz command line

event_id:1 AND (event_data.CommandLine:(*DumpCreds* *invoke-mimikatz*) OR (event_data.CommandLine:(*rpc* *token* *crypto* *dpapi* *sekurlsa* *kerberos* *lsadump* *privilege* *process*) AND event_data.CommandLine.raw:*\\:*))

Time ▾	computer_name	task	event_data.Image	event_data.CommandLine
▶ November 16th 2017, 02:48:48.213	pc0002.test.local	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	"C:\Windows\System32\cmd.exe" /c C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit >> C:\Users\Public\result.txt
▶ November 7th 2017, 20:07:59.545	pc0002.test.local	Process Create (rule: ProcessCreate)	C:\tools\mimikatz\win32\mimikatz.exe	" token::elevate service::+ exit "
▶ November 7th 2017, 18:54:19.286	WIN-FJRNSLDJHD2.test.local	Process Create (rule: ProcessCreate)	C:\tools\mimikatz\x64\notepad.exe	" privilege::debug sekurlsa::logonpasswords sekurlsa::tickets /export "

event_id:4688 AND (event_data.CommandLine:(*DumpCreds* *invoke-mimikatz*) OR (event_data.CommandLine:(*rpc* *token* *crypto* *dpapi* *sekurlsa* *kerberos* *lsadump* *privilege* *process*) AND event_data.CommandLine.raw:*\\:*))

Time ▾	computer_name	event_id	event_data.NewProcessName	event_data.CommandLine
▶ November 16th 2017, 21:35:44.151	WIN-FJRNSLDJHD2.test.local	4,688	C:\tools\mimikatz\x64\notepad.exe	"C:\tools\mimikatz\x64\notepad.exe" rpc::server service::me exit
▶ November 16th 2017, 02:48:47.859	pc0002.test.local	4,688	C:\Windows\System32\cmd.exe	"C:\Windows\System32\cmd.exe" /c C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit >> C:\Users\Public\result.txt
▶ November 7th 2017, 20:07:59.519	pc0002.test.local	4,688	C:\tools\mimikatz\win32\mimikatz.exe	" token::elevate service::+ exit "
▶ November 7th 2017, 18:54:19.256	WIN-FJRNSLDJHD2.test.local	4,688	C:\tools\mimikatz\x64\notepad.exe	" privilege::debug sekurlsa::logonpasswords sekurlsa::tickets /export "



Hunting for credentials dumping by AV detects

	Kaspersky	Microsoft	Symantec	TrendMicro
mimikatz	Exploit.Win32.Palsas.vyl HackTool.Win32.Mimikatz.gen	HackTool:Win32/Mimikatz	Hacktool.Mimikatz	HKTL_MIMIKATZ64.A HKTL_MIMIKATZ
Gsecdump	PSWTool.Win64.Gsecdmp.e	HackTool:Win32/Gsecdump	Hacktool.PTHToolkit	HKTL_PWDUMP
Fgdump	PSWTool.Win32.PWDump.f	HackTool:Win32/Fgdump	Pwdump	HKTL_FGDUMP
WCE	HackTool.Win32.WinCred.e	HackTool:Win32/Wincred.G	SecurityRisk.WinCredEd	HKTL_WINCRED
PWDumpX	HackTool.Win32.PWDump.a	HackTool:Win32/PWDumpX	-	HKTL_PWDUMP.SM
Cachedump	PSWTool.Win32.CacheDump.a	HackTool:Win32/Cachedump	Trojan.Gen.NPE	HKTL_PWDUMPPBD
Pwdump6	PSWTool.Win32.PWDump.lv	HackTool:Win64/PWDump HackTool:Win32/PWDump.A	Pwdump	HKTL_PWDUMP
pwdump7	PSWTool.Win32.PWDump.bve	HackTool:Win32/PWDump.l	Pwdump	HKTL_PWDUMP
lsadump	HackTool.Win32.Lsadump.a	-	Hacktool.LSADump	-
samex	HackTool.Win32.Samer.a	-	-	-

**ASK ME
QUESTIONS!**